System Command Reference

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context
config>cron>action
config>cron>sched
config>cron>script
config>system>time>ntp
config>system>time>sntp
config>system>sync-if-timing>ref1
config>system>sync-if-timing>ref2
config>system>sync-if-timing>ptp
config>system>sync-if-timing>bits>input
config>system>sync-if-timing>bits>output
config>system>persistence>app-assure
config>system>persistence>dhcp-server
config>system>persistence>nat-port-forward
config>system>persistence>subscriber-mgmt
config>redundancy>multi-chassis>peer
config>redundancy>multi-chassis>peer>mc-lag
config>redundancy>multi-chassis>peer>sync
config>redundancy>mc>peer>mcr>node>cv
config>system>lldp
config>redundancy>multi-chassis>peer>mc-ep

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Default **no shutdown**

description

Syntax **description** *description-string*
no description

Context config>cron>sched

config>system>persistence>ancp
config>system>persistence>app-assure
config>system>persistence>dhcp-server
config>system>persistence>nat-fwd
config>system>persistence>sub-mgmt
config>system>persistence>dhcp-server
config>redundancy>multi-chassis>peer

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

System Information Commands

atm

Syntax **atm**

Context config>system

Description This command enables the context to configure system-wide ATM parameters.

atm-location-id

Syntax **atm-location-id** *location-id*

Context config>system

Description This command indicates the location ID for ATM OAM.

Refer to the *7750 SR OS Services Guide* for information about ATM QoS policies and ATM-related service parameters.

Default no atm-location-id

Parameters *location-id* — Specify the 16 octets that identifies the system loopback location ID as required by the ATM OAM Loopback capability. This textual convention is defined in ITU-T standard I.610.

Invalid values include a location ID where the first octet is : 00, FF, 6A
Acceptable *location-ids* include values where the first octet is: 01, 03
Other values are not accepted.

Values 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

oam

Syntax **oam**

Context config>system>atm

Description This command configures system-wide ATM parameters.

loopback-period

Syntax **loopback-period** *period*
no loopback-period

Context config>system>atm>oam

Description This command specifies the number of seconds between periodic loopback attempts on an ATM endpoint that has periodic loopback enabled.

Parameters *period* — Specify the time, in seconds, between periodic loopback attempts.

Values 1 — 40

Default 10

retry-down

Syntax **retry-down** *retries*
no retry-down

Context config>system>atm>oam

Description Specifies the number of OAM loopback attempts that must fail after the periodic attempt before the endpoint will transition to AIS-LOC state.

The retry values are configured on a system wide basis and are affective on the next period cycle of any ATM VC SAP using **periodic-loopback**, if changed. The timeout for receiving a loopback response from the remote peer and declaring the loopack failed is 1 second and is not configurable.

Parameters *retries* — Specify the number of failed loopback attempts before an ATM VC goes down.

Values 0 — 10 (A zero value means that the endpoint will transition to AIS-LOC state immediately if the periodic loopback attempt fails.)

Default 4

retry-up

Syntax **retry-up** *retries*
no retry-up

Context config>system>atm>oam

Description This command specifies the number of consecutive OAM loopback attempts that must succeed after the periodic attempt before the endpoint will transition the state to up.

Parameters *retries* — Specify the number of successful loopback replies before an ATM VC goes up.

Values 0 — 10 (A zero value means that the endpoint will transition to the up state immediately if the periodic loopback attempt succeeds.)

Default 2

boot-bad-exec

Syntax **boot-bad-exec** *file-url*
no boot-bad-exec

Context config>system

Description Use this command to configure a URL for a CLI script to exec following a failure of a boot-up configuration. The command specifies a URL 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**).

Default no boot-bad-exec

Parameters *file-url* — Specifies the location and name of the CLI script file executed following failure of the boot-up configuration file execution. When this parameter is not specified, no CLI script file is executed.

Values	file url:	local-url | remote-url: 255 chars max	
	local-url:	[*cflash-id*/][*file-path*]	
	remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]	
		remote-locn [*hostname* | *ipv4-address* | [*ipv6- address*]]	
		ipv4-address	a.b.c.d
		ipv6-address -	x:x:x:x:x:x:x:x[-interface]
			x:x:x:x:x:x:d.d.d.d[-interface]
			x - [0..FFFF]H
			d - [0..255]D
			interface - 32 chars max, for link local addressescflash-
	id:	cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:	

Related Command s **exec command on page 91 —** This command executes the contents of a text file as if they were CLI commands entered at the console.

boot-good-exec

Syntax **boot-good-exec** *file-url*
no boot-good-exec

Context config>system

Description Use this command to configure a URL for a CLI script to exec following the success of a boot-up configuration.

Default no boot-good-exec

Parameters *file-url* — Specifies the location and name of the file executed following successful completion of the boot-up configuration file execution. When this parameter is not specified, no CLI script file is executed.

Values	file url:	local-url | remote-url: 255 chars max
	local-url:	[*cflash-id*/][*file-path*]
	remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]
		remote-locn [*hostname* | *ipv4-address* | [*ipv6- address*]
		ipv6-address - x:x:x:x:x:x:x:x[-interface]
		x:x:x:x:x:x:d.d.d.d[-interface]
		x - [0..FFFF]H
		d - [0..255]D
		interface - 32 chars max, for link local addressescflash-
	id:	cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

Related Commands **exec command on page 91 —** This command executes the contents of a text file as if they were CLI commands entered at the console.

chassis-mode

Syntax **chassis-mode** [*chassis-mode*] [**force**]

Context config>system

Description This command configures the chassis scaling and feature set.

Note that, if you are in chassis-mode **d** and configure an IOM type as iom2-20g and then downgrade to chassis-mode **a** or **b** (must specify **force** keyword), a warning appears about the IOM downgrade. In this case, the IOM`s provisioned type will downgrade to iom-20g-b. Once this is done, the ASAP MDA cannot be configured.

The ASAP MDA can only be configured if the iom2-20g IOM type is provisioned and equipped and the chassis mode is configured as **a** or **b**.

If this is the desired behavior, for example, chassis-mode **d** is configured and IPv6 is running, you can then downgrade to chassis-mode **a** or **b** if you want to disable IPv6.

For chassis mode **d**, the default must be changed from the default mode **a** which assumes the least available features. Mode **d** enables the new feature sets available with newer generations of IOMs. Chassis mode **d** supports the P2/Q2/T2-based IOMs products and the extensive queuing/policing/bandwidth. Mode **d** assumes that the **iom3-xp** is installed.

Default a

Parameters *chassis-mode* — Specify the one of the following chassis modes:

a: This mode corresponds to scaling and feature set associated with iom-20g.

b: This mode corresponds to scaling and feature set associated with iom-20g-b.

c: This mode corresponds to scaling and feature set associated with iom2-20g.

d: This mode corresponds to scaling and feature set associated with iom3-xp.

If the chassis mode is not explicitly provisioned in the configuration file, the chassis will come up in chassis mode a by default. The behavior for the IOMs is described in the following table:

Table 25: Chassis Mode Behavior

IOM	Behavior
iom-20g-b	Comes online if provisioned as iom-20g or iom-20g-b.
iom2-20g	Comes online if provisioned as iom-20g, iom-20g-b or iom2-20g.
iom-10g	Comes online if provisioned as iom-10g.
iom3-xp	Comes online if provisioned as iom3-xp.

force — Forces an upgrade from mode **a** to mode **b** or **d**, or an upgrade from mode **b** to mode **d**.

clli-code

Syntax **clli-code** *clli-code*
no clli-code

Context config>system

Description This command creates a Common Language Location Identifier (CLLI) code string for the 7750 SR-Series router. A CLLI code is an 11-character standardized geographic identifier that uniquely identifies geographic locations and certain functional categories of equipment unique to the telecommunications industry.

No CLLI validity checks other than truncating or padding the string to eleven characters are performed.

Only one CLLI code can be configured, if multiple CLLI codes are configured the last one entered overwrites the previous entry.

The **no** form of the command removes the CLLI code.

Default none — No CLLI codes are configured.

Parameters *clli-code* — The 11 character string CLLI code. Any printable, seven bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. If more than 11 characters are entered, the string is truncated. If less than 11 characters are entered the string is padded with spaces.

config-backup

Syntax **config-backup** *count*
no config-backup

Context config>system

Description This command configures the maximum number of backup versions maintained for configuration files and BOF.

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.

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 CPM is performed for all configurations and their associated persistent index files.

The **no** form of the command returns the configuration to the default value.

Default 5

Parameters *count* — The maximum number of backup revisions.

Values 1 — 9

contact

Syntax **contact** *contact-name*
no contact

Context config>system

Description This command creates a text string that identifies the contact name for the device.

Only one contact can be configured, if multiple contacts are configured the last one entered will overwrite the previous entry.

The **no** form of the command reverts to default.

Default none — No contact name is configured.

Parameters *contact-name* — The contact name character string. The string can be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

coordinates

Syntax **coordinates** *coordinates*
no coordinates

Context config>system

Description This command creates a text string that identifies the system coordinates for the device location. For example, the command **coordinates** "*37.390 -122.0550*" is read as latitude 37.390 north and longitude 122.0550 west.

Only one set of coordinates can be configured. If multiple coordinates are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default none — No coordinates are configured.

Parameters *coordinates* — The coordinates describing the device location character string. The string may be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. If the coordinates are subsequently used by an algorithm that locates the exact position of this node then the string must match the requirements of the algorithm.

dns

Syntax **dns**

Context config>system

Description This command configures DNS settings.

address-pref

Syntax **address-pref** {**ipv4-only** | **ipv6-first**
no address-pref

Context config>system>dns

Description This command configures the DNS address resolving order preference. By default 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 will be queried for AAAA-records (IPv6) first and if a successful replied is not received, then the DNS server is queried for A-records.

enable-icmp-vse

Syntax [**no**] **enable-icmp-vse**

Context config>system

Description This command enables vendor specific extensions to ICMP.

l4-load-balancing

Syntax [**no**] **l4-load-balancing**

Context config>system

Description This command configures system-wide Layer 4 load balancing. The configuration at system level can enable or disable load balancing based on Layer 4 fields. If enabled, Layer 4 source and destination port fields will be included in hashing calculation for TCP/UDP packets.

The hashing algorithm addresses finer spraying granularity where many hosts are connected to the network.

To address more efficient traffic distribution between network links (forming a LAG group), a hashing algorithm extension takes into account L4 information (i.e., src/dst L4-protocol port).

The hashing index can be calculated according to the following algorithm:

```
If [(TCP or UDP traffic) & enabled]
        hash (<TCP/UDP ports>, <IP addresses>)
else if (IP traffic)
        hash (<IP addresses>)
else
        hash (<MAC addresses>)
endif
```

This algorithm will be used in all cases where IP information in per-packet hashing is included (see LAG and ECMP Hashing in the Interfaces Guide). However the Layer 4 information (TCP/UDP ports) will not be used in the following cases:

- Fragmented packets

Default no l4-load-balancing

mc-enh-load-balancing

Syntax [**no**] **mc-enh-load-balancing**

Context config>system

Description This command enables enhanced egress multicast load balancing behavior for Layer 3 multicast. When enabled, the router will spray the multicast traffic using as hash inputs from the packet based on lsr-load-balancing, l4-load-balancing and system-ip-load-balancing configurations, namely an ingress LER or IP PE will spray traffic based on IP hash criteria: SA/DA + optional L4 port + optional system IP egress LER or

LSR - will spray traffic based on label or IP hash criteria outlined above or both based on configuration of lsr-load-balancing, l4-load-balancing and system-ip-load-balancing.

The **no** form preserves the default behavior for per flow hashing of multicast traffic.

lacp-system-priority

Syntax **lacp-system-priority** *lacp-system-priority*
no lacp-system-priority

Context config>system

Description This command configures the Link Aggregation Control Protocol (LACP) system priority on aggregated Ethernet interfaces. LACP allows the operator to aggregate multiple physical interfaces to form one logical interface.

Default 32768

Parameters *lacp-system-priority* — Specifies the LACP system priority.

Values 1 — 65535

location

Syntax **location** *location*
no location

Context config>system

Description This command creates a text string that identifies the system location for the device.

Only one location can be configured. If multiple locations are configured, the last one entered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default **none** — No system location is configured.

Parameters *location* — Enter the location as a character string. The string may be up to 80 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

name

Syntax **name** *system-name*
no name

Context config>system

Description This command creates a system name string for the device.

For example, system-name parameter ALA-1 for the **name** command configures the device name as ALA-1.

```
ABC>config>system# name "ALA-1"
ALA-1>config>system#
```

Only one system name can be configured. If multiple system names are configured, the last one encountered overwrites the previous entry.

The **no** form of the command reverts to the default value.

Default The default system name is set to the chassis serial number which is read from the backplane EEPROM.

Parameters *system-name* — Enter the system name as a character string. The string may be up to 32 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

system-ip-load-balancing

Syntax **system-ip-load-balancing**
no system-ip-load-balancing

Context config>system

Description This command enables the use of the system IP address in the ECMP hash algorithm to add a per system variable. This can help guard against cases where multiple routers, in series, will end up hashing traffic to the same ECMP/LAG path.

This command is set at a system wide basis, however if certain IOMs do not support the new load-balancing algorithm, they will continue to use the default algorithm.

The **no** form of the command resets the system wide algorithm to default.

Default no system-ip-load-balancing

switchover-exec

Syntax **switchover-exec** *file-url*
no switchover-exec

Context config>system

Description This command specifies the location and name of the CLI script file executed following a redundancy switchover from the previously active CPM card. A switchover can happen because of a fatal failure or by manual action.

The CLI script file can contain commands for environment settings, debug (excluding mirroring settings), and other commands not maintained by the configuration redundancy.

The following commands are not supported in the switchover-exec file: clear, configure, candidate, oam, tools, oam, ping, traceroute, mstat, mtrace and mrinfo.

When the *file-url* parameter is not specified, no CLI script file is executed.

Default none

Parameters *file-url* — Specifies the location and name of the CLI script file.

Values		
	file url:	local-url | remote-url: 255 chars max
	local-url:	[*cflash-id*/][*file-path*]
	remote-url:	[{ftp://|tftp://} login:pswd@remote-locn/][file-path]
	cflash-id:	cf1:, cf1-A:, cf1-B:, cf2:, cf2-A:, cf2-B:, cf3:, cf3-A:, cf3-B:

System Alarm Commands

alarm

Syntax **alarm** *rmon-alarm-id* **variable-oid** *oid-string* **interval** *seconds* [*sample-type*] [**startup-alarm** *alarm-type*] [**rising-event** *rmon-event-id* **rising-threshold** *threshold*] [**falling-event** *rmon-event-id* **falling threshold** *threshold*] [**owner** *owner-string*]
no alarm *rmon-alarm-id*

Context config>system>thresholds>rmon

Description The alarm command configures an entry in the RMON-MIB alarmTable. 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.

Use the **no** form of this command to remove an rmon-alarm-id from the configuration.

Parameters *rmon-alarm-id* — The rmon-alarm-id is a numerical identifier for the alarm being configured. The number of alarms that can be created is limited to 1200.

