Configuration Commands

Generic Commands

description

Syntax **description** *string*
no description

Context config>log>filter
config>log>filte>entry
config>log>log-id
config>log>accounting-policy
config>log>file-id
config>log>syslog
config>log>snmp-trap-group

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 the command removes the string from the configuration.

Default No text description is associated with this configuration. The string must be entered.

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

shutdown

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

Context config>log>log-id
config>log>accounting-policy

Description This command administratively disables an 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 administratively enables an entity.

Default **no shutdown**

Special Cases **log-id** *log-id* — When a *log-id* is shut down, no events are collected for the entity. This leads to the loss of event data.

accounting-policy *accounting Policy* — When an accounting policy is shut down, no accounting data is written to the destination log ID. Counters in the billing data reflect totals, not increments, so when the policy is re-enabled (**no shutdown**) the counters include the data collected during the period the policy was shut down.

app-route-notifications

Syntax **app-route-notifications**

Context config>log

Description Specific system applications in SR OS can take action based on a route to certain IP destinations being available. This CLI branch contains configuration related to these route availability notifications. A delay can be configured between the time that a route is determined as available in the CPM, and the time that the application is notified of the available route. For example, this delay may be used to increase the chances that other system modules (such as IOMs/XCMs/MDAs/XMAs) are fully programmed with the new route before the application takes action. Currently, the only application that acts upon these *route available* or *route changed* notifications with their configurable delays is the SNMP replay feature, which receives notifications of route availability to the SNMP trap receiver destination IP address.

cold-start-wait

Syntax [**no**] **cold-start-wait**

Context config>log>app-route-notifications

Description The time delay that must pass before notifying specific CPM applications that a route is available after a cold reboot.

Default no cold-start-wait

Parameters — **Values** seconds: 1 – 300

Default 0

route-recovery-wait

Syntax [**no**] **route-recovery-wait**

Context config>log>app-route-notifications

Description The time delay that must pass before notifying specific CPM applications after the recovery or change of a route during normal operation.

Default no route-recovery-wait

Parameters — **Values** seconds: 1 – 100

Default 0

event-control

Syntax **event-control** *application-id* [*event-name* | *event-number*] [**generate**][*severity-level*] [**throttle**] [**specific-throttle-rate** *events-limit* **interval** *seconds* | **disable-specific-throttle**]
event-control *application-id* [*event-name* | *event-number*] **suppress**
no event-control *application* [*event-name* | *event-number*]

Context config>log

Description This command is used to specify that a particular event or all events associated with an application is either generated or suppressed.

Events are generated by an application and contain an event number and description explaining the cause of the event. Each event has a default designation which directs it to be generated or suppressed.

Events are generated with a default severity level that can be modified by using the *severity-level* option.

Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are squelched. In reverse, indiscriminate application may cause excessive overhead.

The rate of event generation can be throttled by using the **throttle** parameter.

The **no** form of the command reverts the parameters to the default setting for events for the application or a specific event within the application. The severity, generate, suppress, and throttle options will also be reset to the initial values.

Default Each event has a set of default settings. To display a list of all events and the current configuration use the **event-control** command.

Parameters *application-id* — The application whose events are affected by this event control filter.

Default None, this parameter must be explicitly specified.

Values A valid application name. To display a list of valid application names, use the **applications** command. Some examples of valid applications are:

bgp, cflowd, chassis, debug, igmp, lldp, mirror, ospf, pim, port, snmp, system, user, vrtr

event-name | *event-number* — To generate, suppress, or revert to default for a single event, enter the specific number or event short name. If no event number or name is specified, the command

applies to all events in the application. To display a list of all event short names use the **event-control** command.

Default none

Values A valid event name or event number.

generate — Specifies that logger event is created when this event occurs. The generate keyword can be used with two optional parameters, *severity-level* and **throttle**.

Default generate

severity-name — An ASCII string representing the severity level to associate with the specified generated events

Default The system assigned severity name

Values One of: cleared, indeterminate, critical, major, minor, warning.

throttle — Specifies whether or not events of this type will be throttled.
By default, event throttling is on for most event types.

suppress — This keyword indicates that the specified events will not be logged. If the **suppress** keyword is not specified then the events are generated by default. For example, **event-control bgp suppress** will suppress all BGP events.

Default generate

specific-throttle-rate *events-limit* **—** The log event throttling rate can be configured independently for each log event using this keyword. This specific-throttle-rate overrides the globally configured throttle rate (**configure>log>throttle-rate**) for the specific log event.

Values 1 — 20000

interval *seconds* **—** specifies the number of seconds that the specific throttling intervals lasts.

Values 1 — 1200

disable-specific-throttle — Specifies to disable the **specific-throttle-rate**.

event-damping

Syntax [**no**] **event-damping**

Context config>log

Description This command allows the user to set the event damping algorithm to suppress QoS or filter change events.

Note that while this event damping is original behavior for some modules such as service manager, QoS, and filters it can result in the NMS system database being out of sync because of missed change events. On the other hand, if the damping is disabled (**no event-damping**), it may take much longer for a large CLI configuration file to be processed when manually "execed" after system bootup.

route-preference

Syntax **route-preference primary** {**inband** | **outband**} **secondary** {**inband** | **outband** | **none**}
no route-preference

Context config>log

Description This command specifies the primary and secondary routing preference for traffic generated for SNMP notifications and syslog messages. If the remote destination is not reachable through the routing context specified by primary route preference then the secondary routing preference will be attempted.

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

Default no route-preference

Parameters **primary —** Specifies the primary routing preference for traffic generated for SNMP notifications and syslog messages.

Default outband

secondary — Specifies the secondary routing preference for traffic generated for SNMP notifications and syslog messages. The routing context specified by the secondary route preference will be attempted if the remote destination was not reachable by the primary routing preference, specified by primary route preference. The value specified for the secondary routing preference must be distinct from the value for primary route preference.

Default inband

inband — Specifies that the logging utility will attempt to use the base routing context to send SNMP notifications and syslog messages to remote destinations.

outband — Specifies that the logging utility will attempt to use the management routing context to send SNMP notifications and syslog messages to remote destinations.

none — Specifies that no attempt will be made to send SNMP notifications and syslog messages to remote destinations.

