Show Commands

accounting-policy

Syntax **accounting-policy** [*acct-policy-id*] [**access** | **network**]

Context show>log

Description This command displays accounting policy information.

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

Values 1 — 99

access — Only displays access accounting policies.

network — Only displays network accounting policies.

Output **Accounting Policy Output —** The following table describes accounting policy output fields.

Table 46: Show Accounting Policy Output Fields

Label	Description
Policy ID	The identifying value assigned to a specific policy.
Type	Identifies accounting record type forwarded to the configured accounting file.
	access – Indicates that the policy is an access accounting policy.
	network – Indicates that the policy is a network accounting policy.
	none – Indicates no accounting record types assigned.
Def	Yes – Indicates that the policy is a default access or network policy.
	No – Indicates that the policy is not a default access or network policy.
Admin State	Displays the administrative state of the policy.
	Up – Indicates that the policy is administratively enabled.
	Down – Indicates that the policy is administratively disabled.
Oper State	Displays the operational state of the policy.
	Up – Indicates that the policy is operationally up.
	Down – Indicates that the policy is operationally down.

Table 46: Show Accounting Policy Output Fields (Continued)

Label	Description
Intvl	Displays the interval, in minutes, in which statistics are collected and written to their destination. The default depends on the record name type.
File ID	The log destination.
Record Name	The accounting record name which represents the configured record type.
This policy is applied to	Specifies the entity where the accounting policy is applied.

Sample Output

```
A:ALA-1# show log accounting-policy
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
1      network No  Up    Up    15        1    network-ingress-packets
2      network Yes Up    Up    15        2    network-ingress-octets
10     access  Yes Up    Up    5         3    complete-service-ingress-egress
===============================================================================
A:ALA-1#


A:ALA-1# show log accounting-policy 10
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3 complete-service-ingress-egress

Description : (Not Specified)

This policy is applied to:
    Svc Id: 100  SAP : 1/1/8:0     Collect-Stats
    Svc Id: 101  SAP : 1/1/8:1     Collect-Stats
    Svc Id: 102  SAP : 1/1/8:2     Collect-Stats
    Svc Id: 103  SAP : 1/1/8:3     Collect-Stats
    Svc Id: 104  SAP : 1/1/8:4     Collect-Stats
    Svc Id: 105  SAP : 1/1/8:5     Collect-Stats
    Svc Id: 106  SAP : 1/1/8:6     Collect-Stats
    Svc Id: 107  SAP : 1/1/8:7     Collect-Stats
    Svc Id: 108  SAP : 1/1/8:8     Collect-Stats
    Svc Id: 109  SAP : 1/1/8:9     Collect-Stats
...
===============================================================================
A:ALA-1#
```

```
A:ALA-1# show log accounting-policy network
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
1      network No  Up    Up    15        1    network-ingress-packets
2      network Yes Up    Up    15        2    network-ingress-octets
===============================================================================
A:ALA-1#


A:ALA-1# show log accounting-policy access
===============================================================================
Accounting Policies
===============================================================================
Policy Type    Def Admin Oper  Intvl     File Record Name
Id                 State State           Id
-------------------------------------------------------------------------------
10     access  Yes Up    Up    5         3 complete-service-ingress-egress
===============================================================================
A:ALA-1#
```

accounting-records

Syntax **accounting-records**

Context show>log

Description This command displays accounting policy record names.

Output **Accounting Records Output.** The following table describes accounting records output fields.

Table 47: Accounting Policy Output Fields

Label	Description
Record #	The record ID that uniquely identifies the accounting policy, expressed as a decimal integer.
Record Name	The accounting record name.
Def. Interval	The default interval, in minutes, in which statistics are collected and written to their destination.

Sample Output

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

```
A:ALA-1# 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
22       aa-subscriber-app-group              15
=============================================================
A:ALA-1#
```

applications

Syntax **applications**

Context show>log

Description This command displays a list of all application names that can be used in event-control and filter commands.

