Show Commands

counters

Syntaxì **counters**

Context show>snmp

Description This command displays SNMP counters information. SNMP counters will continue to increase even when SNMP is shut down. Some internal modules communicate using SNMP packets.

Output **Counters Output —** The following table describes SNMP counters output fields.

Table 30: Counters Output Fields

Label	Description
in packets	Displays the total number of messages delivered to SNMP from the transport service.
in gets	Displays the number of SNMP get request PDUs accepted and processed by SNMP.
in getnexts	Displays the number of SNMP get next PDUs accepted and processed by SNMP.
in sets	Displays the number of SNMP set request PDUs accepted and processed by SNMP.
out packets	Displays the total number of SNMP messages passed from SNMP to the transport service.
out get responses	Displays the number of SNMP get response PDUs generated by SNMP.
out traps	Displays the number of SNMP Trap PDUs generated by SNMP.
variables requested	Displays the number of MIB objects requested by SNMP.
variables set	Displays the number of MIB objects set by SNMP as the result of receiving valid SNMP set request PDUs.

Sample Output

```
A:ALA-1# show snmp counters
===============================================================================
SNMP counters:
===============================================================================
  in packets :  463
```

```
-------------------------------------------------------------------------------
    in gets     : 93
    in getnexts : 0
    in sets     : 370
  out packets:  463
-------------------------------------------------------------------------------
    out get responses :  463
    out traps         :  0
  variables requested:  33
  variables set      :  497
===============================================================================
A:ALA-1#
```

counters

Syntax **counters**

Context show>snmp>streaming

Description This command displays counters information for the proprietary SNMP streaming protocol.Output: Counters Output - The following table describes SNMP streaming counters output fields.

Output **Counters Output —** The following table describes SNMP streaming counters output fields.

Table 31: Counters Output Fields

Label	Description
in getTables	Displays the number of GetTable request packets received.
in getManys	Displays the number of GetMany request packets received.
out responses	Displays the number of response packets sent.

Sample Output

```
*A:Dut-B# show snmp streaming counters
===============================================================================
STREAMING counters:
===============================================================================
    in getTables   : 772
    in getManys    : 26
-------------------------------------------------------------------------------
    out responses  : 848
===============================================================================
```

information

Syntax **information**

Context show>system

Description This command lists the SNMP configuration and statistics.

Output **System Information Output Fields —** The following table describes system information output fields.

Table 32: Show System Information Output Fields

Label	Description
System Name	The name configured for the device.
System Contact	The text string that identifies the contact name for the device.
System Location	The text string that identifies the location of the device.
System Coordinates	The text string that identifies the system coordinates for the device location. For example, “37.390 -122.0550" is read as latitude 37.390 north and longitude 122.0550 west.
System Up Time	The time since the last reboot.
SNMP Port	The port which SNMP sends responses to management requests.
SNMP Engine ID	The ID for either the local or remote SNMP engine to uniquely identify the SNMPv3 node.
SNMP Max Message Size	The maximum size SNMP packet generated by this node.
SNMP Admin State	Enabled – SNMP is administratively enabled.
	Disabled – SNMP is administratively disabled.
SNMP Oper State	Enabled – SNMP is operationally enabled.
	Disabled – SNMP is operationally disabled.
SNMP Index Boot Status	Persistent – Persistent indexes at the last system reboot was enabled.
	Disabled – Persistent indexes at the last system reboot was disabled.
SNMP Sync State	The state when the synchronization of configuration files between the primary and secondary CPMs finish.
Telnet/SSH/FTP Admin	Displays the administrative state of the Telnet, SSH, and FTP sessions.