Log File Commands

file-id

Syntax [**no**] **file-id** *file-id*

Context config>log

Description This command creates the context to configure a file ID template to be used as a destination for an event log or billing file.

This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting/billing information. The file defined in this context is subsequently specified in the **to** command under **log-id** or **accounting-policy** to direct specific logging or billing source streams to the file destination.

A file ID can only be assigned to either *one* **log-id** or *one* **accounting-policy**. It cannot be reused for multiple instances. A file ID and associated file definition must exist for each log and billing file that must be stored in the file system.

A file is created when the file ID defined in this command is selected as the destination type for a specific log or accounting record. Log files are collected in a "log" directory. Accounting files are collected in an "act" directory.

The file names for a log are created by the system as summarized in the table below:

File Type	File Name
Log File	`log`*`ll`*`ff-timestamp`
Accounting File	`act`*`aa`*`ff-timestamp`

Where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the file-id
- The *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
  - *yyyy* is the year (for example, 2006)
  - *mm* is the month number (for example, 12 for December)
  - *dd* is the day of the month (for example, 03 for the 3rd of the month)
  - *hh* is the hour of the day in 24 hour format (for example, 04 for 4 a.m.)
  - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
  - *ss* is the number of seconds (for example, 14 for 14 seconds)
- The accounting file is compressed and has a gz extension.

When initialized, each file will contain:

- The *log-id* description.
- The time the file was opened.
- The reason the file was created.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

The **no** form of the command removes the *file-id* from the configuration. A *file-id* can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

Default No default file IDs are defined.

Parameters *file-id* — The file identification number for the file, expressed as a decimal integer.

Values 1 — 99

location

Syntax **location** *cflash-id* [*backup-cflash-id*]
no location

Context config>log>file *file-id*

Description This command specifies the primary and optional backup location where the log or billing file will be created.

The **location** command is optional. If the location command not explicitly configured, log files will be created on cf1: and accounting files will be created on cf2: without overflow onto other devices. Generally, cf3: is reserved for system files (configurations, images, etc.).

When multiple location commands are entered in a single file ID context, the last command overwrites the previous command.

When the location of a file ID that is associated with an active log ID is changed, the log events are not immediately written to the new location. The new location does not take affect until the log is rolled over either because the rollover period has expired or a **clear log** *log-id* command is entered to manually rollover the log file.

When creating files, the primary location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

A medium severity trap is issued to indicate that a compact flash is either not available or that no space is available on the specified flash and that the backup location is being used.

A high priority alarm condition is raised if none of the configured compact flash devices for this file ID are present or if there is insufficient space available. If space does becomes available, then the alarm condition will be cleared.

Use the **no** form of this command to revert to default settings.

Default Log files are created on cf1: and accounting files are created on cf2:.

Parameters *cflash-id* — Specify the primary location.

Values cflash-id: cf1:, cf2:, cf3:

backup-cflash-id — Specify the secondary location.

Values cflash-id: cf1:, cf2:, cf3:

rollover

Syntax **rollover** *minutes* [**retention** *hours*]
no rollover

Context config>log>file *file-id*

Description This command configures how often an event or accounting log is rolled over or partitioned into a new file.

An event or accounting log is actually composed of multiple, individual files. The system creates a new file for the log based on the **rollover** time, expressed in minutes.

The **retention** option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file.

When multiple **rollover** commands for a *file-id* are entered, the last command overwrites the previous command.

Default **rollover 1440 retention 12**

Parameters *minutes* — The rollover time, in minutes.

Values 5 — 10080

retention hours. The retention period in hours, expressed as a decimal integer. The retention time is based on the time creation time of the file. The file becomes a candidate for removal once the creation datestamp + rollover time + retention time is less than the current timestamp.

Default 12

Values 1 — 500

Log Filter Commands

filter

Syntax [**no**] **filter** *filter-id*

Context config>log

Description This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.

Filters are configured in the **filter** *filter-id* context and then applied to a log in the **log-id** *log-id* context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.

Any changes made to an existing filter, using any of the sub-commands, are immediately applied to the destinations where the filter is applied.

The **no** form of the command removes the filter association from log IDs which causes those logs to forward all events.

Default No event filters are defined.

Parameters filter-id — The filter ID uniquely identifies the filter.

Values 1 — 1000

default-action

Syntax **default-action** {**drop** | **forward**}
no default-action

Context config>log>filter *filter-id*

Description The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.

When multiple **default-action** commands are entered, the last command overwrites the previous command.

The **no** form of the command reverts the default action to the default value (forward).

Default **default-action forward** — The events which are not explicitly dropped by an event filter match are forwarded.

Parameters **drop —** The events which are not explicitly forwarded by an event filter match are dropped.

forward — The events which are not explicitly dropped by an event filter match are forwarded.

Log Filter Entry Commands

action

Syntax **action** {**drop** | **forward**}
no action

Context config>log>filter *filter-id*>entry *entry-id*

Description This command specifies a drop or forward action associated with the filter entry. If neither **drop** nor **forward** is specified, the **default-action** will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.

Multiple action statements entered will overwrite previous actions.

The **no** form of the command removes the specified **action** statement.

Default Action specified by the **default-action** command will apply.

Parameters **drop —** Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

entry

Syntax [**no**] **entry** *entry-id*

Context config>log>filter *filter-id*

Description This command is used to create or edit an event filter entry. Multiple entries may be created using unique *entry-id* numbers. The TiMOS implementation exits the filter on the first match found and executes the action in accordance with the action command.

Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and are rendered inactive.

The **no** form of the command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log-id's where the filter is applied.

Default No event filter entries are defined. An entry must be explicitly configured.

Parameters *entry-id.* The entry ID uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 — 999

Log Filter Entry Match Commands

match

Syntax [**no**] **match**

Context config>log>filter *filter-id*>entry *entry-id*

Description This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.

If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied (AND functional) before the action associated with the match is executed.

