ACOS 6.0.8

System Configuration and Administration Guide

December, 2025

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc.. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

System Overview

This chapter provides a brief overview of the A10 Thunder Series systems and features.

The following topics are covered:

Intended Audience

ACOS is typically deployed by IT teams in enterprise and service provider environments. The content in this guide is written for technical professionals who install, configure, or maintain Thunder appliances in production networks.

This guide is intended for:

- System Administrators and Network Engineers configuring and maintaining Thunder or vThunder appliances.
- Data Center Operators managing device health, system logs, and upgrades.
- Integration Specialists working with third-party platforms such as Microsoft SCVMM.
- Security Administrators enforcing compliance, securing access, and monitoring system activity.

Prerequisite

Before using this guide, administrators should be comfortable with basic networking and system management concepts. Prior knowledge ensures smoother configuration and reduces the chance of deployment errors.

You should have:

- Working knowledge of TCP/IP networking concepts (IP addressing, routing, and VLANs).
- Familiarity with Ethernet and Layer 2/3 networking.
- Experience with command-line interfaces (CLI) and/or web-based management interfaces.
- Understanding of system administration practices, such as backups, logging, and user access controls.
- (Optional but recommended) Familiarity of A10 Thunder-specific deployment models (hardware, vThunder, or cThunder).

ACOS Product Overview

ACOS is available in multiple form factors to support a wide range of deployment environments, from physical appliances to cloud and containerized solutions. Each form factor offers the same ACOS capabilities, tailored for different infrastructures.

A10 Thunder Series Physical Appliance

A10 Thunder Series is the high-performance hardware solutions for various A10 Networks services. Hardware specifications vary by model, with options for different processors, memory, storage, network interfaces, and power supplies, all designed for high reliability and regulatory compliance. For more information, see Thunder Documentation and Thunder Datasheet.

Virtual Thunder (vThunder) Appliance

vThunder is a virtual appliance solution from A10 Networks that provides secure, agile, and programmable application delivery. They are designed to run on virtualized infrastructures, including public and private clouds like AWS, Microsoft

Azure, Google Cloud, and Oracle Cloud. For more information, see vThunder Documentation.

Thunder Container (cThunder)

[[[Undefined variable sagTOC.Product_Name_Short4]]] is a containerized ACOS image designed to be deployed using docker or Openshift on a host operating system. For more information, see cThunder Documentation.

BareMetal

The Thunder Bare Metal product line offers high-performance software to manage the high demands of today's application networking and security workloads. The Thunder software (ACOS) includes Application Delivery Controller (ADC) and Carrier-grade Network address translation (CGNAT) solutions.

For more information, see Baremetal Documentation.

ACOS Software Processes

The ACOS software performs its many tasks using the following processes:

- a10mon – Parent process of the ACOS device. This process is executed when the system comes up. The a10mon process does the following:
  - Brings user-space processes up and down.
  - Monitors all its child processes and restarts a process and all dependent processes if any of them die.
- syslogd – System logger daemon that logs kernel and system events.
- a10logd – Fetches all the logs from the ACOS Log database.
- a10timer – Schedules and executes scheduled tasks.
- a10stat – Monitors the status of all the main processes of the ACOS device, such as a10switch and a10lb. Also probes every thread within these processes to ensure that they are responsive. If a thread is deemed unhealthy, a10stat kills the process, after which a10mon restarts the process and other processes associated with it.
- a10switch – Contains libraries and APIs to program the Switching ASIC to perform Layer 2 and Layer 3 switching at wire speed.

- a10hm – Performs health-checks for real servers and services. This process sends pre-configured requests to external servers at pre-defined intervals. If a server or individual service does not respond, it is marked down. Once the server or service starts responding again, it is marked up.
- a10rt – Routing daemon, which maintains the routing table with routes injected from OSPF, as well as static routes.
- a10rip – Implements RIPv1 and v2 routing protocols.
- a10ospf – Implements the OSPFv2 routing protocol.
- a10snmpd – SNMPv2c and v3 agent, which services MIB requests.
- a10wa – Embedded Web Server residing on the ACOS device. This process serves the Web-based management Graphical User Interface (GUI).
- a10gmpd – Global SLB (GSLB) daemon.
- a10snpm_trapd – Handles SNMP traps initiated by a10lb.
- a10lb – The heart of the ACOS device. This process contains all the intelligence to perform Application Delivery Control.
- rimacli – This process is automatically invoked when an admin logs into the ACOS device through an interface address. The admin is presented a Command Line Interface (CLI) that can issue and save commands to configure the system.

Memory Pre-allocation

As part of normal operation, ACOS pre-allocates memory. For this reason, memory utilization can be high even when the device first boots up. The system allocates more memory if needed for burst conditions. In this case, the additional memory is freed only slowly, in case further burst conditions occur.

Thunder Hardware Interfaces

See the Installation Guide for your A10 Thunder Series model.

Data Interfaces and IP Subnet Support

The ACOS device has a management interface and data interfaces. The management interface is a physical Ethernet port. A data interface is a physical Ethernet port, a trunk group, or a Virtual Ethernet (VE) interface.

The management interface can have a single IPv4 address and/or a single IPv6 address.

An ACOS device deployed in transparent mode (Layer 2) can have a single IP address for all data interfaces. The IP address of the data interfaces must be in a different subnet than the management interface's address.

An ACOS device deployed in route mode (Layer 3) can have separate IP addresses on each data interface. No two interfaces can have IP addresses that are in the same subnet. This applies to the management interface and all data interfaces.

Deployment Modes

You can deploy the ACOS device into your network as a Layer 2 switch (transparent mode) or a Layer 3 router (route mode). In either of the deployment modes, the ACOS device has a dedicated Ethernet management interface, different from the Ethernet data interfaces. You can assign an IPv4 address and/or an IPv6 address to the management interface.

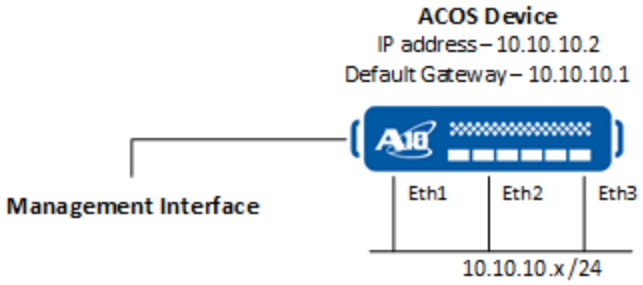
For network deployment examples, see the following:

- Transparent Mode Deployment
- Routed Mode Deployment

Transparent Mode Deployment Examples

The following Figure 1 shows an example of a Thunder Series device deployed in transparent mode.

Figure 1 : ACOS Deployment Example – Transparent Mode



NOTE:

- For simplicity, this example and the other examples in this chapter show the physical links on single Ethernet ports. Everywhere a single Ethernet connection is shown, you can use a trunk, which is a set of multiple ports configured as a single logical link.
- Transparent mode deployments are not valid for CGNv6 configurations. CGNv6 is only supported in Routed Mode Deployment Example.

Configure Using CLI

The following commands configure the global IP address and default gateway:

```
ACOS(config)# ip address 10.10.10.2 /24
ACOS(config)# ip default-gateway 10.10.10.1
```

The following commands enable the Ethernet interfaces used in the example:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# interface ethernet 3
ACOS(config-if:ethernet:3)# enable
ACOS(config-if:ethernet:3)# exit
```

Configure Using GUI

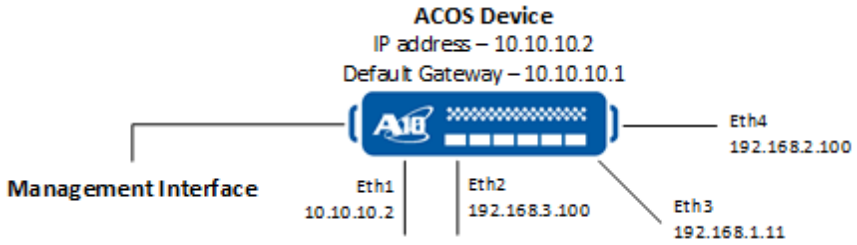
1. Hover over **Network** in the navigation bar, and select **Interfaces**.
2. Click on **Transparent** on the menu bar.
3. Enter the IP Address, IP Mask, and Default Gateway, or alternatively, the IPv6 address and gateway.
4. Click **Configure**.
5. The data interface is added to the table, which can be seen if you click LAN in the menu bar.
6. Select the checkbox next to each Ethernet data interface you wish to enable, and click **Enable**.

Route Mode Deployment Example

The following Figure 2 shows an example of an ACOS device deployed in route mode.

NOTE: Route mode is also called "**gateway**" mode.

Figure 2 : ACOS Deployment Example – Route Mode



In this example, the ACOS device has separate IP interfaces in different subnets on each of the interfaces connected to the network. The ACOS device can be configured with static IP routes and can be enabled to run OSPF and IS-IS. In this example, a static route is configured to be used as the default route through 10.10.10.1.

Although this example illustrates single physical links, you could use trunks as physical links. You also could use multiple VLANs. In this case, the IP addresses would be configured on Virtual Ethernet (VE) interfaces, one per VLAN, instead of being configured on individual Ethernet ports.

Since the ACOS device is a router in this deployment, downstream devices can use the ACOS device as their default gateway. For example, devices connected to Ethernet port 2 would use 192.168.3.100 as their default gateway, devices connected to port 3 would use 192.168.1.111 as their default gateway, and so on.

If multiple ACOS devices in a VRRP-A high availability configuration is used, the downstream devices will use a floating IP address shared by the two ACOS devices as their default gateway.

NOTE: For more information, see the *Configuring VRRP-A High Availability* guide.

Configuring the Default Route

1. Hover over **Network** in the navigation bar and select **Routes**.
2. Select either the IPv4 Static Routes or IPv6 Static Routes tab, then click **Create**.
3. Complete the IP Dest Address and IP Mask fields.

NOTE: For detailed information about these configurations and other fields on this page, see the latest version of the **Online Help**.

4. Click **Create Route**.

Configure Using CLI

The following commands enable the Ethernet interfaces used in the example and configure IP addresses on them:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address 10.10.10.2 /24
ACOS(config-if:ethernet:1)# interface ethernet 2
ACOS(config-if:ethernet:2)# enable
ACOS(config-if:ethernet:2)# ip address 192.168.3.100 /24
ACOS(config-if:ethernet:2)# interface ethernet 3
ACOS(config-if:ethernet:3)# enable
ACOS(config-if:ethernet:3)# ip address 192.168.1.111 /24
ACOS(config-if:ethernet:3)# interface ethernet 4
ACOS(config-if:ethernet:4)# enable
ACOS(config-if:ethernet:4)# ip address 192.168.2.100 /24
ACOS(config-if:ethernet:4)# exit
ACOS(config)#
```

The following command configures the default route through 10.10.10.1:

```
ACOS(config)# ip route 0.0.0.0 /0 10.10.10.1
```

Configure Using GUI

1. Hover over **Network** in the navigation bar and select **Interfaces**.
2. If you are not already on the LAN index page, click **LAN** on the menu bar.
3. Click **Edit** in the Actions column for the interface number (for example, Interface

"e1"). The configuration page appears.

a. To assign an IPv4 address, locate the "IP" section and then click the plus symbol ( ) to display the configuration fields for that section, and enter the address information.

b. To assign an IPv6 address, locate the "IPv6" section and then click the plus symbol ( ) to display the configuration fields for that section, and enter the address information.

c. Click **Update**.

Where Do I Start?

Tasks	Refer
Configure basic system settings	Common Setup Tasks
Configure partition in ACOS	Application Delivery Partition
Configure network settings	Network Configuration Guide
Configure overlay network settings	Overlay Networks
Configure management access security features	Management Access and Security Guide
Configure external event logging for ACOS	Event Logging

Common Setup Tasks

This part of the document outlines the steps to access the ACOS device device and configure essential system settings. It includes instructions and examples for the following tasks:

- Log In
- Upgrade ACOS Image
- Basic System Parameters
- System Security Settings
- Thunder Device Specific Settings

Log In

The following topics are covered:

User Interfaces

ACOS devices provide the following user interfaces:

- Command-Line Interface (CLI) – Text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
  - Secure protocol – Secure Shell (SSH) (versions 1 and 2)
  - Unsecure protocol – Telnet (if enabled)
- Graphical User Interface (GUI) – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using either of the following protocols:
  - Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
  - Unsecure protocol – Hypertext Transfer Protocol (HTTP)
- aXAPI – XML Application Programming Interface based on the Representational State Transfer (REST) architecture. The aXAPI enables you to use custom third-party applications to configure and monitor Application Delivery Controller (ADC) parameters on the ACOS device, and to monitor Ethernet interfaces. (For more information, see the aXAPI Reference.)

NOTE: By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP, HTTPS, and SNMP access are enabled by default on the management interface only, and disabled by default on all data interfaces.
The maximum number of CLI, GUI, and aXAPI sessions that can be opened simultaneously on an ACOS device depends on the specific device.

Log Into CLI

NOTE: ACOS devices provide advanced features for securing management access to the device. This section assumes that only the basic security settings are in place.

To log into the CLI using SSH:

1. On a PC connected to a network that can access the ACOS device's management interface, open an SSH connection to the IP address of the management interface.
2. If it is the first time the SSH client has accessed the ACOS device, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. (Press Enter.)
3. At the `login as:` prompt, enter the admin username.
4. At the `Password:` prompt, enter the admin password.
   A message is displayed to change the default password.

   NOTE: The password is hidden for security.

5. At the `Please enter your password:` prompt, enter the new password.
6. At the `Please re-enter your password:` prompt, re-enter the new password for verification.

   NOTE: You will only be prompted to change the default password when you log in for the first time on a new device or if the device is reset using the `system-reset` command. Starting with ACOS 6.0.0, any release that supports enforcing default password change will not prompt you to change the password again.
   The default password must not be set back as an admin password.

   If the default password is changed successfully, the command prompt for the User EXEC level of the CLI appears:

```
ACOS>
```

The User EXEC level allows you to enter a few basic commands, including some **show** commands as well as **ping** and **traceroute**.

NOTE: The "ACOS" in the CLI prompt represents the host name configured on the device; "ACOS" is the default host name used in all technical publications. The host name on your device may be different. The default host name on a system represents the system type; for example, on an A10 Thunder Series 5435 device, the default prompt is: `TH5435>`.

7. To access the Privileged EXEC level of the CLI and allow access to all configuration levels, enter the **enable** command.

   At the `Password:` prompt, enter the enable password. (This is not the same as the admin password, although it is possible to configure the same value for both passwords.

   For more information on System Password Policy Complexity, see the *Management Access and Security Guide*.

   If the enable password is correct, the command prompt for the Privileged EXEC level of the CLI appears:

   ```
   ACOS#
   ```

8. To access the global configuration level, enter the **configure** command. The following command prompt appears:

   ```
   ACOS(config)#
   ```

Log Into GUI

Web access to the ACOS device is supported on the Web browsers listed in the Table 1.

Table 1 : GUI Browser Support

Browser	Windows	Linux	MAC
Firefox 40.0.3 and higher	Supported	Supported	N/A

Table 1 : GUI Browser Support

Browser	Windows	Linux	MAC
Safari 3.0 and higher	Not Supported	N/A	Supported
Chrome 45.0.2454.93 and higher	Supported	Supported	Supported
Microsoft Edge 44.18362.387.0 and higher	Supported	N/A	N/A

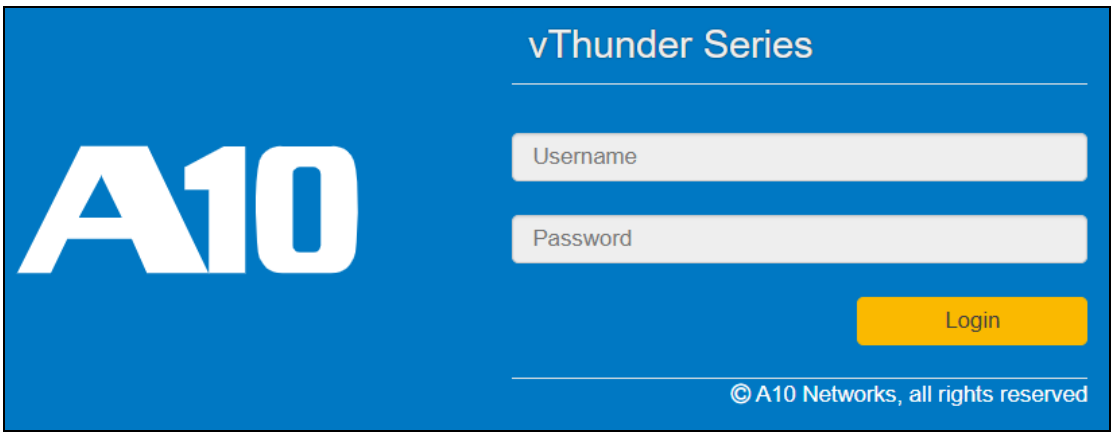
A screen resolution of at least 1024x768 is recommended.

1. Open a supported Web browser.
2. In the URL field, enter the IP address of the ACOS device's management interface.
3. If the browser displays a certificate warning, select the option to continue to the server (the ACOS device).

NOTE: To prevent the certificate warning from appearing in the future, you can install a certificate signed by a Certificate Authority. For more information, see Replace Web Certificate.

A log in page is displayed in the Figure 3. The name and appearance of the dialog depends on the browser you are using and the specific device which you are trying to access.

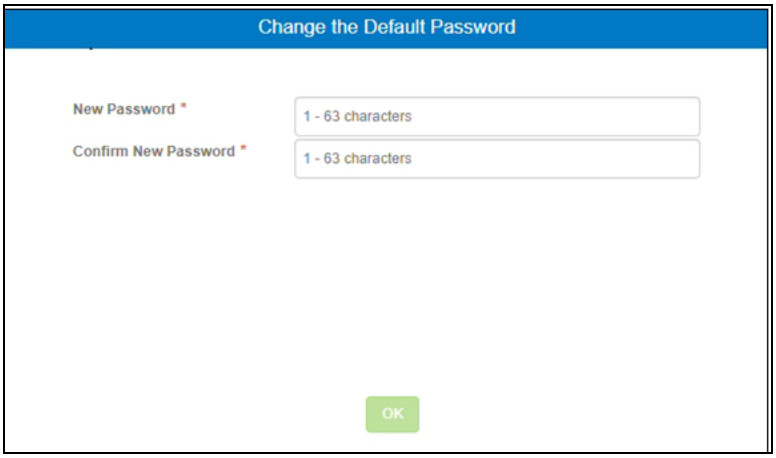
Figure 3 : Example GUI Login Dialog



4. Enter your admin username and password and click **Login**.

5. The Change the Default Password page is displayed as shown in Figure 4.

Figure 4 : Change the Default Password



6. Enter the new password as per the Default Password-Policy Complexity Criteria, re-enter the new password for verification, and click **OK**.

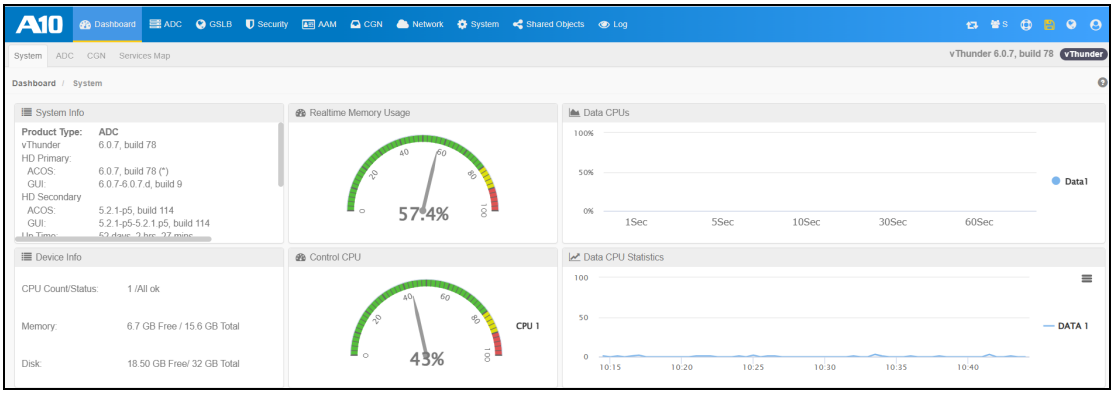
NOTE: You will only be prompted to change the default password when you log in for the first time on a new device or if the device is reset using the `system-reset` command. Starting with ACOS 6.0.0, any ACOS release that supports enforcing default password change will not prompt you to change the password again.
The default password must not be set back as an admin password.

The Dashboard (As in the Figure 5) appears, showing at-a-glance information for your ACOS device.

You can access this page again at any time while using the GUI by selecting **Dashboard**.

NOTE: For a detailed information about this option and all other GUI screens, see the latest version of the **GUI Online Help**.

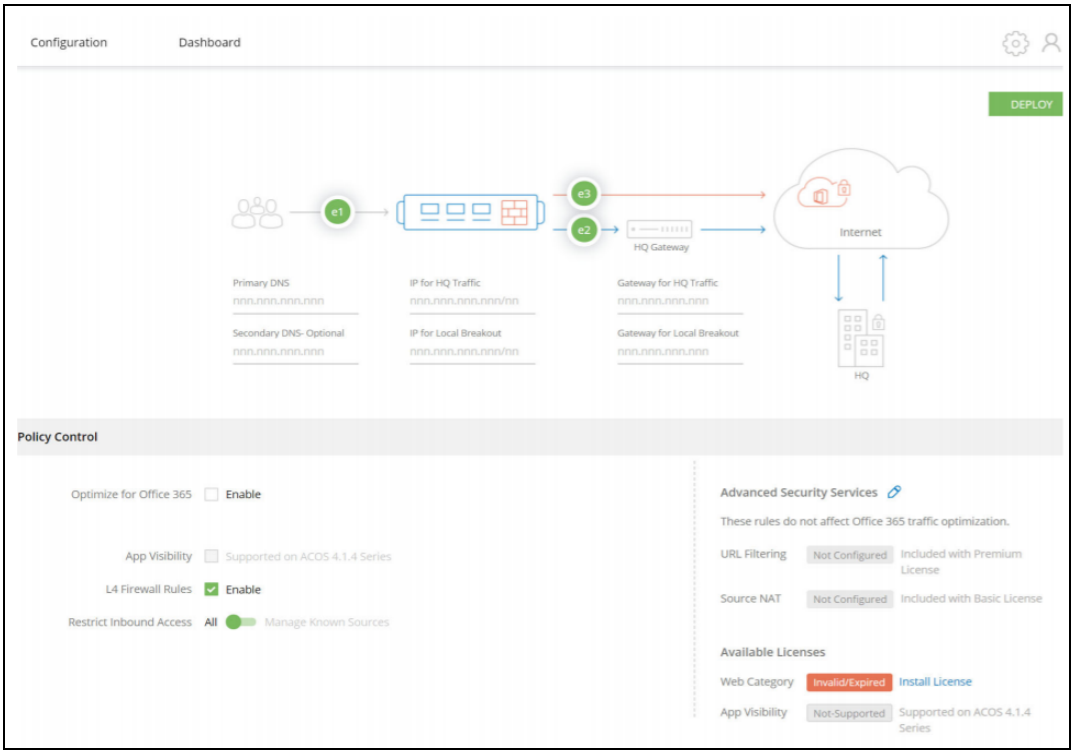
Figure 5 : Dashboard



NOTE: GUI management sessions are not automatically terminated when you close the browser window. The session remains in effect until it times out. To immediately terminate a GUI session, click the Sign Out icon in the menu bar.

7. If the ACOS is a CPE device, the user will redirect to the CPE web page instead of the ACOS Dashboard (Figure 5).
   For more information about the CPE web page, see the latest version of the **GUI Online Help (System > APP Template)**.

Figure 6 : Dashboard



Default Password-Policy Complexity Criteria

As per the default password-policy complexity, the following criteria should be met:

- The password length should be at least nine characters.
- The password should contain at least one number, an uppercase letter (English), a lowercase letter (English), and a special character.
- The password should have at least one letter or number different from the previous password.
- The password should not contain its corresponding username with the same capitalization of letters.
- The password should not contain consecutive repeated characters of the same letter or number with the same capitalization of letters.
- The password should not contain the sequential row keyboard input of four letters or numbers with the same capitalization of letters.

For more information, see *Management Access and Security Guide*.

Console Restart

Use the **clear console** command to terminate the current login process and start a new one:

```
ACOS(config)# clear console
```

Use this command if you notice that SSH and data traffic still appear to be operational, though the console session is hung. This may be caused if rimacli is in a hung state. rimacli is the process that is automatically invoked when an admin logs into the ACOS device through an interface address. This process provides admins access to the Command Line Interface (CLI) to be able to issue and save commands to configure the system.

To resolve the issue of the hung console due to an underlying hung `rimacli` process, use the **clear console** command. After the hung login process is terminated, the console will revert to the login prompt.

ADC and CGN on Same Device

ACOS supports both ADC and CGNv6 configuration. Either one may be configured in any partition, but they may not be configured together in the same partition.

