NOKIA

7450 ETHERNET SERVICE SWITCH
7750 SERVICE ROUTER
7950 EXTENSIBLE ROUTING SYSTEM
VIRTUALIZED SERVICE ROUTER

BASIC SYSTEM CONFIGURATION GUIDE
RELEASE 21.5.R1

3HE 17141 AAAB TQZZA 01

Issue: 01

May 2021

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of Contents

1 Getting Started

1.1 About This Guide

This guide describes system concepts and provides configuration explanations and examples to configure SR OS boot option file (BOF), file system and system management functions. For information on the concepts and descriptions of the classic Command Line Interface (CLI) syntax and command usage, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow.

The topics and commands described in this document apply to the:

- 7450 ESS
- 7750 SR
- 7950 XRS
- VSR

Table 1 lists the available chassis types for each SR OS router.

Table 1 **Supported SR OS Router Chassis Types**

7450 ESS	7750 SR	7950 XRS
• 7450 ESS-7/12	• 7750 SR-a4/a8 • 7750 SR-1e/2e/3e • 7750 SR-12e • 7750 SR-1 • 7750 SR-7/12 • 7750 SR-1s/2s • 7750 SR-7s/14s	• 7950 XRS-16c • 7950 XRS-20/40 • 7950 XRS-20e

For a list of unsupported features by platform and chassis, refer to the SR OS 21.*x*.R*x* Software Release Notes, part number 3HE 17177 000*x* TQZZA.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.

Note: The SR OS CLI trees and command descriptions can be found in the following guides:

- *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*
- *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Show, and Tools Command Reference Guide* (for both MD-CLI and Classic CLI)
- *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*

Note: This guide generically covers Release 21.*x*.R*x* content and may contain some content that will be released in later maintenance loads. Refer to the SR OS 21.*x*.R*x* Software Release Notes, part number 3HE 17177 000*x* TQZZA, for information about features supported in each load of the Release 21.*x*.R*x* software.

1.2 Router System Configuration Process

Table 2 lists the tasks necessary to configure boot option files (BOF) and system and file management functions. Each chapter in this book is presented in an overall logical configuration flow. Each section describes a software area and how to configure parameters for a functional area. After the hardware installation has been properly completed, proceed with the router configuration tasks in the following order:

Table 2 **Configuration Process**

Area	Task	Section
Operational functions	Directory and file management	File Management Tasks in the Classic CLI File Management Tasks in the MD-CLI
Boot options	Configure boot option files (BOF)	Configuring Boot Options File with CLI
	Service management	System Administration Commands in the Classic CLI
Zero touch provisioning	ZTP Overview	ZTP Overview
	ZTP Processes	ZTP Processes

Table 2 **Configuration Process (Continued)**

Area	Task	Section (Continued)
System configuration	Perform administrative tasks	Administrative Tasks
	Configure system management features	Configuring System Management with CLI
	Configure system parameters	Common Configuration Tasks
	Configure system timing	System Timing
	Configure system monitoring thresholds	Configuring System Monitoring Thresholds
	Configure LLDP	Configuring LLDP
	Configure satellite parameters	Satellite Configuration

2 File System Management

2.1 The File System

The SR OS file system is used to store files used and generated by the system, for example, image files, configuration files, logging files and accounting files.

The file commands allow you to copy, create, move, and delete files and directories, navigate to a different directory, display file or directory contents and the image version.

Although some of the storage devices on routers are not actually compact flash devices (for example, cf1: on the 7950 XRS is an internal SSD), we refer to all storage devices as compact flash.

2.1.1 Storage Devices

The file system is based on a DOS file system. In the 7750 SR and 7450 ESS, each control processor can have up to three storage devices numbered one through three. In the 7950 XRS, each CCM has an SSD and up to two compact flash devices. The names for these devices are:

- cf1:
- cf2:
- cf3:

The above device names are *relative* device names as they refer to the devices local to the control processor with the current console session. As in the DOS file system, the colon (":") at the end of the name indicates it is a device.

The three compact flash devices on the 7450 ESS and 7750 SR OS are removable and have an administrative state.

The cf2: and cf3: compact flash devices on the 7950 XRS routers are removable and have an administrative state. cf1: is an internal SSD.

Devices vary by platform as compact flash, SD card, USB, or embedded SSD. The format used for the removable storage devices is DOS FAT32. The maximum size supported is 32 GB.

Note: To prevent corrupting open files in the file system, you should only remove a compact flash that is administratively shutdown. SR OS gracefully closes any open files on the device, so it can be safely removed.

2.1.2 URLs

The arguments for the SR OS file commands are modeled after standard universal resource locater (URL). A URL refers to a file (a *file-url*) or a directory (a *directory-url*).

The SR OS supports operations on both the local file system and on remote files. For the purposes of categorizing the applicability of commands to local and remote file operations, URLs are divided into five types of URLs: local, ftp, tftp, http, and https. The syntax for each of the URL types are listed in Table 3.

Table 3 **URL Types and Syntax**

URL Type	Syntax	Notes
local-url	[*cflash-id*:\]*path*	*cflash-id* is the compact flash device name. Values: cf1:, cf2:, cf3:
ftp-url	**ftp://**[*username*[**:***password*]**@**]*host*/*path*	An absolute ftp path from the root of the remote file system. *username* is the ftp user name *password* is the ftp user password *host* is the remote host *path* is the path to the directory or file
	ftp://[*username*[**:***password*]**@**]*host*/**.**/*path*	A relative ftp path from the user's home directory. Note the period and slash ("**./**") in this syntax compared to the absolute path.
tftp-url	**tftp://***host*[/*path*]/*filename*	tftp is only supported for operations on file-urls.
http-url	**http://***[username[:password]@]host*[*:port*]/*path*	*host* is an HTTP server *port* defaults to 80
https-url	**https://** *[username[:password]@]host*[*:port*]/*path*	*host* is an HTTPS server *port* defaults to 443

If the host portion of the URL is an IPv6 address, then the address should be enclosed in square brackets. For example:

ftp://user:passw@[3ffe::97]/./testfile.txt

tftp://[2001:db8:3333:4444:5555:6666:7777:8888]/./testfile.txt

The system accepts either forward slash (/) or backslash (\) characters to delimit directory and/or filenames in URLs. Similarly, the SR OS SCP client application can use either slash or backslash characters, but not all SCP clients treat backslash characters as equivalent to slash characters. In particular, UNIX systems will often times interpret the backslash character as an escape character. This can cause problems when using an external SCP client application to send files to the SCP server. If the external system treats the backslash like an escape character, the backslash delimiter will get stripped by the parser and will not be transmitted to the SCP server.

For example, a destination directory specified as “cf1:\dir1\file1” will be transmitted to the SCP server as “cf1:dir1file1” where the backslash escape characters are stripped by the SCP client system before transmission. On systems where the client treats the backslash like an escape character, a double backslash (\\) or the forward slash (/) can typically be used to properly delimit directories and the filename.

When a special character is used in a password, it can cause issues when that password is encoded as part of a URL. To prevent this issue, percent encoding can be used. Percent encoding is a mechanism to encode 8-bit characters that have specific meaning in the context of URLs. The encoding consists of substitution of a percent character (%) followed by the hexadecimal representation of the ASCII value of the replaced character.

Some file manipulation commands such as copying, removing, or moving files, may request access to an HTTP or HTTPS server. If an HTTP or HTTPS server redirects the system to a different URL (from an "HTTP 301" error or similar response), the system prompts the user "y/n" to either repeat the operation with the new URL or terminate it. These file commands can be configured to force the HTTP redirects without prompting or they can be configured to refuse HTTP redirects. If a file command is redirected more than eight times, or if it queries an HTTPS URL and gets redirected to an HTTP URL, the command automatically terminates as a security measure.

For example, to refuse HTTP redirects, use the **no-redirect** parameter in the classic CLI command.

Example: `A:n-2>file cf3:\ # copy source-url dest-url no-redirect`

To refuse HTTP redirects with the MD-CLI command, use the **direct-http** parameter.

Example:
```
[file "cf3:\"]
A:admin@node-2# copy source-url destination-url direct-
 http
```

To force the HTTP redirects without prompting, use the **force** parameter in either the classic CLI or the MD-CLI.

CLI Syntax: `(Classic): # copy source-url dest-url force`

CLI Syntax: `(MD-CLI): # copy source-url destination-url force`

When connecting to an HTTPS server, the system verifies the server's TLS certificate. For the certificate to pass verification, the system must have a CA profile already configured for the server's Certificate Authority (CA), which specifies up-to-date certificate and CRL files. HTTPS file commands do not use the Online Certificate Status Protocol (OCSP). If the certificate was issued by an intermediate CA, the system must have a CA profile for every CA tracing back to the root CA. If the server's certificate fails verification for any reason, the file command terminates. Refer to the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter and Extended Services Appliance Guide* for more information about CA profiles.

The CLI command to configure the CA profile is in the **configure system security pki ca-profile** context.

An HTTPS **file** command may also include a **client-tls-profile** parameter, referring to a client TLS profile that provides the cipher list, client certificate, and trust anchor the system uses when communicating with the HTTPS server. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide* for more information about client TLS profiles.

A **file** command that connects to an HTTP or HTTPS server outside the local network may need to use an HTTP proxy. The user may add the **proxy** parameter to point to a proxy server (which must be an HTTP URL).

2.1.3 Wildcards and Special Characters

SR OS supports the standard DOS wildcard characters. The asterisk (*) can represent zero or more characters in a string of characters. The question mark (?) represents any one character and must be enclosed in quotation marks (" ").

Classic CLI example:

```
A:node-2>file cf3:\ # copy bof.* testdir
Copying file cf3:\bof.cfg-1 ... OK
Copying file cf3:\bof.cfg-2 ... OK
Copying file cf3:\bof.cfg-3 ... OK
Copying file cf3:\bof.cfg-4 ... OK
Copying file cf3:\bof.cfg-5 ... OK
Copying file cf3:\bof.cfg-6 ... OK
Copying file cf3:\bof.cfg-7 ... OK
```

```
Copying file cf3:\bof.cfg-8 ... OK
Copying file cf3:\bof.cfg-9 ... OK
Copying file cf3:\bof.cfg.1 ... OK
Copying file cf3:\bof.cfg ... OK
11 file(s) copied.
A:node-2>file cf3:\ #
```

MD-CLI Example:

```
[/file "cf3:\"]
A:admin@node-2# copy bof.* testdir
11 file(s) copied.

[/file "cf3:\"]
A:admin@node-2#
```

2.2 File Management Tasks in the Classic CLI

The following sections are basic system tasks that can be performed in the classic CLI.

For more information about the supported classic CLI commands, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

When a file system operation is performed that can potentially remove or overwrite a file system entry, a prompt appears to confirm the action. The **force** keyword performs the operation without displaying the confirmation prompt.

All the commands can operate on the local file system. Table 4 indicates which commands also support remote file operations.

Table 4 **File Command Local and Remote File System Support**

Command	local-url	ftp-url	tftp-url	http-url	https-url
attrib	✓				
cd	✓	✓			
copy	✓	✓	✓	✓	✓
delete	✓	✓		✓	✓
dir	✓	✓			
md		✓			
move	✓	✓		✓	✓

Table 4 **File Command Local and Remote File System Support (Continued)**

Command	local-url	ftp-url	tftp-url	http-url	https-url
rd		✓			
scp	source only				
type	✓	✓	✓	✓	✓
unzip	✓	source only	source only		
version	✓	✓	✓		
vi	✓				

2.2.1 Displaying Directory and File Information

Use the **dir** command to display a list of files on a file system. The **type** command displays the contents of a file. The **version** command displays the version of an SR OS image file.

Use the following CLI syntax to display directory and file information:

CLI Syntax:
```
file>
dir [file-url]
type file-url
version file-url
```

The following shows an example of the command syntax:

```
A:ALA-1>file cf1:\ # dir
 Volume in drive cf1 on slot A has no label.
Directory of cf1:\
01/01/1980  12:00a               7597 test.cfg
01/01/1980  12:00a                957 b.
08/19/2001  02:14p             230110 BOOTROM.SYS
01/01/1980  12:00a                133 NVRAM.DAT
04/03/2003  05:32a               1709 103.ndx
01/28/2003  05:06a               1341 103.cftg.ndx
01/28/2003  05:06a              20754 103.cftg
04/05/2003  02:20a      <DIR>         test
              15 File(s)                338240 bytes.
               3 Dir(s)                1097728 bytes free.
A:ALA-1>file cf1:\ # type fred.cfg
# Saved to /cflash1/fred.cfg
# Generated THU FEB 21 01:30:09 2002 UTC
exit all
config
#------------------------------------------
# Chassis Commands
```

```
#------------------------------------------
card 2 card-type faste-tx-32
exit
#------------------------------------------
# Interface Commands
#------------------------------------------
# Physical port configuration
interface faste 2/1
    shutdown
    mode network
exit
interface faste 2/2
    shutdown
exit
interface faste 2/3
    shutdown
exit
interface faste 2/4
A:ALA-1>file cf1:\ # version boot.tim
TiMOS-L-1.0.B3-8
A:ALA-1>file cf1:\ #
```

2.2.2 Modifying File Attributes

The system administrator can change the read-only attribute in the local file.

Enter the **attrib** command with no options to display the contents of the directory and the file attributes.

Use the following CLI syntax to modify file attributes:

CLI Syntax:
```
# file>
# attrib [+r | -r] file-url
```

Example:
```
# file
file cf3:\ # attrib
file cf3:\ # attrib +r BOF.SAV
file cf3:\ # attrib
```

The following example shows the file configuration:

```
    A:ALA-1>file cf3:\ # attrib
    cf3:\bootlog.txt
    cf3:\bof.cfg
    cf3:\boot.ldr
    cf3:\bootlog_prev.txt
    cf3:\BOF.SAV
A:ALA-1>file cf3:\ # attrib +r BOF.SAV
A:ALA-1>file cf3:\ # attrib
    cf3:\bootlog.txt
    cf3:\bof.cfg
```

```
     cf3:\boot.ldr
     cf3:\bootlog_prev.txt
R    cf3:\BOF.SAV
```

2.2.3 Creating Directories

New directories can be created in the local file system, one level at a time.

Use the **md** command to create a new directory.

The **cd** command navigates to different directories.

CLI Syntax:
```
file>
md file-url
```

The following example shows the creation of three levels of directories.

```
A:node-2>file cf3:\ # md test1
A:node-2>file cf3:\ # cd test1
A:node-2>file cf3:\test1\ # md test2
A:node-2>file cf3:\test1\ # cd test2
A:node-2>file cf3:\test1\test2\ # md test3
A:node-2>file cf3:\test1\test2\ # cd test3
A:node-2>file cf3:\test1\test2\test3\ #
```

2.2.4 Copying Files

A variety of files and file types, including image files and configuration files, can be uploaded or downloaded to and from flash cards or TFTP servers.

Use the **copy** command to copy files locally.

The **scp** command copies files between hosts on a network. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH.

The source file for the **scp** command must be local. The file must reside on the router. The destination file has to be of the format: user@host:file-name. The destination does not need to be local.

CLI Syntax:
```
# file>
# copy <source-file-url> <dest-file-url> [force] [no-
  redirect] [client-tls-profile <tls-profile-name>] [proxy
  <proxy-url>]
# scp <local-file-url> <destination-file-url> [router
  <router-instance>] [force]
```

```
# scp <local-file-url> <destination-file-url> [force]
 service <service-name>
```

The following displays examples of the command syntax:

```
A:node-2>file cf3:\ # copy 104.cfg cf1:\test1\test2\test3\test.cfg

A:node-2>file cf3:\ # scp file1 admin@192.168.0.1:cf1:\file1

A:node-2>file cf3:\ # scp file2 user2@192.168.0.1:/user2/file2

A:node-2>file cf3:\ # scp cf2:/file3 admin@192.168.0.1:cf1:\file3
```

2.2.5 Moving Files

Files or directories can be moved from one location to another.

Use the following CLI syntax to move files:

CLI Syntax:

```
# file>
# move old-file-url new-file-url [force]
```

Example:

```
A:ALA-1>file cf1:\test1\test2\test3\ # move test.cfg
cf1:\test1
cf1:\test1\test2\test3\test.cfg
A:ALA-1>file cf1:\test1\test2\test3\ # cd ..
A:ALA-1>file cf1:\test1\test2\ # cd ..
A:ALA-1>file cf1:\test1\ # dir

Directory of cf1:\test1\
    05/04/2006 07:58a      <DIR>          .
    05/04/2006 07:06a      <DIR>          ..
    05/04/2006 07:06a      <DIR>          test2
    05/04/2006 07:58a              25278 test.cfg
     1 File(s)                 25278 bytes.
     3 Dir(s)                1056256 bytes free.
A:ALA-1>file cf1:\test1\ #
```

2.2.6 Deleting Files and Removing Directories

Use the **delete** and **rd** commands to delete files and remove directories. Directories can be removed even if they contain files and/or subdirectories. To remove a directory that contains files and/or subdirectories, use the **rd rf** command. When files or directories are deleted, they cannot be recovered.

The **force** option deletes the file or directory without prompting the user to confirm.

Use the following CLI syntax to delete files and then remove directories:

CLI Syntax:
```
file#
delete file-url [force]
rd file-url [force]
```

The following displays an example of the command syntax:

```
A:ALA-1>file cf1:\test1\ # delete test.cfg
A:ALA-1>file cf1:\test1\ # delete abc.cfg
A:ALA-1>file cf1:\test1\test2\ # cd test3
A:ALA-1>file cf1:\test1\test2\test3\ # cd ..
A:ALA-1>file cf1:\test1\test2\ # rd test3
A:ALA-1>file cf1:\test1\test2\ # cd ..
A:ALA-1>file cf1:\test1\ # rd test2
A:ALA-1>file cf1:\test1\ # cd ..
A:ALA-1>file cf1:\ # rd test1
A:ALA-1>file cf1:\ #
```

Use the following CLI syntax to remove a directory without first deleting files or subdirectories:

CLI Syntax:
```
file
   rd file-url rf
```

2.2.7 Unzipping Files

Use the **unzip** command to expand the contents of a ZIP file to the local file system. Any file that is zipped using the store, deflate, or zip64 compression methods can be unzipped. An example is the SR OS software image available from the Nokia customer support portal.

The source ZIP file location can be a locally installed solid-state storage device or a remote FTP or TFTP server.

The **create-destination** keyword ensures that any non-existent directory structure that is explicitly entered as the destination file URL is created as part of the unzip operation. This parameter is required to create new directories.

Note:

- The destination for the unzipped files and directories must be a locally installed solid-state storage device in the active CPM.
- ZIP filenames, or the filenames of any contained files, must not include special characters.

To unzip files, use the following CLI syntax:

CLI Syntax:
```
file>
unzip source-file-url [dest-file-url] list
unzip source-file-url dest-file-url [create-destination]
  [force]
```

The following example displays the unzip command syntax:

```
A:test# file unzip demo.zip cf3:/mynewfolder/mynewsubfolder create-destination force
Verifying cf3:\demo.zip .. ... OK
Unzipping cf3:\demo.zip to cf3:\mynewfolder\mynewsubfolder\ .. .Processing demodir/
Processing demodir/myfile1.txt
Processing demodir/myfile2.txt
Processing demodir/demosubdir/
Processing demodir/demosubdir/myfile3.txt
Writing...OK
```

2.2.8 Repairing the File System

Use the **repair** command to check a compact flash device for errors and repair any errors found.

Use the following CLI syntax to check and repair a compact flash device:

CLI Syntax:
```
file
  repair [cflash-id]
```

The following example shows the command syntax:

```
A:ALA-1>file cf3:\ # repair
Checking drive cf3: on slot A for errors...
Drive cf31: on slot A is OK.
```

2.3 File Management Tasks in the MD-CLI

The following sections are basic system tasks that can be performed in the MD-CLI.

For more information about the supported MD-CLI commands, refer to the *7450 ESS, 7750 SR, and 7950 XRS MD-CLI Command Reference Guide*.

When a file system operation is performed that can potentially remove or overwrite a file system entry, a prompt appears to confirm the action. The **force** keyword performs the operation without displaying the confirmation prompt.

All the commands can operate on the local file system. Table 5 indicates which commands also support remote file operations.

Table 5 **File Command Local and Remote File System Support**

Command	local-url	ftp-url	tftp-url	http-url	https-url
change-directory	✓	✓			
checksum	✓	✓	✓		
copy	✓	✓	✓	✓	✓
list	✓	✓			
make-directory		✓			
move	✓	✓		✓	✓
permission	✓				
remove	✓	✓		✓	✓
remove-directory		✓			
show	✓	✓	✓	✓	✓
unzip	✓	source only	source only		
version	✓	✓	✓		

2.3.1 Displaying Directory and File Information

Use the **list** command to list the files on a file system, with an option to indicate the list order based on the date, name, or size of the files. The **show** command displays the contents of a specified file or multiple files. The **version** command displays the version of an SR OS image file.

Use the following CLI syntax to display directory and file information:

- **file**
  - **list** [[**sort-order**] {**date** | **name** | **size**}] [[**url**] *string*]
  - **show** [[**url**] *string*]
  - **version** [**url**] *string*

The following shows an example of the command syntax:

```
[/file "cf3:\"]
A:admin@node-2# list

Volume in drive cf3 on slot A is .

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\

09/01/2020  11:27p      <DIR>          .ssh/
01/01/1980  12:00a                170 NVRAM.DAT
01/01/1980  12:00a                679 bof.cfg
09/01/2020  11:27p                319 nvsys.info
09/01/2020  11:27p                  1 restcntr.txt
09/02/2020  04:32p      <DIR>          tstdir/
               4 File(s)                   1169 bytes.
               2 Dir(s)                       0 bytes free.

[/file "cf3:\"]
A:admin@node-2# list size

Volume in drive cf3 on slot A is .

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\

09/01/2020  11:27p      <DIR>          .ssh/
09/02/2020  04:32p      <DIR>          tstdir/
09/01/2020  11:27p                  1 restcntr.txt
01/01/1980  12:00a                170 NVRAM.DAT
09/01/2020  11:27p                319 nvsys.info
01/01/1980  12:00a                679 bof.cfg
               4 File(s)                   1169 bytes.
               2 Dir(s)                       0 bytes free.
[/file "cf3:\"]
A:admin@node-3# show md-config.cfg
File: md-config.cfg
-------------------------------------------------------------------------------
configure {
    card 1 {
        mda 1 {
        }
    }
    log {
        filter 1001 {
            entry 10 {
                description "Collect only events of major severity or higher"
```

```
                action forward
                match {
                    severity {
                        gte major
                    }
                }
            }
        }
        log-id 99 {
            description "Default System Log"
            source {
                main true
Press Q to quit, Enter to print next line or any other key to print next page.
```

2.3.2 Modifying File Attributes

The system administrator can change the attribute of a local file or files in a directory.

Enter the **permission** command with no options to display the contents of the directory and the file attributes.

- **file**
  - **permission** [[**attribute**] {**read-only**| **read-write**}] [[**url**] *string*]

A single local file can be specified or the wildcard character (*) can be used to indicate multiple files. If no URL is specified, the command applies to all files in the directory.

The following shows an example of the command syntax. A file with an “R” preceding the filename indicate the file is read-only; otherwise, the file is read-write.

```
[/file "cf3:\"]
A:admin@node-2# permission
            cf3:\NVRAM.DAT
            cf3:\bof.cfg
            cf3:\nvsys.info
            cf3:\restcntr.txt
            cf3:\.ssh
            cf3:\my.txt

[/file "cf3:\"]
A:admin@node-2# permission read-only my.txt

[/file "cf3:\"]
A:admin@node-2# permission
            cf3:\NVRAM.DAT
            cf3:\bof.cfg
            cf3:\nvsys.info
            cf3:\restcntr.txt
            cf3:\.ssh
 R          cf3:\my.txt
```

```
[/file "cf3:\"]
A:admin@node-2# permission read-only

[/file "cf3:\"]
A:admin@node-2# permission
 R          cf3:\NVRAM.DAT
 R          cf3:\bof.cfg
 R          cf3:\nvsys.info
 R          cf3:\restcntr.txt
 R          cf3:\.ssh
 R          cf3:\my.txt
```

2.3.3 Creating and Navigating Directories

New directories can be created in the local file system, one level at a time.

Use the **make-directory** command to create a new directory.

The **change-directory** command navigates to different directories.

- **file**
  - **change-directory** [**url**] *string*
  - **make-directory** [**url**] *string*

The following example shows the creation of three levels of directories.

```
[/file "cf3:\"]
A:admin@node-2# make-directory test1

[/file "cf3:\"]
A:admin@node-2# change-directory test1

[/file "cf3:\test1"]
A:admin@node-2# make-directory test2

[/file "cf3:\test1"]
A:admin@node-2# change-directory test2

[/file "cf3:\test1\test2"]
A:admin@node-2# make-directory test3

[/file "cf3:\test1\test2"]
A:admin@node-2# change-directory test3

[/file "cf3:\test1\test2\test3"]
A:admin@node-2# change-directory ..

[/file "cf3:\test1\test2"]
A:admin@node-2#
```

2.3.4 Copying Files

A variety of files and file types, including image files and configuration files, can be uploaded or downloaded to and from flash cards or TFTP servers.

Use the **copy** command to copy files.

- **file**
  - **copy** [**source-url**] *string* [**destination-url**] *string* [**client-tls-profile** *string*] [**direct-http**] [**force**] [**proxy** *string*]

The following example copies the md-config.cfg file to the test1 directory.

```
[/file "cf3:\"]
A:admin@node-2# list test1
...
04/05/2019  09:36a                 167 nvram.dat-9
08/19/2020  06:05p                 320 nvsys.info
04/16/2014  10:15a      <DIR>          syslinux/
09/01/2020  08:13p      <DIR>          test1/
04/16/2014  10:15a      <DIR>          timos/
              27 File(s)                 45399 bytes.
               4 Dir(s)                10668032 bytes free.


[/file "cf3:\"]
A:admin@node-2# copy md-config.cfg test1
1 file copied.

[/file "cf3:\"]
A:admin@node-2# list test1

Volume in drive cf3 on slot A is TIMOS_VM_CF.

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\test1

09/01/2020  08:13p      <DIR>          ./
09/01/2020  08:13p      <DIR>          ../
09/02/2020  07:48p               11401 md-config.cfg
09/01/2020  08:13p      <DIR>          test2/
               1 File(s)                  11401 bytes.
               3 Dir(s)                10656256 bytes free.
```

2.3.5 Moving Files

Files or directories can be moved from one location to another.

Use the following CLI syntax to move files:

— **file**
  — **move** [**source-url**] *string* [**destination-url**] *string* [**client-tls-profile** *string*] [**direct-http**] [**force**] [**proxy** *string*]

The following example moves the md-config.cfg file to the test1/test2 directory.

```
[/file "cf3:\test1\"]
A:admin@node-2# list cf3:\test1/test2

Volume in drive cf3 on slot A is TIMOS_VM_CF.

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\test1\test2

09/01/2020  08:13p      <DIR>          ./
09/01/2020  08:13p      <DIR>          ../
09/04/2020  06:36p                   874 bof.cfg
09/04/2020  06:35p                 11788 my_test.cfg
09/04/2020  06:43p      <DIR>          test3/
               2 File(s)                 12662 bytes.
               3 Dir(s)                10629632 bytes free.

[/file "cf3:\test1\"]
A:admin@node-2# move md-config.cfg test2
Moving file cf3:\test1\md-config.cfg ... OK
cf3:\test1\md-config.cfg

[/file "cf3:\test1\"]
A:admin@node-2# change-directory test2

[file "cf3:\test1\test2"]
A:admin@node-2# list

Volume in drive cf3 on slot A is TIMOS_VM_CF.

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\test1\test2

09/01/2020  08:13p      <DIR>          ./
09/01/2020  08:13p      <DIR>          ../
09/04/2020  06:36p                   874 bof.cfg
04/28/2020  03:15p                 11401 md-config.cfg
09/04/2020  06:35p                 11788 my_test.cfg
09/04/2020  06:43p      <DIR>          test3/
               3 File(s)                 24063 bytes.
               3 Dir(s)                10629632
```

2.3.6 Deleting Files and Removing Directories

Use the **remove** and **remove-directory** commands to delete files and remove directories. Directories can be removed even if they contain files or subdirectories.

Use the following CLI syntax to delete files and then remove directories:

- **file**
  - **remove** [**url**] *string* [**client-tls-profile** *string*] [**direct-http**] [**force**] [**proxy** *string*]
  - **remove-directory** [**url**] *string* [**force**] [**recursive**]

The following example removes the test1/test2/test3 directory.

```
[/file "cf3:\test1\test2"]
A:admin@node-2# list

Volume in drive cf3 on slot A is TIMOS_VM_CF.

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\test1\test2

09/01/2020  08:13p      <DIR>          ./
09/01/2020  08:13p      <DIR>          ../
09/04/2020  06:36p                874 bof.cfg
04/28/2020  03:15p              11401 md-config.cfg
09/04/2020  06:43p      <DIR>          test3/
               2 File(s)                 12275 bytes.
               3 Dir(s)                10641920 bytes free.

[/file "cf3:\test1\test2"]
A:admin@node-2# list test3

Volume in drive cf3 on slot A is TIMOS_VM_CF.

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\test1\test2\test3

09/01/2020  08:13p      <DIR>          ./
09/01/2020  08:13p      <DIR>          ../
09/04/2020  06:43p              11788 conf3.cfg
09/04/2020  04:24p               6645 mybof.cfg
               2 File(s)                 18433 bytes.
               2 Dir(s)                10641920 bytes free.

[/file "cf3:\test1\test2"]
A:admin@node-2# remove-directory test3 ?

 remove-directory
 force                - Force removal without prompting
 recursive            - Remove directory and its content recursively

[/file "cf3:\test1\test2"]
A:admin@node-2# remove-directory test3 recursive
Deleting all subdirectories and files in specified directory. y/n ?y
Deleting file cf3:\test1\test2\test3\mybof.cfg ... OK
Deleting file cf3:\test1\test2\test3\conf3.cfg ... OK
Deleting directory cf3:\test1\test2\test3 ... OK

[/file "cf3:\test1\test2"]
A:admin@node-2# list
```

```
Volume in drive cf3 on slot A is TIMOS_VM_CF.

Volume in drive cf3 on slot A is formatted as FAT32

Directory of cf3:\test1\test2

09/01/2020  08:13p      <DIR>          ./
09/01/2020  08:13p      <DIR>          ../
09/04/2020  06:36p                   874 bof.cfg
04/28/2020  03:15p                 11401 md-config.cfg
               2 File(s)                 12275 bytes.
               2 Dir(s)               10661376 bytes free.
```

2.3.7 Unzipping Files

Use the **unzip** command to expand the contents of a ZIP file to the local file system. Any file zipped using the store, deflate, or zip64 compression methods can be unzipped. An example is the SR OS software image available from the Nokia customer support portal.

The source ZIP file location can be a locally installed solid-state storage device or a remote FTP or TFTP server.

The **create-destination** keyword ensures that any non-existent directory structure that is explicitly entered as the destination file URL is created as part of the unzip operation. This parameter is required to create new directories.

Note:

- The destination for the unzipped files and directories must be a locally installed solid-state storage device in the active CPM.
- ZIP filenames, or the filenames of any contained files, must not include special characters.

To unzip files, use the following CLI syntax:

— **file**
  — **unzip** [**source-url**] *string* [[**destination-url**] *string*] [**create-destination**] [**force**] [**list**]

The following example shows the command syntax:

```
[/file "cf3:\"]
A:admin@node-2# unzip demo.zip cf3:/mynewfolder/mynewsubfolder create-destination
   force
Verifying cf3:\demo.zip .. ... OK
Unzipping cf3:\demo.zip to cf3:\mynewfolder\mynewsubfolder\ .. .Processing demodir/
Processing demodir/myfile1.txt
```

```
Processing demodir/myfile2.txt
Processing demodir/demosubdir/
Processing demodir/demosubdir/myfile3.txt
Writing...OK
```

2.3.8 Repairing the File System

Use the **repair** command to check a compact flash device for errors and repair any errors found.

Use the following CLI syntax to check and repair a compact flash device:

- **file**
  - **repair** [[**cflash-id**] *string*]

The following example shows the command syntax:

```
[/file "cf3:\"]
A:admin@node-2# repair cflash-id cf3:
Checking drive cf3: on slot A for errors...
Drive cf3: on slot A is OK.

[/file "cf3:\"]
A:admin@node-2# repair
Checking drive cf3: on slot A for errors...
Drive cf3: on slot A is OK.
```

2.3.9 Displaying File Checksums

Use the **checksum** command to display file checksums of an SR OS image file.

Use the following CLI syntax to display checksums:

- **file**
  - **checksum type** [**url**] *string*

The following example shows the command syntax:

```
[/file "cf3:\"]
A:admin@node-2# checksum image cpm.timTiMOS-C-20.10.R1
Wed Nov 4 09:18:17 PST 2020 by builder in /builds/c/2010B/R1/panos/main/sros
Checking file ... OK
```

3 Boot Options

3.1 System Initialization

The primary copy of SR OS software is located on a compact flash card. The removable media is shipped with each router and contains a copy of the OS image.

Note:

- The modules contain three slots for removable compact flash cards. The drives are named Compact Flash Slot #1 (cf1), Compact Flash Slot #2 (cf2), and Compact Flash Slot #3 (cf3). Configurations and executable images can be stored on flash cards or an FTP file location.
- The flash card containing the bootstrap and boot option files must be installed in Compact Flash Slot #3 (cf3).
- You must have a console connection.

Starting a router begins with hardware initialization (a reset or power cycle). By default, the system searches Compact Flash Slot #3 (cf3) for the boot.ldr file (also known as the bootstrap file). The boot.ldr file is the image that reads and executes the system initialization commands configured in the boot option file (BOF). The default value to initially search for the boot.ldr file on cf3 cannot be modified.

The following is an example of a console display output when the boot.ldr file cannot be located on cf3.

```
...
(memory test messages)
(serial number information)
Searching for boot.ldr on local drives:
No disk in cf3
No disk in cf3
No disk in cf3
Error - file boot.ldr not found on any drive
Please insert CF containing boot.ldr. Rebooting in 5 seconds.
```

When the bootstrap image is loaded, the BOF is read to obtain the location of the image and configuration files. The BOF must be located on the same compact flash drive as the boot.ldr file.

Figure 1 displays the system initialization sequence. In the figure, “A” refers to Figure 2, and “B” refers to the list of files on the compact flash.

Figure 1 **System Initialization - Part 1**

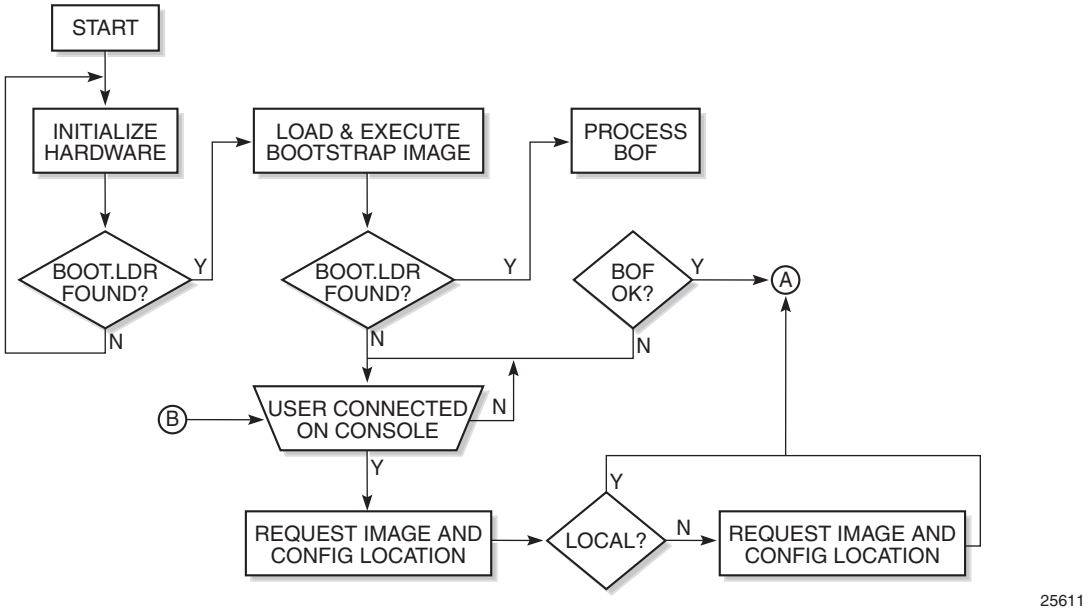
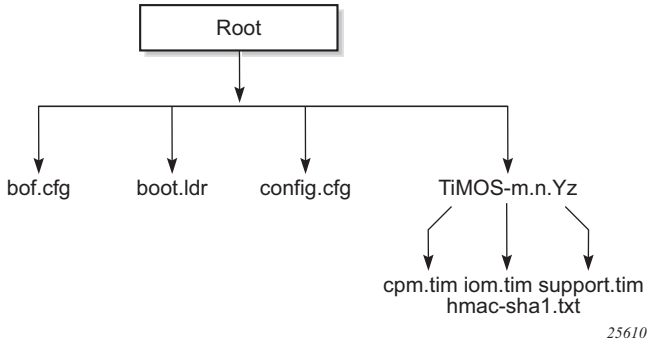


Figure 2 displays the compact flash directory structure and file names for the multislot models.

Figure 2 **Files on the Compact Flash**



Files on compact flash are:

- bof.cfg — Boot option file
- boot.ldr — Bootstrap image
- config.cfg — Default configuration file
- TIMOS-m.n.Yz:

  m — Major release number

n — minor release number

Y:A — Alpha release

B — Beta release

M — Maintenance release

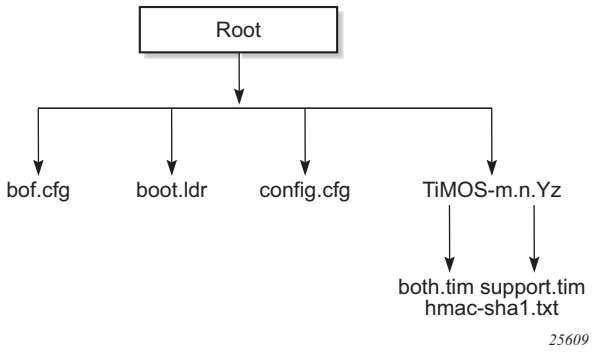
R — Released software

z — Version number

- cpm.tim — CPM image file
- iom.tim — XCM/IOM image file
- support.tim — required data for SR OS .tim files
- hmac-sha1.txt (in FIPS-140-2 mode only)

Figure 3 displays the compact flash directory structure and file names for the 1-slot models (7750 SR-1 and 7750 SR-1s).

Figure 3 **Files on the Compact Flash (1-slot and 1-slot non-redundant)**



Files on the compact flash (1-slot models) are:

- bof.cfg — Boot option file
- boot.ldr — Bootstrap image
- config.cfg — Default configuration file
- TIMOS-m.n.Yz:

  m — Major release number

  n — Minor release number

  - Y:A — Alpha release
  - B — Beta release
  - M — Maintenance release
  - R — Released software

  z — Version number

- both.tim — CPM and IOM image file
- support.tim — required data for SR OS .tim files
- hmac-sha1.txt (in FIPS-140-2 mode only)

The 7750 SR includes a boot option for running the node in a FIPS-140-2 mode. This mode limits the use of cryptographic algorithms on the CPM to only those that are in accordance with the FIPS-140-2 certifications associated with the 7750 SR.

3.1.1 Configuration and Image Loading

When the system executes the boot.ldr file, the initialization parameters from the BOF are processed. Three locations can be configured for the system to search for the files that contains the runtime image. The locations can be local or remote. The first location searched is the primary image location. If not found, the secondary image location is searched, and lastly, the tertiary image location is searched.