Use the **application** command to display a list of the valid applications.

Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Default No match context is defined.

application

Syntax **application** {**eq | neq**} *application-id*
no application

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an OS application as an event filter match criterion.

An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES etc. Only one application can be specified. The latest **application** command overwrites the previous command.

The **no** form of the command removes the application as a match criterion.

Default **no application** — No application match criterion is specified.

Parameters **eq** | **neq —** The operator specifying the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	equal to
neq	not equal to

application-id — The application name string.

Values port, ppp, rip, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrp, vrtr

number

Syntax **number** {**eq | neq | lt | lte | gt | gte**} *event-id*
no number

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an SR OS application event number as a match criterion.

SR OS event numbers uniquely identify a specific logging event within an application.

Only one **number** command can be entered per event filter entry. The latest **number** command overwrites the previous command.

The **no** form of the command removes the event number as a match criterion.

Default **no event-number** — No event ID match criterion is specified.

Parameters **eq | neq | lt | lte | gt | gte —** This operator specifies the type of match. Valid operators are listed in the table below. Valid operators are:

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

event-id — The event ID, expressed as a decimal integer.

Values 1 — 4294967295

router

Syntax **router** {**eq** | **neq**} *router-instance* [**regexp**]
no router

Context config>log>filter>entry>match

Description This command specifies the log event matches for the router.

Parameters **eq —** Determines if the matching criteria should be equal to the specified value.

neq — Determines if the matching criteria should not be equal to the specified value.

router-instance — Specifies a router name up to 32 characters to be used in the match criteria.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** keyword is specified, the string in the **router** command is a regular expression string that will be matched against the subject string in the log event being filtered.

severity

Syntax **severity** {**eq | neq | lt | lte | gt | gte**} *severity-level*
no severity

Context config>log>filter>entry>match

Description This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command.

The **no** form of the command removes the severity match criterion.

Default **no severity** — No severity level match criterion is specified.

Parameters **eq | neq | lt | lte | gt | gte —** This operator specifies the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	equal to
neq	not equal to
lt	less than
lte	less than or equal to
gt	greater than
gte	greater than or equal to

severity-name — The ITU severity level name. The following table lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

Severity Number	Severity Name
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

Values cleared, intermediate, critical, major, minor, warning

subject

Syntax **subject** {**eq|neq**} *subject* [**regexp**]
no subject

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case the port-id string would be the subject. Only one **subject** command can be entered per event filter entry. The latest **subject** command overwrites the previous command.

The **no** form of the command removes the subject match criterion.

Default **no subject** — No subject match criterion specified.

Parameters **eq** | **neq** — This operator specifies the type of match. Valid operators are listed in the following table:

Operator	Notes
eq	equal to
neg	not equal to

subject — A string used as the subject match criterion.

regexp — Specifies the type of string comparison to use to determine if the log event matches the value of **subject** command parameters. When the **regexp** keyword is specified, the string in the **subject** command is a regular expression string that will be matched against the subject string in the log event being filtered.

When **regexp** keyword is not specified, the **subject** command string is matched exactly by the event filter.

Syslog Commands

syslog

Syntax [**no**] **syslog** *syslog-id*

Context config>log

Description This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from this network element.

A valid *syslog-id* must have the target syslog host address configured.

A maximum of 10 syslog-id's can be configured.

No log events are sent to a syslog target address until the syslog-id has been configured as the log destination (**to**) in the log-id node.

Default No syslog IDs are defined.

Parameters *syslog-id* — The syslog ID number for the syslog destination, expressed as a decimal integer.

Values 1 — 10

address

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

Context config>log>syslog *syslog-id*

Description This command adds the syslog target host IP address to/from a syslog ID.

This parameter is mandatory. If no **address** is configured, syslog data cannot be forwarded to the syslog target host.

Only one address can be associated with a *syslog-id*. If multiple addresses are entered, the last address entered overwrites the previous address.

The same syslog target host can be used by multiple log IDs.

The **no** form of the command removes the syslog target host IP address.

Default **no address** — There is no syslog target host IP address defined for the syslog ID.

Parameters *ip-address* — The IP address of the syslog target host in dotted decimal notation.

Values		
	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 characters maximum, mandatory for link local addressesipv6-addressx: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 characters maximum, mandatory for link local addresses

facility

Syntax **facility** *syslog-facility*
no facility

Context config>log>syslog *syslog-id*

Description This command configures the facility code for messages sent to the syslog target host.

Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last *facility-code* entered overwrites the previous facility-code.

If multiple facilities need to be generated for a single syslog target host, then multiple **log-id** entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.

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

Default **local7** — syslog entries are sent with the local7 facility code.

Parameters *syslog-facility* — The syslog facility name represents a specific numeric facility code. The code should be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.

Values kernel, user, mail, systemd, auth, syslogd, printer, netnews, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Valid responses per RFC3164, *The BSD syslog Protocol,* are listed in the table below.

Numerical Code	Facility Code
0	kernel
1	user
2	mail
3	systemd
4	auth
5	syslogd
6	printer
7	net-news
8	uucp

Numerical Code	Facility Code
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

Values 0 — 23

log-prefix

Syntax **log-prefix** *log-prefix-string*
no log-prefix

Context config>log>syslog *syslog-id*

Description This command adds the string prepended to every syslog message sent to the syslog host.

RFC3164, *The BSD syslog Protocol,* allows a alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.

Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.

The **no** form of the command removes the log prefix string.

Default **no log-prefix** — no prepend log prefix string defined.

Parameters *log-prefix-string* — An alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

level

Syntax **level** *syslog-level*
no level

Context config>log>syslog *syslog-id*

Description This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.

Only a single threshold level can be specified. If multiple levels are entered, the last **level** entered will overwrite the previously entered commands.

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

Parameters *value* — The threshold severity level name.