When you login to the device using the CLI, all ADC and CGN options are available by default in the shared partition (see the *Configuration Application Delivery Partitions* guide for more information about partitions). When an ADC object is configured (for example, an SLB server), all CGN options are automatically disabled until all ADC objects are removed. Similarly, if a CGN object is configured, then all ADC options are disabled until the CGN objects are all removed.

When an L3V partition is created, the behavior is the same as the shared partition. All ADC and CGN objects are available until either one is configured.

While creating partitions, you can use the `application-type` command to explicitly specify the type of objects that are available in any partition, before any objects are configured. For example, the following command creates an L3V partition called “PART-ADC” which will only have ADC options available:

```
ACOS(config)# partition PART-ADC id 1 application-type adc
```

The behavior in the GUI is slightly different. The GUI menu options are static and will not make ADC or CGN objects unavailable based on the existing configuration. Therefore, it is up to the user to maintain records about which types of objects are configured in each partition. If an attempt is made to use the GUI to configure a CGN object in a partition that already contains ADC objects, the user will see an error message.

Upgrade ACOS Image

The Thunder device is provided with pre-installed ACOS software along with the purchased license. When you power ON the device, it boots up with the pre-installed software. To access the new features, security patches, and software fixes as they become available, you must upgrade the ACOS software.

The upgrade process involves selecting the upgrade method, defining the target partition, and specifying additional options based on your environment:

1. Select the upgrade method:
   - Graphical User Interface (**gui**)
   - Hard Disk (**hd**)
2. Define the target partition:
   - Primary partition (**pri**)
   - Secondary partition (**sec**)
3. Specify additional options:
   - Install an image from a local directory (**local** *image-name*)
   - Display upgrade progress (**show-percentage**)
   - Specify the source IP (**source-ip-address** *<ip-address>*)
   - Use the management port for the upgrade (**use-mgmt-port**)
   - Retrieve the upgrade image from a remote source (**url**)

     The supported protocols for remote upgrades are:
     - Trivial File Transfer Protocol (tftp://)
     - File Transfer Protocol (ftp://)
     - Secure Copy Protocol (scp://)
     - Hypertext Transfer Protocol (http://)

- Secure HTTP (https://)
- Secure FTP (sftp://)

After upgrading the ACOS software, enable the Multi-Factor Authentication in your ACOS device.

For release-specific upgrade instructions, see the *Release Notes*.

Multi-Factor Authentication

ACOS supports Multi-Factor Authentication (MFA) mechanism for upgrading ACOS software image. This enhances security by ensuring that only authorized users can perform upgrades.

If a multi-factor authentication is set up, then ACOS can automatically detect whether the authentication server enforces an additional verification step. This feature applies to all A10 products running ACOS.

Supported MFA

ACOS currently supports only Cisco Duo MFA for SCP-based upgrades.

Supported Duo MFA Authentication Methods

Duo MFA provides three authentication methods for SCP-based ACOS upgrades:

- Direct Passcode: A 6-digit passcode is generated in the Duo mobile app.
- Duo Push Notification: A push notification is sent to the Duo mobile app for approval.
- SMS Passcode: A passcode is sent to the registered phone number via SMS.

NOTE: Some authentication methods may not be available depending on the Duo configuration of the remote server.

Pre-requisites

Before starting an SCP-based upgrade with Duo MFA, ensure the following:

- Set up Duo Unix on the authentication server. For more information, see Duo Unix Get Started and Enable Password Login.

- Perform an SSH/SCP login test to confirm whether the authentication method is configured for direct passcodes, push notifications, or SMS passcodes.

Enabling Duo MFA for SCP-based Upgrades

To enable Duo MFA for SCP-based Upgrades, perform the following steps:

1. Initiate the upgrade process, using the following command.

```
ACOS(config)# upgrade hd pri use-mgmt-port scp://root@path_to_ACOS_
image.upg
Password []?
```

   ACOS prompts you to enter a password.

2. Enter the password for SCP authentication.
3. Enter **yes** to reboot the system immediately after the upgrade.

```
Do you want to reboot the system after the upgrade?[yes/no]: yes
Getting upgrade package ...
```

   The device attempts to download the upgrade package from the SCP server.

4. If Duo Unix is enabled, ACOS detects the additional authentication requirement and displays the Duo MFA prompt:

```
Duo two-factor login for root
Enter a passcode or select one of these options:
1. Duo Push to iOS
2. SMS passcodes to XXX-XXX-6097
```

   At this stage, proceed with Direct Passcode, Duo Push Notification, or SMS Passcode Authentication.

   Authenticate Using Direct Passcode

   a. Open the Duo mobile app.

   b. Enter the 6-digit passcode generated in the app (this code refreshes periodically).

```
Passcode or option (1-2): XXXXXX
```

   Option 1: Authenticate Using Duo Push Notification

a. Select option 1.

```
Passcode or option (1-2): 1
```

A push notification is sent to your configured Duo mobile app.

b. Approve the notification on your mobile device.

Option 2: Authenticate Using SMS Passcode

a. Select option 2.

```
Passcode or option (1-2): 2
```

A one-time passcode via SMS is sent on your registered mobile number.

b. Enter the received passcode when prompted again.

```
Duo two-factor login for root

Enter a passcode or select one of the following options:

 1. Duo Push to iOS
 2. SMS passcodes to XXX-XXX-6097 (next code starts with: 1)

Passcode or option (1-2): 656155
```

5. Once the authentication is successful, ACOS proceeds with the upgrade.

```
Authentication successful!
.................
Done (0 minutes 27 seconds)
Decrypting upgrade package...
```

Basic System Parameters

This chapter describes the basic system parameters and provides CLI and GUI steps for configuring them.

The following topics are covered:

NOTE:

- The only basic parameters that you are required to configure are date/time settings. Configuring the other parameters is optional.
- This chapter does not describe how to access the serial console interface. For that information, see the installation guide for your specific ACOC device.

Set System Time and Date

This section provides instructions for setting the time and date on your system.

The following topics are covered:

Set the Clock

The time and date are not set at the factory. Therefore, you must manually set them or configure NTP (see Setting the NTP Server).

The following topics are covered:

Configure Using GUI

To set the clock using the GUI:

1. Navigate to **System > Settings > Time**.
2. In the Clock section, you can:
   - Set the date and time. Click in the Date/Time field to select the date from the pop-up calendar.
   - Set the timezone.
   - Select whether or not you want to enable or disable daylight savings time.

NOTE: When you change the ACOS timezone, the statistical database is cleared. This database contains general system statistics (performance, CPU, memory, and disk utilization) and SLB statistics.

By default, daylight savings is enabled on the ACOS device. The ACOS device automatically adjusts the time for Daylight Savings Time based on the timezone you select. The UTC time standard does not observe daylight savings time.

3. Click **OK** to save your changes.

Configure Using CLI

To set the clock using the CLI:

1. From Privileged EXEC mode, use the **clock set** command to set the time. This command must be run in Privileged EXEC mode.

   The following example sets the time to 10:31 AM on February 13, 2015:

   ```
   ACOS# clock set 10:31:00 February 13 2015
   ```

   The following example sets the time to 7:15 PM and 33 seconds on December 17, 2015 (for times beyond 12:00 PM, use the 24-hour notation):

   ```
   ACOS# clock set 19:15:33 December 17 2015
   ```

2. Enter Global configuration mode to use the **timezone** command to set the time zone.

   The following example sets the timezone to America/Los_Angeles:

   ```
   ACOS# configure
   ACOS(config)# timezone America/Los_Angeles
   ```

3. To verify your settings, use the **show clock** command:

   ```
   ACOS# show clock
   .08:43:07 PDT Thu Oct 2 2015
   ACOS#
   ```

If you manually set the time or the time comes from the NTP configuration on the server, there will not be an extra dot (.) in the display when you use the `show clock`

command. If, however, the NTP configuration does not work properly, the time displays an extra dot as shown in the example above. An extra dot also displays if there is neither an NTP configuration nor a manual configuration.

Setting the NTP Interface

NTP listens on the management port, data port, and virtual Ethernet (VE) interface by default.

Setting the NTP Server

The following topics are covered:

Configure Using GUI

To configure an NTP server using the GUI:

1. Navigate to **System > Settings > Time**.
2. In the NTP Servers section:
   - Configure an NTP hos with either an IP or hostname.
   - Select **Enable** in the status field to enable the server.
   - To designate this server as the preferred server, select the **Preferred** checkbox.

     This option allows you to specify a preferred NTP server. You now direct ACOS to use the prioritized NTP server by default and rely on additional NTP servers as backups if the preferred NTP server becomes unavailable.

NOTE: It is recommended that you enable the **Preferred** option for a single NTP server only. If the preference is selected for more than one NTP server, the prioritized NTP server is determined by an internal calculation.

3. Click **OK** to save your changes. The new server is added to the NTP Server table below the configuration fields.

Configure Using CLI

To configure a preferred NTP server using the CLI, use the **ntp server** command from Global Configuration mode, then use the **prefer** command to make this the preferred server:

```
ACOS(config)# ntp server 216.171.124.36
ACOS(config-ntpsvr:216.171.124.36)# prefer
```

Use the **show running-config** command to verify your configuration:

```
ACOS(config-ipv4-serveraddr:216.171.124.36)# show run | begin ntp server
ntp server 207.69.131.204
!
ntp server 207.69.131.205
!
ntp server 216.171.124.36
  prefer
!
...
```

Setting the NTP Server Authentication

NTP server authentication keys are stored using a special A10 Networks encryption algorithm to conceal the clear-text form of the authentication key. You can add the ID numbers of encrypted authentication keys to a list of trusted keys, and apply the trusted keys to one or more NTP servers.

An NTP server can operate in either an authentication or a non-authentication mode. If an authentication key is specified in the client's NTP request, the NTP server appends a message authentication code (MAC) to the response packet header, using the authentication key. The NTP client compares the MAC of the NTP server against the specified authentication key and accepts the packet from the NTP server if the MAC matches.

The following topics are covered:

Configure NTP Server Authentication

1. Create a list of authentication keys, which are stored on the ACOS device.
2. Add the identification numbers of one or more authentication keys to the list of trusted keys. Only keys from the trusted key list are valid for NTP server authentication.
3. Configure an NTP server and apply a trusted authentication key.

NOTE:

- The NTP server and NTP client must reference the same authentication key ID number. If the NTP server and NTP client are configured with different authentication key ID numbers, NTP server authentication will always fail.
- Currently, aXAPI is not supported for SHA and SHA1 authentication of NTP servers.

Configure Using GUI

To set up NTP server authentication in the GUI:

1. Navigate to **System > Settings > Time**.
2. In the NTP Keys section:
   - Enter a Key ID.
   - Configure the encryption type and ASCII or Hex key parameters.
3. Click **OK** to save your configuration.

You can add multiple trusted keys using this screen. After you create the keys, you can then configure an NTP server in the NTP section (see Setting the NTP Server), then select one of the trusted authentication keys from the drop-down menu to assign to the NTP server. Keys created here can be used while creating NTP servers.

Configure Using CLI

The example in this section shows how to configure NTP server authentication.

1. Create two authentication keys (13579 and 24680). Both keys use MD5 encryption and ASCII key strings:

```
ACOS(config)# ntp auth-key 13579 M ascii XxEnc192
ACOS(config)# ntp auth-key 24680 M ascii Vke1324as
```

2. Add keys 13579 and 24680 to the list of trusted keys.

```
ACOS(config)# ntp trusted-key 13579
ACOS(config)# ntp trusted-key 24680
```

3. Configure the NTP server at 207.69.131.204 to use trusted key 13579.

```
ACOS(config)# ntp server 207.69.131.204
AOCS(config-ipv4-serveraddr:207.69.131.204)# key 13579
```

4. You can verify the NTP server and authentication key configuration with the **show running-config** command. The following example includes an output modifier to display only NTP-related configuration:

```
ACOS(config)# show running-config | include ntp
ntp auth-key 13579 M ascii encrypted
zIJptJHuaQaw/5o10esBTDwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
ntp auth-key 24680 M ascii encrypted
FSNiuf10Dtzc4aY0tk2J4DwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
ntp trusted-key 13579
ntp trusted-key 24680
ntp server 207.69.131.204
ntp server 207.69.131.205
ntp server 216.171.124.36
ACOS(config)#
```

Set Hostname and DNS Parameters

The following topics are covered:

NOTE: Do not use a period (.) in the hostname. The ACOS device will interpret text that appears after the period as the DNS suffix instead of the DNS suffix you configure.

Configure Using GUI

To use the GUI to set the hostname and DNS parameters:

1. Navigate to **System > Settings > DNS**.
2. On the Configure DNS screen, you can specify:
   - Host name (required)
   - Domain suffix (domain name to which the host belongs)
   - Primary IP
   - Secondary IP
3. Click **Update DNS** to store your changes.

Configure Using CLI

This section provides an example of how to use the CLI to change the name and DNS parameters on your device. You must be in the global configuration mode:

1. To begin using the CLI, make sure you are in the Global Configuration mode.
2. Use the **hostname** command to change the hostname to “ACOS-SLB2”:

```
ACOS(config)# hostname ACOS-SLB2
ACOS-SLB2(config)#
```

   After you enter this command, note that the command prompt is changed to reflect the new hostname.

   NOTE: The “>” or “#” character and characters in parentheses before “#” indicate the CLI level you are on and are not part of the hostname.

3. Use the **ip dns suffix** command to set the default domain name (DNS suffix) for

host names on the ACOS device. The suffix “a10networks.com” is used in this example:

```
ACOS(config)# ip dns suffix a10networks.com
```

4. Use the **ip dns primary** command to set the primary DNS server (10.10.128.101 in this example) for resolving DNS requests:

```
ACOS(config)# ip dns primary 10.10.128.101
```

5. Use the **ip dns secondary** command to set the secondary DNS server (10.10.128.102 in this example) for resolving DNS requests:

```
ACOS(config)# ip dns secondary 10.10.128.102
```

6. Use the **show running-config** command to view your configuration:

```
ACOS-SLB2(config)# show running-config | include dns
ip dns primary 10.10.128.101
ip dns secondary 10.10.128.102
ip dns suffix a10networks.com
ACOS-SLB2(config)#
```

Set Up CLI Banners

The CLI displays banner messages when you log onto the CLI. By default, the messages shown in bold type in the following example are displayed:

```
login as: admin

Welcome to ACOS
Using keyboard-interactive authentication.
Password:
Last login: Thu Feb  7 13:44:32 2008 from 192.168.1.144

[type ? for help]
```

You can format banner text as a single line or multiple lines.

If you configure a banner message that occupies multiple lines, you must specify the end marker that indicates the end of the last line. The end marker is a simple string

up to 2-characters long, each of the which must be an ASCII character from the following range: 0x21-0x7e.

The multi-line banner text starts from the first line and ends at the marker. If the end marker is on a new line by itself, the last line of the banner text will be empty. If you do not want the last line to be empty, put the end marker at the end of the last non-empty line.

The following topics are covered:

Configure Using GUI

To set the CLI banners using the GUI:

1. Navigate to **System > Settings > Terminal**.
2. On the Terminal page:
   - Configure the **Login** banner.
   - Configure the **EXEC** banner.
3. Click **OK** to save your changes.

Configure Using CLI

This section describes how to change the CLI banners using CLI commands.

1. Use the **`banner login`** command to set the login banner. This is the banner that will be seen after you enter the admin username and password. This example sets the banner to “welcome to login mode:”

```
ACOS(config)# banner login “welcome to login mode”
```

2. Use the **`banner exec`** command to set the exec banner to “welcome to exec mode.” This banner is displayed after you enter the admin password:

```
ACOS(config)# banner login “welcome to exec mode”
```

To use blank spaces within the banner, enclose the entire banner string with double quotation marks.

Replace Web Certificate

You can replace the web certificate shipped with the ACOS device. Replacing the certificate with a CA-signed certificate prevents the certificate warning from being displayed by your browser when you log in to the GUI.

The following topics are covered:

Configure Using GUI

1. Select **Config Mode** > **System** > **Settings** > **Web Certificate**.
2. Select the location(s) of the certificate and key files to be imported:
   - Local – The file is on the PC you are using to run the GUI, or is on another PC or server in the local network. Go to step 3.
   - Remote – The file is on a remote server. Go to step 5.
   - Likewise, to import certificate chains, select the location.
3. Click Browse and navigate to the location of the class list.
4. Click Open. The path and file name appear in the Source field. Go to step 11.
5. To use the management interface as the source interface for the connection to the remote device, select Use Management Port. Otherwise, the ACOS device will attempt to reach the remote server through a data interface.
6. Select the file transfer protocol: FTP, TFTP, RCP, SCP, or SFTP.
7. In the Host field, enter the directory path and file name.
8. Specify the Key Source.
9. If needed, change the protocol port number n the port field. By default, the default port number for the selected file transfer protocol is used.

10. In the User and Password fields, enter the username and password required for access to the remote server.
11. Click OK.

Configure Using CLI

Use the following command at the global configuration level of the CLI:

```
ACOS(config)# web-service secure wipe
ACOS(config)# web-service secure certificate load [use-mgmt-port]
tftp/ftp/scp/sftp
ACOS(config)# web-service secure private-key load [use-mgmt-port]
tftp/ftp/scp/sftp
```

Increased I/O Buffer Support

On some higher-end models only, you can enable the **big-buff-pool** option to expand support from 4 million to 8 million buffers and increase the buffer index from 22 to 24 bits.

NOTE: Some models may require 96 GB of memory to support this feature. Please check that your system meets this requirement by using the **show memory system** command and checking the output.

Enter the following command to enable more I/O buffers for the system:

```
ACOS(config)# big-buff-pool
```

Use the **no** version of the command to remove a larger buffer for the system:

```
ACOS(config)# no big-buff-pool
This will modify your boot profile to disable big I/O buffer pool.
It will take effect starting from the next reboot.
Please confirm: You want to disable the big I/O buffer pool(N/Y)?:
```

Use the **show system platform buffer-stats** command to view statistics for the I/O buffer pool:

```
ACOS(config)# show system platform buffer-stats
Buffers available in various states/threads...
```

```
-------------------------------------------------
Thread       Cache        App    AppQueue       Misc
-------------------------------------------------
Q0          136034          0           0          0
Q1          127873          0           0          0
Q2          154496          0           0          0
Q3          154515          0           0          0
Q4          154511          0           0          0
Q5          153147          0           0          0
Q6          154511          0           0          0
Q7          153147          0           0          0
Q8          153829          0           0          0
Q9          153147          0           0          0
Q10         154511          0           0          0
Q11         153147          0           0          0
Approximate # buffers in App      0
Approximate # buffers in App_cp   0
Approximate # buffers in Cache_cp 1024
Approximate # buffers in Cache    1802868
Approximate # buffers in Queue    0
Approximate # buffers in misc     0
Approximate # buffers in dfree    745472
Approximate # buffers free        2391436
Approximate # buffers avail in HW 1639073
# Capsules in per thread pool:
          t00 t01 t02 t03 t04 t05
  FPGA0:   9  11  11  11  11  11
  FPGA1:  21  15  15  15  15  15
  FPGA2:  10  19  19  19  19  19
  FPGA3:  21  22  22  22  22  22
          t06 t07 t08 t09 t10 t11
  FPGA0:   5  16  16  16  16  16
  FPGA1:  17  17  17  17  17  17
  FPGA2:  12  12  11  11  11  11
  FPGA3:  21  22  22  22  22  22
Approximate # of operations on Global buffer pool:
             GetsD0     PutsD0     GetsD1     PutsD1
  FPGA0: 0x00000016 0x00000052 0x00000000 0x00000037
  FPGA1: 0x00000000 0x00000033 0x00000000 0x00000032
  FPGA2: 0x00000000 0x0000003d 0x00000016 0x0000004a
```

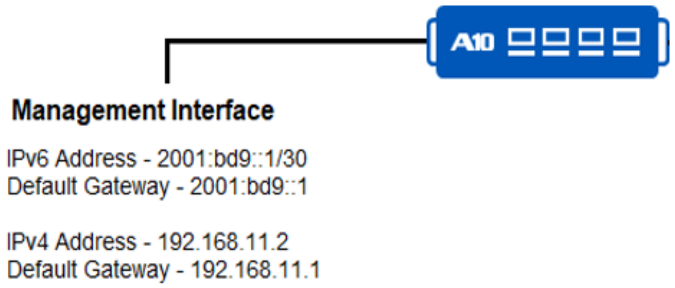
```
  FPGA3: 0x00000000 0x00000010 0x00000000 0x00000013
Approximate # buffers in total    4194304
```

Single Management Interface

The management interface (MGMT) is an Ethernet interface to which you can assign a single IPv4 address and a single IPv6 address. The management interface is separate from the Ethernet data interfaces.

The following Figure 7 shows an example of the management interface on a Thunder Series device.

Figure 7 : ACOS Deployment Example – Single Management Interface



By default, the ACOS device attempts to use a route from the main route table for management connections originated on the ACOS device. You can enable the ACOS device to use the management route table to initiate management connections instead. (For information, see Source Interface for Management Traffic.)

NOTE: ACOS allows the usage of the same IP address for both the mgmt IP address and the NAT pool address. However, in Layer 2 (transparent) deployments, if you do configure the same address in both places, and later delete one of the addresses, a reload is required for the changes to take effect.

The following topics are covered:

Configure Using CLI

The following commands configure access to the management interface:

1. Use the **interface management** command to enter the interface management mode and to continue the management interface configuration.

```
ACOS(config)# interface management
```

2. Use the **ipv6** commands to configure IPv6 access.

```
ACOS(config-if:management)# ipv6 address 2001:db9::1/30
ACOS(config-if:management)# ipv6 default-gateway 2001:db9::1
```

3. Use the **ip** commands to configure IPv4 access.

```
ACOS(config-if:management)# ip address 192.168.11.2 /21
ACOS(config-if:management)# ip default-gateway 192.168.11.1
```

4. Use the **show interfaces management** command to verify the configuration.

```
ACOS(config-if:management)# show interfaces management
Management 0 is up, line protocol is up.
 Hardware is 10Gig, Address is 001f.a044.7167
 Internet address is 192.168.11.2, Subnet mask is 255.255.255.0
 Internet V6 address is 2001:db9::1/30
 Configured Speed auto, Actual 1000, Configured Duplex auto, Actual fdx
 Flow Control is disabled, IP MTU is 1500 bytes
 781 packets input,  58808 bytes
 Received 33 broadcasts,  Received 66 multicasts,  Received 662
unicasts
 0 input errors,  0 CRC  0 frame
 0 runts  0 giants
 924 packets output 3549 bytes
 Transmitted 157 broadcasts  7 multicasts  770 unicasts
 0 output errors  0 collisions
```

Configure Using GUI

This section describes how to use the GUI to configure a single management interface.

NOTE: Unless you have already configured an IP interface, navigate to the default IP address: http://172.31.31.31.

1. Navigate to **Network > Interfaces > Management**.
2. On the Management page:
   - Configure the duplexity of the management interface.
   - Configure the speed of the management interface.

     NOTE: The available selection of speeds in this field depends on the device you are configuring. Devices with no 1G interface, for example, will not have a 1G option in this field.

   - Configure the IPv4, IPv6, and LLDP settings.
3. Click **Configure** to save your changes.

Dual Management Interface

The dual management interfaces enhance reliability. They are supported only on the Thunder 8665S platform. Each port can be configured separately and operates independently of the other.

The second management interface (management2) is an Ethernet interface to which you can assign a single IPv4 address and a single IPv6 address.

NOTE: The second management interface is referred to as management2 or mgmt2.

The following Figure 8 shows an example of the management2 interface on an Thunder Series device.

Figure 8 : ACOS Deployment Example – Dual Management Interfaces

By default, the ACOS device attempts to use a route from the main route table for management connections originated on the ACOS device. You can enable the ACOS device to use the management route table to initiate management connections instead. (For information, see Source Interface for Management Traffic.)

NOTE: The `dac-link-training-enable` command enables the Direct Attach Copper (DAC) cable link training to establish a link with the interface. This command is recommended only when the ACOS device is connected to the 400G DAC Copper cable and must interoperate with the Dell Fabric switch. It is not required for other switches.

The following topics are covered:

Configure Using CLI

The following commands configure access to the second management interface:

1. Use the **`interface management2`** command to enter the interface management mode and to continue the management interface configuration.

```
ACOS(config)# interface management2
```

2. Use the **`ipv6`** commands to configure IPv6 access.

```
ACOS(config-if:management2)# ipv6 address 2001:db8::2/32
ACOS(config-if:management2)# ipv6 default-gateway 2001:db8::1
```

3. Use the **`ip`** commands to configure IPv4 access.

```
ACOS(config-if:management2)# ip address 192.168.10.2 /24
ACOS(config-if:management2)# ip default-gateway 192.168.10.1
```

NOTE: The `duplexity`, `flow control`, `speed`, `sampling-enable`, `bcast-rate-limit`, and `lldp` commands are unavailable in both the management interface and the second management interface mode.