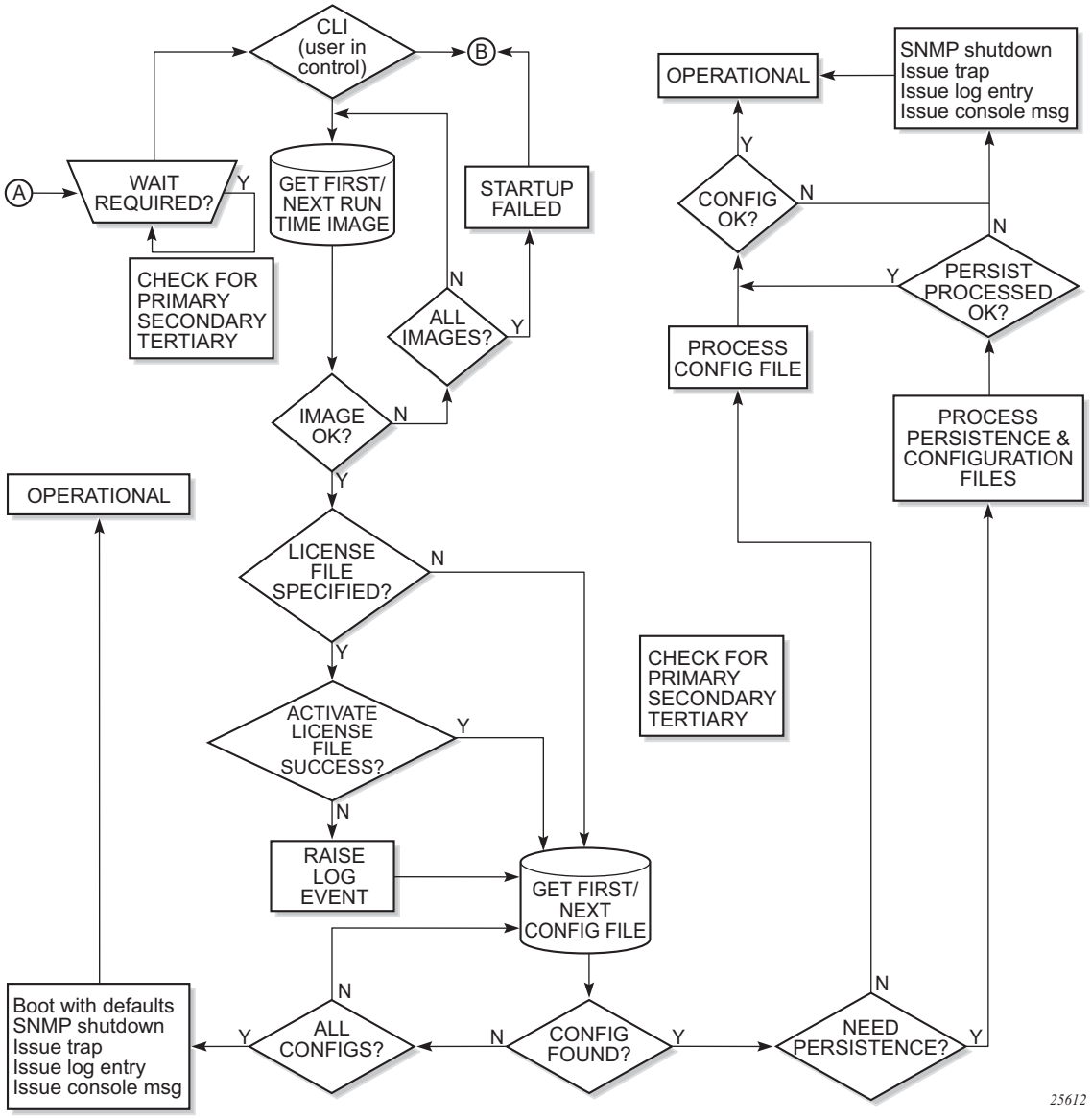
If the BOF cannot be found or loaded, then the system enters a console message dialog session prompting the user to enter alternate file locations and file names.

The boot loader can be interrupted during the boot sequence by pressing any key on the CPM console port. The operator must then type **sros** and press **ENTER** within 30 seconds or the boot loader continues to try to boot the system. This key sequence ensures that noise or misconfiguration does not inadvertently interrupt the boot sequence. If the operator types **sros** and presses **ENTER** within 30 seconds, they are brought to a console message dialog session prompting the user to enter file locations and other boot information.

When the runtime image is successfully loaded, control is passed from the bootstrap loader to the image. The runtime image first attempts to read the license file if one has been included in the bof. If a license file is found, it is activated. If there are any issues with the activation, a log event is raised but the startup processing continues with the reading of the configuration file. The runtime image next attempts to locate the configuration file as configured in the BOF. Like the runtime image, three locations can be configured for the system to search for the configuration file. The locations can be local or remote. The first location searched is the primary configuration location. If not found, the secondary configuration location is searched, and lastly, the tertiary configuration location is searched. The configuration file includes chassis, card, MDA, and port configurations, as well as system, routing, and service configurations.

Figure 4 displays the boot sequence.

Figure 4 **System Initialization - Part 2**



The following displays an example of BOF output:

```
A:ALA-1>bof# show bof
===============================================================================
Memory BOF
===============================================================================
no autonegotiate
duplex      full
speed      100
address    10.10.0.1/20 active
```

```
wait    3
primary-image cf3:\both.tim
primary-config cf3:\test123.cfg
primary-dns 192.168.10.20
persist     on
dns-domain test.nokia.com
===============================================================
A:ALA-1>bof#
```

3.1.1.1 Persistent Indices in the Classic and Mixed Configuration Mode

Optionally, the BOF **persist** parameter can specify whether the system should preserve system indices when a **save** command is executed. During a subsequent boot, the index file is read along with the configuration file. As a result, a number of system indices are preserved between reboots, including the interface index, LSP IDs, path IDs, etc. If persistence is not required and the configuration file is successfully processed, then the system becomes operational. If persist is required, then a matching x.ndx file must be located and successfully processed before the system can become operational. Matching files (configuration and index files) must have the same filename prefix such as **test123.cfg** and **test123.ndx** and are created at the same time when a **save** command is executed. Note that the persistence option must be enabled to deploy the Network Management System (NMS). The default is off.

Traps, logs, and console messages are generated if problems occur and SNMP shuts down for all SNMP gets and sets, however, traps are issued.

Note: System indices in model-driven configuration mode are always persistent.

3.1.1.2 Lawful Intercept

Lawful Intercept (LI) describes a process to intercept telecommunications by which law enforcement authorities can unobtrusively monitor voice and data communications to combat crime and terrorism with higher security standards of lawful intercept capabilities in accordance with local law and after following due process and receiving proper authorization from competent authorities. The interception capabilities are sought by various telecommunications providers.

As lawful interception is subject to national regulation, requirements vary from one country to another. This implementation satisfies most national standard's requirements. LI is configurable for all service types.

3.1.1.3 FIPS-140-2 Mode

The 7750 SR includes a configurable parameter in the bof.cfg file to make the node run in FIPS-140-2 mode. When the node boots in FIPS-140-2 mode, the following behaviors are enabled on the node:

- The node performs an HMAC-SHA1 integrity test on the software images .tim files.
- The node limits the use of encryption and authentication algorithms to only those allowed for the associated FIPS-140-2 certification of the 7750-SR.
- Cryptographic module startup tests are executed on the CPM when the node boots to ensure the associated approved FIPS-140-2 algorithms are operating correctly.
- Cryptographic module conditional tests are executed when required during normal operation of associated when using FIPS-140-2 approved algorithms.
- When configuring user-defined encryption or authentication keys, the CLI prompts for the key to be re-entered. For keys entered in hash format, for example, the key must be re-entered in hash format, followed by the appropriate hash keyword. If the re-entered key does not match the original, the CLI command is canceled. This affects several protocols and applications.

To support FIPS-140-2, an HMAC-SHA-1 integrity check is performed to verify the integrity of the software images. The following file is included in the TIMOS-m.n.Yz software bundle containing the hmac-sha-1 signature:

- hmac-sha1.txt

During the loading of the cpm.tim or both.tim, a HMAC-SHA-1 check is performed to ensure that the calculated HMAC-SHA-1 of the loaded image matches that stored in the hmac-sha1.txt file.

The HMAC-SHA-1 check is performed on the data loaded from the .tim file. Note that when configuring the primary-image, secondary-image and tertiary-image, the hmac-sha1.txt file must exist in the same directory as the .tim files. If the load has been verified correctly from the HMAC-SHA-1 integrity check, the load continues to start up as normal. If the load is not verified by the HMAC-SHA-1 integrity check, the image load fails.

After the HMAC-SHA-1 integrity check passes, the nodes continue their normal startup sequence including reading the config.cfg file and loading the configuration. The config.cfg file used to boot the node in FIPS-140-2 mode must not contain any configuration that is not supported in FIPS-140-2 mode. If such configuration is present in the config.cfg file when the node boots, the node loads the config.cfg file until the location of the offending configuration and then halt the configuration at that point. Upon a failure to load the config.cfg file, a failure message is printed on the console.

Enabling FIPS-140-2 restricts the ability to configure and use cryptographic algorithms and functions that are not FIPS approved. FIPS-140-2 impacts the ability to configure SSH, SNMP and certificates. Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide* for details of FIPS-140-2 related items.

In addition, signature algorithms of the following combinations only are approved for FIPS:

- FIPS-140 Approved - Digital Signature Standard (DSS)
  - DSA
  - RSA
  - ECDSA
- FIPS-140 Approved - Secured Hash Standard (SHS)
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512

Any other combination is not supported in FIPS mode. Using other FIPS signature algorithms in certificates affecting IPsec can cause tunnels to fail. Restrictions to cryptographic algorithms are listed in the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*.

3.1.1.4 System Profiles

System profiles provide flexibility when using FP4-based line cards by supporting different system capabilities. The system profile is defined in the BOF and is used by the system when it is next rebooted. Contact your Nokia representative for system profile information.

The following system profiles are supported:

- Profile none

  This profile represents the existing system capabilities and allows FP3- and FP4-based hardware to co-exist within a system. This profile is indicated by the omission of the profile parameter in the BOF.

- Profile A

  This profile is primarily targeted at subscriber services and Layer 2 and 3 VPN business services and is defined by configuring the BOF profile parameter to **profile-a**.

- Profile B

  This profile is primarily targeted at infrastructure routing, core, peering, and DC-GW applications.

System profile **profile-a** and **profile-b** support only FP4-based line cards. Provisioning FP2- or FP3-based line cards is prohibited when the system profile is set to **profile-a** or **profile-b**. If FP2- or FP3-based card types are present in the boot configuration when using these profiles, the boot sequence aborts the loading of the configuration file when it encounters their configuration.

When changing between system profiles, it is mandatory to remove all configuration commands for features that are not supported in the target system profile before rebooting the system, otherwise the reboot fails at the unsupported configuration command on startup.

On 7750 SR-1 and 7750 SR-s systems, the following conditions apply regarding the profile parameter:

- The parameter should be configured to either **profile-a** or **profile-b**.
- If the parameter is omitted, profile **profile-a** is used by the system.
- If the parameter is configured to an invalid value, it is ignored and profile **profile-a** is used by the system.

On 7750 SR-7-B/12-B/12e and 7950 XRS-20/20e systems, the following conditions apply regarding the profile parameter:

- The default system profile is **none** when the parameter is omitted.
- The parameter can be configured to either **profile-a** or **profile-b**, in which case only FP4-based line cards are supported.
- If the parameter is configured to an invalid value, it is ignored and profile **none** is used by the system.

On all other systems, the following conditions apply regarding the profile parameter:

- These systems must use profile **none** (the existing system capabilities). As a result, the parameter must not be configured.
- If the parameter is configured to **profile-a** or **profile-b**, the system boots, allowing access using the console and CPM management interface, but FP2-based and FP3-based line cards cannot be provisioned; if these card types are present in the boot configuration, the boot sequence aborts loading the configuration file when it encounters their configuration. This issue can be corrected by removing the parameter and rebooting the system.
- If the parameter is configured to an invalid value, it is ignored and profile **none** is used by the system.

If a system has two CPMs, and the standby CPM boots with a different profile parameter than is used on the active CPM, the active CPM reboot the standby CPM and keep it in a down state. To correct the situation, the BOF can be reconfigured on the standby CPM to match the one configured on the active CPM, and then reboot the system. Alternatively, automatic BOF synchronization can be enabled to keep both CPMs in sync using the following command:

configure redundancy synchronize boot-env

When performing a minor or major ISSU software upgrade on dual CPM systems, it is important that the system profile in the BOF on both the active and standby CPM is the same and has a value supported on the pre-upgrade software release. If the standby CPM happened to have a system profile which is only supported in the post-upgrade release, the active CPM reboots the standby and keeps it down due to a system profile mis-match.

The BOF system profile can be displayed as follows:

Classic CLI:

```
*A:node-2# show bof | match system-profile
    system-profile profile-a
*A:node-2#
```

MD-CLI:

```
[/]
A:admin@node-2# admin show configuration bof | match profile
        profile profile-a

[/]
```

The BOF system profile used by the system when it booted can be seen in the boot messages (using the **show boot-messages** command), which display the BOF read when rebooting.

The system profile in use on the system can be displayed as follows:

Classic CLI:

```
A:node-2# show chassis | match "System Profile"
  System Profile                     : none
A:node-2#
```

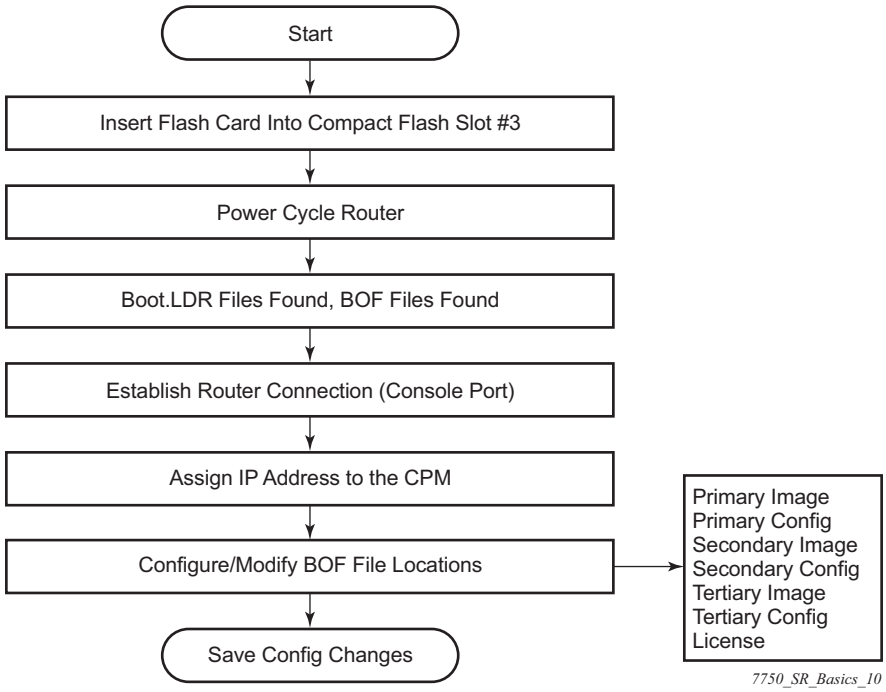
MD-CLI:

```
[/]
A:admin@node-2# show chassis | match "System Profile"
  System Profile                     : none
```

3.2 Initial System Startup Process Flow

Figure 5 displays the process start your system. Note that this example assumes that the boot loader and BOF image and configuration files are successfully located.

Figure 5 **System Startup Flow**



3.3 Configuration Notes

This section describes BOF configuration caveats.

- For router initialization, the compact flash card must be installed in the Compact Flash #3 slot.
- The loading sequence is based on the order in which it is placed in the configuration file. It is loaded as it is read in at boot time.

3.4 Configuring Boot Options File with CLI

This section provides information to configure BOF parameters with CLI.

3.4.1 BOF Configuration Overview

Nokia routers do not contain a boot EEPROM. The boot loader code is loaded from the boot.ldr file. The BOF file performs the following tasks:

Step 1. Sets up the CPM and CCM Ethernet port (speed, duplex, auto).
Step 2. Assigns the IP address for the CPM and CCM Ethernet port.
Step 3. Creates static routes for the CPM/CCM Ethernet port.
Step 4. Sets the console port speed.
Step 5. Configures the Domain Name System (DNS) name and DNS servers.
Step 6. Configures the primary, secondary, tertiary configuration source.
Step 7. Configures the primary, secondary, and tertiary image source.
Step 8. Configures the license source.
Step 9. Configures operational parameters.

3.4.2 Basic BOF Configuration

The parameters which specify location of the image filename that the router will try to boot from and the configuration file are in the BOF.

The most basic BOF configuration should have the following:

- Primary address
- Primary image location
- Primary configuration location

The following is a sample of a basic BOF configuration.

Classic CLI:

```
A:node-2# show bof
===============================================================================
BOF (Memory)
===============================================================================
    primary-image    ftp://.../i386-both.tim
```

```
    primary-config   ftp://.../config.cfg
    license-file     ftp://.../license
    address          192.168.189.52/24 active
    static-route     192.168.0.0/16 next-hop 192.168.189.1
    static-route     172.16.0.0/16 next-hop 192.168.189.1
    autonegotiate
    duplex           full
    speed            100
    wait             3
    persist          on
    no li-local-save
    no li-separate
    no fips-140-2
    console-speed    115200
===============================================================================
A:node-2#
```

MD-CLI:

```
[/]
A:admin@node-2# admin show configuration bof
# TiMOS-B-20.10.R1 both/x86_64 Nokia 7750 SR Copyright (c) 2000-2020 Nokia.
# All rights reserved. All use subject to applicable license agreements.
# Built on Wed Nov 4 09:18:17 PST 2020 by builder in /builds/c/2010B/R1/panos/main/
sros
# Configuration format version 20.10 revision 0

# Generated MON OCT 19 13:39:54 2020 UTC

bof {
    configuration {
        primary-location "ftp://.../config.cfg"
    }
    console {
        speed 115200
    }
    dns {
        primary-server ::
        secondary-server ::
        tertiary-server ::
    }
    image {
        primary-location "ftp://.../i386-both.tim"
    }
    li {
        local-save false
        separate false
    }
    license {
        primary-location "ftp://.../license"
    }
    port "management" {
        autonegotiate true
    }
    router "management" {
        interface "management" {
            cpm active {
                ipv4 {
```

```
                    ip-address 192.168.189.52
                    prefix-length 24
                }
            }
            cpm standby {
            }
        }
        static-routes {
            route 192.168.0.0/16 {
                next-hop 192.168.189.1
            }
            route 172.16.0.0/16 {
                next-hop 192.168.189.1
            }

        }
    }
    system {
        fips-140-2 false
        persistent-indices true
    }
}

# Finished MON OCT 19 13:39:58 2020 UTC

[/]
A:admin@node-2#
```

3.4.3 Common Configuration Tasks

The following sections are basic system tasks that must be performed.

For details about hardware installation and initial router connections, refer to the specific router hardware installation guide.

3.4.3.1 Searching for the BOF

The BOF should be on the same drive as the boot loader file. If the system cannot load or cannot find the BOF then the system checks whether the boot sequence was manually interrupted. The system prompts for a different image and configuration location.

The following example shows an example of the output when the boot sequence is interrupted.

```
. . .

###########################################
```

```
Sample output:
Hit a key within 3 seconds to change boot parameters...
Type "sros" and hit ENTER within 29 seconds to begin changing parameters: sros
You must supply some required Boot Options. At any prompt, you can type:
   "restart" - restart the query mode.
   "reboot"  - reboot.
   "exit"    - boot with existing values.
Press ENTER to begin, or 'flash' to enter firmware update...
Software Location
-----------------
   You must enter the URL of the TiMOS software.
   The location can be on a Compact Flash device,
   or on the network.
   Here are some examples
      cf3:/timos1.0R1
      ftp://user:passwd@192.168.1.150/./timos1.0R1
      ftp://user:passwd@[3FFE::1]/./timos1.0R1
The existing Image URL is 'ftp://*:*@192.168.192.20/./images'
Press ENTER to keep it.
Software Image URL: ftp://vxworks:vxw0rks@192.168.10.20/./rel/0.0/xx
Configuration File Location
---------------------------
   You must enter the location of configuration
   file to be used by TiMOS.  The file can be on
   a Compact Flash device, or on the network.
   Here are some examples
      cf1:/config.cfg
      ftp://user:passwd@192.168.1.150/./config.cfg
      ftp://user:passwd@[3FFE::1]/./config.cfg
      tftp://192.168.1.150/./config.cfg
      tftp://[3FFE::1]/./config.cfg
The existing Config URL is 'ftp://*:*@192.168.192.20/./images/dut-b.cfg'
Press ENTER to keep it, or the word 'none' for no Config URL.
Config File URL: cf1:/config.cfg
License File Location
---------------------------
   You must enter the location of the license
   file to be used by TiMOS.  The file can be on
   a Compact Flash device, or on the network.
   Here are some examples
      cf1:/license.txt
      ftp://user:passwd@192.168.1.150/./license.txt
      ftp://user:passwd@[3FFE::1]/./license.txt
      tftp://192.168.1.150/./license.txt
      tftp://[3FFE::1]/./license.txt
License File URL:
No license file specified.
IP Autoconfiguration
--------------------
   This device supports IP autoconfiguration of the management port.
   When the Software Image URL and the License File URL are not local,
   the network configuration must be static (no autoconfiguration).
   When the Config File URL is not local,
   the network configuration is recommended to be static (no autoconfiguration).
   Per address family the configuration must be either static, either auto.
The Software Image URL is not local and does require that the IPv4 network is static
ally configured.
   [IPv4 Autoconfiguration cannot be enabled]
Would you like to enable IPv4 Autoconfiguration? (yes/no) no
```

```
Would you like to enable IPv6 Autoconfiguration? (yes/no) no
Network Configuration
---------------------
   You specified a network location for either the
   software or the configuration file.  You need to
   configure IP(v6) for this system.
   IP addresses should be entered in standard
   dotted decimal form with a network length.
       example:   192.168.1.169/24
The existing Active IP address is 192.168.192.23/18. Press ENTER to keep it.
Enter Active IP Address (Type 0 if none desired): 192.168.10.1/20
The existing Standby IP address is 192.168.192.24/18. Press ENTER to keep it.
Enter Standby IP Address (Type 0 if none desired): 192.168.10.2/20
   In case of an IPv6, the IPv6 address should be
   entered in standard colon hexadecimal notation
   with a prefix length.
       example:   3FFE::1/112
The existing Active IPv6 address is 3000::c0a8:c015/114. Press ENTER to keep it.
Enter Active IPv6 Address (Type 0 if none desired): 3ABC::AAAA:1/100
The existing Standby IPv6 address is 3000::c0a8:c016/114. Press ENTER to keep it.
Enter Standby IPv6 Address (Type 0 if none desired): 3ABC::AAAA:2/100
Would you like to add a static route? (yes/no) yes
Static Routes
-------------
   You specified network locations which require
   static routes to reach. You will be asked to
   enter static routes until all the locations become
   reachable.
   Static routes should be entered in the following format:
   prefix/mask next-hop ip-address
       example:     192.168.0.0/16 next-hop 192.168.1.254
       example:     3FFE::1:0/112 next-hop 3FFE::2:1
Enter ip route: 1.1.1.0/24 next-hop 192.168.1.250
1.1.1.0/24 next-hop 192.168.1.250
A route to that subnet already exists.
Would you like to add a static route? (yes/no) no
Would you like to add an IPv6 static route? (yes/no) no
The existing fips-140-2 configuration is : 'no fips-140-2'
If you would like to change it please enter 'fips-140-2' followed by ENTER
or press ENTER to keep existing fips configuration
Auto-Boot
---------
   This device supports automated provisioning
   from the network.  When this mode is enabled
   the system will not execute the boot configuration
   file. Instead, it will boot to the default
   configuration and automatically provision supported
   equipment for further loading from the network.
Would you like to enable Automated-Provisioning? (yes/no) no
New Settings
------------
    primary-image    ftp://*:*@192.168.10.20/./rel/0.0/xx
    primary-config   cf1:/config.cfg
    address          192.168.10.1/20 active
    address          192.168.10.2/20 standby
    address          3abc::aaaa:1/100 active
    address          3abc::aaaa:2/100 standby
    static-route     1.1.1.0/24 next-hop 192.168.1.250
    autonegotiate
```

```
    duplex           full
    speed            100
    wait             3
   persist          off
    no fips-140-2
    console-speed    115200
Do you want to overwrite cf3:/bof.cfg with the new settings? (yes/no): yes
Successfully saved the new settings in cf3:/bof.cfg
###########################################
```

3.4.3.2 Accessing the CLI

To access the CLI to configure the software for the first time, follow these steps:

- When the CPM/CCM is installed, and power to the chassis is turned on, the SR OS software automatically begins the boot sequence.
- When the boot loader and BOF image and configuration files are successfully located, establish a router connection (console session).

3.4.3.2.1 Console Connection

To establish a console connection, you will need the following:

- An ASCII terminal or a PC running terminal emulation software set to the parameters shown in the table below.
- A standard serial cable with a male DB9.

Table 6 lists the console configuration parameter values.

Table 6 **Console Configuration Parameter Values**

Parameter	Value
Baud Rate	115,200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

To establish a console connection:

Step 1. Connect the terminal to the Console port on the CPM/CCM using the serial cable.

Step 2. Power on the terminal.

Step 3. Establish the connection by pressing the <Enter> key a few times on your terminal keyboard.

Step 4. At the router prompt, enter the login and password.

The default login is admin.

The default password is admin.

3.4.4 Autoconfigure

When autoconfigure is enabled, the router performs a DHCP discovery or solicit (IPv6) to get the IP address of the out-of-band (OOB) management port.

The OOB management port can support a DHCP client for IPv4, IPv6, or dual stack. For dual stack, both IPv4 and IPv6 DHCP are configured. When the offer for either of the address families arrives, the management port is configured with the IP address in the offer. Eventually, both offers arrive and the management port is configured with both address families.

When a DHCP client is configured using autoconfigure, all image and license files should be placed and loaded from the CF. The configuration file could be loaded from the network, but Nokia recommends that the config file be on the CF as well. The configuration file is not loaded until the DHCP client offer is received and programmed successfully for the management port IP address, or the DHCP client timeout is expired.

3.4.4.1 Autoconfigure Restrictions

When autoconfigure is enabled, a static IP address or static route cannot be configured in the BOF.

Similarly, a DNS server cannot be configured in the BOF, and only the DNS server provided by the DHCP offer can be used to resolve URLs.

The option 15 DNS domain name is not supported. The user can configure the DNS domain in the BOF so that the domain is not blocked when autoconfigure is used. Otherwise, the user must use the absolute URL with the host name and domain included.

3.4.4.2 DHCP Discovery of MAC Addresses

When autoconfigure is used on redundant CPM chassis, the DHCP discovery uses the chassis MAC address. Only the active CPM performs a DHCP discovery and not the inactive CPM. When the offer arrives, the node uses that IP and the chassis MAC as addresses for management. Consequently, the inactive CPM is not reachable by the network, because it has no separate IP address. On activity switch, the inactive CPM inherits the active IP and chassis MAC.

For non-redundant CPMs, the management port MAC is used.

Note: The router must be rebooted when enabling autoconfigure for the first time to ensure that the CPM card uses the chassis MAC address.

3.4.4.3 IPv6 DUID

SR OS supports type 2 DUID (link local), which is set to the chassis serial number. Type 3 (enterprise) is set to the chassis MAC address. Type 1 is not supported.

For type 2 DUID, the SR OS sends the Nokia Enterprise ID as the second byte of the DUID, followed by the chassis serial number. The first byte is the DUID type code. The chassis serial number starts with capital ASCII letters, which ensures that the serial number is unique as an application ID in the SR OS IPv6 DHCP application domain.

DUID type codes are as follows:

- DHCP6C_DUID_ENT_ID__IPSEC_IPV4ADDR - 1
- DHCP6C_DUID_ENT_ID__IPSEC_ASN1DN - 2
- DHCP6C_DUID_ENT_ID__IPSEC_FQDN - 3
- DHCP6C_DUID_ENT_ID__IPSEC_USER_FQDN - 4
- DHCP6C_DUID_ENT_ID__IPSEC_IPV6ADDR - 5
- DHCP6C_DUID_ENT_ID__IPSEC_ASN1GN - 6
- DHCP6C_DUID_ENT_ID__IPSEC_KEYID - 7
- DHCP6C_DUID_ENT_ID__WLAN_GW - 8
- DHCP6C_DUID_ENT_ID__AUTOBOOT - 9
- DHCP6C_DUID_ENT_ID__ZTP_BOF_AUTOP - Capital letters in ASCII

3.4.4.4 IPv6 DHCP RAs

An IPv6 DHCP offer does not have an IP prefix within the offer, unlike an IPv4 DHCP offer. The IPv6 prefix is usually obtained from the IPv6 Route Advertisement (RA) arriving from the upstream router. For ZTP, SR OS is a host and assigns a /128 prefix to the IPv6 address obtained from the DHCP offer.

In addition, SR OS supports the installation of IPv6 default and static routes from upstream routers using the IPv6 RA. Multiple upstream routers can respond to a route solicitation with their own RA. SR OS installs all the routes advertised by the RA. If the same route is advertised by multiple upstream routers (next hops), the SR OS installs the route with the highest preference. The SR OS does not support ECMP when the same route is advertised from multiple next hops by multiple RAs.

To ensure that all the RAs are obtained before the auto-provisioning process is started for IPv6, SR OS follows the RFC 4861 recommendation that the host (in this case SR OS) send a minimum of three route solicitations. This is to ensure that if a route solicitation is lost, at least one of the three would reach the upstream routers. Each route solicitation is followed by a 4 s timeout. If the first route solicitation is sent at T0, the second is sent at T0+4 s and the third is sent at T0+8 s. The upstream routers must respond to the route solicitation with in 0.5 s. This means that the SR OS will have all of the RAs and the routes within 8.5 s of the first route solicitation. Therefore, SR OS waits for a maximum of 9 s to receive all RAs.

If the DHCPv6 timeout is less than 9 s, the DHCPv6 timeout is honored even for the RA wait time. If the node has received a single RA and DHCP offer, the process is considered a success. However, it is possible that not all the RAs have arrived on the node because the node has waited less than 9 s.

3.5 System Administration Commands in the Classic CLI

For more information about the supported classic CLI commands, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

Use the following administrative commands to perform management tasks.

CLI Syntax:
```
A:ALA-1# admin
display-config
reboot [active | standby | upgrade] [hold] [now]
save [file-url] [detail] [index]
```

3.5.1 Viewing the Current Configuration

Use one of the following CLI commands to display the current configuration. The **detail** option displays all default values. The **index** option displays only the persistent indices. The info command displays context-level information.

CLI Syntax: `admin# display-config [detail | index]`
`info detail`

The following example shows a configuration file for the 7750 SR:

```
A:7750-3>admin# display-config
# TiMOS B-1.0.Ixxx - Copyright (c) 2000-2016 Nokia
# Built on Tues Jan 21 21:39:07 2007 by builder in /rel1.0/xx/panos/main

# Generated WED Jan 31 06:15:29 2007 UTC

exit all
configure
#------------------------------------------------
echo "System Configuration"
#------------------------------------------------
system
        name "7750-3"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        ccm 1
        exit
        snmp
        exit
        login-control
            idle-timeout 1440
            motd text "7750-3"
        exit
        time
            sntp
                shutdown
            exit
            zone UTC
        exit
        thresholds
            rmon
            exit
        exit
    exit...
...
------------------------------------------------
echo "Redundancy Configuration"
#------------------------------------------------
    redundancy
        synchronize boot-env
    exit
...exit all
```

```
# Finished FRI Nov 21 15:06:16 2008 UTC
A:7750#
```

3.5.2 Modifying and Saving a Configuration

If you modify a configuration file, the changes remain in effect only during the current power cycle unless a save command is executed. Changes are lost if the system is powered down or the router is rebooted without saving.

- Specify the file URL location to save the running configuration. If a destination is not specified, the files are saved to the location where the files were found for that boot sequence. The same configuration can be saved with different file names to the same location or to different locations.
- The **detail** option adds the default parameters to the saved configuration.
- The **index** option forces a save of the index file.
- Changing the active and standby addresses without reboot standby CPM may cause a boot-env sync to fail.

The following command saves a configuration:

CLI Syntax: `bof# save [cflash-id]`

Example:
```
A:ALA-1# bof
A:ALA-1>bof# save cf3:
A:ALA-1>bof#
```

The following command saves the system configuration:

CLI Syntax: `admin# save [file-url] [detail] [index]`

Example:
```
A:ALA-1# admin save cf3:\test123.cfg
Saving config.# Saved to cf3:\test123.cfg
... complete
A:ALA-1#
```

Note: If the persist option is enabled and the **admin save** *file-url* command is executed with an FTP path used as the *file-url* parameter, two FTP sessions simultaneously open to the FTP server. The FTP server must be configured to allow multiple sessions from the same login, otherwise, the configuration and index files will not be saved correctly.

3.5.3 Deleting Bof Parameters

You can delete specific BOF parameters. The **no** form of these commands removes the parameter from configuration. The changes remain in effect only during the current power cycle unless a **save** command is executed. Changes are lost if the system is powered down or the router is rebooted without saving.

Deleting a BOF address entry is not allowed from a remote session.

Use the following CLI syntax to save and remove BOF configuration parameters:

CLI Syntax:
```
bof# save [cflash-id]
```

Example:
```
A:ALA-1# bof
A:ALA-1>bof# save cf3:
A:ALA-1>bof#
```

CLI Syntax:
```
bof#
bof autoconfigure ipv4 no dhcp
bof autoconfigure ipv6 no dhcp
no address ip-address/mask [active | standby]
no autonegotiate
no console-speed
no dns-domain
no li-local-save
no li-separate
no primary-config
no primary-dns
no primary-image
no secondary-config
no secondary-dns
no secondary-image
no static-route ip-address/mask next-hop ip-address
no system-profile
no tertiary-config
no tertiary-dns
no tertiary-image
```

3.5.4 Saving a Configuration to a Different Filename

Save the current configuration with a unique filename to have additional backup copies and to edit parameters with a text editor. You can save your current configuration to an ASCII file.

Use the following CLI syntax to save a configuration to a different location:

CLI Syntax: `admin# save [file-url] [detail] [index]`

Example:
```
A:ALA-1>admin# save cf3:\testABC.cfg
Saving config.# Saved to cf3:\testABC.cfg
... complete
A:ALA-1#
```

3.5.5 Rebooting

When an **admin**>**reboot** command is issued, routers with redundant CPM are rebooted as well as the XMAs, XCMs, and IOMs. Changes are lost unless the configuration is saved. Use the **admin**>**save** *file-url* command to save the current configuration. If no command line options are specified, the user is prompted to confirm the reboot operation.

Use the following CLI syntax to reboot:

CLI Syntax: `admin# reboot [active | standby | upgrade] [hold] [now]`

Example:
```
A:ALA-1>admin# reboot
A:DutA>admin# reboot
Are you sure you want to reboot (y/n)? y
Nokia 7xxx Boot ROM. Copyright 2000-2020 Nokia.
All rights reserved. All use is subject to applicable
 license agreements.
Build: X-20.7.R2 on Fri September 5 18:09:16 PDT 2020 by
 builder
```

3.5.6 Setting the MTU Value for the Management Port

The **ip-mtu** command in the **bof** context configures the MTU for IP packets transmitted out the interface of the management router instance associated to the management port. The command applies to the SR OS but does not necessarily apply during the boot loader processing.

The operational MTU for the port is set to the lesser of the values configured with the **ip-mtu** command and the management port MTU. For example, with the port MTU fixed at 1514 bytes and an Ethernet header size of 14 bytes, the MTU of the management port is1500 bytes (the default operational IP MTU).

If the interface supports IPv6 packets, the command value must be set to 1280 or higher, in accordance with RFC 2460 *Internet Protocol, Version 6 (IPv6) Specification*.

CLI Syntax: `bof# ip-mtu <octets>`

3.6 System Administration Commands in the MD-CLI

For more information about the supported MD-CLI commands, refer to the *7450 ESS, 7750 SR, and 7950 XRS MD-CLI Command Reference Guide*.

Use the following administrative commands to perform management tasks.

- **admin**
  - **reboot** [[**card**] **active** | **standby** | **upgrade**] [**now**]
  - **save** [**bof** | **configure** | **debug** | **li**] [[**url**] *string*]
  - **show**
    - **configuration** [**bof** | **configure** | **debug** | **li**] [**detail** | **units**] [**booted** | **cflash-id**] [**intended** | **running**] [**flat** | **full-context** | **json** | **xml**]

3.6.1 Viewing the Current Configuration

The **admin show configuration** command displays the current configuration for a specified configuration region (the default region is **configure**). The **booted** and **cflash-id** options are valid only for the **bof** configuration region.

- **admin**
  - **show**
    - **configuration** [**bof** | **configure** | **debug** | **li**] [**detail** | **units**] [**booted** | **cflash-id**] [**intended** | **running**] [**flat** | **full-context** | **json** | **xml**]

The following example shows a BOF configuration file with the **detail** option to display all default and unconfigured values and the units option to show **units** where applicable:

```
[/admin]
A:admin@node-2# show configuration bof units detail
...
# Generated THU SEP 03 15:29:11 2020 UTC

bof {
    configuration {
        primary-location "ftp://.../config.cfg"
```

```
 ## secondary-location
 ## tertiary-location
}
console {
    speed 115200 bps
    wait-time 3 seconds
}
dns {
 ## domain
 ## primary-server
 ## secondary-server
 ## tertiary-server
}
image {
    primary-location "ftp://.../i386-both.tim"
 ## secondary-location
 ## tertiary-location
}
li {
    local-save false
    separate false
}
license {
    primary-location "ftp://.../license"
}
port "management" {
    autonegotiate true
    duplex full
    speed 100 megabps
}
router "management" {
    interface "management" {
     ## ip-mtu
        cpm active {
            ipv4 {
                ip-address 192.168.189.52
                prefix-length 24
            }
         ## ipv6
        }
        cpm standby {
         ## ipv4
         ## ipv6
        }
    }
    static-routes {
        route 192.168.0.0/16 {
            next-hop 192.168.189.1
        }
        route 172.16.0.0/16 {
            next-hop 192.168.189.1
        }
    }
}
system {
 ## base-mac-address
    fips-140-2 false
 ## gateway-role
    persistent-indices true
```

```
        ## profile
       }
}
```

3.6.2 Modifying BOF Parameters

Changing the active and standby addresses without rebooting the standby CPM may cause synchronization with the **boot-env** option to fail.

Deleting a BOF address entry is not allowed from a remote session.

BOF parameters can be modified via a BOF session in exclusive, private, or read-only configuration mode in the MD-CLI. The same configuration management commands that are available in the configure region are available in the bof region.

```
[/]
A:admin@node-2# bof exclusive
INFO: CLI #2060: Entering exclusive configuration mode
INFO: CLI #2061: Uncommitted changes are discarded on configuration mode exit

[ex:/bof]
A:admin@node-2# ?

 configuration         + Enter the configuration context
 console               + Enter the console context
 dns                   + Enter the dns context
 image                 + Enter the image context
 li                    + Enter the li context
 license               + Enter the license context
 port                  + Enter the port list instance
 router                + Enter the router list instance
 system                + Enter the system context
```

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide* and Configuring in the MD-CLI in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI User Guide* for more information.

3.6.3 Saving a Configuration

Configuration changes are lost if the system is powered down or the router is rebooted before the changes are saved. If the URL location to save the running configuration is not specified, the files are saved to the location where the files were found for the boot sequence. The same configuration can be saved with different file names to the same location or to different locations.

Changing the active and standby addresses without rebooting the standby CPM may cause synchronization with the **boot-env** option to fail.

The following command saves the running configuration for the configure region. If no URL is specified, the configuration is saved to file config.cfg.

- **admin**
  - **save** [**url**] *string*

```
[/admin]
A:admin@node-2# save
Writing configuration to ftp://.../config.cfg
Saving configuration OK
Completed.
```

The following command saves a BOF configuration:

- **admin**
  - **save bof** [**url**] *string*

The BOF configuration is saved to cf3:\bof.cfg with every **commit** command. The BOF configuration can be manually saved to a backup file on a server or to a different location.

```
[/]
A:admin@node-2# admin save bof ftp://10.9.236.68/backup/node-2/bof.cfg
Writing configuration to ftp://10.9.236.68/backup/node-2/bof.cfg OK
Completed.
```

The following command saves the BOF configuration to the file named testbof.cfg on cf3:

```
[/]
A:admin@node-2# admin save bof testbof.cfg
Writing configuration to cf3:\testbof.cfg OK
Completed.
```

Note: The BOF configuration file is saved in classic format.

3.6.4 Rebooting

When a **reboot** command is issued, routers with redundant CPM are rebooted as well as the XMAs, XCMs, and IOMs. If the **now** option is not specified, the user is prompted to confirm the reboot operation.

Use the following syntax to reboot the router:

- **admin**
  - **reboot** [[**card**] **active** | **standby** | **upgrade**] [**hold**] [**now**]

3.6.5 Setting the MTU Value for the Management Port

The **ip-mtu** command in the **bof router "managment" interface "management"** context configures the MTU for IP packets transmitted out the interface of the management router instance associated to the management port. The command applies to the SR OS but does not necessarily apply during the boot loader processing.

The operational MTU for the port is set to the lesser of the values configured with the **ip-mtu** command and the management port MTU. For example, with the port MTU fixed at 1514 bytes and an Ethernet header size of 14 bytes, the MTU of the management port is1500 bytes (the default operational IP MTU).

If the interface supports IPv6 packets, the command value must be set to 1280 or higher, in accordance with RFC 2460 *Internet Protocol, Version 6 (IPv6) Specification*.

```
[ex:/bof]
A:admin@node-2# router "management" interface "management" ip-mtu ?

 ip-mtu <number>
 <number>  - <512..9786>  - bytes

    Interface IP MTU

    Note: The new value of this element takes effect when the candidate is
    committed.
```

4 Debug Configuration

The **debug** commands enable detailed debugging information for various protocols.

4.1 Debug Commands in the Classic CLI

The **debug** commands in the classic CLI are available by entering the **debug** configuration context.

