Show Commands

Security Commands

access-group

Syntax **access-group** [*group-name*]

Context show>system>security

Description This command displays SNMP access group information.

Parameters *group-name* — This command displays information for the specified access group.

Output **Security Access Group Output —** The following table describes security access group output fields..

Table 12: Show System Security Access Group Output Fields

Label	Description
Group name	The access group name.
Security model	The security model required to access the views configured in this node.
Security level	Specifies the required authentication and privacy levels to access the views configured in this node.
Read view	Specifies the variable of the view to read the MIB objects.
Write view	Specifies the variable of the view to configure the contents of the agent.
Notify view	Specifies the variable of the view to send a trap about MIB objects.

Sample Output

```
A:ALA-4# show system security access-group
===============================================================================
Access Groups
===============================================================================
group name        security  security  read          write         notify
                  model     level     view          view          view
-------------------------------------------------------------------------------
snmp-ro           snmpv1    none      no-security                 no-security
snmp-ro           snmpv2c   none      no-security                 no-security
snmp-rw           snmpv1    none      no-security   no-security   no-security
snmp-rw           snmpv2c   none      no-security   no-security   no-security
snmp-rwa          snmpv1    none      iso           iso           iso
snmp-rwa          snmpv2c   none      iso           iso           iso
```

```
snmp-trap         snmpv1    none                                        iso
snmp-trap         snmpv2c   none                                        iso
===============================================================================
A:ALA-7#
```

authentication

Syntax **authentication** [**statistics**]

Context show>system>security

Description This command displays system login authentication configuration and statistics.

Parameters **statistics —** Appends login and accounting statistics to the display.

Output **Authentication Output —** The following table describes system security authentication output fields.

Table 13: Show System Security Authentication Output Fields

Label	Description
`Sequence`	The sequence in which authentication is processed.
`Server address`	The IP address of the RADIUS server.
`Status`	Current status of the RADIUS server.
`Type`	The authentication type.
`Timeout (secs)`	The number of seconds the router waits for a response from a RADIUS server.
`Single connection`	`Enabled` — Specifies a single connection to the TACACS+ server and validates everything via that connection. `Disabled` — The TACACS+ protocol operation is disabled.
`Retry count`	Displays the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server.
`Connection errors`	Displays the number of times a user has attempted to login irrespective of whether the login succeeded or failed.
`Accepted logins`	The number of times the user has successfully logged in.
`Rejected logins`	The number of unsuccessful login attempts.
`Sent packets`	The number of packets sent.
`Rejected packets`	The number of packets rejected.

Sample Output

```
A:ALA-4# show system security authentication
===============================================================================
Authentication                  sequence : radius tacplus local
===============================================================================
server address   status  type    timeout(secs)  single connection  retry count
-------------------------------------------------------------------------------
10.10.10.103     up      radius  5              n/a                5
10.10.0.1        up      radius  5              n/a                5
10.10.0.2        up      radius  5              n/a                5
10.10.0.3        up      radius  5              n/a                5
-------------------------------------------------------------------------------
radius admin status  : down
tacplus admin status : up
health check         : enabled
-------------------------------------------------------------------------------
No. of Servers: 4
===============================================================================
A:ALA-4#
```

```
A:ALA-7>show>system>security# authentication statistics
===============================================================================
Authentication                  sequence : radius tacplus local
===============================================================================
server address   status  type    timeout(secs)  single connection  retry count
-------------------------------------------------------------------------------
10.10.10.103     up      radius  5              n/a                5
10.10.0.1        up      radius  5              n/a                5
10.10.0.2        up      radius  5              n/a                5
10.10.0.3        up      radius  5              n/a                5
-------------------------------------------------------------------------------
radius admin status  : down
tacplus admin status : up
health check         : enabled
-------------------------------------------------------------------------------
No. of Servers: 4
===============================================================================
Login Statistics
===============================================================================
server address      connection errors   accepted logins     rejected logins
-------------------------------------------------------------------------------
10.10.10.103        0                   0                   0
10.10.0.1           0                   0                   0
10.10.0.2           0                   0                   0
10.10.0.3           0                   0                   0
local               n/a                 1                   0
===============================================================================
Authorization Statistics (TACACS+)
===============================================================================
server address      connection errors   sent packets        rejected packets
-------------------------------------------------------------------------------
===============================================================================
Accounting Statistics
===============================================================================
server address      connection errors   sent packets        rejected packets
-------------------------------------------------------------------------------
10.10.10.103        0                   0                   0
```

```
10.10.0.1           0                   0                   0
10.10.0.2           0                   0                   0
10.10.0.3           0                   0                   0
===============================================================================
A:ALA-7#
*A:Dut-C# show system security authentication statistics

==============================================================================
Authentication                  sequence : radius tacplus local
==============================================================================
type                               status  timeout     single      retry
   server address                          (secs)      conn        count
------------------------------------------------------------------------------
------------------------------------------------------------------------------
health check         : enabled (interval 30)

===============================================================================
Login Statistics
===============================================================================
server address                                       conn   accepted  rejected
                                                     errors logins    logins
-------------------------------------------------------------------------------
local                                                n/a    4         0

===============================================================================
Authorization Statistics (TACACS+)
===============================================================================
server address                                       conn   sent      rejected
                                                     errors pkts      pkts
-------------------------------------------------------------------------------

===============================================================================
Accounting Statistics
===============================================================================
server address                                       conn   sent      rejected
                                                     errors pkts      pkts
-------------------------------------------------------------------------------
==============================================================================
```

communities

Syntax **communities**

Context show>system>security

Description This command displays SNMP communities.

Output **Communities Output —** The following table describes community output fields.

Table 14: Show Communities Output Fields

Label	Description
Community	The community string name for SNMPv1 and SNMPv2c access only.
Access	r — The community string allows read-only access. rw — The community string allows read-write access. rwa — The community string allows read-write access. mgmt — The unique SNMP community string assigned to the management router.
View	The view name.
Version	The SNMP version.
Group Name	The access group name.
No of Communities	The total number of configured community strings.

Sample Output

```
A:ALA-48# show system security communities
==============================================================================
Communities
==============================================================================
community            access  view                version   group name
------------------------------------------------------------------------------
cli-readonly         r       iso                 v2c       cli-readonly
cli-readwrite        rw      iso                 v2c       cli-readwrite
public               r       no-security         v1 v2c    snmp-ro
------------------------------------------------------------------------------
No. of Communities: 3
==============================================================================
A:ALA-48#
```

cpm-filter

Syntax **cpm-filter**

Context show>system>security

Description This command displays CPM filters.

ip-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context show>system>security>cpm-filter

Description This command displays CPM IP filters.

Parameters **entry** *entry-id* **—** Identifies a CPM filter entry as configured on this system.

Values 1 — 2048

Output **CPM Filter Output —** The following table describes CPM IP filter output fields..

Table 15: Show CPM IP Filter Output Fields

Label	Description
`Entry-Id`	Displays information about the specified management access filter entry
`Dropped`	Displays the number of dropped events.
`Forwarded`	Displays the number of forwarded events.
`Description`	Displays the CPM filter description.
`Log ID`	Displays the log ID where matched packets will be logged.
`Src IP`	Displays the source IP address(/netmask or prefix-list)
`Dest. IP`	Displays the destination IP address(/netmask).
`Src Port`	Displays the source port number (range).
`Dest. Port`	Displays the destination port number (range).
`Protocol`	Displays the Protocol field in the IP header.
`Dscp`	Displays the DSCP field in the IP header.
`Fragment`	Displays the 3-bit fragment flags or 13-bit fragment offset field.
`ICMP Type`	Displays the ICMP type field in the ICMP header.
`ICMP Code`	Displays the ICMP code field in the ICMP header.
`TCP-syn`	Displays the SYN flag in the TCP header.
`TCP-ack`	Displays the ACK flag in the TCP header
`Match action`	When the criteria matches, displays drop or forward packet.
`Next Hop`	In case match action is forward, indicates destination of the matched packet.

Table 15: Show CPM IP Filter Output Fields (Continued)

Label	Description
`Dropped pkts`	Indicates number of matched dropped packets
`Forwarded pkts`	Indicates number of matched forwarded packets.