4. Use the **`show interfaces management2`** command to verify the configuration:

```
ACOS(config-if:management2)# show interfaces management2
Management 2 is up, line protocol is up
 Hardware is 10Gig, Address is 001f.a044.7166
 Internet address is 192.168.10.2, Subnet mask is 255.255.255.0
 Internet V6 address is 2001:db8::2/32
 IPv6 link-local address is fe80::200:ff:fe00:0/64
 Configured Speed N/A, Actual 1000, Configured Duplex N/A, Actual Full
 Flow Control is disabled,IP MTU is 1500 bytes
 23922 packets input,  2448254 bytes
 Received 21648 broadcasts,  Received 602 multicasts,  Received 1672
unicasts
 0 input errors,  0 CRC  0 frame
 0 runts  0 giants
 1690 packets output  214668 bytes
 Transmitted 12 broadcasts  24 multicasts  1654 unicasts
 0 output errors  0 collisions
```

Limitations

- The following features or commands are not supported for the second management - 'management2' interface:
  - Logging
  - SNMP
  - Licensing
  - GSLB
  - Event Notification
  - Web Services

- Visibility
- LLDP
- Enable or disable Management services such as ping, telnet, traceroute, and ssh
- Network Time Protocol (NTP)
- Management interface as the source interface for the connection to the remote device (use-mgmt-port)
- Management interface as the source interface for the automated traffic (ip control-apps-use-mgmt-port)

- The dual management interface can be configured only through CLI.
- The **`show management`** command does not support the second management interface (mgmt2), on TH8665 device.
- `use-mgmt-port` support across all applications (For example, ping/ssh/telnet/import/export and so on).

Disable Deletion of Referenced Objects Using CLI

This section provides the instructions for disabling the deletion of referenced Server Load Balancer (SLB) objects.

The following topics are covered:

Disable Deletion Using CLI

To disable the deletion of referenced objects using CLI:

```
ACOS(config)# system config-mgmt delete-referenced-tagged-objects disable
```

The **`system config-mgmt`** command provides **`delete-referenced-tagged-objects`** option for automatic and manual deletion.

- When this option is enabled and if an attempt is made to delete, the referenced objects are deleted directly without any prompt message, which is the legacy and default behaviour. This applies to SLB real server, service-group, virtual server, and

SLB template within Shared and L3V partition.

- When this option is disabled and if an attempt is made to delete, a message is displayed indicating that the object has tagged references that must be removed first. These references must be manually deleted before the object can be successfully removed. This applies to SLB real server, service-group, virtual server, and SLB template within Shared and L3V partition.

The following example shows an attempt to delete a referenced real server named 's1' in the Shared partition:

```
ACOS(config)# system config-mgmt delete-referenced-tagged-objects disable
ACOS(config)# no slb server s1
This object has other objects referencing this. Please remove references
first.
```

For more information about the configuration options and commands, see Command Line Interface Reference.

System Security Settings

This chapter describes the system security settings in the ACOS device device.

The following topics are covered:

Set Control Plane Security

ACOS supports the system-level configurations to improve the control plane security. These are applied to all control plane packets, and it is not partition specific.

The following security features are supported:

- **Broadcast Ping Protection** - Prevents replies to ICMP echo requests sent to broadcast addresses.
- **ICMP Redirect Control** - Disables sending ICMP redirects messages to prevent traffic hijacking.
- **Reverse Path Filtering (RPF)** - Enables verifying that the source IP address of an incoming packet is reachable through the same interface on which the packet was received. This supports both IPv4 and IPv6, helping to prevent IP spoofing. The drop counters are maintained for both IPv4 and IPv6.
- **ICMP Unreachable Filtering** - Drops ICMP unreachable messages.
- **ACL Filter Support** - Extends ACL support for filtering specific ICMP types on management interfaces.

CLI Configuration

This command applies at the system level and impacts all control plane packets on the ACOS device. It is not specific to any partition.

- To disable the sending of IPv4 ICMP destination unreachable messages, use the following command:

```
ACOS(config)# system ip icmp-unreachable-disable
```

- To disable the sending of IPv6 ICMP destination unreachable messages, use the following command:

```
ACOS(config)# system ipv6 icmpv6-unreachable-disable
```

- To disable the sending of IPv4 ICMP redirect messages, use the following command:

```
ACOS(config)# system ip icmp-redirect-disable
```

- To disable the sending of IPv6 ICMP redirect messages, use the following command:

```
ACOS(config)# system ipv6 icmpv6-redirect-disable
```

- To enable RPF in strict mode for IPv4 source address, use the following command:

```
ACOS(config)# system ip rpf-check-enable
```

- To enable RPF in strict mode for IPv6 source address, use the following command:

```
ACOS(config)# system ipv6 rpf-check-enable
```

Set Source-Routed Packet Drop

Source-routed packets allow you to specify the exact path a route must take through the network. ACOS supports dropping IPv4 and IPv6 source-routed packets at the system-level for both control and data plane packets. It enhances the system-level security by preventing IP spoofing, traffic redirection, and packet sniffing.

Source-routed packets are dropped at the kernel level, and drop counters are maintained for both IPv4 and IPv6. It applies only to Layer 3 forwarded traffic.

CLI Configuration

The following commands enable dropping source-routed packets:

- To drop the IPv4 source-routed packets, use the following command:

```
ACOS(config)# system ip source-route-pkt-drop-enable
```

- To drop the IPv6 source-routed packets, use the following command:

```
ACOS(config)# system ipv6 source-route-pkt-drop-enable
```

Limitation

The following is the limitation:

It impacts only the Layer 3 forwarded traffic.

Set Up SSH Access

ACOS devices use Secure Shell (SSH) to securely access and manage over an unprotected network.

To improve ACOS security and lower the attack surface, you can modify the default SSH port and disable the following SSH functionalities:

- **SSH Agent Forwarding** - This enables an SSH client to use credentials saved in a local SSH agent to authenticate a remote SSH server when connecting from a different system. This causes security risks such as credential theft and lateral movement.
- **SSH TCP Port Forwarding** - This can be exploited by attackers to hide unauthorized communications or exfiltrate stolen data from the target network.
- **SSH X11 Forwarding** - This allows displaying local and running graphical applications on a remote server. Enabling it increases the attack surface and security vulnerabilities.

NOTE: You can use the `no` command to enable agent forwarding, TCP port forwarding, and X11 forwarding.

- **Modify Default SSH Port** - This helps to prevent brute-force attempts and reduce automated attacks. The available port numbers are 22 and the range of 1025-64999.

NOTE: After changing the SSH port, you must use the new port to connect to the remote host.

CLI Configuration

- To disable the SSH agent forwarding, use the following command:

```
ACOS(config)# ssh-config disable-agent-forwarding
```

- To disable SSH TCP port forwarding, use the following command:

```
ACOS(config)# sshd-config disable-tcp-forwarding
```

- To disable SSH X11 forwarding, use the following command:

```
ACOS(config)# sshd-config disable-x11-forwarding
```

- To disable the SSH port number, use the following command:

```
ACOS(config)# sshd-config tcp-port
```

Disk Encryption

Disk Encryption is a security technique that is used to protect data stored on an ACOS device's hard drive or other storage devices, referred to as data-at-rest. It uses encryption algorithms to convert readable data into an unreadable format known as *ciphertext*. This makes the data inaccessible to unauthorized users without a valid passphrase.

ACOS generates logs, core files, debug files, cache, and traces that may contain sensitive data. If the device that contains data is plugged in or mounted on another

system, it is possible to gain access to all sensitive data. To prevent this, the disk containing the data must be encrypted.

The disk encryption feature is supported on the following devices:

- Thunder 3745
- Thunder 3350
- Thunder 5960
- Thunder 1060

To configure this feature on any of the above devices, you need to obtain the disk encryption license. For more information, reach out to the *A10 Sales team*.

NOTE: Once the disk is encrypted, the process cannot be reversed, and the data cannot be decrypted.

Prerequisites

Before enabling disk encryption, ensure the device is in maintenance window and not:

- Engaged in processing traffic
- Undergoing a reboot, upgrade, or backup process.

The following topics are covered:

CLI Configuration

To configure disk encryption, perform the following steps:

1. Check the disk encryption status using the following command:

```
ACOS(config)#show system disk-encryption status
Disk encryption status:(Unsupported)
Configured:No
Encrypted:No
```

An "`Unsupported`" status indicates that the disk encryption license is not applied.

2. Import the license provided for disk encryption using the following command:

```
ACOS#import glm-license disk_encryption_lic use-mgmt-port <license_
filepath>
```

3. Check the available ciphers for disk encryption using the following command:

```
ACOS(config)#system enable-disk-encryption cipher ?
aes      cipher aes
serpent  cipher serpent
twofish  cipher twofish
```

4. Encrypt the disk using the following command syntax:

```
ACOS(config)#system enable-disk-encryption cipher {aes | serpent |
twofish} {passphrase <passphrase_string> | passphrase-base64 <base64_
format_passphrase>}
```

NOTE: Back up the passphrase securely as it cannot be recovered if lost.

5. Execute the following disk encryption command:

NOTE: The passphrase must be between 16 and 64 characters.

```
ACOS(config)#system enable-disk-encryption cipher aes passphrase
<plain_passphrase_string>
Creating backup.
It will take some time...
.....................................................................
.............................
.....................................................................
.............................
.....................................................................
.............
Disk encryption is enabled
Reboot the system to encrypt the disk
```

6. Check the disk encryption status using the following command:

```
ACOS(config)#show system disk-encryption status
Disk encryption status:
Configured:Yes
```

```
Encrypted:No
```

"`Configured:Yes`" indicates that the system has applied disk encryption, and it will complete after a reboot.

7. To complete the encryption process, reboot the device.
8. Check the disk encryption status after the reboot, using the following command:

```
ACOS(config)#show system disk-encryption status
Disk encryption status:
Configured:Yes
Encrypted:Yes
```

To reconfigure the disk encryption (either to change the encryption cipher or passphrase), perform the following steps:

Prerequisite: Before changing the cipher or passphrase format, ensure that you have the original passphrase in either plain-text or base64 format.

1. Reconfigure the device with a new cipher or passphrase using the following command:

```
ACOS(config)#system enable-disk-encryption cipher serpent passphrase-
base64 <new_base64-encoded_passphrase_string>
Disk encryption already configured. Do you want configure again?
[yes/no]:yes
Enter the old passphrase:<old_passphrase_string>
Creating backup.
It will take some time...
.....................................................................
.........................
.....................................................................
.........................
.....................................................................
................
Disk encryption is enabled
Reboot the system to encrypt the disk
```

NOTE: To reconfigure the device with a plain-text passphrase, replace **`passphrase-base64`** with **`passphrase`** in the above command.

2. Check the disk encryption status before reboot using the following command:

```
ACOS(config)#show system disk-encryption status
Disk encryption status:
Configured:Yes
Encrypted:Yes: Encrypted with old config
```

3. Check the disk encryption status after reboot.

```
ACOS(config)#show system disk-encryption status
Disk encryption status:
Configured:Yes
Encrypted:Yes
```

Additional Notes

- Once the data partition is encrypted, it cannot be decrypted.
- After disk encryption configuration or reconfiguration, the initial boot time may be longer due to restoration of the backup. Subsequent boot times remain unaffected.
- CPU usage may temporarily spike to 100% during disk encryption.
- The disk encryption process may take up to two hours or more, depending on disk usage.
- If the backup fails because the file size is larger than the available RAM, the system prompts the user to confirm a system-reset. This reset frees up space by deleting logs, core dumps, and debug files and then continues with encryption.

Limitations

The Disk Encryption feature has the following limitations:

- Upgrading or downgrading is supported only if the disk encryption feature is available in the target ACOS version.
- Both primary and secondary boot images must support disk encryption feature.

Encryption Keys

ACOS supports configuration encryption to protect information stored in configuration files (passwords, API keys, and so on). The encryption keys are used to secure information and prevent unauthorized access to it.

Each device's configuration is encrypted using symmetric encryption and a dynamic hash-key mechanism based on its unique properties. For encrypting the password, you can create a unique passphrase. The passphrase keeps changing periodically to maintain security.

Once the passphrase is set, the running profile cannot be switched. Additionally, upgrades or downgrades can only be performed between the versions that support the passphrase feature. For VCS and VRRP, the passphrase must be the same on all devices in a cluster to maintain synchronization. Furthermore, the image in both the primary and secondary partitions must be compatible with the encryption update.

The passphrase encrypts the passwords or secret keys used by the authentication servers, such as TACACS, RADIUS, and LDAP. It is also used to secure passwords related to upgrading or downgrading ACOS versions, ensuring the protection of sensitive credentials.

The following topics are covered:

Key Considerations

The following are the key considerations:

- If the passphrase is lost, it cannot be recovered. A system reset is required to downgrade the system.
- The VCS must be disabled on each device in the cluster to update the system passphrase; it can be enabled after the passphrase is set on all devices.
- The L3V support allows configuration synchronization within partitions.
- The passphrase is supported in Multi-PU platforms.

CLI Configuration

Initial Passphrase Setup

The passphrase enhances system security. After setting the **`system upgrade-passphrase`** and running the write memory command, the password or secret key will be encrypted using the new passphrase. The command **`show running config`** displays the encrypted password.

For example, to set up the passphrase for the first time on the configured TACACS+ server to enable authentication:

1. Enter the `system update-passphrase` command. If you want to continue setting a new passphrase, type **yes**. Else, type **no** to discard the process.

```
ACOS(config)# system update-passphrase
Note: After changing to a new passphrase, you cannot downgrade to the
previous release. Do you want to continue with updating to new
passphrase? [yes/no]: yes
```

2. Enter the passphrase.

```
Please enter your new passphrase (minimum 8 characters): passwords
```

NOTE: A passphrase can have a minimum of 8 and a maximum of 64 characters.

3. Once the passphrase is set, use the following command to save the passphrase:

```
ACOS(config)#write memory all-partitions
```

4. Run the `show running config` command. The shared secret will be encrypted, and the encrypted string will be longer and change with each update.

```
ACOS(config)# show running config
Current configuration: 384 bytes
!
multi-config enable
!
!
!
```

```
tacacs-server host 192.000 secret encrypted
fftthMgh/ruk5RlnvqT3rRI92/mrt9yjR4lk0Phz
!
interface management
 ip address 10.23.21.76 255.255.254.0
 ip default-gateway 10.23.20.1
!
!
!
```

Updating Existing Passphrase

To update the existing passphrase:

1. Enter the current passphrase.

```
The passphrase has been configured. Do you want to continue to update a
new passphrase? [yes/no]: yes
Please enter your old passphrase before change to new one:xxxxxxxxxx
```

2. Enter the new passphrase.

```
Please enter your new passphrase (minimum 8 characters): yyyyyyyyyy
```

3. Once the passphrase is set, use the following command to save the passphrase:

```
ACOS(config)#write memory all-partitions
```

Downgrade the System

A system reset is required to downgrade the system after the passphrase is set and lost.

```
ACOS(config)#system-reset
```

NOTE: Once the passphrase is set, downgrading to software versions that do not have the passphrase feature is not allowed.

Limitations

The following are the limitations:

- The 'no' functionality is not supported.
- The downgrading to software versions that do not have this feature is not supported after the password is set.
- The copying of external configuration to the running configuration is not supported because it is not in an interactive mode.
- aXAPI is not supported.

Thunder Device Specific Settings

This section describes settings or configurations specific to certain Thunder devices.

The following topics are covered:

Interface Ethernet Port Group Speed on TH7460

This topic explains how to configure the ethernet port speed using the **`system forced-group-speed`** command on TH7460S and TH7460S-MAX platforms.

Interface Ethernet Ports

The TH7460S and TH7460S-MAX platforms have 32 interface ethernet ports that are divided based on their speed handling capacity:

- Ports 1-24 do not support auto speed detection. These ports are grouped in sets of four port (quads) and must be manually configured to operate at 1G, 10G, or 25G. The default speed for these ports is 10G.
- Ports 25-32 support auto speed detection and can operate at 100G or 40G speeds. The default speed for these ports is 100G.

The following topics are covered:

Configure Group Speed Interface Ethernet Port 1-24

This section describes how to configure ethernet port 1-24 group speed. The ports are organized into the following six quad port groups for the group speed configuration:

Quad Port Group Mapping

Quad Group	Ports	Interface Range
Quad 1	Ports 1–4	eth01_to_eth04
Quad 2	Ports 5–8	eth05_to_eth08
Quad 3	Ports 9–12	eth09_to_eth12
Quad 4	Ports 13–16	eth13_to_eth16
Quad 5	Ports 17–20	eth17_to_eth20
Quad 6	Ports 21–24	eth21_to_eth24

To set the speed for a specific group of four Ethernet ports, use the **system forced-group-speed** command with the port range **<ethXX_to_ethYY>** and desired speed **<1g | 10g | 25g>**.

NOTE: This command is only supported for TH7460S and TH7460S-MAX platforms.

Example

The following command sets the ethernet ports 05 to 08 to their maximum speed of 25Gbps.

```
ACOS(config)#system forced-group-speed eth05_to_08 25G
Please save your configuration and reload/reboot for the configuration to
take effect
```

After executing this command, use **write memory** to save the configuration and and **reload** to apply the group speed configuration.

After restarting the system, you can use the **show interfaces brief** command to verify the speed of the configured ports.

Example

The following command displays the ports 05 to 08 configured to maximum speed of 25Gbps.

```
ACOS(config)# show interfaces brief
Port                Link   Dupl   Speed   Trunk Vlan Encap     MAC             IP Address
IPs Flags   Name
```

```
-------------------------------------------------------------------------------------------------------------
-------------
mgmt                 Up    Full  1000   N/A   N/A  N/A       001f.a046.84f0  10.67.3.193/24
1
1                    Up    Full  25000  none  17   N/A       001f.a046.84f8  0.0.0.0/0
0
2                    Up    Full  25000  none  2    N/A       001f.a046.84f9  0.0.0.0/0
0
3                    Up    Full  25000  none  2    N/A       001f.a046.84fa  0.0.0.0/0
0
4                    Up    Full  25000  none  3    N/A       001f.a046.84fb  0.0.0.0/0
0
5                    Up    Full  25000  none  3    N/A       001f.a046.84fc  0.0.0.0/0
0
6                    Up    Full  25000  none  4    N/A    x  001f.a046.84fd  0.0.0.0/0
0
7                    Up    Full  25000  none  4    N/A       001f.a046.84fe  0.0.0.0/0
0
8                    Up    Full  25000  none  5    N/A       001f.a046.84ff  0.0.0.0/0
0
9                    Down  None  None   none  5    N/A       001f.a046.8500  0.0.0.0/0
0
10                   Down  None  None   none  6    N/A       001f.a046.8501  0.0.0.0/0
0
11                   Down  None  None   none  6    N/A       001f.a046.8502  0.0.0.0/0
0
12                   Down  None  None   none  7    N/A       001f.a046.8503  0.0.0.0/0
0
13                   Down  None  None   none  7    N/A       001f.a046.8504  0.0.0.0/0
0
14                   Down  None  None   none  8    N/A       001f.a046.8505  0.0.0.0/0
0
15                   Down  None  None   none  8    N/A       001f.a046.8506  0.0.0.0/0
0
16                   Down  None  None   none  9    N/A       001f.a046.8507  0.0.0.0/0
0
17                   Up    Full  10000  none  9    N/A       001f.a046.8508  0.0.0.0/0
0
```

```
18                  Up    Full  10000  none  10   N/A       001f.a046.8509  0.0.0.0/0
0
19                  Up    Full  10000  none  10   N/A       001f.a046.850a  0.0.0.0/0
0
20                  Up    Full  10000  none  11   N/A       001f.a046.850b  0.0.0.0/0
0
21                  Up    Full  25000  none  11   N/A       001f.a046.850c  0.0.0.0/0
0
22                  Up    Full  25000  none  12   N/A       001f.a046.850d  0.0.0.0/0
0
23                  Up    Full  25000  none  12   N/A       001f.a046.850e  0.0.0.0/0
0
24                  Up    Full  25000  none  13   N/A       001f.a046.850f  0.0.0.0/0
0
25                  Up    Full  40000  none  13   N/A       001f.a046.8510  0.0.0.0/0
0
26                  Up    Full  40000  none  14
```

Limitations

The **`system forced-group-speed`** command does not allow you to configure different speeds for individual ports within a group. For example, you cannot set 10G on ports 01–02 and 25G on ports 03–04.

Dynamic Port Breakout for Thunder 7x50 Series

This feature helps in enhancing the dynamic port splitting/breakout support for the **Thunder 7x50** series.

Overview

The third generation **Thunder xx30** series and the fourth generation Thunder series, such as *TH4440*, *TH5440*, and *TH5840*, supports the breaking out 40G interfaces into 4x10G using the command "`system-4x10g-mode`".

The dynamic port breakout was first extended to the port-level configuration on the **Thunder 5x50** platform, and now this feature is also supported on the **Thunder 7x50** platform.

The following topics are covered:

Dynamic Port Breakout Support Features

This feature helps the user to perform and understand the following tasks:

1. Adding support of interface level CLI command "`port-breakout`" on the **Thunder 7x50** platform.
2. Supporting and generating the dynamic **`plat_if`** table, which defines the front ports to and/or from Broadcom chipset internal mapping along with the total number of interfaces.
3. Supporting dynamic generation of Broadcom chipset configuration, which defines total numbers of its internal ports along with per-port parameters, such as speed.
4. Supporting dynamic parse of ACOS startup configuration file to support the above-mentioned task items 2 and 3.

The following topics are covered:

Logical Port Mapping Support

The logical port mapping helps in redirecting the various communication request from multiple sources.

For the reference, Broadcom SDK uses a configuration text file for logical ports management.

The following is a synopsis of its Syntax:

```
portmap_logical_port.unit=physical_port:speed
```

Support for Dynamic Port Breakout

The following are the steps and representations to support the dynamic port breakout feature:

1. The CLI validates the users entered port breakout command, corresponding messages are shown which could be rejected or a prompt for saving the configuration before it can be applied on the next reload or reboot.
2. At the system initialization phase, startup configuration is parsed for per-physical port breakout and per-platform **`plat_if`** table generation.
3. The configuration file is generated before the control is passed to Broadcom SDK, per-platform.

Port Mapping Implementation Example

The following is an example of a partial of port mapping scenario:

```
# port breakout begin
portmap_5.1=5:25
portmap_6.1=6:25
portmap_7.1=7:25
portmap_8.1=8:25
portmap_13.1=13:100
portmap_21.1=21:50
portmap_23.1=23:50
portmap_29.1=29:50
portmap_31.1=31:50
portmap_41.1=41:25
portmap_42.1=42:25
portmap_43.1=43:25
portmap_44.1=44:25
portmap_49.1=49:50
portmap_51.1=51:50
portmap_57.1=57:25
portmap_58.1=58:25
portmap_59.1=59:25
portmap_60.1=60:25
portmap_61.1=61:25
portmap_62.1=62:25
portmap_63.1=63:25
portmap_64.1=64:25
```

```
portmap_67.1=65:100
portmap_71.1=69:100
portmap_79.1=77:100
portmap_87.1=85:100
portmap_99.1=97:100
portmap_107.1=105:100
portmap_115.1=113:100
portmap_123.1=121:100
```

Dynamic Port Breakout Application

The following topics are covered:

Port Numbering

In the **Thunder Series 7650**, there are **16x100G** physical front ports. The port numbering is illustrated as the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Breakout Feature - Important Points

The following is a list of important points for applying this feature:

- As each lane of a Falcon chip can optionally run at a flexible speed of **10G**, the port-level command "`speed-forced-40g`" can be applied.
- With ACOS implementation, all the front ports of **Thunder 7650** are "`speed-forced capable`", while only the front ports from one to eight are "`breakout capable`."
- The "***speed-forced***" feature can be applied without even a system reload or reboot on-the-go.

  But the "***breakout***" feature must be reloaded for configuration to take effect.

This could create a configuration event issue among the threads or the processes.

- This implies enabling both features simultaneously on the same front ports is not presently supported.

  Only one feature can be enabled at a time on a given physical port.

- To enable the port breakout feature on a given physical interface, the cited `port-breakout` command can be issued with a mandatory keyword to specify the desired breakout mode.

  Presently, **4x25G** and **2x50G** are two breakout modes that are supported.

- When a physical front port is breaking out into two or four logical ones, the physical port number of it stays unchanged while one or three logical ports are augmented after the last physical one.

Feature Implementation Example

The following is an example scenario for this feature implementation:

When *port one* is in the **4x25G** *breakout mode*, it becomes ports [**1, 17, 18, 19]** after a system reboot or reload. At this time, if *port breakout mode* **4x25G** is also enabled on *port three*, it then results into a total of *22 front ports* with *two ports breakout* [**1, 17, 18, 19]** and **[3, 20, 21, 22**].

This is reflected in the startup configuration and can be realized with the command "`show startup-config`". Only the first *eight front ports* can be broken out into **4x25G** or **2x50G** mode, the combination of total numbers of ports is illustrated in the following table, where only *39 front ports* are not possible from the range **[16 to 40]**.

