

### Commands

<code>enable</code>	To access the Privileged EXEC level of the CLI and allow access to all configuration levels.
<code>config</code>	To access the global configuration level.
<code>clear console</code>	Terminate the current login process and start a new one.

### Time & Date Parameters

<code>#show clock</code>	Shows the time.
<code>#clock set 19:15:33 December 17 2023</code>	The following example sets the time to 7:15 PM and 33 seconds on December 17, 2015 (for times beyond 12:00 PM, use 24-hour notation).
<code>#timezone Europe /Is tanbul</code>	The following example sets the timezone to Europe/Istanbul.
<code>#ntp server 216.17 1.1 24.36</code>	To configure a preferred NTP server.
<code>#prefer</code>	Then use the prefer command to make this the preferred server:.
<code>#ntp auth-key 13579 M ascii XxEnc192</code>	Create authentication keys (13579).
<code>#ntp truste d-key 13579</code>	Add key (13579) to the list of trusted keys.
<code>#ntp server 207.69.13 1.204</code>	Configure the NTP server at 207.69.131.204 to use trusted key (13579).
<code>#show runnin g-c onfig   include ntp</code>	Verify the NTP server and authentication key configuration.

### Basic System Parameters

<code>#hostname ACOS-TPS2</code>	Change the hostname.
<code>#ip dns suffix a10net wor ks.com</code>	To set the default domain name (DNS suffix) for host names on the ACOS device.
<code>#ip dns primary 10.10.1 28.101</code>	To set the primary DNS server for resolving DNS requests.
<code>#ip dns secondary 10.10.1 28.102</code>	To set the secondary DNS server for resolving DNS requests.
<code>#show runnin g-c onfig   include dns</code>	Show running-config command to view your configuration.
<code>#banner login "welcome to login mode"</code>	To set the login banner.
<code>#banner login "welcome to exec mode"</code>	To set the exec banner.
<code>#web-s ervice secure wipe</code>	
<code>#import cert</code>	To import a CA-signed certificate.
<code>#interface management</code>	Puts you in interface management mode, where you can continue the management interface configuration.
<code>#ip address 192.16 8.10.2 /24</code>	To configure IPv4 access.
<code>#ip defaul t-g ateway 192.16 8.2.1</code>	To configure IPv4 access.
<code>#ipv6 address 2001:d b8: :2/32</code>	To configure IPv6 access.
<code>#ipv6 defaul t-g ateway 2001:d b8::1</code>	To configure IPv6 access.
<code>#show interfaces management</code>	To verify the configuration.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 2 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Parameters

#security -reset	Destroys all sensitive information.
#snmp- server SNMPv3	SNMPv3 Configuration
#system fips enable	Enabling FIPS.
#system fips disable	Disabling FIPS.
#system default t-mtu	To configure the MTU for supported physical and logical ports at the global configuration level.
#system-jumbo global enable -jumbo	To enable jumbo frame support on FTA models.
#system-jumbo global enable -jumbo	To enable jumbo frame support on a non-FTA model.
#write memory #reboot	
#no system-jumbo global enable -jumbo	To disable jumbo frame support on FTA models.
#no system-jumbo global enable -jumbo	To disable jumbo frame support on a non-FTA model.
#write memory #reboot	
#system default t-mtu 9216	To configure the MTU for all interface ports at the global configuration level.
#interface ethernet 1 mtu 1800	To change the MTU on a particular interface, use the mtu command at the configuration level for the interface.
#show interface ve 300	To view VE interface information.
#show interface ethernet 15	To view Ethernet interface information.

### SSL

#import key	To import a key. (RSA & ECDSA)
#import cert	To import a CA-signed certificate. (RSA & ECDSA)
#web-service secure private-key load	(RSA & ECDSA)
#web-service secure certificate load	(RSA & ECDSA)
#import glm-cert	(RSA)
#sshd key load	(RSA)
#ssh-private-key import	(RSA)

### Backup

```
#backup system scp:// exa mpl eus er@ 192.16 8.3.3/ hom e/u ser s/e xam ple use r/b ack ups /ba cku pfi le.t  
z
```

```
#backup log period 1 use-mg mt-port scp:// exa mpl eus er@ 192.16 8.3.3/ hom e/u ser s/e xam ple use r/b ack  
/ba cku plo g.t ar.gz
```



By **M. Yasin Cavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 3 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Configuration Management

#### Save Configurations

<code>#write memory</code>	Replaces the configuration profile in the image area with the running-config.
<code>#write force</code>	Forces the ACOS device to save the configuration regardless of whether the system is ready.
<code>#write memory primary</code>	Replaces the configuration profile stored in the primary image area with the running-config
<code>#write memory secondary</code>	Replaces the configuration profile stored in the secondary image area with the running-config.
<code>#write memory profil e-name</code>	The ACOS device replaces the commands in the specified profile-name with the running-config.

#### View Configurations

<code>#show startu p-c onfig</code>	To view locally stored configuration information.
<code>#show startu p-c onfig all</code>	To display a list of the locally stored configuration profiles.
<code>#show startu p-c onfig profile profil e-name</code>	Displays the commands that are in the specified configuration profile.

#### Copy Configurations

<code>#copy</code>	To copy configurations.
<code>#copy startu p-c onfig profil e-name</code>	Copies the configuration profile that is currently linked to "startup-config" and saves the copy under the specified profile-name.
<code>#copy startu p-c onfig runnin g-c onfig</code>	Copies the configuration profile that is currently linked to "startup-config" and replaces the current running-config.
<code>#copy runnin g-c onfig startu p-c onfig</code>	Copies the running-config and saves it to the configuration profile currently linked to the startup-config.

#### Compare Configurations

<code>#diff startu p-c onfig runnin g-c onfig</code>	Compares the configuration profile that is currently linked to "startup-config" with the running-config.
<code>#diff startu p-c onfig profil e-name</code>	Compares the configuration profile that is currently linked to "startup-config" with the specified configuration profile-name.
<code>#diff profil e-name1 profil e-name2</code>	To compare any two configuration profiles.