Debugging configuration is not persistent across CPM switchovers or router reboots.The **admin debug-save** command saves debugging configuration to config.dbg at the BOF **primary-config** location if a URL is not specified. The **show debug** command displays debugging information.

To display debugging output, configure a log using the **from debug-trace** command and then view the output of the log.

For a description of individual **debug** commands, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

4.2 Debug Commands in the MD-CLI

A set of **debug** commands is available natively in the MD-CLI in an exclusive, private, or read-only session via the explicit or implicit configuration mode. The same configuration management commands that are available in the configure region are available in the debug region.

Debugging configuration is not persistent across router reboots.The **admin save debug** command saves debugging configuration to debug.cfg at the BOF **configuration primary-location** if a URL is not specified. The **admin show configuration debug** command displays debugging information and supports all configuration formats, datastores, and output formats that are supported for other regions.

```
[/]
A:admin@node-2# admin show configuration debug
# Generated THU MAY 06 16:13:08 2021 UTC
debug {
    system {
        management-interface {
            netconf info
        }
```

```
    }
}
# Finished THU MAY 06 16:13:08 2021 UTC

[/]
A:admin@node-2# admin save debug
Writing configuration to ftp://.../debug.cfg
Saving configuration OK
Completed.
```

For descriptions of individual **debug** commands, see the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*.

4.2.1 Logging Debug Events in the MD-CLI

The following MD-CLI commands log debug events to an active CLI session.

- **configure**
  - **log**
    - **log-id** [**id**] *string*
      - **source**
        - **debug** *boolean*
      - **destination**
        - **cli**
          - **max-entries** *number*

The following is a sample configuration for debug events that are stored in destination CLI log identifier "7". The log entries wrap at 50 entries (the configured value of **max-entries**).

```
(ex)[configure log]
A:admin@node-2# log-id "7"

*(ex)[configure log log-id "7"]
A:admin@node-2# source debug

*(ex)[configure log log-id "7"]
A:admin@node-2# destination cli max-entries 50

*(ex)[configure log log-id "7"]
A:admin@node-2# info
    source {
        debug true
    }
    destination {
        cli {
            max-entries 50
        }
    }
```

After the **commit** command is issued to include the log in the running configuration, the following **tools** command can be executed in the CLI session that is intended to display outputs of the debug events. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Show, and Tools Command Reference Guide* for more information about the **tools** command.

```
[/]
A:admin@node-2# tools perform log subscribe-to log-id "7"
```

Debug events can be displayed using the **show log** command and cleared using the **clear log** command.

```
[/]
A:admin@node-2# show log log-id "7"
===============================================================================
Event Log 7 log-name 7
===============================================================================
Description : (Not Specified)
Log contents  [size=50   next event=2  (not wrapped)]

---snip---

[/]
A:admin@node-2# clear log log-id "7"
```

The following is an example of terminating the output of the logs to the CLI session using the **unsubscribe-from** command.

```
[/]
A:admin@node-2# tools perform log unsubscribe-from log-id "7"
```

5 Zero Touch Provisioning

Traditional deployment of a new node in a network is a multistep process in which the user connects to the hardware to provision global and local parameters. Zero Touch Provisioning (ZTP) automatically configures a node by obtaining the required information from the network and provisioning the node with minimal manual intervention and configuration. When new nodes that support ZTP are connected and boot up, the node is auto-provisioned.

Note: To support ZTP, make sure the new nodes are purchased with the **auto-boot** flag enabled in the factory-loaded BOF.

5.1 ZTP Overview

ZTP is used to automatically install and provision new nodes in the field. For out-of-band management, the nodes can be installed and powered up with network connectivity on the management (Mgmt) port. For in-band management, the first two connectors on the first two slots can be used for ZTP.

Note: For breakout connectors, only the first breakout port on the first two connectors can be used for ZTP.

ZTP VLAN discovery is enabled by default.

After network connectivity is established, the ZTP process starts automatically. The node sends a DHCP discovery request to the DHCP server using a ZTP-capable port and the DHCP server returns an IPv4/IPv6 FTP or HTTP URL from which the provisioning information can be retrieved. The provisioning information is in a file called the provisioning file, which contains the URL of the image, config, and other files to be downloaded. After downloading these files and successfully provisioning, the node automatically reboots and comes back up in normal mode.

5.1.1 Network Requirements

ZTP requires the following network components:

- **DHCP server (IPv4 or IPv6)**

The DHCP server supports assignment of IP addresses through DHCP requests and offers.

- **file server**

  The FTP or HTTP URL is used for staging and transfer of RPMs, configurations, images, and scripts.

- **DHCP relay**

  DHCP relay is required if the servers are across a Layer 3 network.

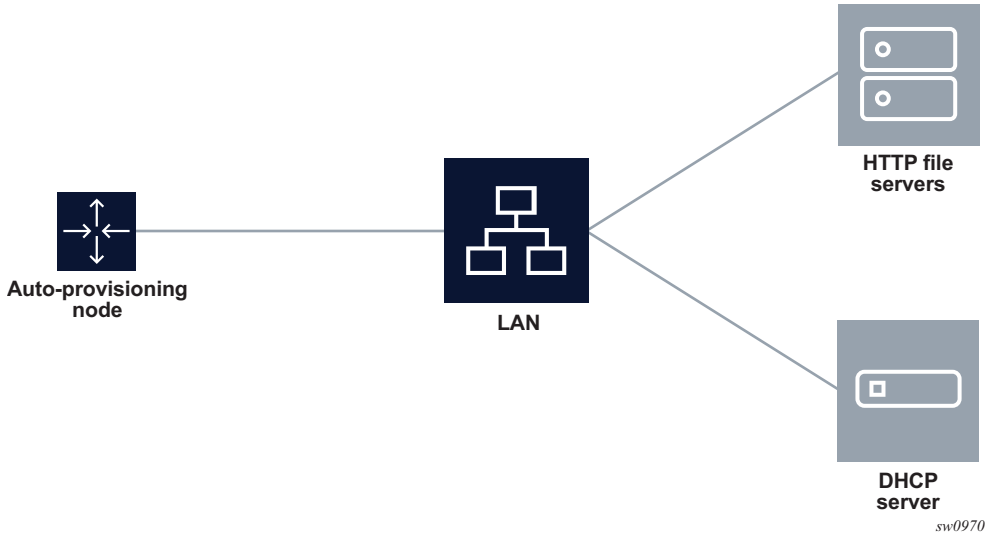
5.1.2 Network Support

ZTP operates in the following network environments:

- **node, file servers, and DHCP server in the same subnet**

  Figure 6 shows the scenario where all components are in a Layer 2 broadcast domain. There is no DHCP relay and all IP addresses are assigned from a single pool.

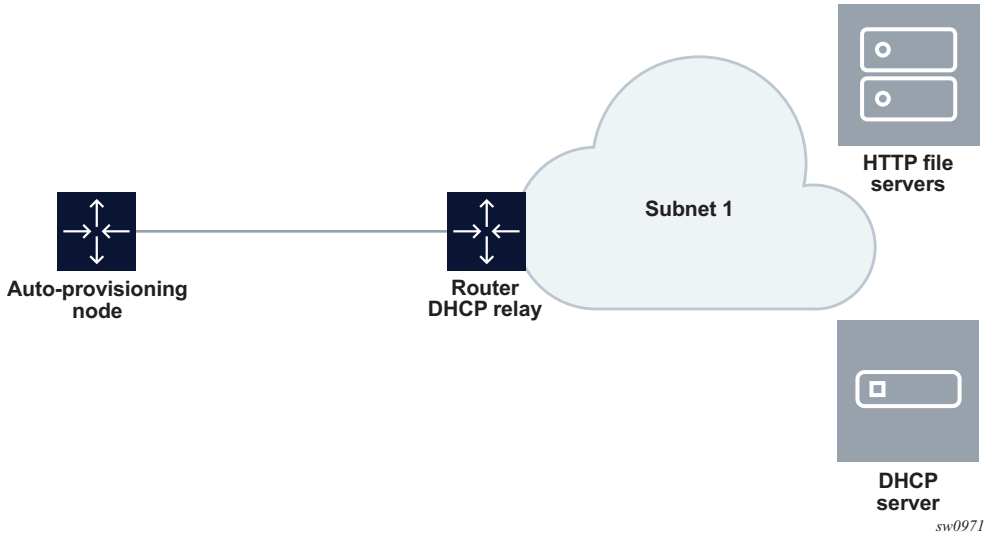
Figure 6 **Auto-provisioning with all Components in a Layer 2 Broadcast Domain**



- **file servers and DHCP server in the same subnet, separate from the node**

  Figure 7 shows the scenario, where only the file servers and DHCP server are in the same subnet. DHCP relay is used to fill Option 82 as the gateway address. The gateway address is used to find the appropriate pool in the DHCP server to assign the correct subnet IP address to the system.

Figure 7 **Auto-provisioning with all Components in a Layer 2 Broadcast Domain**

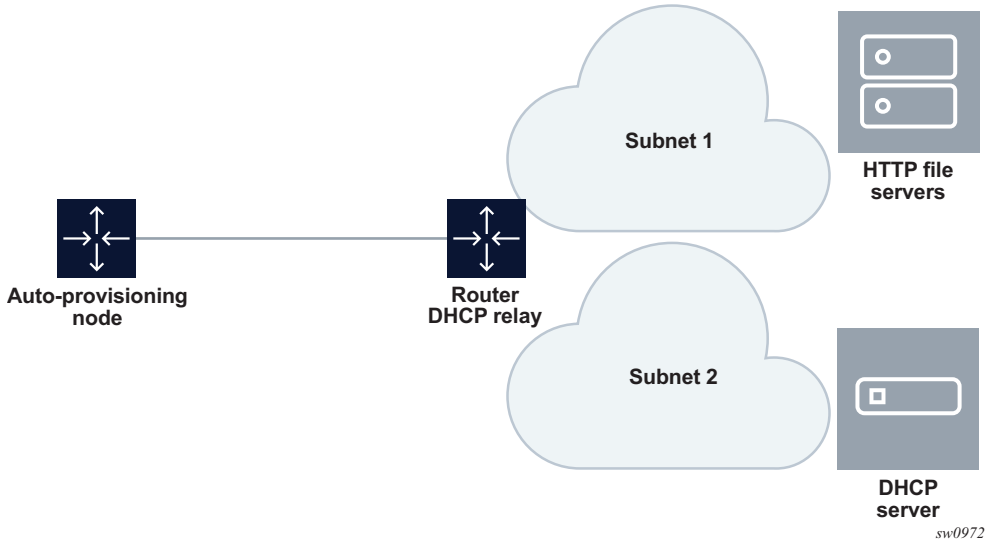


DHCP allows the Option 3 router to define the default gateway. If multiple addresses are provided using Option 3, the first address is used for the default gateway.

- **node, file servers, and DHCP server in different subnets**

  Figure 8 shows the scenario, where all components are in different subnets. DHCP relay adds the Option 82 gateway address to the DHCP request, and the DHCP server adds the Option 3 gateway address of the file server.

Figure 8 **Auto-provisioning with all Components in Different Subnets**



5.2 ZTP Processes

ZTP consists of the following processes:

- auto-boot process
- auto-provisioning process

5.2.1 Auto-boot Process

In this process, the node discovers and provisions the chassis and installed cards.

1. The node is powered up.
2. The out-of-band management port is checked for link connectivity. If a link is not found, the in-band management ports are checked for a link.
3. The first two card or MDA slots are auto-provisioned based on the installed card types. See ZTP Overview for information about the specific card or MDA slots that are used.
4. The auto-boot process switches control to the auto-provisioning process.

See Auto-boot Process for more information about the auto-boot process.

5.2.2 Auto-provisioning Process

In this process, the node detects operational ports, attempts to discover its IP address, and downloads the relevant files for provisioning.

1. The node sends a DHCP discovery request to the DHCP server using the out-of-band management port. If DHCP discovery is unsuccessful, the node reattempts it using the in-band management ports.
2. After DHCP discovery is successful, the DHCP server returns an IPv4 or IPv6 FTP or HTTP URL of a file server from which the node can retrieve provisioning information.
3. The node downloads the provisioning information and performs the auto-provisioning according to the specifications in the files.
4. After the node is successfully provisioned, it automatically reboots and becomes operationally up.

See Auto-provisioning Process for more information about the auto-provisioning process.

The SR OS can also initiate the auto-provisioning process using a **tools** command.

5.3 DHCP Support for ZTP

This section provides information about DHCP messages, DHCP clients, and DHCP servers that are supported by ZTP.

5.3.1 DHCP Server Offer Options 66, 67, and 43

Options 66, 67, and 43 are supported for indicating the location of the provisioning file. If both Options 66 and 67 are present in the DHCP offer, they take precedence over Option 43.

Option 66 contains the server URL or IP address, and Option 67 contains the URL of the provisioning file location.

Options 66 and 67 are meant for use by PXE TFTP, but are also used for HTTP and FTP. If an offer arrives with Options 66 and 67, Option 66 should resolve the server IP address and Option 67 should resolve the file location. Option 66 can be omitted by the provider, in which case Option 67 is used for both the server IP address and provider file URL. If an offer arrives with Option 67 only, it should resolve both the server IP address and file URL.

The auto-provisioning process distinguishes the host part of the URL and can resolve it using DHCP DNS.

5.3.1.1 Nokia-specific TLV

The Nokia-specific TLV is NOKIA-DCTOR-AUTOCONFIG. The location of the BOF for each system to use is configured in the optional **autoboot** file parameter, which is a standard Option 43 value initialized at the beginning of the process. The BOF location is sent in Option 43 as part of the DHCP offer and Ack messages from the DHCP server to the system. The system uses the location specified in Option 43 to initiate an FTP download of the BOF.

5.3.2 Supported DHCP Client Options for ZTP

Table 7 lists the supported DHCP client options for ZTP.

Table 7 **Supported DHCP Client Options for ZTP**

Options	DHCP IPv4 Option	IPv4 Comments	DHCP IPv6 Option	IPv6 Comments
Lease time	Option 51	Always infinite	—	—
Requested option list	Option 55	—	—	—
Client ID	Option 61	Default is chassis serial ID	Option 1 (DUID)	Type 2 — vendor-assigned unique ID (default with chassis serial ID) Type 3 — link-layer address
User class	Option 77	“*platform*;timos-*release*;ztp”	Option 15	“*platform*;timos-*release*;ztp”

Table 7 **Supported DHCP Client Options for ZTP (Continued)**

Options	DHCP IPv4 Option	IPv4 Comments	DHCP IPv6 Option	IPv6 Comments
Class ID	Option 60	“NOKIA: FmtChassisType Strings”	—	—

5.3.3 Supported DHCP Server Options for ZTP

Table 8 lists the supported DHCP server options for ZTP.

Table 8 **Supported DHCP Server Options for ZTP**

Options	DHCP IPv4 Option	IPv4 Comments	DHCP IPv6 Option	IPv6 Comments
Subnet mask	Option 1	—	—	—
Router	Option 3	Default gateway	—	—
DNS server	Option 6	DNS server	—	—
Lease time	Option 51	Must be infinite	—	—
Server address	Option 54	Identifies the DHCP server	—	—
Classless static route	Option 121	Used to install static routes	—	—
NTP server [1]	Option 42	—	Option 56	—
TFTP server name	Option 66	Server IP address	—	—
Bootfile name	Option 67	URL of the file Can be used without Option 66, in which case it will contain the server name and the URL	Option 59	Server name and URL of the file

Table 8 **Supported DHCP Server Options for ZTP (Continued)**

Options	DHCP IPv4 Option	IPv4 Comments	DHCP IPv6 Option	IPv6 Comments
Vendor-specific options (See Nokia-specific TLV)	Option 43	Nokia proprietary file location Can be used instead of Options 66 or 67, but Options 66 and 67 take precedence over Option 43	Option 17	Nokia proprietary file location Can be used instead of Option 59, but Option 59 takes precedence over Option 17

Note:

1. When the node is running in ZTP mode, the date and time are set by NTP. This information is required for HTTPs certificate verification, and to record date and time stamps in events and logs.

5.3.4 DHCP Discovery and Solicitation

IPv4 DHCP discovery and IPv6 DHCP solicitation are supported.

IPv4 DHCP discovery messages and IPv6 DHCP solicitation messages are sent from out-of-band and in-band management ports with active links. The first valid DHCP offer for the address family that arrives on the node is used.

In the BOF, the auto-boot option can be configured to send out IPv4, IPv6, or both IPv4 and IPv6 DHCP requests.

5.3.4.1 DHCP Discovery (IPv4 and IPv6)

This section describes DHCP discovery options.

5.3.4.1.1 DHCP Discovery Options 61 and 77

The SR OS supports both Option 61 (client ID) and Option 77 (user class) DHCP discovery options.

Option 61 provides the client ID; the serial ID of the chassis is used by default. Option 61 is used for DHCP server pool selection. By default, the chassis serial ID is sent in Option 61 with a type of 0. This option is configurable using the **bof auto-boot [client-identifier {string | hex | chassis-mac}]** command.

Option 77 provides the user class, describing what the device is and other information, such as the OS version. This option is set automatically, but can be removed using the BOF configuration. For example, the user can omit **include-user-class** in the BOF auto-boot configuration, to avoid sending Option 77.

For ZTP, the DHCP discovery message should be sent with Option 77; the following information is automatically configured:

platform;timos-*release*;ztp

For auto-provisioning, Option 77 should use the following information:

platform;timos-*release*;AP

5.3.4.1.2 DHCP Discovery Option 1 DUID (IPv6)

By default, the node will use RFC 3315 DUID Type 2 vendor-assigned unique IDs. The value for *enterprise-id* is 6527 and the identifier is the chassis serial number.

Note: The system uses the chassis serial number for ZTP pool selection and auto-provisioning.

The option to use Type 3 is configured in the BOF. For MAC, the chassis MAC address is configured in a string format.

Type 1 is not supported.

5.3.4.2 DHCP Solicitation (IPv6)

Unlike IPv4 DHCP offers, which contain the prefix and default route, IPv6 DHCP offers only contain the IP address assignment. The IPv6 route advertisement (RA) provides the default router and the prefix is set to /128 for the IP address supplied by the DHCP server.

For further information about RA support, see IPv6 DHCP/RA Details. For further information about DHCP server offers, see DHCP Server Offer Options 66, 67, and 43.

5.3.5 IPv4 and IPv6 DHCP Support

The ZTP process supports the use of IPv4 and IPv6 DHCP clients to obtain the provisioning file.

For ZTP processes, the node transmits both IPv4 and IPv6 discovery and solicitation messages. If offers arrive from both IPv4 and IPv6 servers, both offers are cached and the first offer received is processed. If the first offer does not fulfill the ZTP requirements and is rejected, the second offer is processed and accepted or rejected. If both offers received on an interface are rejected, ZTP will go to the next interface.

The provisioning file only allows file transfer in the address family of the DHCP offer that is used. If the offer is IPv4, the provisioning files are downloaded using IPv4. If the offer is IPv6, the provisioning files are downloaded using IPv6.

5.3.5.1 IPv4 Route Installation Details

Option 3 (default route) and Option 121 (classless static route) are supported for IPv4 DHCP.

For identical routes with different next hops, only the first route is installed and the second route is kept as a backup route. ECMP is not supported.

There is no route limit for Option 121.

5.3.5.2 IPv6 DHCP/RA Details

IPv6 DHCP offers do not contain an IP prefix. The IPv6 prefix is usually obtained from the IPv6 RA arriving from the upstream router. For ZTP, the 7750 SR is a host; therefore, the system assigns a /128 prefix to the IPv6 address obtained from the DHCP offer.

The 7750 SR supports the use of an IPv6 RA to install IPv6 default and static routes from upstream routers. The system installs all the routes advertised using the RA. If the same route has been advertised from multiple upstream routers (next hops), the system installs the route with the highest preference. The 7750 SR does not support ECMP if the same route is advertised from multiple next hops by multiple RAs.

In accordance with RFC 4861 recommendations, the 7750 SR ensures that all RAs are obtained before the auto-provisioning process is started for IPv6. RFC 4861 recommends that the host (in this case, the 7750 SR) send a minimum of three route solicitations to increase the likelihood of at least one route solicitation being received by the upstream routers.

Each route solicitation is followed by a 4-second timeout, so the third route solicitation is sent 8 seconds after the first. The upstream routers must respond within 0.5 seconds. As a result, the 7750 SR receives all RAs and routes within 8.5 seconds of the first route solicitation, and will wait a maximum of 9 seconds to receive all RAs; ZTP always waits 20 seconds to receive all RAs, however, only the first RA received will be used.

5.3.5.3 ZTP and DHCP Timeouts

The ZTP timeout interval is 30 minutes. After each ZTP timeout, the node reboots and reattempts the ZTP process. The node does not reboot if the ZTP timeout interval expires while the node is executing a DHCP offer or downloading files. The node executes the DHCP offer until it succeeds or fails, at which point the node reboots; if the offer is successful, the node comes up in normal operation mode.

The DHCP timeout interval is 20 seconds. If a DHCP offer is not received within the DHCP timeout interval, the auto-provisioning process is reattempted using the next valid interface.

5.4 ZTP Procedure Details

This section describes ZTP procedures including node bootup, BOF, auto-provisioning, logs, and events.

5.4.1 Node Bootup

After the node is powered up, the BOF is examined for the **auto-boot** flag status. If the **auto-boot** flag is set in the bof.cfg file, the node goes into ZTP mode. If the **auto-boot** flag is not set in the bof.cfg file, the node continues booting normally.

If it is in ZTP mode, the node provisions all hardware necessary for the ZTP process. This includes the fabric, the first two card slots, and the MDAs for the first two card slots. The node then checks for links on the management (Mgmt) port and valid Ethernet ports.

Note: A bof.cfg file with the **auto-boot** flag enabled can be shipped as an orderable part with the applicable software license. The auto-boot flag can also be set using the **bof>auto-boot** command.

For more information about the BOF, see BOF.

5.4.1.1 Reinitiating ZTP During Normal Node Bootup

ZTP can be reinitiated any time by setting the **auto-boot** flag and configuring the flag options in the BOF. After the auto-boot flag is set, any reboot forces the node into ZTP mode, including DHCP discovery, and downloading and reprocessing the provisioning file. The old BOF is kept in the storage medium until the ZTP process is successful, then the old BOF information is overwritten. If an unsuccessful ZTP process is interrupted and the **auto-boot** flag is removed, the node boots using the old BOF.

5.4.2 BOF

Two versions of each supported 7750 SR platform software license are currently available: one for non-ZTP bootup, and one for ZTP bootup. Software packages for ZTP bootup contain a bof.cfg file with the **auto-boot** flag set, which causes the node to automatically boot up in ZTP mode and execute ZTP processes.

The **auto-boot** flag contains the following information:

- **client ID**

  The client ID is sent to the DHCP server to identify the chassis or node and to find a pool for the DHCP offer. If no client ID is configured, the chassis serial number is sent.

  This option is used for both IPv4 client ID and IPv6 DUID Type 2.

- **port (port:vlan)**

  The port is used to send DHCP discovery; the port number must be configured manually in the BOF.

  For more information about the BOF, see Boot Options.

5.4.2.1 SD Card and Compact Flash Support

Nokia recommends that the provisioning file be downloaded to an SD card, and the BOF should point to the SD card for imaging and configuration.

The BOF does not support loading from the network using HTTP or HTTPS.

5.4.3 Auto-boot Process

This section describes the ZTP auto-boot process.

5.4.3.1 Options and Option Modification

By default, the auto-boot process scans all ZTP-enabled ports to find a port with an operational link. The scanned ports include:

- out-of-band management port (Mgmt port)
- Ethernet ports on the first two card or MDA slots (used for in-band management)

Note: For breakout connectors, only the first breakout port in the connector can be used for ZTP.

ZTP will attempt to discover the node IP via DHCP and will identify the node using DHCP client ID Option 61 (IPv4) or Option 1 (IPv6). The client ID uses the chassis serial number by default. The chassis serial number is visible on the shipping box of the chassis.

Table 7 lists the default DHCP client options for ZTP. Some client options can be manually configured in the BOF using the **bof>auto-boot** command.

The optional **auto-boot** command parameters are as follows:

- [**management-port**]

  This keyword specifies that ZTP should only be performed using the out-of-band management port (Mgmt port).
- [**in-band** [**vlan** *vlan-id*]]

This keyword specifies that ZTP should only be performed using Ethernet ports on the first two card or MDA slots. The *vlan-id* parameter can be used to specify an in-band VLAN to use for the auto-boot process.

- [**ipv4**] [**ipv6**]

  These keywords specify that IPv4 discovery, IPv6 discovery, or both, should be performed. If both keywords are specified, the system will dual-stack.

- [**client-identifier** {**string** *ascii-string* | **hex** *hex-string* | **chassis-mac**}]

  These parameters identify the node to the DHCP server and find a pool for DHCP offers. This information is sent using Option 61 (IPv4) or Option 1 (IPv6). If the parameters are not configured, the chassis serial number is sent by default. This option is used for both IPv4 client ID and IPv6 DUID Type 2.

- [**include-user-class**]

  This keyword specifies that Option 77 should be included.

The **auto-boot** options can be modified using the **bof**>**auto-boot** command, or by interrupting the bootup process and manually modifying the bof.cfg file.

Caution: Manually modifying the bof.cfg file is not recommended. When modifying **auto-boot** options using CLI, all required options must be explicitly configured because the default cases will no longer be used. When modifying the bof.cfg file manually, the format must be correct.

5.4.3.2 CLI Access

The auto-boot process is executed in the background and does not block CLI usage. The user can enter CLI commands while the auto-boot process is running in the background. A warning message is displayed to notify the user that the auto-boot process is being executed. Any configurations performed using the CLI may be lost when the node reboots following successful auto-boot and auto-provisioning processes. After the node has finished booting and if the **auto-boot** flag is set in the BOF, the node displays the login prompt.

The user can access the CLI using a console and can change and save the BOF configuration; the user can remove or modify the **auto-boot** parameter in the BOF.

5.4.3.3 Interrupting Auto-boot

The auto-boot process can be interrupted using the **tools**>**auto-boot terminate** command. After the auto-boot process is terminated, use the **bof**>**auto-boot** command to modify the **auto-boot** flag.

Note: The **auto-boot** flag can also be modified without interrupting the auto-boot process.

5.4.4 Auto-provisioning Process

This section describes the ZTP auto-provisioning process.

See Provisioning Files for information about files that are downloaded during the auto-provisioning process.

5.4.4.1 VLAN Discovery

The node can perform VLAN discovery if it is shipped in ZTP mode. VLAN discovery is supported only for the in-band management port. It is not supported for the out-of-band management ports.

After the node is installed and powered up:

1. ZTP is attempted on the null (untagged) port first, including the out-of-band management port, and then on all in-band management ports with operational links.
   - SR OS scans each port with an operational link and sends IPv4 DHCP discovery messages.
   - SR OS waits for the DHCP offer within the DHCP timeout.
2. If there is no offer or the offer does not have the relevant or correct options, SR OS floods the network with DHCP discovery messages on all remaining non-reserved VLANs (1 to 4094).

   The first VLAN with a valid offer that includes the IPv4 DHCP Options 66 and 67, or Option 67 or 43, or IPv6 DHCP Option 59 or 17 is selected as the working VLAN and the ZTP process is executed on this VLAN.
3. When a VLAN is discovered, the ZTP process is executed on the respective VLAN as described in the following sections.

4. If there is no offer on any VLAN or the offer does not have the relevant or correct options, the node starts over from step 1.

5.4.4.1.1 VLAN Discovery Option

By default, the auto-boot flag in the bof.cfg file has the VLAN discovery option enabled. The option can be disabled manually in the bof.cfg file or implicitly from the CLI bof menu, using the command **bof auto-boot inband**. When the VLAN discovery option is disabled, the node executes the ZTP process using the untagged method only.

5.4.4.2 Auto-provisioning Procedure

After the node enters ZTP mode, the auto-discovery process is executed to provision the necessary hardware for node discovery.

The following are the operational steps of the auto-discovery process.

1. DHCP is used to discover the IP address of the node.
2. Options 66 and 67, or Option 43 is used to find and download the provisioning file.

   The provisioning file includes the location of necessary files, such as configuration information, system image, and licenses, along with the DNS needed to resolve these location URLs. The file also includes BOF information required to boot the node into operational mode.
3. The provisioning file is executed to download the named files to the node.
4. After all files are successfully downloaded, the node is rebooted and the **auto-boot** flag is cleared from the BOF.

After the node reboots, it comes up in normal operational mode.

The node can be put back into ZTP mode by editing the BOF to include the **auto-boot** flag and saving the BOF. Doing so causes the node to enter ZTP mode after it is rebooted.

Use one of the following methods to run the auto-provisioning process.

- **automatic execution**

  The auto-boot process will automatically execute the auto-provisioning process if the **auto-boot** flag is set in the BOF.
- **manual execution**

The auto-provisioning process can be executed manually using the **tools>perform>system>auto-node-provisioning** command.

If the auto-provisioning process is executed manually, only interfaces without IP addresses are considered part of the discovery mechanism. Additionally, while the process is running, it will attempt to discover DHCP servers using all card or MDA slots and ports with Layer 3 interfaces that do not have IP addresses.

Note: Using the **tools>perform>system>auto-node-provisioning** command while the auto-boot process is running is not allowed.

5.4.4.3 Out-of-band Management Versus In-band Management

The auto-provisioning process can use the out-of-band management port (Mgmt port) or in-band management on Ethernet ports.

The node attempts the auto-provisioning process using any port with an operational link, starting with the out-of-band management port. If the node cannot be discovered using the out-of-band management port, either because the port is down or is not receiving a DHCP offer from the DHCP server, the process is reattempted using the Ethernet ports. If the Ethernet ports fail, the management port is tried again and the cycle repeats sequentially.

The following operational guidelines apply to in-band and out-of-band management ports.

- Out-of-band management and in-band management support untagged frames.
- Out-of-band management does not support dot1q (VLAN tags).
- In-band management supports dot1q interfaces if the VLAN is correctly configured in the BOF.
- In-band ports support VLAN Discovery for IPv4 by default, if not disabled in the BOF.

If out-of-band management is used, no card or MDA provisioning is necessary and the auto-provisioning process executes as soon as an active link is detected on the Mgmt port.

To use out-of-band management exclusively, use the **bof>auto-boot management-port** command.

To use in-band management exclusively, use the **bof>auto-boot inband** [**vlan** *vlan-id*] command.

5.4.4.3.1 Supported In-band Management Ports

See ZTP Overview for information about which ports support in-band management for ZTP.

5.4.5 Provisioning Files

Provisioning files are created by the operator, based on requirements and the locations of the necessary files. A provisioning file contains the locations and URLs of critical files, such as the system image, configuration information, and necessary licenses, and can also contain DNS server information used to resolve these locations.

A provisioning file consists of two main parts:

- location of file types

  Contains locations of the following file types:

  - system image
  - configuration information
  - licenses

  These items can be downloaded using HTTP, HTTPS, or FTP; DNS server information can also be included.
- BOF information

  BOF information can be loaded on the node after the ZTP processes are completed; the BOF portion of the file must be formatted correctly.

Caution: Ensure that the **auto-boot** flag is not set on the BOF that will be downloaded by the auto-provisioning process. Failure to do so will cause the node to go back into ZTP mode after it reboots.

The provisioning file is stored on the SD card and can be executed using the **tools>perform>system>auto-node-provisioning>file** command to re-download the named files.

5.4.5.1 Provisioning File Download

The provisioning file location is discovered using DHCP offer Options 66, 67, or 43, and is downloaded using HTTP or FTP.

The provisioning file URL can be resolved using DNS, in which case up to three DNS server IP addresses should be present in the DHCP offer using Option 6 (IPv4). The DHCP DNS is only used for resolving the provisioning file URL, and not for resolving the URLs of the files named within the provisioning file.

ZTP does not support Option 15 domain names; the URL of the provisioning file should be in "*host*/*domain*" format, or a simple IP address should be used.

5.4.5.2 Provisioning File Resolution Using DNS

If the downloaded provisioning file includes a DNS IP in the DNS section of the file, the URLs of the files in the provisioning file must be resolved using this DNS server or by the DNS server listed in the DHCP offer.

Up to three DNS addresses (primary, secondary, tertiary) can be listed in the DNS section of the provisioning file. If all three DNS addresses are listed, they are attempted in the order they are listed, to resolve the file URLs.

5.4.5.3 File Download and Redundancy

Up to three locations can be set for each file type, using the primary-url, secondary-url, and tertiary-url fields. The auto-provisioning process attempts to download all files using the primary-url information for each file. If this attempt is unsuccessful, the process will reattempt using the secondary-url information for each file. If this attempt is not successful, the process will reattempt, using the tertiary-url information.

A ZTP operation is considered successful when all files named in the provisioning file are downloaded. If all file locations are attempted and all named files are not successfully downloaded, the auto-provisioning process fails and ZTP will reattempt the provisioning process using the next valid interface.

5.4.5.4 Sample Provisioning File

The following output is an example of provisioning file information.

```
dns {
    primary 192.0.2.1
    secondary 192.0.2.2
    tertiary 192.0.2.3
    domain sample.domain.com
}
download {
```

```
  image "cf3:/both.tim" {
    primary-url "http://192.168.40.140:81/both.tim"
    secondary-url "http://192.168.40.140:81/both.tim"
    tertiary-url "http://192.168.40.140:81/both.tim"
  }
  image "cf3:/support.tim" {
    primary-url "http://192.168.40.140:81/support.tim"
    secondary-url "http://192.168.40.140:81/support.tim"
    tertiary-url "http://192.168.40.140:81/support.tim"
  }
  config "cf3:/config.cfg" {
    primary-url "ftp://ftpserv:name@192.168.194.50/./images/dut-a.cfg"
    secondary-url "http://192.168.41.140:81/dut-a.cfg"
    tertiary-url "http://192.168.42.140:81/dut-a.cfg"
  }
  file "cf3:/license.txt" {
    primary-url "ftp://ftpserv:name@192.168.194.50/./images/provision_example.cfg"
    secondary-url "http://192.168.41.140:81/dut-a.cfg"
    tertiary-url "http://192.168.42.140:81/dut-a.cfg"
  }
}
bof {
  primary-image cf3:/both.tim
  primary-config cf3:/config.tim
  address 192.168.100.1 active
  autonegotiate
  duplex full
  speed 100
  wait 3
  persist off
  console-speed 115200
}
```

For an HTTPS URL, the trust anchor needs to be referenced in the provisioning file. The trust anchor name references the entry in the import >trust-anchor section of the file. In the following example, the trust anchor name is TRUST_ANCHOR.

```
import {
    client {
        cert "cf3:/client.crt" {
            format pem
            primary-url http://10.10.10.67:81/client.crt
        }
        key "cf3:/client.key" {
            format pem
            primary-url http://10.10.10.67:81/client.key
        }
    }
    trust-anchor TRUST_ANCHOR{
        cert "cf3:/ca.crt" {
            format pem
            primary-url ftp://user-name:password@10.10.10.66//user-name/logs/
fileserver-4/ca.crt
        }
        crl "cf3:/ca.crl" {
            format der
            primary-url ftp://user-name:password@10.10.10.66//user-name/logs/
fileserver-4/ca.crl
```

```
        }
    }
}
<snip>
download {
  config "cf3:/ztp/ztp_dut-a.cfg" {
    primary-url "https://10.10.10.64:81/ztp_dut-a.cfg"
    primary-trust-anchor "TRUST_ANCHOR"
  }
```

5.4.5.5 Proxy Support

HTTP and HTTPS can connect to public servers using a proxy. The proxy is in URL format and the URL must be resolved using the provisioning file DNS.

The proxy can include a username and password. Proxy Auto-Configuration (PAC) is not supported.

Proxy information formatting is as follows:

http://*user@hostname*:*file-path*

https://*user@hostname*:*file-path*

proxy http://*ip-or-url user@hostname*:*port*

The HTTP (or HTTPS) proxy support information is included in **file** commands as *proxy-url* parameter and in the ZTP provisioning file. The following output is an example of HTTP proxy information in the provisioning file:

```
image "cf3:/both.tim" {
    primary-url "http://200.150.40.140:81/both.tim"
    secondary-url "http://200.150.40.140:81/both.tim"
    tertiary-url "http://200.150.40.140:81/both.tim"
    primary-proxy http://132.2.3.1:8080
    secondary-proxy http://133.3.4.1:8080
  }
```

5.4.6 Logs and Events

ZTP displays detailed events about all stages of the auto-boot and auto-provisioning processes. All events are saved in a log file on the SD card at the end of the ZTP process.

6 Tools Commands

The tools commands provide two primary functions:

- dump
- perform

The **tools dump** commands are used to provide additional detailed and enhanced information about various aspects of the router.

The **tools perform** commands provide the ability to trigger a variety of actions in the router such as a card power cycle (**tools perform card power-cycle**), APS switchovers, and so on.

Individual tools commands are described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Show, and Tools Command Reference Guide*.

7 System Management

7.1 System Management Parameters

System management commands allow you to configure basic system management functions such as the system name, the router's location and coordinates, and Common Language Location Identifier (CLLI) code as well as time zones, Network Time Protocol (NTP), Simple Network Time Protocol (SNTP) properties, CRON and synchronization properties.

On SR OS routers, it is possible to query the DNS server for IPv6 addresses. By default, the DNS names are queried for A-records only (address-preference is IPv4-only). If the address-preference is set to IPv6 first, the DNS server is queried for AAAA-records first, and if there is no successful reply, then A-records.

7.1.1 System Information

This section describes system information components.

7.1.1.1 System Name

The system name is the MIB II (RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol* (*SNMPv2*)) sysName object. By convention, this text string is the node's fully-qualified domain name. The system name can be any ASCII-printable text string of up to 64 characters.

7.1.1.2 System Contact

The system contact is the MIB II sysContact object. By convention, this text string is a textual identification of the contact person for this managed node, together with information on how to contact this person. The system contact can be any ASCII-printable text string of up to 80 characters.

7.1.1.3 System Location

The system location is the MIB II sysLocation object which is a text string conventionally used to describe the node's physical location, for example, "Bldg MV-11, 1st Floor, Room 101". The system location can be any ASCII-printable text string of up to 80 characters.

7.1.1.4 System Coordinates

The system coordinates is the Nokia Chassis MIB tmnxChassisCoordinates object. This text string indicates the Global Positioning System (GPS) coordinates of the location of the chassis.

Two-dimensional GPS positioning offers latitude and longitude information as a four dimensional vector:

<direction, hours, minutes, seconds>

where *direction* is one of the four basic values: N, S, W, E, *hours* ranges from 0 to 180 (for latitude) and 0 to 90 for longitude, and minutes and seconds range from 0 to 60.

<W, 122, 56, 89> is an example of longitude and <N, 85, 66, 43> is an example of latitude.

System coordinates can be expressed in different notations, examples include:

- N 45 58 23, W 34 56 12
- N37 37' 00 latitude, W122 22' 00 longitude
- N36*39.246', W121*40.121

The system coordinates can be any ASCII-printable text string up to 80 characters.

7.1.1.5 Naming Objects

Do not configure named objects with a name that starts with "_tmnx_", or with "_" in general.

7.1.1.6 Common Language Location Identifier

A CLLI code string for the device is an 11-character standardized geographic identifier that uniquely identifies the geographic location of places and certain functional categories of equipment unique to the telecommunications industry. The CLLI code is stored in the Nokia Chassis MIB tmnxChassisCLLICode object.

The CLLI code can be any ASCII-printable text string of up to 11 characters.

7.1.1.7 DNS Security Extensions

DNS Security (DNSSEC) Extensions are now implemented in the SR OS, allowing operators to configure DNS behavior of the router to evaluate whether the Authenticated Data bit was set in the response received from the recursive name server and to trust the response, or ignore it.

7.1.2 System Time

SR-series routers are equipped with a real-time system clock for time keeping purposes. When set, the system clock always operates on Coordinated Universal Time (UTC), but the SR-series routers OS software has options for local time translation as well as system clock synchronization.

7.1.2.1 Time Zones

Setting a time zone in SR OS allows for times to be displayed in the local time rather than in UTC. SR OS has both user-defined and system-defined time zones.

A user-defined time zone has a user-assigned name of up to four printable ASCII characters in length and is unique from the system-defined time zones. For user-defined time zones, the offset from UTC is configured as well as any summer time adjustment for the time zone.

SR OS includes multiple commands to control the presentation of times in either UTC or local time zone format. For a CLI session, the environment variable **time-display** may be set to indicate UTC or local time zone. This setting only affects time strings shown during that specific CLI session. In addition, a global setting of **config**>**system**>**time**>**prefer-local-time** can be used to control time strings for objects with larger scope that a single CLI session, including the following:

- log filenames and log header information
- times in rollback information
- times in rollback and configuration files header information
- times related to CRON scripts
- times in the event handler system

A separate control per log file controls the format of the time strings on the event recorded into the logs (separate from the log filename and header information). Use the **config>log>log-id>time-format** command to set these time strings.

The SR OS system-defined time zones are listed in Table 9, which includes both time zones with and without summer time correction.