Table 2 : Feature Implementation - Dynamic Port Breakout Support - Combination of Total Numbers of Ports

Number of Non-Breakout Capable Port	***Number of 4x25G Ports, Denoted by:*** ***Q [0 to 8]***	***Number of 2x50G Ports, Denoted by:*** ***B [0 to (8 - Q)]***	***Total Number of Ports***	***8 + (4xQ) + (2xB) +*** ***(8 - Q - B), (Q + B) < = 8***
8	8	0	40	8 + (4x8) + (2x0) + 0

Table 2 : Feature Implementation - Dynamic Port Breakout Support - Combination of Total Numbers of Ports

Number of Non-Breakout Capable Port	***Number of 4x25G Ports, Denoted by: Q [0 to 8]***	***Number of 2x50G Ports, Denoted by: B [0 to (8 - Q)]***	***Total Number of Ports***	***8 + (4xQ) + (2xB) + (8 - Q - B), (Q + B) < = 8***
8	7	1	38	8 + (4x7) + (2x1) + 0
8	7	0	37	8 + (4x7) + (2x0) + 1
8	6	2	36	8 + (4x6) + (2x2) + 0
8	6	1	35	8 + (4x6) + (2x1) + 1
8	6	0	34	8 + (4x6) + (2x0) + 2
8	5	3	34	8 + (4x5) + (2x3) + 0
8	5	2	33	8 + (4x5) + (2x2) + 1
8	5	1	32	8 + (4x5) + (2x1) + 2
8	5	0	31	8 + (4x5) + (2x0) + 3
8	4	4	32	8 + (4x4) + (2x4) + 0
8	4	3	31	8 + (4x4) + (2x3) + 1
8	4	2	30	8 + (4x4) + (2x2) + 2
8	4	1	29	8 + (4x4) + (2x1) +

Table 2 : Feature Implementation - Dynamic Port Breakout Support - Combination of Total Numbers of Ports

Number of Non-Breakout Capable Port	***Number of 4x25G Ports, Denoted by: Q [0 to 8]***	***Number of 2x50G Ports, Denoted by: B [0 to (8 - Q)]***	***Total Number of Ports***	***8 + (4xQ) + (2xB) + (8 - Q - B), (Q + B) < = 8***
				3
8	4	0	28	8 + (4x4) + (2x0) + 4
8	3	5	30	8 + (4x3) + (2x5) + 0
8	3	4	29	8 + (4x3) + (2x4) + 1
8	3	3	28	8 + (4x3) + (2x3) + 2
8	3	2	27	8 + (4x3) + (2x2) + 3
8	3	1	26	8 + (4x3) + (2x1) + 4
8	3	0	25	8 + (4x3) + (2x0) + 5
8	2	6	28	8 + (4x2) + (2x6) + 0
8	2	5	27	8 + (4x2) + (2x5) + 1
8	2	4	26	8 + (4x2) + (2x4) + 2
8	2	3	25	8 + (4x2) + (2x3) + 3
8	2	2	24	8 + (4x2) + (2x2) + 4

Table 2 : Feature Implementation - Dynamic Port Breakout Support - Combination of Total Numbers of Ports

Number of Non-Breakout Capable Port	***Number of 4x25G Ports, Denoted by: Q [0 to 8]***	***Number of 2x50G Ports, Denoted by: B [0 to (8 - Q)]***	***Total Number of Ports***	***8 + (4xQ) + (2xB) + (8 - Q - B), (Q + B) < = 8***
8	2	1	23	8 + (4x2) + (2x1) + 5
8	2	0	22	8 + (4x2) + (2x0) + 6
8	1	7	26	8 + (4x1) + (2x7) + 0
8	1	6	25	8 + (4x1) + (2x6) + 1
8	1	5	24	8 + (4x1) + (2x5) + 2
8	1	4	23	8 + (4x1) + (2x4) + 3
8	1	3	22	8 + (4x1) + (2x3) + 4
8	1	2	21	8 + (4x1) + (2x2) + 5
8	1	1	20	8 + (4x1) + (2x1) + 6
8	1	0	19	8 + (4x1) + (2x0) + 7
8	0	8	24	8 + (4x0) + (2x8) + 0
8	0	7	23	8 + (4x0) + (2x7) + 1
8	0	6	22	8 + (4x0) + (2x6) +

Table 2 : Feature Implementation - Dynamic Port Breakout Support - Combination of Total Numbers of Ports

Number of Non-Breakout Capable Port	***Number of 4x25G Ports, Denoted by: Q [0 to 8]***	***Number of 2x50G Ports, Denoted by: B [0 to (8 - Q)]***	***Total Number of Ports***	***8 + (4xQ) + (2xB) + (8 - Q - B), (Q + B) < = 8***
				2
8	0	5	21	8 + (4x0) + (2x5) + 3
8	0	4	20	8 + (4x0) + (2x4) + 4
8	0	3	19	8 + (4x0) + (2x3) + 5
8	0	2	18	8 + (4x0) + (2x2) + 6
8	0	1	17	8 + (4x0) + (2x1) + 7
8	0	0	16	8 + (4x0) + (2x0) + 8

Feature Impact Details

The following is a list of important points regarding the impact of this feature:

- There must be no impact on fast path traffic after the breakout is enabled.
- The control CPUs may experience minor higher usage because of the augmented front ports.
- The details regarding the configuration to breakout ports cannot be preserved before or after the feature is enabled or disabled.
- The LED microprocessor does not need to be reprogrammed to reflect the link or activity status of the newly acquired breakout ports.

NOTE:

- For more information on this feature, see *Dynamic Port Breakout Support* or *Port Splitting Support* under the various guides from the *Hardware or Platform Documents* section.
- The CLI/command details are also available in the *Command Line Interface Reference* and *aXAPI Reference Guide* for this feature.

Configuration Management

This part of the document describes how to configure the following management features for ACOS devices:

- Configuration Synchronization
- Back Up System Information
- Source Interface for Management Traffic
- Dynamic and Block Configuration
- Boot Options
- Power On Auto Provisioning
- Fail-Safe Automatic Recovery
- Jumbo Frames on ACOS Devices

Configuration Synchronization

The `configure sync` command is used to manually synchronize the configuration commands running-config and startup-config of all or specific partitions such as Shared Partition, L3V Partitions, and Service Partitions from one ACOS device to another ACOS device.

This feature is supported for the ACOS devices that are deployed in VRRP-A or non-VRRP-A environments.

The synchronization is possible only between specific partitions. For example, consider a scenario with Thunder devices T1 and T2 in a VRRP-A environment.

Configuration synchronization is permitted in the following scenarios:

- From T1 Shared partition to T2 Shared/L3V/Service partition
- From T1 all partitions including shared to T2 all partitions including shared partitions
- From T1 L3V partition to and the same T2 L3V partition
- From T1 Service partition to the same T2 Service partition

NOTE: Only running and startup configurations are synchronized; while the device-specific configurations, such as interface configurations, are not synchronized.

For more information about configuration options, see configure sync in the *Command Line Interface Reference.* For information on configuration objects that are included or not included in a manual synchronization, see the appropriate topic below.

NOTE: Manual configuration is not necessary for running ACOS Virtual Chassis System (aVCS). For more information, see the Configuration Synchronization without Reload section in the *Configuring ACOS Virtual Chassis Systems* Guide.

The following topics are covered:

Synchronization Link Requirements

Following are the pre-requisites for configuration synchronization:

- SSH management access must be enabled on both ends of the link before performing a manual synchronization.
- The destination device must be reachable and route-able from the current partition.
- Before synchronizing the Active and Standby ACOS devices, verify that both are running the same software version. Configuration synchronization between two different software versions is not recommended, since some configuration commands in the newer version might not be supported in the older version.
- While performing synchronization, you must have write privileges on the destination node.
- The configuration synchronization process does not check user privileges on the Standby ACOS device and will synchronize to it using read-only privileges. However, you must be logged onto the Active ACOS device with configuration (read-write) access.
- If the configuration includes Policy-based SLB (black/white lists), the time it takes for synchronization depends on the size of the black/white-list file. This is because the synchronization process is blocked until the files are transferred from active to standby mode.
- Do not make other configuration changes to the Active or Standby ACOS device during synchronization.
- Data that is synchronized from a Standby ACOS device to an Active ACOS device is not available on the Active ACOS device until that device is rebooted or the software is reloaded.
- The **`configure sync`** command will not function if **`vcs enabled`** is active.

NOTE: In 4.x, the reload action is not allowed.

Configuration Items that are Backed Up

The following configuration items are backed up during the configuration synchronization:

- Admin accounts and settings
- AAA settings
- ACLs
- CGN
- DDoS protection settings
- Floating IP addresses
- FW
- Health Monitors
- IPsec
- ICMP rate limiting
- IP NAT configuration, including LSN and DS-Lite
- IP limiting settings
- PBSLB settings
- SLB
- RAM caching
- DNS security and caching
- FWLB
- GSLB
- Data Files:
  - aFleX files
  - External health check files
  - SSL certificates, private-key files, and CRLs
  - Class-list files
  - Black/white-list files

NOTE: The order of Firewall rule-set is not synced during the configuration synchronization. If you want to sync the order of Firewall rule-set, you must use the aVCS as an alternative.

Configuration Items that are Not Backed Up

The following configuration items are *not* backed up during the configuration synchronization:

- Interface-specific management access settings
- LACP settings
- Interface settings

• Hostname • MAC addresses • Management IP addresses • Static Trunks or VLANs	• OSPF or IS-IS settings • ARP entries or settings

NOTE: On multi-PU platforms, the partitions on PU2 do not get synchronized.

Perform Configuration Synchronization

To synchronize the ACOS device configurations, use the steps described below.

Configure Using CLI

The **`configure sync`** commands are available at the global configuration level of the CLI.

- To synchronize the running-config and startup-config, use the **`configure sync all`** command. This will also sync data files in addition to the local running configuration and startup configuration to the peer device.
- The following example of a command synchronizes both the running configuration and startup configuration from the shared partition of the local device to the shared partition on the peer device with IP address 192.168.105.127.

```
ACOS(config)# configure sync all auto-authentication 192.168.105.127
```

- To synchronize the running-config of the Active ACOS device to the running-config of the Standby ACOS device, use the configure sync running command. This syncs the data files, in addition to the running configuration to the peer device.
- The following example of a command synchronizes only the running configuration from the shared partition of the local device to the shared partition on the peer device with IP address 192.168.105.127.

```
ACOS(config)# configure sync running auto-authentication 192.168.105.127
```

- To synchronize the running-config from a specific L3V partition of one device to

the L3V partition on the peer ACOS device, use the **configure sync running** command.

The following example of a command synchronizes the running configuration from the p1 partition of the local device to the p1 partition on the peer device with IP address 192.168.105.127.

```
ACOS(config)# configure sync running auto-authentication 192.168.105.127
```

For more detailed information, see `configure sync` in the *Command Line Interface Reference*.

NOTE: Synchronization of just the data files is not available in 4.x.

Configure Using GUI

1. Select **System > Settings > Sync Settings.**
2. In the User, Password, and Destination IP Address fields, enter the admin username, password credentials, and IP address of the peer device.
3. Configure the other fields on this page as desired; refer to the GUI online help for more information about each field.
4. Click **OK**.

Display Configure Sync State

Introduced in 4.x, the synchronization state for running and startup configurations can be viewed by using the CLI command **show config-sync**.

An example output is shown from the source device.

```
ACOS-Active(config)# show config-sync
Partition Name   Sync Status for running-config and startup-config
-------------------------------------------------------------
shared           (running-config) sync to ip 192.168.105.127 at 20:04:04
IST Thu Jul 17 2008
shared           (startup-config) sync to ip 192.168.105.127 at 20:04:04
IST Thu Jul 17 2008
```

An example output is shown from the destination device.

```
ACOS-standby# show config-sync
Partition Name   Sync Status for running-config and startup-config
-------------------------------------------------------------
shared           (running-config) is synced from ip 192.168.105.120 at
06:25:19 GMT Mon Nov 27 2017
shared           (startup-config) is synced from ip 192.168.105.120 at
06:25:20 GMT Mon Nov 27 2017
```

Performing a write operation, or modifying a configuration will change the sync status for the modified configuration.

For example, running the **write memory** command will change the start-up config state from “sync” to “not-synced”.

```
ACOS-Active# write memory
Building configuration...
Write configuration to profile "conn_40"
[OK]
ACOS-Active#show con
ACOS-Active#show config-s
ACOS-Active# show config-sync
Partition Name   Sync Status for running-config and startup-config
-------------------------------------------------------------
shared           (running-config) sync to ip 192.168.105.127 at 20:04:04
IST Thu Jul 17 2008
shared           (startup-config) not synced because write memory at
20:09:25 IST Thu Jul 17 2008
```

If the running configuration is modified, the running-config state will change from “sync” to “not-synced”.

For example, the following configuration is added to the running configuration.

```
ACOS-Active(config)# cgnv6 nat pool a 1.1.1.1 netmask /24
```

Now, running the **show config-sync** command, the running configuration is no longer synced.

```
ACOS-Active(config)# show config-sync
Partition Name   Sync Status for running-config and startup-config
-------------------------------------------------------------
```

```
shared           (running-config) not synced because it's changed at
07:02:33 GMT Mon Nov 27 2017
shared           (startup-config) not synced because write memory at
06:30:24 GMT Mon Nov 27 2017
```

Monitor Multi-PU Synchronization

In a multi-PU environment, Processing Unit 1 (PU1) acts as the primary PU and Processing Unit 2 (PU2) as the secondary PU. Any configuration changes on PU1 are automatically propagated to PU2.

To monitor the synchronization status of PU2 with PU1 periodically, you can use the `system config-mgmt pu-sync-detection` command. This command allows you to enable, disable, or set the interval for detecting the status of configuration synchronization between PU1 and PU2.

You can also view inconsistency in the configuration and associated warning message using the `show log` command.

NOTE:

- This command applies only to the multi-PU platform.
- By default, the detection is disabled. If enabled, it may affect the control place performance and CPU usage, especially if a large configuration is applied or too many partitions are configured.

CLI Configuration

- To enable or disable the detection of configuration synchronization between PU1 and PU2:

```
ACOS(config)# system config-mgmt pu-sync-detection
ACOS(config-pu-sync-detection)# enable | disable
```

- To set an interval to detect configuration synchronization between PU1 and PU2:

```
ACOS(config)# system config-mgmt pu-sync-detection
ACOS(config-pu-sync-detection)# interval <30-86400>
```

Show Command

To view the warning message on configurations that are not synchronized between PU1 and PU2, use the `show log` command.

```
Nov 27 2024 12:18:04 Info    [CFGMGR]: - PU1 - Partition 'shared' is in
sync now in PU2.
Nov 27 2024 12:17:04 Warning   [CFGMGR]: - PU1 - Partition 'shared' has
2 objects out of sync in PU2, including slb.server(s4,s5).
Nov 27 2024 12:11:45 Warning   [CFGMGR]: - PU1 - Partition 'shared' has
2 objects out of sync in PU2, including slb.server(s4,s5).
```

Back Up System Information

By default, when you click the **Save** button in the GUI or enter the `write memory` command in the CLI, all unsaved configuration changes are saved to the startup-config. The next time the ACOS device is rebooted, the configuration is reloaded from this file.

In addition to these simple configuration management options, the ACOS device has advanced configuration management options that allow you to save multiple configuration files. You can save configuration files remotely on a server and locally on the ACOS device itself.

NOTE:

- For information about managing configurations for separate partitions on an ACOS device, see the *Configuring Application Delivery Partitions* guide.
- For information about synchronizing configuration information between multiple ACOS devices configured for VRRP-A high availability, see the *Configuring VRRP-A High Availability* guide.
- For upgrade instructions, see the *Release Notes* for the ACOS release to which you plan to upgrade.

The following topics are covered:

Overview of System Backup

The ACOS device allows you to back up the system, individual configuration files, and log entries onto remote servers. You can use any of the following file transfer protocols:

- Trivial File Transfer Protocol (TFTP)
- File Transfer Protocol (FTP)
- Secure Copy Protocol (SCP)
- SSH File Transfer Protocol (SFTP)

NOTE: Backing up system from one hardware platform and restoring it to another hardware platform is not supported.

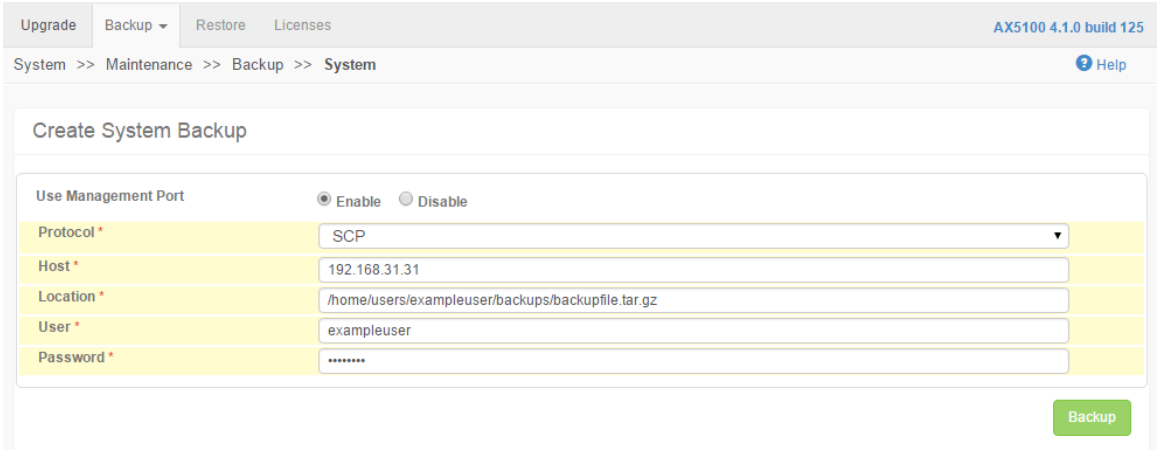
The following topics are covered:

Back Up Using GUI

To configure backup using the GUI:

1. Navigate to **System > Maintenance**.
2. In the menu bar, click **Backup**. From the drop-down menu that appears, select one of the following:
   - System — This option performs an immediate backup of the configuration file (s), aFleX scripts, and SSL certificates and keys.
   - Log — This option perform an immediate backup of the log entries in the ACOS device's syslog buffer (along with any core files on the system).
   - Periodic Backup — This option performs a scheduled backup of either the system or log files.
3. Complete your backup configuration by specifying any necessary information (for example, the remote host and port, file transfer protocol, location and name of the backup file, and remote system access information).

The following example shows an example of a system backup:



Back Up Using CLI

This section provides examples of how to back up your system using the CLI.

The following example creates a backup of the system (startup-config file, aFleX scripts, and SSL certificates and keys) on a remote server using SCP.

```
ACOS(config)# backup system
scp://exampleuser@192.168.3.3/home/users/exampleuser/backups/backupfile.tar.gz
```

The following example creates a daily backup of the log entries in the syslog buffer. The connection to the remote server will be established using SCP on the management interface (**use-mgmt-port**).

```
ACOS(config)# backup log period 1 use-mgmt-port
scp://exampleuser@192.168.3.3/home/users/exampleuser/backups/backuplog.tar.gz
```

Restore from Backup

You can use a saved backup to restore your current system; for example, if you are upgrading the devices in your network to the newer A10 Thunder Series devices.

This section contains some important things to consider before performing a restore operation:

- System Memory
- FTA versus Non-FTA
- L3V Partitions
- Port Splitting
- Port Mapping

System Memory

If your current device has less memory than the backup device (for example, 16 GB on the current device but 32 GB on the previous device), this can adversely affect system performance.

FTA versus Non-FTA

If you are restoring from an FTA device to a non-FTA device, for example, some commands may not be available after the restore operation. This command is lost and cannot be restored.

L3V Partitions

L3v partitions and their configurations are restored; however, if you are restoring to a device which supports a fewer number of partitions (for example, 32) than you have configured from the backup device (for example, 64) then any partitions and corresponding configuration beyond 32 are lost.

Port Splitting

If you are restoring between devices with various 40 GB port splitting configurations, see the following Table 3 for more information.

Table 3 : Restore Behavior for Port Splitting Combinations

Backup Device	Current Device	Behavior During the Restore Operation
Port splitting disabled.	Port splitting disabled.	Allow user to perform port mapping (See Port Mapping.)
Port splitting enabled.	Port splitting enabled.	Allow user to perform port mapping (See Port Mapping.)
Port splitting enabled.	Port splitting disabled.	Ask the user if they want to perform port

Table 3 : Restore Behavior for Port Splitting Combinations

Backup Device	Current Device	Behavior During the Restore Operation
		mapping. If yes, enable port splitting, reboot the device, then perform the restore operation again, where port mapping will be enabled.
Port splitting disabled.	Port splitting enabled.	Exit the restore operation. The user will have to perform a `system-reset` or disable port splitting, reboot the system, and then perform the restore operation again.

Port Mapping

When restoring from a device that has a different number of ports, or even the same number of ports, you can map the port number from the previous configuration to a new port number (or same port number) in the new configuration.

In cases where the original number of ports is greater than the number of ports on the new system, some configuration may be lost.

If you choose to skip port mapping (see the example below) then the original port numbers and configurations are preserved. If the original device had ports 1-10 configured, and the new device only has ports 1-8, and you skip port mapping, then ports 9 and 10 are lost. If you choose port mapping, you can decide which 8 out of the original 10 ports you want to preserve during the port mapping process.

Save Multiple Configuration Files Locally

The ACOS device has CLI commands that enable you to store and manage multiple configurations on the ACOS device.

NOTE: Unless you plan to locally store multiple configurations, you do not need to use any of the advanced commands or options described in this section. You can enter the **`write memory`** command in the CLI to save configuration changes. These simple options replace the commands in the startup-config stored in the image area the ACOS device booted from with the commands in the running-config.

The following topics are covered:

Understanding Configuration Profiles

Configuration files are managed as configuration profiles. A configuration profile is simply a configuration file. You can locally save multiple configuration profiles on the ACOS device. The configuration management commands described in this section enable you to do the following:

- Save the startup-config or running-config to a configuration profile.
- Copy locally saved configuration profiles.
- Delete locally saved configuration profiles.
- Compare two configuration profiles side by side to see the differences between the configurations.
- Link the command option “startup-config” to a configuration profile other than the one stored in the image area used for the most recent reboot. (This is the profile that “startup-config” refers to by default.) This option makes it easier to test a configuration without altering the configuration stored in the image area.

NOTE: Although the enable and admin passwords are loaded as part of the system configuration, they are not saved in the configuration profiles. Changes to the enable password or to the admin username or password take effect globally, regardless of the values that were in effect when a given configuration profile was saved.

Save Configurations Using CLI

To manage multiple locally stored configurations, use the **write memory** or **write force** commands (available at the global configuration level of the CLI).

- If you enter **write memory** without additional options, the command replaces the configuration profile that is currently linked to by startup-config with the commands in the running-config. If startup-config is set to its default (linked to the configuration profile stored in the image area that was used for the last reboot), then **write memory** replaces the configuration profile in the image area with the running-config.
- If you enter **write force**, the command forces the ACOS device to save the configuration regardless of whether the system is ready.
- If you enter **write memory primary**, the command replaces the default configuration profile of the primary image area with the running-config. Likewise, if you enter **write memory secondary**, the command replaces the default configuration profile of the secondary image area with the running-config.
- If you enter **write memory** *profile-name*, the ACOS device replaces the commands in the specified *profile-name* with the running-config.
- You can also specify a specific L3V partition or **all-partitions** with the **write memory** and **write force** commands; these options save the configuration changes in your L3V partitions. Without either option, only the configuration in the shared partition is saved.

NOTE: For CLI syntax information about write memory and write force, see the *Command Line Interface Reference* Guide.

View Configurations Using CLI

To view locally stored configuration information, use the **show startup-config** command.

- To display a list of the locally stored configuration profiles, use the **show startup-config all** command.

- The **`show startup-config all-partitions`** command shows all resources in all partitions. In this case, the resources in the shared partition are listed first, followed by the resources in each L3V partition. You can also specify a single partition instead of **`all-partitions`** to view the startup-config for the specified partition only.
- The **`show startup-config profile`** *`profile-name`* command displays the commands that are in the specified configuration profile.

NOTE: For CLI syntax information about show startup-config, see the *Command Line Interface Reference* Guide.

Copy Configurations Using CLI

To copy configurations, use the **`copy`** command.

- The **`copy startup-config`** *`profile-name`* command copies the configuration profile that is currently linked to "startup-config" and saves the copy under the specified profile name.
- The **`copy startup-config running-config`** command copies the configuration profile that is currently linked to "startup-config" and replaces the current running-config.
- The **`copy running-config startup-config`** command copies the running-config and saves it to the configuration profile currently linked to the startup-config.

NOTE: You cannot use the profile name "default". This name is reserved and always refers to the configuration profile that is stored in the image area from which the ACOS device most recently rebooted.

- For all commands, specify the *url* to the remote device where you want to back up the configuration. See Back Up System Information.)

NOTE: For CLI syntax information about the copy command, see the *Command Line Interface Reference* Guide.

Compare Configurations Using CLI

To view a side-by-side comparison of configurations, use the **diff** command.

- The **diff startup-config running-config** command compares the configuration profile that is currently linked to "startup-config" with the running-config. Similarly, the **diff startup-config** *profile-name* command compares the configuration profile that is currently linked to "startup-config" with the specified configuration profile.
- To compare any two configuration profiles, enter their profile names.