Values emergency, alert, critical, error, warning, notice, info, debug

Router severity level	Numerical Severity (highest to lowest)	Configured Severity	Definition
	0	emergency	system is unusable
3	1	alert	action must be taken immedi-ately
4	2	critical	critical condition
5	3	error	error condition
6	4	warning	warning condition
	5	notice	normal but significant condition
1 cleared 2 indeterminate	6	info	informational messages
	7	debug	debug-level messages

port

Syntax **port** *value*
no port

Context config>log>syslog *syslog-id*

Description This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

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

Default **no port**

Parameters *value* — The value is the configured UDP port number used when sending syslog messages.

Values 1 — 65535

throttle-rate

Syntax **throttle-rate** *events* [**interval** *seconds*]
no throttle-rate

Context config>log

Description This command configures an event throttling rate.

Parameters *events* — Specifies the number of log events that can be logged within the specified interval for a specific event. Once the limit has been reached, any additional events of that type will be dropped, for example, the event drop count will be incremented. At the end of the throttle interval if any events have been dropped a trap notification will be sent.

Values 1 — 20000

Default 2000

interval *seconds* — Specifies the number of seconds that an event throttling interval lasts.

Values 1 — 1200

Default 1

SNMP Trap Groups

snmp-trap-group

Syntax [**no**] **snmp-trap-group** *log-id*

Context config>log

Description This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given log-id.

A group specifies the types of SNMP traps and specifies the log ID which will receive the group of SNMP traps. A trap group must be configured in order for SNMP traps to be sent.

To suppress the generation of all alarms and traps see the **event-control** command. To suppress alarms and traps that are sent to this log-id, see the **filter** command. Once alarms and traps are generated they can be directed to one or more SNMP trap groups. Logger events that can be forwarded as SNMP traps are always defined on the main event source.

The **no** form of the command deletes the SNMP trap group.

Default There are no default SNMP trap groups.

Parameters *log-id* — The log ID value of a log configured in the **log-id** context. Alarms and traps cannot be sent to the trap receivers until a valid *log-id* exists.

Values 1 — 99

trap-target

Syntax **trap-target** *name* [**address** *ip-address*] [**port** *port*] [**snmpv1** | **snmpv2c** | **snmpv3**] **notify-community** *communityName* | *snmpv3SecurityName* [**security-level** {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**}] [**replay**]
no trap-target *name*

Context config>log>snmp-trap-group

Description This command adds/modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the **log-id**, **snmp-trap-group** and at least one **trap-target** must be configured.

The **trap-target** command is used to add/remove a trap receiver from an **snmp-trap-group**. The operational parameters specified in the command include:

- The IP address of the trap receiver
- The UDP port used to send the SNMP trap
- SNMP version

- SNMP community name for SNMPv1 and SNMPv2c receivers.
- Security name and level for SNMPv3 trap receivers.

A single **snmp-trap-group** *log-id* can have multiple trap-receivers. Each trap receiver can have different operational parameters.

An address can be configured as a trap receiver more than once as long as a different port is used for each instance.

To prevent resource limitations, only configure a maximum of 10 trap receivers.

Note that if the same **trap-target** *name* **port** *port* parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different *notify-community* value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each router event log when multiple event logs are directed to the same IP address and port destination.

The **no** form of the command removes the SNMP trap receiver from the SNMP trap group.

Default No SNMP trap targets are defined.

Parameters *name* — Specifies the name of the trap target up to 28 characters in length.

address *ip-address* — The IP address of the trap receiver in dotted decimal notation. Only one IP address destination can be specified per trap destination group.

Values

ipv4-address	a.b.c.d (host bits must be 0)
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 characters maximum, mandatory for link local addresses

port *port* — The destination UDP port used for sending traps to the destination, expressed as a decimal integer. Only one port can be specified per **trap-target** statement. If multiple traps need to be issued to the same address then multiple ports must be configured.

Default 162

Values 1 — 65535

snmpv1 | *snmpv2c* | *snmpv3* — Specifies the SNMP version format to use for traps sent to the trap receiver.

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv1,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv2c** selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv2c,** then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv3** selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** must be configured for the SNMP *security-name*. If the SNMP version is changed from **snmpv1** or **snmpv2c** to **snmpv3**, then the **notify-community** parameter must be changed to reflect the *security-name* rather than the community string used by **snmpv1** or **snmpv2c**.

Pre-existing conditions are checked before the snmpv3SecurityName is accepted. These are:

- The user name must be configured.
- The v3 access group must be configured.
- The v3 notification view must be configured.

Default snmpv3

Values snmpv1, snmpv2c, snmpv3

notify-community *community* | *security-name* — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** *security-name*. If no **notify-community** is configured, then no alarms nor traps will be issued for the trap destination. If the SNMP version is modified, the **notify-community** must be changed to the proper form for the SNMP version.

community — The community string as required by the **snmpv1** or **snmpv2c** trap receiver. The community string can be an ASCII string up to 31 characters in length.

security-name — The *security-name* as defined in the config>system>security>user context for SNMP v3. The *security-name* can be an ASCII string up to 31 characters in length.

security-level {*no-auth-no-privacy* | *auth-no-privacy* | *privacy*} — Specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies authentication is required but no privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies both authentication and privacy (encryption) is required. When this option is configured the *security-name* must be configured for **authentication** and **privacy**.

Default no-auth-no-privacy. This parameter can only be configured if SNMPv3 is also configured.

Values no-auth-no-privacy, auth-no-privacy, privacy

replay — Enable replay of missed events to target. If replay is applied to an SNMP trap target address, the address is monitored for reachability. Reachability is determined by whether or not there is a route in the routing table by which the target address can be reached. Before sending a trap to a target address, the SNMP module asks the PIP module if there is either an in-band or out-of-band route to the target address. If there is no route to the SNMP target address, the SNMP module saves the sequence-id of the first event that will be missed by the trap target. When the routing table changes again so that there is now a route by which the SNMP target address can be reached, the SNMP module replays (for example, retransmits) all events generated to the SNMP notification log while the target address was removed from the route table. Note that because of route table change convergence time, it is possible that one or more events may be lost at the beginning or end of a replay sequence. The cold-start-wait and route-

recovery-wait timers under config>log>app-route-notifications can help reduce the probability of lost events.