Output **Sample Output**

```
*A:7950 XRS-20# show log applications

==================================
Log Event Application Names
==================================
Application Name
----------------------------------
BGP
...
CHASSIS
...
IGMP
...
LDP
LI
...
MIRROR
...
MPLS
```

```
...
OSPF
PIM
...
PORT
...
SYSTEM
...
USER
...
VRTR
...
===================================
A:ALA-1#
```

event-control

Syntax **event-control** [**application** [*event-name* | *event-number*]]

Context show>log

Description This command displays event control settings for events including whether the event is suppressed or generated and the severity level for the event.

If no options are specified all events, alarms and traps are listed.

Parameters **application —** Only displays event control for the specified application.

Default All applications.

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

event-name — Only displays event control for the named application event.

Default All events for the application.

event-number — Only displays event control for the specified application event number.

Default All events for the application.

Output **Show Event Control Output —** The following table describes the output fields for the event control.

Label	Description
Application	The application name.
ID#	The event ID number within the application. L ID# – An "L" in front of an ID represents event types that do not generate an associated SNMP notification. Most events do generate a notification, only the exceptions are marked with a preceding "L".
Event Name	The event name.
P	CL – The event has a cleared severity/priority.

Label	Description (Continued)
	CR – The event has critical severity/priority.
	IN – The event has indeterminate severity/priority.
	MA – The event has major severity/priority.
	MI – The event has minor severity/priority.
	WA – The event has warning severity/priority.
g/s	gen – The event will be generated/logged by event control.
	sup – The event will be suppressed/dropped by event control.
	thr – Specifies that throttling is enabled.
Logged	The number of events logged/generated.
Dropped	The number of events dropped/suppressed.