  For example: **diff** *profile-name1 profile-name2*

In the CLI output, the commands in the first profile name you specify are listed on the left side of the terminal screen. The commands in the other profile that differ from the commands in the first profile are listed on the right side of the screen, across from the commands they differ from. The following Table 4 describes the flags indicating how the two profiles differ:

Table 4 : Description of the Flags in the diff Command Output

Flag	Description
|	Indicates that the corresponding command has different settings in each profile.
>	Indicates that the corresponding command is in the second profile, but not the first.
<	Indicates that the corresponding command is in the first profile, but not the second.

Link Configuration Profiles Using CLI

Use the **link** command to link configuration profiles. 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.

This command enables you to easily test new configurations without replacing the configuration stored in the image area. For example, the following command links the startup-config to a new profile called as the **test_profile**:

```
ACOS(config)# link startup-config test-profile primary
```

You can specify the **primary** or **secondary** option to indicate an image area; if you omit this option, the image area last used to boot is selected.

The profile you link to must be stored on the boot device you select. For example, if you use the default boot device selection (hard disk), the profile you link to must be stored on the hard disk. (To display the profiles stored on the boot devices, use the **show startup-config all** command.)

After you link "startup-config" to a different configuration profile, configuration management commands that affect "startup-config" affect the linked profile instead of affecting the configuration stored in the image area. For example, if you enter the **write memory** command without specifying a profile name, the command saves the running-config to the linked profile instead of saving it to the configuration stored in the image area.

Likewise, the next time the ACOS device is rebooted, the linked configuration profile is loaded instead of the configuration that is in the image area.

To relink "startup-config" to the configuration profile stored in the image area, use the default option:

```
ACOS(config)# link startup-config default
```

Delete Profile Using CLI

Use the **delete startup-config** command to remove a specific configuration profile.

For example:

```
ACOS(config)# delete startup-config slb_profile1
```

Although the command uses the **startup-config** option, the command only deletes the configuration profile linked to "startup-config" if you enter that profile's name. The command deletes only the profile you specify.

If the configuration profile you specify is linked to "startup-config", "startup-config" is automatically relinked to the default. (The default is the configuration profile stored in the image area from which the ACOS device most recently rebooted).

CLI Example of Configuration Profile Management

The following command saves the running-config to a configuration profile named "**slbconfig2**":

```
ACOS(config)# write memory slbconfig2
```

The following command shows a list of the configuration profiles locally saved on the ACOS device. The first line of output lists the configuration profile that is currently linked to "startup-config". If the profile name is "default", then "startup-config" is linked to the configuration profile stored in the image area from which the ACOS device most recently rebooted.

```
ACOS(config)# show startup-config all
Current Startup-config Profile: slb-v6
Profile-Name                                Size    Time
-------------------------------------------------------------
1210test                                    1957    Jan 28  18:39
ipnat                                       1221    Jan 25  10:43
ipnat-l3                                    1305    Jan 24  18:22
ipnat-phy                                   1072    Jan 25  19:39
ipv6                                        2722    Jan 22  15:05
local-bwlist-123                            3277    Jan 23  14:41
mgmt                                        1318    Jan 28  10:51
slb                                         1354    Jan 23  18:12
slb-v4                                     12944    Jan 23  19:32
slb-v6                                     13414    Jan 23  19:19
```

The following command copies the configuration profile currently linked to "startup-config" to a profile named "slbconfig3":

```
ACOS(config)# copy startup-config slbconfig3
```

The following command compares the configuration profile currently linked to "startup-config" with configuration profile "testcfg1". This example is abbreviated for clarity. The differences between the profiles are shown in this example in bold type.

```
ACOS(config)# diff startup-config testcfg1
!Current configuration: 13378 bytes                              (
!Configuration last updated at 19:18:57 PST Wed Jan 23 2008      (
!Configuration last saved at 19:19:37 PST Wed Jan 23 2008        (
!version 1.2.1                                                   (
```

```
!                                                                    (
hostname ACOS (
!                                                                    (
clock timezone America/Tijuana                                       (
!                                                                    (
ntp server 10.1.11.100 1440                                          (
!                                                                    (
...
!                                                                    (
interface ve 30                                                      (
 ip address 30.30.31.1 255.255.255.0                                 |  ip
address 10.10.20.1 255.255.255.0
 ipv6 address 2001:144:121:3::5/64                                   |  ipv6
address fc00:300::5/64
!                                                                    (
!                                                                    (
> ip nat range-list v6-1 fc00:300::300/64 2001:144:121:1::900/6
!                                                                    (
ipv6 nat pool p1 2001:144:121:3::996 2001:144:121:3::999 netm        <
!                                                                    <
slb server ss100 2001:144:121:1::100                                 <
   port 22  tcp                                                      <
--MORE--
```

The following command links configuration profile "**slbconfig3**" with "**startup-config**":

```
ACOS(config)# link startup-config slbconfig3
```

The following command deletes configuration profile "**slbconfig2**":

```
ACOS(config)# delete startup-config slbconfig2
```

ACOS System Reset

A system reset clears active processes, reloads the system services, and boots the device and brings up to the stable state.

For example, the system reset is required in the following scenarios:

- To clear the corrupted or unstable state
- After upgrade fail or incomplete
- When hardware related issues are detected
- When unable to save the configurations on the system

It supports Thunder (FTA and non-FTA) and vThunder devices.

The following topics are covered:

CLI Configuration

To reset the ACOS device, perform the following:

1. Run the following command:

```
ACOS(config)# system-reset
```

The system prompts the following confirmation:

```
System reset requires reboot, do you want to continue? [yes/no]: yes
```

2. Type **yes** and press **Enter** the following confirmation is displayed:

```
Proceed to reset System to its default configuration [yes/no] : yes
```

3. Type **yes** and press **Enter** the following information is displayed:

```
System is about to be reset to its default configuration. Please wait
....
Big I/O buffer pool is not enabled currently.
Audit log has been successfully reset.
Core files has been successfully reset.
License product will remain ADC.
```

The system resets to its factory default settings.

The following table summarizes what is removed and preserved on the system:

What is Erased	What is Preserved
Saved configuration files	Running configuration
System files, including SSL certificates and keys, aFleX policies, black/white lists, and system logs	Audit log entries
Management IP address	
Admin-configured admins	
Enable password	
Imported files	
Inactive partitions	
Enable-password follow-password-policy	
Audit log entries	
Running configuration	

ACOS Device License Restore After System Reset

ACOS restores the ACOS device license after the device is reset to its factory default settings. This feature is helpful when you want to reapply or reactivate your A10 license after the system reset. This capability is available only on the ACOS devices that use modular licensing.

A system reset clears active processes, reloads the system services, boots the device, and brings it up to a stable state.

For example, the system reset is required in the following scenarios:

- To clear the corrupted or unstable state
- After upgrade fail or incomplete
- When hardware related issues are detected
- When unable to save the configurations on the system

It supports Thunder (FTA and non-FTA) and vThunder devices.

The following topics are covered:

CLI Configuration

To restore the ACOS device license, perform the following:

1. Run the following command:

```
ACOS(config)# system-reset preserve-license
```

The system prompts the following confirmation:

```
System reset requires reboot, do you want to continue? [yes/no]: yes
```

2. Type **yes** and press **Enter** the following confirmation is displayed:

```
Proceed to reset System to its default configuration [yes/no] : yes
```

3. Type **yes** and press **Enter** the following information is displayed:

```
System is about to be reset to its default configuration. Please wait
....
Big I/O buffer pool is not enabled currently.
Audit log has been successfully reset.
Core files has been successfully reset.
```

The system resets to its factory default settings and restores the ACOS device license.

The following table summarizes what is removed and preserved on the system:

What is Erased	What is Preserved
Saved configuration files	ACOS device license
System files, including SSL certificates and keys, aFleX policies, black/white lists, and system logs	
Management IP address	
Admin-configured admins	
Enable password	
Imported files	

What is Erased	What is Preserved
Inactive partitions	
Enable-password follow-password-policy	
Audit log entries	
Running configuration	

Verify Preserved License

To verify the preserved ACOS device license, use the following show command:

```
show license-info
```

Limitations

This feature has the following limitations:

- It does not support cThunder devices.
- It does not support ACOS devices that use Perpetual license.

Source Interface for Management Traffic

By default, the ACOS device uses data interfaces as the source for management traffic. This chapter describes how you can configure the management interface and loopback interfaces to act as the source for management traffic instead of using data interfaces.

The following topics are covered:

Management Interface as Source for Management Traffic

The following topics are covered:

Understanding Route Tables

By default, the ACOS device attempts to use a route from the main route table for management connections originated on the ACOS device. You can enable the ACOS device to use the management route table to initiate management connections instead.

This section describes the ACOS device's two route tables, for data and management traffic, and how to configure the device to use the management route table.

The ACOS device uses separate route tables for management traffic and data traffic.

- Management route table – Contains all static routes whose next hops are connected to the management interface. The management route table also contains the route to the device configured as the management default gateway.
- Main route table – Contains all routes whose next hop is connected to a data interface. These routes are sometimes referred to as data plane routes. Entries in this table are used for load balancing and Layer 3 forwarding on data ports.

You can configure the ACOS device to use the management interface as the source interface for automated management traffic. In addition, on a case-by-case basis, you can enable the use of the management interface and management route table for various types of management connections to remote devices.

The ACOS device automatically uses the management route table for reply traffic on connections initiated by a remote host that reaches the ACOS device on the management port. For example, this occurs for SSH or HTTP connections from remote hosts to the ACOS device.

Separating Management and Data Interfaces Across Networks

The management interface and the data interfaces must be in separate networks. If both tables have routes to the same destination subnet, some operations (for example, **ping**) may have unexpected results. An exception is the default route (0.0.0.0/0), which can be in both tables.

To display the routes in the management route table, use the **show ip route mgmt** command.

To display the data plane routes, use the **show ip route** or **show ip fib** commands.

Management Routing Options

You can configure the ACOS device to use the management interface as the source interface for the following management protocols, used for automated management traffic:

- SYSLOG
- SNMPD
- NTP
- RADIUS
- TACACS+
- SMTP

For example, when use of the management interface as the source interface for control traffic is enabled, all log messages sent to remote log servers are sent through the management interface. Likewise, the management route table is used to find a route to the log server. The ACOS device does not attempt to use any routes from the main route table to reach the server, even if a route in the main route table could be used.

In addition, on a case-by-case basis, you can enable use of the management interface and management route table for the following types of management connections to remote devices:

- Upgrade of the ACOS software
- SSH or Telnet connection to a remote host
- Import or export of files
- Export of **show techsupport** output
- Reload of black/white lists
- SSL loads (keys, certificates, and Certificate Revocation Lists)
- Copy or restore of configurations
- Backups

Management Interface as Source for Automated Management Traffic

By default, use of the management interface as the source interface for automated management traffic is disabled.

To enable it, use the **ip control-apps-use-mgmt-port** command at the configuration level for the management interface:

```
ACOS(config)# interface management
ACOS(config-if:management)# ip control-apps-use-mgmt-port
```

To ensure the TACACS authorization traffic follows the intended management plane route, configure either of the following option:

- Set the management interface as the source IPv6 address in the TACACS server configuration:

  ```
  ACOS(config)# tacacs-server host <tacacs-server_host_name> secret
  encrypted  <encrypted-secret-string> source ipv6 <ipv6_address>
  ```

- Add a static route through the management interface:

```
ACOS(config)# interface management
ACOS(config-if:management)# ipv6 address <ipv6_address>
ACOS(config-if:management)# exit
.
.
.
ACOS(config)# ipv6 route <tacacs-server_host_name> <ipv6_address>
```

Management Interface as Source for Manually Generated Management Traffic

To use the management interface as the source interface for manually generated management traffic, use the **use-mgmt-port** option as part of the command string. This option is available with certain file management commands, including the **import** command:

```
ACOS(config)# import ssl-cert-key bulk ?
  use-mgmt-port      Use management port as source port
  tftp:              Remote file path of tftp: file system(Format:
tftp://host/file)
  ftp:               Remote file path of ftp: file system(Format:
                     ftp://[user@]host[:port]/file)
  scp:               Remote file path of scp: file system(Format:
                     scp://[user@]host/file)
  sftp:              Remote file path of sftp: file system(Format:
                     sftp://[user@]host/file)
  NAME<length:1-31>  profile name for remote url
```

Loopback or Virtual Ethernet Interface as Source for Management Traffic

You can configure the ACOS device to use a loopback or virtual Ethernet interface IP address to be used as the source interface for management traffic originated by the device.

The following topics are covered:

Loopback Interface Management Traffic Types

You can enable use of a specific loopback interface as the source for one or more of the following management traffic types:

- FTP
- NTP
- RCP
- SNMP
- SSH
- SYSLOG
- Telnet
- TFTP
- Web

FTP, RCP, and TFTP apply to file export and import, such as image upgrades and system backups.

Telnet and SSH apply to remote login from the ACOS device to another device. They also apply to RADIUS and TACACS+ traffic. SSH also applies to file import and export using SCP.

Web applies to GUI login.

Loopback Interface Implementation Notes

Some notes to consider for loopback interfaces:

- Loopback interface IP address – The loopback interface you specify when configuring this feature must have an IP address configured on it. Otherwise, this feature does not take effect.
- Management interface – If use of the management interface as the source for management traffic is also enabled, the loopback interface takes precedence over the management interface. The loopback interface's IP address will be used instead of the management interface's IP address as the source for the management traffic. In conjunction, the **use-mgmt-port** CLI option will have no effect.
- Ping traffic – Configuration for use of a loopback interface as the source for management traffic does not apply to ping traffic. By default, ping packets are sourced from the best interface based on the ACOS route table. You can override the default interface selection by specifying a loopback or other type of interface as part of the **ping** command. (See the *Command Line Interface Reference* for syntax information.)

Limitations

The current release has the following limitations related to this feature:

- Floating loopback interfaces are not supported.
- IPv6 interfaces are not supported.

Configure Loopback Interface for Management Traffic

The following commands configure an IP address on loopback interface 2 in the shared partition:

```
ACOS(config)# interface loopback 2
ACOS(config-if:loopback:2)# ip address 10.10.10.66 /24
ACOS(config-if:loopback:2)# exit
```

The following command configures the device to use loopback interface 2 as the source interface for management traffic of all types:

```
ACOS(config)# ip mgmt-traffic all source-interface loopback 2
```

Configure Virtual Ethernet Interface for Management Traffic

The following commands configure virtual Ethernet interface 2 in the L3V partition called p1:

```
ACOS[p1](config)# vlan 2
ACOS[p1](config-vlan:2)# router-interface ve 2
ACOS[p1](config-if:ve2)# ip address 10.1.1.254 /24
ACOS[p1](config-if:ve2)# exit
```

The following command configures the device to use ve 2 as the source interface for management traffic in the p1 partition:

```
ACOS[p1](config)# ip mgmt-traffic traffic-type source-interface ve 2
```

NOTE:

- If the virtual Ethernet interface belongs to the shared vlan, then the shared virtual Ethernet interface IP address will be used. For example, if `vlan 2` above is also in the shared partition, the IP address `10.1.1.254 /24` will not be used for management traffic, but the IP address as configured for the virtual Ethernet in the shared partition will be used.
- See the *Configuring Application Delivery Partitions* guide for more information about partitions.

Dynamic and Block Configuration

In the classical (default) mode of the CLI, configuration commands take effect as they are entered. For example, `slb server s1 10.10.10.1` creates an SLB server "s1" with an IP address of 10.10.10.1 without having to take any further action.

Using the CLI or aXAPI, block configuration modes allow you to update portions of your configuration without having to take your ACOS device off-line or disrupting live traffic.

The following topics are covered:

Overview of Dynamic and Block Configuration

The Configuration Management Database (CMDB) allows for dynamic changes to be made to the running configuration using either the CLI or the aXAPI using the `cli.deploy` method. You enter a block configuration mode to create a new configuration file in the CMDB. ACOS compares the existing running configuration with this new file (your new configuration), which is considered the primary configuration. ACOS parses the commands in the new configuration file and rearranges them into an order in which the new commands will be applied so that live traffic is not disturbed.

For replicated configurations, the old configuration is left in place rather than removed and then re-entered.

During this process, some dependency checks may be disabled. After parsing the new configuration, ACOS will ensure that all dependency checks are passed and all configurations are complete and valid.

NOTE: This feature is not supported in the GUI. Multiple users cannot configure ACOS through the CLI. Concurrent aXAPI calls are possible although they will be queued.

Block Configuration Modes for CMDB

The following topics are covered:

Block-Merge Mode

In block-merge mode, existing elements edited in block-merge mode are replaced with your new definitions and then merged with the remaining configuration with **`block-merge-end`**.

If the running configuration is not committed before entering “block-merge” mode, then all changes made before and after “block-merge” mode are committed when you end “block-merge” mode.

NOTE: In this release, a setting to control the behavior of block-merge mode called merge mode is supported. In the merge mode, any child instances of the old configuration are retained if not present in the new configuration. The merge mode can be accessed using the merge-mode-add command from the Global configuration mode.

The following is an example showing how block-merge mode works. First, view the existing SLB configuration:

```
ACOS(config)# show run | sec slb
slb server s1 2.2.2.2
  port 80 tcp
    sampling-enable all
slb virtual-server vip1 1.1.1.1
  port 80 tcp
    sampling-enable curr_conn
    sampling-enable total_conn
ACOS(config)#
```

Next, edit the SLB server configuration to exclude the baselining configuration (**sampling-enable** command):

```
ACOS(config)# block-merge-start
Beginning merge mode. Enter configuration followed by 'block-merge-end' to
merge configuration into running.
ACOS(config)# slb server s1 2.2.2.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# block-merge-end
Configuration merged into running.
ACOS(config)#
```

View the running configuration again:

```
ACOS(config)# show run | sec slb
slb server s1 2.2.2.2
  port 80 tcp
```

```
slb virtual-server vip1 1.1.1.1
  port 80 tcp
    sampling-enable curr_conn
    sampling-enable total_conn
ACOS(config)#
```

The changes are merged into the existing running-config so that "**sampling-enable all**" is no longer part of the SLB real server configuration.

Block-Replace Mode

In block-replace mode, instead of individual SLB configuration elements, the entire SLB configuration gets discarded and replaced when the new configuration is committed with **block-replace-end**. The rest of the configuration remains intact.

All configurations before entering "block-replace" mode, whether committed or not, are removed unless they also are configured in "block-replace" mode.

Below is an example showing how block-replace mode works. First, view the existing SLB configuration:

```
ACOS(config)# show run | sec slb
slb server s1 2.2.2.2
  port 80 tcp
    sampling-enable all
slb virtual-server vip1 1.1.1.1
  port 80 tcp
    sampling-enable curr_conn
    sampling-enable total_conn
ACOS(config)#
```

Next, edit the SLB server configuration to exclude the SLB virtual server:

```
ACOS(config)# block-replace-start
Beginning replace mode. Enter configuration followed by 'block-replace-
end' to apply diff and replace configuration into running.
ACOS(config)# slb server s1 2.2.2.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# sampling-enable all
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# block-replace-end
```

```
Configuration replaced into running.
ACOS(config)#
```

View the running configuration again:

```
ACOS(config)# show run | sec slb
slb server s1 2.2.2.2
  port 80 tcp
    sampling-enable all
ACOS(config)#
```

The changes have completely replaced the existing SLB configuration; there is no longer an SLB virtual server configured.

Expected Behaviors in Block Mode

ACOS parses the configurations entered in block mode before it commits those changes. Any invalid command that results in a configuration error will void all of the block-mode configurations, and none of those changes will be made. The configuration will revert to the original running configuration. All configurations done in a block mode must succeed or else none of the configurations take effect.

If an undesired command or an erroneous command is entered in block mode, most of those can be removed using the **no** form of the command. However, using the CLI only, syntax errors will be ignored when the “block-replace” mode configuration is committed. If you run into a syntax error but still enter the **block-replace-end** command, then all valid configurations made in “block-replace” mode, prior to the syntax error, will still be committed and entirely replace the old running configuration. Using the aXAPI, if there is an error in both syntax and configuration while using the cli.deploy method, then ACOS will rollback to the original configuration. If an error is detected and ACOS reverts to the old running configuration, the configuration entered in block mode will be cleared.

To avoid erasing the old running configuration with an erroneous configuration entered in block mode, exit block mode using the **block-abort** command. This will erase all configuration commands entered in block mode and retain the old running configuration.

In block mode, you can view the current running configuration with the **show config** command. This is the same as the **show running-config** command in the classical

mode of the CLI. The changes you are currently making in block mode are not visible in the output of this command.

To view the configuration you are making in either “block-merge” or “block-replace” mode, enter the **`show config-block`** command.

Block Configuration Modes for aFleX

aFleX can also be configured in-line within block-merge and block-replace mode. Within the CLI, you enter the command **`aflex-scripts start`** to enter the aFleX configuration mode. aFleX commands should be entered in-line following that. When you are finished, simply enter a period (.) to indicate the end of the aFleX commands to be committed. All of these commands should be entered within the “block-merge” or “block-replace” mode in order for the aFleX commands to take effect.

Like the “block-merge” and “block-replace” mode in the CLI, the application of the aFleX commands is dependent on all features passing. One failed command will mean that not of the commands are entered into the running configuration.

To enter aFleX commands in-line within “block-merge” or “block-replace” mode, enter the following command at the block configuration level:

```
aflex-scripts start
```

Each aFlex can then be entered using the convention where the header contains `<aflex-script aflexName`, followed by the actual aFleX and then a closing bracket (>). A period is used to indicate the end of all scripts.

```
<aflex-script aflexName
aflex code {
...
}
>
```

To indicate the end of all the aFleX commands, enter the following symbol at the end of the aFleX commands:

```
.
```

To view all aFleX commands as part of the running configuration, enter the `running-config display aflex` global configuration command in the CLI, then enter the `show running-config` command.

Boot Options

This chapter describes how to display or change the storage area from which the ACOS device boots.

The following topics are covered:

NOTE: This chapter does not describe how to upgrade the system image. For upgrade instructions, see the "*Release Notes*" for the release to which you plan to upgrade.

Storage Areas

The ACOS device has four storage areas (also called “image areas”) that can contain software images and configuration files:

- Primary storage on the Solid State Drive (SSD) or disk
- Secondary storage on the SSD or disk
- Primary storage on the compact flash (CF)
- Secondary storage on the compact flash

NOTE: Not all storage areas are available on all devices.

The SSD or disk storage areas are used for normal operation. The compact flash storage areas are used only for system recovery.

NOTE: In this document, references to SSD can refer to the hard disk in some older ACOS devices.

Normally, each time the ACOS device is rebooted, the device uses the same storage area that was used for the previous reboot. For example, if the primary storage area of the SSD or disk was used for the previous reboot, the system image and startup-config from the primary storage area are used for the next reboot.

Unless you change the storage area selection or interrupt the boot sequence to specify a different storage area, the ACOS device always uses the same storage area each time the device is rebooted.

NOTE: The ACOS device always tries to boot using the SSD or disk first. The compact flash is used only if the SSD or hard disk is unavailable. If you need to boot from compact flash for system recovery, contact A10 Networks.

The following topics are covered:

Current Storage Information

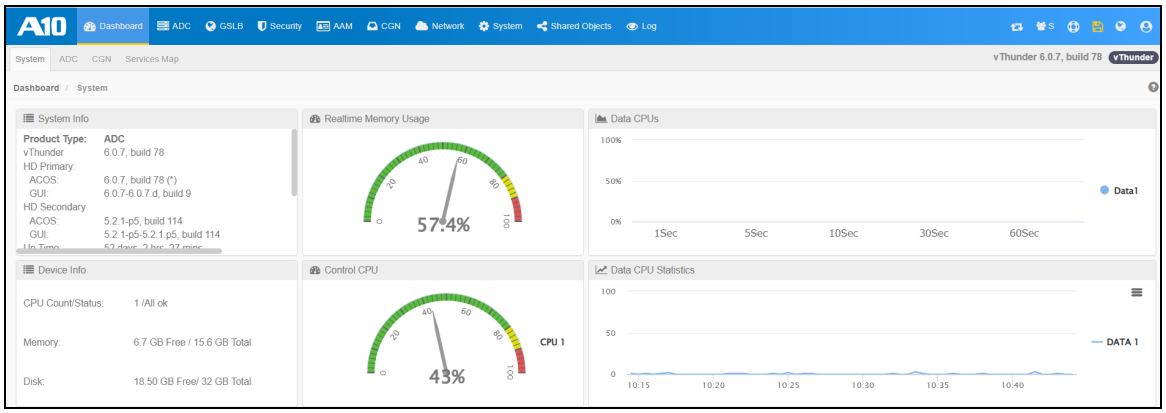
To display the software images installed in the ACOS storage areas, and the currently running software version, use either of the following methods:

The following topics are covered:

View Storage Information Using GUI

Navigate to **System > Dashboard** in the GUI (see the Figure 9).

Figure 9 : System Dashboard in the GUI



The field at upper left, in the System Info area, shows the software version that is currently running.

The system info is also displayed in the top right corner of every page. Hover over the link to display the same system info as shown on the Dashboard.

