

## Configuring System Management with CLI

This section provides information about configuring system management features with CLI.

Topics in this chapter include:

- [Basic System Configuration on page 286](#)
- [Common Configuration Tasks on page 287](#)
- [System Information on page 288](#)
  - [System Information Parameters](#)
    - [Name on page 289](#)
    - [Contact on page 289](#)
    - [Location on page 290](#)
    - [CLLI Code on page 290](#)
    - [Coordinates on page 291](#)
  - [System Time Elements on page 292](#)
    - [Zone on page 292](#)
    - [Summer Time Conditions on page 294](#)
    - [NTP on page 295](#)
    - [SNTP on page 301](#)
    - [CRON on page 303](#)
  - [Configuring Synchronization and Redundancy on page 313](#)
    - [Configuring Synchronization on page 313](#)
    - [Configuring Manual Synchronization on page 314](#)
    - [Forcing a Switchover on page 314](#)
    - [Configuring Synchronization Options on page 315](#)
    - [Configuring Multi-Chassis Redundancy on page 315](#)
- [Configuring Mixed Mode on page 318](#)
- [Configuring Power Supply Parameters on page 320](#)
- [Post-Boot Configuration Extension Files on page 323](#)
- [System Timing on page 326](#)
  - [Edit Mode on page 327](#)
  - [Configuring Timing References on page 328](#)
  - [Using the Revert Command on page 329](#)
  - [Other Editing Commands on page 330](#)
  - [Forcing a Specific Reference on page 331](#)

- [Configuring System Monitoring Thresholds on page 332](#)
- [Configuring LLDP on page 335](#)

# System Management

---

## 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, refer to the *Boot Option Files* section of this manual.

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/or 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, etc. 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.

## 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 on page 289](#)
- [System Time Elements on page 292](#)

---

The following example displays 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#
```

## 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.

- [System Information on page 288](#)
  - [Name on page 289](#)
  - [Contact on page 289](#)
  - [Location on page 290](#)
  - [CLLI Code on page 290](#)
  - [Coordinates on page 291](#)
- [System Time Elements on page 292](#)
  - [Zone on page 292](#)
  - [Summer Time Conditions on page 294](#)
  - [NTP on page 295](#)
  - [SNTP on page 301](#)
  - [CRON on page 303](#)
    - [Schedule on page 303](#)
    - [Time Range on page 303](#)
    - [Time of Day on page 307](#)
- [Synchronization and Redundancy on page 259](#)
  - [Automatic Synchronization on page 307](#)
  - [Manual Synchronization on page 309](#)
- [System Timing on page 326](#)
  - [Configuring Timing References on page 328](#)

## System Information

This section covers the basic system information parameters to configure the physical location of the SR-Series, contact information, location information such as the place the router is located such as an address, floor, room number, etc., global positioning system (GPS) coordinates, and system name.

Use the CLI syntax displayed below to configure the following system components:

- [System Information Parameters on page 289](#)
- [System Time Elements on page 292](#)

General system parameters include:

- [Name on page 289](#)
- [Contact on page 289](#)
- [Location on page 290](#)
- [CLLI Code on page 290](#)
- [Coordinates on page 291](#)

## 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:** `alcatel>config>system# name ALA-12`

The following example displays 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, etc., 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 a 7750 SR 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`



## Coordinates

Use the optional **coordinates** command to specify the GPS location of the device. If the string contains special characters (#, \$, spaces, etc.), 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 displays 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#
```

## 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 display time according to the local time zone.

Time elements include:

- [Zone on page 292](#)
- [Summer Time Conditions on page 294](#)
- [NTP on page 295](#)
- [SNTP on page 301](#)
- [CRON on page 303](#)
  - [Time Range on page 303](#)
  - [Time of Day on page 307](#)

---

## 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 25](#).

**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 displays 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 25: System-defined Time Zones**

<b>Acronym</b>	<b>Time Zone Name</b>	<b>UTC Offset</b>
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
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 Conditions

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 25](#), 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 25](#) or entered as optional parameters in this command.