#### Link Configuration Profiles

<code>#link</code>	To link configuration profiles.
--------------------	---------------------------------



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 4 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Configuration Management (cont)

#link startu p-c onfig test-p rofile primary To links the startup-config to a new profile called test\_profile.

#link startu p-c onfig default To relink "startup-config" to the configuration profile stored in the image area.

#### Delete a Profile

#delete To delete configurations.

#delete startu p-c onfig test\_p rofile1 To remove a specific configuration profile.

### Source Interface for Management Traffic

#show ip route mgmt To display the routes in the management route table.

#show ip route To display the data plane routes.

#show ip fib To display the data plane routes.

#show techsu pport To display general information about the router when reporting a problem.

#ip contro l-a pps -us e-m gmt -port To management interface as the source interface for automated management traffic is enable. (Execute in interface management)

#interface loopback 2 To configure an IP address on loopback interface 2.

#ip address 10.10.1 0.66 /24

#exit

#ip mgmt-t raffic all source -in terface loopbac k 2 To configures the ACOS device to use loopback interface 2 as the source interface for management traffic of all types listed above.

### Boot Options

#show version To shows storage area information.

#show bootimage To view the storage location for future reboots.

#bootimage hd sec To configure the ACOS device to use the secondary storage area on the SSD or hard drive for future reboots, and verify the setting.

### Fail-Safe Automatic Recovery

#### FPGA and Software Fail-Safe

#fail-safe fpga-b uff -re cov ery -th res hold 2 Trigger the fail-safe recovery if the number of free (available) FPGA buffers drops below 2 long enough for the recovery timeout to occur.

#fail-safe sw-err or- rec ove ry- timeout 3 Trigger the fail-safe recovery if a software error remains in effect for longer than 3 minutes.

#show fail-safe config Verify the configuration.

#show fail-safe inform ation To output differs between models that use FPGAs in hardware and models that do not.

#### L2/3 ASIC Fail-Safe



By M. Yasin Çavdar  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 5 of 30.

Sponsored by [Readable.com](https://readable.com)  
Measure your website readability!  
<https://readable.com>

### Fail-Safe Automatic Recovery (cont)

```
#system asic-m mu- fail-safe recovery- threshold 5  
hold 5
```

To configure the error threshold count to 5 (the default value is 2).

### Fail-safe for Total Memory Decrease

```
#fail-safe total-memory-size-check 5 log
```

The fail-safe feature will be triggered when the total memory size is less than 5 GB. When this happens, this event will be logged.

### Power On Auto Provisioning

```
#show poap
```

To show the status (enabled or disabled) of POAP mode.

### Monitoring Tools

#### System Log Messages

```
glid 1  
pkt-rate-limit 4  
over-limit-action drop  
!
```

To configure a custom packet rate limit for TCP traffic from a source, and enable logging of DDoS events for the source.

```
ddos src entry src-v41 10.10.71.7
```

```
log-enable  
log-periodic  
l4-type tcp  
glid 1  
!
```

```
system ddos-attack log  
!
```

```
ddos template logging default
```

```
log-format-cef  
use-obj-name  
!
```

Enable CEF and object name display for DDoS event messages.

```
ddos dst entry dst-host8 10.10.10.8
```

```
log-enable  
log-periodic
```

```
! vsystem ddos-attack log  
!
```

For the template to be used, DDoS event logging also must be enabled globally and in the individual rules that will use logging.

```
#logging single -priority error
```

To configure [single-priority logging](#)

#### Emailing Log Messages

```
#logging email buffer
```

To configure log email settings.

```
#logging email buffer number 32 time 30
```

To configure the ACOS device to buffer log messages to be emailed. Messages will be emailed only when the buffer reaches 32 messages, or 30 minutes passes since the previous log message email, whichever happens first.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 6 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Monitoring Tools (cont)

```
#logging email filter 1 " level inform ation pattern abc and"
```

To configures a filter that matches on log messages if they are information-level messages and contain the string "abc". The messages will be buffered and not emailed immediately.

```
#logging email filter 1 " level inform ation pattern abc and" trigger
```

To reconfigures the filter to immediately email matching messages by using the trigger option.

### DDoS Event Logging in Common Event Format

```
ddos template logging default
log-format-cef
use-obj-name
!
```

To configure the default DDoS logging template.

```
glid 2
conn-limit 800000
!
```

To configure GLID 2, to set a custom connection limit.

```
ddos src entry v4-71 192.168.71.7
log-enable
log-periodic
l4-type tcp
glid 2
!
```

To configure a rule for source 192.168.71.7

```
glid 3
bit-rate-limit 8000000
!
```

To configure GLID 3, to set a custom bandwidth limit (bit rate).

```
ddos dst entry dst-81 10.10.10.8
log-enable
log-periodic
l4-type tcp
glid 3
!
```

To configure a rule for protected destination 10.10.10.8

```
system ddos-attack log
!
```

To globally enables DDoS event logging.

```
ddos protection enable
!
```

To enables DDoS Mitigation.

### Simple Network Management Protocol (SNMP)

```
#snmp- server enable traps
```

To enable SNMP traps.

```
#snmp- server enable traps system start
```

To enables system start traps.

```
#snmp- server view
```

To configure an SNPM view.

```
#snmp- server view exampl eview 1.2.3 included
```

To creates a view called "exampleview" which includes OID 1.2.3



### Monitoring Tools (cont)

```
#snmp- server SNMPv1-v2c user ul
#community read exampl estring
#show runnin g-c onfig | sec snmp
```

```
#snmp- server view exampl eview 1.2.3 included
#snmp- server group exampl egroup v3 auth read exampl eview
#snmp- server SNMPv3 user exampl euser group exampl egroup v3 auth md5 exampl epa ssword1 priv aes exampl ep
sword2
#show runnin g-c onfig | sec snmp
```

```
#remote 192.16 8.20.1 /24
```

```
#oid 1.2.3
remote 192.16 8.40.1 255.25 5.255.0
```

```
#snmp- server group exampl egroup v3 priv read exampl eview
```



```
#snmp- server view exampl eview 1.2.3 included
#snmp- server group exampl egroup v3 auth read exampl eview
#snmp- server SNMPv3 user exampl euser group exampl egroup v3 auth md5 exampl epa ssword1 priv aes exampl ep
sword2
```

```
#snmp enable traps system ?
```

```
#snmp enable traps system packet -drop
```

```
#snmp- server location exampl e-l ocation
```

```
#snmp- server contact exampl e-c ontact
```

```
#snmp- server host exampl e-t rap -host
```

```
#snmp- server community read exampl e-c omm uni ty- string
```

```
snmp- server view exampl e- v iew -name exampl e-oid included
```

```
#snmp- server group exampl e- g rou -name v3 auth read exampl e- r ead -vi ew-name
```

```
#snmp- server user exampl e- user group exampl e- group v3 auth md5 exampl e- p assword
```

```
#snmp- server enable traps all
```