Sample Output

```
A:ALA-35# show system security cpm-filter ip-filter
===============================================================================
CPM IP Filters
===============================================================================
Entry-Id  Dropped   Forwarded Description
-------------------------------------------------------------------------------
101       25880     0         CPM-Filter 10.4.101.2 #101
102       25880     0         CPM-Filter 10.4.102.2 #102
103       25880     0         CPM-Filter 10.4.103.2 #103
104       25882     0         CPM-Filter 10.4.104.2 #104
105       25926     0         CPM-Filter 10.4.105.2 #105
106       25926     0         CPM-Filter 10.4.106.2 #106
107       25944     0         CPM-Filter 10.4.107.2 #107
108       25950     0         CPM-Filter 10.4.108.2 #108
109       25968     0         CPM-Filter 10.4.109.2 #109
110       25984     0         CPM-Filter 10.4.110.2 #110
111       26000     0         CPM-Filter 10.4.111.2 #111
112       26018     0         CPM-Filter 10.4.112.2 #112
113       26034     0         CPM-Filter 10.4.113.2 #113
114       26050     0         CPM-Filter 10.4.114.2 #114
115       26066     0         CPM-Filter 10.4.115.2 #115
116       26084     0         CPM-Filter 10.4.116.2 #116
===============================================================================
A:ALA-35#

A:ALA-35# show system security cpm-filter ip-filter entry 101
===============================================================================
CPM IP Filter Entry
===============================================================================
Entry Id           : 101
Description : CPM-Filter 10.4.101.2 #101
-------------------------------------------------------------------------------
Filter Entry Match Criteria :
-------------------------------------------------------------------------------
Log Id             : n/a
Src. IP            : 10.4.101.2/32      Src. Port          : 0
Dest. IP           : 10.4.101.1/32      Dest. Port         : 0
Protocol           : 6                  Dscp               : ef
ICMP Type          : Undefined          ICMP Code          : Undefined
Fragment           : True               Option-present     : Off
IP-Option          : 130/255            Multiple Option    : True
TCP-syn            : Off                TCP-ack            : True
Match action       : Drop
===============================================================================
A:ALA-35#
```

ipv6-filter

Syntax **ipv6-filter** [**entry** *entry-id*]

Context show>system>security>cpm-filter

Description This command displays CPM IPv6 filters.

Parameters **entry** *entry-id* **—** Identifies a CPM filter entry as configured on this system.

Values 1 — 2048

ipv6-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context show>system>security>cpm-filter

Description Displays CPM IPv6 filters.

Parameters **entry** *entry-id* **—** Identifies a CPM IPv6 filter entry as configured on this system.

Values 1 — 2048

Output **CPM Filter Output —** The following table describes CPM IPv6 filter output fields..

Table 16: Show CPM IPv6 Filter Output Fields

Label	Description
`Entry-Id`	Displays information about the specified management access filter entry
`Dropped`	Displays the number of dropped events.
`Forwarded`	Displays the number of forwarded events.
`Description`	Displays the CPM filter description.
`Log ID`	Log Id where matched packets will be logged.
`Src IP`	Displays Source IP address(/netmask)
`Dest. IP`	Displays Destination IP address(/netmask).
`Src Port`	Displays Source Port Number (range).
`Dest. Port`	Displays Destination Port Number (range).
`next-header`	Displays next-header field in the IPv6 header.
`Dscp`	Displays Traffic Class field in the IPv6 header.
`ICMP Type`	Displays ICMP type field in the icmp header.

Table 16: Show CPM IPv6 Filter Output Fields (Continued)

Label	Description
`ICMP Code`	Displays ICMP code field in the icmp header.
`TCP-syn`	Displays the SYN flag in the TCP header.
`TCP-ack`	Displays the ACK flag in the TCP header
`Match action`	When criteria matches, displays drop or forward packet.
`Next Hop`	In case match action is forward, indicates destination of the matched packet.
`Dropped pkts`	Indicating number of matched dropped packets
`Forwarded pkts`	Indicating number of matched forwarded packets.

Sample Output

```
A:ALA-35# show system security cpm-filter ipv6-filter
===============================================================================
CPM IPv6 Filters
===============================================================================
Entry-Id Dropped Forwarded Description
-------------------------------------------------------------------------------
101      25880   0         CPM-Filter 11::101:2 #101
102      25880   0         CPM-Filter 11::102:2 #102
103      25880   0         CPM-Filter 11::103:2 #103
104      25880   0         CPM-Filter 11::104:2 #104
105      25880   0         CPM-Filter 11::105:2 #105
106      25880   0         CPM-Filter 11::106:2 #106
107      25880   0         CPM-Filter 11::107:2 #107
108      25880   0         CPM-Filter 11::108:2 #108
109      25880   0         CPM-Filter 11::109:2 #109
===============================================================================
A:ALA-35#
```

```
A:ALA-35# show system security cpm-filter ipv6-filter entry 101
===============================================================================
CPM IPv6 Filter Entry
===============================================================================
Entry Id : 1
Description : CPM-Filter 11::101:2 #101
-------------------------------------------------------------------------------
Filter Entry Match Criteria :
-------------------------------------------------------------------------------
Log Id : n/a
Src. IP : 11::101:2       Src. Port : 0
Dest. IP : 11::101:1      Dest. Port : 0
next-header : none        Dscp : Undefined
ICMP Type : Undefined     ICMP Code : Undefined
TCP-syn : Off             TCP-ack : Off
Match action : Drop
Dropped pkts : 25880      Forwarded pkts : 0
===============================================================================
A:ALA-35#
```

cpm-queue

Syntax **cpm-queue** *queue-id*

Context show>system>security

Description Displays CPM queues.

Parameters *queue-id* — Specifies an integer value that identifies a CPM queue.

Values 0, 33 — 2000

CPM queue Output — The following table describes CPM queue output fields..

Table 17: Show CPM IPv6 Filter Output Fields

Label	Description
PIR	Displays the administrative Peak Information Rate (PIR) for the queue.
CIR	Displays the amount of bandwidth committed to the queue.
CBS	Displays the amount of buffer drawn from the reserved buffer portion of the queue's buffer pool.
MBS	Displays the maximum queue depth to which a queue can grow.

Sample Output

```
A:ALA-35# show system security cpm-queue 1001
===============================================================================
CPM Queue Entry
===============================================================================
Queue Id           : 1001
-------------------------------------------------------------------------------
Queue Parameters :
-------------------------------------------------------------------------------
PIR                : 10000000          CIR                : 1000000
CBS                : 4096              MBS                : 8192
===============================================================================
A:ALA-35#
```

cpu-protection

Syntax **cpu-protection**

Context show>system>security

Description This command enables the context to display CPU protection information.