View Storage Information Using CLI

The **`show version`** command shows storage area information. The command also lists other information, including the currently running software version.

```
ACOS# show version
Thunder Series Unified Application Service Gateway vThunder
  Copyright 2007-2015 by A10 Networks, Inc.  All A10 Networks products are
```

```
  protected by one or more of the following US patents:
  Copyright 2007-2025 by A10 Networks, Inc.  All A10 Networks products are
  protected by one or more of the following US patents:
  10749904, 10742559, 10735267, 10708150, 10686683, 10659354, 10637717
  10630784, 0623992,  RE47924,  10601788, 10599680, 10594600, 10581976
  10581907, 10554517, 10536517, 10536481, 10530847, 10523748, 10516730
  10516577, 10505984, 10505964, 10491523, 10484465, 10469594, 10454844
  10447775, 10411956, 10397270, 10389835, 10389538, 10382562, 10360365
  10348631, 10341427, 10341335, 10341118, 10334030, 10318288, 10305904
  10305859, 10298457, 10268467, 10257101, 10250629, 10250475, 10243791
  RE47296,  10230770, 10187423, 10187377, 10178165, 10158627, 10129122
  10116634, 10110429, 10091237, 10069946, 10063591, 10044582, 10038693
  10027761, 10021174, 10020979, 10002141, 9992229,  9992107,  9986061
  9979801, 9979665, 9961136, 9961135, 9961130, 9960967, 9954899, 9954868
  9942162, 9942152, 9912555, 9912538, 9906591, 9906422, 9900343, 9900252
  9860271, 9848013, 9843599, 9843521, 9843484, 9838472, 9838425, 9838423
  9825943, 9806943, 9787581, 9756071, 9742879, 9722918, 9712493, 9705800
  9661026, 9621575, 9609052, 9602442, 9596286, 9596134, 9584318, 9544364
  9537886, 9531846, 9497201, 9477563, 9398011, 9386088, 9356910, 9350744
  9344456, 9344421, 9338225, 9294503, 9294467, 9270774, 9270705, 9258332
  9253152, 9231915, 9219751, 9215275, 9154584, 9154577, 9124550, 9122853
  9118620, 9118618, 9106561, 9094364, 9060003, 9032502, 8977749, 8943577
  8918857, 8914871, 8904512, 8897154, 8868765, 8849938, 8826372, 8813180
  8782751, 8782221, RE44701, 8595819, 8595791, 8595383, 8584199, 8464333
  8423676, 8387128, 8332925, 8312507, 8291487, 8266235, 8151322, 8079077
  7979585, 7804956, 7716378, 7665138, 7675854, 7647635, 7627672, 7596695
  7577833, 7552126, 7392241, 7236491, 7139267, 6748084, 6658114, 6535516
  6363075, 6324286, 8392563, 8103770, 7831712, 7606912, 7346695, 7287084
  6970933, 6473802, 6374300
           64-bit Advanced Core OS (ACOS) version 6.0.7, build 78 (Apr-14-
2025,04                              :20)
           Booted from Hard Disk primary image
           Number of control CPUs is set to 1
           Serial Number: vThunder815D1ED2DBCAF581AE67A355E942BCF55287AB4D
           aFleX version: 2.0.0
           GUI primary image (default) version 6_0_7-6_0_7-d-9
           GUI secondary image version 5_2_1-p5-5_2_1-p5-114
           aXAPI version: 3.0
           Hard Disk primary image (default) version 6.0.7, build 78
           Hard Disk secondary image version 5.2.1-p5, build 114
```

```
            Last configuration saved at May-15-2025, 07:01
            Virtualization type: KVM
            System Polling Mode: On
            Build Type: Internal
            Hardware: 1 CPUs(Stepping 1), Single 32G drive, Free storage is
18G
            Total System Memory 15989 Mbytes, Free Memory 6525 Mbytes
            Hardware Manufacturing Code: N/A
            Current time is Aug-8-2025, 10:50
            The system has been up 52 days, 2 hours, 34 minutes
ACOS#
```

Storage Location for Future Reboots

To display the storage area that will be used for the future reboots, use either of the following methods.

NOTE: The ACOS device always tries to boot using the SSD or disk first. The compact flash is used only if the SSD or hard disk is unavailable. If you need to boot from compact flash for system recovery, contact A10 Networks.

The following topics are covered:

View Storage Location for Future Reboots Using GUI

1. Hover over **System** in the navigation bar, and select **Settings**.
2. Click **Boot Image** on the menu bar.

View Storage Location for Future Reboots Using CLI

Use the **`show bootimage`** command to view the storage location for future reboots.

In the following example, the ACOS device is configured to boot from the primary storage area on the SSD or disk:

```
ACOS# show bootimage
```

```
(* = Default)
                            Version
-------------------------------------------------
Hard Disk primary           6.0.7.78 (*)
Hard Disk secondary         5.2.1-p5.114
```

Booting from Different Storage Area

The ACOS device allows you to change the boot device from the primary image to the secondary image on a single storage device, either the SSD, hard disk, or the CF. You can use the CLI or the GUI to make the change from the primary image to the secondary image or vice versa. However, if you are choosing to change the boot device from the SSD (hard disk) to the CF (Compact Flash) you have to interrupt the boot sequence to do so. Both boot devices, SSD (hard disk) and CF, contain their own primary and secondary boot locations.

To reboot from a different image within the same storage device (SSD or CF), do one of the following:

- Interrupt the boot sequence and use the bootloader menu to temporarily select the other storage area.
- Configure the ACOS device to use the other storage area for all future reboots, then reboot.

The following topics are covered:

Temporarily Boot from Secondary Image on ACOS Device

To temporarily change the storage location within the same boot device (SSD or CF) from the primary to the secondary image, interrupt the boot sequence to access the bootloader menu.

To access the bootloader menu, reboot the ACOS device, then press Esc within 3 seconds when prompted.

When the bootloader menu appears, use the Up and Down arrow keys to select the image area from which to boot, and press Enter. The menu does not automatically time out. You must press Enter to reboot using the selected image.

CAUTION: Each storage area has its own version of the startup-config. When you save configuration changes, they are saved only to the startup-config in the storage area from which the ACOS device was booted.

CAUTION: If you plan to reboot from a different storage area, but you want to use the same configuration, first save the configuration to the other storage area. (The procedures in Permanently Change Storage Area for Future Reboots include steps for this.)

NOTE: The bootloader menu is available on all new ACOS devices. To install the bootloader menu on upgraded devices, see the description of the **`boot-block-fix`** command in the *Command Line Interface Reference*.

```
ACOS# reboot
Rebooting System Now !!!
Proceed with reboot? [yes/no]:yes
INIT:

Shutting down.........Restarting system.
Press `ESC' to enter the boot menu... 1
  Admin presses Esc within 3 seconds.


   #       #      ###      #      #
  # #     ##     #   #     ##     # ###### ##### #     #   ####   #####   #     #
####
 #   #  # #    #      #    # #    # #         #    #     # #     # #     # #    #   #
#     #    #    #      #    #   #  # #####     #    #     # #     # #     # ####
####
#######    #    #      #    #    # # #         #    # ## # #     # #####   #   #
   #
#     #    #    #    #    #    ## #         #    ##   ## #     # #    #   #    #   #
   #
```

```
#     # #####   ###     #     # ######   #   #    #  ####  #    # #    #
####

Copyright 2005-2015 by A10 Networks, Inc.  All A10 Networks products are
protected by one or more of the following US patents and patents pending:
7716378, 7675854, 7647635, 7552126, 20090049537, 20080229418, 20080040789,
20070283429, 20070271598, 20070180101
--------------------------------------------------------------------
 0: ACOS (Primary Image)
 1: ACOS (Secondary Image)
--------------------------------------------------------------------

Use the Up and Down arrow keys to select the image from which to boot.
Press enter to boot the selected image.

  Admin presses down arrow to select 1.

    Highlighted entry is 1:

  Admin presses Enter to reboot using the selected image.

Booting 'ACOS (Secondary Image)'
Please wait while the system boots...

Booting.....................[OK]

ACOS login:
```

Permanently Change Storage Area for Future Reboots

This section describes how to change the storage area that will be used for future reboots:

NOTE: The procedures in this section change the storage area selection for all future reboots (unless you later change the selection again). If you only need to temporarily override the storage area selection for a single reboot, see Temporarily Boot from Secondary Image on ACOS Device.

CAUTION: Each storage area has its own version of the startup-config. When you save configuration changes, they are saved only to the startup-config in the storage area from which the ACOS device was booted.

CAUTION: If you plan to reboot from a different storage area, but you want to use the same configuration, first save the configuration to the other storage area. The procedures in this section include a step for this.

The following topics are covered:

Change Storage Area for Reboots Using GUI

To change the location that will be used for future reboots from the GUI:

1. Hover over **System** in the menu bar, then select **Settings**.
2. Select the **Boot Image** tab.
3. On the Boot Image page, select the location from which the device will be rebooted in the future.
4. Click **OK**.

Change Storage Area for Reboots Using CLI

In this example, the ACOS device was booted from the primary storage area, and will be configured to use the secondary image area for future reboots.

1. Use **show bootimage** to view the current storage area being used for reboots:

```
ACOS# show bootimage
(* = Default)
                            Version
-----------------------------------------------
Hard Disk primary           6.0.7.78 (*)
Hard Disk secondary          5.2.1-p5.114
```

The asterisk (*) indicates that when the system is booted from the hard disk, version 4.1.0.141 will be loaded.

2. Use the **write memory** command to save the configuration, then use the **write memory secondary** command to copy it to the secondary storage area:

```
ACOS(config)# write memory
Building configuration...
Write configuration to primary default startup-config
[OK]
ACOS(config)# write memory secondary
Building configuration...
Write configuration to secondary default startup-config
[OK]
```

3. Use **bootimage** to set the secondary storage area on the SSD or hard drive for future reboots, and verify the setting:

```
ACOS(config)# bootimage hd sec
Secondary image will be used if system is booted from hard disk
ACOS(config)# show bootimage
(* = Default)
                          Version
-----------------------------------------------
Hard Disk primary          6.0.7.78
Hard Disk secondary       5.2.1-p5.114 (*)
```

The asterisk (*) now indicates that the device will be booted from the secondary image on the hard disk.

Power On Auto Provisioning

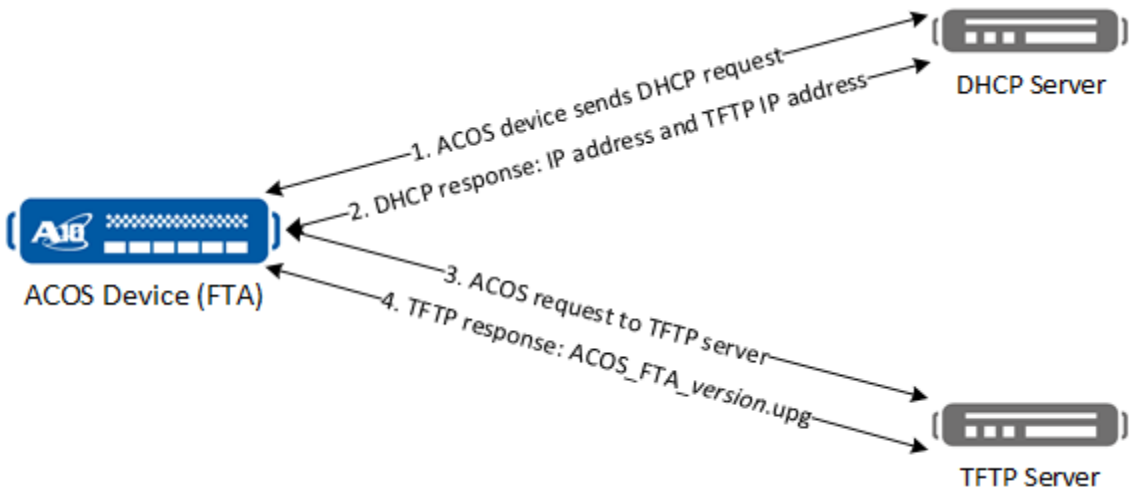
The ACOS Power On Auto Provisioning (POAP) feature offers an efficient way to automate the process of upgrading software images or config file across many ACOS devices on the network.

Use of this feature requires a DHCP server and a TFTP server that has been pre-configured with the proper ACOS software image and config file. The ACOS device must have access to the management port on a DHCP server and access to the TFTP server.

Provisioning Process

The following Figure 10 shows how the POAP process works.

Figure 10 : Power On Auto Provisioning Process



1. The ACOS device boots and sends a broadcast request to the DHCP server.
2. The DHCP server sends a response that includes an IP address for the ACOS device, and an IP address where the TFTP server can be reached.
3. The ACOS device attempts to locate the TFTP server at the IP address it just received from the DHCP server by sending a request to that address.

4. The TFTP server responds to the request from the ACOS device by sending the upgrade file (ACOS_FTA_*version*.upg for FTA devices, or ACOS_non_FTA_ *version*.upg for non-FTA devices).

   Once the ACOS device receives the upgrade file, it performs the following operations:

   - Extracts the upgrade image and configuration file.
   - Upgrades its software using the new image.
   - Links to the configuration file.
   - Then, the ACOS device reboots.

Feature Description

POAP features and the use cases are as follows:

1. POAP is enabled at power on by default

   The customer orders 10 new devices and wants to install them in remote facilities. The customer doesn't have staff at the facility and is relying on the “smart-hands” service. Configuring POAP and power on enables the customer to have the smart-hands rack and connect the box.

2. Capability for referencing configuration and image files by name

   Customer has a pair of FTA devices and a pair of FTA3 devices. Each device requires a new “poap_startup” script and at least one upgrade image “swap”. On the other hand, if devices can POAP and request specific startup scripts and upgrade images based on a unique device ID (such as a serial number), then all files can be prepared (built or linked) in advance allowing all devices to POAP simultaneously.

3. Verbose console logging

   Dropbox is changing their workflow to use significantly more automatic provisioning. Part of the auto-provisioning is automated inspection of the onlining of new devices to determine success or failure of provisioning. Dropbox is currently using a monitoring process that inspects mirrored console output

and determines success status. The console output is used as a success or a failure flag.

4. DHCP client functionality from all interfaces at power on

   The customer does not want to pay for design with a separate management network. The customer also wants to use POAP which requires DHCP. Customer may not know the ports that gets connected to the network in advance. Therefore, POAP can act as a DHCP client on all the interfaces.

5. Multiple file transfer protocol support

   Devices in several remote Data Centers need to be POAP provisioned from a server located at a central location (i.e. HQ) potentially traversing firewalls. TFTP would be non-trivial to make work in this setting.

   Use of this feature requires a DHCP server and a TFTP server that has been pre-configured with the proper ACOS software image and config file. The ACOS device must have access to the management port on a DHCP server and access to the TFTP server.

Configure POAP

The following are the prerequisites before using POAP:

- Create an upgrade package named "**acos_upg.tgz**".

  The package may contain one or both of the following optional files:

  - Image file: "**sto.tar.gz**"
  - Config file: "**poap_startup**"

- Save this upgrade package on a TFTP server that can be accessed by the ACOS device. This package should be stored in the working directory of the TFTP server, (for example, "**tftpboot**").
- To enter POAP mode, the current startup-config file on the ACOS device must be empty; if the startup-config file is not completely empty then the POAP install will fail.

- At the end of the installation process, POAP links to the new startup-config file, which is a text file named "**poap_startup**".

NOTE:

- The POAP installation process does not erase an existing startup-config file, but as a precaution, you can save an existing startup-config file by creating a backup prior to enabling POAP.
- If the ACOS device encounters an existing file named "**poap_startup**" on the ACOS device (perhaps a remnant left over from a prior attempt to enable the feature), the POAP installation process will rename this existing file "**poap_startup.original**".

By default, POAP mode is enabled on all Thunder devices.

NOTE: POAP Mode is not available on the virtual platform.

To enable POAP mode on a physical device, use the **poap enable** command at the Global configuration level of the CLI.

Use the **poap disable** command to disable the feature.

You can use the **show poap** command to show the status (enabled or disabled) of POAP mode:

```
ACOS# show poap
POAP Mode Enabled
ACOS#
```

System Logs and Error Messages

System logs and error messages appear in the following scenarios:

- The startup-config profile "**poap_startup**" exists and new "**poap_startup**" gets installed with the POAP package.
- The link fails or the link is successful.
- The upgrade fails or the upgrade is successful.

Fail-Safe Automatic Recovery

Fail-safe automatic recovery detects critical hardware and software error conditions. The feature also automatically takes action to recover the system if any of these errors occurs, so that the ACOS device can resume service to clients.

Fail-safe automatic recovery is disabled by default, for both hardware and software errors. You can enable the feature for hardware errors, software errors, or both.

The following topics are covered:

Error Types Monitored by Automatic Recovery

Fail-safe automatic recovery monitors and recovers from the following types of system error conditions:

- Hardware Errors
- Software Errors
- Recovery Timeout
- Total Memory Decrease

Hardware Errors

When fail-safe monitoring is enabled for hardware errors, the following types of errors are detected:

- SSL processor stops working – Fail-safe is triggered if an SSL processor stops working.
- Compression processor stops working – Fail-safe is triggered if an HTTP compression processor stops.
- FPGA stops working – Fail-safe is triggered if either of these internal queues stops working.

If any of these types of errors occurs, the ACOS device captures diagnostic information, then reboots.

NOTE: Fail-safe recovery also can be triggered by a “PCI not ready” condition. This fail-safe recovery option is enabled by default and can not be disabled.

Software Errors

When fail-safe monitoring is enabled for software errors, the following types of errors are detected:

- FPGA I/O buffer shortage – The number of free (available) packet buffers is below the configured threshold. By default, at least 512 packet buffers must be free for new data. (Monitoring for this type of FPGA error is applicable to all ACOS device models.)

  On ACOS device models that use FPGA hardware, the FPGA is logically divided into 2 domains, which each have their own buffers. If an FPGA buffer shortage triggers fail-safe, recovery occurs only after both domains have enough free buffers.

- Session memory shortage – The amount of system memory that must be free for new sessions is below the configured threshold. By default, at least 30 percent of the ACOS device's session memory must be free for new sessions.

In VRRP-A deployments, fail-safe recovers from software errors by triggering failover to a standby device. To trigger the failover, fail-safe enables the force-self-standby option.

NOTE: Fail-safe temporarily enables the force-self-standby option. The **`vrrp-a force-self-standby`** command is not added to the running-config.

If VRRP-A is not enabled, fail-safe reloads the ACOS device.

Recovery Timeout

The recovery timeout is the number of minutes the ACOS device waits after detecting one of the hardware or software errors above before recovering the system.

- Recovery timeout for hardware errors – By default, the ACOS device reboots as soon as it has gathered diagnostic information. Typically, this occurs within 1 minute of detection of the error (no timeout). You can change the recovery timeout for hardware errors to 1-1440 minutes.
- Recovery timeout for software errors – Fail-safe waits for the system to recover through normal operation, before triggering a recovery. The default recovery timeout for software errors is 3 minutes. You can change it to 1-1440 minutes.

Total Memory Decrease

At device reload or reboot, the fail-safe feature provides a mechanism to check the total memory decrease when the ACOS device boots up and loads the startup configuration. If the total memory size has decreased, and if the size is less than the configured memory size, a message will be logged (if you have configured the **log** option) or the ACOS device will shut down after logging a message (if you have configured the **kill** option).

When the configured expected physical memory size is larger than the current memory size, a reboot or log message recording the discrepancy will be triggered. The device will remain always in a “loading” state after it reboots or reloads.

Configure Fail-Safe Automatic Recovery

The following CLI commands configure some fail-safe settings and verify the changes.

Trigger the fail-safe recovery if the amount of free memory on your system remains below 30% long enough for the recovery timeout to occur:

```
ACOS(config)# fail-safe session-memory-recovery-threshold 30
```

Trigger the fail-safe recovery if the number of free (available) FPGA buffers drops below 2 long enough for the recovery timeout to occur:

```
ACOS(config)# fail-safe fpga-buff-recovery-threshold 2
```

Trigger the fail-safe recovery if a software error remains in effect for longer than 3 minutes:

```
ACOS(config)# fail-safe sw-error-recovery-timeout 3
```

Verify the configuration:

```
ACOS(config)# show fail-safe config
fail-safe session-memory-recovery-threshold 30
fail-safe fpga-buff-recovery-threshold 2
fail-safe sw-error-recovery-timeout 3
```

The **show fail-safe** command output differs between models that use FPGAs in hardware and models that do not. The following command shows fail-safe settings and statistics on an ACOS device model that uses FPGAs in hardware:

```
ACOS(config)# show fail-safe information
Total Session Memory (2M blocks):                  1012
Free Session Memory (2M blocks):                   1010
Session Memory Recovery Threshold (2M blocks):     809
Total Configured FPGA Buffers (# of buffers):      4194304
Free FPGA Buffers in Domain 1 (# of buffers):      507787
Free FPGA Buffers in Domain 2 (# of buffers):      508078
Total Free FPGA Buffers (# of buffers):            1015865
FPGA Buffer Recovery Threshold (# of buffers):     256
Total System Memory (Bytes):                       2020413440
```

The Table 5 describes the fields in the command output.

Table 5 : show Fail-safe Information Fields (FPGA Models)

Field	Description
Total Session Memory	Total amount of the ACOS device's memory that is allocated for session processing.
Free Session Memory	Amount of the ACOS device's session memory that is free for new sessions.
Session Memory Recovery Threshold	Minimum percentage of session memory that must be free before fail-safe occurs.
Total Configured FPGA Buffers	Total number of configured FPGA buffers the ACOS device has. These buffers are allocated when the ACOS device is booted. This number does not change during system operation. The FPGA device is logically divided into 2 domains, which each have their own buffers. The next two counters are for these logical FPGA domains.
Free FPGA Buffers in Domain 1	Number of FPGA buffers in Domain 1 that are currently free for new data.
Free FPGA Buffers in Domain 2	Number of FPGA buffers in Domain 2 that are currently free for new data.
Total Free FPGA Buffers	Total number of free FPGA buffers in both FPGA domains.
FPGA Buffer Recovery Threshold	Minimum number of packet buffers that must be free before fail-safe occurs.

Table 5 : show Fail-safe Information Fields (FPGA Models)

Field	Description
Total System Memory	Total size the ACOS device's system memory.

The following command shows fail-safe settings and statistics on an ACOS device model that does not use FPGAs in hardware. (The FPGA buffer is an I/O buffer instead.)

```
ACOS(config)# show fail-safe information
Total Session Memory (2M blocks):                    1018
Free Session Memory (2M blocks):                     1017
Session Memory Recovery Threshold (2M blocks):       305
Total Configured FPGA Buffers (# of buffers):        2097152
Free FPGA Buffers (# of buffers):                    2008322
FPGA Buffer Recovery Threshold (# of buffers):       1280
Total System Memory (Bytes):                         4205674496
```

The Table 6 describes the fields in the command output.

Table 6 : show Fail-safe Information Fields (non-FPGA models)

Field	Description
Total Session Memory	Total amount of the ACOS device's memory that is allocated for session processing.
Free Session Memory	Amount of the ACOS device's session memory that is free for new sessions.
Session Memory Recovery Threshold	Minimum percentage of session memory that must be free before fail-safe occurs.
Total Configured FPGA Buffers	Total number of configured FPGA buffers the ACOS device has. These buffers are allocated when the ACOS device is booted. This number does not change during system operation.
Free FPGA Buffers	Number of FPGA that are free for new data.
FPGA Buffer Recovery Threshold	Minimum number of packet buffers that must be free before fail-safe occurs.
Total System Memory	Total size the ACOS device's system memory.

Example of Fail-safe for Total Memory Decrease

In the following example, 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:

```
ACOS(config)# fail-safe total-memory-size-check 5 log
```

The following example helps you decipher if you have a problem with your system memory.