Default None

Values 1 — 65535

variable-oid *oid-string* **—** The oid-string is the SNMP object identifier of the particular variable to be sampled. Only SNMP variables that resolve to an ASN.1 primitive type of integer (integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled. The oid-string may be expressed using either the dotted string notation or as object name plus dotted instance identifier. For example, "1.3.6.1.2.1.2.2.1.10.184582144" or "ifInOctets.184582144".

The oid-string has a maximum length of 255 characters

Default None

interval *seconds* **—** The interval in seconds specifies the polling period over which the data is sampled and compared with the rising and falling thresholds. When setting this interval value, care should be taken in the case of 'delta' type sampling - the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2147483647 - 1 during a single sampling interval. Care should also be taken not to set the interval value too low to avoid creating unnecessary processing overhead.

Default None

Values 1 — 2147483647

sample-type — Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds.

Default **Absolute**

Values **absolute** — Specifies that the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval.
delta — Specifies that the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created.
If the first sample is greater than or equal to the rising threshold value and 'startup-alarm' is equal to 'rising' or 'either', then a single rising threshold crossing event is generated.
If the first sample is less than or equal to the falling threshold value and 'startup-alarm' is equal to 'falling' or 'either', a single falling threshold crossing event is generated.

Default **either**

Values **rising**, **falling**, **either**

rising-event *rmon-event-id* **—** The identifier of the the **rmon>event** that specifies the action to be taken when a rising threshold crossing event occurs.
If there is no corresponding 'event' configured for the specified rmon-event-id, then no association exists and no action is taken.
If the 'rising-event rmon-event-id' has a value of zero (0), no associated event exists.

If a 'rising event rmon-event' is configured, the CLI requires a 'rising-threshold' to also be configured.

Default 0

Values 0 — 65535

rising-threshold *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the 'falling-threshold' value.

Default 0

Values -2147483648 — 2147483647

falling-event *rmon-event-id* **—** The identifier of the **rmon>event** that specifies the action to be taken when a falling threshold crossing event occurs. If there is no corresponding event configured for the specified rmon-event-id, then no association exists and no action is taken. If the falling-event has a value of zero (0), no associated event exists.

If a 'falling event' is configured, the CLI requires a 'falling-threshold to also be configured.

Default 0

Values 0 — 65535

falling-threshold *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated ’startup-alarm’ is equal to ’falling’ or ’either’.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

owner *owner* **—** The owner identifies the creator of this alarm. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarmTable by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner will not normally be configured by CLI users and can be a maximum of 80 characters long.

Default TiMOS CLI

Configuration example:

```
alarm 3 variable-oid ifInOctets.184582144 interval 20 sample-type delta start-alarm either
rising-event 5 rising-threshold 10000 falling-event 5 falling-threshold 9000 owner "TiMOS
CLI"
```

cflash-cap-alarm

Syntax **cflash-cap-alarm** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-alarm *cflash-id*

Context config>system>thresholds

Description This command enables capacity monitoring of the compact flash specified in this command. The severity level is alarm. Both a rising and falling threshold can be specified.

The **no** form of this command removes the configured compact flash threshold alarm.

Parameters *cflash-id* — The cflash-id specifies the name of the cflash device to be monitored.

Values cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

rising-threshold *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated ’startup-alarm’ is equal to ’rising’ or ’either’.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the ’falling-threshold’ value.

Default 0

Values -2147483648 — 2147483647

falling-threshold *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* **—** Specifies the polling period, in seconds, over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 2147483647

rmon-event-type **—** Specifies the type of notification action to be taken when this event occurs.

Values log — An entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — A TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — Both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — No action is taken.

Default **both**

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created.

If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated.

If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Default either

Values rising, falling, either

Configuration example:

cflash-cap-alarm cf1-A: rising-threshold 50000000 falling-threshold 49999900 interval 120 rmon-event-type both start-alarm rising.

cflash-cap-warn

Syntax **cflash-cap-warn** *cflash-id* **rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no cflash-cap-warn *cflash-id*

Context config>system>thresholds

Description This command enables capacity monitoring of the compact flash specified in this command. The severity level is warning. Both a rising and falling threshold can be specified. The no form of this command removes the configured compact flash threshold warning.

Parameters *cflash-id* — The cflash-id specifies the name of the cflash device to be monitored.

Values cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

rising-threshold *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

Default 0

Values -2147483648 — 2147483647

falling-threshold ***threshold*** **—** Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* **—** Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 2147483647

rmon-event-type **—** Specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the show>system>thresholds CLI command.

trap — In the case of trap, a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Configuration example:

cflash-cap-warn cf1-B: rising-threshold 2000000 falling-threshold 1999900 interval 240 rmon-event-type trap start-alarm either

kb-memory-use-alarm

Syntax **kb-memory-use-alarm rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no kb-memory-use-warn

Context config>system>thresholds

Description This command configures memory use, in kilobytes, alarm thresholds.

The **no** form of the command removes the parameters from the configuration.

Default none

Parameters **rising-threshold** *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

Default 0

Values -2147483648 — 2147483647

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* **—** Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 2147483647

rmon-event-type **—** Specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the show>system>thresholds CLI command.

trap — In the case of trap, a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

kb-memory-use-warn

Syntax **kb-memory-use-warn rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no kb-memory-use-warn

Context config>system>thresholds

Description This command configures memory usage, in kilobytes, for warning thresholds

Default none

Parameters **rising-threshold** *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

Default 0

Values -2147483648 — 2147483647

falling-threshold *threshold* — Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* **—** Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence. This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the show>system>thresholds CLI command.

trap — In the case of trap, a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

event

Syntax **event** *rmon-event-id* [*event-type*] [**description** *description-string*] [**owner** *owner-string*]
no event *rmon-event-id*

Context config>system>thresholds>rmon

Description The event command configures an entry in the RMON-MIB event table. 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 if an entry in the RMON-MIB log table should be created to record the occurrence of the event. It may also specify that an SNMP notification (trap) should be generated for the event. The RMON-MIB defines two notifications for threshold crossing events: Rising Alarm and Falling Alarm.

Creating an event entry in the RMON-MIB log table does not create a corresponding entry in the TiMOS event logs. However, when the **event-type** is set to trap, the generation of a Rising Alarm or Falling Alarm notification creates an entry in the TiMOS event logs and that is distributed to whatever TiMOS log destinations are configured: CONSOLE, session, memory, file, syslog, or SNMP trap destination.

The TiMOS 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.

Use the **no** form of this command to remove an rmon-event-id from the configuration.

Parameters **rmon-event-type** — The rmon-event-type specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence.

This does **not** create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — In the case of trap, a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

description — The description is a user configurable string that can be used to identify the purpose of this event. This is an optional parameter and can be 80 characters long. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Default An empty string.

owner *owner* — The owner identifies the creator of this alarm. It defaults to "TiMOS CLI". This parameter is defined primarily to allow entries that have been created in the RMON-MIB alarmTable by remote SNMP managers to be saved and reloaded in a CLI configuration file. The owner will not normally be configured by CLI users and can be a maximum of 80 characters long.

Default TiMOS CLI

Configuration example:

Default event 5 rmon-event-type both description "alarm testing" owner "TiMOS CLI"

memory-use-alarm

Syntax **memory-use-alarm rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no memory-use-alarm

Context config>system>thresholds

Description The memory thresholds are based on monitoring the TIMETRA-SYSTEM-MIB sgiMemoryUsed object. This object contains the amount of memory currently used by the system. The severity level is Alarm. The absolute sample type method is used.

The **no** form of this command removes the configured memory threshold warning.

Parameters **rising-threshold** *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

Default 0

Values -2147483648 — 2147483647

falling-threshold *threshold* **—** Specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* **—** Specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence. This does not create an OS logger entry. The RMON-MIB log table entries can be viewed using the CLI command.

trap — In the case of trap, a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Values rising, falling, either

Default either

Configuration example:

```
memory-use-alarm rising-threshold 50000000 falling-threshold 45999999 interval 500 rmon-event-type
both start-alarm either
```

memory-use-warn

Syntax **memory-use-warn rising-threshold** *threshold* [**falling-threshold** *threshold*] **interval** *seconds* [*rmon-event-type*] [**startup-alarm** *alarm-type*]
no memory-use-warn

Context config>system>thresholds

Description The memory thresholds are based on monitoring MemoryUsed object. This object contains the amount of memory currently used by the system. The severity level is Alarm.

The absolute sample type method is used.

The **no** form of this command removes the configured compact flash threshold warning.

Parameters **rising-threshold** *threshold* **—** The rising-threshold specifies a threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is greater than or equal to this threshold and the associated startup-alarm is equal to rising or either.

After a rising threshold crossing event is generated, another such event will not be generated until the sampled value falls below this threshold and reaches less than or equal the falling-threshold value.

Default 0

Values -2147483648 — 2147483647

falling-threshold *threshold* **—** The falling-threshold specifies a threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single threshold crossing event will be generated. A single threshold crossing event will also be generated if the first sample taken is less than or equal to this threshold and the associated startup-alarm is equal to falling or either.

After a falling threshold crossing event is generated, another such event will not be generated until the sampled value rises above this threshold and reaches greater than or equal the rising-threshold value.

Default 0

Values -2147483648 — 2147483647

interval *seconds* **—** The interval in seconds specifies the polling period over which the data is sampled and compared with the rising and falling thresholds.

Values 1 — 2147483647

rmon-event-type — Specifies the type of notification action to be taken when this event occurs.

Values log — In the case of log, an entry is made in the RMON-MIB log table for each event occurrence.

This does not create a TiMOS logger entry. The RMON-MIB log table entries can be viewed using the **show>system>thresholds** CLI command.

trap — In the case of trap, a TiMOS logger event is generated. The TiMOS logger utility then distributes the notification of this event to its configured log destinations which may be CONSOLE, telnet session , memory log, cflash file, syslog, or SNMP trap destinations logs.

both — In the case of both, both a entry in the RMON-MIB logTable and a TiMOS logger event are generated.

none — In the case of none, no action is taken.

Default both

Values log, trap, both, none

startup-alarm *alarm-type* **—** Specifies the alarm that may be sent when this alarm is first created. If the first sample is greater than or equal to the rising threshold value and startup-alarm is equal to rising or either, then a single rising threshold crossing event is generated. If the first sample is less than or equal to the falling threshold value and startup-alarm is equal to falling or either, a single falling threshold crossing event is generated.

Default either

Values rising, falling, either

Configuration example:

```
memory-use-warn rising-threshold 500000 falling-threshold 400000 interval 800 rmon-event-
type log start-alarm falling
```

rmon

Syntax **rmon**

Context config>system>thresholds

Description This command creates the context to configure generic RMON alarms and events.

Generic RMON alarms can be created on any SNMP object-ID that is valid for RMON monitoring (for example, an integer-based datatype).

The configuration of an event controls the generation and notification of threshold crossing events configured with the alarm command.

thresholds

Syntax **thresholds**

Context config>system

Description This command enables the context to configure monitoring thresholds.

Date and Time Commands

set-time

Syntax **set-time** [*date*] [*time*]

Context admin

Description This command sets the local system time.

The time entered should be accurate for the time zone configured for the system. The system will convert the local time to UTC before saving to the system clock which is always set to UTC. This command does not take into account any daylight saving offset if defined.

Parameters *date* — The local date and time accurate to the minute in the YYYY/MM/DD format.

Values *YYYY* is the four-digit year
MM is the two-digit month
DD is the two-digit date

time — The time (accurate to the second) in the *hh*:*mm*[*:ss*] format. If no seconds value is entered, the seconds are reset to :00.

Default 0

Values *hh* is the two-digit hour in 24 hour format (00=midnight, 12=noon)
mm is the two-digit minute

time

Syntax **time**

Context config>system

Description This command enables the context to configure the system time zone and time synchronization parameters.

Network Time Protocol Commands

ntp

Syntax [**no**] **ntp**

Context config>system>time

Description This command enables the context to configure Network Time Protocol (NTP) and its operation. This protocol defines a method to accurately distribute and maintain time for network elements. Furthermore this capability allows for the synchronization of clocks between the various network elements. Use the no form of the command to stop the execution of NTP and remove its configuration.

Default none

authentication-check

Syntax [**no**] **authentication-check**

Context config>system>time>ntp

Description This command provides the option to skip the rejection of NTP PDUs that do not match the authentication key-id, type or key requirements. The default behavior when authentication is configured is to reject all NTP protocol PDUs that have a mismatch in either the authentication key-id, type or key.

When **authentication-check** is enabled, NTP PDUs are authenticated on receipt. However, mismatches cause a counter to be increased, one counter for type and one for key-id, one for type, value mismatches. These counters are visible in a show command.

The **no** form of this command allows authentication mismatches to be accepted; the counters however are maintained.

Default authentication-check — Rejects authentication mismatches.

authentication-key

Syntax **authentication-key** *key-id* {**key** *key*} [**hash** | **hash2**] **type** {**des** | **message-digest**}
no authentication-key *key-id*

Context config>system>time>ntp

Description This command sets the authentication key-id, type and key used to authenticate NTP PDUs sent to or received by other network elements participating in the NTP protocol. For authentication to work, the authentication key-id, type and key value must match.

The **no** form of the command removes the authentication key.

Default none

Parameters *key-id* — Configure the authentication key-id that will be used by the node when transmitting or receiving Network Time Protocol packets.

Entering the authentication-key command with a key-id value that matches an existing configuration key will result in overriding the existing entry.

Recipients of the NTP packets must have the same authentication key-id, type, and key value in order to use the data transmitted by this node. This is an optional parameter.

Default None

Values 1 — 255

key — The authentication key associated with the configured key-id, the value configured in this parameter is the actual value used by other network elements to authenticate the NTP packet.

The key can be any combination of ASCII characters up to 32 characters in length for message-digest (md5) or 8 characters in length for des (length limits are unencrypted lengths). If spaces are used in the string, enclose the entire string in quotation marks (" ").

hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables then the key value alone, this means that hash2 encrypted variable can't be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

type — This parameter determines if DES or message-digest authentication is used.

This is a required parameter; either DES or message-digest must be configured.

Values des — Specifies that DES authentication is used for this key
message-digest — Specifies that MD5 authentication in accordance with RFC 2104 is used for this key.

broadcast

Syntax **broadcast** [**router** *router-name*] {**interface** *ip-int-name*} [**key-id** *key-id*] [**version** *version*] [**ttl** *ttl*]
no broadcast [**router** *router-name*] {**interface** *ip-int-name*}

Context config>system>time>ntp

Description This command configures the node to transmit NTP packets on a given interface. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended.

The **no** form of this command removes the address from the configuration.

Parameters *router*Specifies the router name used to transmit NTP packets. Base is the default. Select management to use the management port (Ethernet port on the CPM).

Default Base, managementBase

ip-int-name — Specifies the local interface on which to transmit NTP broadcast packets. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 32 character maximum

key-id *key-id* **—** Identifies the configured authentication key and authentication type used by this node to receive and transmit NTP packets to and from an NTP server and peers. If an NTP packet is received by this node both authentication key and authentication type must be valid otherwise the packet will be rejected and an event/trap generated.

Values 1 — 255

Default none

version *version* **—** Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all versions will be accepted.