Table 32: Show System Information Output Fields (Continued)

Label	Description
Telnet/SSH/FTP Oper	Displays the operational state of the Telnet, SSH, and FTP sessions.
BOF Source	The boot location of the BOF.
Image Source	primary – Specifies whether the image was loaded from the primary location specified in the BOF. secondary – Specifies whether the image was loaded from the secondary location specified in the BOF. tertiary – Specifies whether the image was loaded from the tertiary location specified in the BOF.
Config Source	primary – Specifies whether the configuration was loaded from the primary location specified in the BOF. secondary – Specifies whether the configuration was loaded from the secondary location specified in the BOF. tertiary – Specifies whether the configuration was loaded from the tertiary location specified in the BOF.
Last Booted Config File	Displays the URL and filename of the configuration file used for the most recent boot.
Last Boot Cfg Version	Displays the version of the configuration file used for the most recent boot.
Last Boot Config Header	Displays header information of the configuration file used for the most recent boot.
Last Boot Index Version	Displays the index version used in the most recent boot.
Last Boot Index Header	Displays the header information of the index used in the most recent boot.
Last Saved Config	Displays the filename of the last saved configuration.

Table 32: Show System Information Output Fields (Continued)

Label	Description
Time Last Saved	Displays the time the configuration was most recently saved.
Changes Since Last Save	Yes — The configuration changed since the last save.
	No — The configuration has not changed since the last save.
Time Last Modified	Displays the time of the last modification.
Max Cfg/BOF Backup Rev	The maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL — The location and name of the CLI script file executed following successful completion of the boot-up configuration file execution.
	N/A — No CLI script file is executed.
Cfg-OK Script Status	Successful/Failed — The results from the execution of the CLI script file specified in the Cfg-OK Script location.
	Not used — No CLI script file was executed.
Cfg-Fail Script	URL — The location and name of the CLI script file executed following a failed boot-up configuration file execution.
	Not used — No CLI script file was executed.
Cfg-Fail Script Status	Successful/Failed — The results from the execution of the CLI script file specified in the Cfg-Fail Script location.
	Not used — No CLI script file was executed.
Management IP address	The Management IP address of the node.
DNS Server	The DNS address of the node.
DNS Domain	The DNS domain name of the node.
BOF Static Routes	To — The static route destination.
	Next Hop — The next hop IP address used to reach the destination.
	Metric — Displays the priority of this static route versus other static routes.
	None — No static routes are configured.

Sample Output

```
A:ALA-1# show system information
===============================================================================
System Information
===============================================================================
System Name            : ALA-1
System Type            : 7750 SR-12
System Version         : B-0.0.I1204
System Contact         :
System Location        :
System Coordinates     :
System Active Slot     : A
System Up Time         : 1 days, 02:12:57.84 (hr:min:sec)

SNMP Port              : 161
SNMP Engine ID         : 0000197f00000479ff000000
SNMP Max Message Size  : 1500
SNMP Admin State       : Enabled
SNMP Oper State        : Enabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State        : OK

Telnet/SSH/FTP Admin   : Enabled/Enabled/Disabled
Telnet/SSH/FTP Oper    : Up/Up/Down

BOF Source             : cf1:
Image Source           : primary
Config Source          : primary
Last Booted Config File: ftp://172.22.184.249/./debby-sim1/debby-sim1-config.cfg
Last Boot Cfg Version  : THU FEB 15 16:58:20 2007 UTC
Last Boot Config Header: # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR 7750
                         Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                         reserved. All use subject to applicable license
                         agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                         builder in /rel0.0/I1042/panos/main # Generated THU
                         FEB 11 16:58:20 2007 UTC
Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR 7750
                         Copyright (c) 2000-2007 Alcatel-Lucent. # All rights
                         reserved. All use subject to applicable license
                         agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by
                         builder in /rel0.0/I1042/panos/main # Generated THU
                         FEB 15 16:58:20 2007 UTC
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: No
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script          : N/A
Cfg-OK Script Status   : not used
Cfg-Fail Script        : N/A
Cfg-Fail Script Status : not used

Management IP Addr     : 192.168.2.121/20
DNS Server             : 192.168.1.246
DNS Domain             : eng.timetra.com
BOF Static Routes      :
```

access-group

Syntax **access-group** *group-name*

Context show>system>security

Description This command displays access-group information.

Output **System Information Output —** The following table describes the access-group output fields.