By **M. Yasin Cavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 8 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Monitoring Tools (cont)

#### Multiple Port-Monitoring Mirror Ports

#mirro r-port	To configure mirror ports.
#mirro r-port 1 ethernet 4	Example for mirror ports.
#mirro r-port 2 ethernet 7 output	Example for mirror ports.
#mirro r-port 3 ethernet 9	Example for mirror ports.
#mirro r-port 4 ethernet 3 input	Example for mirror ports.
#show mirror	Verifies the mirror configuration.
#interface ethernet 1 #monitor input 1	To access the configuration level for Ethernet interface 1 and enable monitoring of its traffic.
#interface ethernet 2 #monitor output 2	To access the configuration level for Ethernet interface 2 and enable monitoring of its traffic.
#interface ethernet 2 #no monitor output 2	To removing the monitor configuration.
#no mirror -port 2 ethernet 7 output	To removing the mirror port configuration.

#### Link Monitoring

#ddos template monitor 1	To configure monitor template 1 and the physical data interfaces and events to monitor.
#monitor link-down eth 5 sequence 1	
#monitor link-down eth 6 sequence 2	
#monitor link-down eth 9 sequence 3	
#monitor link-down eth 10 sequence 4	
#action clear sessions sequence 1	To configure the actions to take when a monitored event is detected.
#action link-d isable eth 5 sequence 2	
#action link-d isable eth 6 sequence 3	
#action link-d isable eth 9 sequence 4	
#action link-d isable eth 10 sequence 5	
#exit	
#system template monitor 1	To activates the template, to place it into effect.
#clear session	To clears only data sessions.
#clear sessions all	To clear all sessions.

### NetFlow

#### NetFlow Configuration

#netflow monitor test	To configure a NetFlow monitor named "test" to collect all NetFlow v5-compatible flow records and export them to the host at IP 10.10.3.2
#record netflow-v5	
#record netflow-v5-ext	
#destination 10.10.3.2	
#show netflow monitor	



By M. Yasin Çavdar  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 9 of 30.

Sponsored by [Readable.com](https://readable.com)  
Measure your website readability!  
<https://readable.com>

### NetFlow (cont)

```
#netflow monitor test
#protocol v10
#resend-template records 2
#source-address ip 10.10.3.1
#record ddos-general-stat
#record ddos-http-stat
#destination 10.10.3.2
#show netflow monitor
```

To configure a NetFlow monitor named "test" used to export DDoS general statistics and DDoS HTTP statistics to the host IP 10.10.3.2 using IPFIX.

### Network Address Translation (NAT)

#### NAT for DDoS Mitigation Sources and Destinations

```
#ip nat pool p1 172.16 8.6.100 172.16 8.6.100 netmask /24
#ddos dst entry ip-dst -entry 10.10.6.50
#l4-type udp
#stateful
#exit
#source-nat-pool p1
#exit
```

Stateful session mode is required but is disabled by default for UDP. To configure NAT at the Layer 4 UDP level or on individual UDP ports within a rule, you first must enable stateful mode. The following example configures source NAT for client traffic allowed to go to destination 10.10.6.50

```
#ddos dst entry ip-des t-entry 10.10.6.60
#dest-nat 192.16 8.6.50
```

To configure destination NAT for destination 10.10.6.60

#### Configuring NAT ALG for PPTP

```
#access-list 1 permit 10.1.1.0 0.0.0.255
#ip nat pool pptp-pool 192.16 8.1.100 192.16 8.1.110 netmask /24
```

Define the ACL and configure the IP address pool.

```
#interface ethernet 1
#ip address 10.2.2.254 255.255.255.0
#ip nat inside
#exit
#interface ethernet 2
#ip address 10.3.3.254 255.255.255.0
#ip nat outside
```

Enable inside source NAT and outside source NAT on the interfaces.

```
show ip nat alg pptp statistics
```

To displays PPTP NAT ALG statistics.

Make sure you are in Global Configuration mode.

### System Command Reference

#### Session Access Levels

ACOS> User EXEC Level. This is the first level entered when a CLI session begins. At this level, users can view basic system information but cannot configure system or port parameters. (>)



By M. Yasin Çavdar  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 10 of 30.

Sponsored by [Readable.com](https://readable.com)  
Measure your website readability!  
<https://readable.com>

### System Command Reference (cont)

ACOS#	Privileged EXEC Level. Critical commands (configuration and management) require that the user be at the "Privileged EXEC" level. To change to the Privileged EXEC level, type <code>enable</code> then press Enter at the <code>ACOS&gt;</code> prompt. (#)
ACOS(c onfig)#	Privileged EXEC Level - Config Mode. The Privileged EXEC level's configuration mode is used to configure the system IP address and to configure switching and routing features. To access the configuration mode, you must first be logged into the Privileged EXEC level. Enter the <code>config</code> command.
?	System prompt to display a list of available commands for each command mode. The context-sensitive help feature provides a list of the arguments and keywords available for any command.
#terminal history size 500 #show terminal   sec history	To set the buffer size for the current session. For example, to set the buffer to 500, then verify the change with the <code>show terminal</code> command.
no terminal history size	To reset the buffer size for this session to the default value.
> show history	While in EXEC mode, lists the most recent commands entered.
begin string	Begins the output with the line containing the specified string.
include string	Displays only the output lines that contain the specified string.
exclude string	Displays only the output lines that do not contain the specified string.
section string	Displays only the lines for the specified section (for example, "ddos dst entry", or "logging"). To display all DDoS-related configuration lines, you can enter "ddos".
	Delimiter between the <code>show</code> command and the display filter.
show arp   include 192.16 8.1.3 *	The output filter in this example displays only the ARP entries that contain IP addresses that match "192.168.1.3" and any value following "3". The asterisk ( * ) matches on any pattern following the "3".