Sample Output

```
show system security cpu-protection eth-cfm-monitoring
===============================================================================
SAP's where the protection policy Eth-CFM rate limit is exceeded
===============================================================================
SAP-Id                                        Service-Id    Plcy
-------------------------------------------------------------------------------
1/1/1                                         3             100
-------------------------------------------------------------------------------
1 SAP('s) found
===============================================================================
===============================================================================
SDP's where the protection policy Eth-CFM rate limit is exceeded
===============================================================================
SDP-Id            Service-Id    Plcy
-------------------------------------------------------------------------------
1:3               3             100
-------------------------------------------------------------------------------
1 SDP('s) found
===============================================================================

show system security cpu-protection eth-cfm-monitoring service-id 3 sap-id 1/1/1
 ===============================================================================
Flows exceeding the Eth-CFM monitoring rate limit
===============================================================================
Service-Id : 3
SAP-Id     : 1/1/1
Plcy       : 100
-------------------------------------------------------------------------------
Limit  MAC-Address        Level  OpCode
  First-Time            Last-Time             Violation-Periods
-------------------------------------------------------------------------------
0      8c:8c:8c:8c:8c:8c  1      18
  03/21/2009 23:32:29   03/21/2009 23:34:39   4000000019
61234  8d:8d:8d:8d:8d:8d  2      19
  03/21/2009 23:32:39   03/21/2009 23:34:59   4000000020
61234  Aggregated         3      20
  03/21/2009 23:32:49   03/21/2009 23:35:19   4000000021
61234  8f:8f:8f:8f:8f:8f  4      21
  03/21/2009 23:32:59   03/21/2009 23:35:39   4000000022
61234  90:90:90:90:90:90  5      22
  03/21/2009 23:33:09   03/21/2009 23:35:59   4000000023
61234  91:91:91:91:91:91  6      23
  03/21/2009 23:33:19   03/21/2009 23:36:19   4000000024
61234  92:92:92:92:92:92  7      24
  03/21/2009 23:33:29   03/21/2009 23:36:39   4000000025
max    Aggregated         0      25
  03/21/2009 23:33:39   03/21/2009 23:36:59   4000000026
0      94:94:94:94:94:94  1      26
  03/21/2009 23:33:49   03/21/2009 23:37:19   4000000027
-------------------------------------------------------------------------------
9 flows(s) found
===============================================================================

show system security cpu-protection eth-cfm-monitoring service-id 3 sdp-id 1:3
===============================================================================
Flows exceeding the Eth-CFM monitoring rate limit
===============================================================================
Service-Id : 3
SDP-Id     : 1:3
Plcy       : 100
-------------------------------------------------------------------------------
Limit  MAC-Address        Level  OpCode
  First-Time            Last-Time             Violation-Periods
-------------------------------------------------------------------------------
0      8c:8c:8c:8c:8c:8c  1      18
  03/21/2009 23:32:29   03/21/2009 23:34:39   3000000019
61234  8d:8d:8d:8d:8d:8d  2      19
  03/21/2009 23:32:39   03/21/2009 23:34:59   3000000020
61234  Aggregated         3      20
  03/21/2009 23:32:49   03/21/2009 23:35:19   3000000021
61234  8f:8f:8f:8f:8f:8f  4      21
  03/21/2009 23:32:59   03/21/2009 23:35:39   3000000022
61234  90:90:90:90:90:90  5      22
  03/21/2009 23:33:09   03/21/2009 23:35:59   3000000023
61234  91:91:91:91:91:91  6      23
  03/21/2009 23:33:19   03/21/2009 23:36:19   3000000024
61234  92:92:92:92:92:92  7      24
  03/21/2009 23:33:29   03/21/2009 23:36:39   3000000025
max    Aggregated         0      25
  03/21/2009 23:33:39   03/21/2009 23:36:59   3000000026
0      94:94:94:94:94:94  1      26
  03/21/2009 23:33:49   03/21/2009 23:37:19   3000000027
-------------------------------------------------------------------------------
9 flow(s) found
===============================================================================


show system security cpu-protection excessive-sources service-id 3 sdp-id 1:3
===============================================================================
Sources exceeding the per-source rate limit
===============================================================================
Service-Id : 3
SDP-Id     : 1:3
Plcy       : 100
Limit      : 65534
-------------------------------------------------------------------------------
MAC-Address       First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
00:00:00:00:00:01 03/22/2009 00:41:59 03/22/2009 01:53:39 3000000043
00:00:00:00:00:02 03/22/2009 00:43:39 03/22/2009 01:56:59 3000000044
00:00:00:00:00:03 03/22/2009 00:45:19 03/22/2009 02:00:19 3000000045
00:00:00:00:00:04 03/22/2009 00:46:59 03/22/2009 02:03:39 3000000046
00:00:00:00:00:05 03/22/2009 00:48:39 03/22/2009 02:06:59 3000000047
-------------------------------------------------------------------------------
5 source(s) found
===============================================================================


show system security cpu-protection violators sdp
===============================================================================
SDP's where the protection policy overall rate limit is violated
===============================================================================
SDP-Id           Service-Id
  Plcy Limit First-Time           Last-Time           Violation-Periods
-------------------------------------------------------------------------------
1:1              3
```

```
  100  61234 05/01/2010 01:43:53 06/27/2010 22:37:20 3000000007
1:2              3
  255  max   05/01/2010 01:43:55 06/27/2010 22:37:23 3000000008
1:3              3
  100  61234 05/01/2010 01:43:57 06/27/2010 22:37:26 3000000009
1:4              3
  255  max   05/01/2010 01:43:59 06/27/2010 22:37:29 3000000010
1:5              3
  100  61234 05/01/2010 01:44:01 06/27/2010 22:37:32 3000000011
-------------------------------------------------------------------------------
5 SDP('s) found
===============================================================================


show system security cpu-protection excessive-sources
===============================================================================
SAP's where the protection policy per-source rate limit is exceeded
===============================================================================
SAP-Id                                       Service-Id
  Plcy Limit
-------------------------------------------------------------------------------
1/1/1                                        3
  100  65534
-------------------------------------------------------------------------------
1 SAP('s) found
===============================================================================
SDP's where the protection policy per-source rate limit is exceeded
===============================================================================
SDP-Id            Service-Id    Plcy    Limit
-------------------------------------------------------------------------------
1:3               3             100     65534
1:4               3             255     max
1:5               3             100     65534
-------------------------------------------------------------------------------
3 SDP('s) found
===============================================================================


show system security cpu-protection policy association
===============================================================================
Associations for CPU Protection policy 100
===============================================================================
Description : (Not Specified)
SAP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SAP 1/1/1                                         mac-monitoring
  SAP 1/1/2                                         eth-cfm-monitoring aggr car
  SAP 1/1/3                                         eth-cfm-monitoring
  SAP 1/1/4
-------------------------------------------------------------------------------
Number of SAP's : 4
SDP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SDP 1:1                eth-cfm-monitoring aggr car
  SDP 1:3                eth-cfm-monitoring aggr
  SDP 1:5                mac-monitoring
  SDP 17407:4123456789   eth-cfm-monitoring car
```

```
-------------------------------------------------------------------------------
Number of SDP's : 4
Interface associations
-------------------------------------------------------------------------------
  None
Managed SAP associations
-------------------------------------------------------------------------------
  None
Video-Interface associations
-------------------------------------------------------------------------------
  None
===============================================================================
Associations for CPU Protection policy 254
===============================================================================
Description : Default (Modifiable) CPU-Protection Policy assigned to Access
              Interfaces

SAP associations
-------------------------------------------------------------------------------
  None
SDP associations
-------------------------------------------------------------------------------
  None
Interface associations
-------------------------------------------------------------------------------
Router-Name : Base
  ies6If
Router-Name : vprn7
  vprn7If
-------------------------------------------------------------------------------
Number of interfaces : 2
Managed SAP associations
-------------------------------------------------------------------------------
  None
Video-Interface associations
-------------------------------------------------------------------------------
  None
===============================================================================
Associations for CPU Protection policy 255
===============================================================================
Description : Default (Modifiable) CPU-Protection Policy assigned to Network
              Interfaces

SAP associations
-------------------------------------------------------------------------------
  None
SDP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SDP 1:2
  SDP 1:4               eth-cfm-monitoring
Service Id  : 6                         Type   : IES
  SDP 1:6
Service Id  : 7                         Type   : VPRN
  SDP 1:7
Service Id  : 9                         Type   : Epipe
  SDP 1:9
Service Id  : 300                       Type   : VPLS
  SDP 1:300
```

```
-------------------------------------------------------------------------------
Number of SDP's : 6
Interface associations
-------------------------------------------------------------------------------
Router-Name : Base
  system
-------------------------------------------------------------------------------
Number of interfaces : 1
Managed SAP associations
-------------------------------------------------------------------------------
  None
Video-Interface associations
-------------------------------------------------------------------------------
  None
===============================================================================

show system security cpu-protection policy 100 association
===============================================================================
Associations for CPU Protection policy 100
===============================================================================
Description : (Not Specified)

SAP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SAP 1/1/1                                         mac-monitoring
  SAP 1/1/2                                         eth-cfm-monitoring aggr car
  SAP 1/1/3                                         eth-cfm-monitoring
  SAP 1/1/4
-------------------------------------------------------------------------------
Number of SAP's : 4
SDP associations
-------------------------------------------------------------------------------
Service Id  : 3                         Type   : VPLS
  SDP 1:1                eth-cfm-monitoring aggr car
  SDP 1:3                eth-cfm-monitoring aggr
  SDP 1:5                mac-monitoring
  SDP 17407:4123456789   eth-cfm-monitoring car
-------------------------------------------------------------------------------
Number of SDP's : 4
Interface associations
-------------------------------------------------------------------------------
  None
Managed SAP associations
-------------------------------------------------------------------------------
  None
Video-Interface associations
-------------------------------------------------------------------------------
  None
===============================================================================
A:bksim130#

show system security cpu-protection violators
 ==============================================================================
Ports where a rate limit is violated
===============================================================================
Port-Id
  Type Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
```

```
No ports found
===============================================================================
===============================================================================
Interfaces where the protection policy overall rate limit is violated
===============================================================================
Interface-Name                               Router-Name
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No interfaces found
===============================================================================
===============================================================================
SAP's where the protection policy overall rate limit is violated
===============================================================================
SAP-Id                                       Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
1/1/1                                        3
  100  61234 05/01/2010 01:43:41 06/27/2010 22:37:02 3000000001
-------------------------------------------------------------------------------
1 SAP('s) found
===============================================================================
===============================================================================
SDP's where the protection policy overall rate limit is violated
===============================================================================
SDP-Id           Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
1:1              3
  100  61234 05/01/2010 01:43:41 06/27/2010 22:37:02 3000000001
1:2              3
  255  max   05/01/2010 01:43:43 06/27/2010 22:37:05 3000000002
1:3              3
  100  61234 05/01/2010 01:43:45 06/27/2010 22:37:08 3000000003
1:4              3
  255  max   05/01/2010 01:43:47 06/27/2010 22:37:11 3000000004
1:5              3
  100  61234 05/01/2010 01:43:49 06/27/2010 22:37:14 3000000005
-------------------------------------------------------------------------------
5 SDP('s) found
===============================================================================
===============================================================================
Video clients where the protection policy per-source rate limit is violated
===============================================================================
Client IP Address  Video-Interface                 Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No clients found
===============================================================================
```

eth-cfm-monitoring

Syntax **eth-cfm-monitoring** [{**service-id** *service-id* **sap-id** *sap-id*} | {**service-id** *service-id* **sdp-id** *sdp-id:vc-id*}]

Context show>system>security>cpu-protection

Description This command displays sources exceeding their eth-cfm-monitoring rate limit.

dist-cpu-protection

Syntax **dist-cpu-protection**

Context show>card>fp

Description This command displays Distributed CPU Protection parameters and status at the per card and forwarding plane level.