Table 9 **System-Defined Time Zones**

Acronym	Time Zone Name	UTC Offset
Europe		
GMT	Greenwich Mean Time	UTC
BST	British Summer Time	UTC +1
IST	Irish Summer Time	UTC +1*
WET	Western Europe Time	UTC
WEST	Western Europe Summer Time	UTC +1
CET	Central Europe Time	UTC +1
CEST	Central Europe Summer Time	UTC +2
EET	Eastern Europe Time	UTC +2
EEST	Eastern Europe Summer Time	UTC +3
MSK	Moscow Time	UTC +3
MSD	Moscow Summer Time	UTC +4
US and Canada		
AST	Atlantic Standard Time	UTC -4
ADT	Atlantic Daylight Time	UTC -3
EST	Eastern Standard Time	UTC -5
EDT	Eastern Daylight Saving Time	UTC -4

Table 9 **System-Defined Time Zones (Continued)**

Acronym	Time Zone Name	UTC Offset
ET	Eastern Time	Either as EST or EDT, depending on place and time of year
CST	Central Standard Time	UTC -6
CDT	Central Daylight Saving Time	UTC -5
CT	Central Time	Either as CST or CDT, depending on place and time of year
MST	Mountain Standard Time	UTC -7
MDT	Mountain Daylight Saving Time	UTC -6
MT	Mountain Time	Either as MST or MDT, depending on place and time of year
PST	Pacific Standard Time	UTC -8
PDT	Pacific Daylight Saving Time	UTC -7
PT	Pacific Time	Either as PST or PDT, depending on place and time of year
HST	Hawaiian Standard Time	UTC -10
AKST	Alaska Standard Time	UTC -9
AKDT	Alaska Standard Daylight Saving Time	UTC -8
Australia		
AWST	Western Standard Time (e.g., Perth)	UTC +8
ACST	Central Standard Time (e.g., Darwin)	UTC +9.5
AEST	Eastern Standard/Summer Time (e.g., Canberra)	UTC +10

7.1.2.2 Network Time Protocol (NTP)

NTP is the Network Time Protocol defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis* and RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*. It allows for the participating network nodes to keep time more accurately and more importantly they can maintain time in a more synchronized fashion between all participating network nodes.

SR OS uses an NTP process based on a reference build provided by the Network Time Foundation. Nokia strongly recommends that the users review RFC 8633, *Network Time Protocol Best Current Practices*, when they plan to use NTP with the router. The RFC section “Using Enough Time Sources” indicates that using only two time sources (NTP servers) can introduce instability if they provide conflicting information. To maintain accurate time, Nokia recommends configuring three or more NTP servers.

NTP uses stratum levels to define the number of hops from a reference clock. The reference clock is considered to be a stratum-0 device that is assumed to be accurate with little or no delay. Stratum-0 servers cannot be used in a network. However, they can be directly connected to devices that operate as stratum-1 servers. A stratum-1 server is an NTP server with a directly-connected device that provides Coordinated Universal Time (UTC), such as a GPS or atomic clock.

The higher stratum levels are separated from the stratum-1 server over a network path, thus, a stratum-2 server receives its time over a network link from a stratum-1 server. A stratum-3 server receives its time over a network link from a stratum-2 server.

SR OS routers normally operate as a stratum-2 or higher device. The router relies on an external stratum-1 server to source accurate time into the network. However, SR OS also allows for the use of the local PTP recovered time to be sourced into NTP. In this latter case, the local PTP source appears as a stratum-0 server and SR OS advertises itself as a stratum-1 server. Activation of the PTP source into NTP may impact the network NTP topology because the SR OS router is promoted to stratum-1.

SR OS router runs a single NTP clock which then operates NTP message exchanges with external NTP clocks. Exchanges can be made with external NTP clients, servers, and peers. These exchanges can be through the base, management, or VPRN routing instances.

NTP operates associations between clocks as either client or server, symmetric active and symmetric passive, or broadcast modes. These modes of operation are applied according to which elements are configured on the router. To run server mode, the operator must enable NTP server mode for the base and each desired VPRN routing instance. To run client mode, the operator must configure external servers. If both the local router and remote router are configured with each other as peers, then the router operates in symmetric active mode. If only one side of the association has peering configured, then the modes are symmetric passive. To operate using broadcast mode, interfaces must be configured to transmit as broadcast servers or receive as broadcast clients.

NTP server operation for both unicast and broadcast communication within a VPRN is configured within the VPRN (refer to the NTP Within a VPRN Service section in *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN*).

Note: NTP provides lightweight synchronization across a network for alignment of system time for logging purposes. NTP does not provide the high accuracy time needed for the on-air applications of the mobile base stations. The more recent PTP protocol has been developed for these applications (see Network Synchronization).

The following NTP elements are supported:

- Server mode — In this mode, the node advertises the ability to act as a clock source for other network elements. The node, by default, transmits NTP packets in NTP version 4 mode.
- Authentication keys — Authentication keys implement increased security support in carrier and other networks. Both DES and MD5 authentication are supported, as well as multiple keys.
- Operation in symmetric active mode — This capability requires that NTP be synchronized with a specific node that is considered more trustworthy or accurate than other nodes carrying NTP in the system. This mode requires that a specific peer is set.
- Server and peer addressing using IPv6 — Both external servers and external peers may be defined using IPv6 or IPv4 addresses. Other features (such as multicast, broadcast) use IPv4 addressing only.
- Broadcast or multicast modes — When operating in these modes, the node receives or sends using either a multicast (default 224.0.1.1) or a broadcast address. Multicast is supported only on the CPM MGMT port.
- Alert when NTP server is not available — When none of the configured servers are reachable on the node, the system reverts to manual timekeeping and issues a critical alarm. When a server becomes available, a trap is issued indicating that standard operation has resumed.
- NTP and SNTP — If both NTP and SNTP are enabled on the node, then SNTP transitions to an operationally down state. If NTP is removed from the configuration or shut down, then SNTP resumes an operationally up state.
- Gradual clock adjustment — As several applications (such as Service Assurance Agent (SAA)) can use the clock, and if determined that a major (128 ms or more) adjustment needs to be performed, the adjustment is performed by programmatically stepping the clock. If a minor (less than 128 ms) adjustment must be performed, then the adjustment is performed by either speeding up or slowing down the clock.

- In order to avoid the generation of too many events/trap the NTP module rates limit the generation of events/traps to three per second. At that point a single trap is generated that indicates that event/trap squashing is taking place.

7.1.2.3 SNTP Time Synchronization

For synchronizing the system clock with outside time sources, the SR OS includes a Simple Network Time Protocol (SNTP) client. As defined in RFC 2030, SNTP Version 4 is an adaptation of the Network Time Protocol (NTP). SNTP typically provides time accuracy within 100 milliseconds of the time source. SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP is a compact, client-only version of NTP. SNTP does not authenticate traffic.

SNTP can be configured in both unicast client modes (point-to-point) and broadcast client modes (point-to-multipoint). SNTP should be used only at the extremities of the synchronization subnet. SNTP clients should operate only at the highest stratum (leaves) of the subnet and in configurations where no NTP or SNTP client is dependent on another SNTP client for synchronization. SNTP time servers should operate only at the root (stratum 1) of the subnet and then only in configurations where no other source of synchronization other than a reliable radio clock is available. External servers may only be specified using IPv4 addresses.

In the SR OS, the SNTP client can be configured for either broadcast or unicast client mode.

7.1.2.4 CRON

The CRON feature supports periodic and date and time-based scheduling in SR OS. CRON can be used, for example, to schedule Service Assurance Agent (SAA) functions. CRON functionality includes the ability to specify scripts that need to be run, when they are scheduled, including one-time only functionality (one-shot), interval and calendar functions. Scheduled reboots, peer turn ups, service assurance agent tests and more can all be scheduled with CRON, as well as OAM events, such as connectivity checks, or troubleshooting runs.

CRON supports the schedule element. The schedule function configures the type of schedule to run, including one-time only (one-shot), periodic, or calendar-based runs. All runs are determined by month, day of month or weekday, hour, minute, and interval (seconds).

7.2 High Availability

This section discusses the high availability (HA) routing options and features available to service providers that help diminish vulnerability at the network or service provider edge and alleviate the effect of a lengthy outage on IP networks.

High availability is an important feature in service provider routing systems. High availability is gaining momentum due to the unprecedented growth of IP services and applications in service provider networks driven by the demand from the enterprise and residential communities. Downtime can be very costly, and, in addition to lost revenue, customer information and business-critical communications can be lost. High availability is the combination of continuous uptime over long periods (Mean Time Between Failures (MTBF)) and the speed at which failover or recovery occurs (Mean Time To Repair (MTTR)).

The popularity of high availability routing is evident at the network or service provider edge where thousands of connections are hosted and rerouting options around a failed piece of equipment can often be limiting. Or, a single access link exists to a customer because of additional costs for redundant links. As service providers converge business-critical services such as real-time voice (VoIP), video, and VPN applications over their IP networks, high availability becomes much more stringent compared to the requirements for best-effort data. Network and service availability become critical aspects when offering advanced IP services which dictates that IP routers that are used to construct the foundations of these networks be resilient to component and software outages.

For high availability configuration information, see Synchronization and Redundancy.

7.2.1 HA Features

As more and more critical commercial applications move onto the IP/MPLS networks, providing high availability services becomes increasingly important. This section describes high availability features for routers. Most of these features only apply to routers with two Control Processor Modules (CPM).

7.2.1.1 Redundancy

The redundancy features enable the duplication of data elements and software functionality to maintain service continuation in case of outages or component failure.

Refer to the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter and Extended Services Appliance Guide* for information about redundancy for the Integrated Service Adapter (ISA).

7.2.1.1.1 Software Redundancy

Software outages are challenging even when baseline hardware redundancy is in place. There should be a balance to provide high availability routing otherwise router problems typically propagate not only throughout the service provider network, but also externally to other connected networks possibly belonging to other service providers. This could affect customers on a broad scale. Presently, there are several software availability features that contribute to the percentage of time that a router is available to process and forward traffic.

To fully appreciate high availability, you should realize that all routing protocols specify minimum time intervals in which the peer device must receive an acknowledgment before it disconnects the session.

- OSPF default session timeout is approximately 40 seconds. The timeout intervals are configurable.
- BGP default session timeout is approximately 120 seconds. The timeout intervals are configurable for the 7750 SR and 7950 XRS only.

Therefore, router software has to recover faster than the specified time interval to maintain up time.

7.2.1.1.2 Configuration Redundancy

Features configured on the active device CPM are saved on the standby CPM as well. When the active device CPM fails, these features are brought up on the standby device CPM that takes over the mastership.

Even with modern modular and stable software, the failure of route processor hardware or software can cause the router to reboot or cause other service impacting events. In the best circumstances, failure leads to the initialization of a redundant route processor, which hosts the standby software configuration, to become the active processor. The following options are available.

- Warm standby — The router image and configuration is already loaded on the standby route processor. However, the standby could still take a few minutes to become effective since it must first re-initialize connections by bringing up Layer 2 connections and Layer 3 routing protocols and then rebuild routing tables.
- Hot standby — The router image, configuration, and network state is already loaded on the standby and it receives continual updates from the active route processor and the swapover is immediate. However, hot standby affects conventional router performance as more frequent synchronization increases consumption of system resources. Nokia's newer generation service routers address this issue because they already have extra processing built into the system.

7.2.1.1.3 Component Redundancy

Component redundancy is critical to reduce MTTR for the system and primarily consists of the following router features:

- Dual route processor modules — For a highly available architecture, redundant Control Processor Modules (CPM) are essential. The route processing functions of the CPM calculate the most efficient route to an Internet destination and communicate the best path information to peer routers. Rapid information synchronization between the primary and secondary CPMs is crucial to minimize recovery time.
- Switch fabric (SFM) redundancy — Failure of a single switch fabric card with little to no loss of traffic.
- Redundant line cards — LAG, ECMP and other techniques to spread traffic over multiple line cards so that a failure of one line card does not impact the services being delivered.
- Redundant power supply — A power module can be removed without impact on traffic.
- Redundant fan — Failure of a fan module without impacting traffic.
- Hot swap — Components in a live system can be replaced or become active without taking the system down or affecting traffic flow to/from other modules.

Router hardware architecture plays a key role in the availability of the system. The principle router architecture styles are centralized and distributed. In these architectures, both active and standby route processors, I/O modules (IOMs) (also called line cards), fans, and power supplies maintain a low MTTR for the routing system.

However, in a centralized architecture, packet processing and forwarding is performed in a central shared route processor and the individual line cards are relatively simple. The cards rely solely on the route processor for routing and forwarding intelligence and, should the centralized route processor fail, there is greater impact to the system overall, as all routing and packet forwarding stops.

In a distributed system, the packet forwarding functionality is situated on each line card. Distributing the forwarding engines off the central route processor and positioning one on each line card lowers the impact of route processor failure as the line cards can continue to forward traffic during an outage.

The distributed system is better suited to enable the convergence of business critical services such as real-time voice (VoIP), Video, and VPN applications over IP networks with superior performance and scalability. The centralized architecture can be prone to performance bottleneck issues and limits service offerings through poor scalability which may lead to customer and service SLA violations.

7.2.1.1.4 Service Redundancy

All service-related statistics are kept during a switchover. Services, SDPs, and SAPs remains up with a minimum loss of forwarded traffic during a CPM switchover.

7.2.1.1.5 Accounting Configuration Redundancy

When there is a switchover and the standby CPM becomes active, the accounting servers are checked and if they are administratively up and capable of coming online (media present, and so on), the standby is brought online and new accounting files are created at that point. Users must manually copy the accounting records from the failed CPM.

7.2.1.2 Nonstop Forwarding

In a control plane failure or a forced switchover event, the router continues to forward packets using the existing stale forwarding information. Nonstop forwarding requires clean control plane and data plane separation. Usually the forwarding information is distributed to the IOMs, XCMs and XMAs.

Nonstop forwarding is used to notify peer routers to continue forwarding and receiving packets, even if the route processor (control plane) is not working or is in a switch-over state. Nonstop forwarding requires clean control plane and data plane separation and usually the forwarding information is distributed to the line cards. This method of availability has both advantages and disadvantages. Nonstop forwarding continues to forward packets using the existing stale forwarding information during a failure. This may cause routing loops and black holes, and also requires that surrounding routers adhere to separate extension standards for each protocol. Every router vendor must support protocol extensions for interoperability.

7.2.1.3 Nonstop Routing (NSR)

With NSR on the SR-series router devices, routing neighbors are unaware of a routing process fault. If a fault occurs, a reliable and deterministic activity switch to the inactive control complex occurs such that routing topology and reachability are not affected, even in the presence of routing updates. NSR achieves high availability through parallelization by maintaining up to date routing state information, at all times, on the standby route processor. This capability is achieved independently of protocols or protocol extensions, providing a more robust solution than graceful restart protocols between network routers.

The NSR implementation on the SR-series routers supports all routing protocols. NSR makes it possible to keep the existing sessions (BGP, LDP, OSPF, etc.) during a CPM switchover, including support for MPLS signaling protocols. Peers do not see any change.

Protocol extensions are not required. There are no interoperability issues and there is no need to define protocol extensions for every protocol. Unlike nonstop forwarding and graceful restart, the forwarding information in NSR is always up to date, which eliminates possible blackholes or forwarding loops.

Traditionally, addressing high availability issues have been patched through non-stop forwarding solutions. With the implementation of NSR, these limitations are overcome by delivering an intelligent hitless failover solution. This enables a carrier-class foundation for transparent networks, required to support business IP services backed by stringent SLAs. This level of high availability poses a major issue for conventional routers whose architectural design limits or prevents them from implementing NSR.

7.2.1.4 CPM Switchover

During a switchover, system control and routing protocol execution are transferred from the active to the standby CPM.

An automatic switchover may occur under the following conditions:

- A fault condition that causes the active CPM to crash or reboot.
- The active CPM is declared down (not responding).
- Online removal of the active CPM.

A manual switchover can occur under the following conditions:

- To force a switchover from an active CPM to a standby, use the admin redundancy force-switchover command. You can configure a batch file that executes after failover by using the **config system switchover-exec** CLI command.

7.2.1.5 Synchronization

Synchronization between the CPMs includes the following:

- Configuration and boot-env Synchronization
- State Database Synchronization

7.2.1.5.1 Configuration and boot-env Synchronization

Configuration and boot-env synchronization are supported in **admin>redundancy>synchronize** and **config>redundancy>synchronize** contexts.

7.2.1.5.2 State Database Synchronization

If a new standby CPM is inserted into the system, it synchronizes with the active CPM upon a successful boot process.

If the standby CPM is rebooted, it synchronizes with the active CPM upon a successful boot process.

When configuration or state changes occur, an incremental synchronization is conducted from the active CPM to the standby CPM.

If the synchronization fails, the standby does not reboot automatically. The **show redundancy synchronization** command displays synchronization output information.

If the active and standby are not synchronized for some reason, users can manually synchronize the standby CPM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CPM.

7.3 Synchronization and Redundancy

SR-series routers supporting redundancy use a 1:1 redundancy scheme. Redundancy methods facilitate system synchronization between the active and standby Control Processor Modules (CPMs) so they maintain identical operational parameters to prevent inconsistencies in the event of a CPM failure.

When automatic system synchronization is enabled for an entity, any save or delete file operations configured on the primary, secondary or tertiary choices on the active CPM file system are mirrored in the standby CPM file system.

Although software configurations and images can be copied or downloaded from remote locations, synchronization can only occur locally between compact flash drives (cf1:, cf2:, and cf3:).

Synchronization can occur either:

- Automatically — Automatic synchronization is disabled by default. To enable automatic synchronization, the **config>redundancy>synchronization** command must be specified with either the **boot-env** parameter or the **config** parameter.

  When the **boot-env** parameter is specified, the BOF, boot.ldr, config, YANG schema files and image files are automatically synchronized.If the schema YANG files are not found, the files are not copied but the rest of the synchronization is not affected.

When the **config** parameter is specified, only the config files are automatically synchronized.

Automatic synchronization also occurs whenever the BOF is modified and when an **admin>save** command is entered with no filename specified.

- Manually — To execute synchronization manually, the **admin>redundancy> synchronization** command must be entered with the **boot-env** parameter or the **config** parameter.

  When the **boot-env** parameter is specified, the BOF, boot.ldr, config, YANG schema files and image files are synchronized.If the schema YANG files are not found, the files are not copied, but the rest of the synchronization is not affected.

  When the **config** parameter is specified, only the config files are synchronized.

  The following shows the output displayed during a manual synchronization of configuration files.

```
A:ALA-12>admin>redundancy# synchronize config
Syncing configuration......

Syncing configuration.....Completed.
A:ALA-12#
```

7.3.1 Active and Standby Designations

Typically, the first Switch Fabric (SF)/CPM card installed in a redundant SR-series router chassis assumes the role as active, regardless of being inserted in Slot A or B. The next CPM installed in the same chassis then assumes the role as the standby CPM. If two CPM are inserted simultaneously (or almost simultaneously) and are booting at the same time, then preference is given to the CPM installed in Slot A.

If only one CPM is installed in a redundant router device, then it becomes the active CPM regardless of the slot it is installed in.

The active and standby designations can be visually determined by LEDs on the CPM/CCM faceplate. Refer to the appropriate platform *Installation* Guide for LED indicator details.

The following output shows that the CPM installed in Slot A is acting as the active CPM and the CPM installed in Slot B is acting as the standby.

The following is an example of the 7950 XRS output:

```
*A:7950 XRS-20# show card
===============================================================================
Card Summary
===============================================================================
Slot   Provisioned Type                          Admin Operational   Comments
```

```
           Equipped Type (if different)            State State
-------------------------------------------------------------------------------
1      xcm-x20                                     up    provisioned
A      cpm-x20                                     up    up/active
B      cpm-x20                                     up    up/standby
===============================================================================
```

The following console message displays when a CPM boots, sees an active CPM, and becomes the standby CPM:

```
...
Slot A contains the Active CPM
This CPM (Slot B) is the Standby CPM
```

7.3.2 When the Active CPM Goes Offline

When an active CPM goes offline (due to reboot, removal, or failure), the standby CPM takes control without rebooting or initializing itself. It is assumed that the CPMs are synchronized, therefore, there is no delay in operability. When the CPM that went offline boots and then comes back online, it becomes the standby CPM.

When the standby CPM comes online, the following output is shown:

```
Active CPM in Slot A has stopped
Slot B is now active CPM


Attempting to exec configuration file:
'cf3:/config.cfg' ...

...

Executed 49,588 lines in 8.0 seconds from file cf3:\config.cfg
```

7.3.3 OOB Management Ethernet Port Redundancy

The SR OS platform provides a resilient out-of-band (OOB) management Ethernet redundancy mode for system management.

When the management Ethernet port is down on the active CPM, the OOB Ethernet redundancy feature allows the active CPM to use the management Ethernet port of the standby CPM, as shown in Figure 9 and Figure 10.

OOB management Ethernet port redundancy is enabled using the **config**>**redundancy**>**mgmt-ethernet** command.

Figure 9 **Management Ethernet: Normal Mode**

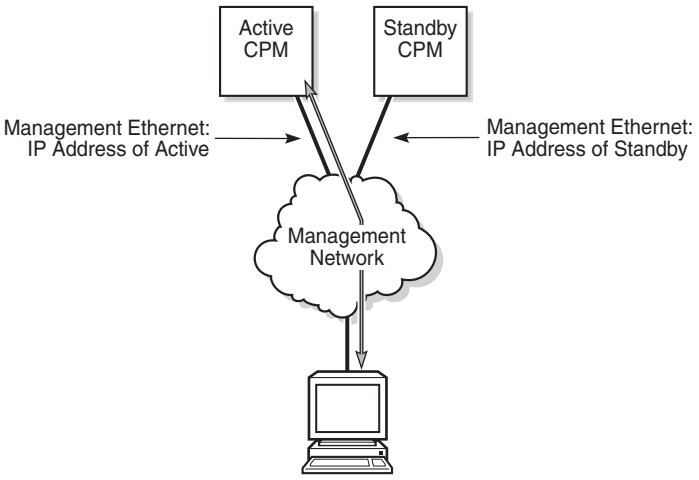
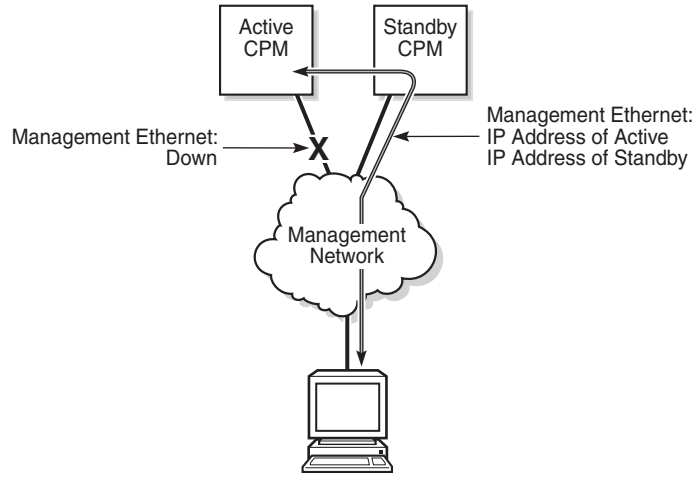


Figure 10 **Management Ethernet: Redundancy Mode**



7.3.4 Persistence

The persistence feature on the 7750 SR allows information learned through DHCP snooping across reboots to be kept. This information can include data such as the IP address, MAC binding information, lease length information, and ingress SAP information (required for VPLS snooping to identify the ingress interface). This information is referred to as the DHCP lease-state information.

When a DHCP message is snooped, there are steps that make the data persistent in a system with dual CPMs. In systems with only one CPM, only Step 1 applies. In systems with dual CPMs, all steps apply.

1. When a DHCP ACK is received from a DHCP server, the entry information is written to the active CPM Compact Flash. If writing was successful, the ACK is forwarded to the DHCP client. If persistency fails completely (bad cflash), a trap is generated indicating that persistency can no longer be guaranteed. If the complete persistency system fails the DHCP ACKs are still forwarded to the DHCP clients. Only during small persistency interruptions or in overload conditions of the Compact Flash, DHCP ACKs may get dropped and not forwarded to the DHCP clients.
2. DHCP message information is sent to the standby CPM and also there the DHCP information is logged on the Compact Flash. If persistency fails on the standby also, a trap is generated.

7.3.4.1 Dynamic Data Persistency (DDP) Access Optimization for DHCP Leases

A high rate of DHCP renewals can create a load on the compact flash file system when subscriber management and/or DHCP server persistence is enabled. To optimize the access to the Dynamic Data Persistency (DDP) files on the compact flash, a lease-time threshold can be specified that controls the eligibility of a DHCP lease for persistency updates when no other data other than the lease expiry time is to be updated.

```
configure
    system
        persistence
            subscriber-mgmt
                location cf2:
            exit
            dhcp-server
                location cf2:
            exit
            options
                dhcp-leasetime-threshold [days <days>] [hrs <hours>]
```

```
[min <minutes>] [sec <seconds>]
            exit
        exit
    exit
```

When the offered lease time of the DHCP lease is less than the configured threshold, the lease is flagged to skip persistency updates and is installed with its full lease time upon a persistency recovery after a reboot.

The **dhcp-leasetime-threshold** command controls persistency updates for:

- DHCPv4 and DHCPv6 leases for a DHCP relay or proxy (enabled with **persistence subscriber-mgmt**)
- DHCPv4 leases for DHCP snooping in a VPLS service (enabled with **persistence subscriber-mgmt**)
- DHCPv4 and DHCPv6 leases for a DHCP server (enabled with **persistence dhcp-server**)

To check if a DHCP relay or proxy lease is flagged to skip persistency updates, use the **tools dump persistence submgt record** *record-key* CLI command. When flagged to skip persistency updates, the persistency record output includes “Skip Persistency Updates: true”.

To check if a DHCP server lease is flagged to skip persistency updates, use the **tools dump persistence dhcp-server record** *record-key* CLI command. When flagged to skip persistency updates, the persistency record output includes “lease mode : LT” (LT = Lease Time) and a “lease time : …” field. When not flagged to skip persistency updates, the persistency record output includes “lease mode : ET” (ET = Expiry Time) and an “expires : …” field.

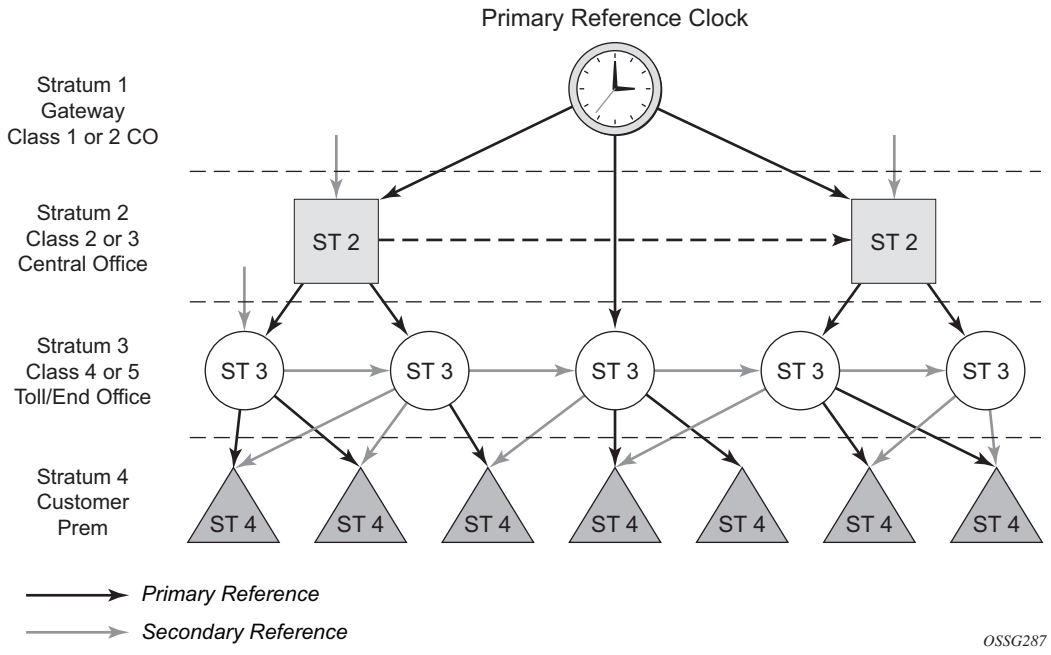
7.4 Network Synchronization

This section describes network synchronization capabilities available on SR OS platforms. These capabilities involve multiple approaches to network timing; namely SDH/SONET, Synchronous Ethernet, BITS, and Adaptive clocking and a Precision Time Protocol (PTP) IEEE 1588v2. These features address barriers to entry by:

- Providing synchronization quality required by the mobile space; such as radio operations and circuit emulation services (CES) transport.
- Augmenting and potentially replacing the existing (SONET/SDH) timing infrastructure and delivering high quality network timing for time sensitive applications in the wireline space.

Network synchronization is commonly distributed in a hierarchical master-slave topology at the physical layer as shown in Figure 11.

Figure 11 **Conventional Network Timing Architecture (North American Nomenclature)**



The architecture shown in Figure 11 provides the following benefits:

- Limits the need for high quality clocks at each network element and only requires that they reliably replicate input to remain traceable to its reference.
- Uses reliable physical media to provide transport of the timing signal; it doesn't consume any bandwidth and requires limited additional processing.

The synchronization network is designed so a clock always receives timing from a clock of equal or higher stratum or quality level. This ensures that if an upstream clock has a fault condition (for example, loses its reference and enters a holdover or free-run state) and begins to drift in frequency, the downstream clock is able to follow it. For greater reliability and robustness, most offices and nodes have at least two synchronization references that can be selected in priority order (such as primary and secondary).

Further levels of resiliency can be provided by designing a capability in the node clock that operates within prescribed network performance specifications without any reference for a specified time-frame. A clock operating in this mode is said to hold the last known state over (or holdover) until the reference lock is once again achieved. Each level in the timing hierarchy is associated with minimum levels of network performance.

Each synchronization capable port can be independently configured to transmit data using the node reference timing or loop timing. In addition, some TDM channels can use adaptive timing.

Transmission of a reference clock through a chain of Ethernet equipment requires that all equipment supports Synchronous Ethernet. A single piece of equipment that is not capable of performing Synchronous Ethernet breaks the chain. Ethernet frames still get through but downstream devices should not use the recovered line timing as it is be traceable to an acceptable stratum source.

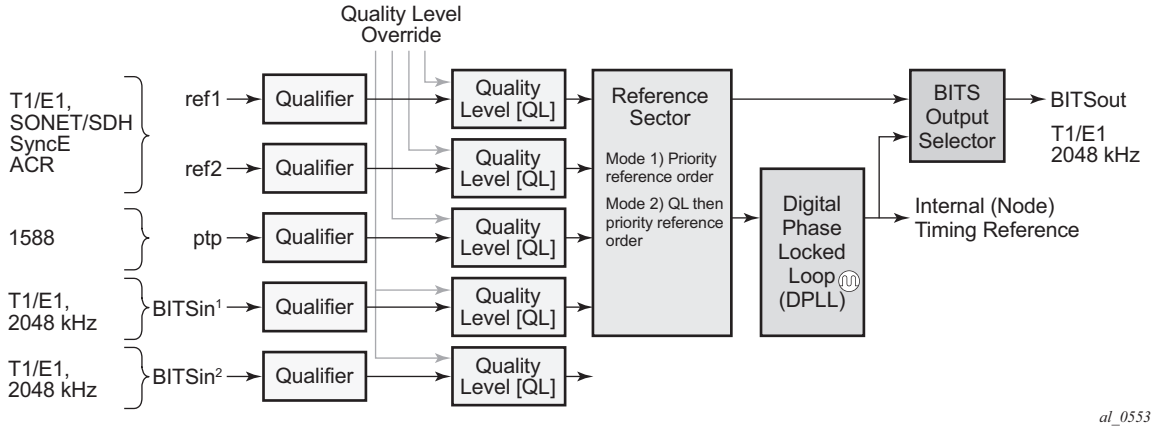
7.4.1 Central Synchronization Sub-System

The timing subsystem for the platforms has a central clock located on the CPM (motherboard). The timing subsystem performs many of the duties of the network element clock as defined by Telcordia (GR-1244-CORE) and ITU-T G.781.

The system can select from up to three (7950 XRS) or four (7450 ESS and 7750 SR) timing inputs to train the local oscillator. The priority order of these references must be specified. This is a simple ordered list of inputs: {bits, ref1, ref2, ptp}. The CPM clock output shall have the ability to drive the clocking for all line cards in the system. The routers support selection of the node reference using Quality Level (QL) indications. See Figure 12 for a description of the synchronization selection process for the CPM clock.

Note: Not all signals are available on all platforms.

Figure 12 **CPM Clock Synchronization Reference Selection**



The recovered clock can derive its timing from any of the following:

- OC3/STM1, OC12/STM4, OC48/STM16, OC192/STM64 ports (7450 ESS and 7750 SR only)
- T1/E1 CES channel (adaptive clocking) (7750 SR only)
- Synchronous Ethernet ports
- T1/E1 port (7750 SR only)
- BITS port on the CPM or CCM module
- 10GE ports in WAN PHY mode
- IEEE 1588v2 slave port (PTP) (7450 ESS and 7750 SR only)
- SyncE/1588 port on the CPM or the CCM

The BITS ports accept T1 or E1 signal formats. Some hardware also supports the 2048 kHz signal format. The format must be common between all BITSin and BITSout ports.

All settings of the signal characteristics for the BITS input apply to both ports. When the active CPM considers the BITS input as a possible reference, it first considers the BITS input port on the active CPM or CCM followed by the BITS input port on the standby CPM or CCM in that relative priority order. This relative priority order is in addition to the user-definable **ref-order**. For example, a **ref-order** of **bits ref1 ref2** would actually be BITS in (active CPM or CCM), followed by BITS in (standby CPM or CCM), followed by ref1, followed by ref2. When **ql-selection** is enabled, the QL of each BITS input port is viewed independently. The higher QL source is chosen.

When the active CPM considers the SyncE/1588 as a possible reference, the active CPM first considers the SyncE/1588 port on the active CPM or CCM, followed by the SyncE/1588 port on the standby CPM or CCM in that relative priority order. This relative priority order is in addition to the user-definable **ref-order**. For example, a **ref-order** of **synce ref1 ref2** would actually be SyncE/1588 (active CPM or CCM), followed by SyncE/1588 (standby CPM or CCM), followed by ref1, followed by ref2. When **ql-selection** is enabled, the QL of each SyncE/1588 input port is viewed independently. The higher QL source is chosen.

The following behavior applies to the platform architecture existing on 7750 SR-7/12/12e, 7750 SR-2s/7s/14s, 7750 SR-1e/2e/3e, 7750 SR-a4/a8, and 7450 ESS-7/12: When the BITS or SyncE port on the standby CPM is an option as input reference into the central clock of the active CPM, a display of the central clock data on the standby CPM indicates that it is locked to its local BITS or SyncE input. This is expected behavior and required to make the BITS input on the standby available to the active CPM as an option for reference selection.

The restrictions on the location for the source-port or source-bits for **ref1** and **ref2** are listed in Table 10.

Table 10 **Ref1 and Ref2 Timing References**

Platform	Ref1 Slots	Ref2 Slots	Notes
7450 ESS-7	1 to 2	3 to 5	—
7450 ESS-12	1 to 5	6 to 10	—
7750 SR-1	1	1	Ref1 and ref2 cannot be on the same MDA
7750 SR-7	1 to 2	3 to 5	—
7750 SR-12	1 to 5	6 to 10	—
7750 SR-12e	1 to 5	6 to 9	—
7750 SR-a4	1	1	Ref1 and ref2 cannot be on the same MDA. Two CPMs must be installed to allow two references to be used.
7750 SR-a8	1 to 2	1 to 2	Ref1 and ref2 cannot be on the same slot.
7750 SR-1e	1	1	Ref1 and ref2 cannot be on the same MDA
7750 SR-2e	1 to 2	1 to 2	Ref1 and ref2 cannot be on the same MDA

Table 10 **Ref1 and Ref2 Timing References (Continued)**

Platform	Ref1 Slots	Ref2 Slots	Notes
7750 SR-3e	1 to 3	1 to 3	Ref1 and ref2 cannot be on the same MDA
7750 SR-1s	1	1	Ref1 and ref2 cannot be on the same MAC chip. Refer to the *7750 SR-1s Installation Guide* or use the **show datapath** command for the mappings.
7750 SR-2s	1 to 2	1 to 2	Ref1 and ref2 cannot be on the same slot.
7750 SR-7s	1 to 6	1 to 6	Ref1 and ref2 cannot be on the same slot. Slot 6 cannot be used if a CPM has been installed in that slot.
7750 SR-14s	1 to 6	1 to 6	Ref1 and ref2 cannot be on the same slot.
7950 XRS-20	1 to 10	1 to 10	Ref1 and ref2 cannot be on the same slot
7950 XRS-20e	1 to 10	1 to 10	Ref1 and ref2 cannot be on the same slot
7950 XRS-40	1 to 10	1 to 10	Ref1 and ref2 cannot be on the same slot

The BITS output ports can be configured to provided either the unfiltered recovered line clock from a line card port or the output of the central clock. The first case would be used if the port was connected to deliver an input reference directly to dedicated timing device in the facility (BITS or SASE device). The second case would be used to test the quality of the clocking used by the router.

When QL selection mode is disabled, then the reversion setting controls when the central clock can re-select a previously failed reference.

The Table 11 shows the selection followed for two reference in both revertive and non-revertive modes:

Table 11 **Revertive, non-Revertive Timing Reference Switching Operation**

Status of Reference A	Status of Reference B	Active Reference Non-revertive Case	Active Reference Revertive Case
OK	OK	A	A
Failed	OK	B	B
OK	OK	B	A
OK	Failed	A	A
OK	OK	A	A
Failed	Failed	holdover	holdover
OK	Failed	A	A
Failed	Failed	holdover	holdover
Failed	OK	B	B
Failed	Failed	holdover	holdover
OK	OK	A or B	A

7.4.2 7950 XRS-40 Extension Chassis Central Clocks

The central clock architecture described above applies to each chassis of the 7950 XRS-40. There is a central clock located on each of the CPMs present in the extension chassis. However, there is no configuration for the central clocks on the CPMs of the extension chassis. The central clocks only use the BITS input ports of the extension chassis for their input reference. It is assumed that the quality of the reference provided into the BITS input ports of the extension chassis CPMs is equal to the quality of the Master chassis central clocks. Refer to the *Installation* Guide for appropriate physical cabling to support this architecture.

7.4.3 Synchronization Status Messages (SSM)

SSM provides a mechanism to allow the synchronization distribution network to both determine the quality level of the clock sourcing a given synchronization trail and to allow a network element to select the best of multiple input synchronization trails. Synchronization Status messages have been defined for various transport protocols including SONET/SDH, T1/E1, and Synchronous Ethernet, for interaction with office clocks, such as BITS or SSUs and embedded network element clocks.

SSM allows equipment to autonomously provision and reconfigure (by reference switching) their synchronization references, while helping to avoid the creation of timing loops. These messages are particularly useful to allow synchronization reconfigurations when timing is distributed in both directions around a ring.

The following sections provide details about the SSM message functionality for different signal types. These functions apply to all platforms that support the given signal type.

7.4.3.1 DS1 Signals

DS1 signals can carry an indication of the quality level of the source generating the timing information using the SSM transported within the 1544 kb/s Extended Super Frame (ESF) Data Link (DL) of the signal as specified in Recommendation G.704. No such provision is extended to SF formatted DS1 signals.

The format of the data link messages in ESF frame format is "0xxx xxx0 1111 1111", transmitted rightmost bit first. The six bits denoted "xxx xxx" contain the actual message; some of these messages are reserved for synchronization messaging. It takes 32 frames (such as 4 ms) to transmit all 16 bits of a complete DL.

7.4.3.2 E1 Signals

E1 signals can carry an indication of the quality level of the source generating the timing information using the SSM as specified in Recommendation G.704.

One of the Sa4 to Sa8 bits, (the actual Sa bit is for operator selection), is allocated for Synchronization Status Messages. To prevent ambiguities in pattern recognition, it is necessary to align the first bit (San1) with frame 1 of a G.704 E1 multi-frame.

The numbering of the San (n = 4, 5, 6, 7, 8) bits. A San bit is organized as a 4-bit nibble San1 to San4. San1 is the most significant bit; San4 is the least significant bit.

The message set in San1 to San4 is a copy of the set defined in SDH bits 5 to 8 of byte S1.

7.4.3.3 SONET/SDH Signals

The SSM of SDH and SONET interfaces is carried in the S1 byte of the frame overhead. Each frame contains the four bit value of the QL.

7.4.3.4 DS3/E3

DS3/E3 signals are not required to be synchronous. However, it is acceptable for their clocking to be generated from a synchronization source. The 7750 SR and the 7450 ESS permit E3/DS3 physical ports to be specified as a central clock input reference.