Logging Destination Commands

filter

Syntax **filter** *filter-id*
no filter

Context config>log>log-id *log-id*

Description This command adds an event filter policy with the log destination.

The **filter** command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.

An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination **snmp-trap-group**.

The application of filters for debug messages is limited to application and subject only.

Accounting records cannot be filtered using the **filter** command.

Only one filter-id can be configured per log destination.

The **no** form of the command removes the specified event filter from the *log-id*.

Default **no filter** — No event filter policy is specified for a *log-id.*

Parameters *filter-id.* The event filter policy ID is used to associate the filter with the *log-id* configuration. The event filter policy ID must already be defined in **config>log>filter** *filter-id*.

Values 1 — 1000

from

Syntax **from** {[**main**] [**security**] [**change**] [**debug-trace**]}
no from

Context config>log>log-id *log-id*

Description This command selects the source stream to be sent to a log destination.

One or more source streams must be specified. The source of the data stream must be identified using the **from** command before you can configure the destination using the **to** command. The **from** command can identify multiple source streams in a single statement (for example: **from main change debug-trace**).

Only one **from** command may be entered for a single *log-id*. If multiple **from** commands are configured, then the last command entered overwrites the previous **from** command.

The **no** form of the command removes all previously configured source streams.

Default No source stream is configured.

Parameters ***main*** — Instructs all events in the main event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the **filter** command.

security — Instructs all events in the security event stream to be sent to the destination defined in the **to** command for this destination *log-id*. The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted. To limit the events forwarded to the destination, configure filters using the **filter** command.

change — Instructs all events in the user activity stream to be sent to the destination configured in the **to** command for this destination *log-id*. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the **filter** command.

debug-trace — Instructs all debug-trace messages in the debug stream to be sent to the destination configured in the **to** command for this destination *log-id*. Filters applied to debug messages are limited to application and subject.

log-id

Syntax [**no**] **log-id** *log-id*

Context config>log

Description This command creates a context to configure destinations for event streams.

The **log-id** context is used to direct events, alarms/traps, and debug information to respective destinations.

A maximum of 10 logs can be configured.

Before an event can be associated with this log-id, the **from** command identifying the source of the event must be configured.

Only one destination can be specified for a *log-id*. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.

Use the **event-control** command to suppress the generation of events, alarms, and traps for all log destinations.

An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.

Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages.
Log-ID 100 captures log messages with a severity level of major and above.

Note that Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.

The **no** form of the command deletes the log destination ID from the configuration.

Default No log destinations are defined.

Parameters *log-id* — The log ID number, expressed as a decimal integer.

Values 1 — 100

to console

Syntax **to console**

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, then all the entries are dropped.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default No destination is specified.

to file

Syntax **to file** *log-file-id*

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a specified file.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default No destination is specified.

Parameters *log-file-id* — Instructs the events selected for the log ID to be directed to the *log-file-id*. The characteristics of the *log-file-id* referenced here must have already been defined in the **config>log>file** *log-file-id* context.

Values 1 — 99

to memory

Syntax **to memory** [*size*]

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a memory log. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

Parameters *size* — The *size* parameter indicates the number of events that can be stored in the memory.

Default 100

Values 50 — 1024

to session

Syntax **to session**

Context config>log>log-id *log-id*

Description This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the current console or telnet session. This command is only valid for the duration of the session. When the session is terminated the log ID is removed. A log ID with a *session* destination is not saved in the configuration file.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

to snmp

Syntax **to snmp** [*size*]

Context config>log>log-id *log-id*

Description This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the alarms and traps to be directed to the **snmp-trap-group** associated with *log-id*.

A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the *log-id*.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

Parameters *size* — The *size* parameter defines the number of events stored in this memory log.

Default 100

Values 50 — 1024

to syslog

Syntax **to syslog** *syslog-id*

Context config>log>log-id

Description This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.

This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1k bytes.

The source of the data stream must be specified in the **from** command prior to configuring the destination with the **to** command.

The **to** command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

Default none

Parameters *syslog-id* — Instructs the events selected for the log ID to be directed to the *syslog-id*. The characteristics of the *syslog-id* referenced here must have been defined in the **config>log>syslog** *syslog-id* context.

Values 1 — 10

time-format

Syntax **time-format {local | utc}**

Context config>log>log-id

Description This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.

Default utc

Parameters **local** — Specifies that timestamps are written in the system's local time.

utc — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.

Accounting Policy Commands

accounting-policy

Syntax **accounting-policy** *policy-id* [**interval** *minutes*]
no accounting-policy *policy-id*

Context config>log

Description This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.

Access accounting policies are policies that can be applied to one or more SAPs. Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.

If an accounting policy is not specified on a SAP, then accounting records are produced in accordance with the access policy designated as the **default**. If a default access policy is not specified, then no accounting records are collected other than the records for the accounting policies that are explicitly configured.

Only one policy can be regarded as the default access policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new access default policy can be configured.

Network accounting policies are policies that can be applied to one or more network ports or SONET/SDH channels. Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports or SONET/SDH channels where this policy is applied.

If no accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy as designated with the **default** command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one policy can be regarded as the default network policy. If a policy is configured as the default policy, then a **no default** command must be used to allow the data that is currently being collected to be written before a new network default policy can be configured.

The **no** form of the command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs, network ports or channels where the policy is applied.

Default No default accounting policy is defined.

Parameters *policy-id* — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values 1 — 99

collection-interval

Syntax **collection-interval** *minutes*
no collection-interval

Context config>log>acct-policy

Description This command configures the accounting collection interval.

Parameters *minutes* — Specifies the interval between collections, in minutes.

Values 1 — 120
A range of 1 — 4 is only allowed when the record type is set to SAA.

auto-bandwidth

Syntax [**no**] **auto-bandwidth**

Context config>log>accounting-policy

Description In the configuration of an accounting policy this designates the accounting policy as the one used for auto-bandwidth statistics collection.

Default no auto-bandwidth

default

Syntax [**no**] **default**

Context config>log>accounting-policy

Description This command configures the default accounting policy to be used with all SAPs that do not have an accounting policy.

