# Configuring Logging with CLI

This section provides information to configure logging using the command line interface.

Topics in this section include:

# Log Configuration Overview

Configure logging parameters to save information in a log file or direct the messages to other devices. Logging does the following:

- Provides you with logging information for monitoring and troubleshooting.
- Allows you to select the types of logging information to be recorded.
- Allows you to assign a severity to the log messages.
- Allows you to select the source and target of logging information.

## Log Types

Logs can be configured in the following contexts:

- Log file — Log files can contain log event message streams or accounting/billing information. Log file IDs are used to direct events, alarms/traps and debug information to their respective targets.
- SNMP trap groups — SNMP trap groups contain an IP address and community names which identify targets to send traps following specified events.
- Syslog — Information can be sent to a syslog host that is capable of receiving selected syslog messages from a network element.
- Event control — Configures a particular event or all events associated with an application to be generated or suppressed.
- Event filters — An event filter defines whether to forward or drop an event or trap based on match criteria.
- Accounting policies — An accounting policy defines the accounting records that will be created. Accounting policies can be applied to one or more service access points (SAPs).
- Event logs — An event log defines the types of events to be delivered to its associated destination.
- Event throttling rate — Defines the rate of throttling events.

# Basic Event Log Configuration

The most basic log configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays a log configuration example.

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
        event-control "bgp" 2001 generate critical
        file-id 1
            description "This is a test file-id."
            location cf1:
        exit
        file-id 2
            description "This is a test log."
            location cf1:
        exit
        snmp-trap-group 7
            trap-target 11.22.33.44 "snmpv2c" notify-community "public"
        exit
        log-id 2
            from main
            to file 2
        exit
----------------------------------------------
A:ALA-12>config>log#
```

# Common Configuration Tasks

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



## Configuring an Event Log

A event log file contains information used to direct events, alarms, traps, and debug information to their respective destinations. One or more event sources can be specified. File IDs, SNMP trap groups, or syslog IDs must be configured before they can be applied to an event log ID.

Use the following CLI syntax to configure a log file:

**CLI Syntax:**

```
config>log
 log-id log-id
    description description-string
    filter filter-id
    from {[main] [security] [change] [debug-trace]}
    to console
    to file file-id
    to memory [size]
    to session
    to snmp [size]
    to syslog syslog-id}
    time-format {local|utc}
    no shutdown
```

The following displays a log file configuration example:

```
ALA-12>config>log>log-id# info
----------------------------------------------
...
    log-id 2
           description "This is a test log file."
           filter 1
           from main security
           to file 1
    exit
...
----------------------------------------------
ALA-12>config>log>log-id#
```

# Configuring a File ID

To create a log file a file ID is defined, specifies the target CF drive, and the rollover and retention interval period for the file. The rollover interval is defined in minutes and determines how long a file will be used before it is closed and a new log file is created. The retention interval determines how long the file will be stored on the CF before it is deleted.

Use the following CLI syntax to configure a log file:

**CLI Syntax:**
```
config>log
    file-id log-file-id
        description description-string
        location cflash-id [backup-cflash-id]
        rollover minutes [retention hours]
```

The following displays a log file configuration example:

```
A:ALA-12>config>log# info
----------------------------------------
        file-id 1
            description "This is a log file."
            location cf1:
            rollover 600 retention 24
        exit
----------------------------------------
A:ALA-12>config>log#
```

# Configuring an Accounting Policy

Before an accounting policy can be created a target log file must be created to collect the accounting records. The files are stored in system memory of compact flash (cf1: or cf2:) in a compressed (tar) XML format and can be retrieved using FTP or SCP. See Configuring an Event Log on page 408 and Configuring a File ID on page 410.

Accounting policies must be configured in the **config>log** context before they can be applied to a service SAP or service interface, or applied to a network port.

The default accounting policy statement cannot be applied to LDP nor RSVP statistics collection records.

An accounting policy must define a record type and collection interval. Only one record type can be configured per accounting policy.

When creating accounting policies, one service accounting policy and one network accounting policy can be defined as default. If statistics collection is enabled on a SAP or network port and no accounting policy is applied, then the respective default policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.

Use the following CLI syntax to configure an accounting policy:

**CLI Syntax:**
```
config>log
 accounting-policy acct-policy-id interval minutes
    description description-string
    default
    record record-name
    to file log-file-id
    no shutdown
```

The following displays a accounting policy configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
    accounting-policy 4
        description "This is the default accounting policy."
        record complete-service-ingress-egress
        default
        to file 1
    exit
    accounting-policy 5
        description "This is a test accounting policy."
        record service-ingress-packets
        to file 3
    exit
----------------------------------------------
A:ALA-12>config>log#
```

# Configuring Event Control

Use the following CLI syntax to configure event control. Note that the **throttle** parameter used in the **event-control** command syntax enables throttling for a specific event type. The **config>log>throttle-rate** command configures the number of events and interval length to be applied to all event types that have throttling enabled by this **event-control** command.