Output

Table 18: Show Distributed CPU Protection Output Fields

Label	Description
Card	The card identifier
Forwarding Plane(FP)	Identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, an IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMAs).
Dynamic Enforcement Policer Pool	The configured size of the dynamic-enforcement-policer-pool for this card/FP.
Dynamic-Policers Currently In Use	The number of policers from the dynamic enforcement policer pool that are currently in use. The policers are allocated from the pool and instantiated as per-object-per-protocol dynamic enforcement policers after a local monitor triggered for an object (such as a SAP or Network Interface).
Hi-WaterMark Hit Count	The maximum Currently In Use value since it was last cleared (clear card x fp y dist-cpu-protection)
Hi-WaterMark Hit Time	The time at which the current Hi-WaterMark Hit Count was first recorded.
Dynamic-Policers Allocation Fail Count	Indicates how many times the system attempted to allocate dynamic enforcement policers but could not get enough the fill the request.

```
*A:nodeA# show card 1 fp 1 dist-cpu-protection
```

```
===============================================================================
Card : 1 Forwarding Plane(FP) : 1
===============================================================================
Dynamic Enforcement Policer Pool : 2000
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Statistics Information
-------------------------------------------------------------------------------
Dynamic-Policers Currently In Use      : 48
Hi-WaterMark Hit Count                 : 72
Hi-WaterMark Hit Time                  : 01/03/2013 15:08:42 UTC
Dynamic-Policers Allocation Fail Count : 0
-------------------------------------------------------------------------------
===============================================================================
```

dist-cpu-protection

Syntax **dist-cpu-protection [detail]**

Context show>service>id>sap

Description This command displays Distributed CPU Protection parameters and status at the per SAP level.

Parameters **detail —** Include the adapted operational rate parameters in the CLI output. The adapted Oper. parameters are only applicable if the policer is instantiated (for example, if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed.

Output **Distributed CPU Protection Policer Output —** The following table describes Distributed CPU Protection Policer Output output fields.

Table 19: Show Distributed CPU Protection Policer Output Fields

Label	Description
Distributed CPU Protection Policy	The DCP policy assigned to the object.
Policer-Name	The configured name of the static policer
Card/FP	The card and FP identifier. FP identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMAs).
Policer-State	The state of the policer with the following potential values:

Table 19: Show Distributed CPU Protection Policer Output Fields (Continued)

Label	Description
	Exceed - The policer has been detected as non-conformant to the associated DCP policy parameters (e.g. packets exceeded the configured rate and the DCP polling process identified this occurrence) *Conform* - The policer has been detected as conformant to the associated DCP policy parameters (rate) *not-applicable* - Newly created policers or policers that are not currently instantiated. This includes policers configured on linecards that are not in service.
`Protocols Mapped`	A list of protocols that are configured to map to the particular policer.
`Oper. xyz fields`	The actual hardware may not be able to perfectly rate limit to the exact configured rate parameters in a DCP policy. In this case the configured rate parameters will be adapted to the closest supported rate. These adapted operational values are displayed in CLI when the “detail” keyword is included in the show command. The adapted Oper. parameters are only applicable if the policer is instantiated (e.g. if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed. *Oper. Kbps* - The adapted ‘kilobits-per-second’ value for DCP ‘kbps’ rates *Oper. MBS* - The adapted ‘mbs size’ value for DCP ‘kbps’ rates *Oper. Depth* - The calculated policer bucket depth in packets (for DCP ‘packets’ rates) or in bytes (for DCP ‘kbps’rates) *Oper. Packets* - The adapted ‘ppi’ value for DCP ‘packets’ rates *Oper. Within* - The adapted ‘within seconds’ value for DCP ‘packets’ rates *Oper. Init. Delay* - The adapted ‘initial-delay packets’ value for DCP ‘packets’ rates
`Exceed-Count`	The count of packets exceeding the policing parameters since the given policer was previously declared as conformant or newly instantiated. This counter has the same behavior as the exceed counter in the DCP the log events – they are baselined (reset) when the policer transitions to conformant.

Table 19: Show Distributed CPU Protection Policer Output Fields (Continued)

Label	Description
`Detec. Time Remain`	The remaining time in the detection-time countdown during which a policer in the exceed state is being monitored to see if it is once again conformant.
`Hold-Down Remain`	The remaining time in the hold-down countdown during which a policer is treating all packets as exceeding.
`All Dyn-Plcr Alloc.`	Indicates that all the dynamic enforcement policers have been allocated and instantiated for a given local-monitor.
`Dyn-Policer Alloc.`	Indicates that a dynamic policer has been instantiated.

Sample Output

```
*A:nodeA# show service id 33 sap 1/1/3:33 dist-cpu-protection detail

===============================================================================
Service Access Points(SAP) 1/1/3:33
===============================================================================
Distributed CPU Protection Policy :  test1

-------------------------------------------------------------------------------
Statistics/Policer-State Information
===============================================================================
-------------------------------------------------------------------------------
Static Policer
-------------------------------------------------------------------------------
Policer-Name        : arp
Card/FP             : 1/1                Policer-State      : Conform
Protocols Mapped    : arp
Exceed-Count        : 0
Detec. Time Remain  : 0 seconds          Hold-Down Remain.  : none
Operational (adapted) rate parameters:
 Oper. Packets      : 5 ppi              Oper. Within       : 8 seconds
 Oper. Initial Delay: 6 packets
 Oper. Depth        : 0 packets

Policer-Name        : dhcp
Card/FP             : 1/1                Policer-State      : Conform
Protocols Mapped    : dhcp
Exceed-Count        : 0
Detec. Time Remain  : 0 seconds          Hold-Down Remain.  : none
Operational (adapted) rate parameters:
 Oper. Kbps         : 2343 kbps          Oper. MBS          : 240 kilobytes
 Oper. Depth        : 0 bytes

… (snip)


*A:nodaA# show service id 33 sap 1/1/3:34 dist-cpu-protection detail
```

```
===============================================================================
Service Access Points(SAP) 1/1/3:34
===============================================================================
Distributed CPU Protection Policy :  test2

-------------------------------------------------------------------------------
Statistics/Policer-State Information
===============================================================================
-------------------------------------------------------------------------------
Static Policer
-------------------------------------------------------------------------------
No entries found
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Local-Monitoring Policer
-------------------------------------------------------------------------------

Policer-Name        : my-local-mon1
Card/FP             : 1/1                Policer-State      : conform
Protocols Mapped    : arp, pppoe-pppoa
Exceed-Count        : 0
All Dyn-Plcr Alloc. : False
Operational (adapted) rate parameters:
 Oper. Packets      : 10 ppi             Oper. Within       : 8 seconds
 Oper. Initial Delay: 8 packets
 Oper. Depth        : 0 packets

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Dynamic-Policer (Protocol)
-------------------------------------------------------------------------------

Protocol(Dyn-Plcr)  : arp
Card/FP             : 1/1                Protocol-State     : not-applicable
Exceed-Count        : 0
Detec. Time Remain  : 0 seconds          Hold-Down Remain.  : none
Dyn-Policer Alloc.  : False
Operational (adapted) rate parameters: unknown

Protocol(Dyn-Plcr)  : pppoe-pppoa
Card/FP             : 1/1                Protocol-State     : not-applicable
Exceed-Count        : 0
Detec. Time Remain  : 0 seconds          Hold-Down Remain.  : none
Dyn-Policer Alloc.  : False
Operational (adapted) rate parameters: unknown

-------------------------------------------------------------------------------
```

dist-cpu-protection

Syntax **dist-cpu-protection [detail]**

Context show>router>interface

Description This command displays Distributed CPU Protection parameters and status at the router Interface level.

Parameters **detail** — Include the adapted operational rate parameters in the CLI output. The adapted Oper. parameters are only applicable if the policer is instantiated (for example, if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed.

Output **Distributed CPU Protection Policer Output —** The following table describes Distributed CPU Protection Policer Output output fields.

pol

Table 20: Show Distributed CPU Protection Policer Output Fields

Label	Description
`Distributed CPU Protection Policy`	The DCP policy assigned to the object.
`Policer-Name`	The configured name of the static policer
`Card/FP`	The card and FP identifier. FP identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMAs).
`Policer-State`	The state of the policer with the following potential values: *Exceed* - The policer has been detected as non-conformant to the associated DCP policy parameters (e.g. packets exceeded the configured rate and the DCP polling process identified this occurence) *Conform* - The policer has been detected as conformant to the associated DCP policy parameters (rate) *not-applicable* - Newly created policers or policers that are not currently instantiated. This includes policers configured on linecards that are not in service.
`Protocols Mapped`	A list of protocols that are configured to map to the particular policer.
`Oper. xyz fields`	The actual hardware may not be able to perfectly rate limit to the exact configured rate parameters in a DCP policy. In this case the configured rate parameters will be adapted to the closest supported rate. These adapted operational values are displayed in CLI when the "detail" keyword is included in the show command. The adapted Oper. parameters are only applicable if the policer is instantiated (e.g. if the associated forwarding plane is operational, or for an interface if there is a physical port configured for the interface, or if the dynamic policers are allocated), otherwise values of 0 kbps, etc are displayed.