If no access accounting policy is defined on a SAP, accounting records are produced in accordance with the default access policy. If no default access policy is created, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

If no network accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one access accounting policy ID can be designated as the default access policy. Likewise, only one network accounting policy ID can be designated as the default network accounting policy.

The record name must be specified prior to assigning an accounting policy as default.

If a policy is configured as the default policy, then a **no default** command must be issued before a new default policy can be configured.

The **no** form of the command removes the default policy designation from the policy ID. The accounting policy will be removed from all SAPs or network ports that do not have this policy explicitly defined.

include-system-info

Syntax [**no**] **include-system-info**

Context config>log>accounting-policy

Description This command allows the operator to optionally include router information at the top of each accounting file generated for a given accounting policy.

When the **no** version of this command is selected, optional router information is not include at the top of the file.

Default no include-router-info

record

Syntax [**no**] **record** *record-name*

Context config>log>accounting-policy *policy-id*

Description This command adds the accounting record type to the accounting policy to be forwarded to the configured accounting file. A record name can only be used in one accounting policy. To obtain a list of all record types that can be configured, use the **show log accounting-records** command.

NOTE: aa, video and subscriber records are not applicable to the 7950 XRS.

```
A:ALA-49# show log accounting-records
============================================================
Accounting Policy Records
============================================================
Record # Record Name                          Def. Interval
------------------------------------------------------------
1        service-ingress-octets               5
2        service-egress-octets                5
3        service-ingress-packets              5
4        service-egress-packets               5
5        network-ingress-octets               15
6        network-egress-octets                15
7        network-ingress-packets              15
8        network-egress-packets               15
9        compact-service-ingress-octets       5
10       combined-service-ingress             5
11       combined-network-ing-egr-octets      15
12       combined-service-ing-egr-octets      5
13       complete-service-ingress-egress      5
14       combined-sdp-ingress-egress          5
15       complete-sdp-ingress-egress          5
16       complete-subscriber-ingress-egress   5
17       aa-protocol                          15
18       aa-application                       15
19       aa-app-group                         15
20       aa-subscriber-protocol               15
21       aa-subscriber-application            15
23       custom-record-subscriber             5
24       custom-record-service                5
25       custom-record-aa-sub                 15
26       queue-group-octets                   15
27       queue-group-packets                  15
28       combined-queue-group                 15
29       combined-mpls-lsp-ingress            5
30       combined-mpls-lsp-egress             5
31       combined-ldp-lsp-egress              5
32       saa                                  5
33       video                                10
34       kpi-system                           5
35       kpi-bearer-mgmt                      5
36       kpi-bearer-traffic                   5
37       kpi-ref-point                        5
38       kpi-path-mgmt                        5
39       kpi-iom-3                            5
40       kci-system                           5
41       kci-bearer-mgmt                      5
42       kci-path-mgmt                        5
```

```
43       complete-kpi                       5
44       complete-kci                       5
45       kpi-bearer-group                   5
46       kpi-ref-path-group                 5
47       kpi-kci-bearer-mgmt                5
48       kpi-kci-path-mgmt                  5
49       kpi-kci-system                     5
50       complete-kpi-kci                   5
51       aa-performance                     15
52       complete-ethernet-port             15
53       extended-service-ingress-egress    5
54       complete-network-ing-egr           15
===============================================================
A:ALA-49#
```

To configure an accounting policy for access ports, select a service record (for example, service-ingress-octets). To change the record name to another service record then the record command with the new record name can be entered and it will replace the old record name.

When configuring an accounting policy for network ports, a network record should be selected. When changing the record name to another network record, the record command with the new record name can be entered and it will replace the old record name.

If the change required modifies the record from network to service or from service to network, then the old record name must be removed using the **no** form of this command.

Only one record may be configured in a single accounting policy. For example, if an accounting-policy is configured with a **access-egress-octets** record, in order to change it to **service-ingress-octets**, use the **no record** command under the accounting-policy to remove the old record and then enter the **service-ingress-octets** record.

Note that collecting excessive statistics can adversely affect the CPU utilization and take up large amounts of storage space.

The **no** form of the command removes the record type from the policy.

Default No accounting record is defined

Parameters *record-name* — The accounting record name. The following table lists the accounting record names available and the default collection interval.

Record Type	Accounting Record Name	Default Interval
1	service-ingress-octets	5
2	service-egress-octets	5
3	service-ingress-packets	5
4	service-egress-packets	5
5	network-ingress-octets	15
6	network-egress-octets	15
7	network-ingress-packets	15

Record Type	Accounting Record Name	Default Interval
8	network-egress-packets	15
9	compact-service-ingress-octets	5
10	combined-service-ingress	5
11	combined-network-ing-egr-octets	15
12	combined-service-ing-egr-octets	5
13	complete-service-ingress-egress	5
14	combined-sdp-ingress-egress	5
15	complete-sdp-ingress-egress	5
16	complete-subscriber-ingress-egress	5
17	aa-protocol	15
18	aa-application	15
19	aa-app-group	15
20	aa-subscriber-protocol	15
21	aa-subscriber-application	15
23	custom-record-subscriber	5
24	custom-record-service	5
25	custom-record-aa-sub	15
26	queue-group-octets	15
27	queue-group-packets	15
28	combined-queue-group	15
29	combined-mpls-lsp-ingress	5
30	combined-mpls-lsp-egress	5
31	combined-ldp-lsp-egress	5
32	saa	5
33	video	10
34	kpi-system	5
35	kpi-bearer-mgmt	5
36	kpi-bearer-traffic	5

Record Type	Accounting Record Name	Default Interval
37	kpi-ref-point	5
38	kpi-path-mgmt	5
39	kpi-iom-3	5
40	kci-system	5
41	kci-bearer-mgmt	5
42	kci-path-mgmt	5
43	complete-kpi	5
44	complete-kci	5
45	kpi-bearer-group	5
46	kpi-ref-path-group	5
47	kpi-kci-bearer-mgmt	5
48	kpi-kci-path-mgmt	5
49	kpi-kci-system	5
50	complete-kpi-kci	5
51	aa-performance	15
52	complete-ethernet-port	15
53	extended-service-ingress-egress	5
54	complete-network-ing-egr	15

to

Syntax **to file** *file-id*

Context config>log>accounting-policy *policy-id*

This command specifies the destination for the accounting records selected for the accounting policy.