**CLI Syntax:**
```
config>log
 event-control application-id [event-name|event-number] gen-
       erate [severity-level] [throttle]
 event-control application-id [event-name|event-number] sup-
       press
 throttle-rate events [interval seconds]
```

The following displays an event control configuration:

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
        throttle-rate 500 interval 10
        event-control "oam" 2001 generate throttle
        event-control "ospf" 2001 suppress
        event-control "ospf" 2003 generate cleared
        event-control "ospf" 2014 generate critical
..
------------------------------------------
A:ALA-12>config>log>filter#
```

# Configuring Throttle Rate

This command configures the number of events and interval length to be applied to all event types that have throttling enabled by the **event-control** command.

Use the following CLI syntax to configure the throttle rate.

**CLI Syntax:**
```
config>log#
          throttle-rate events [interval seconds]
```

The following displays a throttle rate configuration example:

```
*A:gal171>config>log# info
----------------------------------------------
        throttle-rate 500 interval 10
        event-control "bgp" 2001 generate throttle
----------------------------------------------
*A:gal171>config>log#
```

# Configuring a Log Filter

The following displays a log filter configuration example:

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
        file-id 1
            description "This is our log file."
            location cf1:
            rollover 600 retention 24
        exit
        filter 1
            default-action drop
            description "This is a sample filter."
            entry 1
                action forward
                match
                    application eq "mirror"
                    severity eq critical
                exit
            exit
        exit
...
       log-id 2
            shutdown
            description "This is a test log file."
            filter 1
            from main security
            to file 1
        exit
...
------------------------------------------
A:ALA-12>config>log#
```

## Configuring an SNMP Trap Group

The associated *log-id* does not have to configured before a **snmp-trap-group** can be created, however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

The following displays a basic SNMP trap group configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
...
      snmp-trap-group 2
         trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
        exit
...
     log-id 2
            description "This is a test log file."
            filter 1
            from main security
            to file 1
     exit
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays a SNMP trap group, log, and interface configuration examples:

```
A:SetupCLI>config>log# snmp-trap-group 44
A:SetupCLI>config>log>snmp-trap-group# info
----------------------------------------------
            trap-target "xyz-test" address xx.xx.x.x snmpv2c notify-community "xyztesting"
            trap-target "test2" address xx.xx.xx.x snmpv2c notify-community "xyztesting"
----------------------------------------------
*A:SetupCLI>config>log>log-id# info
----------------------------------------------
            from main
            to snmp
----------------------------------------------
*A:SetupCLI>config>router# interface xyz-test
*A:SetupCLI>config>router>if# info
----------------------------------------------
            address xx.xx.xx.x/24
            port 1/1/1
----------------------------------------------
*A:SetupCLI>config>router>if#
```

## Setting the Replay Parameter

For this example the replay parameter was set by a SNMP SET request for the trap-target address 10.10.10.3 which is bound to port-id 1/1/1.

```
A:SetupCLI>config>log>snmp-trap-group 44
A:SetupCLI>config>log>snmp-trap-group# info
----------------------------------------------
          trap-target "xyz-test" address 10.10.10.3 snmpv2c notify-community "xyztesting"
replay
            trap-target "test2" address 20.20.20.5 snmpv2c notify-community "xyztesting"
----------------------------------------------
A:SetupCLI>config>log>snmp-trap-group#
```

In the following output, note that the **Replay** field changed from disabled to enabled.