Values 1 — 4

Default 4

ttl *ttl* **—** Specifies the IP Time To Live (TTL) value.

Values 1 — 255

Default none

broadcastclient

Syntax **broadcastclient** [**router** *router-name*] {**interface** *ip-int-name*} [**authenticate**]
no broadcastclient [**router** *router-name*] {**interface** *ip-int-name*}

Context config>system>time>ntp

Description When configuring NTP, the node can be configured to receive broadcast packets on a given subnet. Broadcast and multicast messages can easily be spoofed, thus, authentication is strongly recommended. If broadcast is not configured then received NTP broadcast traffic will be ignored. Use the **show** command to view the state of the configuration.

The **no** form of this command removes the address from the configuration.

Parameters **router** *router-name* — Specifies the router name used to receive NTP packets.

Default Base, managementBase

interface *ip-int-name* — Specifies the local interface on which to receive NTP broadcast packets. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 32 character maximum

authenticate — Specifies whether or not to require authentication of NTP PDUs. When enabled, NTP PDUs are authenticated upon receipt.

multicast

Syntax **multicast** [**version** *version*] [**key-id** *key-id*]
no multicast

Context config>system>time>ntp

Description This command configures NTP the node to transmit multicast packets on the CPMCCM MGMT port. Broadcast and multicast messages can easily be spoofed; authentication is strongly recommended.

The **no** form of this command removes the multicast address from the configuration.

Parameters **version** *version* **—** Specifies the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all three versions are accepted.

Values 2 — 4

Default 4

key-id *key-id* **—** Specifies the configured authentication key and authentication type used by this version to transmit NTP packets. If this command is omitted from the configuration, packets are sent unencrypted.

Values 1 — 255

Default None

multicastclient

Syntax **multicastclient** [**authenticate**]
no multicastclient

Context config>system>time>ntp

Description This command configures the node to receive multicast NTP messages on the CPM MGMT port. If multicastclient is not configured, received NTP multicast traffic will be ignored. Use the **show** command to view the state of the configuration.

The **no** construct of this message removes the multicast client for the specified interface from the configuration.

Parameters **authenticate —** This optional parameter makes authentication a requirement. If authentication is required, the authentication key-id received must have been configured in the “authentication-key” command, and that key-id’s type and key value must also match.

ntp-server

Syntax **ntp-server** [**transmit** *key-id*]
no ntp-server

Context config>system>time>ntp

Description This 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.

Default no ntp-server

Parameters *key-id* — If specified, requires client packets to be authenticated.

Values 1 — 255

Default None

peer

Syntax **peer** *ip-address* [**key-id** *key-id*] [**version** *version*] [**prefer**]
no peer *ip-address*

Context config>system>time>ntp

Description 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.

The **no** form of the command removes the configured peer.

Parameters *ip-address* — Configure the IP address of the peer that requires a peering relationship to be set up. This is a required parameter.

Default None

Values Any valid IP-address

key-id *key-id* **—** Successful authentication requires that both peers must have configured the same authentication key-id, type and key value.

Specify the *key-id* that identifies the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP peer. If an NTP packet is received by this node, the authentication key-id, type, and key value must be valid otherwise the packet will be rejected and an event/trap generated.

Default None

Values 1 — 255

version *version* **—** Specify the NTP version number that is generated by this node. This parameter does not need to be configured when in client mode in which case all three nodes are accepted.

Default 4

Values 2 — 4

prefer — When configuring more than one peer, one remote system can be configured as the preferred peer. When a second peer is configured as preferred, then the new entry overrides the old entry.

server

Syntax **server** *ip address* [**key-id** *key-id*] [**version** *version*] [**prefer**]
no server *ip address*

Context config>system>time>ntp

Description This command is used when the node should operate in client mode with the ntp server specified in the address field of this command. The no construct of this command removes the server with the specified address from the configuration.

Up to ten NTP servers can be configured.

If the internal PTP process is to be used as a source of time for System Time and OAM time, then it must be specified as a server for NTP. If PTP is specified then the prefer parameter must also be specified. Once PTP has established a UTC traceable time from an external grandmaster, then it shall always be the source for time into NTP even if PTP goes into time holdover.

Parameters *ip-address* — Configures the IP address of a node that acts as an NTP server to this network element. This is a required parameter.

Values Any valid IP address

key-id *key-id* **—** Enters the key-id that identifies the configured authentication key and authentication type used by this node to transmit NTP packets to an NTP server. If an NTP packet is received by this node, the authentication key-id, type, and key value must be valid otherwise the packet will be rejected and an event/trap generated. This is an optional parameter.

Values 1 — 255

version *version* **—** Configures the NTP version number that is expected by this node. This is an optional parameter

Default 4

Values 2 — 4

prefer — When configuring more than one peer, one remote system can be configured as the preferred peer. When a second peer is configured as preferred, then the new entry overrides the old entry.

SNTP Commands

sntp

Syntax [**no**] **sntp**

Context config>system>time

Description This command creates the context to edit the Simple Network Time Protocol (SNTP).

SNTP can be configured in either broadcast or unicast client mode. 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.

The system clock is automatically adjusted at system initialization time or when the protocol first starts up.

When the time differential between the SNTP/NTP server and the system is more than 2.5 seconds, the time on the system is gradually adjusted.

SNTP is created in an administratively enabled state (**no shutdown**).

The **no** form of the command removes the SNTP instance and configuration. SNTP does not need to be administratively disabled when removing the SNTP instance and configuration.

Default no sntp

broadcast-client

Syntax [**no**] **broadcast-client**

Context config>system>time>sntp

Description This command enables listening to SNTP/NTP broadcast messages on interfaces with broadcast client enabled at global device level.

When this global parameter is configured then the **ntp-broadcast** parameter must be configured on selected interfaces on which NTP broadcasts are transmitted.

SNTP must be shutdown prior to changing either to or from broadcast mode.

The **no** form of the command disables broadcast client mode.

Default **no broadcast-client**

server-address

Syntax **server-address** *ip-address* [**version** *version-number*] [**normal | preferred**] [**interval** *seconds*]
no server-address

Context config>system>time>sntp

Description This command creates an SNTP server for unicast client mode.

Parameters *ip-address* — Specifies the IP address of the SNTP server.

version *version-number* **—** Specifies the SNTP version supported by this server.

Values 1 — 3

Default 3

normal | preferred — Specifies the preference value for this SNTP server. When more than one time-server is configured, one server can have preference over others. The value for that server should be set to **preferred**. Only one server in the table can be a preferred server.

Default normal

interval *seconds* **—** Specifies the frequency at which this server is queried.

Values 64 — 1024

Default 64

CRON Commands

cron

Syntax **cron**

Context config

Description This command creates the context to create scripts, script parameters and schedules which support the Service Assurance Agent (SAA) functions.

CRON features are saved to the configuration file on both primary and backup control modules. If a control module switchover occurs, CRON events are restored when the new configuration is loaded. If a control module switchover occurs during the execution of a cron script, the failover behavior will be determined by the contents of the script.

action

Syntax [**no**] **action** *action-name* [**owner** *action-owner*]

Context config>cron
config>cron>sched

Description This command configures action parameters for a script.

Default none

Parameters **action** *action-name* **—** Specifies the action name.

Values Maximum 32 characters.

owner *action-owner* **—** Specifies the owner name.

Default TiMOS CLI

expire-time

Syntax **expire-time** {**seconds | forever**}

Context config>cron>action

Description This command configures the maximum amount of time to keep the results from a script run.

Parameters **seconds —** Specifies the maximum amount of time to keep the results from a script run.

Values 1 — 21474836

Default 3600 (1 hour)

forever — Specifies to keep the results from a script run forever.

lifetime

Syntax **lifetime** {**seconds** | **forever**}

Context config>cron>action

Description This command configures the maximum amount of time the script may run.

Parameters **seconds —** Specifies the maximum amount of time to keep the results from a script run.

Values	1 — 21474836
Default	3600 (1 hour)

forever — Specifies to keep the results from a script run forever.

max-completed

Syntax **max-completed** *unsigned*

Context config>cron>action

Description This command specifies the maximum number of completed sessions to keep in the event execution log. If a new event execution record exceeds the number of records specified this command, the oldest record is deleted.

The **no** form of this command resets the value to the default.

Parameters *unsigned* — Specifies the maximum number of completed sessions to keep in the event execution log.

Values	0 — 255
Default	1

results

Syntax [**no**] **results** *file-url*

Context config>cron>action

Description This command specifies the location where the system writes the output of an event script's execution.

The **no** form of this command removes the file location from the configuration.

Parameters *file-url* — Specifies the location where the system writes the output of an event script's execution.

Values

```
file url:     local-url | remote-url: 255 chars max
local-url:    [cflash-id/][file-path]
remote-url:   [{ftp://} login:pswd@remote-locn/][file-path]
              remote-locn [ hostname | ipv4-address | [ipv6- address]
              ipv6-address  -  x:x:x:x:x:x:x:x[-interface]
                               x:x:x:x:x:x:d.d.d.d[-interface]
                               x - [0..FFFF]H
```

d - [0..255]D
interface - 32 chars max, for link local addressescflash-
id: cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

script

Syntax [**no**] **script** *script-name* [**owner** *owner-name*]

Context config>cron>action

Description This command creates action parameters for a script including the maximum amount of time to keep the results from a script run, the maximum amount of time a script may run, the maximum number of script runs to store and the location to store the results.

The **no** form of this command removes the script parameters from the configuration.

Default none — No server-address is configured.

Parameters **script** *script-name* **—** The script command in the action context connects and event to the script which will run when the event is triggered.

owner *owner-name* **—** Owner name of the schedule.

Default TiMOS CLI

The **no** form of this command removes the script entry from the action context.

schedule

Syntax [**no**] **schedule** *schedule-name* [**owner** *owner-name*]

Context config>cron

Description This command 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).

The **no** form of the command removes the context from the configuration.

Default none

Parameters *schedule-name* — Name of the schedule.

owner *owner-name* **—** Owner name of the schedule.

count

Syntax **count** *number*

Context config>cron>sched

Description This command configures the total number of times a CRON "interval" schedule is run. For example, if the interval is set to 600 and the count is set to 4, the schedule runs 4 times at 600 second intervals.

Parameters *number* — The number of times the schedule is run.

Values 1 — 65535

Default 65535

day-of-month

Syntax [**no**] **day-of-month** {*day-number* [..*day-number*] **all**}

Context config>cron>sched

Description This command specifies which days of the month that the schedule will occur. Multiple days of the month can be specified. When multiple days are configured, each of them will cause the schedule to trigger. If a day-of-month is configured without configuring month, weekday, hour and minute, the event will not execute.

Using the **weekday** command as well as the **day-of-month** command will cause the script to run twice. For example, consider that "today" is Monday January 1. If "Tuesday January 5" is configured, the script will run on Tuesday (tomorrow) as well as January 5 (Friday).

The **no** form of this command removes the specified day-of-month from the list.

Parameters *day-number* — The positive integers specify the day of the month counting from the first of the month. The negative integers specify the day of the month counting from the last day of the month. For example, configuring **day-of-month -5, 5** in a month that has 31 days will specify the schedule to occur on the 27th and 5th of that month.

Integer values must map to a valid day for the month in question. For example, February 30 is not a valid date.

Values 1 — 31, -31 — -1 (maximum 62 day-numbers)

all — Specifies all days of the month.

end-time

Syntax [**no**] **end-time** [*date* **|** *day-name*] *time*

Context config>cron>sched

Description This command is used concurrently with type **periodic** or **calendar**. Using the type of **periodic**, end-time determines at which interval the schedule will end. Using the type of **calendar**, end-time determines on which date the schedule will end.

When **no end-time** is specified, the schedule runs forever.

Parameters *date* — Specifies the date to schedule a command.

Values YYYY:MM:DD in year:month:day number format

day-name — Specifies the day of the week to schedule a command.

Values sunday|monday|tuesday|wednesday|thursday|friday|saturday

time — Specifies the time of day to schedule a command.

Values hh:mm in hour:minute format

hour

Syntax [**no**] **hour** {..*hour-number* [..*hour-number*]| **all**}

Context config>cron>sched

Description This command specifies which hour to schedule a command. Multiple hours of the day can be specified. When multiple hours are configured, each of them will cause the schedule to trigger. Day-of-month or weekday must also be specified. All days of the month or weekdays can be specified. If an hour is configured without configuring month, weekday, day-of-month, and minute, the event will not execute.

The **no** form of this command removes the specified hour from the configuration.

Parameters *hour-number* — Specifies the hour to schedule a command.

Values 0 — 23 (maximum 24 hour-numbers)

all — Specifies all hours.

interval

Syntax [**no**] **interval** *seconds*

Context config>cron>sched

Description This command specifies the interval between runs of an event.

Parameters *seconds* — The interval, in seconds, between runs of an event.

Values 30 — 4,294,967,295

minute

Syntax [**no**] **minute** {*minute-number* [..*minute-number*]| **all**}

Context config>cron>sched

Description This command specifies the minute to schedule a command. Multiple minutes of the hour can be specified. When multiple minutes are configured, each of them will cause the schedule to occur. If a minute is configured, but no hour or day is configured, the event will not execute. If a minute is configured without configuring month, weekday, day-of-month, and hour, the event will not execute.

The **no** form of this command removes the specified minute from the configuration.

Parameters *minute-number* — Specifies the minute to schedule a command.

Values 0 — 59 (maximum 60 minute-numbers)

all — Specifies all minutes.

month

Syntax [**no**] **month** {*month-number* [..*month-number*]|*month-name* [..*month-name*]| **all**}

Context config>cron>sched

Description This command specifies the month when the event should be executed. Multiple months can be specified. When multiple months are configured, each of them will cause the schedule to trigger. If a month is configured without configuring weekday, day-of-month, hour and minute, the event will not execute.

The **no** form of this command removes the specified month from the configuration.

Parameters **month-number** — Specifies a month number.

Values 1 —12 (maximum 12 month-numbers)

all — Specifies all months.

month-name — Specifies a month by name

Values january, february, march, april, may, june, july, august, september, october, november, december (maximum 12 month names)

type

Syntax **type** {*schedule-type*}

Context config>cron>sched

Description This command specifies how the system should interpret the commands contained within the schedule node.

Parameters *schedule-type* — Specify the type of schedule for the system to interpret the commands contained within the schedule node.

Values **periodic** — Specifies a schedule which runs at a given interval. interval must be specified for this feature to run successfully.
calendar — Specifies a schedule which runs based on a calendar. weekday, month, day-of-month, hour and minute must be specified for this feature to run successfully.
oneshot — Specifies a schedule which runs one time only. As soon as the first event specified in these parameters takes place and the associated event occurs, the schedule enters a shutdown state. month, weekday, day-of-month, hour and minute must be specified for this feature to run successfully.

Default periodic

weekday

Syntax [**no**] **weekday** {*weekday-number* [..*weekday-number*]|*day-name* [..*day-name*]| **all**}

Context config>cron>sched

Description This command specifies which days of the week that the schedule will fire on. Multiple days of the week can be specified. When multiple days are configured, each of them will cause the schedule to occur. If a weekday is configured without configuring month, day-of-month, hour and minute, the event will not execute.