The following example displays 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.

NTP time elements include:

- [Authentication-check on page 295](#)
- [Authentication-key on page 296](#)
- [Broadcast on page 296](#)
- [Broadcastclient on page 297](#)
- [Multicast on page 297](#)
- [Multicastclient on page 298](#)
- [NTP-Server on page 298](#)
- [Peer on page 299](#)
- [Server on page 300](#)

---

### 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] 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. 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. 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.

SNTP time elements include:

- [Broadcast-client on page 301](#)
- [Server-address on page 302](#)

---

**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, time range, and time of day 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#
```

---

### Time Range

Filter (ACL) policy configurations may be enhanced to support time-based matching by referring to a time-range policy.

Time range elements include:

- [Create on page 304](#)
- [Absolute on page 304](#)
- [Daily on page 304](#)
- [Weekdays on page 305](#)

- [Weekend on page 305](#)
  - [Weekly on page 306](#)
- 

### Create

Use the **create** command to enable the time-range context.

The following example creates a time-range called test1.

**Example:** `config>system>cron# time-range test1 create`

---

### Absolute

The **absolute** command configures a start and end time that will not repeat.

**Example:** `config>system>cron>time-range$ absolute start 2006/05/05,11:00  
end 2006/05/06,11:01`

The following example shows an absolute time range beginning on May 5, 2006 at 11:00 and ending May 6, 2006 at 11:01:

```
A:sim1>config>system>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name       : test1
Triggers   : 0
Status     : Inactive
Absolute   : start 2006/05/05,11:00 end 2006/05/06,11:01
=====
A:sim1>config>system>cron>time-range#
```

---

### Daily

The **daily** command configures the start and end of a periodic schedule for every day of the week (Sunday through Saturday).

**Example:** `config>system>cron>time-range$ daily start 11:00 end 12:00`

The following example shows a daily time range beginning at 11:00 and ending at 12:00.

```
A:sim1>config>system>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name       : 1
Triggers   : 0
Status     : Inactive
Periodic   : daily   Start 11:00 End 12:00
=====
A:sim1>config>system>cron>time-range#
```

---

## Weekdays

The **weekdays** command configures the start and end of a periodic schedule for weekdays (Monday through Friday).

**Example:** `config>system>cron>time-range$ weekdays start 11:00 end 12:00`

The following command shows a time range beginning at 11:00 and ending at 12:00. This schedule runs all weekdays during this time period.

```
A:sim1>config>system>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
Name       : 1
Triggers   : 0
Status     : Inactive
Periodic   : weekdays Start 11:00 End 12:00
=====
A:sim1>config>system>cron>time-range#
```

---

## Weekend

The **weekend** command configures the start and end of a periodic schedule for weekends (Saturday and Sunday). The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. A start time and end time of 11:00 is invalid.

**Example:** `config>system>cron>time-range$ weekend start 11:00 end 12:00`

The following command shows a weekend time range beginning at 11:00am and ending at 12:00pm, both Saturday and Sunday.

To specify 11:00am to 12:00pm on Saturday or Sunday only, use the [Absolute](#) parameter for one day, or the [Weekly](#) parameter for every Saturday or Sunday accordingly. In addition, see the [Schedule](#) parameter to schedule oneshot or periodic events in the `config>cron>` context.

```
A:sim1>config>system>cron>time-range# show cron time-range detail
=====
Cron time-range details
=====
```

## System Information

```
Name       : 1
Triggers   : 0
Status     : Inactive
Periodic   : weekend Start 11:00 End 12:00
```

---

## Weekly

The **weekly** command configures the start and end of a periodic schedule for the same day every week, for example, every Friday. The start and end dates must be the same. The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. A start time and end time of 11:00 is invalid.

**Example:** `config>system>cron>time-range$ start fri,01:01 end fri,01:02`

The following command shows a weekly time range beginning on Friday at 1:01am ending Friday at 1:02am.