DS3/E3 signals do not support an SSM channel. QL-override should be used for these ports if ql-selection is enabled

7.4.4 Synchronous Ethernet

Traditionally, Ethernet-based networks employ the physical layer transmitter clock to be derived from an inexpensive +/-100ppm crystal oscillator and the receiver locks onto it. There is no need for long term frequency stability because the data is packetized and can be buffered. For the same reason there is no need for consistency between the frequencies of different links. However, you can derive the physical layer transmitter clock from a high quality frequency reference by replacing the crystal with a frequency source traceable to a primary reference clock. This would not affect the operation of any of the Ethernet layers, for which this change would be transparent. The receiver at the far end of the link would lock onto the physical layer clock of the received signal, and thus itself gain access to a highly accurate and stable frequency reference. Then, in a manner analogous to conventional hierarchical master-slave network synchronization, this receiver could lock the transmission clock of its other ports to this frequency reference and a fully time synchronous network could be established.

The advantage of using Synchronous Ethernet, compared with methods that rely on sending timing information in packets over an unclocked physical layer, is that it is not influenced by impairments introduced by the higher levels of the networking technology (packet loss, packet delay variation). Hence, the frequency accuracy and stability may be expected to exceed those of networks with unsynchronized physical layers.

Synchronous Ethernet allows operators to gracefully integrate existing systems and future deployments into conventional industry-standard synchronization hierarchy. The concept behind synchronous Ethernet is analogous to SONET/SDH system timing capabilities. It allows the operator to select any (optical) Ethernet port as a candidate timing reference. The recovered timing from this port is then used to time the system (for example, the CPM locks to this configured reference selection). The operator then could ensure that any of system output would be locked to a stable traceable frequency source.

If the port is a fixed copper Ethernet port and in 1000BASE-T mode of operation, there is a dependency on the 802.3 link timing for the Synchronous Ethernet functionality (refer to ITU-T G.8262). The 802.3 link Master-Slave timing states must align with the desired direction of Synchronous Ethernet timing flow. When a fixed copper Ethernet port is specified as an input reference for the node or when it is removed as an input reference for the node, an 802.3 link auto-negotiation is triggered to ensure the link timing aligns properly.

The SSM of Synchronous Ethernet uses an Ethernet OAM PDU that uses the slow protocol subtype. For a complete description of the format and processing, refer to ITU-T G.8264.

7.4.5 Clock Source Quality Level Definitions

The following clock source quality levels have been identified for the purpose of tracking network timing flow. These levels make up all of the defined network deployment options given in Recommendation G.803 and G.781. The Option I network is a network developed on the original European SDH model; whereas, the Option II network is a network developed on the North American SONET model.

In addition to the QL values received over SSM of an interface, the standards also define additional codes for internal use. These include the following:

- QL INVx is generated internally by the system if and when an unallocated SSM value is received, where x represents the binary value of this SSM. All of these independent values are assigned as the singled value of QL-INVALID.
- QL FAILED is generated internally by the system if and when the terminated network synchronization distribution trail is in the signal fail state.

There is also an internal quality level of QL-UNKNOWN. This is used to differentiate from a received QL-STU code but is equivalent for the purposes of QL selection.

Table 12 lists the synchronization message coding and source priorities for SSM received.

Table 12 **Synchronization Message Coding and Source Priorities — SSM Value Received on Port**

SSM value received on port				
SDH interface SyncE interface in SDH mode	**SONET Interface SyncE interface in SONET mode**	**E1 interface**	**T1 interface (ESF)**	**Internal Relative Quality Level**
0010 (prc)	0001 (prs)	0010 (prc)	00000100 11111111 (prs)	1 - Best quality
	0000 (stu)		00001000 11111111 (stu)	2
	0111 (st2)		00001100 11111111 (ST2)	3
0100 (ssua)	0100 (tnc)	0100 (ssua)	01111000 11111111 (TNC)	4
	1101 (st3e)		01111100 11111111 (ST3E)	5
1000 (ssub)		1000 (ssub)		6
	1010 (st3/eec2)		00010000 11111111 (ST3)	7
1011 (sec/eec1)		1011 (sec)		8 - Lowest quality qualified in QL-enabled mode
	1100 (smc)		00100010 11111111 (smc)	9
			00101000 11111111 (st4)	10
	1110 (pno)		01000000 11111111 (pno)	11
1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)	12
Any other	Any other	Any other	N/A	13- QL_INVALID
				14- QL-FAILED
				15 - QL-UNC

Table 13 lists the synchronization message coding and source priorities for SSM transmitted.

Table 13 **Synchronization Message Coding and Source Priorities — SSM Values Transmitted by Interface of Types**

SSM values to be transmitted by interface of type				
Internal Relative Quality Level	**SDH interface SyncE interface in SDH mode**	**SONET Interface SyncE interface in SONET mode**	**E1 interface**	**T1 interface (ESF)**
1 - Best quality	0010 (prc)	0001 (PRS)	0010 (prc)	00000100 11111111 (PRS)
2	0100 (ssua)	0000 (stu)	0100 (ssua)	00001000 11111111 (stu)
3	0100 (ssua)	0111 (st2)	0100 (ssua)	00001100 11111111 (st2)
4	0100 (ssua)	0100 (tnc)	0100 (ssua)	01111000 11111111 (tnc)
5	1000 (ssub)	1101 (st3e)	1000 (ssub)	01111100 11111111 (st3e)
6	1000 (ssub)	1010 (st3/eec2)	1000 (ssub)	00010000 11111111 (st3)
7	1011 (sec/eec1)	1010 (st3/eec2)	1011 (sec)	00010000 11111111 (st3)
8 - Lowest quality qualified in QL-enabled mode	1011 (sec/ eec1)	1100 (smc)	1011 (sec)	00100010 11111111 (smc)
9	1111 (dnu)	1100 (smc)	1111 (dnu)	00100010 11111111 (smc)
10	1111 (dnu)	1111 (dus)	1111 dnu	00101000 11111111 (st4)
11	1111 (dnu)	1110 (pno)	1111 (dnu)	01000000 11111111 (pno)
12	1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)
13- QL_INVALID	1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)
14- QL-FAILED	1111 (dnu)	1111 (dus)	1111 (dnu)	00110000 11111111 (dus)
15 - QL-UNC	1011 (sec/eec1)	1010 (st3/eec2)	1011 (sec)	00010000 11111111 (st3)

Note: When the internal Quality level is in the range of 9 through 14, the output codes shown in Table 13, only appear if QL selection is disabled. If ql-selection is enabled, then all of these internal states are changed to internal state 15 (Holdover) and the ssm value generated reflects the holdover quality of the internal clock.

7.4.6 Advanced G.781 Features

The central clock of the node supports several advanced features of the G.781 standard. These include the specification of a minimum acceptable QL value for the input references, the specification of a minimum acceptable QL value for the BITS output port, the ability to squelch the BITS output signal, and the specification of a Wait To Restore timer for input references. These features allow for more options in the management of the synchronization topology.

7.4.7 IEEE 1588v2 PTP

Precision Time Protocol (PTP) is a timing-over-packet protocol defined in the IEEE 1588v2 standard 1588 PTP 2008.

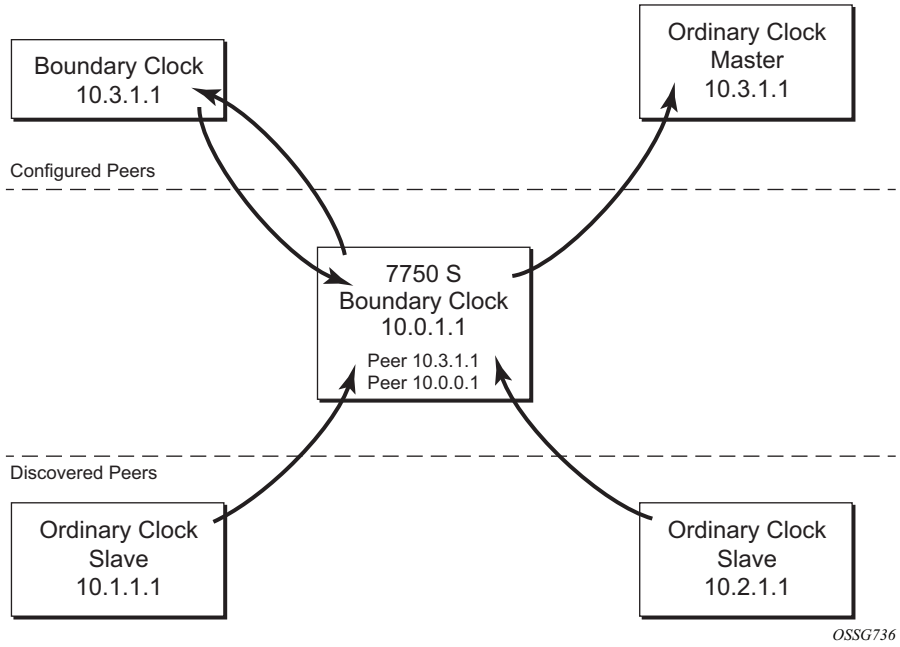
PTP may be deployed as an alternative timing-over-packet option to Adaptive Clock Recovery (ACR). PTP provides the capability to synchronize network elements to a Stratum-1 clock or primary reference clock (PRC) traceable frequency source over a network that may or may not be PTP-aware. PTP has several advantages over ACR. It is a standards-based protocol, has lower bandwidth requirements, can transport both frequency and time, and can potentially provide better performance.

Support is provided for an ordinary clock in slave or master mode or a boundary clock. When configured as an ordinary clock master, PTP can only be used for the distribution of a frequency reference, not a time reference. The boundary clock and ordinary clock slave can be used for both frequency and time distribution.

The ordinary clock master, ordinary clock slave, and boundary clock communicate with neighboring IEEE 1588v2 clocks. These neighbor clocks can be ordinary clock masters, ordinary clock slaves, or boundary clocks. The communication can be based on either unicast IPv4 sessions transported through IP interfaces or multicast Ethernet transported through Ethernet ports.

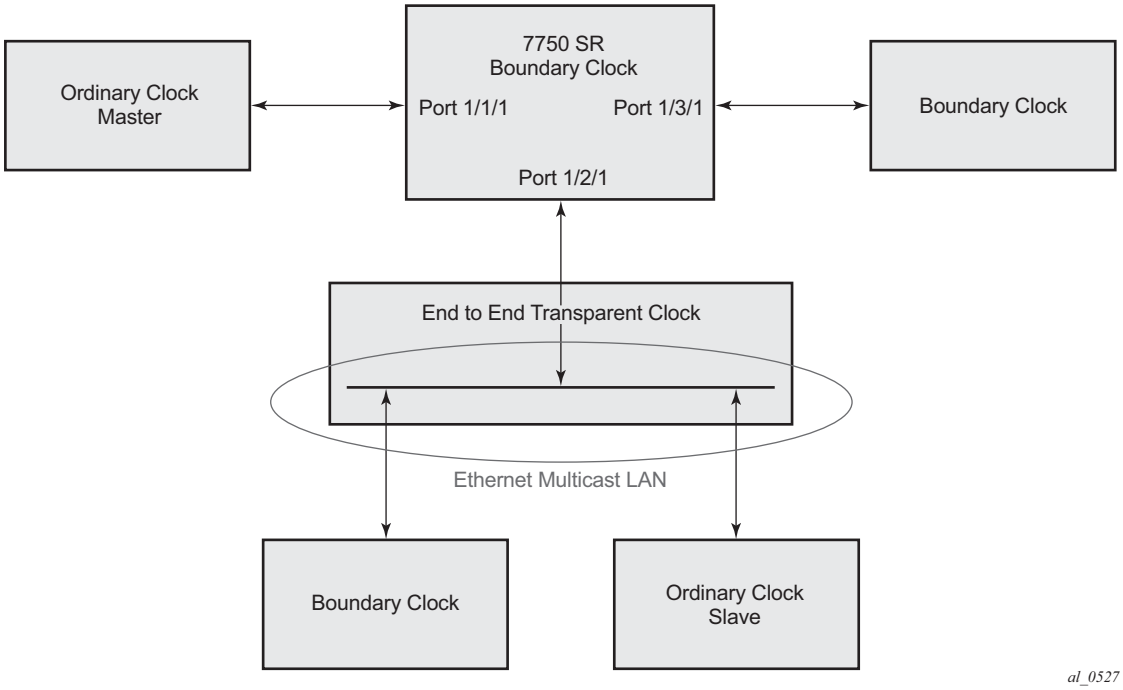
For the unicast IP sessions, the external clocks are labeled 'peers'. There are two types of peers: configured and discovered. An ordinary clock slave or a boundary clock should have configured peers for each PTP neighbor clock from which it might accept synchronization information. The router initiates unicast sessions with all configured peers. An ordinary clock master or boundary clock accepts unicast session requests from external peers. If the peer is not a configured peer, then it is considered a discovered peer. An ordinary clock master or boundary clock can deliver synchronization information toward discovered peers. Figure 13 shows the relationship of various neighbor clocks using unicast IP sessions to communicate with a 7750 SR configured as a boundary clock with two configured peers.

Figure 13 **Peer Clocks**



For multicast Ethernet operation, the router shall listen for and transmit PTP messages using the configured multicast MAC address. Neighbor clocks are discovered via the reception of messages through an enabled Ethernet port. An ordinary clock master, ordinary clock slave, and a boundary clock support more than one neighbor PTP clock connecting into a single port. This might be encountered with the deployment of an Ethernet multicast LAN segment between the local clock and the neighbor PTP ports using an End to end transparent clock or an Ethernet switch. The Ethernet switch is not recommended due to the introduction of PDV and the potential degradation of performance but it can be used if appropriate to the application. Figure 14 shows the relationship of various neighbor clocks using multicast Ethernet sessions to a 7750 SR configured as a boundary clock. The 7750 SR has three ports configured for multicast Ethernet communications. Port 1/2/1 of the 7750 SR shows a connection where there are two neighbor clocks connecting to one port of the 7750 SR through an end-to-end transparent clock.

Figure 14 **Ethernet Multicast Ports**



The ordinary clock master, ordinary clock slave, and boundary clock allow for PTP operation over both unicast IPv4 and multicast Ethernet at the same time.

The IEEE 1588v2 standard includes the concept of PTP profiles. These profiles are defined by industry groups or standards bodies that define how IEEE 1588v2 is to be used for a particular application.

Currently, three profiles are supported:

- IEEE 1588v2 default profile
- ITU-T Telecom profile for frequency (G.8265.1)
- ITU-T Telecom profile for time with full timing support (G.8275.1)

When an ordinary clock slave or a boundary clock receive *Announce* messages from one or more configured peers or multicast neighbors, it executes a Best Master Clock Algorithm (BMCA) to determine the state of communication between itself and the peers. The system uses the BMCA to create a hierarchical topology allowing the flow of synchronization information from the best source (the Grandmaster clock) out through the network to all boundary and slave clocks. Each profile has a dedicated BMCA.

If the **profile** setting for the clock is ieee1588-2008, the precedence order for the best master selection algorithm is as follows:

- priority1
- clockClass
- clockAccuracy
- PTP variance (offsetScaledLogVariance)
- priority2
- clockIdentity
- stepsRemoved from the grandmaster

The ordinary clock master, ordinary clock slave, and boundary clock set their local parameters as listed in Table 14:

Table 14 **Local Clock Parameters When Profile is set to ieee1588-2008**

Parameter	Value
clockIdentity	Chassis MAC address following the guidelines of 7.5.2.2.2 of IEEE 1588
clockClass	13 — local clock configured as ordinary clock master and is locked to an external reference 14 — local clock configured as ordinary clock master and in holdover after having been locked to an external source 248 — local clock configured as ordinary clock master and is in free run or the router is configured as a boundary clock 255 — local clock configured as ordinary clock slave
clockAccuracy	FE — unknown
offsetScaledLogVariance	FFFF — not computed

If the **profile** setting for the clock is g8265dot1-2010, the precedence order for the best master selection algorithm is:

- clockClass
- priority

The ordinary clock master, ordinary clock slave, and boundary clock set their local parameters as listed in Table 15:

Table 15 **Local Clock Parameters When Profile is set to: itu-telecom-freq**

Parameter	Value
clockClass	80-110 — value corresponding to the QL out of the central clock as per Table 1/G.8265.1 255 — the clock is configured as ordinary clock slave

The g8265dot1-2010 profile is for use in an environment with only ordinary clock masters and slaves for frequency distribution.

If the **profile** setting for the clock is g8275dot1-2014, the precedence order for the best master selection algorithm is very similar to that used with the default profile. It ignores the **priority1** parameter, includes a **localPriority** parameter and includes the ability to force a port to never enter slave state (**master-only**). The precedence is as follows:

- clockClass
- clockAccuracy
- PTP variance (offsetScaledLogVariance)
- priority2
- localPriority
- clockIdentity (See Note)
- stepsRemoved from the grandmaster

Note: If the two clocks being compared have a clockClass less than 128, then this step is skipped. skipping this step will be the normal case as the vast majority of clocks used as grandmasters advertise clockClass less than 128.

The ordinary clock master, ordinary clock slave, and boundary clock set their local parameters as listed in Table 16:

Table 16 **Local Clock Parameters When Profile is set to: g8275dot1-2014**

Parameter	Value
clockIdentity	Chassis MAC address following the guidelines of 7.5.2.2.2 of IEEE 1588

Table 16 **Local Clock Parameters When Profile is set to: g8275dot1-2014**

Parameter	Value
clockClass	165 — local clock configured to a boundary clock and the boundary clock was previously locked to a grandmaster with a clock class of 6 248 — local clock configured as boundary clock 255 — local clock configured as ordinary clock slave
clockAccuracy	FE — unknown
offsetScaledLogVariance	FFFF — not computed

There is a limit on the number of external PTP clocks to which the ordinary clock slave or boundary clock requests unicast service (# configured peers) and also a limit to the number of external PTP clocks to which the ordinary clock master or boundary clock grants unicast service (# discovered peers). An association where the boundary clock has a symmetric relationship with another boundary clock (in other words, they both have the other as a configured peer) consumes a request and a grant unicast service in each router.

The number of configured Ethernet ports is not restricted.

There are limits to the maximum transmitted and received event message rates supported in the router. Each unicast IP service established consumes a portion of one of the unicast message limits. Once either limit is reached, additional unicast service requests are refused by sending a grant response with zero in the duration field.

Refer to the scaling guide for the appropriate release for the specific unicast message limits related to PTP.

Multicast messages are not considered when validating the unicast message limit. When multicast messaging on Ethernet ports is enabled, the PTP load needs to be monitored to ensure the load does not exceed the capabilities. There are several commands that can be used for this monitoring:

- The **show system cpu** command identifies the load of the PTP software process. If the capacity usage reaches 100%, the PTP software process on the router is at its limit of transmitting and/or receiving PTP packets.

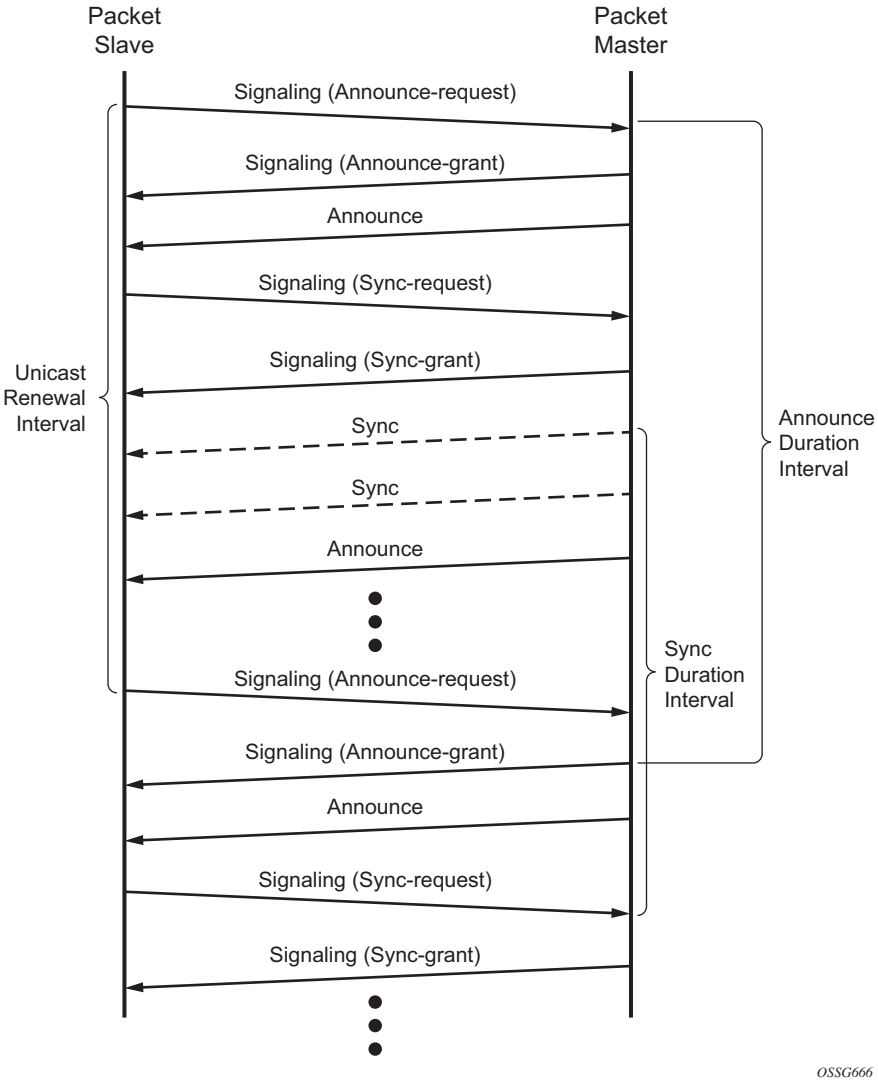
Because the user cannot control the amount of PTP messages being received over the Ethernet ports, the statistics commands can be used to identify the source of the message load:

- **show system ptp statistics** has aggregate packet rates

- **show system ptp port** and **show system ptp port** *port-id* [**detail**] display received packet rates

Figure 15 shows the unicast negotiation procedure performed between a slave and a peer clock that is selected to be the master clock. The slave clock requests Announce messages from all peer clocks but only request Sync and Delay_Resp messages from the clock selected to be the master clock.

Figure 15 **Messaging Sequence Between the PTP Slave Clock and PTP Master Clock**



7.4.7.1 PTP Clock Synchronization

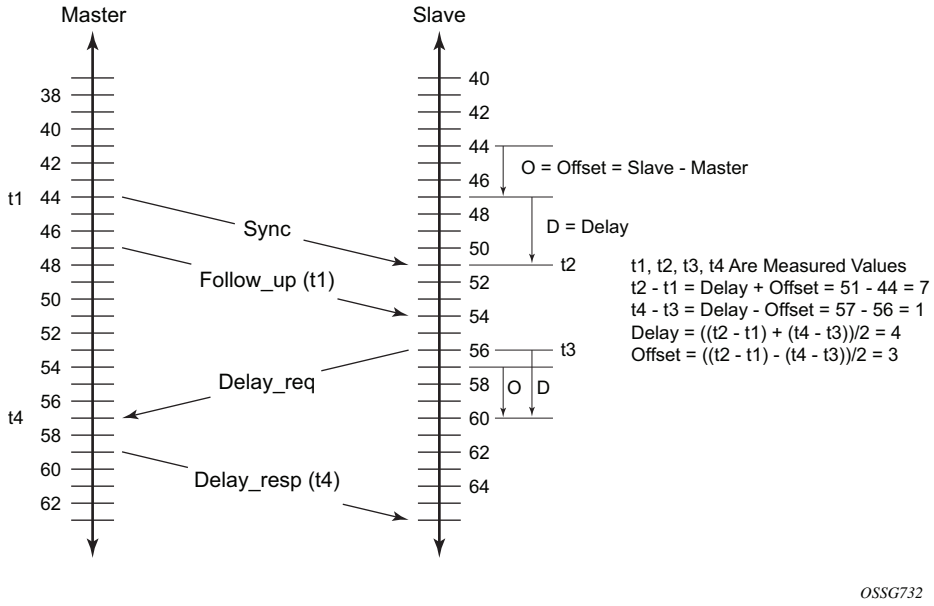
The IEEE 1588v2 standard allows for synchronization of the frequency and time from a master clock to one or more slave clocks over a packet stream. This packet-based synchronization can be over unicast UDP/IPv4 or multicast Ethernet.

As part of the basic synchronization timing computation, a number of event messages are defined for synchronization messaging between the PTP slave port and PTP master port. A one-step or two-step synchronization operation can be used, with the two-step operation requiring a follow-up message after each synchronization message. Ordinary clock master and boundary clock master ports use one-step operation; ordinary clock slave and boundary clock slave ports can accept messages from either one-step or two-step operation master ports.

The IEEE 1588v2 standard includes a mechanism to control the topology for synchronization distribution. The Best Master Clock Algorithm (BMCA) defines the states for the PTP ports on a clock. One port is set into slave state and the other ports are set to master (or passive) states. Ports in slave state recovered synchronization delivered by from an external PTP clock and ports in master state transmit synchronization to toward external PTP clocks.

The basic synchronization timing computation between the PTP slave and PTP master is shown in Figure 16. This figure illustrates the offset of the slave clock referenced to the best master signal during startup.

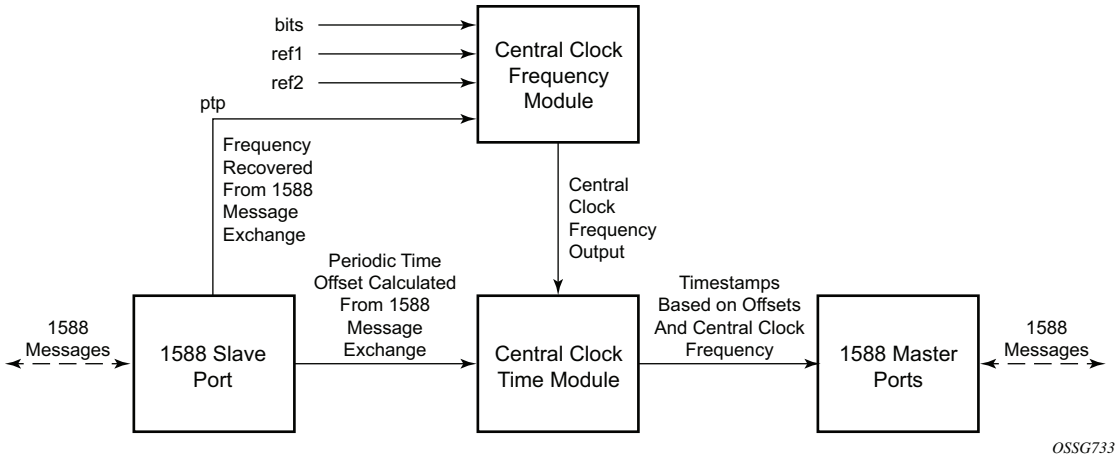
Figure 16 **PTP Slave and Master Time Synchronization Computation**



When using IEEE 1588v2 for distribution of a frequency reference, the slave calculates a message delay from the master to the slave based on the timestamps exchanged. A sequence of these calculated delays contain information of the relative frequencies of the master clock and slave clock but has a noise component related to the packet delay variation (PDV) experienced across the network. The slave must filter the PDV effects so as to extract the relative frequency data and then adjust the slave frequency to align with the master frequency.

When using IEEE 1588v2 for distribution of time, the 7750 SR and 7450 ESS use the four timestamps exchanged using the IEEE 1588v2 messages to determine the offset between the router time base and the external master clock time base. The router determines the offset adjustment and then in between these adjustments, the router maintains the progression of time using the frequency from the central clock of the router. This allows time to be maintained using a BITS input source or a Synchronous Ethernet input source even if the IEEE 1588v2 communications fail. When using IEEE 1588v2 for time distribution, the central clock should at a minimum have a system timing input reference enabled. Figure 17 displays how IEEE 1588v2 is used for time distribution.

Figure 17 **Using IEEE 1588v2 For Time Distribution**



7.4.7.2 Performance Considerations

Although IEEE 1588v2 can be used on a network that is not PTP-aware, the use of PTP-aware network elements (boundary clocks) within the packet switched network improves synchronization performance by reducing the impact of PDV between the grand master clock and the slave clock. In particular, when IEEE 1588v2 is used to distribute high accuracy time, such as for mobile base station phase requirements, then the network architecture requires the deployment of PTP awareness in every device between the Grandmaster and the mobile base station slave.

In addition, performance is also improved by the removal of any PDV caused by internal queuing within the boundary clock or slave clock. This is accomplished with hardware that is capable of detecting and time stamping the IEEE 1588v2 packets at the Ethernet interface. This capability is referred to as port-based time stamping.

7.4.7.2.1 Port-Based Timestamping of PTP Messages

For optimal performance, the 1588 packets should be time-stamped at the ingress and egress. This avoids any possible PDV that might be introduced between the port and the CPM. The ability to timestamp in the interface hardware is provided on a subset of the IMM and MDA assemblies of the routers. Generally, all FP4-based XMA, XMA-s, and MDA-e-XP modules support 1588 port-based timestamping. For other assemblies, contact your Nokia representative to verify the support for 1588 port-based timestamping.

In order for this to operate, the CPM, IOM, IMM, and MDAs must be running firmware that supports this capability. The CPM firmware upgrade occurs automatically when the CPM card software is updated. Since upgrading of IOM, IMM, and MDA firmware is service impacting, this upgrade is not performed automatically on a soft reset of the MDA. The IOM/IMM firmware is upgraded when the IOM/IMM card is hard reset. The MDA firmware is programmed during system initialization, when the MDA is inserted, or when the MDA is hard reset via a **clear mda** or **clear card** command. However, when an MDA is soft reset via either a **clear card soft** command or during a major ISSU, the MDA firmware is not updated.

Port-based timestamping of 1588 packets cannot be used at the same time for Ethernet encapsulation and IP encapsulation on a given port. This means that PTP cannot be configured on an Ethernet port if **ptp-hw-assist** is already configured on a L3 interface associated with that port. Similarly, **ptp-hw-assist** cannot be configured on a L3 interface if its associated port is already configured as a PTP port.

7.4.7.3 PTP Capabilities

For each PTP message type to be exchanged between the router and an external 1588 clock, a unicast session must be established using the unicast negotiation procedures. The router allows the configuration of the message rate to be requested from external 1588 clocks. The router also supports a range of message rates that it grants to requests received from the external 1588 clocks. The IEEE 1588 standard allows the grantor port to respond with a shorter duration than what was in the request. The router can accept such a grant and uses that duration. The router issues a renegotiation before the duration expires.

Table 17 describes the ranges for both the rates that the router can request and grant.

Table 17 **Message Rates Ranges and Defaults**

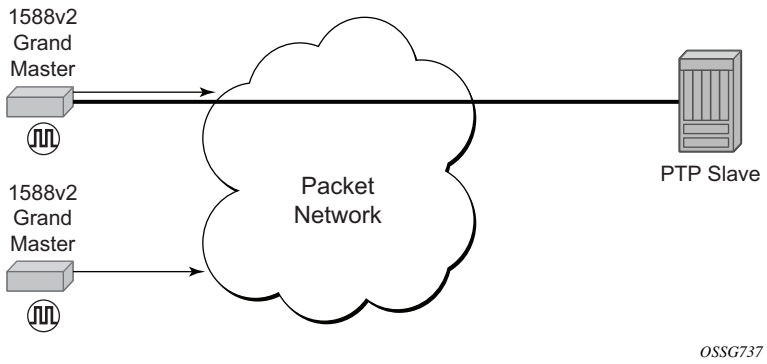
Message Type	Rates Requested by the 7450 ESS, 7750 SR, and 7950 XRS		Rates Granted by the 7450 ESS, 7750 SR, and 7950 XRS	
	Min	**Max**	**Min**	**Max**
Announce	1 packet every 16 seconds	8 packets/second	packet every 16 seconds	8 packets/second
Sync	1 packet/second	64 packet/second	1 packet/second	128 packet/second
Delay_Resp	1 packet/second	64 packets/second	1 packet/second	128 packets/ second
(Duration)	300	300	1	1000

State and statistics data for each PTP peer are available to assist in the detection of failures or unusual situations.

7.4.7.4 PTP Ordinary Slave Clock For Frequency

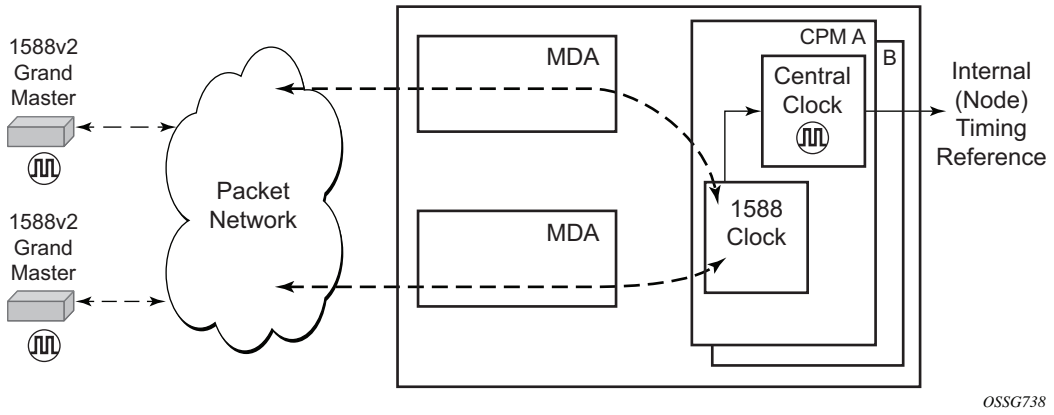
Traditionally, only clock frequency is required to ensure smooth transmission in a synchronous network. The PTP ordinary clock with slave capability on the router provides another option to reference a Stratum-1 traceable clock across a packet switched network. The recovered clock can be referenced by the internal SSU and distributed to all slots and ports. Figure 18 shows a PTP ordinary slave clock network configuration.

Figure 18 **Slave Clock**



The PTP slave capability is implemented on the CPM, version 3 or later. The IEEE 1588v2 messages can ingress and egress the router on any line interface. Figure 19 shows the operation of an ordinary PTP clock in slave mode.

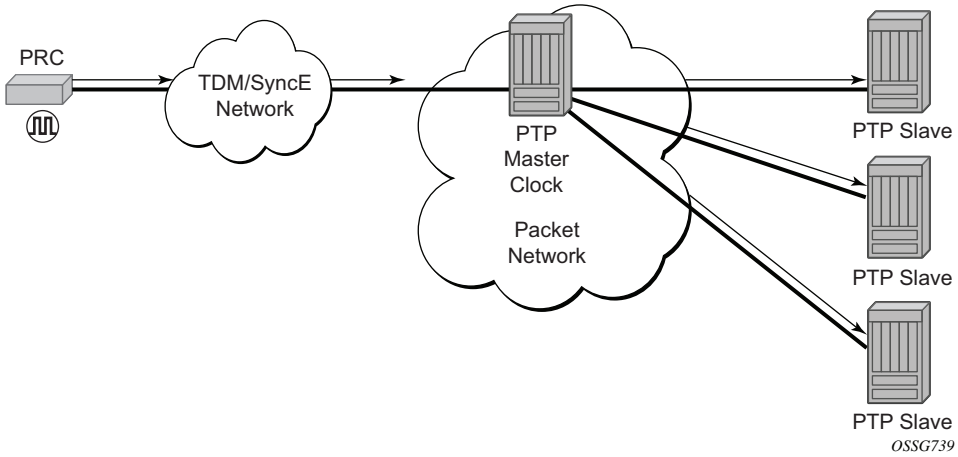
Figure 19 **Ordinary Slave Clock Operation**



7.4.7.5 PTP Ordinary Master Clock For Frequency

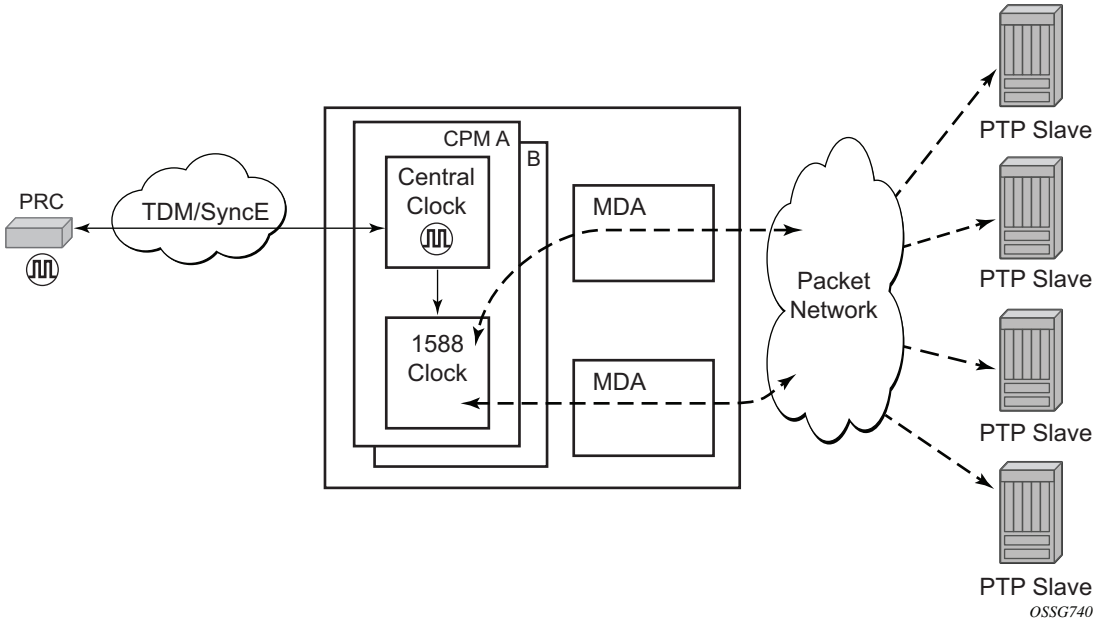
The router supports the PTP ordinary clock in master mode. Normally, a IEEE 1588v2 grand master is used to support many slaves and boundary clocks in the network. In cases where only a small number of slaves and boundary clocks exist and only frequency is required, a PTP integrated master clock can greatly reduce hardware and management costs to implement PTP across the network. It also provides an opportunity to achieve better performance by placing a master clock closer to the edge of the network, as close to the slave clocks as possible. Figure 20 shows a PTP master clock network configuration.

Figure 20 **PTP Master Clock**



All packets are routed to their destination via the best route as determined in the route table; see Figure 21. It does not matter which ports are used to ingress and egress these packets (unless port based time stamping is enabled for higher performance).

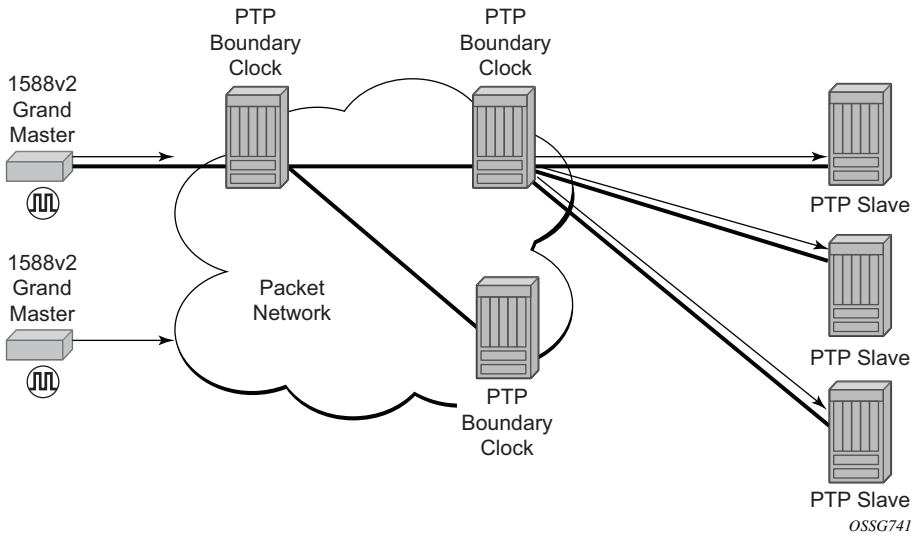
Figure 21 **Ordinary Master Clock Operation**



7.4.7.6 PTP Boundary Clock for Frequency and Time

The router supports boundary clock PTP devices in both master and slave states. IEEE 1588v2 can function across a packet network that is not PTP-aware; however, the performance may be unsatisfactory and unpredictable. PDV across the packet network varies with the number of hops, link speeds, utilization rates, and the inherent behavior of the routers. By using routers with boundary clock functionality in the path between the grand master clock and the slave clock, one long path over many hops is split into multiple shorter segments, allowing better PDV control and improved slave performance. This allows PTP to function as a valid timing option in more network deployments and allows for better scalability and increased robustness in certain topologies, such as rings. Boundary clocks can simultaneously function as a PTP slave of an upstream grand master (ordinary clock) or boundary clock, and as a PTP master of downstream slaves (ordinary clock) and/or boundary clocks, as shown in Figure 22.

Figure 22 **Boundary Clock**



In addition, the use of port based timestamping in every network element between the grandmaster and the end slave application is highly recommended for delivering time to meet one microsecond accuracies required of mobile applications.