Using the **weekday** command as well as the **day-of month** command will cause the script to run twice. For example, consider that “today” is Monday January 1. If “Tuesday January 5” is configured, the script will run on Tuesday (tomorrow) as well as January 5 (Friday).

The **no** form of this command removes the specified weekday from the configuration.

Parameters **day-number —** Specifies a weekday number.

Values 1 —7 (maximum 7 week-day-numbers)

day-name — Specifies a day by name

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday (maximum 7 weekday names)

all — Specifies all days of the week.

script

Syntax [**no**] **script** *script-name* [**owner** *owner-name*]

Context config>cron>script

Description This command configures the name associated with this script.

Parameters *script-name* — Specifies the script name.location

Syntax [**no**] **location** *file-url*

Context config>cron>script

Description This command configures the location of script to be scheduled.

Parameters *file-url* — Specifies the location where the system writes the output of an event script's execution.

Values

file url:	local-url | remote-url: 255 chars max
local-url:	[*cflash-id*/][*file-path*]
remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]
	remote-locn [*hostname* | *ipv4-address* | [*ipv6- address*]
	ipv6-address - x:x:x:x:x:x:x:x[-interface]
	x:x:x:x:x:x:d.d.d.d[-interface]
	x - [0..FFFF]H
	d - [0..255]D
	interface - 32 chars max, for link local addressescflash-
id:	cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

Time Range Commands

time-range

Syntax [**no**] **time-range** *name*

Context config>cron

Description This command configures a time range.

The **no** form of the command removes the *name* from the configuration.

Default none

Parameters *name* — Configures a name for the time range up to 32 characters in length.

absolute

Syntax **absolute start** *start-absolute-time* **end** *end-absolute-time*
no absolute start *absolute-time*

Context config>cron>time-range

Description This command configures an absolute time interval that will not repeat.

The **no** form of the command removes the absolute time range from the configuration.

Parameters **start** *absolute-time* **—** Specifies starting parameters for the absolute time-range.

Values	absolute-time:	year/month/day,hh:mm
	year:	2005 — 2099
	month:	1 — 12
	day:	1 — 31
	hh:	0 — 23
	mm: [	0 — 59

end *absolute-time* **—** Specifies end parameters for the absolute time-range.

Values	absolute-time:	year/month/day,hh:mm
	year:	2005 — 2099
	month:	1 — 12
	day:	1 — 31
	hh:	0 — 23
	mm: [	0 — 59

daily

Syntax **daily start** *start-time-of-day* **end** *end-time-of-day*
no daily start *start-time-of-day*

Context config>cron>time-range

Description This command configures the start and end of a schedule for every day of the week. 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.

The **no** form of the command removes the daily time parameters from the configuration.

Parameters *start-time-of-day* — Specifies the starting time for the time range.

Values	Syntax:	hh:mm	
		hh	0 — 23
		mm	0 — 59

end-time-of-day — Specifies the ending time for the time range.

Values	Syntax:	hh:mm	
		hh	0 — 24
		mm	0 — 59

weekdays

Syntax **weekdays start** *start-time-of-day* **end** *end-time-of-day*
no weekdays start *start-time-of-day*

Context config>cron>time-range

Description This command configures the start and end of a weekday schedule.

The **no** form of the command removes the weekday parameters from the configuration.

Parameters *start-time-of-day* — Specifies the starting time for the time range.

Values	Syntax:	hh:mm	
		hh	0 — 23
		mm	0 — 59

end-time-of-day — Specifies the ending time for the time range.

Values	Syntax:	hh:mm	
		hh	0 — 24
		mm	0 — 59

weekend

Syntax **weekend start** *start-time-of-day* **end** *end-time-of-day*
no weekend start *start-time-of-day*

Context config>cron>time-range

Description This command configures a time interval for every weekend day in the time range.

The resolution must be at least one minute apart, for example, start at 11:00 and end at 11:01. An 11:00 start and end time is invalid. This example configures a start at 11:00 and an end at 11:01 on both Saturday and Sunday.

The **no** form of the command removes the weekend parameters from the configuration.

Parameters *start-time-of-day* — Specifies the starting time for the time range.

Values Syntax: hh:mm
hh 0 — 23
mm 0 — 59

end-time-of-day — Specifies the ending time for the time range.

Values Syntax: hh:mm
hh 0 — 24
mm 0 — 59

weekly

Syntax **weekly start** *start-time-in-week* **end** *end-time-in-week*
no weekly start *start-time-in-week*

Context config>cron>time-range

Description This command configures a weekly periodic interval in the time range.

The **no** form of the command removes the weekly parameters from the configuration.

Parameters *start-time-in-week* — Specifies the start day and time of the week.

Values Syntax: day,hh:mm

day sun, mon, tue, wed, thu, fri, sat
sunday, monday, tuesday, wednesday, thursday, friday, saturday
hh 0 — 23
mm 0 — 59

end-time-in-week — Specifies the end day and time of the week.

Values Syntax: day,hh:mm

Values day sun, mon, tue, wed, thu, fri, sat
sunday, monday, tuesday, wednesday, thursday, friday, saturday

hh	0 — 24
mm	0 — 59

weekly start *time-in-week* **end** *time-in-week* **—** This parameter configures the start and end of a 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.

Values 00 — 23, 00 — 59

Default no time-range

Time of Day Commands

tod-suite

Syntax [**no**] **tod-suite** *tod-suite name* **create**

Context config>cron

Description This command creates the tod-suite context.

Default no tod-suite

egress

Syntax **egress**

Context config>cron>tod-suite

Description This command enables the TOD suite egress parameters.

ingress

Syntax **ingress**

Context config>cron>tod-suite

Description This command enables the TOD suite ingress parameters.

filter

Syntax **filter ip** *ip-filter-id* [**time-range** *time-range-name*] [**priority** *priority*]
filter ipv6 *ipv6-filter-id* [**time-range** *time-range-name*] [**priority** *priority*]
filter mac *mac-filter-id* [**time-range** *time-range-name*] [**priority** *priority*]
no ip *ip-filter-id* [**time-range** *time-range-name*]
no filter ipv6 *ipv6-filter-id* [**time-range** *time-range-name*]
no filter mac *mac-filter-id* [**time-range** *time-range-name*]

Context config>cron>tod-suite>egress
config>cron>tod-suite>ingress

Description This command creates time-range based associations of previously created filter 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.

Parameters **ip-filter** *ip-filter-id* — Specifies an IP filter for this tod-suite.

Values 1 — 65535

ipv6-filter *ipv6-filter-id* — Specifies an IPv6 filter for this tod-suite.

Values 1 — 65535

time-range *time-range-name* — Name for the specified time-range. If the time-range is not populated the system will assume the assignment to mean “all times”. Only one entry without a time-range is allowed for every type of policy. The system does not allow the user to specify more than one policy with the same time-range and priority.

Values Up to 32 characters

priority *priority* — Priority of the time-range. Only one time-range assignment of the same type and priority is allowed.

Values 1 — 10

mac *mac-filter-id* — Specifies a MAC filter for this tod-suite.

Values 1 — 65535

qos

Syntax **qos** *policy-id* [**time-range** *time-range-name*] [**priority** *priority*]
no qos *policy-id* [**time-range** *time-range-name*] [

Context config>cron>tod-suite>egress
config>cron>tod-suite>ingress

Description This command creates time-range based associations of previously created QoS 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.

The no form of the command reverts to the

Parameters **policy-id** — Specifies an egress QoS policy for this tod-suite.

Values 1 — 65535

time-range *time-range-name* — Name for the specified time-range. If the time-range is not populated the system will assume the assignment to mean “all times”. Only one entry without a time-range is allowed for every type of policy. The system does not allow the user to specify more than one policy with the same time-range and priority.

Values Up to 32 characters

Default "NO-TIME-RANGE" policy

priority *priority* — Priority of the time-range. Only one time-range assignment of the same type and priority is allowed.

Values 1 — 10

Default 5

scheduler-policy

Syntax [**no**] **scheduler-policy** *scheduler-policy-name* [**time-range** *time-range-name*] [**priority** *priority*]

Context config>cron>tod-suite>egress
config>cron>tod-suite>ingress

Description This command creates time-range based associations of previously created 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.

Parameters *scheduler-policy-name* — Specifies a scheduler policy for this tod-suite.

Values Up to 32 characters

time-range *time-range-name* **—** Specifies the name for a time-range. If the time-range is not populated the system will assume the assignment to mean "all times". Only one entry without a time-range is allowed for every type of policy. The system does not allow the user to specify more than one policy and the same time-range and priority.

Values Up to 32 characters

priority *priority* **—** Specifies the time-range priority. Only one time-range assignment of the same type and priority is allowed.

Values 1 — 10

System Time Commands

dst-zone

Syntax [**no**] **dst-zone** [*std-zone-name* | *non-std-zone-name*]

Context config>system>time

Description This command 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 is adjusted by adding the configured offset when summer time starts and subtracting the configured offset when summer time ends.

If the time zone configured is listed in Table 21, System-defined Time Zones, on page 214, then the starting and ending parameters and offset do not need to be configured with this command unless it is necessary to override the system defaults. The command returns an error if the start and ending dates and times are not available either in Table 21 on or entered as optional parameters in this command.

Up to five summer time zones may be configured, for example, for five successive years or for five different time zones. Configuring a sixth entry will return an error message. If no summer (daylight savings) time is supplied, it is assumed no summer time adjustment is required.

The **no** form of the command removes a configured summer (daylight savings) time entry.

Default none — No summer time is configured.

Parameters *std-zone-name* — The standard time zone name. The standard name must be a system-defined zone in Table 21. For zone names in the table that have an implicit summer time setting, for example MDT for Mountain Daylight Saving Time, the remaining **start-date**, **end-date** and **offset** parameters need to be provided unless it is necessary to override the system defaults for the time zone.

Values std-zone-name ADT, AKDT, CDT, CEST, EDT, EEST, MDT, PDT, WEST

non-std-zone-name — The non-standard time zone name. Create a user-defined name created using the **zone** command on page 371

Values 5 characters maximum

end

Syntax **end** {*end-week*} {*end-day*} {*end-month*} [*hours-minutes*]

Context config>system>time>dst-zone

Description This command configures start of summer time settings.

Parameters *end-week* — Specifies the starting week of the month when the summer time will end.

Values first, second, third, fourth, last

Default first

end-day — Specifies the starting day of the week when the summer time will end.

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

Default sunday

end-month — The starting month of the year when the summer time will take effect.

Values january, february, march, april, may, june, july, august, september, october, november, december}

Default january

hours — Specifies the hour at which the summer time will end.

Values 0 — 24

Default 0

minutes — Specifies the number of minutes, after the hours defined by the *hours* parameter, when the summer time will end.

Values 0 — 59

Default 0

offset

Syntax **offset** *offset*

Context config>system>time>dst-zone

Description This command specifies the number of minutes that will be added to the time when summer time takes effect. The same number of minutes will be subtracted from the time when the summer time ends.

Parameters *offset* — The number of minutes added to the time at the beginning of summer time and subtracted at the end of summer time, expressed as an integer.

Default 60

Values 0 — 60

start

Syntax **start** {*start-week*} {*start-day*} {*start-month*} [*hours-minutes*]

Context config>system>time>dst-zone

Description This command configures start of summer time settings.

Parameters **start-week —** Specifies the starting week of the month when the summer time will take effect.

Values first, second, third, fourth, last

Default first

start-day — Specifies the starting day of the week when the summer time will take effect.

Default sunday

Values sunday, monday, tuesday, wednesday, thursday, friday, saturday

start-month — The starting month of the year when the summer time will take effect.

Values january, february, march, april, may, june, july, august, september, october, november, december

Default january

hours — Specifies the hour at which the summer time will take effect.

Default 0

minutes — Specifies the number of minutes, after the hours defined by the *hours* parameter, when the summer time will take effect.

Default 0

zone

Syntax **zone** [*std-zone-name* | *non-std-zone-name*] [*hh* [:*mm*]]
no zone

Context config>system>time

Description This command sets the time zone and/or time zone offset for the device.

7750 SR OS supports system-defined and user-defined time zones. The system-defined time zones are listed in Table 21, System-defined Time Zones, on page 214.

For user-defined time zones, the zone and the UTC offset must be specified.

The **no** form of the command reverts to the default of Coordinated Universal Time (UTC). If the time zone in use was a user-defined time zone, the time zone will be deleted. If a **dst-zone** command has been configured that references the zone, the summer commands must be deleted before the zone can be reset to UTC.

Default **zone utc** - The time zone is set for Coordinated Universal Time (UTC).

Parameters *std-zone-name* — The standard time zone name. The standard name must be a system-defined zone in Table 21. For zone names in the table that have an implicit summer time setting, for example MDT for Mountain Daylight Saving Time, the remaining **start-date**, **end-date** and **offset** parameters need to be provided unless it is necessary to override the system defaults for the time zone.

For system-defined time zones, a different offset cannot be specified. If a new time zone is needed with a different offset, the user must create a new time zone. Note that some system-defined time zones have implicit summer time settings which causes the switchover to summer time to occur automatically; configuring the **dst-zone** parameter is not required.

A user-defined time zone name is case-sensitive and can be up to 5 characters in length.

Values A user-defined value can be up to 4 characters or one of the following values:
GMT, BST, IST, WET, WEST, CET, CEST, EET, EEST, MSK, MSD, AST, ADT, EST,

EDT, ET, CST, CDT, CT, MST, MDT, MT, PST, PDT, PT, HST, AKST, AKDT, WAST, CAST, EAST

non-std-zone-name — The non-standard time zone name.

Values Up to 5 characters maximum.

hh [**:mm**] — The hours and minutes offset from UTC time, expressed as integers. Some time zones do not have an offset that is an integral number of hours. In these instances, the *minutes-offset* must be specified. For example, the time zone in Pirlanngimpi, Australia UTC + 9.5 hours.

Default hours: 0
minutes: 0

Values hours: -11 — 11
minutes: 0 — 59

source-ptp

Syntax [**no**] **source-ptp**

Context config>system>time

Description This command is used to configure the use of the time recovered by ptp as the source of system time. PTP recovered time can only be used if grandmaster sourcing the timescale toward the router is advertising both timeTraceable = TRUE and ptpTimescale = TRUE.

The **no** form of the command reverts to the default of not using the time recovered by ptp as the source of system time.

Default no source-ptp

System Synchronization Configuration Commands

sync-if-timing

Syntax **sync-if-timing**

Context config>system

Description This command creates or edits the context to create or modify timing reference parameters.
This command is not enabled in the 7750 SR-1.

Default Disabled

abort

Syntax **abort**

Context config>system>sync-if-timing

Description This command is required to discard changes that have been made to the synchronous interface timing configuration during a session.

Default No default

begin

Syntax **begin**

Context config>system>sync-if-timing

Description This command is required in order to enter the mode to create or edit the system synchronous interface timing configuration.

Default No default

bits

Syntax **bits**

Context config>system>sync-if-timing

Description This command enables the context to configure parameters for the Building Integrated Timing Supply (BITS). The settings specified under this context apply to both the BITS input and BITS output ports and to both the bits1 and bits2 ports on the 7750 SR-c4. The **bits** command subtree is only available on the 7450 ESS-7 and 7450 ESS-12.