```
A:sim1>config>system>cron>time-range$ info
-----
        weekly start fri,01:01 end fri,01:02
-----
A:sim1>config>system>cron>time-range$
```

---



## Time of Day

Time of Day (TOD) suites are useful when configuring many types of time-based policies or when a large number of subscribers or SAPs require the same type of TOD changes. The TOD suite may be configured while using specific ingress or egress ACLs or QoS policies, and is an enhancement of the ingress and egress CLI trees.

---

## SAPs

- If a TOD Suite is assigned to a SAP, statistics collection are not collected for that SAP and scheduler overrides cannot be collected on the SAP. If the SAP has an egress aggregate rate limit configured, an egress scheduler policy assignment cannot be applied
  - When an item is configured both on SAP level and in the TOD suite assigned to the SAP, the TOD-suite defined value takes precedence. If a SAP belongs to an IES Interface, TOD Suites are allowed only with generic interfaces (no subscriber, group, redundant, etc.).
  - A policy or filter assignment configured directly on a SAP has a lower priority than any assignment in a TOD Suite. Hence, it is possible that a new direct configuration has no immediate effect. If the configuration is made by CLI, a warning is given.
- 

## Multiservice Site

When applying a TOD Suite to a multi-service-site, only the scheduler policy assignment is active. If the multi-service-site has an egress aggregate rate limit configured, any egress scheduler policy assignment cannot be applied. While a TOD Suite is assigned to a multi-service-site, it is not possible to configure a scheduler to override it.

## ANCP (Access Node Control Protocol)

Static ANCP string mapping and TOD suites must be configured on separate SAPs or multiservice sites.

Time of day elements include:

- [Egress on page 308](#)
  - [Ingress on page 310](#)
- 

## Egress

The **egress** command is an enhancement for specific egress policies including filter lists, schedulers and QoS. Use this command to create time-range based associations of previously created filter lists, QoS and scheduler policies. Multiple policies may be included and each must be assigned a different priority; in case time-ranges overlap, the priority will be used to determine the prevailing policy. Only a single reference to a policy may be included without a time-range.

---

## Egress Aggregate Rate Limit

Having an egress aggregate rate limit is incompatible with having a scheduler policy. If a SAP or multi-service-site has a configured egress aggregate rate limit, and the TOD suite assigns a scheduler policy to it, that assignment cannot be applied: the configured aggregate rate limit takes precedence over the TOD suite's scheduler policy assignment.

---

## Egress Multicast Group

SAPs may not have a TOD suite while belonging to an egress multicast group (EMG). Since all SAPs that belong to the same EMG must have the same egress filter, it is imperative to ensure that the TOD Suite does not modify the egress filter assignment.

## Filters

In a TOD suite, filters that have entries with time-ranges may not be selected. Similarly, filter entries with a time-range may not be created while a TOD suite refers to that filter. QoS policies and filters referred to by a TOD suite must have scope “template” (default).

The following syntax is used to configure TOD-suite egress parameters.

**Example:** `config>system>cron>tod-suite$ egress filter ip 100`

The following command shows an egress IP filter association with filter ID 100.

```
sim1>config>filter# ip-filter 100 create
A:sim1>config>filter>ip-filter$ entry 10 create
A:sim1>config>filter>ip-filter>entry$
A:sim1>config>system>cron>tod-suite# egress filter ip 100
A:sim1>config>system>cron>tod-suite# info detail
-----
      no description
      egress
          filter ip 100
      exit
-----
A:sim1>config>cron>tod-suite#
```

**Example:** `config>system>cron>tod-suite$ egress qos 101`

The following command shows an association with egress QoS-SAP policy 101.