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

Since no events are waiting to be replayed, the log displays as before.

```
A:SetupCLI>config>log>snmp-trap-group# show log log-id 44
===============================================================================
Event Log 44
===============================================================================
SNMP Log contents  [size=100   next event=3819  (wrapped)]

3818 2008/04/22 23:35:39.89 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed
administrative state: inService, operational state: inService"

3817 2008/04/22 23:35:39.89 UTC WARNING: SNMP #2005 Base xyz-test
"Interface xyz-test is operational"

3816 2008/04/22 23:35:39.89 UTC WARNING: SNMP #2005 Base 1/1/1
"Interface 1/1/1 is operational"

3815 2008/04/22 23:35:39.71 UTC WARNING: SYSTEM #2009 Base CHASSIS
"Status of Mda 1/1 changed administrative state: inService, operational state: inService"

3814 2008/04/22 23:35:38.88 UTC MINOR: CHASSIS #2002 Base Mda 1/2
"Class MDA Module : inserted"

3813 2008/04/22 23:35:38.88 UTC MINOR: CHASSIS #2002 Base Mda 1/1
```

## Shutdown In-Band Port

A **shutdown** on the in-band port that the trap-target address is bound to causes the route to that particular trap target to be removed from the route table. When the SNMP module is notified of this event, it marks the trap-target as inaccessible and saves the sequence-id of the first SNMP notification that will be missed by the trap-target.

**Example:**

```
config>log>snmp-trap-group# exit all
#configure port 1/1/1 shutdown
#
# tools perform log test-event
#
```

The **Replay from** field is updated with the sequence-id of the first event that will be replayed when the trap-target address is added back to the route table.

```
*A:SetupCLI# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : xyz-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : enabled
Replay from : event #3819
Last replay : never
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
*A:SetupCLI#
```

A display of the event log indicates which trap targets are not accessible and waiting for notification replay and the sequence ID of the first notification that will be replayed. Note that if there are more missed events than the log size, the replay will actually start from the first available missed event.

```
*A:SetupCLI# show log log-id 44
===============================================================================
Event Log 44
===============================================================================
SNMP Log contents  [size=100   next event=3821  (wrapped)]
Cannot send to SNMP target address 10.10.10.3.
Waiting to replay starting from event #3819

3820 2008/04/22 23:41:28.00 UTC INDETERMINATE: LOGGER #2011 Base Event Test
"Test event has been generated with system object identifier tmnxModelSR12Reg.
System description: TiMOS-B-0.0.private both/i386 ALCATEL SR 7750 Copyright (c) 2000-2008
Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Tue Apr 22 14:41:18 PDT 2008 by test123 in /test123/ws/panos/main"

3819 2008/04/22 23:41:20.37 UTC WARNING: MC_REDUNDANCY #2022 Base operational state of
peer chan*
"The MC-Ring operational state of peer 2.2.2.2 changed to outOfService."

3818 2008/04/22 23:35:39.89 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed
administrative state: inService, operational state: inService"

3823 2008/04/22 23:41:49.82 UTC WARNING: SNMP #2005 Base xyz-test
"Interface xyz-test is operational"
```

## No Shutdown Port

A **no shutdown** command executed on the in-band port to which the trap-target address is bound will cause the route to that trap target to be re-added to the route table. When the SNMP trap module is notified of this event, it resends the notifications that were missed while there was no route to the trap-target address.

**Example:**

```
configure# port 1/1/1 no shutdown
#
# tools perform log test-event
```

After the notifications have been replayed the **Replay from** field indicates n/a because there are no more notifications waiting to be replayed and the **Last replay** field timestamp has been updated.

```
*A:SetupCLI# show log snmp-trap-group 44
===============================================================================
SNMP Trap Group 44
===============================================================================
Description : none
-------------------------------------------------------------------------------
Name        : xyz-test
Address     : 10.10.10.3
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : enabled
Replay from : n/a
Last replay : 04/22/2008 18:52:36
-------------------------------------------------------------------------------
Name        : test2
Address     : 20.20.20.5
Port        : 162
Version     : v2c
Community   : xyztesting
Sec. Level  : none
Replay      : disabled
Replay from : n/a
Last replay : never
===============================================================================
*A:SetupCLI#
```