Sample Output

```
A:gal171# show log event-control
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                          P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
BGP:
   2001 bgpEstablished                      MI  gen          0           0
   2002 bgpBackwardTransition               WA  gen          0           0
   2003 tBgpMaxPrefix90                     WA  gen          0           0
   2004 tBgpMaxPrefix100                    CR  gen          0           0
L  2005 sendNotification                    WA  gen          0           0
L  2006 receiveNotification                 WA  gen          0           0
L  2007 bgpInterfaceDown                    WA  gen          0           0
L  2008 bgpConnNoKA                         WA  gen          0           0
L  2009 bgpConnNoOpenRcvd                   WA  gen          0           0
L  2010 bgpRejectConnBadLocAddr             WA  gen          0           0
L  2011 bgpRemoteEndClosedConn              WA  gen          0           0
L  2012 bgpPeerNotFound                     WA  gen          0           0
L  2013 bgpConnMgrTerminated                WA  gen          0           0
L  2014 bgpTerminated                       WA  gen          0           0
L  2015 bgpNoMemoryPeer                     CR  gen          0           0
L  2016 bgpVariableRangeViolation           WA  gen          0           0
L  2017 bgpCfgViol                          WA  gen          0           0
CFLOWD:
   2001 cflowdCreated                       MI  gen          0           0
   2002 cflowdCreateFailure                 MA  gen          0           0
   2003 cflowdDeleted                       MI  gen          0           0
   2004 cflowdStateChanged                  MI  gen          0           0
   2005 cflowdCleared                       MI  gen          0           0
   2006 cflowdFlowCreateFailure             MI  gen          0           0
   2007 cflowdFlowFlushFailure              MI  gen          0           0
   2008 cflowdFlowUnsuppProto               MI  sup          0           0
CCAG:
```

```
...
CHASSIS:
   2001 cardFailure                       MA  gen          0           0
   2002 cardInserted                      MI  gen          4           0
   2003 cardRemoved                       MI  gen          0           0
   2004 cardWrong                         MI  gen          0           0
   2005 EnvTemperatureTooHigh             MA  gen          0           0
...
DEBUG:
L  2001 traceEvent                        MI  gen          0           0
DOT1X:
FILTER:
   2001 filterPBRPacketsDropped           MI  gen          0           0
IGMP:
   2001 vRtrIgmpIfRxQueryVerMismatch      WA  gen          0           0
   2002 vRtrIgmpIfCModeRxQueryMismatch    WA  gen          0           0
IGMP_SNOOPING:
IP:
L  2001 clearRTMError                     MI  gen          0           0
L  2002 ipEtherBroadcast                  MI  gen          0           0
L  2003 ipDuplicateAddress                MI  gen          0           0
L  2004 ipArpInfoOverwritten              MI  gen          0           0
L  2005 fibAddFailed                      MA  gen          0           0
L  2006 qosNetworkPolicyMallocFailed      MA  gen          0           0
L  2007 ipArpBadInterface                 MI  gen          0           0
L  2008 ipArpDuplicateIpAddress           MI  gen          0           0
L  2009 ipArpDuplicateMacAddress          MI  gen          0           0
ISIS:
   2001 vRtrIsisDatabaseOverload          WA  gen          0           0
   2002 vRtrIsisManualAddressDrops        WA  gen          0           0
   2003 vRtrIsisCorruptedLSPDetected      WA  gen          0           0
   2004 vRtrIsisMaxSeqExceedAttempt       WA  gen          0           0
   2005 vRtrIsisIDLenMismatch             WA  gen          0           0
   2006 vRtrIsisMaxAreaAddrsMismatch      WA  gen          0           0
....
USER:
L  2001 cli_user_login                    MI  gen          2           0
L  2002 cli_user_logout                   MI  gen          1           0
L  2003 cli_user_login_failed             MI  gen          0           0
L  2004 cli_user_login_max_attempts       MI  gen          0           0
L  2005 ftp_user_login                    MI  gen          0           0
L  2006 ftp_user_logout                   MI  gen          0           0
L  2007 ftp_user_login_failed             MI  gen          0           0
L  2008 ftp_user_login_max_attempts       MI  gen          0           0
L  2009 cli_user_io                       MI  sup          0          48
L  2010 snmp_user_set                     MI  sup          0           0
L  2011 cli_config_io                     MI  gen       4357           0
VRRP:
   2001 vrrpTrapNewMaster                 MI  gen          0           0
   2002 vrrpTrapAuthFailure               MI  gen          0           0
   2003 tmnxVrrpIPListMismatch            MI  gen          0           0
   2004 tmnxVrrpIPListMismatchClear       MI  gen          0           0
   2005 tmnxVrrpMultipleOwners            MI  gen          0           0
   2006 tmnxVrrpBecameBackup              MI  gen          0           0
L  2007 vrrpPacketDiscarded               MI  gen          0           0
VRTR:
   2001 tmnxVRtrMidRouteTCA               MI  gen          0           0
   2002 tmnxVRtrHighRouteTCA              MI  gen          0           0
   2003 tmnxVRtrHighRouteCleared          MI  gen          0           0
```

```
   2004 tmnxVRtrIllegalLabelTCA          MA  gen          0           0
   2005 tmnxVRtrMcastMidRouteTCA         MI  gen          0           0
   2006 tmnxVRtrMcastMaxRoutesTCA        MI  gen          0           0
   2007 tmnxVRtrMcastMaxRoutesCleared    MI  gen          0           0
   2008 tmnxVRtrMaxArpEntriesTCA         MA  gen          0           0
   2009 tmnxVRtrMaxArpEntriesCleared     MI  gen          0           0
   2011 tmnxVRtrMaxRoutes                MI  gen          0           0
===============================================================================
A:ALA-1#
```

```
A:ALA-1# show log event-control ospf
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                          P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
   2001 ospfVirtIfStateChange               WA  gen          0           0
   2002 ospfNbrStateChange                  WA  gen          1           0
   2003 ospfVirtNbrStateChange              WA  gen          0           0
   2004 ospfIfConfigError                   WA  gen          0           0
   2005 ospfVirtIfConfigError               WA  gen          0           0
   2006 ospfIfAuthFailure                   WA  gen          0           0
   2007 ospfVirtIfAuthFailure               WA  gen          0           0
   2008 ospfIfRxBadPacket                   WA  gen          0           0
   2009 ospfVirtIfRxBadPacket               WA  gen          0           0
   2010 ospfTxRetransmit                    WA  sup          0           0
   2011 ospfVirtIfTxRetransmit              WA  sup          0           0
   2012 ospfOriginateLsa                    WA  sup          0         404
   2013 ospfMaxAgeLsa                       WA  gen          3           0
   2014 ospfLsdbOverflow                    WA  gen          0           0
   2015 ospfLsdbApproachingOverflow         WA  gen          0           0
   2016 ospfIfStateChange                   WA  gen          2           0
   2017 ospfNssaTranslatorStatusChange      WA  gen          0           0
   2018 vRtrOspfSpfRunsStopped              WA  gen          0           0
   2019 vRtrOspfSpfRunsRestarted            WA  gen          0           0
   2020 vRtrOspfOverloadEntered             WA  gen          1           0
   2021 vRtrOspfOverloadExited              WA  gen          0           0
   2022 ospfRestartStatusChange             WA  gen          0           0
   2023 ospfNbrRestartHelperStatusChange    WA  gen          0           0
   2024 ospfVirtNbrRestartHelperStsChg      WA  gen          0           0
===============================================================================
A:ALA-1#
```

```
A:ALA-1# show log event-control ospf ospfVirtIfStateChange
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                          P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
   2001 ospfVirtIfStateChange               WA  gen          0           0
===============================================================================
A:ALA-1#
```