```
A:sim1>config>qos# sap-egress 101 create
...
A:sim1>config>system>cron>tod-suite# egress qos 101
A:sim1>config>system>cron>tod-suite# info detail
-----
      no description
      egress
          qos 101
      exit
-----
A:sim1>config>system>cron>tod-suite#
```

**Example:** `config>system>cron>tod-suite$ egress scheduler-policy test1`

The following command shows an association with an egress scheduler-policy called test1.

```
A:sim1>config# qos scheduler-policy test1 create
A:sim1>config>qos>scheduler-policy#
...
A:sim1# configure system cron tod-suite test1 create
A:sim1>config>system>cron>tod-suite# egress scheduler-policy test1
A:sim1>config>system>cron>tod-suite# info detail
-----
      no description
      egress
          scheduler-policy test1
-----
```

```

                                exit
-----
A:sim1>config>system>cron>tod-suite$

```

## Ingress

This command is an enhancement for specific ingress policies including filter lists, schedulers and QoS policies. Use this command to create time-range based associations of previously created filter lists QoS and scheduler policies. Multiple policies may be included and each must be assigned a different priority; in case time-ranges overlap, the priority will be used to determine the prevailing policy. Only a single reference to a policy may be included without a time-range. To configure a daily time-range across midnight, use a combination of two entries. An entry that starts at hour zero will take over from an entry that ends at hour 24.

**Example:** `config>system>cron>tod-suite$ ingress filter ip 100`  
`config>system>cron>tod-suite$`

The following command shows an ingress IP filter association with filter ID 100.

```

sim1>config>filter# ip-filter 100 create
A:sim1>config>filter>ip-filter$ entry 10 create
A:sim1>config>filter>ip-filter>entry$
...
A:sim1>config>system>cron>tod-suite# ingress filter ip 100
A:sim1>config>system>cron>tod-suite# info detail
-----
no description
ingress
    filter ip 100
exit
-----
A:sim1>config>system>cron>tod-suite#

```

**Example:** `config>system>cron>tod-suite$ ingress qos 101`  
`config>system>cron>tod-suite$`

The following command shows an association with ingress QoS-SAP policy 101.

```

A:sim1>config>qos# sap-egress 101 create
...
A:sim1>config>system>cron>tod-suite# ingress qos 101
A:sim1>config>system>cron>tod-suite# info detail
-----
no description
ingress
    qos 101
exit
-----
A:sim1>config>system>cron>tod-suite#

```

**Example:** config>system>cron>tod-suite\$ ingress scheduler-policy test1  
config>system>cron>tod-suite\$

The following command shows an association with an ingress scheduler-policy named test1.

```
A:sim1>config# qos scheduler-policy test1 create
A:sim1>config>qos>scheduler-policy#
...
A:sim1# configure cron tod-suite test1 create
A:sim1>config>system>cron>tod-suite#ingress scheduler-policy test1
A:sim1>config>system>cron>tod-suite# info detail
-----
          no description
          ingress
             scheduler-policy test1
          exit
-----
A:sim1>config>system>cron>tod-suite#
```

## **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.

## Configuring Synchronization and Redundancy

- [Configuring Persistence on page 313](#)
  - [Configuring Synchronization on page 313](#)
  - [Configuring Manual Synchronization on page 314](#)
  - [Forcing a Switchover on page 314](#)
  - [Configuring Synchronization Options on page 315](#)
  - [Configuring Multi-Chassis Redundancy on page 315](#)
- 

### Configuring Persistence

The following example displays subscriber management system persistence command usage:

**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#
```

---

### 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}
```

**CLI Syntax:**

```
config>system
  switchover-exec file-url
```

## 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 which displays during a manual synchronization:

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

---

## 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.



## 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 displays 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 displays 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#
```

## Configuring Multi-Chassis Redundancy

## Configuring Multi-Chassis Redundancy

Note: When configuring associated LAG ID parameters, the LAG must be in access mode and LACP must be enabled.