Use the **show version** command to see the current memory size of your system. The current memory is shown as highlighted:

```
ACOS# show version
Thunder Series Unified Application Service Gateway vThunder
Copyright 2007-2015 by A10 Networks, Inc. All A10 Networks products are
protected by one or more of the following US patents:
Copyright 2007-2025 by A10 Networks, Inc. All A10 Networks products are
protected by one or more of the following US patents:
10749904, 10742559, 10735267, 10708150, 10686683, 10659354, 10637717
10630784, 0623992, RE47924, 10601788, 10599680, 10594600, 10581976
10581907, 10554517, 10536517, 10536481, 10530847, 10523748, 10516730
10516577, 10505984, 10505964, 10491523, 10484465, 10469594, 10454844
10447775, 10411956, 10397270, 10389835, 10389538, 10382562, 10360365
10348631, 10341427, 10341335, 10341118, 10334030, 10318288, 10305904
10305859, 10298457, 10268467, 10257101, 10250629, 10250475, 10243791
RE47296, 10230770, 10187423, 10187377, 10178165, 10158627, 10129122
10116634, 10110429, 10091237, 10069946, 10063591, 10044582, 10038693
10027761, 10021174, 10020979, 10002141, 9992229, 9992107, 9986061
9979801, 9979665, 9961136, 9961135, 9961130, 9960967, 9954899, 9954868
9942162, 9942152, 9912555, 9912538, 9906591, 9906422, 9900343, 9900252
9860271, 9848013, 9843599, 9843521, 9843484, 9838472, 9838425, 9838423
9825943, 9806943, 9787581, 9756071, 9742879, 9722918, 9712493, 9705800
9661026, 9621575, 9609052, 9602442, 9596286, 9596134, 9584318, 9544364
9537886, 9531846, 9497201, 9477563, 9398011, 9386088, 9356910, 9350744
9344456, 9344421, 9338225, 9294503, 9294467, 9270774, 9270705, 9258332
9253152, 9231915, 9219751, 9215275, 9154584, 9154577, 9124550, 9122853
9118620, 9118618, 9106561, 9094364, 9060003, 9032502, 8977749, 8943577
8918857, 8914871, 8904512, 8897154, 8868765, 8849938, 8826372, 8813180
8782751, 8782221, RE44701, 8595819, 8595791, 8595383, 8584199, 8464333
8423676, 8387128, 8332925, 8312507, 8291487, 8266235, 8151322, 8079077
```

```
7979585, 7804956, 7716378, 7665138, 7675854, 7647635, 7627672, 7596695
7577833, 7552126, 7392241, 7236491, 7139267, 6748084, 6658114, 6535516
6363075, 6324286, 8392563, 8103770, 7831712, 7606912, 7346695, 7287084
6970933, 6473802, 6374300
         64-bit Advanced Core OS (ACOS) version 6.0.7, build 78 (Apr-14-
2025,04 :20)
         Booted from Hard Disk primary image
         Number of control CPUs is set to 1
         Serial Number: vThunder815D1ED2DBCAF581AE67A355E942BCF55287AB4D
         aFleX version: 2.0.0
         GUI primary image (default) version 6_0_7-6_0_7-d-9
         GUI secondary image version 5_2_1-p5-5_2_1-p5-114
         aXAPI version: 3.0
         Hard Disk primary image (default) version 6.0.7, build 78
         Hard Disk secondary image version 5.2.1-p5, build 114
         Last configuration saved at May-15-2025, 07:01
         Virtualization type: KVM
         System Polling Mode: On
         Build Type: Internal
         Hardware: 1 CPUs(Stepping 1), Single 32G drive, Free storage is
18G
         Total System Memory 18155 Mbytes, Free Memory 12551 Mbytes
         Hardware Manufacturing Code: N/A
         Current time is Aug-8-2025, 10:50
         The system has been up 52 days, 2 hours, 34 minutes
ACOS#
```

The current system memory is shown as 12G. In case you configure the fail-safe memory monitoring to be 5G, as shown below, your system will continue to operate normally, since 5G of memory is less than the 12G of memory that your device has at its disposal:

```
ACOS(config)# fail-safe total-memory-size-check 5 kill
```

However, if you use the above command and configure a memory size of 14G (and you save your configuration by issuing the **write memory** command) since 14G exceeds your current device memory size of 12G, your device will experience a problem. When the device reloads, the fail-safe mechanism will be triggered, traffic will be stopped, and the device will be shut down. The abnormal state of the device will be evident in the following log message:

```
[SYSTEM]:Current memory size 12G, less than monitor number 14G. Please
check memory.
```

To correct this issue, use the **`fail-safe total-memory-check`** *`size`* **`kill`** command and specify a memory size that is less than or equal to the current memory size. The next time your device reloads, it will operate normally.

Jumbo Frames on ACOS Devices

A jumbo frame is an Ethernet frame that is more than 1522 bytes long. Support for jumbo frames is offered on Layer 4 VIPs.

By default, the maximum transmission unit (MTU) on all physical Ethernet interfaces is 1500 bytes. The default Ethernet frame size is 1522 bytes, which includes 1500 bytes for the payload, 14 bytes for the Ethernet header, 4 bytes for the CRC, and 4 bytes for a VLAN tag. Jumbo support is disabled by default.

Additional Notes

- Jumbo frame support is not available on all platforms. See the *Release Notes* for a list of supported platforms.
- Jumbo frame support is disabled by default. You can enable jumbo frame support on a global basis for the device.
- The maximum transmission unit (MTU) is not automatically changed on any of the interfaces and must be explicitly configured on those interfaces that will be used for jumbo frames; this can be done using either the GUI or the CLI.
- On non-FTA models, you can increase the MTU on individual Ethernet interfaces up to 9216 bytes.
- Jumbo frames (L4) are supported on most 64-bit models and are not supported on 32-bit models.
- If your configuration uses VEs, you must enable jumbo on the individual Ethernet ports first, then enable it on the VEs that use the ports. If the VE uses more than port, the MTU on the VE should be the same or smaller than the MTU on each port.
- It is not recommended to enable jumbo frame support on 10/100 Mbps ports.
- Setting the MTU on an interface indirectly sets the frame size of incoming packets to the same value. (This is the maximum receive unit [MRU]).

The following topics are covered:

Configure Jumbo Frame Support

This section describes how to configure jumbo frame support on your ACOS device:

The following topics are covered:

Configure Jumbo Frame Using GUI

The following topics are covered:

Change MTU on Interface

To change the MTU on an interface:

1. Hover over **Network** in the navigation bar, and select **Interfaces**.
2. Check the menu bar to confirm you're on the LAN page.
3. Click **Edit** in the Actions column for any interface you choose to apply the jumbo frame config.
4. In the General Fields section, edit the value in the **MTU** field.
5. Click **Update**.

Disable Jumbo Support

To disable jumbo frame support:

1. Hover over **Network** in the navigation bar, and select **Interfaces**.
2. Check the menu bar to confirm you're on the LAN page.
3. Click **Edit** in the Action column for the interface number. The configuration page for the interface appears.
4. Edit the value in the MTU field to be 1500 (or less).

5. Click **Update**.
6. Repeat for each interface on which the MTU is greater than 1500 bytes.
7. On non-FTA platforms, you must also save your configuration and reboot the device:
   a. Hover over **System** in the navigation bar, and select **Settings**.
   b. Click **Actions** on the menu bar.
   c. In the Action field, select **Reboot** from the drop-down list.
   d. In the Save configuration field, select **Yes** from the drop-down list.
   e. Click **OK**.

CAUTION: On non-FTA models, you must save the configuration and reboot after changing the MTU settings to disable jumbo frame support. If you reload or reboot without first saving the configuration, the feature cannot be re-enabled until you first repeat the procedure above to disable it. Then, you can re-enable the feature.

Configure Jumbo Frame Using CLI

The following topics are covered:

Global Jumbo Frame Support on ACOS Device

This section describes how to enable jumbo-frame support globally. This can only be done via the CLI and not through the GUI.

This topic has the following sections:

- Enabling Jumbo Frame Support (FTA Models)
- Enabling Jumbo Support (Non-FTA Models)

Enabling Jumbo Frame Support (FTA Models)

To enable jumbo frame support on FTA models, use the following command:

```
ACOS(config)# system-jumbo-global enable-jumbo
```

Enabling Jumbo Support (Non-FTA Models)

To enable jumbo frame support on a non-FTA model, enter the following series of commands:

```
ACOS(config)# system-jumbo-global enable-jumbo
ACOS(config)# write memory
Building configuration...
Write configuration to primary default startup-config
[OK]
ACOS(config)# reboot
```

Change MTU on Interface

To change the MTU on an interface, use the **mtu** command at the configuration level for the interface. For example:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# mtu 1500
```

Create and Apply TCP-proxy Template to VIP

To create a TCP-proxy template and apply it to a VIP, use the following commands:

```
ACOS(config)# slb template tcp-proxy mss-size
ACOS(config-tcp proxy)# mss 1460
ACOS(config)# slb virtual-server vs1
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)# template tcp-proxy mss-size
```

Disable Jumbo Frame Support

This section describes how to globally disable jumbo frame support.

This topic has the following sections:

- Disable Jumbo Frame Support (FTA Models)
- Disable Jumbo Support (non-FTA Models)

Disable Jumbo Frame Support (FTA Models)

To disable jumbo frame support on FTA models, use the following command:

```
ACOS(config)# no system-jumbo-global enable-jumbo
```

Disable Jumbo Support (non-FTA Models)

To disable jumbo frame support on a non-FTA model, enter the following series of commands:

```
ACOS(config)# no system-jumbo-global enable-jumbo
ACOS(config)# write memory
Building configuration...
Write configuration to primary default startup-config
[OK]
ACOS(config)# reboot
```

CAUTION: On non-FTA models, you must save the configuration and reboot after entering the **`no system-jumbo-global enable-jumbo`** command. If you reload or reboot without first saving the configuration, the feature can not be re-enabled until you first repeat the procedure above to disable it. Then, you can re-enable the feature.

MTU Interface Settings

The following commands show detailed information for the interfaces, which includes the MTU settings:

```
ACOS(config)# show interface ve 10
VirtualEthernet 10 is up, line protocol is up
  Hardware is VirtualEthernet, Address is 001f.a004.c0e2
```

```
  Internet address is 110.10.10.1, Subnet mask is 255.255.255.0
  IPv6 address is 2001:10::241 Prefix 64 Type: unicast
  IPv6 link-local address is fe80::21f:a0ff:fe04:c0e2 Prefix 64 Type:
unicast
  Router Interface for L2 Vlan 10
  IP MTU is 1500 bytes
  28 packets input  2024 bytes
  Received  0 broadcasts, Received 24 multicasts, Received 4 unicasts
  10 packets output  692 bytes
  Transmitted  8 broadcasts, Transmitted 2 multicasts, Transmitted 0
unicasts
  300 second input rate: 48 bits/sec, 0 packets/sec
  300 second output rate: 16 bits/sec, 0 packets/sec

ACOS(config)# show interface ethernet 15
  Ethernet 15 is disabled, line protocol is down
  Hardware is GigabitEthernet, Address is 001f.a005.53e0
  Internet address is 0.0.0.0, Subnet mask is 0.0.0.0
  Configured Speed auto, Actual unknown Configured Duplex auto, Actual
unknown
  Member of L2 Vlan 300, Port is Tagged
  Flow Control is disabled, IP MTU is 6000 bytes
  Port as Mirror disabled, Monitoring this Port disabled
  0 packets input,  0 bytes
  Received 0 broadcasts,  Received 0 multicasts,  Received 0 unicasts
  0 input errors,  0 CRC  0 frame
  0 runts  0 giants
  0 packets output  0 bytes
  Transmitted 0 broadcasts  0 multicasts  0 unicasts
  0 output errors  0 collisions
  300 second input rate: 0 bits/sec, 0 packets/sec, 0% utilization
  300 second output rate: 0 bits/sec, 0 packets/sec, 0% utilization

ACOS(config)# show interface ethernet 16
  Ethernet 16 is disabled, line protocol is down
  Hardware is GigabitEthernet, Address is 001f.a005.53e1
  Internet address is 0.0.0.0, Subnet mask is 0.0.0.0
  Configured Speed auto, Actual unknown Configured Duplex auto, Actual
unknown
  Member of L2 Vlan 300, Port is Tagged
```

```
Flow Control is disabled, IP MTU is 6000 bytes
Port as Mirror disabled, Monitoring this Port disabled
0 packets input,  0 bytes
Received 0 broadcasts,  Received 0 multicasts,  Received 0 unicasts
0 input errors,  0 CRC  0 frame
0 runts  0 giants
0 packets output  0 bytes
Transmitted 0 broadcasts  0 multicasts  0 unicasts
0 output errors  0 collisions
300 second input rate: 0 bits/sec, 0 packets/sec, 0% utilization
300 second output rate: 0 bits/sec, 0 packets/sec, 0% utilization
```

Monitoring and Reporting Tools

This part of the document describes about monitoring tools for the ACOS devices.

The ACOS device can send alerts to administrators through the following methods:

- System Log Messages
- ACOS Event - Hashing
- Emailing Log Messages
- Link Monitoring
- ACE Monitoring and Analytics
- Multiple Port-Monitoring Mirror Ports
- sFlow
- Call Home
- Simple Network Management Protocol (SNMP)
- ACL on Interface Monitoring

System Log Messages

The ACOS device logs system events with system log (Syslog) messages.

The following topics are covered:

Destinations for Syslog Messages

The ACOS device can send Syslog messages to the following places:

- Local buffer (default level: Debugging - 7)
- Console CLI session (default level: Error - 3)
- Console SSH and Telnet sessions
- External Syslog server
- Syslog server in another partition
- Email address(es)
- SNMP servers (for events that are logged by SNMP traps)

Logging to the local buffer and to CLI sessions is enabled by default. Logging to other places requires additional configuration.

Syslog Message Severity Levels

The standard Syslog message severity levels are supported:

- Emergency – 0
- Alert – 1
- Critical – 2
- Error – 3
- Warning – 4
- Notification – 5
- Information – 6
- Debugging – 7

Configurable Syslog Parameters

The following topics are covered:

System Log Settings

The following Table 7 lists the configurable Syslog parameters.

Table 7 : Configurable System Log Settings

Parameter	Description	Supported Values
Disposition (message target)	Output options for each message level. For each message level, you can select which of the following output options to enable: • Console – Messages are displayed in Console sessions. • Buffered – Messages are stored in the system log buffer. • Email – Messages are sent to the email addresses in the Email To list. (See below.) • SNMP – SNMP traps are generated and sent to the SNMP receivers. • Syslog – Messages are sent to the external log servers specified in the Log Server fields. (See below.) • Monitor – Messages are displayed in Telnet and SSH sessions.	The following message levels can be individually selected for each output option: • Emergency (0) • Alert (1) • Critical (2) • Error (3) • Warning (4) • Notification (5) • Information (6) • Debug (7) Only Emergency, Alert, and Critical can be selected for SNMP. Only Emergency, Alert, Critical, and Notification can be selected for Email.

Table 7 : Configurable System Log Settings

Parameter	Description	Supported Values
	NOTE: For information about emailing log messages, see Emailing Log Messages.	
Logging Email Filter	Settings for sending log messages by email.	See Emailing Log Messages.
Logging Email Buffer Number		
Logging Email Buffer Time		
Facility	Standard Syslog facility to use.	Standard Syslog facilities listed in RFC 3164.
Log Buffer Entries	Maximum number of log entries the log buffer can store.	10000 to 50000 entries Default: 30000
Log Server/Host	IP addresses or fully-qualified domain names of external log servers. Only the message levels for which Syslog is selected in the Disposition list are sent to log servers.	Any valid IP address or fully-qualified domain name. Default: None configured

Table 7 : Configurable System Log Settings

Parameter	Description	Supported Values
	NOTE: By default, the ACOS device can reach remote log servers only if they are reachable through the ACOS device's data ports, not the management port. To enable the ACOS device to reach remote log servers through the management port, see Source Interface for Management Traffic.	
Log Server Port	Protocol port to which log messages sent to external log servers are addressed.	Any valid protocol port number Default: 514
Email To	Email addresses to which to send log messages. Only the message levels for which Email is selected in the Disposition list are sent to log servers.	Valid email address. Click the down arrow next to the input field to add another address (up to 10). Each email address can be a maximum of 31 characters long.
SMTP Server	IP address or fully-qualified domain name of an email server using Simple Message Transfer Protocol.	Any valid IP address or fully-qualified domain name. Default: None configured

Table 7 : Configurable System Log Settings

Parameter	Description	Supported Values
	NOTE: By default, the ACOS device can reach SMTP servers only if they are reachable through the ACOS device's data ports, not the management port. To enable the ACOS device to reach SMTP servers through the management port, see Source Interface for Management Traffic.	
SMTP Server Port	Protocol port to which email messages sent to the SMTP server are addressed.	Any valid protocol port number Default: 25
Mail From	Specifies the email From address.	Valid email address Default: Not set
Need Authentication	Specifies whether access to the SMTP server requires authentication.	Selected (enabled) or unselected (disabled) Default: disabled
Username	Username required for access to the SMTP server.	Valid username Default: Not set
Password	Password required for access to the SMTP server.	Valid password Default: Not set

Operational Logging

The following Table 8 lists the types of operational events that are logged.

Table 8 : LSN Operational Logs

Severity Level	Event	Message String
Critical	User-quota creation failure	LSN: User-quota creation failed (out of memory) for pool...
	Full-cone session creation failure	LSN: Full-cone session creation failed (out-of-memory) for pool...
Warning	New inside user unable to get NAT IP	LSN: New user could not get a NAT IP on pool..
	Current inside user on NAT IP can not get new NAT port	LSN: NAT port usage exceeded on pool...
Notice	User quota exceeded	LSN: ICMP user-quota exceeded on pool... LSN: UDP user-quota exceeded on pool... LSN: TCP user-quota exceeded on pool...
	Extended user quota exceeded	LSN: UDP extended user-quota exceeded on pool... LSN: TCP extended user-quota exceeded on pool...

Configure Single-Priority Logging

Single-priority logging allows you to identify one specific severity level to be logged from among the standard syslog message severity levels (See Syslog Message Severity Levels).

This allows you to remove excess data so that you can see a desired subset of log messages at your target severity level.

In prior releases, when you specify a severity level to be logged, the selected level becomes the “basement level”, or the most trivial level that will appear along with the more important messages. For example, if you specify level 3 (error), you would also get severities 2, 1, and 0, but 3 would be the most trivial severity level to be included in the log messages.

Prior releases did not offer a way for you to single out a particular subset of log messages at a singular severity level; for example, there was no way to display severity level 5 log messages without also seeing messages from severity levels 4–0.

Single-priority logging offers more granular control of syslog messages.

To configure single-priority logging, use the `logging single-priority` command.

The following example logs only error (level 3) messages:

```
ACOS(config)# logging single-priority error
```

Configure Log Rate Limiting

The ACOS device uses a log rate limiting mechanism to ensure against overflow of external log servers and the internal logging buffer.

The rate limit for external logging is 15,000 messages per second from the device.

The rate limit for internal logging is 32 messages per second from the device.

- If the number of new messages within a one-second interval exceeds 32, then during the next one-second interval, the ACOS device sends log messages only to the external log servers.
- If the number of new messages generated within the new one-second interval is 32 or less, then during the following one-second interval, the ACOS device will again send messages to the local logging buffer as well as the external log server. In any case, all messages (up to 15,000 per second) get sent to the external log servers.

The following topics are covered:

Configure Using GUI

To configure log rate limiting using the GUI:

1. Hover over **System** in the navigation bar, and select **Settings**.
2. Click **Logging** on the menu bar.
3. Change settings as needed. (For descriptions of the settings, see Configurable System Log Settings.)
4. Click **OK**.

Configure Using CLI

Use the `logging` command to configure log rate limiting using the CLI.

For example, to change the severity level of messages logged in the local buffer to "warning" (level 4):

```
ACOS(config)# logging buffered warning
```

Replace buffered with a different destination, as desired (see Destinations for Syslog Messages).

NOTE: Only severity levels **emergency**, **alert**, **critical**, and **notification** can be sent by email. Sending log messages by email requires additional configuration. See Emailing Log Messages.

To configure the ACOS device to send log messages to an external Syslog server, use the **logging host** command to specify the server:

```
ACOS(config)# logging host 20.20.10.8
```

The following topics are covered:

Specify Multiple Syslog Servers

To specify multiple server names or IP addresses, use multiple commands. The following example configures 20.20.10.8, 30.30.10.5, and “loghost1” as syslog servers:

```
ACOS(config)# logging host 20.20.10.8
ACOS(config)# logging host 30.30.10.5
ACOS(config)# logging host loghost1
```

Specify Protocol Ports

You can also specify a protocol port. The default port is 514. If you specify multiple servers, then all servers specified must use the same protocol port to listen for syslog messages; you can only specify one protocol port per command.

The following example configures 20.20.10.8 and 30.30.10.5 as syslog servers listening on port 515, and 40.40.5.9 as a syslog server listening on port 517:

```
ACOS(config)# logging host 20.20.10.8 port 515
ACOS(config)# logging host 30.30.10.5 port 515
ACOS(config)# logging host 40.40.5.9 port 517
```

Send the Syslog Over TLS/SSL

To send the syslog over TLS/SSL to the remote server, perform the following steps:

1. Create the CA root self-signed certificate in the Linux server:
   a. Generate the RSA private key for the CA root:

   ```
   $ openssl genrsa -des3 -out <key-name.key> 2048
   ```

   b. Create the self-signed CA root certificate:

   ```
   $ openssl req -x509 -new -nodes -key <key-name.key> -sha256 -days
   1825 -out <CAroot-name.pem>
   ```

   c. Generate a certificate signing request (CSR):

   ```
   $ openssl req -out <csr-name.csr> -new -newkey rsa:2048 -nodes -
   keyout <server-keyname.key>
   ```

   d. Sign the CSR with the CA root certificate to create the server certificate using

'.csr':

```
$ openssl x509 -req -days 360 -in <csr-name.csr> -CA <CAroot-
name.pem> -CAkey <CAkey key> -CAcreateserial -out <cert-name.crt>
```

NOTE: Use different common names for the CA root and the certificate signing request.

e. To receive messages over TLS/SSL socket, OpenSSL provides the socket listening API:

```
$ openssl s_server -accept <port> -cert <server-certificate> -key
<server-key>
```

2. Import the CA root certificate into the ACOS device.
3. In the ACOS device, create the template for logging using syslog over TLS:

   The `syslog-over-tls` template command is used to configure the self-signed CA root certificate for TLS handshake. This template is shared across all the configured syslog servers. Following are the example CLI commands.

```
ACOS(config)# template syslog-over-tls
ACOS(config)# ca-cert <CAcert-name>
```

4. Configure the logging using syslog over TLS:

   To configure remote logging over TLS, use the `over-tls` parameter in `logging host` command. Following is the example CLI command.

```
ACOS(config)# logging host <host-ip> use-mgmt-port port <port-no> tcp
over-tls
```

- The `over-tls` parameter is available only when the `tcp` parameter is included in the `logging host` command.
- When the port number is not configured, by default port 514 is used, similar to syslog over TLS.

Deleting the Configuration and Template using Syslog Over TLS

1. To delete the configuration of logging using syslog over TLS, use the following command:

```
ACOS(config)# no logging host <host-ip> use-mgmt-port port <port-no>
tcp over-tls
```

2. To delete the syslog over TLS template, use one of the following commands:

```
ACOS(config)# no template syslog-over-tls
ACOS(config-syslog-over-tls template)# no ca-cert <CA certificate name>
```

Send Log Messages to Server in Another Partition

The following example configures a a log server in the shared partition:

```
ACOS(config)# logging host 44.3.2.1
```

The following commands configured a logging server 45.3.2.1 in partition LOG1, and also sends logging information to the shared partition:

```
ACOS[LOG1](config)# logging host 45.3.2.1
ACOS[LOG1](config)# logging host partition shared
```

In partition LOG2, a third syslog server 46.3.2.1 is configured, and log messages are sent to the syslog server configured in partition LOG1:

```
ACOS[LOG2](config)# logging host 46.3.2.1
ACOS[LOG2](config)# logging host partition LOG1
```

Send Log Messages by Email

To configure the ACOS device to send log messages by email, use the following commands to specify the email server and the email addresses:

```
ACOS(config)# smtp 10.10.10.5
ACOS(config)# logging syslog@myexamplecompany.com
```

The `smtp` command specifies the mail server. By default, it uses port 25 to send email. You can customize this with the optional `port` parameter.

To send event messages to an external SNMP server, see *SNMP MIB Reference Guide*.

Configure Alerts for Modular License

ACOS supports monitoring and alert management of the modular license (software-driven license) bandwidth usage for Thunder or vThunder devices. This feature provides SNMP messages and Syslog logging when the device's bandwidth usage exceeds the configurable threshold. The `axSystemBandwidthThresholdAlert` trap is provided to support this feature.

If you have modular license enabled on the device and the ACOS software image is upgraded to 6.0.4, the following threshold is set by default.

- Warning Threshold: When bandwidth usage reaches 75% and persists for 7 consecutive days, the SNMP and Syslog messages are triggered.
- Critical Threshold: When bandwidth usage reaches 95% and persists for two consecutive days, the SNMP and Syslog messages are triggered.

These threshold can be customized based on your business need.

An emergency alert is generated when bandwidth usage hits 100%, which is regarded as an emergency threshold and its value cannot be modified. The system will send a message every time the bandwidth hits 100% at a rate of one message per hour at most.

Let's say the modular license bandwidth utilization over the next 7 days is as follows:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
73%	77%	97%	97%	83%	62%	103%

- Monday shows a 77% bandwidth utilization. However, it does not qualify as a critical, warning, or emergency alert.
- Tuesday and Wednesday show 97% bandwidth utilization for two consecutive days. Therefore, the system triggers a critical message and sends the Syslog and SNMP traps to alert the user.
- Saturday shows 103% bandwidth utilization. Therefore, the system triggers an emergency message and sends the Syslog and SNMP trap to alert the user.

Configuration Overview

1. Setup event logging infrastructure. See Event Logging Guide.
2. Enable and configure SNMP service, traps, and client. See SNMP MIB Reference.
3. Modify the bandwidth threshold at the system-level, if required.

   When the bandwidth exceeds the threshold, an event is triggered.
4. Check the logs using the **show varlog** command.

Configuration Example

- To modify the default warning threshold percentage, use the following command:

```
ACOS(config)# system bandwidth warning-threshold <50-80>
```

- To modify the critical threshold percentage, use the following command:

```
ACOS(config)# system bandwidth critical-threshold <81-99>
```

NOTE: You cannot remove these configurations from the system using **no system bandwidth {warning-threshold | critical-threshold}** command. Instead, the system will revert to the default threshold values 75% and 95% respectively.

Log Example

The alert messages only display the time of the threshold being exceeded and the percentage of bandwidth consumption.