Default disabled

commit

Syntax **commit**

Context config>system>sync-if-timing

Description This command saves changes made to the system synchronous interface timing configuration.

Default No default

interface-type

Syntax **interface-type** {**ds1** [{**esf** | **sf**}] | **e1** [{**pcm30crc** | **pcm31crc**}]}
no interface-type

Context config>system>sync-if-timing>bits

Description This command configures the Building Integrated Timing Source (BITS) timing reference. This command is not supported on the 7450 ESS-6, 7450 ESS-6v, 7450 ESS-1.

The **no** form of the command reverts to the default configuration.

Default ds1 esf

Parameters **ds1 esf** — Specifies Extended Super Frame (ESF). This is a framing type used on DS1 circuits that consists of 24 192-bit frames, The 193rd bit provides timing and other functions.

ds1 sf — Specifies Super Frame (SF), also called D4 framing. This is a common framing type used on DS1 circuits. SF consists of 12 192-bit frames. The 193rd bit provides error checking and other functions. ESF supersedes SF.

e1 pcm30crc — Specifies the pulse code modulation (PCM) type. PCM30CRC uses PCM to separate the signal into 30 user channels with CRC protection.

e1 pcm31crc — Specifies the pulse code modulation (PCM) type. PCM31CRC uses PCM to separate the signal into 31 user channels with CRC protection.

bits-interface-type

Syntax **bits-interface-type**

Context config>system>sync-if-timing>ref1
config>system>sync-if-timing>ref2

Description This command configures the interface type of the BITS timing reference.

This command is only supported on the 7750 SR-c12 (and 7710 SR-c12).

input

Syntax **input**

Context config>system>sync-if-timing>bits

Description This command provides a context to enable or disable the external BITS timing reference inputs to the SR/ESS router. In redundant systems with BITS ports, there are two possible BITS-in interfaces, one for each CPM. In the 7750 SR-c4 system, there are two bits ports on the CFM. They are configured together, but they are displayed separately in the show command.

Default shutdown

output

Syntax **output**

Context config>system>sync-if-timing>bits

Description This command provides a context to configure and enable or disable the external BITS timing reference output to the SR/ESS router. On redundant systems, there are two possible BITS-out interfaces, one for each CPM. On the 7750 SR-c4 system, there are two possible BITS-out interfaces on the chassis front panel. They are configured together, but they are displayed separately in the show command.

Default shutdown

line-length

Syntax **line-length** {110,220,330,440,550,660}

Context config>system>sync-if-timing>bits

Description This command configures the line-length parameter of the BITS output, This is the distance in feet between the network element and the office clock (BITS/SSU). There are two possible BITS-out interfaces, one for each CPM. They are configured together, but they are displayed separately in the show command. This command is only applicable when the interface-type is DS1.

Default 110

Parameters *110* — Distance is from 0 to 110 feet

220 — Distance is from 110 to 220 feet

330 — Distance is from 220 to 330 feet

440 — Distance is from 330 to 440 feet

550 — Distance is from 440 to 550 feet

660 — Distance is from 550 to 660 feet

source

Syntax **source** {**line-ref** | **internal-clock**}

Context config>system>sync-if-timing>bits>output

Description This command configures the values used to identity the source of the BITS (Building Integrated Timing Supply) output. This is either the signal recovered directly from ref1, ref2 or ptp or it is the output of the node's central clock. The directly recovered signal would be used when the BITS output signal is feeding into an external stand alone timing distribution device (BITS/SASE). The specific directly recovered signal used is the best of the available signals based of the QL and/or the ref-order. The central clock output would be used when no BITS/SASE device is present and the BITS output signal is used to monitor the quality of the recovered clock within the system.

Default line-ref

Parameters **line-ref —** Specifies that the BITS output timing is selected from one of the input references, without any filtering.

internal-clock — Specifies that the BITS output timing is driven from the system timing.

ssm-bit

Syntax **ssm-bit** *sa-bit*

Context config>system>sync-if-timing>bits
config>system>sync-if-timing>ref1
config>system>sync-if-timing>ref2

Description This command configures which sa-bit to use for conveying SSM information when the interface-type is E1.

Default 8

Parameters *sa-bit* — Specifies the sa-bit value.

Values 4–8

ql-override

Syntax **ql-override** {**prs|stu|st2|tnc|st3e|st3|eec1|sec|prc|ssu-a|ssu-b|eec2**}
no ql-override

Context config>system>sync-if-timing>bits
config>system>sync-if-timing>ptp
config>system>sync-if-timing>ref1
config>system>sync-if-timing>ref2

Description This command configures the QL value to be used for the reference for SETS input selection and BITS output. This value overrides any value received by that reference's SSM process.

Default no ql-overide

Parameters **prs** — SONET Primary Reference Source Traceable

stu — SONET Synchronous Traceability Unknown

st2 — SONET Stratum 2 Traceable

tnc — SONET Transit Node Clock Traceable

st3e — SONET Stratum 3E Traceable

st3 — SONET Stratum 3 Traceable

eec1 — Ethernet Equipment Clock Option 1 Traceable (sdh)

eec2 — Ethernet Equipment Clock Option 2 Traceable (sonet)

prc — SDH Primary Reference Clock Traceable

ssu-a — SDH Primary Level Synchronization Supply Unit Traceable

ssu-b — SDH Second Level Synchronization Supply Unit Traceable

sec — SDH Synchronous Equipment Clock Traceable

ql-selection

Syntax [**no**] **ql-selection**

Context config>system>sync-if-timing

Description When enabled the selection of system timing reference and BITS output timing reference takes into account quality level. This command turns -on or turns-off SSM encoding as a means of timing reference selection.

Default no ql-selection

ptp

Syntax **ptp**

Context config>system>sync-if-timing

Description This command enables the context to configure parameters for system timing via IEEE 1588-2008, Precision Time Protocol.

This command is only available on the systems supporting the 1588-2008 frequency recovery engine.

ref-order

Syntax **ref-order** *first second* [*third* [f*ourth*]]
no ref-order

Context config>system>sync-if-timing

Description The synchronous equipment timing subsystem can lock to different timing reference inputs, those specified in the **ref1, ref2**, **bits** and **ptp** command configuration. This command organizes the priority order of the timing references.

If a reference source is disabled, then the clock from the next reference source as defined by **ref-order** is used. If all reference sources are disabled, then clocking is derived from a local oscillator.

Note that if a **sync-if-timing** reference is linked to a source port that is operationally down, the port is no longer qualified as a valid reference.

For systems with two SF/CPM modules, the system distinguishes between the BITS inputs on the active and standby CPMs. The active CPM will use its BITS input port providing that port is qualified. If the local port is not qualified, then the active CPM will use the BITS input port from the standby CPM as the next priority reference. For example, the normal ref-order of “bits ref1 ref2” will actually be bits (active CPM), followed by bits (standby CPM), followed by ref1, followed by ref2.

For 7750 SR-c4 systems, the system distinguishes between the two BITS inputs on the CFM. The CFM will use its BITS input port “bits1” providing that port is qualified. If port “bits1” is not qualified, then the CFM will use the BITS input port “bits2” as the next priority reference. For example, the normal ref-order of “bits ref1 ref2” will actually be bits1 followed by bits2, followed by ref1, followed by ref2.

The **no** form of the command resets the reference order to the default values.

The **bits** option is not supported on the 7750 SR-c12 chassis.

Default **bitsref1 ref2 ptp**

first — Specifies the first timing reference to use in the reference order sequence.

Values ref1, ref2, bits, ptp

second — Specifies the second timing reference to use in the reference order sequence.

Values ref1, ref2, bits, ptp

third — Specifies the third timing reference to use in the reference order sequence.

Values ref1, ref2, bits, ptp

ref1

Syntax **ref1**

Context config>system>sync-if-timing

Description This command enables the context to configure parameters for the first timing reference. Note that source ports for ref1 and ref2 must be on different slots.

The timing reference for **ref1** must be specified for the following chassis slots:

7750 Model	Ref1/Slots
SR-1	Not enabled
SR-7	1 — 2
SR-12	1 — 5
SR-c12	No restriction
SR-c4	No restriction

Note: ref1 and ref2 cannot be configured on the same MDA/CMA for the SR-c12 nor the SR-c4.

ref2

Syntax **ref2**

Context config>system>sync-if-timing

Description This command enables the context to configure parameters for the second timing reference. Note that source ports for ref1 and ref2 must be on different slots.

The timing reference for **ref2** must be specified for the following chassis slots.

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

7750 Model	Ref2/Slots
SR-1	Not enabled
SR-7	3 — 5
SR-12	6 — 10
SR-c12	No restriction
SR-c4	No restriction

Note: ref1 and ref2 cannot be configured on the same MDA/CMA for the SR-c12 nor the SR-c4.

revert

Syntax [**no**] **revert**

Context config>system>sync-if-timing

Description This 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 the mode is non-revertive, a failed clock source is not selected again.

Default no revert

source-bits

Syntax **source-bits** *slot/mda*
no source-bits

Context config>system>sync-if-timing>ref1 config>system>sync-if-timing>ref2

Description This comand configures the source bits for the first (ref1) or second (ref2) timing reference. Note that this command is only applicable to the 7750 SR-c12 chassis.

Parameters *slot/mda* — Specifies the chassis slot and MDA containing the BITS port to be used as one of the two timing reference sources in the system timing subsystem.

Values slot: 1
mda: 1 — 12

source-port

Syntax **source-port** *port-id*
no source-port

Context config>system>sync-if-timing>ref1
config>system>sync-if-timing>ref2

Description This command configures the source port for timing reference **ref1** or **ref2**. If the port is unavailable or the link is down, then the reference sources are re-evaluated according to the reference order configured in the **ref-order** command.

In addition to physical port, T1 or E1 channels on a Channelized OC3/OC12/STM1/STM4 Circuit Emulation Service port can be specified if they are using adaptive timing.

The timing reference for **ref1** and **ref2** must be specified for ports in the following chassis slots:

7750 Model	Ref1/Slots	Ref2/Slots
SR-1	Not enabled	Not enabled
SR-7	1 — 2	3 — 5
SR-12	1 — 5	6 — 10
SR-c12	No restriction	No restriction
SR-c4	No restriction	No restriction

Note that ref1 and ref2 cannot be configured on the same MDA/CMA for the SR-c12 nor the SR-c4.

Parameters *port-id* — Identify the physical port in the *slot/mda/port* format.

System Administration Commands

admin

Syntax **admin**

Context <ROOT>

Description The context to configure administrative system commands. Only authorized users can execute the commands in the **admin** context.

Default none

application-assurance

Syntax **application-assurance**

Context admin

Description This command enables the context to perform application-assurance operations.

upgrade

Syntax **upgrade**

Context admin>app-assure

Description This command loads a new protocol list from the isa-aa.tim file into the CPM.

Note that an ISA-AA reboot is required.

clear-policy-lock

Syntax **clear-policy-lock**

Context admin>

Description This command allows an authorized administrator to clear an exclusive policy lock. This will reset the lock flag and end the policy editing session in progress, aborting any policy edits.

debug-save

Syntax **debug-save** *file-url*

Context admin

Description This command saves existing debug configuration. Debug configurations are not preserved in configuration saves.

Default none

Parameters *file-url* — The file URL location to save the debug configuration.

Values

```
file url:       local-url | remote-url: 255 chars max
local-url:      [cflash-id/][file-path], 200 chars max, including the cflash-id
                directory length, 99 chars max each
remote-url:     [{ftp://} login:pswd@remote-locn/][file-path]
                remote-locn [ hostname | ipv4-address | [ipv6- address] ]
                ipv4-address        a.b.c.d
                ipv6-address   -    x:x:x:x:x:x:x:x[-interface]
                                    x:x:x:x:x:x:d.d.d.d[-interface]
                                    x - [0..FFFF]H
                                    d - [0..255]D
                                    interface - 32 chars max, for link local addresses255
chars max, directory length 99 chars max each
cflash-id:      cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:
```

disconnect

Syntax **disconnect** {**address** *ip-address* **| username** *user-name* **| console | telnet | ftp | ssh**}

Context admin

Description This command disconnects a user from a console, Telnet, FTP, or SSH session.

If any of the console, Telnet, FTP, or SSH options are specified, then only the respective console, Telnet, FTP, or SSH sessions are affected.

If no console, Telnet, FTP, or SSH options are specified, then all sessions from the IP address or from the specified user are disconnected.

Any task that the user is executing is terminated. FTP files accessed by the user will not be removed.

A major severity security log event is created specifying what was terminated and by whom.

Default none — No disconnect options are configured.

Parameters **address** *ip-address* **—** The IP address to disconnect, specified in dotted decimal notation.

```
ipv4-address              a.b.c.d
                ipv6-address  -   x:x:x:x:x:x:x:x[-interface]
                                  x:x:x:x:x:x:d.d.d.d[-interface]
                                  x - [0..FFFF]H
                                  d - [0..255]Dusername user-name — The name of the user.
```

console — Disconnects the console session.

telnet — Disconnects the Telnet session.

ftp — Disconnects the FTP session.

ssh — Disconnects the SSH session.

display-config

Syntax **display-config** [**detail** | **index**]

Context admin

Description This command displays the system’s running configuration.

By default, only non-default settings are displayed.

Specifying the **detail** option displays all default and non-default configuration parameters.

Parameters **detail —** Displays default and non-default configuration parameters.

index — Displays only persistent-indices.

reboot

Syntax **reboot** [**active** | **standby** | **upgrade**] [**now**]

Context admin

Description This command reboots the router including redundant CPMs and all IOMs or upgrades the boot ROMs.

If no options are specified, the user is prompted to confirm the reboot operation. For example:

```
ALA-1>admin# reboot
Are you sure you want to reboot (y/n)?
```

If the **now** option is specified, boot confirmation messages appear.

Parameters **active —** Keyword to reboot the active CPM.

Default active

standby — Keyword to reboot the standby CPM.

Default active

upgrade — Forces card firmware to be upgraded during chassis reboot. Normally, the 7750 SR OS automatically performs firmware upgrades on CPMs and IOM cards without the need for the "upgrade" keyword.

When the **upgrade** keyword is specified, a chassis flag is set for the BOOT Loader (boot.ldr) and on the subsequent boot of the 7750 SR OS on the chassis, firmware images on CPMs or IOMs will be upgraded automatically.

Any CPMs that are installed in the chassis will be upgraded automatically. For example, if a card is inserted with down revision firmware as a result of a card hot swap with the latest OS version running, the firmware on the card will be automatically upgraded before the card is brought online.

If the card firmware is upgraded automatically, a chassis cardUpgraded (event 2032) log event is generated. The corresponding SNMP trap for this log event is tmnxEqCardFirmwareUpgraded.

During any firmware upgrade, automatic or manual, it is imperative that during the upgrade procedure:

- Power must NOT be switched off or interrupted.
- The system must NOT be reset.
- No cards are inserted or removed.

Any of the above conditions may render cards inoperable requiring a return of the card for resolution.