event-handling

Syntax **event-handling**

Context show>log

Description This command enables the context to display Event Handling System (EHS) information.

handler

Syntax **handler** [*handler-name*]
handler detail

Context show>log>event-handling

Description This command enters the context to display EHS handler information.

Parameters *handler-name* — Specifies the name of a specific handler. 32 characters maximum.

detail — Keyword to list details of all handlers.

Output **Show Handler Output —** The following table describes handler output fields.

Label	Description
Handler	The name of the handler.
Description	The handler description string.
Admin State	The administrative state of the handler.
Oper State	The operational state of the handler.
Handler Action-List Entry	
Entry-id	The action-list entry identifier.
Description	The action-list entry description string.
Admin State	The administrative state of the action-list entry.
Policy Name	The name of the related script policy.
Policy Owner	The owner of the related script policy.
Last Exec	The timestamp of the last successful execution of the action-list entry.
Handler Action-List Entry Execution Statistics	

Label	Description (Continued)
Enqueued	The number of times the action-list entry was successfully passed on to the SR OS sub-system or module that will attempt to process and execute the action. For a script-policy entry, this indicates that the script request has been enqueued but does not necessarily indicate that the script has successfully launched or completed. For status and information about the script, use the **show**>**system**>**script-control** command.
Err Launch	The number of times the action-list entry was not successfully handed over to the next SR OS sub-system or module in the processing chain. This can be caused by a variety of conditions including a full script request input queue.
Err Adm Status	The number of times the action-list entry was not executed because the entry was administratively disabled.
Total	The total number of times that the action-list entry attempted execution.

Sample Output

```
A:node1>show>log>event-handling# handler

===============================================================================
Event Handling System - Handler List
===============================================================================
Handler                         Admin   Oper    Description
Name                            State   State
-------------------------------------------------------------------------------
h-sample                        up      up
h-main                          up      up
h-backup                        down    down
===============================================================================



*A:7950 XRS-20# show log event-handling handler "h-sample"

===============================================================================
Event Handling System - Handlers
===============================================================================

===============================================================================
Handler          : h-sample
===============================================================================
Description      : (Not Specified)
Admin State      : up                                Oper State : up

-------------------------------------------------------------------------------
Handler Action-List Entry
-------------------------------------------------------------------------------
Entry-id         : 10
Description      : (Not Specified)
Admin State      : up                                Oper State : up
Script
  Policy Name    : sp-sample
```

```
  Policy Owner   : TiMOS CLI
Min Delay        : 0
Last Exec        : 05/24/2015 19:03:31
-------------------------------------------------------------------------------
Handler Action-List Entry Execution Statistics
  Enqueued       : 4
  Err Launch     : 0
  Err Adm Status : 0
Total            : 4
===============================================================================
```

file-id

Syntax **file-id** [*log-file-id*]

Context show>log

Description This command displays event file log information.

If no command line parameters are specified, a summary output of all event log files is displayed.

Specifying a file ID displays detailed information on the event file log.

Parameters *log-file-id* — Displays detailed information on the specified event file log.

Output **Log File Output —** The following table describes the output fields for a log file summary.