A display of the event log shows that it is no longer waiting to replay notifications to one or more of its trap target addresses. An event message has been written to the logger that indicates the replay to the trap-target address has happened and displays the notification sequence ID of the first and last replayed notifications.

```
*A:SetupCLI# show log log-id 44
===============================================================================
```

```
Event Log 44
===============================================================================
SNMP Log contents  [size=100   next event=3827  (wrapped)]

3826 2008/04/22 23:42:02.15 UTC MAJOR: LOGGER #2015 Base Log-id 44
"Missed events 3819 to 3825 from Log-id 44 have been resent to SNMP notification target
address 10.10.10.3."

3825 2008/04/22 23:42:02.15 UTC INDETERMINATE: LOGGER #2011 Base Event Test
"Test event has been generated with system object identifier tmnxModelSR12Reg.
System description: TiMOS-B-0.0.private both/i386 ALCATEL SR 7750 Copyright (c) 2000-2008
Alcatel-Lucent.
All rights reserved. All use subject to applicable license agreements.
Built on Tue Apr 22 14:41:18 PDT 2008 by test123 in /test123/ws/panos/main"

3824 2008/04/22 23:41:49.82 UTC WARNING: SYSTEM #2009 Base IP
"Status of vRtrIfTable: router Base (index 1) interface xyz-test (index 35) changed admin-
istrative s
tate: inService, operational state: inService"

3823 2008/04/22 23:41:49.82 UTC WARNING: SNMP #2005 Base xyz-test
"Interface xyz-test is operational"
```

## Configuring a Syslog Target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

The following displays a syslog configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        syslog 1
            description "This is a syslog file."
            address 10.10.10.104
            facility user
            level warning
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

## Configuring an Accounting Custom Record

```
A:ALA-48>config>subscr-mgmt>acct-plcy# info
----------------------------------------------
..
            custom-record
                queue 1
                    i-counters
                        high-octets-discarded-count
                        low-octets-discarded-count
                        in-profile-octets-forwarded-count
                        out-profile-octets-forwarded-count
                    exit
                    e-counters
                        in-profile-octets-forwarded-count
                        in-profile-octets-discarded-count
                        out-profile-octets-forwarded-count
                        out-profile-octets-discarded-count
                    exit
                exit
                significant-change 20
                ref-queue all
                    i-counters
                        in-profile-packets-forwarded-count
                        out-profile-packets-forwarded-count
                    exit
                    e-counters
                        in-profile-packets-forwarded-count
                        out-profile-packets-forwarded-count
                    exit
                exit
..
----------------------------------------------
A:ALA-48>config>subscr-mgmt>acct-plcy#
```

The following is an example custom record configuration.

```
Dut-C>config>log>acct-policy>cr# info
----------------------------------------------
                aa-specific
                    aa-sub-counters
                        short-duration-flow-count
                        medium-duration-flow-count
                        long-duration-flow-count
                        total-flow-duration
                        total-flows-completed-count
                    exit
                    from-aa-sub-counters
                        flows-admitted-count
                        flows-denied-count
                        flows-active-count
                        packets-admitted-count
                        octets-admitted-count
                        packets-denied-count
                        octets-denied-count
                        max-throughput-octet-count
```

```
                        max-throughput-packet-count
                        max-throughput-timestamp
                        forwarding-class
                    exit
                    to-aa-sub-counters
                        flows-admitted-count
                        flows-denied-count
                        flows-active-count
                        packets-admitted-count
                        octets-admitted-count
                        packets-denied-count
                        octets-denied-count
                        max-throughput-octet-count
                        max-throughput-packet-count
                        max-throughput-timestamp
                        forwarding-class
                    exit
                exit
                significant-change 1
                ref-aa-specific-counter any
------------------------------------------------
```

# Log Management Tasks

This section discusses the following logging tasks:

# Modifying a Log File

Use the following CLI syntax to modify a log file:

**CLI Syntax:**
```
config>log
 log-id log-id
    description description-string
    filter filter-id
    from {[main] [security] [change] [debug-trace]}
    to console
    to file file-id
    to memory [size]
    to session
    to snmp [size]
    to syslog syslog-id}
```

The following displays the current log configuration:

```
ALA-12>config>log>log-id# info
----------------------------------------------
...
    log-id 2
           description "This is a test log file."
           filter 1
           from main security
           to file 1
    exit
...
----------------------------------------------
ALA-12>config>log>log-id#
```

The following displays an example to modify log file parameters:

**Example:**
```
config# log
config>log# log-id 2
config>log>log-id# description "Chassis log file."
config>log>log-id# filter 2
config>log>log-id# from security
config>log>log-id# exit
```

The following displays the modified log file configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
     log-id 2
            description "Chassis log file."
            filter 2
            from security
            to file 1
     exit
...
----------------------------------------------
A:ALA-12>config>log#
```

# Deleting a Log File

The log ID must be shutdown first before it can be deleted. In a previous example, **file 1** is associated with **log-id 2**.