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 11 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference (cont)

`show startup p-c onfig | section logging` To displays the startup-config lines for "logging".

#### EXEC Commands

<code>enable</code>	Enter privileged EXEC mode, or any other security level set by a system administrator.
<code>exit</code>	When used from User EXEC mode, this command closes an active terminal session by logging off the system. In any other mode, it will move the user to the previous configuration level.
<code>help</code>	Display a description of the interactive help system of the ACOS device.
<code>no</code>	Most configuration commands have a <code>no</code> form. Typically, you use the <code>no</code> form to disable a feature or function. The command without the <code>no</code> keyword is used to re-enable a disabled feature or to enable a feature that is disabled by default.
<code>ping</code>	Send an ICMP echo packet to test network connectivity.
<code>show</code>	Show system or configuration information.
<code>ssh</code>	Establish a Secure Shell (SSH) connection from the Thunder Series to another device.
<code>telnet</code>	Open a Telnet tunnel connection from the Thunder Series to another device.
<code>traceroute</code>	Display the router hops through which a packet sent from the ACOS device can reach a remote device.

#### Privileged EXEC Commands

<code>axdebug</code>	Access the AXdebug subsystem.
<code>backup log</code>	Configure log backup options and save a backup of the system log.
<code>backup system</code>	Back up the system. The startup-config file, and SSL certificates and keys will be backed up to a tar file.
<code>clear</code>	Clear statistics or reset functions. Sub-command parameters are required for specific sub-commands.
<code>clock</code>	Set the system time and date.
<code>configure</code>	Enter Global configuration mode from the Privileged EXEC mode.



By **M. Yasin Çavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 12 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference (cont)

<code>ddos run-time-use-rs t ring</code>	Set the DDoS runtime user string. The runtime user string provides a way to add a nonpersistent memo to the device. The runtime user string does not appear in the runningconfig and is not saved across reboots or reloads.
<code>debug</code>	Access debug options.
<code>diff</code>	Display a side-by-side comparison of the commands in a pair of locally stored configurations.
<code>disable</code>	Exit the Privileged EXEC mode and enter the EXEC mode.
<code>enable -bg p-a dve rti se ment</code>	Enable BGP advertisements.
<code>exit</code>	Exit the Privileged EXEC mode and enter the EXEC Mode.
<code>export</code>	Export a file to a remote site using the specified transport method.
<code>help</code>	Display a description of the interactive help system of the ACOS device.
<code>import</code>	Get a file from a remote site.
<code>locale</code>	Set the locale for the current terminal session.
<code>no</code>	Negate a command or set it to its default setting.
<code>ping</code>	Test network connectivity.
<code>reboot</code>	Reboot the device.
<code>reload</code>	Restart ACOS system processes and reload the startup-config, without rebooting.
<code>repeat</code>	Periodically re-enter a <code>show</code> command.
<code>show</code>	Display system or configuration information.
<code>shutdown</code>	Schedule a system shutdown at a specified time or after a specified interval, or cancel a scheduled system shutdown.
<code>ssh</code>	Establish a Secure Shell (SSH) connection from the Thunder Series to another device.
<code>telnet</code>	Establish a Telnet connection from the ACOS device to another device.
<code>terminal</code>	Set terminal display parameters for the current session.
<code>traceroute</code>	Display the route hops to a destination.
<code>write force</code>	Forces the ACOS device to save the configuration regardless of whether the system is ready.



By **M. Yasin Çavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 13 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference (cont)

<code>write memory</code>	Write the running-config to a configuration profile.
<code>write terminal</code>	Display the current running-config on your terminal.

### System Command Reference 2

#### Global Configuration Commands

<code>access -list</code>	Standard. Configure a standard Access Control List (ACL) to permit or deny source IP addresses.
<code>access -list</code>	Extended. Configure an extended Access Control List (ACL) to permit or deny traffic based on source and destination IP addresses, IP protocol, and TCP/UDP ports.
<code>accounting</code>	Configure TACACS+ as the accounting method for recording information about user activities.
<code>admin</code>	Configure an admin account for management access to ACOS.
<code>admin- lockout</code>	Set lockout parameters for admin sessions.
<code>admin- session clear</code>	Clear current ACOS admin sessions.
<code>arp</code>	Create a static ARP entry.
<code>arp-ti meout</code>	Change the aging timer for dynamic ARP entries.
<code>audit</code>	Configure command auditing.
<code>authen tic ation console type</code>	Configure a console authentication type.
<code>authen tic ation enable</code>	Configuration authentication of admin enable (Privileged mode) access.
<code>authen tic ation login privil ege - mode</code>	Place admins into the CLI directly at the Privileged EXEC level following successful authentication. The admin does not need to navigate to the Privileged EXEC level from the User EXEC level.
<code>authen tic ation mode</code>	Enable tiered authentication.
<code>authen tic ation multip le- aut h-r eject</code>	Configure support for multiple concurrent admin sessions using the same account.
<code>authen tic ation type</code>	Set the authentication method used to authenticate administrative access to ACOS.
<code>author ization</code>	Configure authorization for controlling access to functions in the CLI. The ACOS device can use TACACS+ for authorizing commands executed under a specified privilege level. This command also allows you to specify the level for authorization debugging.