The time required to upgrade the firmware on the cards in the chassis depends on the number of cards to be upgraded. The progress of a firmware upgrade can be monitored at the console.

now — Forces a reboot of the router immediately without an interactive confirmation.

save

Syntax **save** [*file-url*] [**detail**] [**index**]

Context admin

Description This command saves the running configuration to a configuration file. For example:

```
A:ALA-1>admin# save ftp://test:test@192.168.x.xx/./100.cfg
Saving configuration .........Completed.
```

By default, the running configuration is saved to the primary configuration file.

Parameters *file-url* — The file URL location to save the configuration file.

Default The primary configuration file location.

Values

file url:	local-url | remote-url: 255 chars max	
local-url:	[*cflash-id*/][*file-path*], 200 chars max, including the cflash-id directory length, 99 chars max each	
remote-url:	[{ftp://} login:pswd@remote-locn/][file-path]	
	remote-locn [*hostname* | *ipv4-address* | [*ipv6- address*]]	
	ipv4-address	a.b.c.d
	ipv6-address -	x:x:x:x:x:x:x:x[-interface]
		x:x:x:x:x:x:d.d.d.d[-interface]
		x - [0..FFFF]H
		d - [0..255]D
		interface - 32 chars max, for link local addresses
	255 chars max, directory length 99 chars max each	
cflash-id:	cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:	

detail — Saves both default and non-default configuration parameters.

index — Forces a save of the persistent index file regardless of the persistent status in the BOF file. The index option can also be used to avoid an additional boot required while changing your system to use the persistence indices.

enable-tech

Syntax [**no**] **enable-tech**

Context admin

Description This command enables the shell and kernel commands.

NOTE: This command should only be used with authorized direction from the Alcatel-Lucent Technical Assistance Center (TAC).

radius-discovery

Syntax **radius-discovery**

Context admin

Description This command performs RADIUS discovery operations.

force-discover

Syntax **force-discover** [**svc-id** *service-id*]

Context admin>radius-discovery

Description When enabled, the server is immediately contacted to attempt discovery.

Parameters **svc-id** *service-id* — Specifies an existing service ID.

Values 1 — 2147483648 | *svc-name*, up to 64 char max

tech-support

Syntax **tech-support** *file-url*

Context admin

Description This command creates a system core dump.

NOTE: This command should only be used with authorized direction from the Alcatel-Lucent Technical Assistance Center (TAC).

file-url — The file URL location to save the binary file.

file url:	local-url | remote-url: 255 chars max	
local-url:		[*cflash-id*/][*file-path*], 200 chars max, including the cflash-id directory length, 99 chars max each

remote-url: [{ftp://} login:pswd@remote-locn/][file-path]
remote-locn [*hostname* | *ipv4-address* | [*ipv6- address*]]
ipv4-address a.b.c.d
ipv6-address - x:x:x:x:x:x:x:x[-interface]
x:x:x:x:x:x:d.d.d.d[-interface]
x - [0..FFFF]H
d - [0..255]D
interface - 32 chars max, for link local addresses
255 chars max, directory length 99 chars max each
cflash-id: cf1:, cf1-A:,cf1-B:,cf2:,cf2-A:,cf2-B:,cf3:,cf3-A:,cf3-B:

view

Syntax **view** {**bootup-cfg|active-cfg|candidate-cfg|latest-rb|** *checkpoint-id***|rescue**}

Context <ROOT>

Description The context to configure administrative system viewing parameters. Only authorized users can execute the commands in the **admin** context.

Default none

Parameters **bootup-cfg —** Specifies the bootup configuration.

active-cfg — Specifies current running configuration.

candidate-cfg — Specifies candidate configuration.

latest-rb — Specifies the latest configuration.

***checkpoint-id* —** Specifies a specific checkpoint file configuration.

Values 1 — 9

rescue — Specifies a rescue checkpoint configuration.

Persistence Commands

persistence

Syntax [**no**] **persistence**

Context config>system

Description This command enables the context to configure persistence parameters on the system.

The persistence feature enables state on information learned through DHCP snooping across reboots to be retained. This information includes data such as the IP address and MAC binding information, lease-length information, and ingress sap information (required for VPLS snooping to identify the ingress interface).

If persistence is enabled when there are no DHCP relay or snooping commands enabled, it will simply create an empty file.

Default no persistence

ancp

Syntax **ancp**

Context config>system>persistence

Description This command configures ANCP persistence parameters.

application-assurance

Syntax **application-assurance**

Context config>system>persistence

Description This command configures application assurance persistence parameters.

dhcp-server

Syntax **dhcp-server**

Context config>system>persistence

Description This command configures DHCP server persistence parameters.

nat-port-forwarding

Syntax **nat-port-forwarding**

Context config>system>persistence

Description This command configures NAT port forwarding persistence parameters.

subscriber-mgmt

Syntax **subscriber-mgmt**

Context config>system>persistence

Description This command configures subscriber management persistence parameters.

location

Syntax **location** [**cf1:** | **cf2:** | **cf3:**]
no location

Context config>system>persistence>ancp
config>system>persistence>sub-mgmt
config>system>persistence>dhcp-server

Description This command instructs the system where to write the file. The name of the file is: dhcp-persistence.db. On boot the system scans the file systems looking for dhcp-persistence.db, if it finds it starts to load it.

In the subscriber management context, the location specifies the flash device on a CPM card where the data for handling subscriber management persistency is stored.

The **no** form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.

Default no location

PTP Commands

ptp

Syntax **ptp**

Context config>system

Description This command enables the context to configure parameters for IEEE 1588-2008, Precision Time Protocol.

This command is only available on the control assemblies that support 1588.

shutdown

Syntax [**no**] **shutdown**

Context config>system>ptp

Description This command disables or enables the PTP protocol. If PTP is disabled, the router will not transmit any PTP packets, and will ignore all received PTP packets. If the user attempts execute a **no shutdown** command on hardware that does not support PTP, an alarm will be raised to indicate limited capabilities.

When PTP is shutdown, the PTP slave port is not operational. It shall not be considered as a source for system timing.

Default shutdown

clock-type

Syntax **clock-type ordinary** {{**master** | **slave**} | **boundary**}

Context config>system>ptp

Description This command configures the type of clock. The clock-type can only be changed when PTP is shutdown.

The clock-type cannot be changed to master-only if PTP reference is no shutdown. In addition, clock-type cannot be changed to master-only if there are peers configured.

Default ordinary slave

Parameters **boundary —** The system is a boundary clock, which may be anywhere in the master-slave clock hierarchy. It can obtain timing from a master clock, and provide timing to multiple slave clocks concurrently.

ordinary master — The system is a grandmaster clock in the master-slave hierarchy. The system provides timing to multiple slave clocks in the network.

ordinary slave — The system is always a slave clock in the master-slave hierarchy. The system derives its timing from one or more master clocks in the network.

domain

Syntax [**no**] **domain** *domain*

Context config>system>ptp

Description This command configures the PTP domain.

The **no** form of the command reverts to the default configuration. Note some profiles may require a domain number in a restricted range. It is up to the operator to ensure the value aligns with what is expected within the profile.

Domain cannot be changed unless PTP is shutdown. If the PTP profile is changed, the domain is changed to the default domain for the new PTP profile.

Default 0 for ieee1588-2008 or 4 for g.8265.1-2010

Parameters *domain* — The PTP domain.

Values 0 — 255

network-type

Syntax **network-type** {**sdh** | **sonet**}

Context config>system>ptp

Description This command configures the codeset to be used for the encoding of QL values into PTP clockClass values when the profile is configured for G.8265.1. The codeset is defined in Table 1/G.8265.1. This setting only applies to the range of values observed in the clockClass values transmitted out of the node in Announce messages. The 7750 will support the reception of any valid value in Table 1/G.8265.1

Default sdh

Parameters **sdh** — Specifies the values used on a G.781 Option 1 compliant network.

sonet — Specifies the values used on a G.781 Option 2 compliant network

priority1

Syntax [**no**] **priority1** *priority*

Context config>system>ptp

This command configures the priority1 value of the local clock. This parameter is only used when the profile is set to ieee1588-2008. This value is used by the Best Master Clock Algorithm to determine which clock should provide timing for the network.

Note: This value is used for the value to advertise in the Announce messages and for the local clock value in data set comparisons.

The **no** form of the command reverts to the default configuration.

Default 128

Parameters *priority* — Specifies the value of the priority1 field.

Values 0 — 255

priority2

Syntax [**no**] **priority2** *priority*

Context config>system>ptp

This command configures the priority2 value of the local clock. This parameter is only used when the profile is set to ieee1588-2008. This value is used by the Best Master Clock algorithm to determine which clock should provide timing for the network.

Note: This value is used for the value to advertise in the Announce messages and for local clock value in data set comparisons..

The no form of the command reverts to the default configuration.

Default 128

Parameters *priority* — Specifies the value of the priority2 field.

Values 0 — 255

profile

Syntax **profile** {**g8265dot1-2010** | **ieee1588-2008**}

Context config>system>ptp

Description This command configures the profile to be used for the internal PTP clock. It defines the BMCA behavior.

The profile cannot be changed unless PTP is shutdown.

When you change the profile, the domain changes to the default value for the new profile.

Default ieee1588-2008

Parameters ieee1588-2008 — Conform to the default BMCA of the 2008 version of the IEEE1588 standard.

g.8265.1-2010 — Conform to the BMCA specified in the ITU-T G.8264.1 specification.

peer

Syntax **peer** *ip-address*

Context config>system>ptp

This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer.

Up to 20 remote PTP peers may be configured.

The no form of the command deletes the specified peer.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last peer cannot be deleted. This prevents the user from having PTP enabled without any peer configured & enabled.

Peers cannot be created when the clock-type is ordinary master.

Default none

Parameters *ip-address* — The IP address of the remote peer.

Values ipv4-address a.b.c.d

priority

Syntax **priority** *local_priority*

Context configure>system>ptp>peer

This command configures the local priority used to choose between PTP masters in the best master clock algorithm (BMCA). This setting is only relevant when the g.8265.1-2010 profile is selected. The parameter is ignored when the ieee1588-2008 profile is selected. The value 1 is the highest priority and 255 is the lowest priority. The priority of a peer cannot be configured if the PTP profile is ieee1588-2008

Default 128

Parameters *local_priority* — Specifies the value of the local priority.

Values 1-255

profile

Syntax **profile {ieee1588-2008 | g.8265.1-2010}**

Context configure>system>ptp

Description This command configures the profile to be used for the internal ptp clock. This principally defines the BMCA behavior.

The profile cannot be changed unless ptp is shutdown.

When the profile is changed, the domain is changed to the default value for the new profile. In addition, if the profile is changed to ieee1588-2008, the wait-to-restore timer is disabled.

Profile may only be set to g.8265.1-2010 when the clock is Ordinary-Slave or Ordinary-Master.

Default ieee1588-2008

Parameters **ieee1588-2008 —** Conforms to the default BMCA of the 2008 version of the IEEE1588 standard.

g.8265.1-2010 — Conforms to the BMCA specified in the ITU-T G.8265.1 specification.

shutdown

Syntax [**no**] **shutdown**

Context configure>system>ptp>peer

This command disables or enables a specific PTP peer. Shutting down a peer sends cancel unicast negotiation messages on any established unicast sessions. When shutdown, all received packets from the peer are ignored.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last enabled peer cannot be shutdown. This prevents the user from having PTP enabled without any peer configured & enabled

Default no shutdown

Redundancy Commands

redundancy

Syntax **redundancy**

Context admin
config

Description This command enters the context to allow the user to perform redundancy operations.

cert-sync

Syntax [**no**] **cert-sync**

Context admin>redundancy

Description This command automatically synchronizes the certificate/CRL/key automatically when importing or generating (for the key); also, if there is new CF card inserted into slot3 into backup CPM, the system will sync the whole system-pki directory from the active CPM.

Default none

rollback-sync

Syntax **no rollback-sync**

Context admin>redundancy

Description This command copies the entire set of rollback checkpoint files from the active CPM CF to the inactive CPM CF.

Default None.

synchronize

Syntax **synchronize** {**boot-env|config**}
no synchronize

Context admin>redundancy

Description This command performs a synrchonization of the standby CPM's images and/or configuration files to the active CPM. Either the **boot-env** or **config** parameter must be specified.

In the **admin>redundancy** context, this command performs a manually triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPM have identical operational parameters. This includes the saved configuration, CPM and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM. If synchronization fails, alarms and log messages that indicate the type of error that caused the failure of the synchronization operation are generated. When the error condition ceases to exist, the alarm is cleared.

Only files stored on the router are synchronized. If a configuration file or image is stored in a location other than on a local compact flash, the file is not synchronized (for example, storing a configuration file on an FTP server).

The **no** form of the command removes the parameter from the configuration.

Default none

Parameters **boot-env —** Synchronizes all files required for the boot process (loader, BOF, images, and config).

config — Synchronizes only the primary, secondary, and tertiary configuration files.

force-switchover

Syntax **force-switchover** [**now**]

Context admin>redundancy

Description This command forces a switchover to the standby CPM card. The primary CPM reloads its software image and becomes the secondary CPM.

Parameters **now —** Forces the switchover to the redundant CPM card immediately.

bgp-multi-homing

Syntax **bgp-multi-homing**

Context config>redundancy

Description This command configures BGP multi-homing parameters.

boot-timer

Syntax **boot-timer** *seconds*
no boot-timer

Context config>redundancy>bgp-multi-homing

Description This command configures the time the service manger waits after a node reboot before running the DF election algorithm. The boot-timer value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed/exchanged.

The **no** form of the command reverts the default.

Default no boot-timer

Parameters *seconds* — Specifies the BGP multi-homing boot-timer in seconds.

Values 1 — 100

site-activation-timer

Syntax **site-activation-timer** *seconds*
no site-activation-timer

Context config>redundancy>bgp-multi-homing

Description This command defines the amount of time the service manager will keep the local sites in standby status, waiting for BGP updates from remote PEs before running the DF election algorithm to decide whether the site should be unblocked. The timer is started when one of the following events occurs if the site is operationally up:

- Manual site activation using the **no shutdown** command at site-id level or at member object(s) level (SAP(s) or PW(s))
- Site activation after a failure

Default no site-activation-timer

Parameters *seconds* — Specifies the standby status in seconds.

Values 1 — 100

Default 2

synchronize

Syntax **synchronize** {**boot-env | config**}

Context config>redundancy

Description This command performs a synrchonization of the standby CPM's images and/or config files to the active CPM. Either the **boot-env** or **config** parameter must be specified.

In the **config>redundancy** context, this command performs an automatically triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPMs have identical operational parameters. This includes the saved configuration, CPM and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM.

If synchronization fails, alarms and log messages that indicate the type of error that caused the failure of the synchronization operation are generated. When the error condition ceases to exist, the alarm is cleared.

Only files stored on the router are synchronized. If a configuration file or image is stored in a location other than on a local compact flash, the file is not synchronized (for example, storing a configuration file on an FTP server).

Default enabled

Parameters **boot-env —** Synchronizes all files required for the boot process (loader, BOF, images, and config).

config — Synchronize only the primary, secondary, and tertiary configuration files.

Default **config**

synchronize

Syntax **synchronize** {**boot-env | config**}

Context admin>redundancy

Description This command performs a synrchonization of the standby CPM's images and/or config files to the active CPM. Either the **boot-env** or **config** parameter must be specified.