The router always uses the frequency output of the central clock to maintain the timebase within the router. The PTP reference into the central clock should always be enabled as an option if the router is configured as a boundary clock. This avoids the situation of the router entering holdover while propagating time with 1588.

Note: The ITU-T defined a network architecture for node-by-node time distribution in their Recommendations. These recommendations require that Synchronous Ethernet be used with IEEE 1588 (using the G.8275.1 profile) to meet the target performance.

7.4.7.7 PTP Clock Redundancy

The PTP module in the router exists on the CPM. The PTP module on the standby CPM is kept synchronized to the PTP module on the active CPM. All sessions with external PTP peers are maintained over a CPM switchover.

7.4.7.8 PTP Time for System Time and OAM Time

PTP has the potential to provide much more accurate time into the router than can be obtained with NTP. This PTP recovered time can be made available for system time and OAM packet time stamping to improve the accuracies of logged events and OAM delay measurements. The mechanism to activate PTP as the source for these internal time bases is to allocate PTP as a local server into NTP. This permits the NTP time recovery to use PTP as a source for time and then distribute it within the router to system time and the OAM process. This activation also affects the operation of the NTP server within the SR OS. The PTP server appears as NTP stratum 0 server and therefore the SR OS advertises itself as an NTP Stratum 1 server to external peers and clients. This activation may impact the NTP topology.

7.4.7.9 PTP within Routing Instances

PTP is supported over direct Ethernet encapsulation (that is, PTP ports) and UDP/IP encapsulation (that is, PTP peers). PTP ports operate below the routing plane. They can be used on appropriate ports irrespective of any type of router interface also on the port. PTP peers operate at the routing plane and have restrictions based on and across the following router instances.

Transmission and reception of PTP messages using PTP peers is supported in the following contexts:

- Network interface in the Base routing instance (**config**>**router**>**interface**)
- IES interface (**config**>**service**>**ies**>**interface**)
- VPRN interface (**config**>**service**>**vprn**>**interface**)

Transmission and reception of PTP messages using PTP peers is not supported in the following contexts:

- IES spoke SDP interface (**config**>**service**>**ies**>**spoke-sdp**>**interface**)
- VPRN spoke SDP interface (**config**>**service**>**vprn**>**spoke-sdp**>**interface**)
- VPRN transport tunnel (**config**>**service**>**vprn**>**auto-bind-tunnel** or **config**>**service**>**vprn**>**spoke-sdp**)
- Any interface of the management router instance
- Any interface of the vpls-management router instance
- Any interface of a user created CPM router instance

It is important to note that there is only one PTP clock within the router. All PTP ports and PTP peers communicate into one clock instance. Only one router instance may have PTP peers configured, which means that only that router instance (or PTP port) can run the slave functionality and recover time from an external PTP clock. All other router instances only support the dynamic PTP peers. The PTP process in the router only includes outward server time towards the dynamic PTP peers. The dynamic PTP peers are shared across all router instances. If it is desired to control the number of dynamic peers that can be consumed by a given routing instance, then it must be configured for that routing instance.

7.4.7.10 PTSF-unusable for G.8275.1

The PTP clock in the router monitors the Sync, Follow_Up (if present), and Delay_Resp messages received from external neighbor ports. If a high variation is detected in the network path between the external neighbor port and the local port, that neighbor port is considered unusable (PTSF-unusable as defined in the ITU-T G.8275.1 recommendation). When a neighbor is unusable, all Announce messages from that neighbor are discarded on reception and excluded from the BMCA. If the neighbor is the parent clock to the local clock, the local clock must either select a new parent clock or go into holdover. In addition, any neighbor clock marked as unusable cannot act as the parent to the local PTP clock until underlying condition is investigated and resolved, and the unusable state is cleared. The unusable state is cleared when PTP, PTSF-unusable monitoring, or the local PTP port is administratively disabled, the PTP port is deleted, or the external neighbor port stops sending messages to the node. It can also be cleared by using the appropriate **clear** command.

7.5 System-Wide ATM Parameters

On the 7750 SR, the ATM ping OAM loopback feature can be enabled on an ATM SAP for a period of time configured through the interval and the send-count parameters. When the ATM SAP terminates on IES or VPRN services, a failure of the loopback state machine does not bring down the Layer 3 interface. Only receiving AIS/RDI OAM cells or entering the AIS/RDI state brings down the Layer 3 interface.

The ATM ping OAM loopback feature can also be enabled on a continuous basis on an ATM SAP terminating on IES or VPRN services. When the loopback state machine fails, the Layer 3 interface is brought down.

The ATM OAM loopback parameters must first be enabled and configured in the **config>system>atm>oam** context, and then enabled in the IES or VPRN service interface SAP **atm oam** context.

Refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN* for further information. For command descriptions, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

7.6 QinQ Network Interface Support

The creation of network interfaces on a QinQ-encapsulated VLAN can be enabled on a system-wide level using the **config>system>ip>allow-qinq-network-interface** command.

When enabled, the egress IOM limits are changed to allow a maximum of 11 MPLS labels instead of 12.

Table 18 lists the allowed and restricted QinQ combinations.

Table 18 **QinQ Combination (✓) and Restriction (x) Table**

	SAP x.0	**SAP x.***	**SAP x.y**	**Nw interface x.0**	**Nw interface x.***	**Nw interface x.y**	**SAP *.***	**SAP *.NULL**	**SAP 0.***	**Inverse SAP**
SAP x.0	x	✓	✓	x	x	x	✓	✓	✓	x
SAP x.*	✓	x	✓	x	x	x	✓	✓	✓	x
SAP x.z	✓	✓	✓	x	x	✓	✓	✓	✓	✓

Table 18 **QinQ Combination (✓) and Restriction (x) Table (Continued)**

	SAP x.0	**SAP x.***	**SAP x.y**	**Nw interface x.0**	**Nw interface x.***	**Nw interface x.y**	**SAP *.***	**SAP *.NULL**	**SAP 0.***	**Inverse SAP**
Nw interface x.0	x	x	x	x	x	✓	✓	✓	✓	x
Nw interface x.*	x	x	x	x	x	x	✓	✓	✓	x
Nw interface x.z	x	x	✓	✓	x	✓	✓	✓	✓	x
SAP *.*	✓	✓	✓	✓	✓	✓	x	✓	✓	✓
SAP *.NULL	✓	✓	✓	✓	✓	✓	✓	x	✓	x
SAP 0.*	✓	✓	✓	✓	✓	✓	✓	✓	x	x
Inverse SAP	x	x	✓	x	x	x	✓	x	x	x

7.7 Link Layer Discovery Protocol (LLDP)

The IEEE 802.1ab Link Layer Discovery Protocol (LLDP) is a unidirectional protocol that uses the MAC layer to transmit specific information related to the capabilities and status of the local device. Separately from the transmit direction, the LLDP agent can also receive the same kind of information for a remote device which is stored in the related MIBs.

LLDP itself does not contain a mechanism for soliciting specific information from other LLDP agents, nor does it provide a specific means of confirming the receipt of information. LLDP allows the transmitter and the receiver to be separately enabled, making it possible to configure an implementation so the local LLDP agent can either transmit only or receive only, or can transmit and receive LLDP information.

The information fields in each LLDP frame are contained in a LLDP Data Unit (LLDPDU) as a sequence of variable length information elements, that each include type, length, and value fields (known as TLVs), where:

- Type identifies what kind of information is being sent.

- Length indicates the length of the information string in octets.
- Value is the actual information that needs to be sent (for example, a binary bit map or an alphanumeric string that can contain one or more fields).

Each LLDPDU contains four mandatory TLVs and can contain optional TLVs as selected by network management:

- Chassis ID TLV
- Port ID TLV
- Time To Live TLV
- Zero or more optional TLVs, as allowed by the maximum size of the LLDPDU
- End Of LLDPDU TLV

The chassis ID and the port ID values are concatenated to form a logical identifier that is used by the recipient to identify the sending LLDP agent/port. Both the chassis ID and port ID values can be defined in a number of convenient forms. Once selected however, the chassis ID/port ID value combination remains the same as long as the particular port remains operable.

A non-zero value in the TTL field of the time-to-live TLV tells the receiving LLDP agent how long all information pertaining to this LLDPDU's identifier is valid so that all the associated information can later be automatically discarded by the receiving LLDP agent if the sender fails to update it in a timely manner. A zero value indicates that any information pertaining to this LLDPDU's identifier is to be discarded immediately.

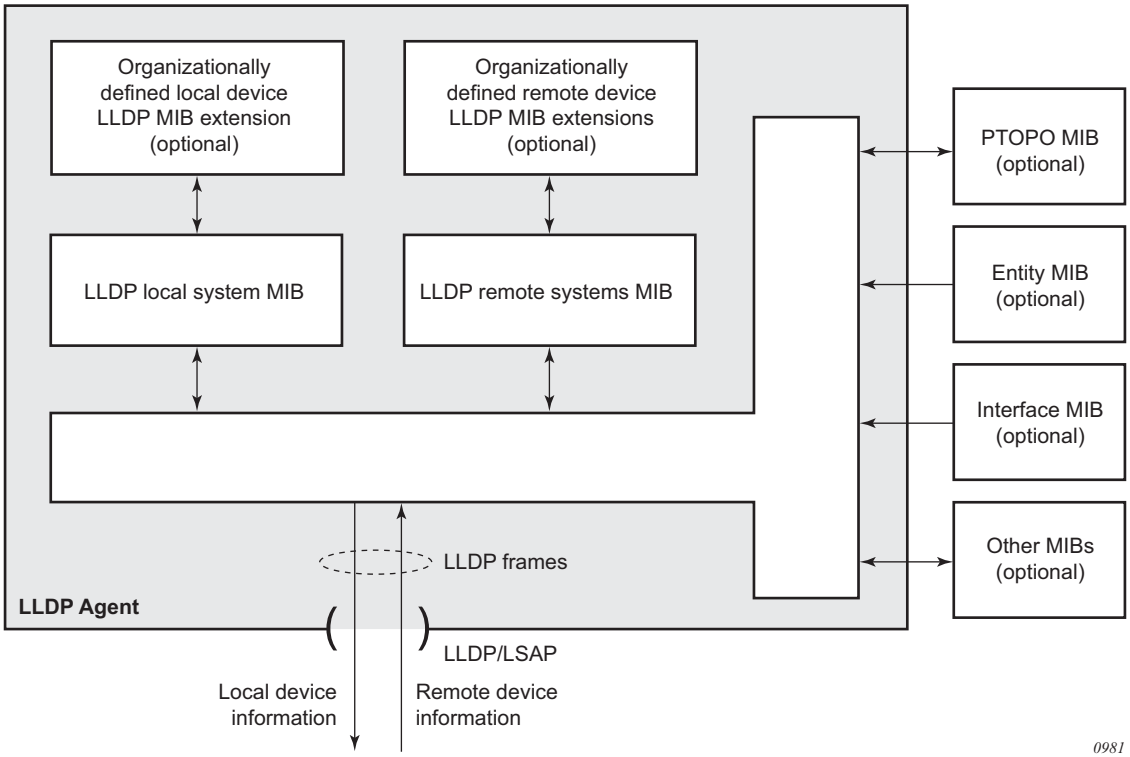
A TTL value of zero can be used, for example, to signal that the sending port has initiated a port shutdown procedure.

The end of a LLDPDU TLV marks the end of the LLDPDU.

The IEEE 802.1ab standard defines a protocol that:

- Advertises connectivity and management information about the local station to adjacent stations on the same IEEE 802 LAN.
- Receives network management information from adjacent stations on the same IEEE 802 LAN.
- Operates with all IEEE 802 access protocols and network media.
- Establishes a network management information schema and object definitions that are suitable for storing connection information about adjacent stations.
- Provides compatibility with a number of MIBs as depicted in Figure 23.

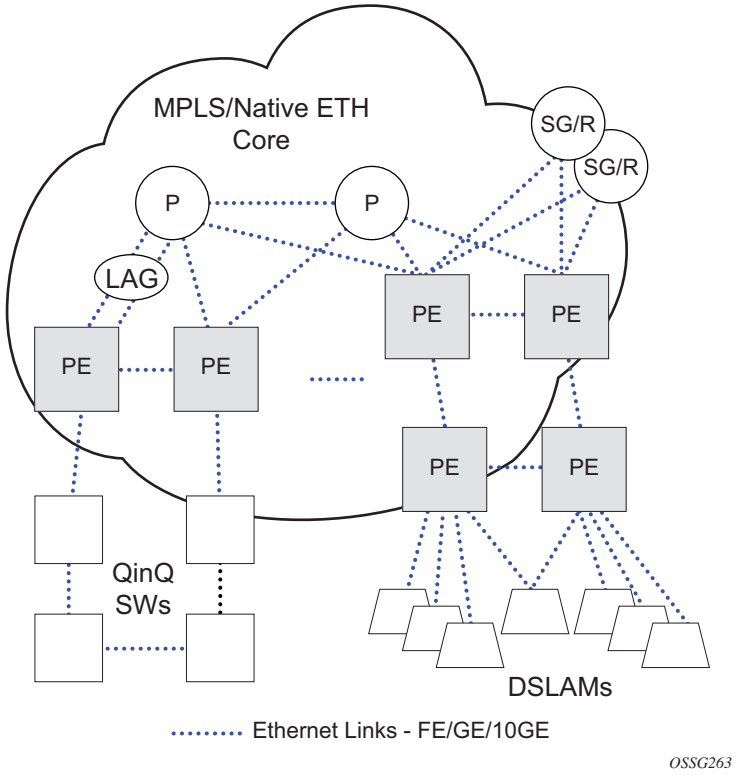
Figure 23 **LLDP Internal Architecture for a Network Node**



Network operators must be able to discover the topology information in order to detect and address network problems and inconsistencies in the configuration. Moreover, standard-based tools can address the complex network scenarios where multiple devices from different vendors are interconnected using Ethernet interfaces.

The example displayed in Figure 24 depicts a MPLS network that uses Ethernet interfaces in the core or as an access/hand off interfaces to connect to different kind of Ethernet enabled devices such as service gateway/routers, QinQ switches, DSLAMs or customer equipment.

Figure 24 **Customer Use Example For LLDP**



IEEE 802.1ab LLDP running on each Ethernet interfaces in between all the above network elements may be used to discover the topology information.

7.8 IP Hashing as an LSR

It is now possible to include IP header in the hash routine at an LSR for the purpose of spraying labeled-IPv4 and labeled-IPv6 packets over multiple equal cost paths in ECMP in an LDP LSP and/or over multiple links of a LAG group in all types of LSPs.

A couple of configurable options are supported. The first option is referred to as the Label-IP Hash option and is designated in the CLI as **lbl-ip**. When enabled, the hash algorithm parses down the label stack and once it hits the bottom of the stack, it checks the next nibble. If the nibble value is four or six then it assumes it is an IPv4 or IPv6 packet. The result of the hash of the label stack, along with the incoming port and system IP address, is fed into another hash along with source and destination address fields in the IP packet's header. The second option is referred to as IP-only

hash and is enabled in CLI by entering the **iponly** keyword. It operates the same way as the Label-IP Hash method except the hash is performed exclusively on the source and destination address fields in the IP packet header. This method supports both IPv4 and IPv6 payload and operates on packets received on an IP interface on an IOM3-XP/IMM port only.

By default, MPLS packet hashing at an LSR is based on the whole label stack, along with the incoming port and system IP address. This method is referred to as Label-Only Hash option and is enabled in CLI by entering the **lbl-only** keyword.

The **lbl-only**, **lbl-ip** and **ip-only** hashing options can be configured system-wide and can also be overridden on a per-IP-interface basis.

7.9 Satellites

There are two types of SAS-Sx satellites supported on the 7750 SR:

- Ethernet satellites
- TDM satellites

The following primary tasks must be performed to configure a satellite.

1. Create a software repository that specifies where the SAS-Sx should obtain its correct software image.
2. Create an Ethernet or TDM satellite association that binds a chassis to a set of uplinks and a software repository.
3. Configure the satellite ports to specify port configuration and service association.

7.9.1 Ethernet Satellites

The Ethernet satellite support feature allows a 7210 SAS-Sx or SAS-S chassis to act as a port extension for the 7750 SR host. In this configuration, all configuration and management functions are performed through the host node. Management of the SAS-Sx/SAS-S node is not required when it is configured in an Ethernet satellite operations mode. A direct, non-switched, Ethernet connection between the 7750/7950 host and the 7210 satellite must be provided. The use of active Layer 2 switching devices in the path between the host and satellite is not supported.

Table 19 lists the supported Ethernet satellite chassis.

Table 19 **Supported Ethernet Satellite Chassis**

Chassis Type	Sat-Type String
7210 SAS-Sx 24-port fiber	es24-1gb-sfp
7210 SAS-Sx 48-port fiber	es48-1gb-sfp
7210 SAS-S 24F4SFP+	es24-sass-1gb-sfp
7210 SAS-S 48F4SFP+	es48-sass-1gb-sfp
7210 SAS-Sx 24-port copper 7210 SAS-S 24-port copper	es24-1gb-tx
7210 SAS-Sx 48-port copper 7210 SAS-S 48-port copper	es48-1gb-tx
7210 SAS-Sx 24-port copper + PoE 7210 SAS-S 24-port copper + PoE	es24-1gb-tx
7210 SAS-Sx 48-port copper + PoE 7210 SAS-S 48-port copper + PoE	es48-1gb-tx
7210 SAS-Sx 64-port 10GE (CFP)	es64-10gb-sfpp+4-100gb-cfp4
7210 SAS-Sx 64-port 10GE + 4-port QSFP28	es64-10gb-sfpp+4-100gb-qsfp28
7210 SAS-Mxp	es24-sasmxp-1gb-sfp

Note:

- The 7210 SAS-Sx 64-port 10GE Ethernet satellite supports both 10GE and 1GE optics. See the *7210 Optics Guide* for a list of supported modules.
- The 64x10GE + 4xQSFP28 SAS-Sx satellite does not support the local-forwarding feature.
- The 7210 SAS-Mxp does not support the local forwarding feature.
- PoE functionality is not supported when the 7210 PoE capable switches are used in satellite mode.
- For traffic sent by the 7750 SR or 7950 XRS host to the 7210 SAS satellite, the satellite Q-tag P-bits and DEI bits are set based on the forwarding class and profile associated with the traffic through the 7750 SR or 7950 XRS system.

7.9.2 TDM Satellites

The SONET/SDH ETR chassis is the only available TDM satellite and can be configured for different modes. Table 20 lists the supported modes of the satellite chassis.

Table 20 **Supported SONET/SDH Satellite Chassis**

Chassis Type	Sat-Type String
4 port OC3	ts4-choc3-sfp
4 port STM1	ts4-chstm1-sfp
1 port OC12	ts1-choc12-sfp
1 port STM4	ts1-chstm4-sfp

The default type on a supplied TDM satellite is ts4-choc3-sfp. Updating to another type initiates a reboot of the satellite.

The TDM satellite provides CEM functionalities supported on the 7750 SR OC3/OC12 CES MDAs. The satellite is built using the same architecture as the 7705 SAR-8 adapter cards and is designed to transport existing TDM services including:

- Cpipe service of DS1/E1 channels within SONET/SDH in structure-agnostic mode (SATOP) as described in RFC4553
- MEF8 service of DS1/E1 channels within SONET/SDH in structure-agnostic mode

The following types of synchronization are supported:

- DS1/E1 channels can be independently loop-timed, node-timed, or differentially-timed
- OC3/STM1/OC12/STM4 ports can be node-timed

To provide a stable frequency from the host to the SONET/SDH satellite, ensure that the host's clock is referenced to a suitable timing source (for example, BITS) and configure Synchronous Ethernet from the host's Ethernet port connecting to the satellite. Copper Ethernet SFPs are not supported because they do not support Synchronous Ethernet.

The TDM satellite is entirely managed through a 7750 SR host system, such as 7750 SR, 7750 SR-a, or 7750 SR-e. As a satellite, no new IP address needs to be assigned. Services on the satellite are configured on the host in the same manner as any ports in a native MDA. The TDM satellite connects to the SR host using a Gigabit Ethernet link, thereby not occupying valuable slots space in the host system. APS is supported across satellites connecting to a single host.

7.9.3 Software Repositories for Satellites

The software repositories define the locations from where the host can obtain software for subcomponents including Ethernet satellites. The software repository is also used to upgrade an existing subcomponent by changing the location of the image to be served to the remote device. The software repositories are not used for management of the host router software, which is managed using the standard procedures described in the *SR OS 21.x*.R*x* Software Release Notes.

Each software repository supports up to three locations to search for the software. A location may be a URL or a directory on a compact flash. When an upgrade operation is initiated, each of the three locations is checked in sequence to locate the required software. The upgrade operation fails if the software is not located in any of the configured locations. The satellite booting operation also fails if the software cannot be located.

At least one software repository must be configured to support a satellite connected to the local host by using the **config>system>software-repository** CLI tree, as follows.

1. Create a software repository using a unique repository name.
2. Specify the primary location for the SAS-Sx image.
3. Optionally, specify a secondary or tertiary image location and a description.

Caution: Software for TDM satellites and Ethernet satellites should be stored in separate software repositories. There is one file that has the same name for both types of software, that is overwritten if they are placed in the same repository.

7.9.4 Satellite Software Upgrade Overview

The process to change or upgrade the satellite software consists of the following steps.

1. Copy the new satellite software images to a local compact flash card. It is recommended that the new image files be placed in a different directory.

   Although you can store the satellite software on a remote server and use a URL to reference the remote location, it is recommended that the primary image location is locally accessible.
2. Create a new software repository using a new name and at least a primary-location for the 7210 SAS-Sx image.
3. Modify the satellite configuration such that the **software-repository** parameter references the newly created software repository.

   Use the following CLI context:

   config>system>satellite>eth-sat *sat-id*

   or

   config>system>satellite>tdm-sat *sat-id*
4. Reboot the satellite to load the new software.

   Depending on whether a firmware update is needed, perform one of the following steps to reboot the satellite.

   a. A satellite firmware update is not required.

      i. The satellite loads the new software the next time it reboots.

      ii. You can reset the satellite with the following administrative command, if required.

      admin satellite eth-sat *sat-id* **reboot [now]**

      or

      admin satellite tdm-sat *sat-id* **reboot [now]**

   b. A satellite firmware update is required.

      i. To continue the upgrade to the 7210 firmware image, enter one of the following commands and allow it to execute completely:

      admin satellite eth-sat *sat-id* **sync-boot-env**

      or

      admin satellite tdm-sat *sat-id* **sync-boot-env**

      ii. Reboot the satellite again using the **upgrade** keyword to update the firmware image.

      The **upgrade** keyword causes the 7210 SAS-Sx to upgrade the included firmware images. This process takes longer than a normal reboot.

      admin satellite eth-sat *sat-id* **reboot upgrade now**

      or

      admin satellite tdm-sat *sat-id* **reboot upgrade now**

7.9.5 Satellite Configuration

After creating the software repositories, configure the satellite. The satellite configuration is required to create a satellite binding to a satellite ID, and to provide additional information that uniquely identifies the satellite chassis, chassis type, and the software repository to be used to boot the remote satellite.

The following parameters can be specified for a satellite.

- **mac-address** — The satellite chassis MAC address must be specified. This is used to bind a specific chassis to the associated satellite ID. (The local host router boots only satellites with configured MAC addresses.) This parameter is mandatory.
- **sat-type** — The satellite chassis type must be specified and must match the chassis type that the satellite advertises during the boot process. This parameter is mandatory.
- **software-repository**— A preconfigured software repository must be specified in the satellite configuration. This defines the location of the software image to boot the associated 7210 SAS-Sx. This parameter is mandatory.
- **no shutdown** — By default, a new satellite is in a shutdown state; use the **no shutdown** command to bring the satellite online. This parameter is mandatory.
- **description** — Use this command to configure a description string associated with the satellite. This parameter is optional.
- **sync-e** — Use this command to enable the **sync-e** option. This parameter is only available for an Ethernet satellite. This parameter is optional.

7.9.5.1 Satellite Client Port ID Formats

Use the following format to reference Ethernet satellite client ports:

port esat- *sat-id*/*slotNum*/*portNum*

where:

- *sat-id* is between 1 and 20
- *slotNum* is always 1
- *portNum* is between 1 and 64

Use the following format to reference Ethernet satellite uplink port:

port esat- *sat-id*/1/*uplink-id*

where:

- *sat-id* is between 1 and 20
- *uplink-id* is between **u**1 and **u**4

Use the following format to reference TDM satellite client ports:

port tsat- *sat-id*/*slotNum*/*portNum.channel*

where:

- *sat-id* is between 1 and 20
- *slotNum* is always 1
- *portNum* is between 1 and 4

Use the following format to reference TDM satellite uplink port:

port tsat- *sat-id*/1/**u**1

where:

- *sat-id* is between 1 and 20

Ethernet satellite client ports support all port modes (access, network, and client).

Configuring services associated with satellite client ports is the same as configuring services on local 7750 SR ports, except that satellite client ports are referenced with the syntax for the Ethernet satellite port described above. It is required that a **port-scheduler-policy** is created to ensure that the 7750 SR is able to shape the traffic for the egress satellite port type and speed.

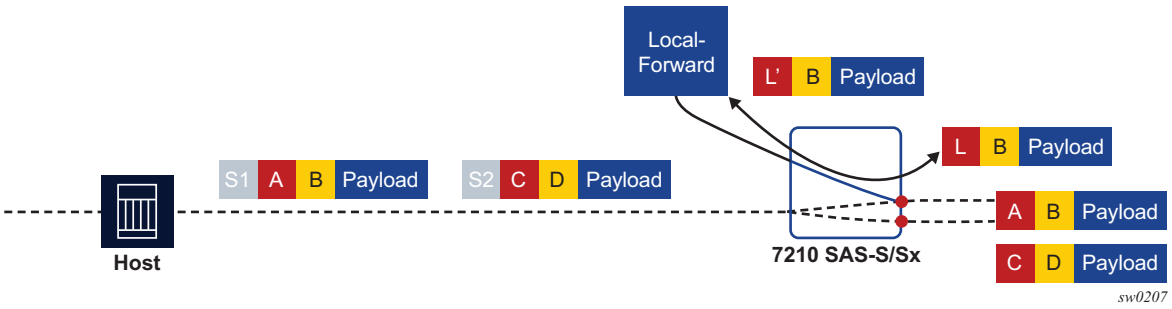
7.9.5.2 Local Forwarding

The local forwarding capability allows traffic to be forwarded between two client satellite ports without going through the SR host, which allows for optimal forwarding by preserving uplink bandwidth.

- Locally forwarded traffic is identified based on the ingress VLAN tag.
- The outer VLAN tag used to identify the traffic to be locally forwarded can be different at the two bypass endpoints. In that case, as traffic is forwarded from the ingress to the egress, the outer VLAN tag is modified.
- The bypass paths are bidirectional, so only a single local-forwarding path needs to be defined to allow for traffic flow in both directions.

Figure 25 shows an example of local forwarding.

Figure 25 **Local Forwarding**



A local-forward bypass is created by using the following commands to create a local-forward bypass, then associating a set of two satellite access points as endpoints for the local-forward bypass.

- The two endpoints must be ports on the same Ethernet satellite chassis.
- If a LAG is used as an endpoint, all member links must be ports on the same Ethernet satellite.
- All satellite ports must be client ports by default, or must be configured as a client port using the port-template command.

```
config system satellite
     local-forward <id> [create]
          description <string>
          sap <sat-port>:qtag | <lag-id>:qtag
          exit
          sap <sat-port>:qtag | <lag-id>:qtag
          exit
          [no] shutdown
     exit
```

Example Configuration:

To configure a local-forward bypass between client ports esat-2/1/1:66 and esat-2/1/50:101, use the following commands:

```
config system satellite
     local-forward 10 create
          description "local-forward to offload router"
          sap esat-2/1/1:66
          exit
          sap esat-2/1/50:101
          exit
          no shutdown
     exit
```

7.9.5.3 Port Template

The **port-template** command hierarchy allows the creation of a satellite template that reconfigures the port role and uplink association for one or more satellite ports. This template can then be applied to one or more Ethernet satellite instances, in which case those satellites inherit the specified port role and uplink associations.

The port template is necessary when reconfiguring a satellite uplink as a client port for use as part of a local-forward bypass path.

```
configure
    system
        satellite
            [no] port-template <template-name> sat-type <sat-type> [create]
                port <port-id>
                   role {none | uplink | client | system-default}
                   uplink {<port-id> | system-default | none}
                exit
                [no] description <string>
                [no] shutdown
```

7.9.5.4 10GE Client Ports

Ports 51 and 52 on the 48xGE + 4x10GE satellite chassis can be reassigned as client ports instead of uplink ports. This provides the flexibility to offer 10GE services from these satellite chassis. These two 10GE ports can be reconfigured as client ports using the **port-template** configuration commands described above. The port template configuration must be done before SAPs, interfaces, or services can be applied to the associated satellite ports.

7.9.5.5 100GE Client Ports

Ports 67 and 68 on the 64x10GE + 4x100GE satellites (sat-type es64-10gb-sfpp+4-100gb-cfp4) and connectors 3 and 4 on the 64x10GE+4xQSFP28 (sat-type es64-10gb-sfpp+4-100gb-qsfp28) can be reassigned as client ports instead of uplinks. This provides the flexibility to offer 100GE services from these satellite chassis. These two 100GE ports can be reconfigured as client ports using the **port-template** configuration commands. The port template must be configured before port topology bindings are configured as well as before SAPs, interfaces, or services can be applied to the associated satellite ports.

7.9.5.6 10GE Uplinks on the 64x10GE+4x100GE Satellite

On the 7210 SAS-Sx 64x10GE+4x100GE (es64-10gb-sfpp+4-100gb-cfp4) and 64x10GE+4xQSFP28 (sat-type es64-10gb-sfpp+4-100gb-qsfp28) satellite, selected 10GE ports can be reconfigured and used as satellite uplinks to the host router running SR OS.

Up to 16 10GE interfaces can be used as uplinks for the associated satellite. A new satellite template that configures the desired 10GE interfaces as uplinks must be created. In addition, use a port template to specify the uplink association between the remaining client ports and configured uplinks.

Apply the new template to the satellite using the **config>system>satellite>eth-sat** *sat-id***>sat-type** *sat-type***>port-template** *template-name* command, where the *template-name* is the name configured in the **port-template** context.

This feature requires the 7210 SAS-Sx to be running Release 9.0.R10 or later for the SAS-Sx 64x10GE+4x100GE and 7210 SAS Release 10.0 or later for the 64x10GE+4xqSFP28 satellite.

The following restrictions apply:

- The 10GE ports used as satellite uplinks must start at port 1 and be sequential, up to the maximum of 16 10GE uplinks.
- When 10GE ports are used as uplinks, the 4x100GE port are not available for use and should be configured as **role none**.

The following is an example configuration:

```
config>system
     satellite
          port-template "10gUp" sat-type "es64-10gb-sfpp+4-100gb-cfp4" create
               port 1/1/1
                    role uplink
                    uplink none
               exit
               port 1/1/2
                    role uplink
                    uplink none
               exit
               port 1/1/3
                    role uplink
                    uplink none
               exit
               port 1/1/4
                    role uplink
                    uplink none
               exit
               ...
               port 1/1/9
                    uplink 1/1/1
```

```
                exit
                port 1/1/10
                ...
                port 1/1/16
                     uplink 1/1/2
                exit
                ...
                port 1/1/65
                     role none
                exit
                port 1/1/66
                     role none
                exit
                ...
                no shutdown
           exit
           eth-sat 20 create
                mac-address d0:99:d5:96:ee:41
                sat-type "es64-10gb-sfpp+4-100gb-cfp4" port-template "10gUp"
                software-repository "rep1"
                no shutdown
           exit
      exit
exit
```

7.9.5.7 Satellite Uplink Resiliency

An option in the **port-map** configuration allows a secondary uplink to be assigned to enable uplink resiliency. A secondary uplink is used to carry the traffic associated with the client port if the primary uplink becomes unavailable. If traffic is switched to the secondary uplink, once the primary uplink becomes available, traffic is reverted to the primary as soon as possible.

The configuration of a secondary uplink is performed on a per-client port basis using the **port-map** command.

config>system>sat>eth-sat>port-map *client-port-id* **primary** *primary-uplink-port-id* [**secondary** *secondary-uplink-port-id*]

config>system>sat>eth-sat>port-map *client-port-id* **system-default**

To configure a secondary uplink, after the primary uplink is specified, the **secondary** keyword should be included, followed by the intended uplink to be used as the secondary uplink.

For example,

```
config>system>satellite>eth-sat 1
     port-map esat-1/1/2 primary esat-1/1/u1 secondary esat-1/1/u3
```

- If there are no SAPs or interfaces bound to a client port, then any change can be made to the uplinks.
- If a SAP or interface is bound to a client port, or the client port is member of a LAG or ETH tunnel, then only one uplink change per configuration command is allowed (see below).
- The primary cannot be changed directly, this requires multiple steps.
  1. swap primary and secondary
  2. remove secondary
  3. add new secondary
  4. perform a second swap of primary and secondary

The following are basic actions allowed with a single command:

- add or delete secondary uplink
- swap primary and secondary
- add a secondary uplink and swap secondary with primary

Uplink mapping can be changed, but a client uplink must be maintained throughout the process. For example, client-10 is mapped to uplink-1 (U-1), but must move to uplink-2 (U-2). To do this, add U-2 as the secondary uplink, then swap the primary and secondary, making U-2 the primary uplink for client-10 and switching traffic to U-2. After the switch is complete, remove U-1. U-1 cannot be directly replaced with U-2, as the client port would have no uplink during the switch.

7.10 Auto-Provisioning

Auto-provisioning is used to provision a node using an external DHCP server and file server. It is used to obtain a configuration file and an image file from an external server using an in-band mechanism. Auto-provisioning is not compatible with an out-of-band management port.

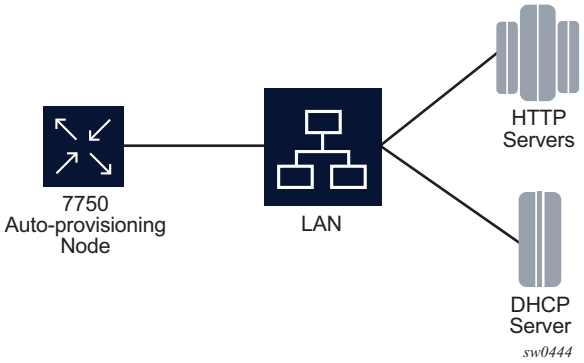
Before using auto-provisioning, the SR OS must be booted up and running the application image. In addition, it needs to have some minimum configuration before the auto-provision script is executed by the operator.

After the auto-provision application is triggered using a tools command, SR OS checks all operationally up ports without IP addresses and send DHCP discovery to these interfaces. The DHCP server needs to be configured with Option 67 and the user must provide the SR OS with the URL of a file server and the corresponding directory for the image.

Figure 26 to Figure 28 describe scenarios in which auto-provisioning are used.

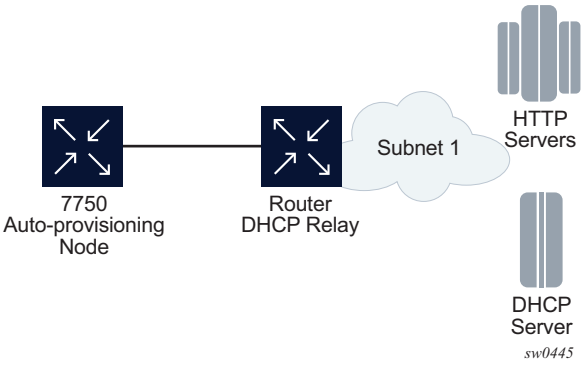
In Figure 26, there is no DHCP relay and all IP addresses are assigned from a single pool.

Figure 26 **Example of a Network with no DHCP Relay**



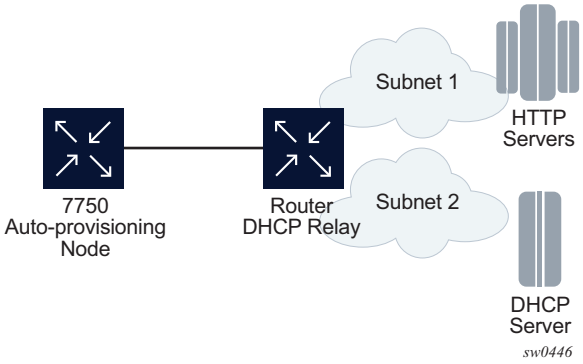
In Figure 27, there is a DHCP relay which injects the Option 82 as a gateway address. The DHCP server is assigned the IP address from the pool dictated by the gateway address option 82. The DHCP server and HTTP server are in the same subnet. The DHCP offer has option 3 "router" which is used for a default gateway creation on the 7750 SR.

Figure 27 **Example of a Network with a DHCP Relay**



In Figure 28, all components are in different subnets. The DHCP relay adds Option 82 to the DHCP request as the gateway address which is used for pool selection. The DHCP server must add option 3 configured with the gateway address of the HTTP server.

Figure 28 **Example of a Network with Multiple Subnets**



7.10.1 Auto-provisioning limits

The following are some configuration limits for auto-provisioning:

- A maximum of 12 Layer 3 interfaces are supported for auto-provisioning
- Only IPv4 auto-provisioning is supported
- It is highly recommended to only have a basic card, MDA, port, and interface configuration as described in this document and no additional static routes or IGP or BGP protocols when performing auto-provisioning because auto-provisioning installs default static routes that may be affected by any extra routing configuration.
- A maximum of 255 characters is supported for the remote URL (200 character maximum for the filepath, the rest for the main URL consisting of the protocol, login credentials, and host IP). A maximum of 200 characters is supported for the local URL. The local file or folder name must not exceed 99 characters.
- The maximum number of file pairs for each image/config record is 10.

7.10.2 Auto-provisioning Process

1. The auto-provisioning process starts by going through interfaces with a port configuration and no IP address (IPv4 or IPv6) one by one.
2. The first interface that matches triggers the DHCP client process. See Auto-provisioning DHCP Rules.
3. A static route is automatically configured with the default gateway received by DHCP offer (Option 3 "Router" in DHCP offer).

4. Option 67 points to the location of a provisioning file. This is a URL in FTP or HTTP format.
5. The node downloads this provisioning file and places it on compact flash or RAM (configurable). The URL is in IP format and there is no need for DNS.
6. The node uses the **primary-image**/**cfg-download** parameters of the provisioning file to download the image and config file and places them at the destination dictated by the provisioning file. Only compact flash is supported.

   If the primary-image/cfg-download server times out, two more redundant servers can be configured using secondary and tertiary options.

   a. The node goes through the config file primary, secondary, and tertiary server first.
   b. Then the node goes through the image primary, secondary, and tertiary server.
   c. If the node fails to download the image or config, then the auto-provisioning process considers this interface unusable and moves to the next interface. The auto-provisioning also informs the DHCP task of the failure so DHCP releases the IP and sends a DHCP release.
7. The node loads the bof part of the provisioning file into the bof and save the bof. The bof must point to compact flash.
8. The user can force a reboot after successful execution or choose to clear the force reboot option and reboot the node manually.
9. After the reboot, the node boots from compact flash and comes back up with an operational bof.cfg
10. Any further image or config updates are done using a console.

7.10.3 Auto-provisioning DHCP Rules

The following are the DHCP rules in the auto-provisioning stage:

1. First, auto-provisioning walks through the interfaces with a configured port, where the port is in operational status up, one by one.
2. It sends a DHCP request to the first configured interface with a port up and no IP address configured.
   a. If, on this interface, multiple DHCP offers arrives, only the first offer is sent to the auto-provisioning task and the other offers are ignored. This could occur if the node is on a LAN and multiple DHCP servers are connected to the interface.

b. The DHCP client has an exponential retry mechanism. If the DHCP offer does not arrive from the server, the client resends a DHCP request at 2, 4, 8, 32 and 64 s, with 64 s being the maximum timeout, If the 64 s timeout interval is reached, the DHCP client keeps retrying every 64 s. The user can configure a timeout value. If no DHCP offer has arrived by this timeout value, the auto-provisioning process moves to the next interface.

c. If the DHCP offer arrives on the port and the DHCP client task does not acknowledge the DHCP offer, for any reason, it disables the DHCP client and remove the IP from the port.

d. If the DHCP offer arrives on the port and the DHCP client acknowledges the offer, it sends the information to auto-provisioning. If auto-provisioning does not like the offer, because there is no Option 67, Option 67 is malformed, or for any other reason listed in Auto-provisioning Failure, the auto-provisioning process deconfigures the DHCP client and the DHCP client sends a DHCP release, and unassigns the IP address.

e. In case of failure, detailed information is displayed by the auto-provisioning process and the process moves to the next port that is up and does not have an IP address.

3. If auto-provisioning is successful using the offer and its option, the provisioning file download starts though the protocol dictated by Option 67.

The **auto-provisioning** command is CLI blocking. All information about the auto-provisioning process is displayed on the CLI and logged.