By **M. Yasin Çavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 14 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>



### System Command Reference 2 (cont)

<code>backup log</code>	Configure log backup options and save a backup of the system log.
<code>backup store</code>	Configure and save file access information for backup. When you back up system information, you can save typing by specifying the name of the store instead of the options in the store.
<code>backup system</code>	Back up the system. The startup-config file, and SSL certificates and keys will be backed up to a tar file.
<code>backup -pe riodic</code>	Schedule periodic backups.
<code>banner</code>	Set the banners to be displayed when an admin logs onto the CLI or accesses the Privileged EXEC mode.
<code>bfd echo</code>	Enables echo support for Bidirectional Forwarding Detection (BFD).
<code>bfd enable</code>	Globally enable BFD packet processing.
<code>bfd interval</code>	Configure BFD timers.
<code>bgp</code>	The commands in this section apply globally to the BGP process running on the ACOS device.
<code>bootimage</code>	Specify the boot image location from which to load the system image the next time the Thunder Series is rebooted.
<code>boot-b loc k-fix</code>	Repair the master boot record (MBR) on the hard drive or compact flash.
<code>bridge -vl an- group</code>	Configure a bridge VLAN group for VLAN-to-VLAN bridging.
<code>captur e-c onfig</code>	This command configures DDoS packet capture so that the packets causing DDoS violations can be reviewed and analyzed.
<code>class-list</code>	Configure a class list.
<code>conver t-s tar tup -co nfig</code>	Convert configuration profile from version 3.0/3.1 to 3.2.
<code>copy</code>	Copy a running-config or startup-config.
<code>ddos</code>	Configure DDoS Mitigation settings.
<code>debug</code>	Legacy debug command. It is recommended to use the AXdebug subsystem instead of these <code>debug</code> commands.
<code>delete</code>	Delete an axdebug capture file.
<code>diff</code>	Display a side-by-side comparison of the commands in a pair of locally stored configurations.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 15 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference 2 (cont)

<code>disabl e-f ailsafe</code>	Disable fail-safe monitoring for software-related errors.
<code>disabl e-m ana gement service</code>	Disable management access to specific protocols on specific Ethernet interfaces.
<code>do</code>	Run a Privileged EXEC level command from a configuration level prompt, without leaving the configuration level.
<code>domain -group</code>	Create a group of related <code>domain -list</code> configurations
<code>domain -list</code>	Create a domain classification list.
<code>enable -core</code>	Change the file size of core dumps.
<code>enable -ma nagement</code>	Enable management access to specific protocols on specific Ethernet interfaces.
<code>enable -pa ssword</code>	Set the enable password, which secures access to the Privileged EXEC level of the CLI.
<code>end</code>	Return to the Privileged EXEC level of the CLI.
<code>enviro nment temper ature thresho ld</code>	Configure the temperature condition under which a log is generated.
<code>enviro nment update -in terval</code>	Configure the hardware polling interval for fault detection and log generation.
<code>erase</code>	Erase the startup-config file. This command returns the device to its factory default configuration after the next reload or reboot.
<code>exit</code>	Return to the Privileged EXEC level of the CLI.
<code>export</code>	Export a file to a remote site using the specified transport method.
<code>export -pe riodic</code>	Export file to a remote site periodically.
<code>fail-safe</code>	Configure fail-safe automatic recovery.
<code>fan-speed</code>	Control fan speed setting.
<code>glid</code>	Configure a Global Limit ID (GLID). A GLID is a set of traffic limits that can be used with other features, such as DDoS Mitigation.
<code>hd-monitor enable</code>	Enable hard disk monitoring on your ACOS device.
<code>hostname</code>	Set the ACOS device's hostname.
<code>icmpv6 -ra te- limit</code>	Configure ICMPv6 rate limiting for IPv6 to protect against denial-of-service (DoS) attacks.
<code>icmp-r ate -limit</code>	Configure ICMP rate limiting, to protect against denial-of-service (DoS) attacks.
<code>import</code>	Get a file from a remote site.
<code>import -pe riodic</code>	Get files from a remote site periodically.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 16 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference 2 (cont)

<code>interface</code>	Access the CLI configuration level for an interface.
<code>ip</code>	Configure global IP settings.
<code>ipmi</code>	Configure Intelligent Platform Management Interface (IPMI) settings on the ACOS device.
<code>ipv6</code>	Configure global IPv6 settings.
<code>key</code>	Configure a key chain for use by routing authentication features.
<code>lACP-p ass through</code>	Configure an LACP tunnel for LACP passthrough. This feature allows the ACOS device to forward traffic on one trunk that originates on another trunk that is down. With this feature, if an LACP trunk goes down, the other trunk is used to continue connectivity for the traffic.
<code>lACP system -pr iority</code>	Set the Link Aggregation Control Protocol (LACP) priority.
<code>ldap-s erver</code>	Set Lightweight Directory Access Protocol (LDAP) parameters for authenticating administrative access to the ACOS device.
<code>link</code>	Link the "startup-config" token to the specified configuration profile. By default, "startup-config" is linked to "default", which means the configuration profile stored in the image area from which the ACOS device most recently rebooted.
<code>lldp enable</code>	Enable the Link Layer Detection Protocol (LLDP). You can enable LLDP to either receive only, transmit only, or transmit and receive.
<code>lldp manage men t-a ddress</code>	Specify the hostname or IP address and Ethernet interface to use as the management interface for the LLDP agent on the ACOS device.
<code>lldp notifi cation interva l</code>	Configure the interval between transmission of LLDP notifications during normal transmission periods. (In the IEEE 802.3AB specification, this the msgTxInterval parameter.)
<code>lldp system -de scr iption</code>	Defines the alpha-numeric string that describes the system in the network.
<code>lldp system -name</code>	Defines the string that will be assigned as the system name.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 17 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