```
A:ALA-12>config>log# info
----------------------------------------------
     file-id 1
            description "LocationTest."
            location cf1:
            rollover 600 retention 24
        exit
...
     log-id 2
            description "Chassis log file."
            filter 2
            from security
            to file 1
     exit
...
----------------------------------------------
A:ALA-12>config>log#
```

Use the following CLI syntax to delete a log file:

**CLI Syntax:**
```
config>log
    no log-id log-id
       shutdown
```

The following displays an example to delete a log file:

**Example**:
```
config# log
config>log# log-id 2
config>log>log-id# shutdown
config>log>log-id# exit
config>log# no log-id 2
```

# Modifying a File ID

**NOTE**: When the **file-id** location parameter is modified, log files are not written to the new location until a rollover occurs or the log is manually cleared. A rollover can be forced by using the **clear>log** command. Subsequent log entries are then written to the new location. If a rollover does not occur or the log not cleared, the old location remains in effect.

Use the following CLI syntax to modify a log file:

**CLI Syntax:**
```
config>log
    file-id log-file-id
       description description-string
       location [cflash-id] [backup-cflash-id]
       rollover minutes [retention hours]
```

The following displays the current log configuration:

```
A:ALA-12>config>log# info
----------------------------------------
        file-id 1
            description "This is a log file."
            location cf1:
            rollover 600 retention 24
        exit
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example to modify log file parameters:

**Example**:
```
config# log
config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# location cf2:
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit
```

The following displays the file modifications:

```
A:ALA-12>config>log# info
----------------------------------------------
...
       file-id 1
            description "LocationTest."
            location cf2:
            rollover 2880 retention 500
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

## Deleting a File ID

**NOTE**: All references to the file ID must be deleted before the file ID can be removed.

Use the following CLI syntax to delete a log ID:

**CLI Syntax:**
```
config>log
 no file-id log-file-id
```

The following displays an example to delete a file ID:

**Example**:
```
config>log# no file-id 1
```

## Modifying a Syslog ID

**NOTE**: All references to the syslog ID must be deleted before the syslog ID can be removed.

Use the following CLI syntax to modify a syslog ID parameters:

**CLI Syntax:**
```
config>log
 syslog syslog-id
    description description-string
    address ip-address
    log-prefix log-prefix-string
    port port
    level {emergency|alert|critical|error|warning|notice|in-
          fo|debug}
    facility syslog-facility
```

The following displays an example of the syslog ID modifications:

**Example**:
```
config# log
config>log# syslog 1
config>log>syslog$ description "Test syslog."
config>log>syslog# address 10.10.0.91
config>log>syslog# facility mail
config>log>syslog# level info
```

The following displays the syslog configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        syslog 1
            description "Test syslog."
            address 10.10.10.91
            facility mail
            level info
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

## Deleting a Syslog

Use the following CLI syntax to delete a syslog file:

**CLI Syntax:**
```
config>log
 no syslog syslog-id
```

The following displays an example to delete a syslog ID:

**Example**:
```
config# log
config>log# no syslog 1
```

# Modifying an SNMP Trap Group

Use the following CLI syntax to modify an SNMP trap group:

**CLI Syntax:**
```
config>log
 snmp-trap-group log-id
    trap-target name [address ip-address] [port port] [sn-
          mpv1|snmpv2c| snmpv3] notify-community communi-
          tyName |snmpv3SecurityName [security-level {no-
          auth-no-privacy|auth-no-privacy|privacy}]
```

The following displays the current SNMP trap group configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
      snmp-trap-group 10
         trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example of the command usage to modify an SNMP trap group:

**Example**:
```
config# log
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.10.104:5
config>log>snmp-trap-group# snmp-trap-group# trap-target
10.10.0.91:1 snmpv2c notify-community "com1"
```

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        snmp-trap-group 10
            trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
        exit
...
----------------------------------------------
A:ALA-12>config>log#
```

## Deleting an SNMP Trap Group

Use the following CLI syntax to delete a trap target and SNMP trap group:

**CLI Syntax:**
```
config>log
    no snmp-trap-group log-id
       no trap-target name
```

The following displays the SNMP trap group configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
       snmp-trap-group 10
           trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
       exit
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example to delete a trap target and an SNMP trap group.