Label	Description
file-id	The log file ID.
rollover	The rollover time for the log file which is how long in between partitioning of the file into a new file.
retention	The retention time for the file in the system which is how long the file should be retained in the file system.
admin location	The primary flash device specified for the file location. none — indicates no specific flash device was specified.
backup location	The secondary flash device specified for the file location if the admin location is not available. none — Indicates that no backup flash device was specified.
oper location	The actual flash device on which the log file exists.
file-id	The log file ID.
rollover	The rollover time for the log file which is how long in between partitioning of the file into a new file.

Label	Description (Continued)
retention	The retention time for the file in the system which is how long the file should be retained in the file system.
file name	The complete pathname of the file associated with the log ID.
expired	Indicates whether or not the retention period for this file has passed.
state	in progress – Indicates the current open log file. complete – Indicates the old log file.

Sample Output

```
A:ALA-1# show log file-id
===============================================================
File Id List
===============================================================
file-id   rollover  retention   admin     backup    oper
                                location  location  location
---------------------------------------------------------------
1           60         4        cf1:      cf2:      cf1:
2           60         3        cf1:      cf3:      cf1:
3         1440        12        cf1:      none      cf1:
10        1440        12        cf1:      none      none
11        1440        12        cf1:      none      none
15        1440        12        cf1:      none      none
20        1440        12        cf1:      none      none
===============================================================
A:ALA-1#


A:ALA-1# show log file-id 10
===============================================================
File Id List
===============================================================
file-id   rollover  retention   admin     backup    oper
                                location  location  location
---------------------------------------------------------------
10   1440        12        cf3:      cf2:      cf1:
Description : Main
===============================================================
File Id 10 Location cf1:
===============================================================
file name                                 expired   state
---------------------------------------------------------------
cf1:\log\log0302-20060501-012205        yes       complete
cf1:\log\log0302-20060501-014049        yes       complete
cf1:\log\log0302-20060501-015344        yes       complete
cf1:\log\log0302-20060501-015547        yes       in progress
===============================================================
A:ALA-1#
```

filter-id

Syntax **filter-id** [*filter-id*]

Context show>log

Description This command displays event log filter policy information.

Parameters *filter-id* — Displays detailed information on the specified event filter policy ID.

Output **Event Log Filter Summary Output —** The following table describes the output fields for event log filter summary information.

Table 48: Event Log Filter Summary Output Fields

Label	Description
Filter Id	The event log filter ID.
Applied	no. The event log filter is not currently in use by a log ID.
	yes. The event log filter is currently in use by a log ID.
Default Action	drop. The default action for the event log filter is to drop events not matching filter entries.
	forward. The default action for the event log filter is to forward events not matching filter entries.
Description	The description string for the filter ID.

Sample Output

```
*A:ALA-48>config>log# show log filter-id
===============================================================================
Log Filters
===============================================================================
Filter Applied Default Description
Id             Action
-------------------------------------------------------------------------------
1      no      forward
5      no      forward
10     no      forward
1001   yes     drop    Collect events for Serious Errors Log
===============================================================================
*A:ALA-48>config>log#
```

Event Log Filter Detailed Output — The following table describes the output fields for detailed event log filter information .

Table 49: Event Log Filter Detail Output Fields

Label	Description
Filter-id	The event log filter ID.
Applied	no — The event log filter is not currently in use by a log ID.
	yes — The event log filter is currently in use by a log ID.
Default Action	drop — The default action for the event log filter is to drop events not matching filter entries.
	forward — The default action for the event log filter is to forward events not matching filter entries.
Description (Filter-id)	The description string for the filter ID.

.

Table 50: Log Filter Match Criteria Output Fields

Label	Description
Entry-id	The event log filter entry ID.
Action	default — There is no explicit action for the event log filter entry and the filter's default action is used on matching events.
	drop — The action for the event log filter entry is to drop matching events.
	forward — The action for the event log filter entry is to forward matching events.
Description (Entry-id)	The description string for the event log filter entry.
Application	The event log filter entry application match criterion.
Event Number	The event log filter entry application event ID match criterion.