In the **admin>redundancy** context, this command performs a manually triggered standby CPM synchronization. When the standby CPM takes over operation following a failure or reset of the active CPM, it is important to ensure that the active and standby CPM have identical operational parameters. This includes the saved configuration, CPM and IOM images.

The active CPM ensures that the active configuration is maintained on the standby CPM. However, to ensure smooth operation under all circumstances, runtime images and system initialization configurations must also be automatically synchronized between the active and standby CPM.

If synchronization fails, alarms and log messages that indicate the type of error that caused the failure of the synchronization operation are generated. When the error condition ceases to exist, the alarm is cleared.

Only files stored on the router are synchronized. If a configuration file or image is stored in a location other than on a local compact flash, the file is not synchronized (for example, storing a configuration file on an FTP server).

Default none

Parameters **boot-env —** Synchronizes all files required for the boot process (loader, BOF, images, and configuration files.

config — Synchronize only the primary, secondary, and tertiary configuration files.

multi-chassis

Syntax **multi-chassis**

Context config>redundancy

Description This command enables the context to configure multi-chassis parameters.

peer-name

Syntax **peer-name** *name*
no peer-name

Context config>redundancy>multi-chassis>peer

Description This command specifies a peer name.

Parameters *name* — The string may be up to 32 characters long. Any printable, seven-bit ASCII characters can be used within the string. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

rollback-sync

Syntax [**no**] **rollback-sync**

Context config>redundancy

Description The operator can enable automatic synchronization of rollback checkpoint files between the active CPM and inactive CPM. When this automatic synchronization is enabled, a rollback save will cause the new checkpoint file to be saved on both the active and standby CPMs. The suffixes of the old checkpoint files on both active and standby CPMs are incremented. Note that automatic sync only causes the ONE new checkpoint file to be copied to both CFs (the other 9 checkpoints are not automatically copied from active to standby but that can be done manually with "admin red rollback-sync").

Automatic synchronization of rollback checkpoint files across CPMs is only performed if the rollback-location is configured as a local file-url (for example, "cf3:/rollback-files/rollback). Synchronization is not done if the rollback-location is remote.

Note that “config red sync {boot-env|config}” and “admin red sync {boot-env|config}” do not apply to rollback checkpoint files. These commands do not manually or automatically sync rollback checkpoint files. The dedicated rollback-sync commands must be used to sync rollback checkpoint files.

source-address

Syntax **source-address** *ip-address*
no source-address

Context config>redundancy>multi-chassis>peer

Description This command specifies the source address used to communicate with the multi-chassis peer.

Parameters *ip-address* — Specifies the source address used to communicate with the multi-chassis peer.

sync

Syntax [**no**] **sync**

Context config>redundancy>multi-chassis>peer

Description This command enables the context to configure synchronization parameters.

igmp

Syntax [**no**] **igmp**

Context config>redundancy>multi-chassis>peer>sync

Description This command specifies whether IGMP protocol information should be synchronized with the multi-chassis peer.

Default no igmp

igmp-snooping

Syntax [**no**] **igmp-snooping**

Context config>redundancy>multi-chassis>peer>sync

Description This command specifies whether IGMP snooping information should be synchronized with the multi-chassis peer.

Default no igmp-snooping

local-dhcp-server

Syntax [**no**] **local-dhcp-server**

Context config>redundancy>multi-chassis>peer>sync

Description This command synchronizes DHCP server information.

mld-snooping

Syntax [**no**] **mld-snooping**

Context config>redundancy>multi-chassis>peer>sync

Description This command synchronizes MLD Snooping information.

port

Syntax **port** [*port-id* | *lag-id*] [**sync-tag** *sync-tag*]
no port [*port-id* | *lag-id*]

Context config>redundancy>multi-chassis>peer>sync

Description This command specifies the port to be synchronized with the multi-chassis peer and a synchronization tag to be used while synchronizing this port with the multi-chassis peer.

Parameters *port-id* — Specifies the port to be synchronized with the multi-chassis peer.

lag-id — Specifies the LAG ID to be synchronized with the multi-chassis peer.

sync-tag *sync-tag* **—** Specifies a synchronization tag to be used while synchronizing this port with the multi-chassis peer.

range

Syntax **range** *encap-range* **sync-tag** *sync-tag*
no range *encap-range*

Context config>redundancy>multi-chassis>peer>sync>port

Description This command configures a range of encapsulation values.

Parameters *encap-range* — Specifies a range of encapsulation values on a port to be synchronized with a multi-chassis peer.

Values	Dot1Q	*start-vlan-end-vlan*
	QinQ	Q1.*start-vlan*-Q1.*end-vlan*

sync-tag *sync-tag* **—** Specifies a synchronization tag up to 32 characters in length to be used while synchronizing this encapsulation value range with the multi-chassis peer.

srrp

Syntax [**no**] **srrp**

Context config>redundancy>multi-chassis>peer>sync

Description This command specifies whether subscriber routed redundancy protocol (SRRP) information should be synchronized with the multi-chassis peer.

Default no srrp

sub-mgmt

Syntax [**no**] **sub-mgmt**

Context config>redundancy>multi-chassis>peer>sync

Description This command specifies whether subscriber management information should be synchronized with the multi-chassis peer.

Default no sub-mgmt

sub-host-trk

Syntax [**no**] **sub-host-trk**

Context config>redundancy>multi-chassis>peer>sync

Description This command specifies whether subscriber host tracking information should be synchronized with the multi-chassis peer.

Default no sub-mgmt

Peer Commands

peer

Syntax [**no**] **peer** *ip-address*

Context config>redundancy>multi-chassis

Description This command configures a multi-chassis redundancy peer.

Parameters *ip-address* — Specifies a peer IP address. Multicast address are not allowed.

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
no authentication-key

Context config>redundancy>multi-chassis>peer

Description This command configures the authentication key used between this node and the multi-chassis peer. The authentication key can be any combination of letters or numbers.

Parameters *authentication-key* — Specifies the authentication key. Allowed values are any string up to 20 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hash-key — The hash key. The key can be any combination of ASCII characters up to 33 (hash1-key) or 55 (hash2-key) characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash — Specifies the key is entered in an encrypted form. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables then the key value alone, this means that hash2 encrypted variable cannot be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash or hash2 parameter specified.

MC Endpoint Commands

mc-endpoint

Syntax [**no**] **mc-endpoint**

Context config>redundancy>multi-chassis>peer

Description This command specifies that the endpoint is multi-chassis. This value should be the same on both MC-EP peers for the pseudowires that must be part of the same group.

The **no** form of this command removes the endpoint from the MC-EP. Single chassis behavior applies.

bfd-enable

Syntax [**no**] **bfd-enable**

Context config>redundancy>multi-chassis>peer>mc-ep
config>router>rsvp
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor
config>redundancy>multi-chassis>peer>mc-ep

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command disables BFD.

Default no bfd-enable

boot-timer

Syntax **boot-timer** *interval*
no boot-timer

Context config>redundancy>multi-chassis>peer>mc-ep

Description This command configures the boot timer interval. This command applies only when the node reboots. It specifies the time the MC-EP protocol keeps trying to establish a connection before assuming a failure of the remote peer. This is different from the keep-alives mechanism which is used just after the peer-peer communication was established. After this time interval passed all the mc-endpoints configured under services will revert to single chassis behavior, activating the best local PW.

The **no** form of this command sets the interval to default.

Default 300

Parameters *interval* — Specifies the boot timer interval.

Values 1 — 600

hold-on-neighbor-failure

Syntax **hold-on-neighbor-failure** *multiplier*
no hold-on-neighbor-failure

Context config>redundancy>multi-chassis>peer>mc-ep

Description This command specifies the number of keep-alive intervals that the local node will wait for packets from the MC-EP peer before assuming failure. After this time interval passed the all the mc-endpoints configured under services will revert to single chassis behavior, activating the best local pseudowire.

The **no** form of this command sets the multiplier to default value

Default 3

Parameters *multiplier* — Specifies the hold time applied on neighbor failure.

Values 2 — 25

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context config>redundancy>multi-chassis>peer>mc-ep

Description This command sets the interval at which keep-alive messages are exchanged between two systems participating in MC-EP when bfd is not enabled or is down. These fast keep-alive messages are used to determine remote-node failure and the interval is set in deci-seconds.

The **no** form of this command sets the interval to default value

Default 5 (0.5s)

Parameters *interval* — The time interval expressed in deci-seconds.

Values 5 — 500 (tenths of a second)

passive-mode

Syntax [**no**] **passive-mode**

Context config>redundancy>multi-chassis>peer>mc-ep

Description This command configures the passive mode behavior for the MC-EP protocol. When in passive mode the MC-EP pair will be dormant until two of the pseudowires in a MC-EP will be signaled as active by the remote PEs, being assumed that the remote pair is configured with regular MC-EP. As soon as more than one pseudowire is active, dormant MC-EP pair will activate. It will use the regular exchange to select the best pseudowire between the active ones and it will block the Rx and Tx directions of the other pseudowires.

The **no** form of this command will disable the passive mode behavior.

Default no passive-mode

system-priority

Syntax **system-priority** *value*
no system-priority

Context config>redundancy>multi-chassis>peer>mc-ep

Description This command allows the operator to set the system priority. The peer configured with the lowest value is chosen to be the master. If system-priority are equal then the one with the highest system-id (chassis MAC address) is chosen as the master.

The **no** form of this command sets the system priority to default

Default no system-priority

Parameters *value* — Specifies the priority assigned to the local MC-EP peer.

Values 1 — 255

MC-LAG Commands

mc-lag

Syntax [**no**] **mc-lag**

Context config>redundancy>multi-chassis>peer>mc-lag

Description This command enables the context to configure multi-chassis LAG operations and related parameters.

The **no** form of this command administratively disables multi-chassis LAG. MC-LAG can only be issued only when mc-lag is shutdown.

hold-on-neighbor-failure

Syntax **hold-on-neighbor-failure** *multiplier*
no hold-on-neighbor-failure

Context config>redundancy>multi-chassis>peer>mc-lag

Description This command specifies the interval that the standby node will wait for packets from the active node before assuming a redundant-neighbor node failure. This delay in switch-over operation is required to accommodate different factors influencing node failure detection rate, such as IGP convergence, or HA switch-over times and to prevent the standby node to take action prematurely.

The **no** form of this command sets this parameter to default value.

Default 3

Parameters *multiplier* — The time interval that the standby node will wait for packets from the active node before assuming a redundant-neighbor node failure.

Values 2 — 25

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context config>redundancy>multi-chassis>peer>mc-lag

Description This command sets the interval at which keep-alive messages are exchanged between two systems participating in MC-LAG. These keep-alive messages are used to determine remote-node failure and the interval is set in deci-seconds.

The **no** form of this command sets the interval to default value

Default 1s (10 hundreds of milliseconds means interval value of 10)

Parameters *interval* — The time interval expressed in deci-seconds

Values 5 — 500

lag

Syntax **lag** *lag-id* **lacp-key** *admin-key* **system-id** *system-id* [**remote-lag** *lag-id*] **system-priority** *system-priority*
no lag *lag-id*

Context config>redundancy>multi-chassis>peer>mc-lag

Description This command defines a LAG which is forming a redundant-pair for MC-LAG with a LAG configured on the given peer. The same LAG group can be defined only in the scope of 1 peer.

The same **lacp-key**, **system-id**, and **system-priority** must be configured on both nodes of the redundant pair in order to MC-LAG to become operational. In order MC-LAG to become operational, all parameters (**lacp-key**, **system-id**, **system-priority**) must be configured the same on both nodes of the same redundant pair.

The partner system (the system connected to all links forming MC-LAG) will consider all ports using the same **lacp-key**, **system-id**, **system-priority** as the part of the same LAG. In order to achieve this in MC operation, both redundant-pair nodes have to be configured with the same values. In case of the mismatch, MC-LAG is kept operationally down.

Default none

Parameters *lag-id* — The LAG identifier, expressed as a decimal integer. Specifying the *lag-id* allows the mismatch between lag-id on redundant-pair. If no **lag-id** is specified it is assumed that neighbor system uses the same *lag-id* as a part of the given MC-LAG. If no matching MC-LAG group can be found between neighbor systems, the individual LAGs will operate as usual (no MC-LAG operation is established.).

Values 1 — 200

lacp-key ***admin-key*** **—** Specifies a 16 bit key that needs to be configured in the same manner on both sides of the MC-LAG in order for the MC-LAG to come up.

Values 1 — 65535

system-id ***system-id*** **—** Specifies a 6 byte value expressed in the same notation as MAC address

Values xx:xx:xx:xx:xx:xx - xx [00..FF]

remote-lag ***lag-id*** **—** Specifies the LAG ID on the remote system.

Values 1 — 200

system-priority ***system-priority*** **—** Specifies the system priority to be used in the context of the MC-LAG. The partner system will consider all ports using the same **lacp-key**, **system-id**, and **system-priority** as part of the same LAG.

Values 1 — 65535

Multi-Chassis Mobile Commands

mc-mobile

Syntax **mc-mobile**

Context config>redundancy>mc>peer

Description This command enables to the context to configure mc-mobile parameters.

Default no mc-mobile

bfd-enable

Syntax **bfd-enable** [**service** <*service-id*>] **interface** <*interface-name*>
no bfd-enable

Context config>redundancy>multi-chassis>peer>mc-mobile

Description This command enables the use of Bi-directional Forwarding Detection (BFD) to be associated with the peer. The mc-mobile redundancy protocol will use the BFD state to determine liveliness of its peer. The parameters for the BFD session are set via the BFD command under the IP interface configuration.

Default no bfd-enable

Parameters *service-id* — Specifies the service identifier string, maximum of 64 characters.

Values 1—2147483648

interface-name — Specifies the interface name, maximum of 32 characters.

hold-on-neighbor-failure

Syntax **hold-on-neighbor-failure** *multiplier*
no hold-on-neighbor-failure

Context config>redundancy>multi-chassis>peer>mc-mobile

Description This command specifies the number of keep-alive-intervals that may expire before the local node decides that the peer has failed. A peer failure will be declared if no keep-alive responses are received after hold-on-neighbor-failure x keep-alive-interval.

Default 3

Parameters *multiplier* — Specifies the multiplier.

Values 2—25

keep-alive-interval

Syntax **keep-alive-interval** *interval*
no keep-alive-interval

Context config>redundancy>multi-chassis>peer>mc-mobile

Description This command sets the interval at which keep-alive messages are sent to the peer when bfd is not enabled or is down.

Default 10 (1 second)

Parameters *interval* — The time interval expressed in deci-seconds.

Values 5—500 (tenths of a second)

Multi-Chassis Ring Commands

mc-ring

Syntax **mc-ring**

Context config>redundancy>mc>peer
config>redundancy>multi-chassis>peer>sync

Description This command enables the context to configure the multi-chassis ring parameters.

ring

Syntax **ring** *sync-tag*
no ring *sync-tag*

Context config>redundancy>mc>peer>mcr

Description This command configures a multi-chassis ring.