Table 33: 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 view to read the MIB objects.
Write view	Specifies the view to configure the contents of the agent.
Notify view	Specifies the view to send a trap about MIB objects.
No. of access groups	The total number of configured access groups.

Sample Output

```
A:ALA-1# 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
-------------------------------------------------------------------------------
No. of Access Groups: 8
===============================================================================
A:ALA-1#


A:ALA-1# show system security access-group detail
```

```
===============================================================================
Access Groups
===============================================================================
group name        security  security  read          write         notify
                  model     level     view          view          view
-------------------------------------------------------------------------------
snmp-ro           snmpv1    none      no-security                 no-security
-------------------------------------------------------------------------------
No. of Access Groups:
...
===============================================================================
A:ALA-1#
```

authentication

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

Context show>system>security

Description This command displays authentication information.

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

Label	Description
sequence	The authentication order in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.
server address	The address of the RADIUS, TACACS+, or local server.
status	The status of the server.
type	The type of server.
timeout (secs)	Number of seconds the server will wait before timing out.
single connection	Specifies whether a single connection is established with the server. The connection is kept open and is used by all the TELNET/SSH/FTP sessions for AAA operations.
retry count	The number of attempts to retry contacting the server.
radius admin status	The administrative status of the RADIUS protocol operation.
tacplus admin status	The administrative status of the TACACS+ protocol operation.

Label	Description (Continued)
health check	Specifies whether the RADIUS and TACACS+ servers will be periodically monitored. Each server will be contacted every 30 seconds. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, based on the type of the server, a trap will be sent.
No. of Servers	The total number of servers configured.

Sample Output

```
A:ALA-49>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-49>show>system>security#
```

password-options

Syntax **password-options**

Context show>system>security

Description This command displays password options.

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

Label	Description
Password aging in days	Number of days a user password is valid before the user must change his password.
Number of invalid attempts permitted per login	Displays the maximum number of unsuccessful login attempts allowed for a user.
Time in minutes per login attempt	Displays the time in minutes that user is to be locked out.

Label	Description
Lockout period (when threshold breached)	Displays the number of minutes the user is locked out if the threshold of unsuccessful login attempts has exceeded.
Authentication order	Displays the most preferred method to authenticate and authorize a user.
Configured complexity options	Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the **authentication** section.
Minimum password length	Displays the minimum number of characters required in the password.

Sample Output

```
A:ALA-48>show>system>security# password-options
===============================================================================
Password Options
===============================================================================
Password aging in days                          : 365
Number of invalid attempts permitted per login  : 5
Time in minutes per login attempt               : 5
Lockout period (when threshold breached)        : 20
Authentication order                            : radius tacplus local
Configured complexity options                   :
Minimum password length                         : 8
===============================================================================
A:ALA-48>show>system>security#
```

per-peer-queuing

Syntax **per-peer-queuing**

Context show>system>security

Description This command displays displays the number of queues in use by the Qchip, which in turn is used by PPQ, CPM filter, SAP, etc.

Output **Per-Peer_Queuing Output —** The following table describes the per-peer-queuing output fields.

Label	Description
Per Peer Queuing	Displays whether per-peer-queuing is enabled or disabled. When enabled, a peering session is established and the router will automatically allocate a separate CPM hardware queue for that peer. When disabled, no hardware queuing per peer occurs.
Total Num of Queues	Displays the total number of CPM hardware queues.
Num of Queues In Use	Displays the number of CPM hardware queues that are 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    : 0
===============================================
A:ALA-48>show>system>security#
```

profile

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

Context show>system>security

Description This command displays user profiles for CLI command tree permissions.

Parameters *profile-name* — Specify the profile name to display information about a single user profile. If no profile name is displayed, the entire list of profile names are listed.

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

Label	Description
`User Profile`	`default` – The action to be given to the user profile if none of the entries match the command. `administrative` – specifies the administrative state for this profile.
`Def. Action`	`none` – No action is given to the user profile when none of the entries match the command. `permit-all` – The action to be taken when an entry matches the command.
`Entry`	`10 - 80` – Each entry represents the configuration for a system user.
`Description`	A text string describing the entry.

Label	Description
Match Command	`administrative` — Enables the user to execute all commands.
	`configure system security` — Enables the user to execute the **config system security** command.
	`enable-admin` — Enables the user to enter a special administrative mode by entering the **enable-admin** command.
	`exec` — Enables the user to execute (exec) the contents of a text file as if they were CLI commands entered at the console.
	`exit` — Enables the user to execute the **exit** command.
	`help` — Enables the user to execute the **help** command.
	`logout` — Enables the user to execute the **logout** command.
	`password` — Enables the user to execute the **password** command.
	`show config` — Enables the user to execute the **show config** command.
	`show` — Enables the user to execute the **show** command.
	`show system security` — Enables the user to execute the **show system security** command.
Action	`permit` — Enables the user access to all commands.
	`deny-all` — Denies the user access to all commands.