Table 20: Show Distributed CPU Protection Policer Output Fields (Continued)

Label	Description
	Oper. Kbps - The adapted 'kilobits-per-second' value for DCP 'kbps' rates *Oper. MBS* - The adapted 'mbs size' value for DCP 'kbps' rates *Oper. Depth* - The calculated policer bucket depth in packets (for DCP 'packets' rates) or in bytes (for DCP 'kbps'rates) *Oper. Packets* - The adapted 'ppi' value for DCP 'packets' rates *Oper. Within* - The adapted 'within seconds' value for DCP 'packets' rates *Oper. Init. Delay* - The adapted 'initial-delay packets' value for DCP 'packets' rates
`Exceed-Count`	The count of packets exceeding the policing parameters since the given policer was previously declared as conformant or newly instantiated. This counter has the same behavior as the exceed counter in the DCP the log events – they are baselined (reset) when the policer transitions to conformant.
`Detec. Time Remain`	The remaining time in the detection-time countdown during which a policer in the exceed state is being monitored to see if it is once again conformant.
`Hold-Down Remain`	The remaining time in the hold-down countdown during which a policer is treating all packets as exceeding.
`All Dyn-Plcr Alloc.`	Indicates that all the dynamic enforcement policers have been allocated and instantiated for a given local-monitor.
`Dyn-Policer Alloc.`	Indicates that a dynamic policer has been instantiated.

Sample Output

```
*A:Dut-A# show router interface "test" dist-cpu-protection detail

===============================================================================
Interface "test" (Router: Base)
===============================================================================
Distributed CPU Protection Policy :  dcpuPol

-------------------------------------------------------------------------------
Statistics/Policer-State Information
```

```
===============================================================================
-------------------------------------------------------------------------------
Static Policer
-------------------------------------------------------------------------------
Policer-Name        : staticArpPolicer
Card/FP             : 4/1                 Policer-State       : Exceed
Protocols Mapped    : arp
Exceed-Count        : 10275218
Detec. Time Remain  : 29 seconds          Hold-Down Remain.   : none
Operational (adapted) Rate Parameters:
 Oper. Packets      : 100 ppi              Oper. Within       : 1 seconds
 Oper. Initial Delay: none
 Oper. Depth        : 100 packets
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Local-Monitoring Policer
-------------------------------------------------------------------------------
Policer-Name        : localMonitor
Card/FP             : 4/1                 Policer-State       : Exceed
Protocols Mapped    : icmp, ospf
Exceed-Count        : 8019857
All Dyn-Plcr Alloc. : True
Operational (adapted) Rate Parameters:
 Oper. Packets      : 200 ppi              Oper. Within       : 1 seconds
 Oper. Initial Delay: none
 Oper. Depth        : 0 packets
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Dynamic-Policer (Protocol)
-------------------------------------------------------------------------------
Protocol(Dyn-Plcr)  : icmp
Card/FP             : 4/1                 Protocol-State      : Exceed
Exceed-Count        : 1948137
Detec. Time Remain  : 29 seconds          Hold-Down Remain.   : none
Dyn-Policer Alloc.  : True
Operational (adapted) Rate Parameters:
 Oper. Kbps         : 25 kbps              Oper. MBS          : 256 bytes
 Oper. Depth        : 274 bytes

Protocol(Dyn-Plcr)  : ospf
Card/FP             : 4/1                 Protocol-State      : Exceed
Exceed-Count        : 1487737
Detec. Time Remain  : 29 seconds          Hold-Down Remain.   : none
Dyn-Policer Alloc.  : True
Operational (adapted) Rate Parameters:
 Oper. Kbps         : 25 kbps              Oper. MBS          : 256 bytes
 Oper. Depth        : 284 bytes
-------------------------------------------------------------------------------
===============================================================================
```

excessive-sources

Syntax **excessive-sources** [**service-id** *service-id* **sap-id** *sap-id*]

Context show>system>security>cpu-protection

Description This command displays sources exceeding their per-source rate limit.

Parameters **service-id** *service-id* — Displays information for services exceeding their per-source rate limit.

sap-id *sap-id* — Displays information for SAPs exceeding their per-source rate limit.

policy

Syntax **policy** [*policy-id*] **association**

Context show>system>security>cpu-protection
show>system>security>dist-cpu-protection

Description This command displays CPU protection policy information.

Parameters *policy-id* — Displays CPU protection policy information for the specified policy ID>

association — This keyword displays policy-id associations.

protocol-protection

Syntax **protocol-protection**

Context show>system>security>cpu-protection

Description This command display all interfaces with non-zero drop counters.

violators

Syntax **violators** [**port**] [**interface**] [**sap**] [**video**] [**sdp**]

Context show>system>security>cpu-protection

Description This command displays all interfaces, ports or SAPs with CPU protection policy violators. It also includes objects (saps, interfaces) that exceed the out-profile-rate and have the log-events keyword enabled for the out-profile-rate in the cpu-protection policy associated with the object.

Parameters **port** — Displays violators associated with the port.

interface — Displays violators associated with the interface.

sap — Displays violators associated with the SAP.

video — Displays violators associated with the video entity.

sdp — Displays violators associated with the SDP.

Sample Output

```
*A:SecuritySR7>config>sys>security>cpu-protection>policy# show system security cpu-
protection violators
===============================================================================
Ports where a rate limit is violated
===============================================================================
Port-Id
  Type Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No ports found
===============================================================================

===============================================================================
Interfaces where the protection policy overall rate limit is violated
===============================================================================
Interface-Name                               Router-Name
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
toIxia                                       Base
  255  1000  10/02/2012 18:38:23 10/02/2012 18:39:31 70
-------------------------------------------------------------------------------
1 interface(s) found
===============================================================================

===============================================================================
SAP's where the protection policy overall rate limit is violated
===============================================================================
SAP-Id                                       Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No SAP's found
===============================================================================

===============================================================================
SDP's where the protection policy overall rate limit is violated
===============================================================================
SDP-Id           Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No SDP's found
===============================================================================

===============================================================================
Video clients where the protection policy per-source rate limit is violated
===============================================================================
Client IP Address  Video-Interface                 Service-Id
  Plcy Limit First-Time          Last-Time           Violation-Periods
-------------------------------------------------------------------------------
No clients found
===============================================================================
```

mac-filter

Syntax **mac-filter** [**entry** *entry-id*]

Context show>system>security>cpm-filter

Description This command displays CPM MAC filters.

Parameters **entry** *entry-id* — Displays information about the specified entry.

Values 1 — 2048

Sample Output

```
*B:bksim67# show system security cpm-filter mac-filter
===============================================================================
CPM Mac Filter (applied)
===============================================================================
Entry-Id  Dropped   Forwarded Description
-------------------------------------------------------------------------------
1         23002     47094
-------------------------------------------------------------------------------
Num CPM Mac filter entries: 1
===============================================================================
*B:bksim67#
```

mac-filter

Syntax **mac-filter** [**entry** *entry-id*]

Context show>system>security>management-access-filter

Description This command displays management access MAC filters.

Parameters **entry** *entry-id* — Displays information about the specified entry.

Values 1 — 9999

Sample Output

```
*B:bksim67# show system security management-access-filter mac-filter
=============================================================================
Mac Management Access Filter
=============================================================================
filter type   : mac
Def. Action   : permit
Admin Status  : enabled (no shutdown)
-------------------------------------------------------------------------------
Entry              : 1                  Action             : deny
FrameType          : ethernet_II        Svc-Id             : Undefined
Src Mac            : Undefined
Dest Mac           : Undefined
Dot1p              : Undefined          Ethertype          : Disabled
```

```
DSAP               : Undefined          SSAP               : Undefined
Snap-pid           : Undefined          ESnap-oui-zero     : Undefined
cfm-opcode         : Undefined
Log                : disabled           Matches            : 0
=============================================================================
*B:bksim67#
```

keychain

Syntax **keychain** [*key-chain*] [**detail**]

Context show>system>security

Description This command displays keychain information.

Parameters *key-chain* — Specifies the keychain name to display.

detail — Displays detailed keychain information.