Table 50: Log Filter Match Criteria Output Fields (Continued)

Label	Description
Severity	cleared — The log event filter entry application event severity cleared match criterion. indeterminate — The log event filter entry application event severity indeterminate match criterion. critical — The log event filter entry application event severity critical match criterion. major — The log event filter entry application event severity cleared match criterion. minor — The log event filter entry application event severity minor match criterion. warning — The log event filter entry application event severity warning match criterion.
Subject	Displays the event log filter entry application event ID subject string match criterion.
Router	Displays the event log filter entry application event ID **router** *router-instance* string match criterion.
Operator	There is an operator field for each match criteria: application, event number, severity, and subject. equal — Matches when equal to the match criterion. greaterThan — Matches when greater than the match criterion. greaterThanOrEqual — Matches when greater than or equal to the match criterion. lessThan — Matches when less than the match criterion. lessThanOrEqual — Matches when less than or equal to the match criterion. notEqual — Matches when not equal to the match criterion. off — No operator specified for the match criterion.

Sample Output

```
*A:ALA-48>config>log# show log filter-id 1001
===============================================================================
Log Filter
===============================================================================
Filter-id     : 1001     Applied       : yes      Default Action: drop
Description   : Collect events for Serious Errors Log
```

```
-------------------------------------------------------------------------------
Log Filter Match Criteria
-------------------------------------------------------------------------------
Entry-id      : 10                      Action        : forward
Application   :                         Operator      : off
Event Number  : 0                       Operator      : off
Severity      : major                   Operator      : greaterThanOrEqual
Subject       :                         Operator      : off
Match Type    : exact string                          :
Router        :                         Operator      : off
Match Type    : exact string                          :
Description   : Collect only events of major severity or higher
-------------------------------------------------------------------------------
===============================================================================
*A:ALA-48>config>log#
```

log-collector

Syntax **log-collector**

Context show>log

Description Show log collector statistics for the main, security, change and debug log collectors.

Output **Log-Collector Output —** The following table describes log-collector output fields.

Table 51: Show Log-Collector Output Fields

Label	Description
<Collector Name>	Main — The main event stream contains the events that are not explicitly directed to any other event stream. Security — 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. Change — The change event stream contains all events that directly affect the configuration or operation of this node. Debug — The debug-trace stream contains all messages in the debug stream.
Dest. Log ID	Specifies the event log stream destination.
Filter ID	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Status	Enabled — Logging is enabled. Disabled — Logging is disabled.

Table 51: Show Log-Collector Output Fields (Continued)

Label	Description
Dest. Type	Console — A log created with the console type destination displays events to the physical console device. Events are displayed to the console screen whether a user is logged in to the console or not. Session — A user logged in to the console device or connected to the CLI via a remote telnet or SSH session can also create a log with a destination type of 'session'. Events are displayed to the session device until the user logs off. Syslog — Log events are sent to a syslog receiver. SNMP traps — Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables. File — All selected log events will be directed to a file on one of the CPM's compact flash disks. Memory — All selected log events will be directed to an in-memory storage area.

Sample Output

```
A:ALA-1# show log log-collector
===============================================================================
Log Collectors
===============================================================================
Main                Logged   : 1224                    Dropped  : 0
  Dest Log Id: 99    Filter Id: 0      Status: enabled    Dest Type: memory
  Dest Log Id: 100   Filter Id: 1001   Status: enabled    Dest Type: memory

Security            Logged   : 3                       Dropped  : 0

Change              Logged   : 3896                    Dropped  : 0

Debug               Logged   : 0                       Dropped  : 0

===============================================================================
A:ALA-1#
```

log-id

Syntax **log-id** [*log-id*] [**severity** *severity-level*] [**application** *application*] [**sequence** *from-seq* [*to-seq*]] [**count** *count*] [**router** *router-instance* [**expression**]] [**message** *message* [**regular-**

expression]] [**subject** *subject* [**regexp**]] [**ascending** | **descending**] [**message** *format* [**msg-regexp**]]

Context show>log

Description This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.

If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics.

If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed.

Contents of logs with console, session or syslog destinations cannot be displayed. The actual events can only be viewed on the receiving syslog or console device.

Parameters *log-id* — Displays the contents of the specified file log or memory log ID. The log ID must have a destination of an SNMP or file log or a memory log for this parameter to be used.

Default Displays the event log summary

Values 1 — 99

severity *severity-level* — Displays only events with the specified and higher severity.