7.10.4 Auto-provisioning Failure

Auto-provisioning fails for the following reasons:

- There is no Option 67.
- The Option 67 format is not acceptable to auto-provisioning.
- The format is a URL or DNS is not supported.
- There is a failure in the download provisioning file or the server is not reachable.
- There is failure in the download of the image or config file using the provisioning file information, for example, the server is not available, the wrong directory is listed, or the wrong credentials are given.
- The image or config fails to copy to the compact flash.
- The image or config fails to sync to the inactive CPM.
- The BOF does not point to the compact flash, for example, it is pointing to the network.

If the auto-provisioning procedure on this interface fails, then auto-provisioning:

1. Displays all information on the blocked CLI and in the log, explaining the failure in detail.
2. Updates the DHCP task so the DHCP task can take the appropriate actions to release the IP address on the interface. This is done by sending a DHCP release for the DHCP ack received from the server.
3. Goes to the next interface with port up and no IP address.
4. If no other interface with port up is found, the auto-provisioning task stops and a failure error is displayed on the CLI and in the log.

7.11 Administrative Tasks

This section contains information to perform administrative tasks.

7.11.1 Saving Configurations

Whenever configuration changes are made, the modified configuration must be saved so they are not lost when the system is rebooted.

Configuration files are saved by executing explicit command syntax which includes the file URL location to save the configuration file as well as options to save both default and non-default configuration parameters. Boot option file (BOF) parameters specify where the system should search for configuration and image files as well as other operational parameters during system initialization.

For more information about boot option files, refer to the Boot Options section.

7.11.2 Specifying Post-Boot Configuration Files

Two post-boot configuration extension files are supported and are triggered when either a successful or failed boot configuration file is processed. The **boot-bad-exec** and **boot-good-exec** commands specify URLs for the CLI scripts to be run following the completion of the bootup configuration. A URL must be specified or no action is taken.

For example, after a configuration file is successfully loaded, the specified URL can contain a nearly identical configuration file with certain commands enabled or disabled, or particular parameters specified and according to the script which loads that file.

7.11.3 Network Timing

In Time Domain Multiplexed (TDM)-based networks (for example, SONET or SDH circuit- switched networks), the concept of network timing is used to prevent over-run or under-run issues where circuits are groomed (rebundled) and switched. Hardware exists in each node that takes a common clock derived from an internal oscillator, a specific receive interface, or special BITS interface and provides it to each synchronous interface in the system. Usually, each synchronous interface is allowed to choose between using the chassis-provided clock or the clocking recovered from the received signal on the interface. The clocking is used to drive the transmit side of the interface. The appropriate configuration at each node which defines how interface clocking is handled must be considered when designing a network that has a centralized timing source so each interface is operating in a synchronous manner.

The effect of timing on a network is dependent on the nature of the type of traffic carried on the network. With bit-wise synchronous traffic (traditional circuit-based voice or video), non-synchronous transmissions cause a loss of information in the streams affecting performance. With packet-based traffic, the applications expect and handle jitter and latency inherent to packet-based networks. When a packet-based network is used to carry voice or video traffic, the applications use data compression and elasticity buffering to compensate for jitter and latency. The network itself relies on appropriate Quality of Service (QoS) definitions and network provisioning to further minimize the jitter and latency the application may experience.

7.11.4 Power Supplies

SR OS supports a **power-supply** command to configure the type and number of power supplies present in the chassis. The operational status of a power source is always displayed by the LEDs on the Control Processor/Switch Fabric Module (CP/SFM) front panel, but the power supply information must be explicitly configured in order for a power supply alarm to be generated if a power source becomes operationally disabled.

7.11.5 Automatic Synchronization

Use the CLI syntax displayed below to configure synchronization components relating to active-to-standby CPM switchover. In redundant systems, synchronization ensures that the active and standby CPMs have identical operational parameters, including the active configuration, CPM, XCM, and IOM images in the event of a failure or reset of the active CPM.

The **force-switchover** command forces a switchover to the standby CPM card.

To enable automatic synchronization, either the **boot-env** parameter or the **config** parameter must be specified. The synchronization occurs when the **admin save** or **bof save** commands are executed.

When the **boot-env** parameter of the **synchronize** command is specified, the bof.cfg, primary/secondary/tertiary configuration files (.cfg and .ndx), li, and ssh files are automatically synchronized. When the **config** parameter is specified, only the configuration files are automatically synchronized.

Synchronization also occurs whenever the BOF is modified and when an **admin>save** command is entered with no filename specified.

7.11.5.1 Boot-Env Option

The **boot-env** option enables a synchronization of all the files used in system initialization.

When configuring the system to perform this synchronization, the following occurs:

1. The BOF used during system initialization is copied to the same compact flash on the standby CPM (in redundant systems). The synchronization parameters on the standby CPM are preserved.
2. The primary, secondary, and tertiary images, (provided they are locally stored on the active CPM) are copied to the same compact flash on the standby CPM.
3. The primary, secondary, and tertiary configuration files, (provided they are locally stored on the active CPM) are copied to the same compact flash on the standby CPM.

7.11.5.2 Config Option

The **config** option synchronizes configuration files by copying the files specified in the active CPM BOF file to the same compact flash on the standby CPM.

Both image files (CPM and IOM) on the 7450 ESS must be located in the same directory. Failure to locate and synchronize both images causes an error to be generated.

7.11.6 Manual Synchronization

The **admin redundancy synchronize** command performs manual CPM synchronizations. The **boot-env** parameter synchronizes the BOF, image, and configuration files in redundant systems. The **config** parameter synchronizes only the configuration files in redundant systems.

7.11.6.1 Forcing a Switchover

The **force-switchover now** command forces an immediate switchover to the standby CPM card.

If the active and standby are not synchronized for some reason, users can manually synchronize the standby CPM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CPM.

7.12 System Router Instances

SR OS supports multiple Layer 3 router instances. These instances have their own IP addressing spaces and parameters. Router instances are isolated from each other.

The following are the different types of router instances in SR OS:

- **Base**

  All SR OS routers have the Base router instance: the system created default router instance used to forward user IP traffic among router line card ports. Router interfaces (that is, network interfaces configured under **configure router** [**Base**]) and IES services and interfaces exist in the Base router instance. The Base router instance is identified in SNMP as vRtrType = baseRouter (1) and has a vRtrID of 1.

- **VPRN instances**

  Another type of router instance is the set of operator configured VPRN services. Each VPRN service has a unique router instance. For more information about VPRN services and their associated router instances, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN*. VPRN router instances are identified in SNMP as vRtrType = vprn (2), and the vRtrID is dynamically allocated.

- **Special system router instances**

  SR OS routers also support the following special router instances:

  - **management**

    The management router instance is a system created router instance that is used for management of the router. The management router instance is bound to CPM/CCM ports A/1 and B/1. This is a CPM router instance which cannot be renamed or deleted by an operator. The management router instance is identified in SNMP as vRtrType = vr(3), and the vRtrID is 4095.

  - **vpls-management**

    The vpls-management router instance is used for management of VPLS services. It is identified in SNMP as vRtrType = vr(3), and the vRtrID is 4094.

- **User created CPM router instances**

  User created CPM router instances are user defined router instances that are mainly used with ethernet ports on the CPM/CCM cards: CPM router instances only use CPM/CCM Ethernet ports as interfaces. CPM router instances have a user-defined name and are the only types of non-VPRN router instances that can be created by the user. User created CPM router instances are identified in SNMP as vRtrType = vr(3), and the vRtrID is dynamically allocated.

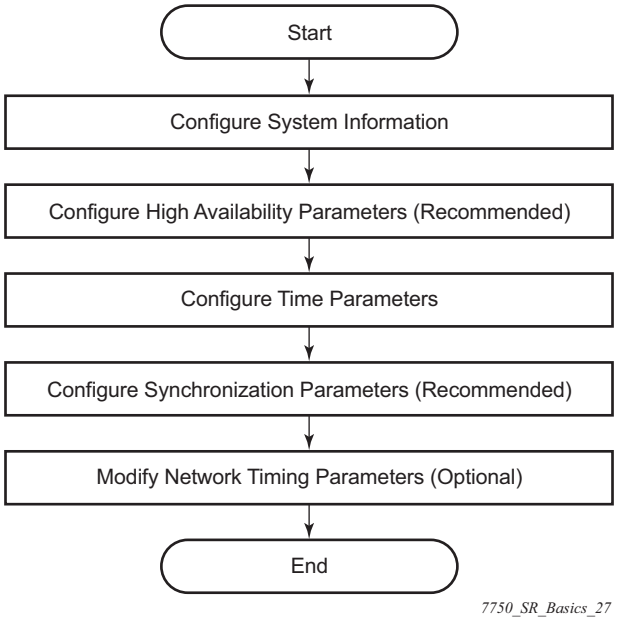
Some management protocols can use either the base routing instance (in-band) or the management routing instance (out-of-band). A listing of these protocols can be found in the CPM Filter: Protocols and Ports section of the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*. Unless otherwise stated in the detailed description of the protocol, when the server or client for the protocol is reachable via the management routing instance, those protocol messages use the management interface for the protocol communication.

If BOF is set up with autoconfiguration and the DHCP server provides a general default route such as 0.0.0.0/0, with some protocols (like PCEP, TACACS+, RADIUS, and LDAP), Authentication, Authorization, Accounting (AAA) always prefers OOB over in-band connectivity. This is because these protocols prefer to use the OOB management port first. If a matching route is not found, in-band is attempted. The static route provided by DHCP must be properly set to ensure the correct route preference is made by these protocols.

7.13 System Configuration Process Overview

Figure 29 shows the process to provision basic system parameters.

Figure 29 **System Configuration and Implementation Flow**



7.14 Configuration Notes

This section describes system configuration caveats.

7.14.1 General

To access the CLI, the system must be properly initialized and the boot loader and BOF files successfully executed.

7.15 Configuring System Management with CLI

This section provides information about configuring system management features with CLI.

7.15.1 Saving Configurations

Whenever configuration changes are made, the modified configuration must be saved so the changes will not be lost when the system is rebooted. The system uses the configuration and image files, as well as other operational parameters necessary for system initialization, according to the locations specified in the boot option file (BOF) parameters. For more information about boot option files, see Boot Options.

Configuration files are saved by executing *implicit* or *explicit* command syntax.

- An *explicit* save writes the configuration to the location specified in the save command syntax (the *file-url* option).
- An *implicit* save writes the configuration to the file specified in the primary configuration location.

  If the *file-url* option is not specified in the save command syntax, the system attempts to save the current configuration to the current BOF primary configuration source. If the primary configuration source (path and filename) changed since the last boot, the new configuration source is used.

The save command includes an option to save both default and non-default configuration parameters (the **detail** option).

The **index** option specifies that the system preserves system indexes when a save command is executed, regardless of the persistent status in the BOF file. During a subsequent boot, the index file is read along with the configuration file. As a result, a number of system indexes are preserved between reboots, including the interface index, LSP IDs, path IDs, and so on. This reduces resynchronizations of the Network Management System (NMS) with the affected network element.

If the save attempt fails at the destination, an error occurs and is logged. The system does not try to save the file to the secondary or tertiary configuration sources unless the path and filename are explicitly named with the save command.

7.15.2 Basic System Configuration

This section provides information to configure system parameters and provides configuration examples of common configuration tasks. The minimal system parameters that should be configured are:

- System Information Parameters
- System Time Elements

The following example shows a basic system configuration:

```
A:ALA-12>config>system# info
#------------------------------------------
echo "System Configuration "
#------------------------------------------
        name "ALA-12"
        coordinates "Unknown"
        snmp
        exit
        security
            snmp
                community "private" rwa version both
            exit
        exit
        time
            ntp
                server 192.168.15.221
                no shutdown
            exit
            sntp
                shutdown
            exit
            zone GMT
        exit
------------------------------------------------
A:ALA-12>config>system#
```

7.15.3 Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure system parameters and provides the CLI commands.

7.15.3.1 System Information

This section covers the basic system information parameters to configure the physical location of the router, contact information, location information (the place the router is located such as an address, floor, room number, and so on), global positioning system (GPS) coordinates, and system name.

7.15.3.1.1 System Information Parameters

Name

Use the **system** command to configure a name for the device. The name is used in the prompt string. Only one system name can be configured, if multiple system names are configured the last one encountered overwrites the previous entry. Use the following CLI syntax to configure the system name:

CLI Syntax:
```
config>system
name system-name
```

Example:
```
config>system# name ALA-12
```

The following example shows the system name:

```
sysName@domain>config>system# info
#------------------------------------------
echo "System Configuration "
#------------------------------------------
        name "ALA-12"
. . .
        exit
----------------------------------------------
sysName@domain>config>system#
```

Contact

Use the **contact** command to specify the name of a system administrator, IT staff member, or other administrative entity.

CLI Syntax:
```
config>system
contact contact-name
```

Example:
```
config>system# contact "Fred Information Technology"
```

Location

Use the **location** command to specify the system location of the device. For example, enter the city, building address, floor, room number, and so on, where the router is located.

Use the following CLI syntax to configure the location:

CLI Syntax:
```
config>system
location location
```

Example:
```
config>system# location "Bldg.1-floor 2-Room 201"
```

CLLI Code

The Common Language Location Code (CLLI code) is an 11-character standardized geographic identifier that is used to uniquely identify the geographic location of an SR-series router.

Use the following CLI command syntax to define the CLLI code:

CLI Syntax:
```
config>system
       clli-code clli-code
```

Example:
```
config>system# clli-code abcdefg1234
```

7.15.3.1.2 Coordinates

Use the optional **coordinates** command to specify the GPS location of the device. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

Use the following CLI syntax to configure the location:

CLI Syntax:
```
config>system
coordinates coordinates
```

Example:
```
config>system# coordinates "N 45 58 23, W 34 56 12"
```

The following example shows the configuration output of the general system commands:

```
sysName@domain>config>system# info
#------------------------------------------
```

```
echo "System Configuration "
#------------------------------------------
name "ALA-12"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"

. . .
        exit
-------------------------------------------------
A:ALA-12>config>system#
```

7.15.3.1.3 System Time Elements

The system clock maintains time according to Coordinated Universal Time (UTC). Configure information time zone and summer time (daylight savings time) parameters to correctly show time according to the local time zone.

Zone

The **zone** command sets the time zone and/or time zone offset for the router. The router supports system-defined and user-defined time zones. The system-defined time zones are listed in Table 21.

CLI Syntax: `config>system>time`
`zone` *`std-zone-name`* | *`non-std-zone-name`* [*`hh`*[`:`*`mm`*]]

Example:
```
config>system>time#
config>system>time# zone GMT
```

The following example shows the zone output:

```
A:ALA-12>config>system>time# info
-----------------------------------------------
ntp
                server 192.168.15.221
                no shutdown
exit
sntp
                shutdown
exit
zone UTC
-----------------------------------------------
A:ALA-12>config>system>time#
```

Table 21 **System-defined Time Zones**

Acronym	Time Zone Name	UTC Offset
Europe		
GMT	Greenwich Mean Time	UTC
WET	Western Europe Time	UTC
WEST	Western Europe Summer Time	UTC +1 hour
CET	Central Europe Time	UTC +1 hour
CEST	Central Europe Summer Time	UTC +2 hours
EET	Eastern Europe Time	UTC +2 hours
EEST	Eastern Europe Summer Time	UTC +3 hours
MSK	Moscow Time	UTC +3 hours
MSD	Moscow Summer Time	UTC +4 hours
US and Canada		
AST	Atlantic Standard Time	UTC -4 hours
ADT	Atlantic Daylight Time	UTC -3 hours
EST	Eastern Standard Time	UTC -5 hours
EDT	Eastern Daylight Saving Time	UTC -4 hours
CST	Central Standard Time	UTC -6 hours
CDT	Central Daylight Saving Time	UTC -5 hours
MST	Mountain Standard Time	UTC -7 hours
MDT	Mountain Daylight Saving Time	UTC -6 hours
PST	Pacific Standard Time	UTC -8 hours
PDT	Pacific Daylight Saving Time	UTC -7 hours
HST	Hawaiian Standard Time	UTC -10 hours
AKST	Alaska Standard Time	UTC -9 hours
AKDT	Alaska Standard Daylight Saving Time	UTC -8 hours
Australia and New Zealand		
AWST	Western Standard Time (e.g., Perth)	UTC +8 hours

Table 21 **System-defined Time Zones (Continued)**

Acronym	Time Zone Name	UTC Offset
ACST	Central Standard Time (e.g., Darwin)	UTC +9.5 hours
AEST	Eastern Standard/Summer Time (e.g., Canberra)	UTC +10 hours
NZT	New Zealand Standard Time	UTC +12 hours
NZDT	New Zealand Daylight Saving Time	UTC +13 hours

Summer Time Coordinates

The **config>system>time>dst-zone** context configures the start and end dates and offset for summer time or daylight savings time to override system defaults or for user defined time zones.

When configured, the time will be adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends.

CLI Syntax:

```
config>system>time
dst-zone zone-name
   end {end-week} {end-day} {end-month} [hours-minutes]
   offset offset
   start {start-week} {start-day} {start-month} [hours-
     minutes]
```

Example:

```
config>system# time
config>system>time# dst-zone pt
config>system>time>dst-zone# start second sunday april
 02:00
end first sunday october 02:00
config>system>time>dst-zone# offset 0
```

If the time zone configured is listed in Table 21, then the starting and ending parameters and offset do not need to be configured with this command unless there is a need to override the system defaults. The command will return an error if the start and ending dates and times are not available either in Table 21 or entered as optional parameters in this command.

The following example shows the configured parameters.

```
A:ALA-48>config>system>time>dst-zone# info
----------------------------------------------
               start second sunday april 02:00
```

```
                end first sunday october 02:00
                offset 0
-------------------------------------------
A:ALA-48>config>system>time>dst-zone# offset 0
```

NTP

Network Time Protocol (NTP) is defined in RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis* and RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*. It allows for participating network nodes to keep time more accurately and maintain time in a synchronized manner between all participating network nodes.

Authentication-check

NTP supports an authentication mechanism to provide some security and access control to servers and clients. The default behavior when any authentication keys are configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type, or key. The authentication-check command provides for the options to skip or maintain this rejection of NTP PDUs that do not match the authentication requirements.

When authentication-check is configured, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for key-id, one for type, and one for key value mismatches.

CLI Syntax:
```
config>system>time>ntp
     authentication-check
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# authentication-check
config>system>time>ntp# no shutdown
```

Authentication-key

The **authentication-key** command configures an authentication key-id, key type, and key used to authenticate NTP PDUs sent to and received from other network elements participating in the NTP protocol. For authentication to work, the authentication key-id, authentication type and authentication key value must match.

CLI Syntax:
```
config>system>time>ntp
     authentication-key key-id {key key} [hash | hash2 |
       custom] type
```

```
                {des | message-digest}
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# authentication-key 1 key A type
 des
config>system>time>ntp# no shutdown
```

The following example shows NTP disabled with the authentication-key parameter enabled.

```
A:sim1>config>system>time>ntp# info
----------------------------------------------
            shutdown
            authentication-key 1 key "OAwgNUlbzgI" hash2 type des
----------------------------------------------
A:sim1>config>system>time>ntp#
```

Broadcast

The **broadcast** command is used to transmit broadcast packets on a given interface. Interfaces in the base routing context or the management interface may be specified. Due the relative ease of spoofing of broadcast messages, it is strongly recommended to use authentication with broadcast mode. The messages are transmitted using a destination address that is the NTP Broadcast address.

CLI Syntax:
```
config>system>time>ntp
     broadcast [router router-name] {interface
        ip-int-name} [key-id key-id] [version version]
        [ttl ttl]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# broadcast interface int11
 version 4
ttl 127
config>system>time>ntp# no shutdown
```

The following example in the **system>time** context shows NTP enabled with the broadcast command configured.

```
A:sim1>config>system>time# info detail
----------------------------------------------
        ntp
            no shutdown
            authentication-check
            ntp-server
            broadcast interface int11 version 4 ttl 127
        exit
A:sim1>config>system>time#
```

Broadcastclient

The **broadcastclient** command enables listening to NTP broadcast messages on the specified interface. Interfaces in the base routing context or the management interface may be specified. Due the relative ease of spoofing of broadcast messages, it is strongly recommended to use authentication with broadcast mode. The messages must have a destination address of the NTP Broadcast address.

CLI Syntax:
```
config>system>time>ntp
          broadcastclient [router router-name]
            {interface ip-int-name} [authenticate]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# broadcastclient interface int11
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the broadcastclient parameter enabled.

```
A:ALA-12>config>system>time# info
----------------------------------------------
            ntp
                broadcastclient interface int11
                no shutdown
            exit
----------------------------------------------
A:ALA-12>config>system>time#
```

Multicast

When configuring NTP the node can be configured to transmit or receive multicast packets on the CPM MGMT port (CPM applies to the 7450 ESS and 7750 SR). Broadcast & Multicast messages can easily be spoofed, therefore, authentication is strongly recommended. Multicast is used to configure the transmission of NTP multicast messages. The **no** construct of this command removes the transmission of multicast packets on the management port.

When transmitting multicast NTP messages the default address of 224.0.1.1 is used.

CLI Syntax:
```
config>system>time>ntp
     multicast [version version] [key-id key-id]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# multicast
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the multicast command configured.

```
A:ALA-12>config>system>time# info
----------------------------------------------
             server 192.168.15.221
             multicast
             no shutdown
----------------------------------------------
A:ALA-12>config>system>time#
```

Multicastclient

The **multicastclient** command is used to configure an address to receive multicast NTP messages on the CPM MGMT port (7450 ESS and 7750 SR). Broadcast & Multicast messages can easily be spoofed, therefore, authentication is strongly recommended. The no construct of this command removes the multicast client. If multicastclient is not configured, all NTP multicast traffic will be ignored.

CLI Syntax:
```
config>system>time>ntp
     multicastclient [authenticate]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# multicastclient authenticate
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the multicastclient command configured.

```
A:ALA-12>config>system>time# info
----------------------------------------------
             server 192.168.15.221
             multicastclient
             no shutdown
----------------------------------------------
A:ALA-12>config>system>time##
```

NTP-Server

The **ntp-server** command configures the node to assume the role of an NTP server. Unless the server command is used this node will function as an NTP client only and will not distribute the time to downstream network elements. If authentication is specified in this command, the NTP server requires client packets to be authenticated based on the key received in the client request.

CLI Syntax:
```
config>system>time>ntp
     ntp-server [authenticate]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# ntp-server
```

```
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the ntp-server command configured.

```
A:sim1>config>system>time>ntp# info
----------------------------------------------
        no shutdown
        ntp-server
----------------------------------------------
A:sim1>config>system>time>ntp#
```

Peer

Configuration of an NTP peer configures symmetric active mode for the configured peer. Although any system can be configured to peer with any other NTP node, it is recommended to configure authentication and to configure known time servers as their peers. Use the **no** form of the command to remove the configured peer.

CLI Syntax:
```
config>system>time>ntp
     peer ip-address [version version] [key-id key-id]
     [prefer]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# peer 192.168.1.1 key-id 1
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the peer command configured.

```
A:sim1>config>system>time>ntp# info
----------------------------------------------
            no shutdown
            peer 192.168.1.1 key-id 1
----------------------------------------------
A:sim1>config>system>time>ntp#
```

Server

The **server** command is used when the node should operate in client mode with the NTP server specified in the address field. Use the **no** form of this command to remove the server with the specified address from the configuration.

Up to ten NTP servers can be configured.

CLI Syntax:
```
config>system>time>ntp
     server ip-address [key-id key-id] [version version]
        [prefer]
```

Example:
```
config>system>time>ntp#
config>system>time>ntp# server 192.168.1.1 key-id 1
config>system>time>ntp# no shutdown
```

The following example shows NTP enabled with the server command configured.

```
A:sim1>config>system>time>ntp# info
----------------------------------------------
            no shutdown
            server 192.168.1.1 key 1
----------------------------------------------
A:sim1>config>system>time>ntp#
```

SNTP

SNTP is a compact, client-only version of the NTP. SNTP can only receive the time from SNTP/NTP servers; it cannot be used to provide time services to other systems. SNTP can be configured in either broadcast or unicast client mode.

CLI Syntax:
```
config>system
time
   sntp
      broadcast-client
      server-address ip-address [version version-number]
         [normal | preferred] [interval seconds]
      no shutdown
```

Broadcast-client

The **broadcast-client** command enables listening at the global device level to SNTP broadcast messages on interfaces with broadcast client enabled.

CLI Syntax:
```
config>system>time>sntp
   broadcast-client
```

Example:
```
config>system>time>sntp#
config>system>time>sntp# broadcast-client
config>system>time>sntp# no shutdown
```

The following example shows SNTP enabled with the **broadcast-client** command enabled.

```
A:ALA-12>config>system>time# info
----------------------------------------------
            sntp
                broadcast-client
                no shutdown
```

```
            exit
            dst-zone PT
                start second sunday april 02:00
                end first sunday october 02:00
                offset 0
            exit
            zone GMT
-----------------------------------------------
A:ALA-12>config>system>time#
```

Server-address

The **server-address** command configures an SNTP server for SNTP unicast client mode.

CLI Syntax:
```
config>system>time>sntp#
config>system>time>sntp# server-address ip-address
 version version-number] [normal | preferred] [interval
 seconds]
```

Example:
```
config>system>time>sntp#
config>system>time# server-address 10.10.0.94 version 1
 preferred interval 100
```

The following example shows SNTP enabled with the **server-address** command configured.

```
A:ALA-12>config>system>time# info
-----------------------------------------------
            sntp
                server-address 10.10.0.94 version 1 preferred interval 100
                no shutdown
            exit
            dst-zone PT start-date 2006/04/04 12:00 end-date 2006/10/25 12:00
            zone GMT
-----------------------------------------------
A:ALA-12>config>system>time#
```

CRON

CRON provides various time and date scheduling functions. Configuration notes for the CRON schedule are provided below.

Schedule

The schedule function configures the type of schedule to run, including one-time only (oneshot), periodic or calendar-based runs. All runs are determined by month, day of month or weekday, hour, minute and interval (seconds). If end-time and interval are both configured, whichever condition is reached first is applied.

Example:
```
config>system>cron# schedule test2
config>system>cron>sched# day-of-month 17
config>system>cron>sched# end-time 2007/07/17 12:00
config>system>cron>sched# minute 0 15 30 45
config>system>cron>sched# weekday friday
config>system>cron>sched# shut
```

The following example schedules a script named “test2” to run every 15 minutes on the 17th of each month and every Friday until noon on July 17, 2007:

```
*A:SR-3>config>system>cron# info
----------------------------------------------
        schedule "test2"
            shutdown
            day-of-month 17
            minute 0 15 30 45
            weekday friday
            end-time 2007/07/17 12:00
        exit
----------------------------------------------
*A:SR-3>config>system>cron#
```

7.15.3.1.4 ANCP Enhancements

Persistency is available for subscriber’s ANCP attributes and is stored on the on-board compact flash card. ANCP data will stay persistence during an ISSU as well as nodal reboots. During recovery, ANCP attributes are first restored fully from the persistence file, and incoming ANCP sessions are temporarily on hold. Afterwards, new ANCP data can overwrite any existing values. This new data is then stored into the compact flash in preparation for the next event.

7.15.3.2 Configuring Synchronization and Redundancy

7.15.3.2.1 Configuring Persistence

The following example shows subscriber management system persistence command usage for the 7450 ESS and 7750 SR:

Example:
```
config>system# persistence
config>system>persistence# subscriber-mgmt
config>system>persistence>sub-mgmt# description
 "cf3:SubMgmt-Test"
config>system>persistence>sub-mgmt# location cf3:
config>system>persistence>sub-mgmt# exit
```

```
A:ALA-12>config>system>persistence# info
----------------------------------------------
            subscriber-mgmt
                description "cf3:SubMgmt-Test"
                location cf1:
            exit
----------------------------------------------
A:ALA-12>config>system>persistence#
```

7.15.3.2.2 Configuring Synchronization

The **switchover-exec** command specifies the location and name of the CLI script file executed following a redundancy switchover from the previously active CPM card.

CLI Syntax:
```
admin>redundancy
synchronize {boot-env | config}
config>system
switchover-exec file-url
```

7.15.3.2.3 Configuring Manual Synchronization

Note that automatic synchronization can be configured in the **config>system> synchronization** context.

CLI Syntax:
```
admin
redundancy
  synchronize {boot-env|config}
```

Example:
```
admin>redundancy# synchronize config
```

The following shows the output shown during a manual synchronization:

```
A:ALA-12>admin# synchronize config

Syncing configuration......

Syncing configuration.....Completed.
A:ALA-12#
```

7.15.3.2.4 Forcing a Switchover

The **force-switchover now** command forces an immediate switchover to the standby CPM card.

CLI Syntax:
```
admin>redundancy
force-switchover [now]
```

Example:
```
admin>redundancy# force-switchover now
```

```
A:ALA-12# admin redundancy force-switchover now
A:ALA-12#
Resetting...
?
```

If the active and standby are not synchronized for some reason, users can manually synchronize the standby CPM by rebooting the standby by issuing the **admin reboot standby** command on the active or the standby CPM.

7.15.3.2.5 Configuring Synchronization Options

Network operators can specify the type of synchronization operation to perform between the primary and secondary CPMs after a change has been made to the configuration files or the boot environment information contained in the boot options file (BOF).

Use the following CLI to configure the boot-env option:

CLI Syntax:
```
config>system
synchronize {boot-env|config}
```

Example:
```
config>system# synchronize boot-env
```

The following example shows the configuration:

```
A:ALA-12>config>system# synchronize boot-env
A:ALA-12>config>system# show system synchronization
===============================================
Synchronization Information
===============================================
Synchronize Mode        : Boot Environment
Synchronize Status      : No synchronization
Last Config Sync Time   : 2006/06/27 06:19:47
Last Boot Env Sync Time : 2006/06/27 06:19:47
===============================================
A:ALA-12>config>system#
```

Use the following CLI to configure the config option:

CLI Syntax: `config>system`
`synchronize {boot-env|config}`

Example: `config>system# synchronize config`

The following example shows the configuration.

```
A:ALA-12>config>system# synchronize config
A:ALA-12>config>system# show system synchronization
===============================================
Synchronization Information
===============================================
Synchronize Mode        : Configuration
Synchronize Status      : No synchronization
Last Config Sync Time   : 2006/06/27 09:17:15
Last Boot Env Sync Time : 2006/06/24 07:16:37
===============================================
A:ALA-12>config>system#
```

7.15.3.3 Configuring Multi-Chassis Redundancy for LAG

When configuring associated LAG ID parameters, the LAG must be in access mode and LACP must be enabled.

Use the CLI syntax shown below to configure multi-chassis redundancy features.

CLI Syntax:

```
config>redundancy
multi-chassis
   peer ip-address
      authentication-key [authentication-key | hash-key]
         [hash | hash2 | custom]
      description description-string
      mc-lag
         hold-on-neighbor-failure duration
         keep-alive-interval interval
         lag lag-id lacp-key admin-key system-id system-id
            [remote-lag lag-id] system-priority system-
            priority
         no shutdown
      no shutdown
      source-address ip-address
      sync
         igmp
```

```
igmp-snooping
pim-snooping [sap]
port [port-id | lag-id] [sync-tag sync-tag]
   range encap-range sync-tag sync-tag
no shutdown
srrp
sub-mgmt
```

Example:

```
config>redundancy#
config>redundancy# multi-chassis
config>redundancy>multi-chassis# peer 10.10.10.2 create
config>redundancy>multi-chassis>peer# description "Mc-
 Lag peer 10.10.10.2"
config>redundancy>multi-chassis>peer# mc-lag
config>redundancy>mc>peer>mc-lag# lag 1 lacp-key 32666
 system-id 00:00:00:33:33:33 system-priority 32888
config>redundancy>mc>peer>mc-lag# no shutdown
config>redundancy>mc>peer>mc-lag# exit
config>redundancy>multi-chassis>peer# no shutdown
config>redundancy>multi-chassis>peer# exit
config>redundancy>multi-chassis# exit
config>redundancy#
```

The following example shows the configuration:

```
A:ALA-48>config>redundancy# info
----------------------------------------------
       multi-chassis
           peer 10.10.10.2 create
               description "Mc-Lag peer 10.10.10.2"
               mc-lag
                   no shutdown
               exit
               no shutdown
           exit
       exit
----------------------------------------------
A:ALA-48>config>redundancy#
```

7.15.3.4 Configuring Power Supply Parameters

The following is an example for the 7750 SR and 7950 XRS:

```
A:ALA-12>config>system# info
----------------------------------------------------------------------
..
        name "ALA-12"
```

```
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        power-supply 1 dc
        power-supply 2 dc
        lacp-system-priority 1
        sync-if-timing
            begin
            ref-order ref1 ref2 bits
            ref1
                shutdown
            exit
            ref2
                shutdown
            exit
            bits
                shutdown
                interface-type ds1 esf
            exit
            commit
        exit
..
```

The following is an example for the 7450 ESS:

```
-------------------------------------------------------------------
A:ALA-12>config>system# info
-------------------------------------------------------------------
..
        name "ALA-12"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        power-supply 1 dc
        power-supply 2 dc
        lacp-system-priority 1
        sync-if-timing
            begin
            ref-order ref1 ref2 bits
            ref1
                shutdown
            exit
            ref2
                shutdown
            exit
            bits
                shutdown
                interface-type ds1 esf
            exit
            commit
        exit
..
-------------------------------------------------------------------
A:ALA-12>config>system#
```

7.15.3.5 Configuring ATM System Parameters

The ATM context configures system-wide ATM parameters for the 7750 SR.

CLI Syntax:

```
config>system#
atm
   atm-location-id location-id
   oam
      loopback-period period
      retry-down retries
      retry-up retries
```

Example:

```
config>system# atm
config>system>atm# atm-location-id
 03:00:00:00:00:00:00:00:00:00: 00:00:00:00:00:00
config>system>atm# oam
config>system>atm>oam# loopback-period 30
config>system>atm>oam# retry-down 5
config>system>atm>oam# retry-up 3
config>system>atm>oam# exit
```

The following example shows the ATM configuration.

```
A:ALA-12>config>system>atm# info
----------------------------------------------
            atm-location-id 03:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
            oam
                retry-up 3
                retry-down 5
                loopback-period 30
            exit
----------------------------------------------
A:ALA-12>config>system>atm#
```

7.15.3.6 Configuring Backup Copies

The config-backup command allows you to specify the maximum number of backup versions of configuration and index files kept in the primary location.

For example, assume the **config-backup** *count* is set to **5** and the configuration file is called *xyz.cfg.* When a **save** command is executed, the file *xyz.cfg* is saved with a .1 extension. Each subsequent **config-backup** command increments the numeric extension until the maximum count is reached. The oldest file (**5**) is deleted as more recent files are saved.

xyz.cfg

xyz.cfg.**1**

xyz.cfg.**2**

xyz.cfg.**3**

xyz.cfg.**4**

xyz.cfg.**5**

xyz.ndx

Each persistent index file is updated at the same time as the associated configuration file. When the index file is updated, then the save is performed to *xyz .cfg* and the index file is created as *xyz.ndx*. Synchronization between the active and standby SF/CPMSF/CPM is performed for all configurations and their associated persistent index files.

CLI Syntax:
```
config>system
   config-backup count
```

Example:
```
config>system#
config>system# config-backup 7
```

The following example shows the config-backup configuration.

```
A:ALA-12>config>system>time# info
#------------------------------------------
echo "System Configuration"
#------------------------------------------
        name "ALA-12"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        config-backup 7
...
-------------------------------------------------
A:ALA-12>config>system>time#
```

7.15.3.7 Post-Boot Configuration Extension Files

Two post-boot configuration extension files are supported and are triggered when either a successful or failed boot configuration file is processed. The commands specify URLs for the CLI scripts to be run following the completion of the bootup configuration. A URL must be specified or no action is taken. The commands are persistent between router (re)boots and are included in the configuration saves (admin>save).

CLI Syntax:

```
config>system
        boot-bad-exec file-url
        boot-good-exec file-url
```

Example:

```
config>system# boot-bad-exec ftp://
 test:test@192.168.xx.xxx/./
fail.cfg
config>system# boot-good-exec ftp://
 test:test@192.168.xx.xxx/./
ok.cfg
```

The following example shows the command output:

```
A:ALA-12>config>system# info
#------------------------------------------
echo "System Configuration"
#------------------------------------------
        name "ALA-12"
        contact "Fred Information Technology"
        location "Bldg.1-floor 2-Room 201"
        clli-code "abcdefg1234"
        coordinates "N 45 58 23, W 34 56 12"
        config-backup 7
        boot-good-exec "ftp://test:test@192.168.xx.xxx/./ok.cfg"
        boot-bad-exec "ftp://test:test@192.168.xx.xxx/./fail.cfg"
        power-supply 1 dc
        power-supply 2 dc
        lacp-system-priority 1
        sync-if-timing
            begin
            ref-order ref1 ref2 bits
..
-------------------------------------------------
A:ALA-12>config>system#
```

7.15.3.7.1 Show Command Output and Console Messages

The **show**>**system**>**information** command shows the current value of the bad/good exec URLs and indicates whether a post-boot configuration extension file was executed when the system was booted. If an extension file was executed, the **show**>**system**>**information** command also indicates if it completed successfully or not.

The following is an example for the 7750 SR:

```
ALA-12>config>system#  show system information
===============================================================================
System Information
===============================================================================
System Name            : ALA-12
System Contact         : Fred Information Technology
System Location        : Bldg.1-floor 2-Room 201
System Coordinates     : N 45 58 23, W 34 56 12
System Up Time         : 1 days, 04:59:33.56 (hr:min:sec)

SNMP Port              : 161
SNMP Engine ID         : 0000197f000000000467ff00
SNMP Max Message Size  : 1500
SNMP Admin State       : Disabled
SNMP Oper State        : Disabled
SNMP Index Boot Status : Not Persistent

BOF Source             : cf1:
Image Source           : primary
Config Source          : primary
Last Booted Config File: ftp://test:test@192.168.xx.xxx/./12.cfg
Last Boot Cfg Version  : THU MAR 04 22:39:03 2004 UTC
Last Boot Config Header: # TiMOS-L-14.0.B1-217 boot/
i386 Nokia 7750 SR Copyright (c)
                        2000-2016 Nokia.
                       # All rights reserved. All use subject to applicable license
                        agreements.
                        # Built on Wed Jul 13 19:08:56 PDT 2016 by builder in /
                        rel14.0/b1/B1-217/panos/main
Last Boot Index Version: N/A
Last Boot Index Header : N/A
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: Yes
Time Last Modified     : 2004/03/06 03:30:45
Max Cfg/BOF Backup Rev : 7
Cfg-OK Script          : ftp://test:test@192.168.xx.xxx/./ok.cfg
Cfg-OK Script Status   : not used
Cfg-Fail Script        : ftp://test:test@192.168.xx.xxx/./fail.cfg
Cfg-Fail Script Status : not used

Management IP Addr     : 192.168.xx.xxx/20
DNS Server             : 192.168.1.254
DNS Domain             : eng.timetra.com
BOF Static Routes      :
  To                   Next Hop
  172.16.0.0/22        192.168.1.251
```

```
ICMP Vendor Enhancement: Disabled
ATM Location ID        : 01:00:00:00:00:11:00:00:00:00:00:00:00:00:00:00
===============================================================================
ALA-12>config>system#
```

When executing a post-boot configuration extension file, status messages are output to the CONSOLE screen prior to the “Login” prompt.

Following is an example of a failed bootup configuration that caused a boot-bad-exec file containing another error to be executed:

```
Attempting to exec configuration file:
'ftp://test:test@192.168.xx.xxx/./12.cfg' ...
System Configuration
Log Configuration
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./12.cfg, Line 195: Command "log" failed.
CRITICAL: CLI #1002 An error occurred while processing the configuration file.
The system configuration is missing or incomplete.
MAJOR: CLI #1008 The SNMP daemon is disabled.
If desired, enable SNMP with the 'config>system>snmp no shutdown' command.
Attempting to exec configuration failure extension file:
'ftp://test:test@192.168.xx.xxx/./fail.cfg' ...
Config fail extension
Enabling SNMP daemon
MAJOR: CLI #1009 An error occurred while processing a CLI command -
File ftp://test:test@192.168.xx.xxx/./fail.cfg, Line 5: Command "abc log" failed.
TiMOS-L-14.0.B1-217 boot/i386 Nokia 7750 SR Copyright (c) 2000-2016 Nokia.
All rights reserved. All use subject to applicable license agreements.
Built on Wed Jul 13 19:08:56 PDT 2016 by builder in /rel14.0/b1/B1-217/panos/main


Login:
```

7.15.4 System Timing

In the event that network timing is required for the synchronous interfaces in the router, a timing subsystem is utilized to provide a clock to all synchronous interfaces within the system.

This section describes the commands used to configure and control the timing subsystem.

7.15.4.1 Edit Mode

To enter the mode to edit timing references, you must enter the **begin** keyword at the **config**>**system**>**sync-if-timing#** prompt.

Use the following CLI syntax to enter the edit mode:

CLI Syntax: `config>system>sync-if-timing`
`begin`

The following error message shows when the you try to modify **sync-if-timing** parameters without entering the keyword **begin**.