```
A:ALA-48>config>system>snmp# show system security profile
===============================================================================
User Profile
===============================================================================
User Profile : test
Def. Action  : none
-------------------------------------------------------------------------------
Entry        : 1
Description  :
Match Command:
Action       : unknown
===============================================================================
User Profile : default
Def. Action  : none
-------------------------------------------------------------------------------
Entry        : 10
Description  :
Match Command: exec
Action       : permit
-------------------------------------------------------------------------------
Entry        : 20
Description  :
Match Command: exit
```

```
Action       : permit
-------------------------------------------------------------------------------
Entry        : 30
Description  :
Match Command: help
Action       : permit
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Entry        : 80
Description  :
Match Command: enable-admin
Action       : permit
===============================================================================

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: 3
===============================================================================
A:ALA-48>config>system>snmp#
```

snmp

Syntax **snmp**

Context show>system>security

Description This command enables the context to show SNMP information.

community

Syntax **community** [*community-string*]

Context show>system>security>snmp

Description This command lists SNMP communities and characterisics. Including the *community-name* parameter modifies the output to include all details for the specified community, including the source IP address list and validation failure counters.

Output **Community Ouput —** The following table describes the community output fields.

Sample Output

Table 34: Show Community 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. vpls-mgmt – The unique SNMP community string assigned for vpls management
View	The view name.
Version	The SNMP version.
Group Name	The access group name.
src-access-list	The name of the list of source IP addresses that are allowed to use the community, as configured using the **community** configuration command.
authFailures	The number of SNMP requests that have failed validation using this **community**.
No of Communities	The total number of configured community strings.

Note: The system-created communities that begin with "cli-" are only used for internal CLI management purposes and are not exposed to external SNMP access.

```
A:ALA-1# show system security snmp community

===============================================================================
Communities
===============================================================================
community           access  view                version   group name
-------------------------------------------------------------------------------
cli-li-readwrite    n/a     li-view             v2c       cli-li-readwrite
cli-readonly        r       iso                 v2c       cli-readonly
cli-readwrite       rw      iso                 v2c       cli-readwrite
my-private1         rw      iso                 v1 v2c    snmp-rwa
my-public2          r       no-security         v1 v2c    snmp-ro
test-123            rwa     n/a                 v2c       snmp-trap
-------------------------------------------------------------------------------
No. of Communities: 6
===============================================================================
A:ALA-1#
```

```
A:ALA-1# show system security snmp community "my-public2"

===============================================================================
Communities
===============================================================================
community           access  view                    version   group name
                              src-access-list                 authFailures
-------------------------------------------------------------------------------
my-public2          r       no-security             v1 v2c    snmp-ro
                              my-list1                          5
===============================================================================
A:ALA-1#
```

src-access-list

Syntax **src-access-list** [*list-name*]

Context show>system>security>snmp

Description This command displays source access lists and the hosts for each. Including the *list-name* parameter modifies the output show only the specified **src-access-list**.

Output **Source Access List Ouput —** The following table describes the source access list output fields.

Sample Output

Table 35: Show Source Access List Output Fields

Label	Description
List Name	The name of the **src-access-list**.
Host Name	The name of the **src-host**.
Host Address	The IP address of the **src-host**.
Total Access Lists	The total number of source access lists displayed.