Sample Output

```
*A:ALA-A# show system security keychain test
===============================================================================
Key chain:test
===============================================================================
TCP-Option number send     : 254                    Admin state   : Up
TCP-Option number receive  : 254                    Oper state    : Up
===============================================================================
*A:ALA-A#
*A:ALA-A#  show system security keychain test detail
===============================================================================
Key chain:test
===============================================================================
TCP-Option number send     : 254                    Admin state   : Up
TCP-Option number receive  : 254                    Oper state    : Up
===============================================================================
Key entries for key chain: test
===============================================================================
Id               : 0
Direction        : send-receive         Algorithm        : hmac-sha-1-96
Admin State      : Up                   Valid            : Yes
Active           : Yes                  Tolerance        : 300
Begin Time       : 2007/02/15 18:28:37  Begin Time (UTC) : 2007/02/15 17:28:37
End Time         : N/A                  End Time (UTC)   : N/A
===============================================================================
Id               : 1
Direction        : send-receive         Algorithm        : aes-128-cmac-96
Admin State      : Up                   Valid            : Yes
Active           : No                   Tolerance        : 300
Begin Time       : 2007/02/15 18:27:57  Begin Time (UTC) : 2007/02/15 17:27:57
End Time         : 2007/02/15 18:28:13  End Time (UTC)   : 2007/02/15 17:28:13
===============================================================================
Id               : 2
Direction        : send-receive         Algorithm        : aes-128-cmac-96
Admin State      : Up                   Valid            : Yes
```

```
Active           : No                   Tolerance        : 500
Begin Time       : 2007/02/15 18:28:13  Begin Time (UTC) : 2007/02/15 17:28:13
End Time         : 2007/02/15 18:28:37  End Time (UTC)   : 2007/02/15 17:28:37
===============================================================================
*A:ALA-A#
```

management-access-filter

Syntax **management-access-filter**

Context show>system>security

Description This commend displays management access filter information for IP and MAC filters.

ip-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context show>system>security>mgmt-access-filter

Description This command displays management-access IP filters.

Parameters *entry-id* — Displays information for the specified entry.

Values 1 — 9999

Output **Management Access Filter Output —** The following table describes management access filter output fields.

Table 21: Show Management Access Filter Output Fields

Label	Description
Def. action	Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted. Deny — Specifies that packets not matching the configured selection criteria in any of the filter entries are denied and that a ICMP host unreachable message will be issued. Deny-host-unreachble — Specifies that packets not matching the configured selection criteria in the filter entries are denied.
Entry	The entry ID in a policy or filter table.
Description	A text string describing the filter.
Src IP	The source IP address used for management access filter match criteria.

Table 21: Show Management Access Filter Output Fields (Continued)

Label	Description
`Src interface`	The interface name for the next hop to which the packet should be forwarded if it hits this filter entry.
`Dest port`	The destination port.
`Matches`	The number of times a management packet has matched this filter entry.
`Protocol`	The IP protocol to match.
`Action`	The action to take for packets that match this filter entry.

```
*A:Dut-F# show system security management-access-filter ip-filter
=============================================================================
IPv4 Management Access Filter
=============================================================================
filter type:  : ip
Def. Action   : permit
Admin Status  : enabled (no shutdown)
-----------------------------------------------------------------------------
Entry         : 1
Src IP        : 192.168.0.0/16
Src interface : undefined
Dest port     : undefined
Protocol      : undefined
Router        : undefined
Action        : none
Log           : disabled
Matches       : 0
=============================================================================
*A:Dut-F#
```

ipv6-filter

Syntax **ipv6-filter** [**entry** *entry-id*]

Context show>system>security>mgmt-access-filter

Description This command displays management-access IPv6 filters.

Parameters *entry-id* — Specifies the IPv6 filter entry ID to display.

Values 1 — 9999

Output

```
*A:Dut-C# show system security management-access-filter ipv6-filter entry 1
=============================================================================
IPv6 Management Access Filter
=============================================================================
filter type   : ipv6
Def. Action   : permit
```

```
Admin Status  : enabled (no shutdown)
-----------------------------------------------------------------------------
Entry         : 1
Src IP        : 2001::1/128
Flow label    : undefined
Src interface : undefined
Dest port     : undefined
Next-header   : undefined
Router        : undefined
Action        : permit
Log           : enabled
Matches       : 0
=============================================================================
*A:Dut-C# s
```

password-options

Syntax **password-options**

Context show>system>security

Description This command displays configured password options.

Output **Password Options Output —** The following table describes password options output fields.

Table 22: Show Password Options Output Fields

Label	Description
`Password aging in days`	Displays the number of days a user password is valid before the user must change their password.
`Time required between password changes`	Displays the time interval between changed passwords.
`Number of invalid attempts permitted per login`	Displays the number of unsuccessful login attempts allowed for the specified **time**.
`Time in minutes per login attempt`	Displays the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.
`Lockout period (when threshold breached)`	Displays the number of minutes that the user is locked out if the threshold of unsuccessful login attempts has been exceeded.
`Authentication order`	Displays the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords.
`User password history length`	Displays the size of the password history file to be stored.
`Accepted password length`	Displays the minimum length required for local passwords.

Table 22: Show Password Options Output Fields (Continued)

Label	Description
`Credits for each character type`	Displays the credit for each character type. A credit is obtained for a particular character type; for example, uppercase, lowercase, numeric, or special character. Credits per character type are configurable. Credits can be used towards the minimum length of the password, so a trade-off can be made between a very long, simple password and a short, complex one.
`Required character types`	Displays the character types that are required in a password; for example, uppercase, lowercase, numeric, or special character.
`Minimum number different character types`	Displays the minimum number of each different character types in a password.
`Required distance with previous password`	Displays the minimum Levenshtein distance between a new password and the old password.
`Allow consecutively repeating a character`	Displays the number of times the same character is allowed to be repeated consecutively.
`Allow passwords containing username`	Displays whether the user name is allowed as part of the password.
`Palindrome allowed`	Displays whether palindromes are allowed as part of the password.

Sample Output

```
A:ALA-7# show system security password-options

===============================================================================
Password Options
===============================================================================

Password aging in days                           : none
Time required between password changes           : 0d 00:10:00

Number of invalid attempts permitted per login   : 3
Time in minutes per login attempt                : 5
Lockout period (when threshold breached)         : 10
Authentication order                             : radius tacplus local
User password history length                     : disabled
Accepted password length                         : 6..56 characters
Credits for each character type                  : none
Required character types                         : none
Minimum number different character types         : 0
Required distance with previous password         : 5
Allow consecutively repeating a character        : always
Allow passwords containing username              : yes
```

```
Palindrome allowed                               : no
===============================================================================
A:ALA-7#
```

per-peer-queuing

Syntax **per-peer-queuing**

Context show>system>security

Description This command enables or disables CPMCFM hardware queuing per peer. TTL security only operates when per-peer-queuing is enabled.

Output **Per-Peer-Queuing Output —** The following table describes per-peer-queuing output fields.

Table 23: Show Per-Peer-Queuing Output Fields

Label	Description
`Per Peer Queuing`	Displays the status (enabled or disabled) of CPM hardware queuing per peer.
`Total Num of Queues`	Displays the total number of hardware queues.
`Num of Queues In Use`	Displays the total number of hardware queues in use.

Sample Output

```
A:ALA-48# show system security per-peer-queuing
=================================================
CPM Hardware Queuing
=================================================
Per Peer Queuing        : Enabled
Total Num of Queues     : 8192
Num of Queues In Use    : 2
=================================================
A:ALA-48# configure
```

profile

Syntax **profile** [*user-profile-name*]

Context show>system>security

Description This command displays user profile information.

If the *profile-name* is not specified, then information for all profiles are displayed.

Parameters *user-profile-name* — Displays information for the specified user profile.

Output **User Profile Output —** The following table describes user profile output fields.

Table 24: Show User Profile Output Fields

Label	Description
`User Profile`	Displays the profile name used to deny or permit user console access to a hierarchical branch or to specific commands.
`Def. action`	`Permit all` — Permits access to all commands.
	`Deny` — Denies access to all commands.
	`None` — No action is taken.
`Entry`	The entry ID in a policy or filter table.
`Description`	Displays the text string describing the entry.
`Match Command`	Displays the command or subtree commands in subordinate command levels.
`Action`	`Permit all` — Commands matching the entry command match criteria are permitted.
	`Deny` — Commands not matching the entry command match criteria are not permitted.
`No. of profiles`	The total number of profiles listed.

Sample Output

```
A:ALA-7# show system security profile administrative
===============================================================================
User Profile
===============================================================================
User Profile : administrative
Def. Action  : permit-all
-------------------------------------------------------------------------------
Entry        : 10
Description  :
Match Command: configure system security
Action       : permit
-------------------------------------------------------------------------------
Entry        : 20
Description  :
Match Command: show system security
Action       : permit
-------------------------------------------------------------------------------
No. of profiles:
===============================================================================
A:ALA-7#
```

source-address

Syntax **source-address**

Context show>system>security

Description This command displays source-address configured for applications.

Output **Source Address Output —** The following table describes source address output fields.

Table 25: Show Source Address Output Fields

Label	Description
Application	Displays the source-address application.
IP address Interface Name	Displays the source address IP address or interface name.
Oper status	Up — The source address is operationally up. Down — The source address is operationally down.

Sample Output

```
A:SR-7# show system security source-address
===============================================================================
Source-Address applications
===============================================================================
Application         IP address/Interface Name                        Oper status
-------------------------------------------------------------------------------
telnet              10.20.1.7                                        Up
radius              loopback1                                        Up
===============================================================================
A:SR-7#
```

ssh

Syntax **ssh**

Context show>system>security

Description This command displays all the SSH sessions as well as the SSH status and fingerprint. The type of SSH application (CLI, SCP, SFTP or NETCONF) is indicated for each SSH connection.