```
A:ALA-12>config>system>sync-if-timing>ref1# source-port 2/1/1
MINOR: CLI The sync-if-timing must be in edit mode by calling begin before any
changes can be made.
MINOR: CLI Unable to set source port for ref1 to 2/1/1
A:ALA-12>config>system>sync-if-timing>ref1#
```

7.15.4.2 Configuring Timing References

Use the following CLI syntax to configure timing reference parameters. The source port specified for **ref1** and **ref2** is dependent on the router model type and chassis slot. Refer to the details in the specific command descriptions in the *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*.

The following shows a timing reference configuration example for the router:

```
ALA-12>config>system>sync-if-timing# info
----------------------------------------------
            ref-order ref2 ref1 bits
            ref1
                source-port 3/1/1
                no shutdown
            exit
            ref2
                source-port 6/1/2
                no shutdown
            exit
            bits
                interface-type ds1 esf
                no shutdown
            exit
----------------------------------------------
ALA-12>config>system>sync-if-timing#
```

7.15.4.3 Using the Revert Command

The **revert** command allows the clock to revert to a higher priority reference if the current reference goes offline or becomes unstable. When the failed reference becomes operational, it is eligible for selection.

When mode is non-revertive, a failed clock source is not selected again. If a node would enter holdover due to the references being in previous failed state, then the node will select one of the previously failed references rather than going into holdover.

CLI Syntax:
```
config>system>sync-if-timing
   revert
```

If the current reference goes offline or becomes unstable the revert command allows the clock to revert to a higher-priority reference.

When revertive switching enabled a valid timing reference of the highest priority is used. If a reference with a higher priority becomes valid, a reference switch over to that reference is initiated. If a failure on the current reference occurs, the next highest reference takes over.

If non-revertive switching is enabled, the valid active reference always remains selected even if a higher priority reference becomes available. If the active reference becomes invalid, a reference switch over to a valid reference with the highest priority is initiated. The failed reference is eligible for selection once it becomes operational.

CLI Syntax:
```
config>system>sync-if-timing
   no revert
```

7.15.4.4 Other Editing Commands

Other editing commands include:

- commit — This command saves changes made to the timing references during a session. Modifications are not persistent across system boots unless this command is entered.
- abort — This command discards changes that have been made to the timing references during a session.

CLI Syntax:
```
config>system>sync-if-timing
abort
commit
```

7.15.4.5 Forcing a Specific Reference

The debug sync-if-timing force-reference command should only be used to test and debug problems. Network synchronization problems may appear if network elements are left with this manual override setting. Once the system timing reference input has been forced, it may be cleared using the **no force-reference** command.

You can force the CPM clock to use a specific input reference using the **force-reference** command.

When the command is executed, the CPM clock on the active CPM immediately switches its input reference to that specified by the command. If the specified input is not available (shutdown), or in a disqualified state, the CPM clock shall use the next qualified input reference based on the selection rules.

This command also affects the BITS output port. If the BITS output port selection is set to line-reference and the reference being forced is not the BITS input port, then the system uses the forced reference to generate the signal out the BITS output port. If the BITS output port selection is set to internal-clock, then the system uses the output of the CPM clock to generate the signal for the BITS output port.

On a CPM activity switch, the force command is cleared and normal reference selection is determined.

Debug configurations are not saved between reboots.

CLI Syntax:
```
debug>sync-if-timing
force-reference {ref1 | ref2 | bits}

debug>sync-if-timing# force-reference
```

7.15.5 Configuring System Monitoring Thresholds

7.15.5.1 Creating Events

The **event** command controls the generation and notification of threshold crossing events configured with the **alarm** command. When a threshold crossing event is triggered, the **rmon event** configuration optionally specifies whether an entry in the RMON-MIB log table be created to record the occurrence of the event. It can also specify whether an SNMP notification (trap) be generated for the event. There are two notifications for threshold crossing events, a rising alarm and a falling alarm.

Creating an event entry in the RMON-MIB log table does not create a corresponding entry in the event logs. However, when the event is set to trap the generation of a rising alarm or falling alarm notification creates an entry in the event logs and that is distributed to whatever log destinations are configured: console, session, memory, file, syslog, or SNMP trap destination. The logger message includes a rising or falling threshold crossing event indicator, the sample type (absolute or delta), the sampled value, the threshold value, the *rmon-alarm-id*, the associated *rmon-event-id* and the sampled SNMP object identifier.

The **alarm** command configures an entry in the RMON-MIB alarm table. The **alarm** command controls the monitoring and triggering of threshold crossing events. In order for notification or logging of a threshold crossing event to occur there must be at least one associated **rmon event** configured.

The agent periodically takes statistical sample values from the MIB variable specified for monitoring and compares them to thresholds that have been configured with the **alarm** command. The **alarm** command configures the MIB variable to be monitored, the polling period (interval), sampling type (absolute or delta value), and rising and falling threshold parameters. If a sample has crossed a threshold value, the associated ‘event’ is generated.

Preconfigured CLI threshold commands are available. Preconfigured commands hide some of the complexities of configuring RMON alarm and event commands and perform the same function. In particular, the preconfigured commands do not require the user to know the SNMP object identifier to be sampled. The preconfigured threshold configurations include memory warnings and alarms and compact flash usage warnings and alarms.

To create events, use the following CLI:

CLI Syntax:

```
config>system>thresholds# cflash-cap-warn cf1-B: rising-
 threshold 2000000 falling-threshold 1999900 interval
 240 trap startup-alarm either

config>system>thresholds# memory-use-alarm rising-
 threshold 50000000 falling-threshold 45999999 interval
 500 both startup-alarm either

config>system>thresh# rmon

config>system>thresh>rmon# event 5 both description
 "alarm testing" owner "Timos CLI"
```

The following example shows the command output:

```
A:ALA-49>config>system>thresholds# info
----------------------------------------------
            rmon
```

```
                event 5 description "alarm testing" owner "Timos CLI"
            exit
            cflash-cap-warn cf1-B: rising-threshold 2000000 falling-threshold
1999900 interval 240 trap
            memory-use-alarm rising-threshold 50000000 falling-threshold
45999999 interval 500
-----------------------------------------------
A:ALA-49>config>system>thresholds#
```

7.15.5.2 System Alarm Contact Inputs

Alarm contact inputs are physical input pins on the Alarms Interface Port of the CPM that allow the operator to monitor and report changes in external environmental conditions. In a remote or outdoor deployment, alarm inputs typically allow an operator to detect conditions such as whether a door is open or closed, an air conditioner fault has occurred, and so on.

There are four input pins, each of which can be configured with an associated severity level and normally open/normally closed state. When an input pin changes state, the router can generate log events and raise facility alarms.

There is a separate log event for each pin (for example, CHASSIS event 3003 tmnxSasAlarminput3StateChanged for input pin 3). The severity level of input pin 3 is controlled by configuring the severity level of the associated log event (using the **configure log event-control** command).

There is also a single +24VDC power output pin on the Alarms Interface Port of the CPM that can be used to supply power for the alarm inputs.

The alarm inputs can be powered in one of two ways:

- using the +24Vdc power output pin
- using an external power source

The power output pin provided on the CPM is monitored, and the router can report when the power source fails.

If using an external power source for the alarm inputs, then it is recommended that the **normal-state closed** configuration be used so that a failure of the external power source will trigger all the alarm pins to detect a change of state. If **normal-state open** is used, a failure of the external power source will not generate any notifications and the alarm input pins will no longer operate correctly.

7.15.6 Configuring LLDP

The following output shows LLDP defaults:

```
A:testSr1>config>system>lldp# info detail
----------------------------------------------
             no tx-interval
             no tx-hold-multiplier
             no reinit-delay
             no notification-interval
             no tx-credit-max
             no message-fast-tx
             no message-fast-tx-init
             no shutdown
----------------------------------------------
A:testSr1>config>system>lldp#
```

The following example shows an LLDP port configuration:

```
*A:ALA-48>config>port>ethernet>lldp# info
----------------------------------------------
                dest-mac nearest-bridge
                    admin-status tx-rx
                    tx-tlvs port-desc sys-cap
                    tx-mgmt-address system
                exit
----------------------------------------------
*A:ALA-48>config>port>ethernet>lldp#
```

The following example shows a global system LLDP configuration:

```
A:ALA-48>config>system>lldp# info
----------------------------------------------
            tx-interval 10
            tx-hold-multiplier 2
            reinit-delay 5
            notification-interval 10
----------------------------------------------
A:ALA-48>config>system>lldp#
```

8 Standards and Protocol Support

Note: The information provided in this chapter is subject to change without notice and may not apply to all platforms.

Nokia assumes no responsibility for inaccuracies.

Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

Application Assurance (AA)

3GPP Release 12, *ADC rules over Gx interfaces*

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

Asynchronous Transfer Mode (ATM)

AF-ILMI-0065.000 Version 4.0, *Integrated Local Management Interface (ILMI)*

AF-PHY-0086.001 Version 1.1, *Inverse Multiplexing for ATM (IMA) Specification*

AF-TM-0121.000 Version 4.1, *Traffic Management Specification*

GR-1113-CORE Issue 1, *Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements*

GR-1248-CORE Issue 3, *Generic Requirements for Operations of ATM Network Elements (NEs)*

RFC 1626, *Default IP MTU for use over ATM AAL5*

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Bidirectional Forwarding Detection (BFD)

draft-ietf-idr-bgp-ls-sbfd-extensions-01, *BGP Link-State Extensions for Seamless BFD*

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*

RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD)*

RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

RFC 7880, *Seamless Bidirectional Forwarding Detection (S-BFD)*

RFC 7881, *Seamless Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6, and MPLS*

RFC 7883, *Advertising Seamless Bidirectional Forwarding Detection (S-BFD) Discriminators in IS-IS*

RFC 7884, *OSPF Extensions to Advertise Seamless Bidirectional Forwarding Detection (S-BFD) Target Discriminators*

Border Gateway Protocol (BGP)

draft-hares-idr-update-attrib-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-guidelines-08, *Best Practices for Advertisement of Multiple Paths in IBGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*

draft-ietf-idr-bgp-flowspec-oid-03, *Revised Validation Procedure for BGP Flow Specifications*

draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*

draft-ietf-idr-bgp-ls-app-specific-attr-01, *Application Specific Attributes Advertisement with BGP Link-State*

draft-ietf-idr-bgp-optimal-route-reflection-10, *BGP Optimal Route Reflection (BGP-ORR)*

draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*

draft-ietf-idr-flowspec-interfaceset-03, *Applying BGP flowspec rules on a specific interface set*

draft-ietf-idr-flowspec-path-redirect-05, *Flowspec Indirection-id Redirect* - localised ID

draft-ietf-idr-flowspec-redirect-ip-02, *BGP Flow-Spec Redirect to IP Action*

draft-ietf-idr-link-bandwidth-03, *BGP Link Bandwidth Extended Community*

draft-ietf-idr-long-lived-gr-00, *Support for Long-lived BGP Graceful Restart*

draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1997, *BGP Communities Attribute*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 2918, *Route Refresh Capability for BGP-4*

RFC 3107, *Carrying Label Information in BGP-4*

RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

RFC 4360, *BGP Extended Communities Attribute*

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*

RFC 4486, *Subcodes for BGP Cease Notification Message*

RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*

RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

RFC 4724, *Graceful Restart Mechanism for BGP* - helper mode

RFC 4760, *Multiprotocol Extensions for BGP-4*

RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*

RFC 5065, *Autonomous System Confederations for BGP*

RFC 5291, *Outbound Route Filtering Capability for BGP-4*

RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* - asplain

RFC 5492, *Capabilities Advertisement with BGP-4*

RFC 5549, *Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop*

RFC 5575, *Dissemination of Flow Specification Rules*

RFC 5668, *4-Octet AS Specific BGP Extended Community*

RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4*

RFC 6793, *BGP Support for Four-Octet Autonomous System (AS) Number Space*

RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*

RFC 6811, *Prefix Origin Validation*

RFC 6996, *Autonomous System (AS) Reservation for Private Use*

RFC 7311, *The Accumulated IGP Metric Attribute for BGP*

RFC 7607, *Codification of AS 0 Processing*

RFC 7674, *Clarification of the Flowspec Redirect Extended Community*

RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*

RFC 7854, *BGP Monitoring Protocol (BMP)*

RFC 7911, *Advertisement of Multiple Paths in BGP*

RFC 7999, *BLACKHOLE Community*

RFC 8092, *BGP Large Communities Attribute*

RFC 8212, *Default External BGP (EBGP) Route Propagation Behavior without Policies*

RFC 8571, *BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions*

Broadband Network Gateway (BNG) - Control and User Plane Separation (CUPS)

3GPP 23.007, *Restoration procedures*

3GPP 29.244, *Interface between the Control Plane and the User Plane nodes*

3GPP 29.281, *General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)*

BBF TR-459, *Control and User Plane Separation for a Disaggregated BNG*

RFC 8300, *Network Service Header (NSH)*

Circuit Emulation

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RFC 5086, *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

Ethernet

IEEE 802.1AB, *Station and Media Access Control Connectivity Discovery*

IEEE 802.1ad, *Provider Bridges*

IEEE 802.1ag, *Connectivity Fault Management*

IEEE 802.1ah, *Provider Backbone Bridges*

IEEE 802.1ak, *Multiple Registration Protocol*

IEEE 802.1aq, *Shortest Path Bridging*

IEEE 802.1ax, *Link Aggregation*

IEEE 802.1D, *MAC Bridges*

IEEE 802.1p, *Traffic Class Expediting*

IEEE 802.1Q, *Virtual LANs*

IEEE 802.1s, *Multiple Spanning Trees*

IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*

IEEE 802.1X, *Port Based Network Access Control*

IEEE 802.3ac, *VLAN Tag*

IEEE 802.3ad, *Link Aggregation*

IEEE 802.3ah, *Ethernet in the First Mile*

IEEE 802.3x, *Ethernet Flow Control*

ITU-T G.8031/Y.1342, *Ethernet Linear Protection Switching*

ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*

ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

Ethernet VPN (EVPN)

draft-ietf-bess-evpn-igmp-mld-proxy-05, *IGMP and MLD Proxy for EVPN*

draft-ietf-bess-evpn-irb-mcast-04, *EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding* - ingress replication

draft-ietf-bess-evpn-pref-df-06, *Preference-based EVPN DF Election*

draft-ietf-bess-evpn-prefix-advertisement-11, *IP Prefix Advertisement in EVPN*

draft-ietf-bess-evpn-proxy-arp-nd-08, *Operational Aspects of Proxy-ARP/ND in EVPN Networks*

draft-ietf-bess-evpn-virtual-eth-segment-06, *EVPN Virtual Ethernet Segment*

draft-ietf-bess-pbb-evpn-isid-cmacflush-00, *PBB-EVPN ISID-based CMAC-Flush*

RFC 7432, *BGP MPLS-Based Ethernet VPN*

RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*

RFC 8214, *Virtual Private Wire Service Support in Ethernet VPN*

RFC 8317, *Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) an Provider Backbone Bridging EVPN (PBB-EVPN)*

RFC 8365, *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*

RFC 8560, *Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents*

RFC 8584, *DF Election and AC-influenced DF Election*

Frame Relay

ANSI T1.617 Annex D, *DSS1 - Signalling Specification For Frame Relay Bearer Service*

FRF.1.2, *PVC User-to-Network Interface (UNI) Implementation Agreement*

FRF.12, *Frame Relay Fragmentation Implementation Agreement*

FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*

FRF.5, *Frame Relay/ATM PVC Network Interworking Implementation*

FRF2.2, *PVC Network-to-Network Interface (NNI) Implementation Agreement*

ITU-T Q.933 Annex A, *Additional procedures for Permanent Virtual Connection (PVC) status management*

Generalized Multiprotocol Label Switching (GMPLS)

draft-ietf-ccamp-rsvp-te-srlg-collect-04, *RSVP-TE Extensions for Collecting SRLG Information*

RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 4204, *Link Management Protocol (LMP)*

RFC 4208, *Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*

RFC 4872, *RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*

RFC 5063, *Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart* - helper mode

gRPC Remote Procedure Calls (gRPC)

cert.proto version 0.1.0, *gRPC Network Operations Interface (gNOI) Certificate Management Service*

file.proto version 0.1.0, *gRPC Network Operations Interface (gNOI) File Service*

gnmi.proto version 0.7.0, *gRPC Network Management Interface (gNMI) Service Specification*

PROTOCOL-HTTP2, *gRPC over HTTP2*

system.proto Version 1.0.0, *gRPC Network Operations Interface (gNOI) System Service*

Intermediate System to Intermediate System (IS-IS)

draft-ietf-isis-mi-02, *IS-IS Multi-Instance*

draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*

ISO/IEC 10589:2002 Second Edition, *Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 2973, *IS-IS Mesh Groups*

RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*

RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information*

RFC 5120, *M-ISIS: Multi Topology (MT) Routing in IS-IS*

RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*

RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*

RFC 5302, *Domain-wide Prefix Distribution with Two-Level IS-IS*

RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*

RFC 5304, *IS-IS Cryptographic Authentication*

RFC 5305, *IS-IS Extensions for Traffic Engineering TE*

RFC 5306, *Restart Signaling for IS-IS* - helper mode

RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 5308, *Routing IPv6 with IS-IS*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5310, *IS-IS Generic Cryptographic Authentication*

RFC 6119, *IPv6 Traffic Engineering in IS-IS*

RFC 6213, *IS-IS BFD-Enabled TLV*

RFC 6232, *Purge Originator Identification TLV for IS-IS*

RFC 6233, *IS-IS Registry Extension for Purges*

RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*

RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*

RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*

RFC 7987, *IS-IS Minimum Remaining Lifetime*

RFC 8202, *IS-IS Multi-Instance* - single topology

RFC 8570, *IS-IS Traffic Engineering (TE) Metric Extensions* - delay metric

RFC 8919, *IS-IS Application-Specific Link Attributes*

Internet Protocol (IP) — Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*

RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*

RFC 7431, *Multicast-Only Fast Reroute*

RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

Internet Protocol (IP) — General

draft-grant-tacacs-02, *The TACACS+ Protocol*

RFC 768, *User Datagram Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specifications*

RFC 1350, *The TFTP Protocol (revision 2)*

RFC 2347, *TFTP Option Extension*

RFC 2348, *TFTP Blocksize Option*

RFC 2349, *TFTP Timeout Interval and Transfer Size Options*

RFC 2428, *FTP Extensions for IPv6 and NATs*

RFC 2784, *Generic Routing Encapsulation (GRE)*

RFC 2818, *HTTP Over TLS*

RFC 2890, *Key and Sequence Number Extensions to GRE*

RFC 3164, *The BSD syslog Protocol*

RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

RFC 4251, *The Secure Shell (SSH) Protocol Architecture*

RFC 4252, *The Secure Shell (SSH) Authentication Protocol* - publickey, password

RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*

RFC 4254, *The Secure Shell (SSH) Connection Protocol*

RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*

RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms* - TLS

RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*

RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* - TLS client, RSA public key

RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer* - ECDSA

RFC 5925, *The TCP Authentication Option*

RFC 5926, *Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)*

RFC 6398, *IP Router Alert Considerations and Usage* - MLD

RFC 6528, *Defending against Sequence Number Attacks*

RFC 7011, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*

RFC 7012, *Information Model for IP Flow Information Export*

RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*

RFC 7232, *Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests*

RFC 7301, *Transport Layer Security (TLS) Application Layer Protocol Negotiation Extension*

Internet Protocol (IP) — Multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast* - version 1

draft-ietf-bier-pim-signaling-08, *PIM Signaling Through BIER Core*

draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*

draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3446, *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)* - auto-RP groups

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

RFC 4607, *Source-Specific Multicast for IP*

RFC 4608, *Source-Specific Protocol Independent Multicast in 232/8*

RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*

RFC 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*

RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*

RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*

RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

RFC 6037, *Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6513, *Multicast in MPLS/BGP IP VPNs*

RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/IP VPNs*

RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs*

RFC 6516, *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages*

RFC 6625, *Wildcards in Multicast VPN Auto-Discover Routes*

RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path*

RFC 7246, *Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context*

RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

RFC 7716, *Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures*

RFC 7761, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

RFC 8279, *Multicast Using Bit Index Explicit Replication (BIER)*

RFC 8296, *Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks* - MPLS encapsulation

RFC 8401, *Bit Index Explicit Replication (BIER) Support via IS-IS*

RFC 8444, *OSPFv2 Extensions for Bit Index Explicit Replication (BIER)*

RFC 8487, *Mtrace Version 2: Traceroute Facility for IP Multicast*

RFC 8534, *Explicit Tracking with Wildcard Routes in Multicast VPN* - (C-*,C-*) wildcard

RFC 8556, *Multicast VPN Using Bit Index Explicit Replication (BIER)*

Internet Protocol (IP) — Version 4

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

RFC 951, *Bootstrap Protocol (BOOTP)* - relay

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery* - router specification

RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*

RFC 1534, *Interoperation between DHCP and BOOTP*

RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

RFC 1812, *Requirements for IPv4 Routers*

RFC 1918, *Address Allocation for Private Internets*

RFC 2003, *IP Encapsulation within IP*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2401, *Security Architecture for Internet Protocol*

RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

RFC 3046, *DHCP Relay Agent Information Option (Option 82)*

RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*

RFC 4884, *Extended ICMP to Support Multi-Part Messages* - ICMPv4 and ICMPv6 Time Exceeded

Internet Protocol (IP) — Version 6

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*

RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*

RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3587, *IPv6 Global Unicast Address Format*

RFC 3596, *DNS Extensions to Support IP version 6*

RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*

RFC 3971, *SEcure Neighbor Discovery (SEND)*

RFC 3972, *Cryptographically Generated Addresses (CGA)*

RFC 4007, *IPv6 Scoped Address Architecture*

RFC 4193, *Unique Local IPv6 Unicast Addresses*

RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 4862, *IPv6 Stateless Address Autoconfiguration* - router functions

RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*

RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*

RFC 5007, *DHCPv6 Leasequery*

RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*

RFC 5722, *Handling of Overlapping IPv6 Fragments*

RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6* - IPv6

RFC 5952, *A Recommendation for IPv6 Address Text Representation*

RFC 6092, *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service* - Internet Control and Management, Upper-Layer Transport Protocols, UDP Filters, IPsec and Internet Key Exchange (IKE), TCP Filters

RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*

RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*

RFC 6437, *IPv6 Flow Label Specification*

RFC 8021, *Generation of IPv6 Atomic Fragments Considered Harmful*

RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 8201, *Path MTU Discovery for IP version 6*

Internet Protocol Security (IPsec)

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*

draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*

RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*

RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*

RFC 2406, *IP Encapsulating Security Payload (ESP)*

RFC 2407, *IPsec Domain of Interpretation for ISAKMP (IPsec DoI)*

RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*

RFC 2409, *The Internet Key Exchange (IKE)*

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*

RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*

RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*

RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*

RFC 3947, *Negotiation of NAT-Traversal in the IKE*

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec ESP*

RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*

RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4303, *IP Encapsulating Security Payload*

RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*

RFC 4308, *Cryptographic Suites for IPsec*

RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*

RFC 4543, *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*

RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*

RFC 4945, *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX*

RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol*

RFC 5903, *ECP Groups for IKE and IKEv2*

RFC 5998, *An Extension for EAP-Only Authentication in IKEv2*

RFC 6379, *Suite B Cryptographic Suites for IPsec*

RFC 6380, *Suite B Profile for Internet Protocol Security (IPsec)*

RFC 6712, *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*

RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

RFC 7427, *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*

RFC 7468, *Textual Encodings of PKIX, PKCS, and CMS Structures*

Label Distribution Protocol (LDP)

draft-pdutta-mpls-ldp-adj-capability-00, *LDP Adjacency Capabilities*

draft-pdutta-mpls-ldp-v2-00, *LDP Version 2*

draft-pdutta-mpls-mldp-up-redundancy-00, *Upstream LSR Redundancy for Multi-point LDP Tunnels*

draft-pdutta-mpls-multi-ldp-instance-00, *Multiple LDP Instances*

draft-pdutta-mpls-tldp-hello-reduce-04, *Targeted LDP Hello Reduction*

RFC 3037, *LDP Applicability*

RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol* - helper mode

RFC 5036, *LDP Specification*

RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*

RFC 5443, *LDP IGP Synchronization*

RFC 5561, *LDP Capabilities*

RFC 5919, *Signaling LDP Label Advertisement Completion*

RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6826, *Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 7032, *LDP Downstream-on-Demand in Seamless MPLS*

RFC 7473, *Controlling State Advertisements of Non-negotiated LDP Applications*

RFC 7552, *Updates to LDP for IPv6*

Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

draft-mammoliti-l2tp-accessline-avp-04, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*

RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

RFC 2809, *Implementation of L2TP Compulsory Tunneling via RADIUS*

RFC 3438, *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*

RFC 3931, *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

RFC 4719, *Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*

RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

Multiprotocol Label Switching (MPLS)

draft-ietf-mpls-lsp-ping-ospfv3-codepoint-02, *OSPFv3 CodePoint for MPLS LSP Ping*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services* - E-LSP

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*

RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*

RFC 5332, *MPLS Multicast Encapsulations*

RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*

RFC 6374, *Packet Loss and Delay Measurement for MPLS Networks* - Delay Measurement, Channel Type 0x000C

RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*

RFC 6425, *Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

RFC 7510, *Encapsulating MPLS in UDP*

RFC 7746, *Label Switched Path (LSP) Self-Ping*

RFC 7876, *UDP Return Path for Packet Loss and Delay Measurement for MPLS Networks* - Delay Measurement

RFC 8029, *Detecting Multiprotocol Label Switched (MPLS) Data-Plane Failures*

Multiprotocol Label Switching — Transport Profile (MPLS-TP)

RFC 5586, *MPLS Generic Associated Channel*

RFC 5921, *A Framework for MPLS in Transport Networks*

RFC 5960, *MPLS Transport Profile Data Plane Architecture*

RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*

RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*

RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*

RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*

RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*

RFC 6478, *Pseudowire Status for Static Pseudowires*

RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

Network Address Translation (NAT)

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6334, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite*

RFC 6887, *Port Control Protocol (PCP)*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7753, *Port Control Protocol (PCP) Extension for Port-Set Allocation*

RFC 7915, *IP/ICMP Translation Algorithm*

Network Configuration Protocol (NETCONF)

RFC 5277, *NETCONF Event Notifications*

RFC 6020, *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*

RFC 6022, *YANG Module for NETCONF Monitoring*

RFC 6241, *Network Configuration Protocol (NETCONF)*

RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*

RFC 6243, *With-defaults Capability for NETCONF*

RFC 8342, *Network Management Datastore Architecture (NMDA)* - Startup, Candidate, Running and Intended datastores

RFC 8525, *YANG Library*

RFC 8526, *NETCONF Extensions to Support the Network Management Datastore Architecture* - <get-data> operation

Open Shortest Path First (OSPF)

RFC 1586, *Guidelines for Running OSPF Over Frame Relay Networks*

RFC 1765, *OSPF Database Overflow*

RFC 2328, *OSPF Version 2*

RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*

RFC 3509, *Alternative Implementations of OSPF Area Border Routers*

RFC 3623, *Graceful OSPF Restart Graceful OSPF Restart* - helper mode

RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*

RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 4222, *Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance*

RFC 4552, *Authentication/Confidentiality for OSPFv3*

RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 5185, *OSPF Multi-Area Adjacency*

RFC 5187, *OSPFv3 Graceful Restart* - helper mode

RFC 5243, *OSPF Database Exchange Summary List Optimization*

RFC 5250, *The OSPF Opaque LSA Option*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5340, *OSPF for IPv6*

RFC 5642, *Dynamic Hostname Exchange Mechanism for OSPF*

RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*

RFC 5838, *Support of Address Families in OSPFv3*

RFC 6549, *OSPFv2 Multi-Instance Extensions*

RFC 6987, *OSPF Stub Router Advertisement*

RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*

RFC 7770, *Extensions to OSPF for Advertising Optional Router Capabilities*

RFC 8362, *OSPFv3 Link State Advertisement (LSA) Extensibility*

RFC 8920, *OSPF Application-Specific Link Attributes*

OpenFlow

TS-007 Version 1.3.1, *OpenFlow Switch Specification* - OpenFlow-hybrid switches

Path Computation Element Protocol (PCEP)

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*

draft-dhs-spring-pce-sr-p2mp-policy-00, *PCEP extensions for p2mp sr policy*

draft-ietf-pce-segment-routing-08, *PCEP Extensions for Segment Routing*

RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

RFC 8231, *Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE*

RFC 8281, *PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model*

Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*

RFC 1661, *The Point-to-Point Protocol (PPP)*

RFC 1662, *PPP in HDLC-like Framing*

RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*

RFC 1989, *PPP Link Quality Monitoring*

RFC 1990, *The PPP Multilink Protocol (MP)*

RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

RFC 2153, *PPP Vendor Extensions*

RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*

RFC 2615, *PPP over SONET/SDH*

RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

RFC 2878, *PPP Bridging Control Protocol (BCP)*

RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*

RFC 5072, *IP Version 6 over PPP*

Policy Management and Credit Control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points* - Gx support as it applies to wireline environment (BNG)

RFC 4006, *Diameter Credit-Control Application*

RFC 6733, *Diameter Base Protocol*

Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS Interworking*

MFA Forum 9.0.0, *The Use of Virtual trunks for ATM/MPLS Control Plane Interworking*

MFA Forum 12.0.0, *Multiservice Interworking - Ethernet over MPLS*

MFA Forum 13.0.0, *Fault Management for Multiservice Interworking v1.0*

MFA Forum 16.0.0, *Multiservice Interworking - IP over MPLS*

RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*

RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3)*

RFC 4385, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*

RFC 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*

RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*

RFC 4619, *Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*

RFC 4717, *Encapsulation Methods for Transport Asynchronous Transfer Mode (ATM) over MPLS Networks*

RFC 4816, *Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service*

RFC 5085, *Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*

RFC 5659, *An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*

RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*

RFC 6073, *Segmented Pseudowire*

RFC 6310, *Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*

RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*

RFC 6718, *Pseudowire Redundancy*

RFC 6829, *Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6*

RFC 6870, *Pseudowire Preferential Forwarding Status bit*

RFC 7023, *MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking*

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

RFC 7392, *Explicit Path Routing for Dynamic Multi-Segment Pseudowires* - ER-TLV and ER-HOP IPv4 Prefix

Quality of Service (QoS)

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2597, *Assured Forwarding PHB Group*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*

Remote Authentication Dial In User Service (RADIUS)

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*

Resource Reservation Protocol — Traffic Engineering (RSVP-TE)

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* - IF_ID RSVP_HOP object with unnumbered interfaces and RSVP-TE graceful restart helper procedures

RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*

RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*

RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

Routing Information Protocol (RIP)

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

Segment Routing (SR)

draft-bashandy-rtgwg-segment-routing-uloop-06, *Loop avoidance using Segment Routing*

draft-filsfils-spring-srv6-net-pgm-insertion-04, *SRv6 NET-PGM extension: Insertion*

draft-ietf-6man-spring-srv6-oam-10, *Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)*

draft-ietf-bess-srv6-services-07, *SRv6 BGP based Overlay Services*

draft-ietf-idr-bgp-ls-segment-routing-ext-16, *BGP Link-State extensions for Segment Routing*

draft-ietf-idr-bgp-ls-segment-routing-msd-09, *Signaling MSD (Maximum SID Depth) using Border Gateway Protocol Link-State*

draft-ietf-idr-segment-routing-te-policy-09, *Advertising Segment Routing Policies in BGP*

draft-ietf-isis-mpls-elc-10, *Signaling Entropy Label Capability and Entropy Readable Label Depth Using IS-IS* - advertising ELC

draft-ietf-lsr-flex-algo-08, *IGP Flexible Algorithm*

draft-ietf-lsr-isis-srv6-extensions-14, *IS-IS Extension to Support Segment Routing over IPv6 Dataplane*

draft-ietf-ospf-mpls-elc-12, *Signaling Entropy Label Capability and Entropy Readable Label-stack Depth Using OSPF* - advertising ELC

draft-ietf-rtgwg-segment-routing-ti-lfa-01, *Topology Independent Fast Reroute using Segment Routing*

draft-ietf-spring-conflict-resolution-05, *Segment Routing MPLS Conflict Resolution*

draft-ietf-spring-segment-routing-policy-08, *Segment Routing Policy Architecture*

draft-ietf-teas-sr-rsvp-coexistence-rec-02, *Recommendations for RSVP-TE and Segment Routing LSP co-existence*

draft-voyer-6man-extension-header-insertion-10, *Deployments With Insertion of IPv6 Segment Routing Headers*

draft-voyer-pim-sr-p2mp-policy-02, *Segment Routing Point-to-Multipoint Policy*

draft-voyer-spring-sr-p2mp-policy-03, *SR Replication Policy for P2MP Service Delivery*

RFC 8287, *Label Switched Path (LSP) Ping/Traceroute for Segment Routing (SR) IGP-Prefix and IGP-Adjacency Segment Identifiers (SIDs) with MPLS Data Planes*

RFC 8476, *Signaling Maximum SID Depth (MSD) Using OSPF* - node MSD

RFC 8491, *Signaling Maximum SID Depth (MSD) Using IS-IS* - node MSD

RFC 8660, *Segment Routing with the MPLS Data Plane*

RFC 8661, *Segment Routing MPLS Interworking with LDP*

RFC 8663, *MPLS Segment Routing over IP* - BGP SR with SR-MPLS-over-UDP/IP

RFC 8665, *OSPF Extensions for Segment Routing*

RFC 8666, *OSPFv3 Extensions for Segment Routing*

RFC 8667, *IS-IS Extensions for Segment Routing*

RFC 8669, *Segment Routing Prefix Segment Identifier Extensions for BGP*

RFC 8754, *IPv6 Segment Routing Header (SRH)*

RFC 8986, *Segment Routing over IPv6 (SRv6) Network Programming*

Simple Network Management Protocol (SNMP)

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1215, *A Convention for Defining Traps for use with the SNMP*

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

RFC 3413, *Simple Network Management Protocol (SNMP) Applications*

RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)* - SNMP over UDP over IPv4

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

Simple Network Management Protocol (SNMP) - Management Information Base (MIB)

draft-ietf-snmpv3-update-mib-05, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*

draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*

draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*

draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*

draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*

draft-ietf-vrrp-unified-mib-06, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6* - IPv6

ianaaddressfamilynumbers-mib, *IANA-ADDRESS-FAMILY-NUMBERS-MIB*

ianagmplstc-mib, *IANA-GMPLS-TC-MIB*

ianaiftype-mib, *IANAifType-MIB*

ianaiprouteprotocol-mib, *IANA-RTPROTO-MIB*

IEEE8021-CFM-MIB, *IEEE P802.1ag(TM) CFM MIB*

IEEE8021-PAE-MIB, *IEEE 802.1X MIB*

IEEE8023-LAG-MIB, *IEEE 802.3ad MIB*

LLDP-MIB, *IEEE P802.1AB(TM) LLDP MIB*

RFC 1212, *Concise MIB Definitions*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1724, *RIP Version 2 MIB Extension*

RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

RFC 2206, *RSVP Management Information Base using SMIv2*

RFC 2213, *Integrated Services Management Information Base using SMIv2*

RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*

RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*

RFC 2515, *Definitions of Managed Objects for ATM Management*

RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

RFC 2579, *Textual Conventions for SMIv2*

RFC 2580, *Conformance Statements for SMIv2*

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*

RFC 4220, *Traffic Engineering Link Management Information Base*

RFC 4273, *Definitions of Managed Objects for BGP-4*

RFC 4292, *IP Forwarding Table MIB*

RFC 4293, *Management Information Base for the Internet Protocol (IP)*

RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*

RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*

RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*

SFLOW-MIB Version 1.3 (Draft 5), *sFlow MIB*

Timing

GR-1244-CORE Issue 3, *Clocks for the Synchronized Network: Common Generic Criteria*

GR-253-CORE Issue 3, *SONET Transport Systems: Common Generic Criteria*

IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC)*

ITU-T G.8261, *Timing and synchronization aspects in packet networks*

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC)*

ITU-T G.8264, *Distribution of timing information through packet networks*

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization*

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network*

RFC 3339, *Date and Time on the Internet: Timestamps*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

Two-Way Active Measurement Protocol (TWAMP)

RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)* - server, unauthenticated mode

RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*

RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*

RFC 8545, *Well-Known Port Assignments for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP)* - TWAMP

RFC 8762, *Simple Two-Way Active Measurement Protocol* - unauthenticated

Virtual Private LAN Service (VPLS)

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

RFC 5501, *Requirements for Multicast Support in Virtual Private LAN Services*

RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

RFC 7041, *Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging*

RFC 7117, *Multicast in Virtual Private LAN Service (VPLS)*

Voice and Video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

ITU-T G.1020 Appendix I, *Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks - Mean Absolute Packet Delay Variation & Markov Models*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550, *RTP: A Transport Protocol for Real-Time Applications* - Appendix A.8

RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

Wireless Local Area Network (WLAN) Gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses* - S2a roaming based on GPRS

Yet Another Next Generation (YANG)

RFC 6991, *Common YANG Data Types*

RFC 7950, *The YANG 1.1 Data Modeling Language*

RFC 7951, *JSON Encoding of Data Modeled with YANG*

Yet Another Next Generation (YANG) - OpenConfig Modules

openconfig-aaa.yang version 0.4.0, *OpenConfig AAA Module*

openconfig-aaa-radius.yang version 0.3.0, *OpenConfig AAA RADIUS Module*

openconfig-aaa-tacacs.yang version 0.3.0, *OpenConfig AAA TACACS+ Module*

openconfig-acl.yang version 1.0.0, *OpenConfig ACL Module*

openconfig-bfd.yang version 0.1.0, *OpenConfig BFD Module*

openconfig-bgp.yang version 3.0.1, *OpenConfig BGP Module*

openconfig-bgp-common.yang version 3.0.1, *OpenConfig BGP Common Module*

openconfig-bgp-common-multiprotocol.yang version 3.0.1, *OpenConfig BGP Common Multiprotocol Module*

openconfig-bgp-common-structure.yang version 3.0.1, *OpenConfig BGP Common Structure Module*

openconfig-bgp-global.yang version 3.0.1, *OpenConfig BGP Global Module*

openconfig-bgp-neighbor.yang version 3.0.1, *OpenConfig BGP Neighbor Module*

openconfig-bgp-peer-group.yang version 3.0.1, *OpenConfig BGP Peer Group Module*

openconfig-bgp-policy.yang version 4.0.1, *OpenConfig BGP Policy Module*

openconfig-if-aggregate.yang version 2.0.0, *OpenConfig Interfaces Aggregated Module*

openconfig-if-ethernet.yang version 2.0.0, *OpenConfig Interfaces Ethernet Module*

openconfig-if-ip.yang version 2.0.0, *OpenConfig Interfaces IP Module*

openconfig-if-ip-ext.yang version 2.0.0, *OpenConfig Interfaces IP Extensions Module*

openconfig-interfaces.yang version 2.0.0, *OpenConfig Interfaces Module*

openconfig-isis.yang version 0.3.0, *OpenConfig IS-IS Module*

openconfig-isis-policy.yang version 0.3.0, *OpenConfig IS-IS Policy Module*

openconfig-isis-routing.yang version 0.3.0, *OpenConfig IS-IS Routing Module*

openconfig-lacp.yang version 1.1.0, *OpenConfig LACP Module*

openconfig-lldp.yang version 0.1.0, *OpenConfig LLDP Module*

openconfig-local-routing.yang version 1.0.1, *OpenConfig Local Routing Module*

openconfig-mpls.yang version 2.3.0, *OpenConfig MPLS Module*

openconfig-mpls-ldp.yang version 3.0.2, *OpenConfig MPLS LDP Module*

openconfig-mpls-rsvp.yang version 2.3.0, *OpenConfig MPLS RSVP Module*

openconfig-mpls-te.yang version 2.3.0, *OpenConfig MPLS TE Module*

openconfig-network-instance.yang version 0.8.0, *OpenConfig Network Instance Module*

openconfig-packet-match.yang version 1.0.0, *OpenConfig Packet Match Module*

openconfig-platform.yang version 0.12.2, *OpenConfig Platform Module*

openconfig-platform-fan.yang version 0.1.1, *OpenConfig Platform Fan Module*

openconfig-platform-linecard.yang version 0.1.2, *OpenConfig Platform Linecard Module*

openconfig-relay-agent.yang version 0.1.0, *OpenConfig Relay Agent Module*

openconfig-routing-policy.yang version 3.0.0, *OpenConfig Routing Policy Module*

openconfig-rsvp-sr-ext.yang version 0.1.0, *OpenConfig RSVP-TE and SR Extensions Module*

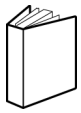
openconfig-system-logging.yang version 0.3.1, *OpenConfig System Logging Module*

openconfig-system-terminal.yang version 0.3.0, *OpenConfig System Terminal Module*

openconfig-telemetry.yang version 0.5.0, *OpenConfig Telemetry Module*

openconfig-vlan.yang version 2.0.0, *OpenConfig VLAN Module*

Customer Document and Product Support



Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback

3HE 17141 AAAB TQZZA 01