Default All severity levels

Values cleared, indeterminate, critical, major, minor, warning

application *application* — Displays only events generated by the specified application.

Default All applications

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

expression — Specifies to use a regular expression as match criteria for the router instance string.

sequence *from-seq* [*to-seq*] — Displays the log entry numbers from a particular entry sequence number (*from-seq*) to another sequence number (*to-seq*). The *to-seq* value must be larger than the *from-seq* value.

If the *to-seq* number is not provided, the log contents to the end of the log is displayed unless the **count** parameter is present in which case the number of entries displayed is limited by the **count**.

Default All sequence numbers

Values 1 — 4294967295

count *count* — Limits the number of log entries displayed to the *number* specified.

Default All log entries

Values 1 — 4294967295

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

message *format* — Specifies a message string up to 400 characters to be used in the display criteria.

msg-regexp — Specifies to use a regular expression as parameters with the specified *message* string.

subject *subject* — Displays only log entries matching the specified text *subject* string. The subject is the object affected by the event, for example the port-id would be the subject for a link-up or link-down event.

regexp — Specifies to use a regular expression as parameters with the specified *subject* string..

ascending | **descending** — Specifies sort direction. Logs are normally shown from the newest entry to the oldest in **descending** sequence number order on the screen. When using the **ascending** parameter, the log will be shown from the oldest to the newest entry.

Default Descending

Output **Show Log-ID Output —** The following table describes the log ID field output.

Label	Description
Log Id	An event log destination.
Source	no – The event log filter is not currently in use by a log ID. yes – The event log filter is currently in use by a log ID.
Filter ID	The value is the index to the entry which defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Admin State	Up – Indicates that the administrative state is up. Down – Indicates that the administrative state is down.
Oper State	Up – Indicates that the operational state is up. Down – Indicates that the operational state is down.
Logged	The number of events that have been sent to the log source(s) that were forwarded to the log destination.
Dropped	The number of events that have been sent to the log source(s) that were not forwarded to the log destination because they were filtered out by the log filter.
Dest. Type	Console – All selected log events are directed to the system console. If the console is not connected, then all entries are dropped. Syslog – All selected log events are sent to the syslog address. SNMP traps – Events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables. File – All selected log events will be directed to a file on one of the CPM's compact flash disks.

Label	Description (Continued)
	Memory – All selected log events will be directed to an in-memory storage area.
Dest ID	The event log stream destination.
Size	The allocated memory size for the log.
Time format	The time format specifies the type of timestamp format for events sent to logs where log ID destination is either syslog or file. When the time format is UTC, timestamps are written using the Coordinated Universal Time value. When the time format is local, timestamps are written in the system's local time.

Sample Output

```
A:ALA-1# show log log-id
===============================================================================
Event Logs
===============================================================================
Log Source    Filter Admin Oper  Logged  Dropped Dest       Dest  Size
Id            Id     State State                Type       Id
-------------------------------------------------------------------------------
1   none      none   up    down  52      0       file       10     N/A
2   C         none   up    up    41      0       syslog     1      N/A
99  M         none   up    up    2135    0       memory             500
===============================================================================
A:ALA-1#
```

Sample Memory or File Event Log Contents Output

```
A:gal171# show log log-id 99
===============================================================================
Event Log 99
===============================================================================
Description : Default System Log
Memory Log contents  [size=500   next event=70  (not wrapped)]

69 2007/01/25 18:20:40.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

68 2007/01/25 17:48:38.16 UTC WARNING: SYSTEM #2006 Base LOGGER
"New event throttle interval 10, configuration modified"



67 2007/01/25 00:34:53.97 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM
card."

66 2007/01/24 22:59:22.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
```

```
"The active CPM card A is operating in singleton mode.  There is no standby CPM card."

65 2007/01/24 02:08:47.92 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode.  There is no standby CPM card."
...
===============================================================================
A:gal171


A:NS061550532>config>log>snmp-trap-group# show log log-id 1
===============================================================================
Event Log 1
===============================================================================
SNMP Log contents  [size=100   next event=3  (not wrapped)]
Cannot send to SNMP target address 10.1.1.1.
Waiting to replay starting from event #2

14 2000/01/05 00:54:09.11 UTC WARNING: MPLS #2007 Base VR 1:
"Instance is in administrative state: inService, operational state: inService"

13 2000/01/05 00:54:09.11 UTC WARNING: MPLS #2008 Base VR 1:
"Interface linkToIxia is in administrative state: inService, operational state:
inService"
....
===============================================================================
A:NS061550532>config>log>snmp-trap-group#
```

snmp-trap-group

Syntax **snmp-trap-group** [*log-id*]

Context show>log

Description This command displays SNMP trap group configuration information.