### System Command Reference 2 (cont)

<code>lldp tx fast-count</code>	Set the initial value for the txFast variable, which determines the number of LLDP data packets that are transmitted during a fast transmission period. (In the IEEE 802.3AB specification, this the txFastInit parameter.)
<code>lldp tx fast-interval</code>	Configure the LLDP PDU transmission interval for fast periods. (In the IEEE 802.3AB specification, this the msgFastTx parameter.)
<code>lldp tx hold</code>	Configure the time to live (TTL) transmission interval that is carried in LLDP frames during normal (non-fast) periods. (In the IEEE 802.3AB specification, this the msgTxHold parameter.)
<code>lldp tx interval</code>	Configure the LLDP packet transmit interval. (In the IEEE 802.3AB specification, this the msgTxInterval parameter.)
<code>lldp tx reinit -delay</code>	Configure the delay between a change to administrative “disabled” status of LDDP and reinitialization of the protocol.
<code>locale</code>	Set the locale for the current terminal session.
<code>logging auditlog host</code>	Configure audit logging to an external server.
<code>logging buffered</code>	Configure the event log on the ACOS device.
<code>logging console</code>	Set the logging level for messages sent to the console.
<code>logging email-addresses</code>	Specify the email addresses to which to send event messages.
<code>logging email buffer</code>	Configure log email settings.
<code>logging email filter</code>	Configure a filter for emailing log messages.
<code>logging export</code>	Send the messages that are in the event buffer to an external file server.
<code>logging facility</code>	Enable logging facilities.
<code>logging host</code>	Specify a Syslog server to which to send event messages.
<code>logging monitor</code>	Set the logging level for messages sent to the terminal monitor.
<code>logging syslog</code>	Set the syslog logging level for events sent to the syslog host.
<code>logging trap</code>	Set the logging level for traps sent to the SNMP host.
<code>mac-address</code>	Configure a static MAC address.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 18 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference 2 (cont)

<code>mac-ag e-time</code>	Set the aging time for dynamic (learned) MAC entries. An entry that remains unused for the duration of the aging time is removed from the MAC table.
<code>maximu m-paths</code>	Change the maximum number of paths a route can have in the Forwarding Information Base (FIB).
<code>mirror -port</code>	Specify a port to receive copies of another port's traffic.
<code>monitor</code>	Specify event thresholds for utilization of resources.
<code>multi- config</code>	Enable simultaneous admin sessions.
<code>multi- ctr l-cpu</code>	Enable use of more than one CPU for control processing.
<code>netflow common max-pa cke t-q ueu e-time</code>	Specify the maximum amount of time ACOS can hold onto a NetFlow record packet in the queue before sending it to the NetFlow collector. ACOS holds a NetFlow packet in the queue until the packet payload is full of record data or until the queue timer expires.
<code>netflow common select or- alg orithm ran dom</code>	Configures the algorithm that Netflow uses to sample traffic. The only option is the random algorithm.
<code>netflow monitor</code>	Enable ACOS to act as a NetFlow exporter, for monitoring traffic and exporting the data to one or more NetFlow collectors for analysis.
<code>no</code>	Remove a configuration command from the running configuration.
<code>ntp</code>	Configure Network Time Protocol (NTP) parameters.
<code>ntp-status</code>	Get the status of the NTP servers.
<code>overla y-t unnel</code>	Configure a remote tunnel endpoint for remote sites where protected objects reside. This can be used in conjunction with OSPF neighbor adjacency via GRE or VXLAN tunnels.
<code>pki delete</code>	Deletes a self-signed certificate or the CSR file.
<code>radius -server host</code>	Set RADIUS parameters, for authenticating administrative access to the ACOS device.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 19 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference 2 (cont)

<code>restore</code>	Restore the startup-config, aFlex policy files, <<when aFlex support is added>> and SSL certificates and keys from a .tar file previously created by the backup command. The restored configuration takes effect following a reboot.
<code>router log file</code>	Configure router logging to a local file.
<code>router log log-buffer</code>	Sends router logs to the logging buffer.
<code>router protocol</code>	Enter the configuration mode for a dynamic routing protocol.
<code>route-map</code>	Configure a route map.
<code>runnin g-c onfig</code>	Enable display of file information in the running-config.
<code>run-hw -diag</code>	Access the hardware diagnostics menu.
<code>sflow</code>	Configure parameters for sFlow packet sampling.
<code>single -bo ard -mode forc ed</code>	On the Thunder 14045 device with dual processing modules, this command causes all traffic to be processed by the master only.
<code>smtp</code>	Configure a Simple Mail Transfer Protocol (SMTP) server to use for sending emails from the ACOS device.
<code>ssh-lo gin -gr ace -time</code>	Configures the time to establish an SSH connection.
<code>sshd</code>	Perform an SSHD operation on the system.
<code>system all-vl an- limit</code>	Set the global traffic limits for all VLANs. The limit applies system-wide to all VLANs; collectively, all ACOS device VLANs cannot exceed the specified limit.
<code>system anomaly</code>	Enable logging for packet anomaly events. This type of logging applies to system-wide attacks such as SYN attacks.
<code>system asic-m mu- fai l-s afe</code>	Configures fail-safe parameters for the Layer 2/3 ASIC.
<code>system attack</code>	Enable logging for DDoS attacks. This type of logging applies to violations of DDoS Mitigation rules.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 20 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference 3

<code>system cpu-load-sharing</code>	Configure thresholds for CPU load sharing. If a threshold is exceeded, CPU load sharing is activated to relieve the stressed CPUs. When activated, CPU load sharing distributes processing of the stressed CPU's operations across the device's other CPUs. Load sharing remains in effect until the threshold is no longer exceeded.
<code>system ddos-attack-log</code>	Enable logging for DDoS attack events.
<code>system default-mtu</code>	Configure the MTU for all interfaces.
<code>system external-only-logging</code>	Enable external only logging for packet driven DDoS logs. When enabled, DDoS non-event logs will not be displayed through <code>show log</code> . Other types of logs are unaffected.
<code>system fips</code>	Enable/Disable FIPS Mode for ACOS devices.
<code>system glid</code>	Globally apply the specified GLID to the whole system.
<code>system jumbo-frame-global-enable -jumbo</code>	Globally enable jumbo frame support. In this release, a jumbo frame is an Ethernet frame that is more than 1522 bytes long.
<code>system module-control-cpu</code>	Throttle CLI and SNMP output when control CPU utilization reaches a specific threshold.
<code>system monitor-template</code>	Configure monitoring of a set of ports for link-state changes, and change the link states of another set of ports, or clear sessions based on the detected changes.
<code>system disable-sockstress-protection</code>	Globally disable Sockstress protection on the system.
<code>system per-vlan-limit</code>	Configure the packet flooding limit per VLAN. The limit applies to each VLAN. No individual can exceed the specified limit.
<code>system -reset</code>	Restore the ACOS device to its factory default settings.
<code>system resource-usage</code>	Change the capacity of a system resource.
<code>system session-reclaim-limit</code>	Set limits for SMP session reclaim; this controls how the system should recover and reclaim DDoS entries.
<code>system template-bind-monitor</code>	Apply a monitor template to the whole TPS system.
<code>system timeout-value</code>	Set the timeout to stop transferring a file.