Use the CLI syntax displayed below to configure multi-chassis redundancy features.

```
CLI Syntax: admin>redundancy
                multi-chassis
                  peer ip-address
                    authentication-key [authentication-key | hash-key]
                    [hash | hash2]
                    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
                  port [port-id | lag-id] [sync-tag]
                    range encap-range sync-tag
                  no shutdown
                  srrp
                  sub-mgmt
```

```
Example: admin>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 displays 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#
```

## Configuring Mixed Mode

The 7450 mixed mode feature allows a 7450 ESS-7 or ESS-12 chassis to utilize 7750 IOM3-XPs, MDAs, and IMMs to enable 7750 SR capabilities on the associated slots. This allows features such as multicast routing, VPRN and IPv6 support as well as others to be enabled on existing 7450 systems.

The following are mixed-mode requirements:

- SR capabilities (for example, IP-VPNs, IPv6 routing and multicast routing) can only be associated with interfaces on 7750 IOM3-XPs, MDAs, and IMMs
- Network interface ports must be located 7750 IOM3-XPs or IMMs
- Only 7750 IOM3-XPs, 7750 MDAs, or 7750 IMMs can be used in 7450 slots with SR capabilities enabled.

Notes:

- The 7x50 SR supports mixed mode, specifically to run IPv6 services in a router that also contains IOM-20G-Bs (chassis mode A).
- ESM for IPv6 must run on IOM-3 or IMM hardware only, not on IOM or IOM-2, because the IOM and IOM2 data planes are not capable of routing incoming traffic to the IPv6 ESM hosts.
- The scaling limits are still defined by the chassis mode. That means only 16k IPv6 ESM subscribers (limited by the ARP scale of chassis mode A).

---

## Enabling Mixed Mode on a 7450 System

To configure mixed mode support, 7750 IOM3-XPs, 7750 MDAs, or 7750 IMMs must be installed in a 7450 ESS-7 or ESS-12 router that is running OS 8.0 or later. All network interfaces must be migrated to ports on the 7750 cards.

The mixed mode state is then enabled by using the **mixed-mode-upgrade** command:

**CLI Syntax:** `mixed-mode-upgrade slot-list`

This tool will take a list of slots that should have 7750 cards installed. The command then checks to ensure that all network interfaces are located on ports on these slots and that they are all 7750 cards. It then enables the **mixed-mode** state at the system level and changes the **capability** setting for the specified slots to **sr**.

At this point the 7450 system is operating in a mixed mode state and supported features and services can now be configured on the slots with SR capabilities enabled.

Once in mixed mode use the **capability** command to configure slots for SR capabilities:

**CLI Syntax:** `config>card>capability sr|ess`

Slots using 7750-capable cards will have to have SR capability enabled on all slots with 7750 IOM3s and IMMs, as well as **mixed-mode** at the system level.

See [Table 26](#) for a description of mixed-mode support.

**Table 26: Mixed-Mode Support**

Feature	7450 Standard Mode	7450 Mixed Mode (Limited to 7750 IOM3/IMM)
Full IES Support	Limited IES support	Yes
Full VPRN Support	No	Yes
BGP for routing (all address families)	No	Yes
IPv6 routing: IPv6 routing (Unicast and Multicast) 6PE 6VPE (IPv6 VPRN)	No	Yes
IP Multicast routing and forwarding Protocols: PIM, MSDP and IGMP mVPN P2MP LSP support	No	Yes
Spoke termination on L3 (IES/VPRN) interfaces	No	Yes
TPSDA IPv4 & v6 Routed subscriber management support PPPoE support SRRP Routed subscriber management for wholesale	No	Yes
IP Mirroring	No	Yes

## Configuring Power Supply Parameters

By default, 7750 SR-SeriesA: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  
..  
-----
```

## Configuring ATM System Parameters

The ATM context configures system-wide ATM parameters.

**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
03:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
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 03:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
      oam
        retry-up 3
        retry-down 5
        loopback-period 30
      exit
-----
A:ALA-12>config>system>atm#
```