Parameters *sync-tag* — Specifies a synchronization tag to be used while synchronizing this port with the multi-chassis peer.

in-band-control-path

Syntax **in-band-control-path**

Context config>redundancy>mc>peer>mcr>ring

Description This command enables the context to configure multi-chassis ring inband control path parameters.

dst-ip

Syntax **dst-ip** *ip-address*
no dst-ip

Context config>redundancy>mc>peer>mcr>ring>in-band-control-path

Description This command specifies the destination IP address used in the inband control connection. If the address is not configured, the ring cannot become operational.

Parameters *ip-address* — Specifies the destination IP address.

interface

Syntax **interface** *ip-int-name*
no interface

Context config>redundancy>mc>peer>mcr>ring>in-band-control-path

Description This command specifies the name of the IP interface used for the inband control connection.If the name is not configured, the ring cannot become operational.

service-id

Syntax **service-id** *service-id*
no service-id

Context config>redundancy>mc>peer>mcr>ring>ibc

Description This command specifies the service ID if the interface used for the inband control connection belongs to a VPRN service. If not specified, the *service-id* is zero and the interface must belong to the Base router.

The **no** form of the command removes the service-id from the IBC configuration.

Parameters *service-id* — Specifies the service ID if the interface.

path-b

Syntax [**no**] **path-b**

Context config>redundancy>mc>peer>mcr>ring

Description This command specifies the set of upper-VLAN IDs associated with the SAPs that belong to path B with respect to load-sharing. All other SAPs belong to path A.

Default If not specified, the default is an empty set.

range

Syntax [**no**] **range** *vlan-range*

Context config>redundancy>mc>peer>mcr>ring>path-b
config>redundancy>mc>peer>mcr>ring>path-excl

Description This command configures a MCR b-path VLAN range.

Parameters *vla-range* — Specifies the VLAN range.

Values 1 to 4094 — 1 to 4094

path-excl

Syntax [**no**] **path-excl**

Context config>redundancy>mc>peer>mcr>ring

Description This command specifies the set of upper-VLAN IDs associated with the SAPs that are to be excluded from control by the multi-chassis ring.

Default If not specified, the default is an empty set.

ring-node

Syntax **ring-node** *ring-node-name* [**create**]
no ring-node *ring-node-name*

Context config>redundancy>mc>peer>mcr>ring

Description This command specifies the unique name of a multi-chassis ring access node.

Parameters *ring-node-name* — Specifies the unique name of a multi-chassis ring access node.

create — Keyword used to create the ring node instance. The **create** keyword requirement can be enabled/disabled in the **environment**>**create** context.

connectivity-verify

Syntax **connectivity-verify**

Context config>redundancy>mc>peer>mcr>ring>ring-node

Description This command enables the context to configure node connectivity check parameters.

dst-ip

Syntax **dst-ip** *ip-address*
no dst-ip

Context config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify

Description This command configures the node cc destination IP address.

Default no dst-ip

Parameters *ip-address* — Specifies the destination IP address used in the inband control connection.

interval

Syntax **interval** *interval*
no interval

Context config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify

Description This command specifies the polling interval of the ring-node connectivity verification of this ring node.

Default 5

Parameters *interval* — Specifies the polling interval, in minutes.

Values 1 — 6000

service-id

Syntax **service-id** *service-id*
no service-id

Context config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify

Description This command specifies the service ID of the SAP used for the ring-node connectivity verification of this ring node.

Default no service-id

Parameters *service-id* — Specifies the service ID of the SAP.

Values 1 — 2147483647

src-ip

Syntax **src-ip** *ip-address*
no src-ip

Context config>redundancy>mc>peer>mcr>ring>ring-node>connectivity-verify

This command specifies the source IP address used in the ring-node connectivity verification of this ring node.

Default no src-ip

Parameters *ip-address* — Specifies the address of the multi-chassis peer.

src-mac

Syntax **src-mac** *ieee-address*
no src-mac

Context config>redundancy>mc>peer>mcr>node>cv

Description This command specifies the source MAC address used for the Ring-Node Connectivity Verification of this ring node.

A value of all zeroes (000000000000 H (0:0:0:0:0:0)) specifies that the MAC address of the system management processor (CPM) is used.

Default no src-mac

Parameters *ieee-address* — Specifies the source MAC address.

vlan

Syntax **vlan** [**0..4094**]
no vlan

Context config>redundancy>mc>peer>mcr>node>cv

Description This command specifies the VLAN tag of the SAP used for the ring-node connectivity verification of this ring node. It is only meaningful if the value of service ID is not zero. A zero value means that no VLAN tag is configured.

Default no vlan

Parameters [**0..4094**] — Specifies the set of VLAN IDs associated with the SAPs that are to be controlled by the slave peer.

Rollback Commands

compare

Syntax **compare** [**to** *source2*]
compare *source1* **to** *source2*

Context admin
admin>rollback

Description This command displays the differences between rollback checkpoints and the active operational configuration, with source1 as the base/first file to which source2 is compared.

Parameters *source1, source2* — Specifies comparison information.

Values **active-cfg** — The currently operational configuration that is active in the node.

latest-rb — The most recent rollback checkpoint (the checkpoint file at the configured rollback-location with "*.rb" as the suffix).

rescue— The rescue configuration (at the configured rescue-location).

checkpoint-id — An id from [1 ..max] indicating a specific rollback checkpoint (where max is the highest checkpoint allowed/configured). A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback-location) with "*.rb.1" as the suffix, 2 for file "*.rb.2", etc.

Default The defaults for source1 and source2 are context aware and differ based on the branch in which the command is executed. In general, the default for source1 matches the context from which the command is issued.

- In the admin node: No defaults. source1 and source2 must be specified.
- In the admin>rollback node:

  source1 default = active-cfg, source2 default = lastest-rb

  compare: Equivalent to "compare active-cfg to lastest-rb"

  compare to source2:Equivalent to "compare active-cfg to source2"

delete

Syntax **delete {latest-rb|** *checkpoint-id* **| rescue}**

Context admin>rollback

Description This command deletes a rollback checkpoint and causes the suffixes to be adjusted (decremented) for all checkpoints older that the one that was deleted (to close the "hole" in the list of checkpoint files and create room to create another checkpoint).

If "**config redundancy rollback-sync**" is enabled, a rollback delete will also delete the equivalent checkpoint on the standby CF and shuffle the suffixes on the standby CF.

It is not advised to manually delete a rollback checkpoint (for example, using a "file delete" command). If a rollback checkpoint file is manually deleted without using the "admin rollback delete" command then the suffixes of the checkpoint files are NOT shuffled, nor is the equivalent checkpoint file deleted from the standby CF. This manual deletion creates a "hole" in the checkpoint file list until enough new checkpoints have been created to roll the "hole" off the end of the list.

Default none

Parameters **latest-rb —** Specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file).

checkpoint-id — An id from [1 ..max] indicating a specific rollback checkpoint (where max is the highest checkpoint allowed/configured). A checkpoint-id of 1 indicates the rollback checkpoint file (at the configured rollback-location) with "*.rb.1" as the suffix, 2 for file "*.rb.2", etc.

rescue — Deletes the rescue checkpoint. No checkpoint suffix numbers are changed.

rollback-location

Syntax **no rollback-location** *file-url*

Context config>system>rollback

Description The location and name of the rollback checkpoint files is configurable to be local (on compact flash) or remote. The file-url must not contain a suffix (just a path/directory + filename). The suffixes for rollback checkpoint files are ".rb", ".rb.1", ..., ".rb.9" and are automatically appended to rollback checkpoint files.

Default None. A valid rollback-location must be configured before a rollback save is executed.

rescue-location

Syntax **no rescue-location** *file-url*

Context config>system>rollback

Description The location and filename of the rescue configuration is configurable to be local (on compact flash)or remote. The suffix ".rc" will be automatically appended to the filename when a rescue configuration file is saved. Trivial FTP (tftp) is not supported for remote locations.

Default None. A valid rescue-location must be configured before a rescue configuration is saved.

remote-max-checkpoints

Syntax **remote-max-checkpoints** *<1..200>*

Context config>system>rollback

Description Configures the maximum number of rollback checkpoint files when the rollback-location is remote (e.g. ftp).

Default 10

local-max-checkpoints

Syntax **local-max-checkpoints** *<1..50>*

Context config>system>rollback

Description Configures the maximum number of rollback checkpoint files when the rollback-location is on local compact flash.

Default 10

save

Syntax **save** [**rescue**] [**comment** *comment-string*]

Context admin>rollback

Description If the optional "rescue" keyword is not used, this command saves a rollback checkpoint at the location and with the filename specified by the rollback-location with a suffix of ".rb". The previously saved checkpoints will have their suffixes incremented by one (.rb.1 becomes .rb.2, etc). If there are already as many checkpoint files as the maximum number supported, then the last checkpoint file is deleted.

If the "rescue" keyword is used, then this command saves the current operational configuration as a rescue configuration at the location and with the filename specified by the rescue-location. The filename will have the suffix ".rc" appended.

Default none

Parameters *comment-string* — A comment of up to 255 characters in length that is associated with the checkpoint.

rescue — Save the rescue checkpoint instead of a normal rollback checkpoint.

revert

Syntax **revert [latest-rb|** *checkpoint-id* **| rescue] [now]**

Context admin>rollback

Description This command initiates a configuration rollback revert operation that will return the configuration state of the node to a previously saved checkpoint. The rollback revert minimizes impacts to running services. There are no impacts in areas of configuration that did not change since the checkpoint. Configuration parameters that changed (or items on which changed configuration have dependencies) are first removed (revert to default) and the previous values are then restored (can be briefly service impacting in changed areas).

Parameters **latest-rb —** Specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file).

checkpoint-id — >Indicates the configuration to return to (which rollback checkpoint file to use). Checkpoint-id of "1" corresponds to the file-url.rb.1 rollback checkpoint file. The higher the id, the older the checkpoint.   Max is the highest rollback checkpoint supported or configured.

Values 1—max, where max is the number of configured checkpoints minus 1 (since, for example, the 10th checkpoint has an id of 9)

rescue — Revert to the rescue checkpoint.

now — Forces a rollback revert without any interactive confirmations (assumes 'y' for any confirmations that would have occurred).

view

Syntax view [**latest-rb** | *checkpoint-id* | **rescue**]

Context admin>rollback

Description This command displays checkpoint..

Default none

Parameters **latest-rb —** Specifies the most recently created rollback checkpoint (corresponds to the file-url.rb rollback checkpoint file).

checkpoint-id — >Indicates rollback checkpoint file to be viewed. Checkpoint-id of "1" corresponds to the file-url.rb.1 rollback checkpoint file. The higher the id, the older the checkpoint. Max is the highest rollback checkpoint supported or configured.

1..max**rescue —** View the rescue configuration.

LLDP System Commands

lldp

Syntax **lldp**

Context config>system

Description This command enables the context to configure system-wide Link Layer Discovery Protocol parameters.

message-fast-tx

Syntax **message-fast-tx** *time*
no message-fast-tx

Context config>system>lldp

Description This command configures the duration of the fast transmission period.

Parameters *time* — Specifies the fast transmission period in seconds.

Values 1 — 3600

Default 1

message-fast-tx-init

Syntax **message-fast-tx-init** *count*
no message-fast-tx-init

Context config>system>lldp

Description This command configures the number of LLDPDUs to send during the fast transmission period.

Parameters *count* — Specifies the number of LLDPDUs to send during the fast transmission period.

Values 1 — 8

Default 4

notification-interval

Syntax **notification-interval** *time*
no notification-interval

Context config>system>lldp

Description This command configures the minimum time between change notifications.

Parameters *time* — Specifies the minimum time, in seconds, between change notifications.

Values 5 — 3600

Default 5

reinit-delay

Syntax **reinit-delay** *time*
no reinit-delay

Context config>system>lldp

Description This command configures the time before re-initializing LLDP on a port.

Parameters *time* — Specifies the time, in seconds, before re-initializing LLDP on a port.

Values 1 — 10

Default 2

tx-credit-max

Syntax **tx-credit-max** *count*
no tx-credit-max

Context config>system>lldp

Description This command configures the maximum consecutive LLDPDUs transmitted.

Parameters *count* — Specifies the maximum consecutive LLDPDUs transmitted.

Values 1 — 100

Default 5

tx-hold-multiplier

Syntax **tx-hold-multiplier** *multiplier*
no tx-hold-multiplier

Context config>system>lldp

Description This command configures the multiplier of the tx-interval.

Parameters *multiplier* — Specifies the multiplier of the tx-interval.

Values 2 — 10

Default 4

tx-interval

Syntax **tx-interval** *interval*
no tx-interval

Context config>system>lldp

Description This command configures the LLDP transmit interval time.

Parameters *interval* — Specifies the LLDP transmit interval time.

Values 1 — 100

Default 5

LLDP Ethernet Port Commands

lldp

Syntax **lldp**

Context config>port>ethernet

Description This command enables the context to configure Link Layer Discovery Protocol (LLDP) parameters on the specified port.

dest-mac

Syntax **dest-mac** {*bridge-mac*}

Context config>port>ethernet>lldp

Description This command configures destination MAC address parameters.

Parameters **bridge-mac —** Specifies destination bridge MAC type to use by LLDP.

Values **nearest-bridge** — Specifies to use the nearest bridge.
nearest-non-tpmr — Specifies to use the nearest non-Two-Port MAC Relay (TPMR) .
nearest-customer — Specifies to use the nearest customer.

admin-status

Syntax **admin-status** {**rx** | **tx** | **tx-rx** | **disabled**}

Context config>port>ethernet>lldp>dstmac

Description This command specifies the administratively desired status of the local LLDP agent.

Parameters **rx —** Specifies the LLDP agent will receive, but will not transmit LLDP frames on this port.

tx — Specifies that the LLDP agent will transmit LLDP frames on this port and will not store any information about the remote systems connected.

tx-rx — Specifies that the LLDP agent will transmit and receive LLDP frames on this port.

disabled — Specifies that the LLDP agent will not transmit or receive LLDP frames on this port. If there is remote systems information which is received on this port and stored in other tables, before the port's admin status becomes disabled, then the information will naturally age out.

notification

Syntax [**no**] **notification**

Context config>port>ethernet>lldp>dstmac

Description This command enables LLDP notifications.

The **no** form of the command disables LLDP notifications.

tx-mgmt-address

Syntax **tx-mgmt-address** [**system**]
no tx-mgmt-address

Context config>port>ethernet>lldp>dstmac

Description This command specifies which management address to transmit.

The no form of the command resets value to the default.

Default no tx-mgmt-address

Parameters **system —** Specifies to use the system IP address. Note that the system address will only be transmitted once it has been configured if this parameter is specified

tx-tlvs

Syntax **tx-tlvs** [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**]
no tx-tlvs

Context config>port>ethernet>lldp>dstmac

Description This command specifies which LLDP TLVs to transmit.

The **no** form of the command resets the value to the default.

Default no tx-tlvs

Parameters **port-desc —** Indicates that the LLDP agent should transmit port description TLVs.

sys-name — Indicates that the LLDP agent should transmit system name TLVs.

sys-desc — Indicates that the LLDP agent should transmit system description TLVs.

sys-cap — Indicates that the LLDP agent should transmit system capabilities TLVs.