Default No destination is specified.

Parameters *file-id* — The *file-id* option specifies the destination for the accounting records selected for this destination. The characteristics of the file-id must have already been defined in the config>log>file context. A file-id can only be used once.

The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics.

If the **to** command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.

Values 1 — 99

Accounting Policy Custom Record Commands

collection-interval

Syntax **collection-interval** *minutes*
no collection-interval

Context config>log>acct-policy

Description This command configures the accounting collection interval.

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

Default 60

Parameters *minutes* — Specifies the collection interval in minutes.

Values 5 — 120

custom-record

Syntax [**no**] **custom-record**

Context config>log>acct-policy

Description This command enables the context to configure the layout and setting for a custom accounting record associated with this accounting policy.

The **no** form of the command reverts the configured values to the defaults.

aa-specific

Syntax [**no**] **aa-specific**

Context config>log>acct-policy>cr

Description This command enables the context to configure information for this custom record.

The **no** form of the command

aa-sub-counters

Syntax **aa-sub-counters** [**all**]
no aa-sub-counters

Context config>log>acct-policy>cr>aa

Description This command enables the context to configure subscriber counter information.

The **no** form of the command

Parameters **all** — Specifies all counters.

long-duration-flow-count

Syntax **long-duration-flow-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the long duration flow count.

The **no** form of the command excludes the long duration flow count in the AA subscriber's custom record.

Default no long-duration-flow-count

medium-duration-flow-count

Syntax [**no**] **medium-duration-flow-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the medium duration flow count in the AA subscriber's custom record.

The **no** form of the command excludes the medium duration flow count.

Default no medium-duration-flow-count

short-duration-flow-count

Syntax [**no**] **short-duration-flow-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the short duration flow count in the AA subscriber's custom record.

The **no** form of the command excludes the short duration flow count.

Default no short-duration-flow-count

total-flow-duration

Syntax [**no**] **total-flow-duration**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the total flow duration flow count in the AA subscriber's custom record.

The **no** form of the command excludes the total flow duration flow count.

total-flows-completed-count

Syntax [**no**] **total-flows-completed-count**

Context config>log>acct-policy>cr>aa>aa-sub-cntr

Description This command includes the total flows completed count in the AA subscriber's custom record.

The **no** form of the command excludes the total flow duration flow count.

from-aa-sub-counters

Syntax [**no**] **from-aa-sub-counters**

Context config>log>acct-policy>cr>aa

Description This command enables the context to configure Application Assurance “from subscriber” counter parameters.

The **no** form of the command excludes the “from subscriber” count.

all

Syntax **all**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Default This command include all counters.

flows-active-count

Syntax [**no**] **flows-active-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the active flow count.

The **no** form of the command excludes the active flow count in the AA subscriber's custom record.

Default no flows-active-count

flows-admitted-count

Syntax [**no**] **flows-admitted-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the admitted flow count.

The **no** form of the command excludes the flow’s admitted count in the AA subscriber's custom record.

Default no flows-admitted-count

flows-denied-count

Syntax [**no**] **flows-denied-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the flow’s denied count in the AA subscriber's custom record.

The **no** form of the command excludes the flow’s denied count.

Default no flows-denied-count

forwarding-class

Syntax [**no**] **forwarding-class**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command enables the collection of a Forwarding Class bitmap information added to the XML aa-sub and router level accounting records.

Default no forwarding-class

max-throughput-octet-count

Syntax [**no**] **max-throughput-octet-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the maximum throughput as measured in the octet count.

The **no** form of the command excludes the maximum throughput octet count.

max-throughput-packet-count

Syntax [**no**] **max-throughput-packet-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the maximum throughput as measured in the packet count.

The **no** form of the command excludes the maximum throughput packet count.

max-throughput-timestamp

Syntax [**no**] **max-throughput-timestamp**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the timestamp of the maximum throughput.

The **no** form of the command excludes the timestamp.

octets-admitted-count

Syntax [**no**] **octets-admitted-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the admitted octet count in the AA subscriber's custom record.

The **no** form of the command excludes the admitted octet count.

Default no octets-admitted-count

octets-denied-count

Syntax [**no**] **octets-denied-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the denied octet count in the AA subscriber's custom record.

The **no** form of the command excludes the denied octet count.

Default no octets-denied-count

packets-admitted-count

Syntax [**no**] **packets-admitted-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the admitted packet count in the AA subscriber's custom record.

The **no** form of the command excludes the admitted packet count.

Default no packets-admitted-count

packets-denied-count

Syntax [**no**] **packets-denied-count**

Context config>log>acct-policy>cr>aa>aa-from-sub-cntr
config>log>acct-policy>cr>aa>aa-to-sub-cntr

Description This command includes the denied packet count in the AA subscriber's custom record.

The **no** form of the command excludes the denied packet count.

Default no packets-denied-count

to-aa-sub-counters

Syntax **to-aa-sub-counters**
no to-aa-sub-counters

Context config>log>acct-policy>cr>aa

Description This command enables the context to configure Application Assurance “to subscriber” counter parameters.

The **no** form of the command excludes the “to subscriber” count.

override-counter

Syntax [**no**] **override-counter** *override-counter-id*

Context config>log>acct-policy>cr

Description This command enables the context to configure override counter (HSMDA) parameters.

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

Parameters *override-counter-id* — Specifies the override counter ID.

Values 1 — 8

queue

Syntax [**no**] **queue** *queue-id*

Context config>log>acct-policy>cr

Description This command specifies the queue-id for which counters will be collected in this custom record. The counters that will be collected are defined in egress and ingress counters.

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

Parameters *queue-id* — Specifies the queue-id for which counters will be collected in this custom record.

e-counters

Syntax [**no**] **e-counters**

Context config>log>acct-policy>cr>override-cntr
config>log>acct-policy>cr>queue
config>log>acct-policy>cr>ref-override-cntr
config>log>acct-policy>cr>ref-queue

Description This command configures egress counter parameters for this custom record.