```
A:ALA-1# show system security snmp src-access-list
===============================================================================
Source Access Lists
===============================================================================
List Name
  HostName                              Host Address
-------------------------------------------------------------------------------
L1
  H1                                    100.100.100.1
  H2                                    100.100.100.2
L2
  HA                                    100.100.101.1
  HB                                    100.100.101.2
-------------------------------------------------------------------------------
Total Access Lists: 2
===============================================================================
```

```
A:ALA-1#


A:ALA-1# show system security snmp src-access-list L1
===============================================================================
Source Access Lists
===============================================================================
List Name
  HostName                                Host Address
-------------------------------------------------------------------------------
L1
  H1                                      100.100.100.1
  H2                                      100.100.100.2
-------------------------------------------------------------------------------
Total Access Lists: 1
===============================================================================
A:ALA-1#
```

ssh

Syntax **ssh**

Context show>system>security

Description This command displays all the SSH sessions as well as the SSH status and fingerprint.

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

Table 36: Show 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.
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.
Number of SSH sessions	The total number of SSH sessions.

Sample output

```
A:ALA-7# show system security ssh
SSH is enabled
Key fingerprint: 34:00:f4:97:05:71:aa:b1:63:99:dc:17:11:73:43:83
=======================================================
Connection    Encryption    Username
=======================================================
192.168.5.218      3des     admin
-------------------------------------------------------
Number of SSH sessions : 1
=======================================================
A:ALA-7#


A:ALA-49>config>system>security# show system security ssh

SSH is disabled

A:ALA-49>config>system>security#
```

user

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

Context show>system>security

Description This command displays user information.

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

Table 37: Show User Output Fields

Label	Description
User ID	The name of a system user.
Need New PWD	Yes — The user must change his password at the next login.
	No — The user is not forced to change his password at the next login.
User Permission	Console — Specifies whether the user is permitted console/Telnet access.
	FTP — Specifies whether the user is permitted FTP access.
	SNMP — Specifies whether the user is permitted SNMP access.
Password expires	The date on which the current password expires.
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.

Table 37: Show User Output Fields (Continued)

Label	Description
Local Conf.	Y — Password authentication is based on the local password database. N — Password authentication is not based on the local password database.

Sample Output

```
A:ALA-1# show system security user
===============================================================================
Users
===============================================================================
user id          need    user permissions  password    attempted failed  local
                 new pwd console ftp snmp  expires     logins    logins  conf
-------------------------------------------------------------------------------
admin            n       y       n   n     never       2         0       y
testuser         n       n       n   y     never       0         0       y
-------------------------------------------------------------------------------
Number of users : 2
```

view

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

Context show>system>security

Description This command lists one or all views and permissions in the MIB-OID tree.

Output **System Security View Output —** The following table describes system security view output fields.

Table 38: Show System Security 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 (OID) value. OIDs uniquely identify MIB objects in the subtree.
Mask	The mask value and the mask type, along with the *oid-value* configured in the **view** command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view.
Permission	Included — Specifies to include MIB subtree objects. Excluded — Specifies to exclude MIB subtree objects.

Table 38: Show System Security View Output Fields (Continued)

Label	Description
No. of Views	The total number of configured views.
Group name	The access group name.

Sample Output

```
A:ALA-1# show system security view
===============================================================================
Views
===============================================================================
view name         oid tree                          mask             permission
-------------------------------------------------------------------------------
iso               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
-------------------------------------------------------------------------------
No. of Views: 6
===============================================================================
A:ALA-1#


A:ALA-1# show system security view no-security detail
===============================================================================
Views
===============================================================================
view name         oid tree                          mask             permission
-------------------------------------------------------------------------------
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
-------------------------------------------------------------------------------
No. of Views: 5
===============================================================================
=======================================
no-security used in
=======================================
group name
---------------------------------------
snmp-ro
snmp-rw
=======================================
A:ALA-1#
```