By **M. Yasin Çavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 21 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### System Command Reference 3 (cont)

<code>system trunk load-b alance</code>	Configure trunk load balancing for Layer 2 switched packets (applicable for both static and LACP trunks).
<code>system ve-mac -scheme</code>	Configure MAC address assignment for Virtual Ethernet (VE) interfaces.
<code>system -ju mbo -global enable -jumbo</code>	Globally enable jumbo frame support. In this release, a jumbo frame is an Ethernet frame that is more than 1522 bytes long.
<code>system default t-mtu</code>	Configure the MTU for all interfaces.
<code>tacacs -server host</code>	Configure TACACS+ for authorization and accounting. If authorization or accounting is specified, the ACOS device will attempt to use the TACACS+ servers in the order they are configured. If one server fails to respond, the next server will be used.
<code>tacacs -server monitor</code>	Check the status of TACACS+ servers.
<code>techreport</code>	Configure automated collection of system information. If you need to contact Technical Support, they may ask you to for the techreports to help diagnose system issues.
<code>terminal</code>	Set the terminal configuration.
<code>tftp blksize</code>	Change the TFTP block size.
<code>timezone</code>	Configure the time zone on your system.
<code>tx-con ges tio n-ctrl</code>	Configure looping on the polling driver, on applicable models.
<code>upgrade</code>	Upgrade the system.
<code>ve-stats</code>	Enable statistics collection for Virtual Ethernet (VE) interfaces.
<code>vlan</code>	Configure a virtual LAN (VLAN). This command changes the CLI to the configuration level for the VLAN.
<code>vlan-g lobal enable -de f-v lan -12 -fo r wa rding</code>	Enable Layer 2 forwarding on the default VLAN (VLAN 1).
<code>vlan-g lobal l3-vla n-f wd- disable</code>	Globally disable Layer 3 forwarding between VLANs.
<code>vlan-group</code>	Configure a group of VLANs.
<code>vrrp-a</code>	Enter VRRP-A configuration mode.
<code>web-se rvice</code>	Configure access parameters for the Graphical User Interface (GUI).
<code>write</code>	Save the configuration.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 22 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>



### SNMP Commands

#snmp- server community	Deprecated command to configure an SNMP community string.
#snmp- server contact	Configure SNMP contact information.
#snmp- server enable service	Enable SNMP service on the ACOS device
#snmp- server enable traps	Enable ACOS to accept SNMP MIB data queries and to send SNMP v1/v2c traps.
#snmp- server engineID	Set the SNMPv3 engine ID of this ACOS device.
#snmp- server group	Configure an SNMP group.
#snmp- server host	Configure an SNMP v1/v2c trap receiver.
#snmp- server location	Configure SNMP location information.
#snmp- server SNMPv1-v2c	Define an SNMPv1 or SNMPv2c community. The members of the community can gain access to the SNMP data available on this device.
#snmp- server SNMPv3	Define an SNMPv3 user.
#snmp- server user	Deprecated command to configure an SNMPv3 user.
#snmp- server view	Configure an SNMP view.

### Show Commands

show access -list	Display the configured Access Control Lists (ACLs). The output lists the configuration commands for the ACLs in the running-config.
show admin	Display the administrator accounts.
show arp	Display ARP table entries.
show audit	Show the command audit log.
show axdebug capture	Display a list of debug files.
show axdebug config	Display the debug filter configuration currently applied on ACOS.
show axdebug config -file	Display a list of the debug configuration files.
Display debug capture files or their contents.	show axdebug file
show axdebug filter	Display the configured debug output filters.
show axdebug status	Display per-CPU packet capture counts for AXdebug.
show backup	Display information about scheduled backups.
show bfd	Display information for Bidirectional Forwarding Detection (BFD).
show bgp	Display information for Border Gateway Protocol (BGP).
show bootimage	Display the software images stored on the ACOS device.
show bridge -vl an- group	View information for any configured bridge VLAN groups.
show capture-configuration	View capture-config information.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 23 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Show Commands (cont)

<code>show class-list</code>	Display information for class lists.
<code>show class- list t-group</code>	Display information for class-list groups.
<code>show clns</code>	Show Connectionless Network Service (CLNS) information.
<code>show clock</code>	Display the time, timezone, and date.
<code>show context</code>	View the configuration for the sub-module in which the command is run.
<code>show core</code>	Display core dump statistics.
<code>show cpu</code>	Display CPU statistics.
<code>show ddos</code>	Show the DDoS action-list configuration on the device.
<code>show disk</code>	Display status information for the device hard disks.
<code>show domain -group</code>	Show domain-group configuration information.
<code>show domain -list</code>	Show domain-list configuration information.
<code>show dumpthread</code>	Show status information about the system threads.
<code>show enviro nment</code>	Display temperature, fan, and power supply status.
<code>show errors</code>	Show error information for the system. This command provides a way to quickly view system status and error statistics.
<code>show fail-safe</code>	Display fail-safe information.
<code>show glid</code>	View the configuration for global IP limiting rules.
<code>show hardware</code>	Displays hardware information for the ACOS device.
<code>show history</code>	Show the CLI command history for the current session.
<code>show interfaces</code>	Display interface configuration and status information.
<code>show interfaces media</code>	Display information about 1-Gbps and 10-Gbps small form-factor pluggable (SFP+) interfaces.
<code>show interfaces statistics</code>	Display interface statistics.
<code>show ip</code>	Show the IP mode in which the ACOS device is running, gateway or transparent mode.
<code>show ip bgp</code>	Show IPv4 BGP information.
<code>show ip dns</code>	Display the DNS configuration.
<code>show ip fib</code>	Display Forwarding Information Base (FIB) entries.
<code>show ipv6 fib</code>	



By **M. Yasin Çavdar**  
(myasincavdar)

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 24 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Show Commands (cont)