## 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/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#
```



## 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 boot-up 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 displays 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#
```

## Show Command Output and Console Messages

The `show>system>information` command displays 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.

```
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            : cfl:
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 B-0.0.I323 - Copyright (c) 2000-2004 Alcatel.
                        # All rights reserved. All use subject to applicable l
                        # license agreements. # Built on Sun Feb 29 21:43:13 PST
                        # 2004 by builder in /rel0.0/I323/panos/main # Generated
                        THU MAR 04 22:39:03 2004 UTC

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
  172.22.184.0/22     192.168.1.251
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 boot-up 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-B-x.0.Rx both/hops ALCATEL SR 7750 Copyright (c) 2000-2009 Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Thu Nov 20 19:19:11 PST 2008 by builder in /rel5x.0/b1/Rx/panos/main
```

Login:

## System Timing

When synchronous Ethernet is enabled, the operator can select an Ethernet port as a candidate for timing reference. The timing information recovered from this port is used by the central clock.

Note: In the current release the derived timing is distributed only through other Ethernet ports.

CLI Syntax:

```
config>system>sync-if-timing
  abort
  begin
  commit
  ref-order ref1 ref2
  ref1
    source-port port-id
    no shutdown
  ref2
    source-port port-id
    no shutdown
  no revert
```

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.

Use the CLI syntax displayed below to:

- [Edit Mode on page 327](#)
- [Configuring Timing References on page 328](#)
- [Using the Revert Command on page 329](#)
- [Other Editing Commands on page 330](#)
- [Forcing a Specific Reference on page 331](#)

## 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 displays 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#
```

## Configuring Timing References

Use the following CLI syntax to configure timing reference parameters. Note that the source port specified for **ref1** and **ref2** is dependent on the 7750 SR-Series model type and chassis slot.

**Note:** For the SR-c12 and SR-c4, the ref1 and ref2 cannot both be from the same slot.

7750 Model	Ref1/Slots	Ref2/Slots
SR-7	1 — 2	3 — 5
SR-12	1 — 5	6 — 10
SR-12e	1 — 5	6 — 9
SR-c12	No restriction	No restriction
SR-c4	No restriction	No restriction

Note that the SR-c12 and SR-c4, ref1 and ref2 cannot be from the same slot.

The following displays a timing reference configuration example:

```
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 dsl esf
  no shutdown
exit
-----
ALA-12>config>system>sync-if-timing#
```

## 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 revert is 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`

## 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`



## Forcing a Specific Reference

Note: 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}`

**Example:** `debug>sync-if-timing# force-reference`

The 7750 SR-c4 has two BITS input ports on the CFM. The force reference command on this system allows the selection of the specific port.

**CLI Syntax:** `debug>sync-if-timing  
force-reference {ref1 | ref2 | bits1 | bits2}`

# Configuring System Monitoring Thresholds

---

## 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:

**Example:** `config>system>thresholds# cflash-cap-warn cfl-B: rising-threshold 2000000 falling-threshold 1999900 interval 240 trap startup-alarm either`

**Example:** config>system>thresholds# memory-use-alarm rising-threshold 50000000 falling-threshold 45999999 interval 500 both startup-alarm either

**Example:** config>system>thresh# rmon

**Example:** config>system>thresh>rmon# event 5 both description "alarm testing" owner "Timos CLI"

The following example displays 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#
```

## System Alarm Contact Inputs

The hardware supports alarm contact inputs that allow an operator to monitor and report changes in the external environmental conditions. In a remote or outdoor deployment, alarm contact inputs allow an operator to detect conditions, for example, air conditioner fault, open door.

An operator can configure generation of events when alarm contact inputs transition between the open and close states. For each generated event, the operator can specify the:

- Action associated with each state transition.
- Severity associated with each state transition.
- Log message associated with each state transition.

## Configuring LLDP

The following output displays LLDP defaults:

```
A:testSrl>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:testSrl>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#
```