Parameters *log-id* — Displays only SNMP trap group information for the specified trap group log ID.

Values 1 — 99

Output **SNMP Trap Group Output —** The following table describes SNMP trap group output fields.

Table 52: SNMP Trap Group Output Fields

Label	Description
Log-ID	The log destination ID for an event stream.
Address	The IP address of the trap receiver,
Port	The destination UDP port used for sending traps to the destination, expressed as a decimal integer.
Version	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are snmpv1, snmpv2c, snmpv3.

Table 52: SNMP Trap Group Output Fields (Continued)

Label	Description
Community	The community string required by **snmpv1** or **snmpv2c** trap receivers.
Security-Level	The required authentication and privacy levels required to access the views on this node.
Replay	Indicates whether or not the replay parameter has been configured, enabled or disabled, for the trap-target address.
Replay from	Indicates the sequence ID of the first missed notification that will be replayed when a route is added to the routing table by which trap-target address can be reached. If no notifications are waiting to be replayed this field shows n/a.
Last Replay	Indicates the last time missed events were replayed to the trap-target address. If no events have ever been replayed this field shows never.

Sample Output

```
A:SetupCLI>config>log>snmp-trap-group# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : ntt-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : ntttesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : ntttesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
A:SetupCLI>config>log>snmp-trap-group#
```

syslog

Syntax **syslog** [*syslog-id*]

Context show>log

Description This command displays syslog event log destination summary information or detailed information on a specific syslog destination.

Parameters *syslog-id* — Displays detailed information on the specified syslog event log destination.

Values 1 — 10

Output **Syslog Event Log Destination Summary Output —** The following table describes the syslog output fields.

Table 53: Show Log Syslog Output Fields

Label	Description
Syslog ID	The syslog ID number for the syslog destination.
IP Address	The IP address of the syslog target host.
Port	The configured UDP port number used when sending syslog messages.
Facility	The facility code for messages sent to the syslog target host.
Severity Level	The syslog message severity level threshold.
Below Level Dropped	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.
Prefix Present	Yes – A log prefix was prepended to the syslog message sent to the syslog host. No – A log prefix was not prepended to the syslog message sent to the syslog host.
Description	A text description stored in the configuration file for a configuration context.
LogPrefix	The prefix string prepended to the syslog message.
Log-id	Events are directed to this destination.

Sample Output

```
*A:ALA-48>config>log# show log syslog
===============================================================================
Syslog Target Hosts
===============================================================================
Id     Ip Address                                      Port        Sev Level
         Below Level Drop                                Facility    Pfx Level
```

```
-------------------------------------------------------------------------------
2      unknown                                          514         info
         0                                                local7      yes
3      unknown                                          514         info
         0                                                local7      yes
5      unknown                                          514         info
         0                                                local7      yes
10     unknown                                          514         info
         0                                                local7      yes
===============================================================================
*A:ALA-48>config>log#

*A:MV-SR>config>log# show log syslog 1
===============================================================================
Syslog Target 1
===============================================================================
IP Address       : 192.168.15.22
Port             : 514
Log-ids          : none
Prefix           : Sr12
Facility         : local1
Severity Level   : info
Prefix Level     : yes
Below Level Drop : 0
Description      : Linux Station Springsteen
===============================================================================
*A:MV-SR>config>log#
```

Clear Commands

log

Syntax **log** *log-id*

Context clear

Description Reinitializes/rolls over the specified memory/file event log ID. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by this command.

This command is only applicable to event logs that are directed to file destinations and memory destinations.

SNMP, syslog and console/session logs are not affected by this command.

Parameters *log-id.* The event log ID to be initialized/rolled over.

Values 1 — 100