<code>show ip fragme ntation statistics</code>	Show statistics for IP fragmentation.
<code>show ipv6 fragme ntation statistic s</code>	
<code>show ip helper -ad dress</code>	Display DHCP relay information.
<code>show ip interfaces</code>	Display IP interface information.
<code>show ipv6 interfaces</code>	
<code>show ip isis</code>	Display the IS-IS routing table.
<code>show ipv6 isis</code>	
<code>show ip map-list</code>	Show IP map list information.
<code>show ip nat</code>	Display NAT information.
<code>show ipv6 nat</code>	
<code>show ip ospf</code>	Display OSPF status information.
<code>show ipv6 ospf</code>	
<code>show ip prefix -list</code>	Show information about configured IP prefix lists.
<code>show ipv6 prefix -list</code>	
<code>show ip protocols</code>	Show information for dynamic routing protocols.
<code>show ipv6 protocols</code>	
<code>show ip route</code>	Display the IPv4 or IPv6 routing table.
<code>show ipv6 route</code>	
<code>show ipmi</code>	Show information for the Intelligent Platform Management Interface (IPMI) on the ACOS device.
<code>show ipv6 ndisc</code>	Display information for IPv6 router discovery.
<code>show ipv6 neighbor</code>	Display information about neighboring IPv6 devices.
<code>show ipv6 stats</code>	Show IPv6 statistics.
<code>show ipv6 traffic</code>	Display IPv6 traffic statistics.
<code>show isis</code>	Display information for Intermediate System to Intermediate System (IS-IS).
<code>show json-c onfig</code>	View the JSON/aXAPI data format associated with the running-config, or for a specific object.
<code>show json-c onf ig- detail</code>	View detailed JSON/aXAPI data format associated with the running-config, or for a specific object.The output is similar to the output for <code>show json-c onfig</code> with the addition of the <code>al0-url</code> and <code>obj-type</code> fields.
<code>show json-c onf ig- wit h-d efault</code>	View JSON/aXAPI data format associated with the running-config, or for a specific object. The output is similar to the output for <code>show json-c onf ig- detail</code> with the addition of default values for objects not explicitly configured.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 25 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Show Commands (cont)

<code>show key-chain</code>	Show configuration information for an authentication key chain.
<code>show lacp</code>	Show configuration information and statistics for Link Aggregation Control Protocol (LACP).
<code>show lacp-p ass throug h</code>	Show LACP passthrough configuration.
<code>show license</code>	Display the host ID and, if applicable, serial number of the license applied to this ACOS device.
<code>show lldp neighbors</code>	Displays information on all remote neighbors or on the specified interface.
<code>show lldp statistics</code>	Displays LLDP receive or send error statistics, You can display information on all interfaces or only display information on a specified interface.
<code>show locale</code>	Display the configured CLI locale.
<code>show log</code>	Display entries in the syslog buffer or display current log settings (policy). Log entries are listed starting with the most recent entry on top.
<code>show mac-ad dre ss- ta ble</code>	Display MAC table entries.
<code>show management</code>	Show the types of management access allowed on each of the device's Ethernet interfaces.
<code>show memory</code>	Display memory usage information.
<code>show mirror</code>	Display port mirroring information.
<code>show monitor</code>	Display the event thresholds for system resources.
<code>show netflow</code>	Display NetFlow information.
<code>show ntp</code>	Show the Network Time Protocol (NTP) servers and status.
<code>show overla y-t unnel</code>	Shows statistics of overlay tunnels on the ACOS device.
<code>show pki</code>	Shows information about the certificates on the ACOS device.
<code>show poap</code>	View the POAP status of your system.
<code>show process system</code>	Display the status of system processes.
<code>show radius -server</code>	Display RADIUS statistics.
<code>show reboot</code>	Display scheduled system reboots.
<code>show route-map</code>	Show the configured route maps.
<code>show router log file</code>	Show router logs.
<code>show runnin g-c onfig</code>	Display the running-config.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 26 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Show Commands (cont)

show session	Display session information.
show sflow	Show sFlow information.
show shutdown	Display scheduled system shutdowns.
show snmp	Display SNMP OIDs for the specified objects.
show snmp stats	Display SNMP statistics.
show startup-config	Display a configuration profile or display a list of all the locally saved configuration profiles.
show statistics	Display packet statistics for interfaces.
show store	Display the configured file transfer profiles in the credential store. The credential store is a saved set of access information for file transfer between the ACOS device and remote file servers.
show system cpu-load-sharing	Displays CPU load sharing information.
show system platform	Display platform-related information and statistics.
show system resource-usage	Display Layer 4 session capacity information.
show tacacs-server	Display TACACS statistics.
show techsupport	Display or export system information for use when troubleshooting.
show terminal	Show the terminal settings.
show tftp	Display the currently configured TFTP block size.
show trunk	Show information about the trunks configured on the system.
show version	Display software, hardware, and firmware version information.
show vlans	Display the configured VLANs.
show vrrp-a	Display VRRP-A information.

### AX Debug Commands

apply-config	Apply an AXdebug configuration file.
capture	Start capturing packets.
count	Specify the maximum number of packets to capture.
delete	Delete an axdebug capture file.
filter-config	Configure an AX debug filter, to specify the types of packets to capture.
incoming	Specify the Ethernet interfaces and traffic direction for which to capture packets.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 27 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### AX Debug Commands (cont)

<code>length</code>	Specify the maximum length of packets to capture. Packets that are longer are not captured.
<code>maxfile</code>	Specify the maximum number of axdebug packet capture files to keep.
<code>outgoing</code>	Limits the packet capture to outbound packets on Ethernet interface "x".
<code>save-c onfig</code>	Save your AXdebug configuration to a file.
<code>sess-f ilt er-dis</code>	Disable the session-based filter.
<code>tcpdump</code>	Capture packets for analysis.
<code>timeout</code>	Specify the maximum number of minutes to capture packets.



By **M. Yasin Çavdar**  
(myasincavdar)

Published 30th January, 2023.  
Last updated 31st January, 2023.  
Page 28 of 30.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

[cheatography.com/myasincavdar/](https://cheatography.com/myasincavdar/)