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

i-counters

Syntax **i-counters** [**all**]
no i-counters

Context config>log>acct-policy>cr>override-cntr
config>log>acct-policy>cr>ref-override-cntr
config>log>acct-policy>cr>ref-queue

Description This command configures ingress counter parameters for this custom record.

The **no** form of the command

Parameters **all** — Specifies all ingress counters should be included.

in-profile-octets-discarded-count

Syntax [**no**] **in-profile-octets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile octets discarded count.

The **no** form of the command excludes the in-profile octets discarded count.

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile octets forwarded count.

The **no** form of the command excludes the in-profile octets forwarded count.

in-profile-packets-discarded-count

Syntax [**no**] **in-profile-packets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile packets discarded count.

The **no** form of the command excludes the in-profile packets discarded count.

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the in-profile packets forwarded count.

The **no** form of the command excludes the in-profile packets forwarded count.

out-profile-octets-discarded-count

Syntax [**no**] **out-profile-octets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile packets discarded count.

The **no** form of the command excludes the out of profile packets discarded count.

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile octets forwarded count.

The **no** form of the command excludes the out of profile octets forwarded count.

out-profile-packets-discarded-count

Syntax [**no**] **out-profile-packets-discarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile packets discarded count.

The **no** form of the command excludes the out of profile packets discarded count.

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>e-count
config>log>acct-policy>cr>roc>e-count
config>log>acct-policy>cr>queue>e-count
config>log>acct-policy>cr>ref-queue>e-count

Description This command includes the out of profile packets forwarded count.

The **no** form of the command excludes the out of profile packets forwarded count.

all-octets-offered-count

Syntax [**no**] **all-octets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes all octets offered in the count.

The **no** form of the command excludes the octets offered in the count.

Default no all-octets-offered-count

all-packets-offered-count

Syntax [**no**] **all-packets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes all packets offered in the count.

The **no** form of the command excludes the packets offered in the count.

Default no all-packets-offered-count

high-octets-discarded-count

Syntax [**no**] **high-octets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high octets discarded count.

The **no** form of the command excludes the high octets discarded count.

Default no high-octets-discarded-count

high-octets-offered-count

Syntax [**no**] **high-octets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high octets offered count.

The **no** form of the command excludes the high octets offered count.

high-packets-discarded-count

Syntax [**no**] **high-packets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high packets discarded count.

The **no** form of the command excludes the high packets discarded count.

Default no high-packets-discarded-count

high-packets-offered-count

Syntax [**no**] **high-packets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the high packets offered count.

The **no** form of the command excludes the high packets offered count.

Default no high-packets-offered -count

in-profile-octets-forwarded-count

Syntax [**no**] **in-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the in profile octets forwarded count.

The **no** form of the command excludes the in profile octets forwarded count.

Default no in-profile-octets-forwarded-count

in-profile-packets-forwarded-count

Syntax [**no**] **in-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the in profile packets forwarded count.

The **no** form of the command excludes the in profile packets forwarded count.

Default no in-profile-packets-forwarded-count

low-octets-discarded-count

Syntax [**no**] **low-octets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low octets discarded count.

The **no** form of the command excludes the low octets discarded count.

Default no low-octets-discarded-count

low-packets-discarded-count

Syntax [**no**] **low-packets-discarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low packets discarded count.

The **no** form of the command excludes the low packets discarded count.

Default no low-packets-discarded-count

low-octets-offered-count

Syntax [**no**] **low-octets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low octets discarded count.

The **no** form of the command excludes the low octets discarded count.

low-packets-offered-count

Syntax [**no**] **low-packets-offered-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the low packets discarded count.

The **no** form of the command excludes the low packets discarded count.

out-profile-octets-forwarded-count

Syntax [**no**] **out-profile-octets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the out of profile octets forwarded count.

The **no** form of the command excludes the out of profile octets forwarded count.

Default no out-profile-octets-forwarded-count

out-profile-packets-forwarded-count

Syntax [**no**] **out-profile-packets-forwarded-count**

Context config>log>acct-policy>cr>oc>i-count
config>log>acct-policy>cr>roc>i-count
config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the out of profile packets forwarded count.

The **no** form of the command excludes the out of profile packets forwarded count.

Default no out-profile-packets-forwarded-count

uncoloured-octets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the uncoloured octets offered in the count.

The **no** form of the command excludes the uncoloured octets offered in the count.

uncoloured-packets-offered-count

Syntax [**no**] **uncoloured-packets-offered-count**

Context config>log>acct-policy>cr>queue>i-count
config>log>acct-policy>cr>ref-queue>i-count

Description This command includes the uncolored packets offered count.

The **no** form of the command excludes the uncoloured packets offered count.

ref-aa-specific-counter

Syntax **ref-aa-specific-counter any**
no ref-aa-specific-counter

Context config>log>acct-policy>cr

Description This command enables the use of significant-change so only those aa-specific records which have changed in the last accounting interval are written.

The **no** form of the command disables the use of significant-change so all aa-specific records are written whether or not they have changed within the last accounting interval.

Parameters **any** — Indicates that a record is collected as long as any field records activity when non-zero significant-change value is configured.

ref-override-counter

Syntax **ref-override-counter** *ref-override-counter-id*
ref-override-counter all
no ref-override-counter

Context config>log>acct-policy>cr

Description This command configures a reference override counter.

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

Default no ref-override-counter

ref-queue

Syntax **ref-queue** *queue-id*
ref-queue all
no ref-queue

Context config>log>acct-policy>cr

Description This command configures a reference queue.

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

Default no ref-queue

significant-change

Syntax **significant-change** *delta*
no significant-change

Context config>log>acct-policy>cr

Description This command configures the significant change required to generate the record.

Parameters *delta* — Specifies the delta change (significant change) that is required for the custom record to be written to the xml file.

Values 0 — 4294967295 (For custom-record-aa-sub only values 0 or 1 are supported.)