Output **SSH Options Output —** The following table describes SSH output fields .

Label	Description
SSH status	SSH is enabled — Displays that SSH server is enabled. SSH is disabled — Displays that SSH server is disabled.

Label	Description (Continued)
SSH Preserve Key	Enabled — Displays that preserve-key is enabled. Disabled — Displays that preserve-key is disabled.
SSH protocol version 1	Enabled — Displays that SSH1 is enabled. Disabled — Displays that SSH1 is disabled.
SSH protocol version 2	Enabled — Displays that SSH2 is enabled. Disabled — Displays that SSH2 is disabled.
Key fingerprint	The key fingerprint is the server's identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed.
Connection	The IP address of the connected router(s) (remote client).
Encryption	des — Data encryption using a private (secret) key. 3des — An encryption method that allows proprietary information to be transmitted over untrusted networks.
Username	The name of the user.
Version	The SSH version number.
Server Name	The type of SSH application (CLI, SCP, SFTP or NETCONF)
Number of SSH sessions	The total number of SSH sessions.

Sample output

```
*A:ALA-49# show system security ssh

===============================================================================
SSH Server
===============================================================================
Administrative State      : Enabled
Operational State         : Up
Preserve Key              : Enabled

SSH Protocol Version 1    : Disabled

SSH Protocol Version 2    : Enabled
DSA Host Key Fingerprint  : 88:41:1c:7e:97:64:df:a0:e4:54:c2:cc:3d:dd:c7:70
RSA Host Key Fingerprint  : 63:b8:c4:8a:17:b7:1c:95:35:91:c9:08:75:cc:31:a3

-------------------------------------------------------------------------------
Connection          Username            Version ServerName  Status
-------------------------------------------------------------------------------
138.120.214.254     admin               2       netconf     connected
138.120.140.148     admin               2       cli         connected
-------------------------------------------------------------------------------
Number of SSH sessions : 2
===============================================================================
```

user

Syntax **user** [*user-id*] [**detail**]
user [*user-id*] **lockout**

Context show>system>security

Description This command displays user registration information.

If no command line options are specified, summary information for all users displays.

Parameters *user-id* — Displays information for the specified user.

Default All users

detail — Displays detailed user information to the summary output.

lockout — Displays information about any users who are currently locked out.

Output **User Output —** The following table describes user output fields.

Label	Description
`User ID`	The name of a system user.
`Need new pwd`	`Y` — The user must change his password at the next login.
	`N` — The user is not forced to change his password at the next login.
`Cannot change pw`	`Y` — The user has the ability to change the login password.
	`N` — The user does not have the ability to change the login password.
`User permissions`	`Console` — Y - The user is authorized for console access. N- The user is not authorized for console access.
	`FTP` — Y - The user is authorized for FTP access. N - The user is not authorized for FTP access.
	`SNMP` — Y - The user is authorized for SNMP access. N - The user is not authorized for SNMP access.
`Password expires`	The number of days in which the user must change his login password.
`Attempted logins`	The number of times the user has attempted to login irrespective of whether the login succeeded or failed.
`Failed logins`	The number of unsuccessful login attempts.
`Local conf`	`Y` — Password authentication is based on the local password database.
	`N` — Password authentication is not based on the local password database.
`Home directory`	Specifies the local home directory for the user for both console and FTP access.

Label	Description (Continued)
`Restricted to home`	`Yes` — The user is not allowed to navigate to a directory higher in the directory tree on the home directory device. `No` — The user is allowed to navigate to a directory higher in the directory tree on the home directory device.
`Login exec file`	Displays the user's login exec file which executes whenever the user successfully logs in to a console session. profile - the security profile(s) associated with the user locked-out - no / yes (time remaining). Indicates the the user is currently locked-out. After the time expires, or the lockout is manually cleared, the user will be able to attempt to log into the node again. Remaining Login attempts - number of login attempts remaining until the user will be locked-out Remaining Lockout Time - The time until the lockout is automatically cleared and the user can attempt to log into the node again.

Sample Output

```
*A:Dut-C# show system security user detail
===============================================================================
Users
===============================================================================
User ID           New  User Permissions     Password    Login     Failed  Local
                  Pwd  console ftp li snmp  Expires     Attempts  Logins  Conf
-------------------------------------------------------------------------------
admin             n    y       n   n  n     never       4         0       y
-------------------------------------------------------------------------------
Number of users : 1
===============================================================================


*A:Dut-C# show system security user detail
===============================================================================
User Configuration Detail
===============================================================================
===============================================================================
user id            : admin
-------------------------------------------------------------------------------
console parameters
-------------------------------------------------------------------------------
new pw required    : no                 cannot change pw   : no
home directory     :
restricted to home : no
login exec file    :
profile            : administrative
locked-out         : yes (9:23 remaining)
-------------------------------------------------------------------------------
```

```
snmp parameters
-------------------------------------------------------------------------------
===============================================================================


*A:Node234# show system security user lockout
===============================================================================
Currently Failed Login Attempts
===============================================================================
User ID Remaining Login attempts Remaining Lockout Time (min:sec)
-------------------------------------------------------------------------------
jason123 N/A 9:56
-------------------------------------------------------------------------------
Number of users : 1
===============================================================================
```

With the introduction of the PKI on an SR (SSH Server) the authentication process can be done via PKI or password. SSH client usually authenticate via PKI and password if PKI is configured on the client. In this case PKI takes precedence over password in most clients.

All client authentications are logged and display in the **show>system>security>user detail**. Table 26 shows the rules where pass and fail attempts are logged.

Table 26: Pass/Fail Login Attempts

Authentication Order	Client (i.e., putty)	Server (i.e., SR)		CLI Show System Security Attempts (SR)	
	Private Key Programmed	Public Key Configured	Password Configured	Logins Attempts	Failed Logins
1. Public Key 2. Password	Yes	Yes	N/A	Increment	
	Yes	Yes (No match between client and server. Go to password.)	Yes	Increment	
	Yes	No	Yes	Increment	
	No	N/A	Yes	Increment	
	No	N/A	No		Increment
1. Public Key (only)	Yes	Yes	N/A	Increment	

Table 26: Pass/Fail Login Attempts (Continued)

Authentica-tion Order	Client (i.e., putty)	Server (i.e., SR)		CLI Show System Security Attempts (SR)	
	Private Key Programmed	Public Key Configured	Password Configured	Logins Attempts	Failed Logins
	Yes	Yes (No match between client and server. Go go password.)			Increment
	Yes		N/A		Increment
	No		N/A		Increment

```
TABLE


*A:Dut-C# show system security user detail
===============================================================================
Users
===============================================================================
User ID           New  User Permissions     Password    Login     Failed  Local
                  Pwd  console ftp li snmp  Expires     Attempts  Logins  Conf
-------------------------------------------------------------------------------
admin             n    y       n   n  n     never       4         0       y
-------------------------------------------------------------------------------
Number of users : 1
===============================================================================
===============================================================================
User Configuration Detail
===============================================================================
===============================================================================
user id            : admin
-------------------------------------------------------------------------------
console parameters
-------------------------------------------------------------------------------
new pw required    : no                 cannot change pw   : no
home directory     :
restricted to home : no
login exec file    :
profile            : administrative
-------------------------------------------------------------------------------
snmp parameters
-------------------------------------------------------------------------------
===============================================================================
```

view

Syntax **view** [*view-name*] [**detail**]

Context show>system>security

Description This command displays the SNMP MIB views.

Parameters *view-name* — Specify the name of the view to display output. If no view name is specified, the complete list of views displays.

detail — Displays detailed view information.

Output **View Output —** The following table describes show view output fields.

Table 27: Show View Output Fields

Label	Description
`view name`	The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.
`oid tree`	The object identifier of the ASN.1 subtree.
`mask`	The bit mask that defines a family of view subtrees.
`permission`	Indicates whether each view is included or excluded
`No. of Views`	Displays the total number of views.