**Example**:
```
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.0.91:1
config>log>snmp-trap-group# exit
config>log# no snmp-trap-group 10
```

## Modifying a Log Filter

Use the following CLI syntax to modify a log filter:

**CLI Syntax:**
```
config>log
    filter filter-id
       default-action {drop|forward}
       description description-string
       entry entry-id
          action {drop|forward}
          description description-string
          match
             application {eq|neq} application-id
             number {eq|neq|lt|lte|gt|gte} event-id
             router {eq|neq} router-instance [regexp]
             severity {eq|neq|lt|lte|gt|gte} severity-level
             subject {eq|neq} subject [regexp]
```

The following output displays the current log filter configuration:

```
ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
...
        filter 1
            default-action drop
            description "This is a sample filter."
            entry 1
                action forward
                match
                    application eq "mirror"
                    severity eq critical
                exit
            exit
        exit
...
------------------------------------------
ALA-12>config>log#
```

The following displays an example of the log filter modifications:

**Example**:
```
config# log
config>log# filter 1
config>log>filter# description "This allows <n>."
config>log>filter# default-action forward
config>log>filter# entry 1
config>log>filter>entry$ action drop
config>log>filter>entry# match
config>log>filter>entry>match# application eq user
config>log>filter>entry>match# number eq 2001
config>log>filter>entry>match# no severity
config>log>filter>entry>match# exit
```

The following displays the log filter configuration:

```
A:ALA-12>config>log>filter# info
----------------------------------------
...
        filter 1
            description "This allows <n>."
            entry 1
                action drop
                match
                    application eq "user"
                    number eq 2001
                exit
            exit
        exit
...
----------------------------------------
A:ALA-12>config>log>filter#
```

## Deleting a Log Filter

Use the following CLI syntax to delete a log filter:

**CLI Syntax:** `config>log`
`no filter filter-id`

The following output displays the current log filter configuration:

```
A:ALA-12>config>log>filter# info
----------------------------------------
...
        filter 1
            description "This allows <n>."
            entry 1
                action drop
                match
                    application eq "user"
                    number eq 2001
                exit
            exit
        exit
...
----------------------------------------
A:ALA-12>config>log>filter#
```

The following displays an example of the command usage to delete a log filter:

**Example**: `config>log# no filter 1`

## Modifying Event Control Parameters

Use the following CLI syntax to modify event control parameters:

**CLI Syntax:** `config>log`
`event-control application-id [event-name|event-number] generate[severity-level] [throttle]`
`event-control application-id [event-name|event-number] suppress`

The following displays the current event control configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
    event-control "bgp" 2014 generate critical
...
----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example of an event control modifications:

**Example**:
```
config# log
        config>log# event-control bgp 2014 suppress
```

The following displays the log filter configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
...
        event-control "bgp" 2014 suppress
...
----------------------------------------------
A:ALA-12>config>log#
```

## Returning to the Default Event Control Configuration

The **no** form of the **event-control** command returns modified values back to the default values.

Use the following CLI syntax to modify event control parameters:

**CLI Syntax:**
```
config>log
    no event-control application [event-name |event-nunmber]
```

The following displays an example of the command usage to return to the default values:

**Example**:
```
config# log
        config>log# no event-control "bgp" 2001
        config>log# no event-control "bgp" 2002
        config>log# no event-control "bgp" 2014
```

```
A:ALA-12>config>log# info detail
----------------------------------------------
#----------------------------------------
echo "Log Configuration"
#----------------------------------------
        event-control "bgp" 2001 generate minor
        event-control "bgp" 2002 generate warning
        event-control "bgp" 2003 generate warning
        event-control "bgp" 2004 generate critical
        event-control "bgp" 2005 generate warning
        event-control "bgp" 2006 generate warning
        event-control "bgp" 2007 generate warning
        event-control "bgp" 2008 generate warning
        event-control "bgp" 2009 generate warning
```

```
        event-control "bgp" 2010 generate warning
        event-control "bgp" 2011 generate warning
        event-control "bgp" 2012 generate warning
        event-control "bgp" 2013 generate warning
        event-control "bgp" 2014 generate warning
        event-control "bgp" 2015 generate critical
        event-control "bgp" 2016 generate warning
...
-------------------------------------------
A:ALA-12>config>log#
```