Sample Output

```
A:ALA-48# show system security view
===============================================================================
Views
===============================================================================
view name         oid tree                        mask              permission
-------------------------------------------------------------------------------
iso               1                                                 included
read1             1.1.1.1                         11111111          included
write1            2.2.2.2                         11111111          included
testview          1                               11111111          included
testview          1.3.6.1.2                       11111111          excluded
mgmt-view         1.3.6.1.2.1.2                                     included
mgmt-view         1.3.6.1.2.1.4                                     included
mgmt-view         1.3.6.1.2.1.5                                     included
mgmt-view         1.3.6.1.2.1.6                                     included
mgmt-view         1.3.6.1.2.1.7                                     included
mgmt-view         1.3.6.1.2.1.31                                    included
mgmt-view         1.3.6.1.2.1.77                                    included
mgmt-view         1.3.6.1.4.1.6527.3.1.2.3.7                        included
mgmt-view         1.3.6.1.4.1.6527.3.1.2.3.11                       included
vprn-view         1.3.6.1.2.1.2                                     included
vprn-view         1.3.6.1.2.1.4                                     included
```

```
vprn-view         1.3.6.1.2.1.5                                     included
vprn-view         1.3.6.1.2.1.6                                     included
vprn-view         1.3.6.1.2.1.7                                     included
vprn-view         1.3.6.1.2.1.15                                    included
vprn-view         1.3.6.1.2.1.23                                    included
vprn-view         1.3.6.1.2.1.31                                    included
vprn-view         1.3.6.1.2.1.68                                    included
vprn-view         1.3.6.1.2.1.77                                    included
vprn-view         1.3.6.1.4.1.6527.3.1.2.3.7                        included
vprn-view         1.3.6.1.4.1.6527.3.1.2.3.11                       included
vprn-view         1.3.6.1.4.1.6527.3.1.2.20.1                       included
no-security       1                                                 included
no-security       1.3.6.1.6.3                                       excluded
no-security       1.3.6.1.6.3.10.2.1                                included
no-security       1.3.6.1.6.3.11.2.1                                included
no-security       1.3.6.1.6.3.15.1.1                                included
on-security       2                               00000000          included
-------------------------------------------------------------------------------
No. of Views: 33
===============================================================================
A:ALA-48#
```

certificate

Syntax **certificate**

Context show

Description This command displays certificate information.

ca-profile

Syntax **ca-profile**
ca-profile *name* [**association**]

Context show>certificate

Description This command shows certificate-authority profile information.

Parameters *name* — Specifies the name of the Certificate Authority (CA) profile.

association — Displays associated CA profiles.

ocsp-cache

Syntax **ocsp-cache** [*entry-id*]

Context show>certificate

Description This command displays the current cached OCSP results. The output includes the following information:

- Certificate issuer
- Certificate serial number
- OCSP result
- Cache entry expire time

Parameters *entry-id* — Specifies the local cache entry identifier of the certificate that was validated by the OCSP responder.

statistics

Syntax **statistics**

Context show>certificate

Description This command shows certificate related statistics.

Login Control

users

Syntax **users**

Context show

Description Displays console user login and connection information.

Output **Users Output —** The following table describes show users output fields.

Table 28: Show Users Output Fields

Label	Description
User	The user name.
Type	The user is authorized this access type.
From	The originating IP address.
Login time	The time the user logged in.
Idle time	The amount of idle time for a specific login.
Number of users	Displays the total number of users logged in.

Sample Console Users Output

```
A:ALA-7# show users
===============================================================================
User              Type    From              Login time          Idle time
===============================================================================
testuser          Console     --            21FEB2007 04:58:55  0d 00:00:00  A
-------------------------------------------------------------------------------
Number of users : 1
'A' indicates user is in admin mode
===============================================================================
A:ALA-7#
```

Clear Commands

statistics

Syntax **statistics** [**interface** *ip-int-name* | *ip-address*]

Context clear>router>authentication

Description This command clears authentication statistics.

Parameters *ip-int-name* — Clears the authentication statistics for the specified interface name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes

ip-address — Clears the authentication statistics for the specified IP address.

ip-filter

Syntax **ip-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears IP filter statistics.

Parameters **entry** *entry-id* — Specifies a particular CPM IP filter entry.

Values 1 — 2048

ipv6-filter

Syntax **ipv6-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears IPv6 filter statistics.

Parameters **entry** *entry-id* — Specifies a particular CPM IP filter entry.

Values 1 — 2048

mac-filter

Syntax **mac-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears MAC filter statistics.

Parameters **entry** *entry-id* **—** Specifies a particular CPM MAC filter entry.

Values 1 — 2048

ipv6-filter

Syntax **ipv6-filter** [**entry** *entry-id*]

Context clear>cpm-filter

Description This command clears IPv6 filter information.

Parameters **entry** *entry-id* **—** Specifies a particular CPM IPv6 filter entry.

Values 1 — 2048

CPU Protection Commands

cpu-protection

Syntax **cpu-protection**

Context clear

Description This command enables the context to clear CPU protection data.

excessive-sources

Syntax **excessive-sources**

Context clear>cpu-protection

Description This command clears the records of sources exceeding their per-source rate limit.

protocol-protection

Syntax **protocol-protection**

Context clear>cpu-protection

Description This command clears the interface counts of packets dropped by protocol protection.

violators

Syntax **violators** [**port**][**interface**][**sap**]

Context clear>cpu-protection

Description This command clears the rate limit violator record.

Parameters **port —** Clears entries for ports.

interface — Clears entries for interfaces.

sap — Clears entries for SAPs.

cpm-queue

Syntax **cpm-queue** *queue-id*

Context clear

Description This command clears CPM queue information.

Parameters *queue-id* — Specifies the CPM queue ID.

Values 33 — 2000

radius-proxy-server

Syntax **radius-proxy-server** *server-name* **statistics**

Context clear>router

Description This command clears RADIUS proxy server data.

Parameters *server-name* — Specifies the proxy server name.

statistics — Clears statistics for the specified server.

Debug Commands

radius

Syntax **radius** [**detail**] [**hex**]
no radius

Context debug

Description This command enables debugging for RADIUS connections.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed output.

hex — Displays the packet dump in hex format.

ocsp

Syntax [**no**] **ocsp**

Context debug

Description This command enables debug output of OCSP protocol for the CA profile.

The **no** form of the command disables the debug output.

ca-profile

Syntax [**no**] **ca-profile** *profile-name*

Context debug>ocsp

Description This command enables debug output of a specific CA profile.

Tools Commands

dist-cpu-protection

Syntax **dist-cpu-protection**

Context tools>perform>security
tools>dump>security

Description This command displays to release Distributed CPU Protection parameters and status at the per card and forwarding plane level.

release-hold-down

Syntax **release-hold-down interface** *interface-name* **[protocol** *protocol***] [static-policer** *name***]**
release-hold-down sap *sap-id* **[protocol** *protocol***] [static-policer** *name***]**

Context tools>perform>security>dist-cput protection

Description This command is used to release a Distributed CPU Protection (DCP) policer from a hold-down countdown (or indefinite hold-down if configured as such).

Parameters **interface** *interface-name* — Specifies Router interface name.

sap *sap-id* — Specify sap identifier.

protocol *protocol* — Specifies DCP protocol name (for example, arp, dhcp)

static-policer *name* — Specifies DCP static policer name as defined in the DCP policy.

violators

Syntax **violators enforcement {sap|interface} card** *slot-number* **[fp** *fp-number***]**
violators local-monitor {sap|interface} card *slot-number* **[fp** *fp-number***]**

Context tools>dump>security>dist-cput protection

Description This command shows the non-conformant enforcement policers and local monitors.

Parameters **sap** — -Indicates to display the violators associated with SAPs

interface — - Indicates to display the violators associated with router interfaces.

enforcement — Shows exceed and hold-down for Static and Dynamic Policers.

local-monitor — Shows state of dynamic policer allocation for Local Monitoring Policers.

card *slot-number* **—** The physical slot number for the card.

Values 1— n (n is platform dependant)

fp *fp-number* **—** Identifies the instance of the FP (FastPath) chipset. Some cards have a single FP (for example, an IOM3-XP) and some cards can contain multiple FPs (for example, an IOM2 has two FPs and an XCM can house two FPs via its two XMAs).

Values 1— 2

Output **Users Output —** The following table describes show users output fields.

Table 29: Output Parameters

Label	Description
`Interface`	The name of the router interface
`Policer/Protocol`	The configured name of the static policer (indicated with an [S]) or the DCP protocol name for a dynamic policer (indicated with a [D]).
`[S] / [D]`	indicates a static vs dynamic policer
`Hld Rem`	The remaining time in the hold-down countdown during which a policer is treating all packets as exceeding.

Sample Output

```
*A:Dut-A# tools dump security dist-cpu-protection violators enforcement interface
card 4 fp 1
===============================================================================
Distributed Cpu Protection Current Interface Enforcer Policer Violators
===============================================================================
Interface                       Policer/Protocol                   Hld Rem
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Violators on Slot-4 Fp-1
-------------------------------------------------------------------------------
test                            staticArpPolicer               [S] none
test                            icmp                           [D] none
test                            ospf                           [D] none
-------------------------------------------------------------------------------
[S]-Static [D]-Dynamic [M]-Monitor
-------------------------------------------------------------------------------
===============================================================================
```

Admin Commands

clear lockout

Syntax **clear lockout** {**user** *name* **| all**}

Context admin>user

Description This command is used to clear any lockouts for a specific user, or for all users.

Parameters *name* — Specifies locked username.

clear password-history

Syntax **clear password-history** {**user** *name* **| all**}

Context admin>user

Description This command is used to clear old passwords used by a specific user, or for all users.

Parameters *name* — Specifies username.