```
ACOS#show varlog | inc BANDWIDTH
Jun  4 00:00:02 localhost a10lb[4832]: BANDWIDTH EMERGENCY - Bandwidth has
reached 100 percent of the license capacity (51200000000 bits). Current
usage is 100.
Jun  4 00:00:02 localhost a10lb[4832]: BANDWIDTH CRITICAL - Bandwidth has
reached 95 percent of the license capacity (51200000000 bits) or greater
for the past two days. Current usage is 100.
Jun  4 01:00:06 TH1-L3V a10lb[4832]: BANDWIDTH WARNING - Bandwidth has
reached 75 percent of the license capacity (51200000000 bits) or greater
for the past seven days. Current usage is 80.
```

ACOS Event - Hashing

The following topic is covered:

Hashing Support for ACOS Event

When multiple external log servers are configured under a collector group, each log is forwarded to only one of the log servers. You can select the log server from the following methods:

- Round-Robin (Default)
- Hashing

The following topics are covered:

Log Distribution by Round-Robin Method

By default, the log messages are forwarded to the external log servers using the round-robin method. The round-robin method distributes the log messages evenly across all log servers. For example, if there are two log servers (LS1 and LS2) in the collector group, the log servers are selected in sequence and the logs are forwarded as follows:

- The first log is sent to LS1
- The second log is sent to LS2
- The third log is sent to LS1
- The fourth log is sent to LS2, and so on

Use the following command to configure the round-robin method in the collector group for distributing the logs (Round-Robin is configured by default):

```
ACOS(config-collector-group:c1)#log-distribution round-robin
```

In the following example, as the log-distribution is not configured, the logs are distributed using the round-robin method by default:

```
ACOS(config)#acos-events message-selector m1
ACOS(config-msg-selector:m1)#rule 1
ACOS(config-msg-selector:m1-rule:1)#message-id slb all
ACOS(config-msg-selector:m1-rule:1)#exit
ACOS(config-msg-selector:m1)#exit
ACOS(config)#acos-events log-server 11 11.11.11.5
ACOS(config-log-server)#port 514 udp
ACOS(config-log-server-logging port)#exit
ACOS(config-log-server)#exit
ACOS(config)#acos-events collector-group c1 udp
ACOS(config-collector-group:c1)#log-server 11 514
ACOS(config-collector-group:c1)#exit
ACOS(config)#acos-events template t1
ACOS(config-template:t1)#message-selector m1
ACOS(config-template:t1-selector:m1)#collector-group c1
ACOS(config-template:t1-selector:m1-colle...)#exit
ACOS(config-template:t1-selector:m1)#exit
ACOS(config-template:t1)#exit
ACOS(config)(NOLICENSE)#
```

Log Distribution by Hashing Method

The log messages can also be forwarded to the external log servers based on hashing. It provides a consistent hashing framework where some logs that are to be sent to the same log server (For example, Session creation and session deletion for the same session or all logs from the same session or connection) are sent to the same external log server rather than randomly selecting the server through Round-Robin.

Use the following command to configure the hashing method in the collector group for distributing the logs:

```
ACOS(config-collector-group:c1)#log-distribution hashing
```

Though hashing is enabled, it is considered only when the generated log is in context within a connection. If not, it will fall back to the Round-Robin method because the hash is calculated based on the destination IP address on the connection. All the logs

generated from the connections with the same destination IP address are sent to the same external log servers.

The log's hash, which is based on the destination IP address, matches the configured log servers and one server out of multiple configured servers is selected. If many log servers are contending for the same hash, then the source IP of the connection is used to break the discrepancy.

When there are any changes to the configured log servers (such as servers going down, coming up, adding, or deleting servers), the mapping of logs to the log servers is preserved on a best effort basis. For example, if the log L1 is sent to the log server s1 based on hashing, while the log server s1 goes down, the log L1 is sent to another log server s2. When the log server s1 is up, the log L1 and the similar logs (with hash L1) must be sent to s1 again.

When the logs servers are down or not usable or due for maintenance, you can perform one of the following:

- Remove the log server from the configuration without replacing the log server – logs are distributed among other log servers.
- Replace a log server with a new log server with the same IP address – logs sent to the old log server are sent to the new log server (Refer to the configuration below).
- Replace a log server with a new log server with the same name – logs sent to the old log server are sent to the new log server (Refer to the configuration below).
- Replace a log server with a new log server with a different name and IP address – Consistency is not maintained (logs sent to the old log server might not be sent to the new log server).

To provide consistent hashing with changes, use the following commands to configure the hashing method as either Name or IP tuple in the collector group:

- Name – Set the hashing method as Name when you always replace the server that is down with the same name but a different IP.

  Use the following command to configure the hashing method as Name in the collector group for distributing the logs:

```
ACOS(config-collector-group:c1)#server-distribution-hash name
```

- IP tuple – Set the hashing method as an IP tuple if you want the log distribution to be consistent based on the log-server IP.

  Use the following command to configure the hashing method as an IP tuple in the collector group for distributing the logs:

```
ACOS(config-collector-group:c1)#server-distribution-hash ip-tuple
```

NOTE:

For an active template, you cannot change:

- log-distribution method from round-robin to hash or vice-versa.
- server-distribution-hash from name to IP-tuple or vice versa.

In the following example, hashing method is configured for distributing the logs:

```
ACOS(config)#acos-events message-selector m1
ACOS(config-msg-selector:m1)#rule 1
ACOS(config-msg-selector:m1-rule:1)#message-id slb all
ACOS(config-msg-selector:m1-rule:1)#exit
ACOS(config-msg-selector:m1)#exit
ACOS(config)#acos-events log-server l1 11.11.11.5
ACOS(config)#port 514 udp
ACOS(config)#acos-events collector-group c1 udp
ACOS(config-collector-group:c1)#log-distribution hashing
ACOS(config-collector-group:c1)#log-server l1 514
ACOS(config-collector-group:c1)#exit
ACOS(config)#acos-events collector-group c2 udp
ACOS(config-collector-group:c2)#log-distribution hashing
ACOS(config-collector-group:c2)#log-server l1 514
ACOS(config-collector-group:c2)#exit
ACOS(config)#acos-events template t1
ACOS(config-template:t1)#message-selector m1
ACOS(config-template:t1-selector:m1)#collector-group c1
ACOS(config-template:t1-selector:m1-colle...)#collector-group c2
ACOS(config-template:t1-selector:m1-colle...)#exit
ACOS(config-template:t1-selector:m1)#exit
ACOS(config-template:t1)#exit
```

Emailing Log Messages

You can configure the ACOS device to email log messages, using email log filters. By default, emailing of log messages is disabled.

Log email filters consist of the following parameters:

- Filter ID – Filter number, 1-8.
- Conditions – One or more of the following:
  - Severity – Severity levels of messages to send in email. If you do not specify a message level, messages of any severity level match the filter and can be emailed.
  - Software Module – Software modules for which to email messages. Messages are emailed only if they come from one of the specified software modules. If you do not specify a software module, messages from all modules match the filter and can be emailed.
  - Regular Expression (Patterns and Operators) – Message text to match on. Standard regular expression syntax is supported. Only messages that meet the criteria of the regular expression can be emailed. The regular expression can be a simple text string or a more complex expression using standard regular expression logic. If you do not specify a regular expression, messages with any text match the filter and can be emailed.

    The operators (AND, OR, NOT) specify how the conditions must be compared. (See Boolean Operators.)
- Trigger option – Specifies to send the matching messages immediately.

The following topics are covered:

Boolean Operators

A logging email filter consists of a set of conditions joined by Boolean expressions (AND / OR / NOT).

The CLI Boolean expression syntax is based on Reverse Polish Notation (also called Postfix Notation), a notation method that places an operator (AND, OR, NOT) after all of its operands (in this case, the conditions list).

After listing all the conditions, specify the Boolean operator(s). The following operators are supported:

- AND – All conditions must match in order for a log message to be emailed.
- OR – Any one or more of the conditions must match in order for a log message to be emailed.
- NOT – A log message is emailed only if it does not match the condition

NOTE: For more information about Reverse Polish Notation, see the link: http://en.wikipedia.org/wiki/Reverse_Polish_notation.

Configure Email Log Settings

The following topics are covered:

Configure Email Log Settings Using GUI

To configure Email logging settings in the GUI:

1. Hover over **System** in the navigation bar, and click **Settings**.
2. Click **Logging** in the menu bar.
3. In the Level field, select the log level you want to enable.

4. The Buffer field contains two optional configuration choices:
   a. To change the maximum number of log messages to buffer before sending them in email, edit the number in the field on the left. You can specify 16-256 messages. The default is 50.
   b. To change the number of minutes the ACOS device waits before sending all buffered messages, edit the number in the field on the right. This option takes effect if the buffer does not reach the maximum number of messages allowed. You can specify 10-1440 minutes. The default is 10.
5. In the Email Addresses field, specify the Email addresses to which the log files will be sent.
6. In the Filters section:
   a. Specify a filter ID (1-8) and regular expression filter in the Filter section.
   b. To immediately send matching messages in an email instead of buffering them, select Trigger. Otherwise, matching messages are buffered until the message buffer becomes full or the send timer for emailed log messages expires.
   c. Click **Save Filter**.
   d. Repeat the process if you want to create multiple filters.
7. When finished configuring log settings, click the **OK** button at the bottom of the page.

Configure Email Log Settings Using CLI

This section contains CLI examples of Email logging configuration.

The following command configures 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.

```
ACOS(config)# logging email buffer number 32 time 30
```

The following command resets the buffer settings to their default values.

```
ACOS(config)# no logging email buffer number time
```

The following command configures a filter that matches on log messages if they are information-level messages and contain the string “abc”. The **trigger** option is not used, so the messages will be buffered rather than emailed immediately.

```
ACOS(config)# logging email filter 1 "level information pattern abc and"
```

The following command reconfigures the filter to immediately email matching messages.

```
ACOS(config)# logging email filter "1 level information pattern abc and"
trigger
```

Link Monitoring

The ACOS device supports link monitoring with automated link disable or session clear.

This feature monitors the link state of Ethernet data interfaces. You can monitor Ethernet data interfaces for the following types of events:

- Link up
- Link down

The feature monitors the link state on a set of Ethernet data interfaces. If the monitored event is detected, the ACOS device evaluates current link status for all the bound monitors and applies the specified action to another set of interfaces.

This feature is especially useful in cases where you want to disable both ACOS interfaces used by traffic flows through the ACOS device, if the link on either interface goes down.

NOTE:

- For an example, see “LACP Passthrough” in the *Network Configuration Guide*.
- You can configure the feature for individual Ethernet data ports. Configuration of the feature for logical interfaces such as Virtual Ethernet (VE) interfaces is not supported.

The following topics are covered:

Link Monitoring Actions

You can configure the ACOS device to take one of the following actions when the specified event type (link up or link down) is detected on a monitored Ethernet data interface:

- Clear sessions
- Disable the link on one or more other interfaces
- Enable the link on one or more other interfaces

The clear session option removes sessions from the session table. You can configure the feature either to clear data sessions only, or to clear sessions of all types.

Link Monitor Template Sequence Numbers

Each monitor template can contain the following types of entries:

- Monitoring entries – A monitoring entry monitors for a specific event type (link up or link down) on a specific Ethernet data interface.
- Action entries – An action entry specifies the action to take when monitored events are detected.

When you configure an entry of either type, you must specify a sequence number, 1-16. The sequence numbers assigned to monitoring entries specify the order in which to check the monitored ports for the specified event type.

Likewise, the sequence number assigned to action entries specify the order in which to apply the actions.

The sequence number can be important in cases such as the following:

- The order in which link state changes take place can affect whether traffic loops occur.
- The template contains action entries that clear sessions and that disable or enable links. In this case, the sequence number controls whether the sessions are cleared before or after the link states are changed. Normally, it is recommended to clear the sessions first, before changing the link states.

The monitor with the lowest sequence number is performed first, then the monitor with the next lowest sequence number is performed, and so on. For example, monitor 1 is performed first, monitor 2 is performed second, and so on. Likewise, if the monitored events are detected, action 1 is performed first, then action 2, and so on.

Link Monitor Template Logical Operators

Each monitor template uses one of the following logical operators:

- **AND** – The actions are performed only if all the monitored events are detected. (This is the default).
- **OR** – The actions are performed if any of the monitored events is detected.

The logical operator applies only to monitor entries, not to action entries. For example, if the logical operator is OR, and at least one of the monitored events occurs, all the actions configured in the template are applied.

You can configure the entries in any order. In the configuration, the entries of each type are ordered based on sequence number.

Configuring Link Monitor

To configure link monitoring with automated link disable or session clear:

1. Configure a monitoring template. Within the template, specify the following parameters:

- Links (Ethernet data ports) to monitor
- Actions to perform on other links, if the monitored event is detected:
  - Clear sessions
  - Disable links
  - Enable links

- (Optional) Set the comparison operator for the monitoring entries:
  - AND – The actions are performed only if all the monitored events are detected.
  - OR – The actions are performed if any of the monitored events is detected.

    Link monitoring template commands are available through global configuration mode (See the *Command Line Interface Reference* guide). A similar set of commands are available through slb template monitor mode (See the *Command Line Interface Reference* guide).

2. Active the monitoring template.

You can configure and activate up to 16 monitor templates. A monitor template does not take effect until you activate it.

The following commands configure monitor template 1 and the physical data interfaces and events to monitor:

```
ACOS(config)# system mon-template monitor 1
ACOS(config-monitor)# monitor link-down eth 5 sequence 1
ACOS(config-monitor)# monitor link-down eth 6 sequence 2
ACOS(config-monitor)# monitor link-down eth 9 sequence 3
ACOS(config-monitor)# monitor link-down eth 10 sequence 4
```

The following commands configure the actions to take when a monitored event is detected.

```
ACOS(config-monitor)# action clear sessions sequence 1
ACOS(config-monitor)# action link-disable eth 5 sequence 2
ACOS(config-monitor)# action link-disable eth 6 sequence 3
ACOS(config-monitor)# action link-disable eth 9 sequence 4
ACOS(config-monitor)# action link-disable eth 10 sequence 5
ACOS(config-monitor)# exit
```

The following command activates the template, to place it into effect:

```
ACOS(config)# system template-bind monitor 1
```

Based on this configuration, when a link-down event is detected for Ethernet port 5 OR 6 OR 9 OR 10, sessions are cleared first. Then the remaining links are disabled, in the following sequence: 5 AND 6 AND 9 AND 10.

NOTE: The `clear session` command clears only data sessions. To clear all sessions, use `clear sessions all`.

ACE Monitoring and Analytics

The ACE (Analytics Computing Engine) implements visibility and analytics as a base ACOS function. ACE collects data from counter library metrics per connection for statistical analysis.

Visibility of anomalies like traffic spikes and traffic failures, provides some guidance on seasonality of traffic to help the user with resource assignment.

The following topics are covered:

ACE Monitoring and Show Command Options

ACE monitoring options can be configured in Visibility Configuration mode in CLI using the **visibility** command.

The following topics are covered:

Discovery Monitoring

Monitoring samples are collected for every ACOS partition receiving and generating the samples, creating keys as specified in the partition configuration.

Related Commands

Example of monitoring commands in CLI:

- Monitor x-flow source information:

```
ACOS(config-visibility)# monitor xflow source
```

Granularity

The granularity can be configured by the user for all rate based calculations. Granularity is the time selection interval specified, for example, a default value of 5 seconds. to collect monitoring information for each monitoring parameter. Supported values are 1 to 300 seconds.

Using the **granularity** command.

```
ACOS (config-visibility)# granularity 60
```

Cumulative Updates

This is a feature that can be enabled when creating the ACE monitor. the statistics counter library on if sends cumulative updates from ACOS .

Collection of Statistics

The following values are calculated and the data is further used for analysis:

- **Minimum**
- **Maximum**
- **Mean**
- **Standard deviation**
- **Threshold**: The highest value that was observed for the given metric that was not an anomaly.
- **Continuous learning**: Through continuous monitoring of data or x-flow traffic, A sample is considered if it is not anomalous. Also, when 3 consecutive spikes, are detected, it is considered an anomaly.

Anomaly Detection

Sensitivity settings help in anomaly detection. 3 consecutive spikes mean the monitored parameter is anomalous. There are two settings:

- **Low sensitivity**: This is what the system defaults to. In this case, any sample that is greater than 2 times the threshold is a spike.
- **High sensitivity**: Any sample that is greater than 2 times the standard deviation mean is a spike.

Related CLI Commands

The important anomaly detection related CLI commands are as follows:

- Enable anomaly detection in Visibility Configuration mode:

```
ACOS(config-visibility)# anomaly-detection
```

- Configure sensitivity for anomaly detection

```
ACOS(config-visibility-anomaly-detection)# sensitivity high
```

Notification Templates

ACE supports for primary and secondary level monitoring. Primary and Secondary key types can be specified from CLI. The module creates monitoring entities based on these keys. ACOS evaluates these baseline metric values. The base line values calculated are **minimum**, **maximum**, **mean** and **standard deviation**. Using these baseline values, 'anomalies are detected or cleared.

This feature adds support to send notifications on different events. The host that should receive these notifications can be configured from the CLI.

The following topics are covered:

Notification Events

Notifications are sent for the following events:

- Monitoring entity creation
- Monitoring entity deletion
- Anomaly detection
- Anomaly clear

Notification Data

The notification data contains:

- Parameter name.
- The type of information (source / destination/ service / Source NAT IP)
- Notification type (entity created / entity deleted /anomaly detected / anomaly cleared)
- Processed metric values (minimum, maximum, current, threshold, mean)
- Anomaly status for every metric.
- Entity type (primary / secondary)

Notification Template Properties

A maximum of 8 notification templates can be configured on ACOS. These templates are global, and can be bound to any partition. Notification templates have the following properties:

- By default, a template is active after creation.
- An incomplete template cannot be bound to a partition.
- Template must be disabled before modification, unless it is not bound.
- Template cannot be deleted when it is bound.

Notification Template Examples

The following topics are covered:

Create Notification Template

- Configure visibility reporting

```
ACOS(config-visibility-reporting)# template notification user1
```

- Configure the host with an IPv4 address

```
ACOS(config-visibility-reporting-notifica...)#host ip 1.1.1.1
!
```

- Use the management port option for notifications

```
ACOS(config-visibility-reporting-notifica...)# host ip 1.1.1.1 use-mgmt-
port
```

- To use IPv6 address as host

```
ACOS(config-visibility-reporting)# template notification ipv6
ACOS(config-visibility-reporting-notification)# host ip6 1::1 use-mgmt-
port
```

Verifying the Configuration

```
ACOS(config-visibility-reporting)#show run visibility
!Section configuration: 94 bytes
!
visibility
  reporting
    template notification ipv6
      host ip6 1::1 use-mgmt-port
```

```
!
```

To use URI as a host, use the command:

```
ACOS(config-visibility-reporting-notifica...)#host host-name
a10networks.com
ACOS(config-visibility-reporting-notifica...)#protocol http 80
```

NOTE: The default protocol is HTTPS and port 443.

Verifying the Configuration

```
ACOS(config-visibility-reporting)#show run visibility
```

```
!Section configuration: 106 bytes
!
visibility
  reporting
    template notification user1
      host ip 1.1.1.1
      protocol http 80
!
```

Delete Template

```
ACOS(config-visibility-reporting)#no template notification user1
ACOS(config-visibility-reporting)#sh run visibility
!Section configuration: 0 bytes
!
```

Enable Template

Enable or bind a complete template

```
ACOS(config-visibility-reporting-notifica...)#host ip 1.1.1.1
ACOS(config-visibility-reporting-notifica...)#enable
ACOS(config-visibility-reporting-notifica...)#show run visibility
!Section configuration: 82 bytes
!
visibility
  reporting
    template notification test
      host ip 1.1.1.1
```

NOTE: Host details are must to enable any template. Incomplete templates cannot be enabled.

Disable Template

Disable template using:

```
ACOS(config-visibility-reporting-notifica...)#disable
ACOS(config-visibility-reporting-notifica...)#show run visibility
!Section configuration: 97 bytes
!
```

```
visibility
  reporting
    template notification user1
      host ip 1.1.1.1
      disable
!
```

Bind Template

To bind a template, enable monitoring and notifications for the template.

```
ACOS(config-visibility)# monitor traffic dest
ACOS(config-visibility-monitor:traffic)# template notification user1
ACOS(config-visibility-monitor:traffic)# show run visibility
!Section configuration: 138 bytes
!
visibility
  reporting
    template notification test
      host ip 1.1.1.1
  monitor traffic dest
    template notification test
!
```

Configure Visibility on ACOS

To configure a new notification template for visibility on vThunder, configure IPv6 AAAA using and then the visibility reporting notifications using the following commands:

```
ACOS(config)# visibility
ACOS(config-visibility)# reporting
ACOS(config-visibility-reporting)# notification-template user1
!
```

1. Template host configuration for IPV6 AAAA.
2. Configure the host IPv6 address.

```
ACOS(config-visibility-reporting-notifica...)# host ip 6.6.6.6 use-
mgmt-port
```

3. Protocol to use. Configure the http port to use <1-65535>:

```
ACOS(config-visibility-reporting-notifica...)# protocol http 8080
```

4. Relative URI.

```
ACOS(config-visibility-reporting-notifica...)# relative-uri companyuri/
```

5. Enable / disable a template.
6. The show command for operation support.

```
ACOS# show run visibility
!Section configuration: 167 bytes
!
visibility
  monitor dest
  reporting
    notification-template test
      host ip 6.6.6.6 use-mgmt-port
      protocol http 8080
      relative-uri testuri/
```

Visibility and Analytics Monitoring

ACOS users with critical infrastructure can monitor network resources through visibility and analytics. ACOS supports a logging system to monitor resources like system interface statistics, virtual server, remote server, and virtual port.

All ACOS platforms, ACOS Thunder, vThunder, and Thunder Container, have native support for Prometheus. A Prometheus server can query various stats and rate metrics for analysis as specified in its configuration.

Functionalities

Users and systems can use the following functionalities:

- Create and view dashboards to communicate with the Prometheus server using a Visualization and Analytics tool, like Grafana.
- Query any API statistics configured in the Prometheus server's YAML file.

- View the default metrics logged, when no filters are specified:
  - All Interface Metrics
  - CPU Usage
  - Memory Usage

Configuration Example

For example, to monitor a particular object or class of objects, add that object or class of objects to the parameters (params) in the Prometheus YAML file as follows.

Sample prometheus.yml Configuration Snippet

```
global:
  scrape_interval: 5s
  evaluation_interval: 5s

scrape_configs:
  - job_name: 'prometheus_job_fetch_metrics'
    scheme: 'https'
        tls_config:
                insecure_skip_verify: true
        static_configs:
        - targets: ["10.65.22.161:443"]
        metrics_path: '/metrics'
        params:
                username:["username"]
                password:["password"]
        api_endpoint: ["/slb/virtual-server/vs1/stats","/slb/service-
group/stats", "/slb/virtual-server/vs1/rate"]
```

The descriptions for the parameters are as follows:

Parameter	Description
scrape_interval	Time intervals for querying the statistics fields.
target	Hostname and port that the Exporter is running on and port must be the same as the port number of the webserver on ACOS Prometheus client.

Parameter	Description
api_endpoint	URI endpoint that the Exporter intercepts to invoke the appropriate aXAPI. (A comma-separated list of APIs can be provided here for a single host.)

In this scenario, once the Prometheus server is up and running, it invokes the query every 15 seconds, as specified in the “scraping interval.api_endpoint”. The API names are passed to them as parameters. The ACOS Prometheus client creates the gauge metrics for each statistics field and exposes the metrics to the Prometheus server.

NOTE: To enable the Prometheus support and learn about the endpoints that are supported, refer to ACOS Prometheus Exporter.

Secondary Monitoring on ACOS

Primary key type for ACE monitoring can be specified from ACOS CLI. A secondary level entity can be configured to monitor each entity. Traffic anomalies can be detected using these baseline values.

User can specify the secondary level key type from CLI. Secondary level entities are created under the primary to help investigate further on primary entity. You can analyze which secondary entity is responsible for the anomaly. Configure using the **`secondary-monitor`** command.

```
vThunder(config-visibility)# monitor traffic dest
vThunder(config-visibility-monitor:traffic)# secondary-monitor service
```

The following topics are covered:

Anomaly Detection Example

When a visibility is enabled on a sample SLB SSL template:

```
!
visibility
  monitor Service secondary-monitor source
```

```
  granularity 1 !
```

If anomaly is caused at client side on the secondary entity, the following show output displays the secondary entity responsible for the anomaly.

```
ACOS# show visibility monitored-entity detail
Entity: ip 12.12.12.203
metric-name    min     max      mean    threshold    error         anomaly
Fwd pkts       126     140      133     140          2.581687      No
Rev pkts       125     140      133     140          2.637233      No
Fwd Bytes      11264   12544    11987   12544        232.692383    No
Rev bytes      14625   16380    15652   16380        308.556244    No
64B_pkt        151     168      160     168          3.108687      No
64-512B_pkt    100     112      107     112          2.109786      No
connections    25      28       26      28           0.527446      No
```

```
sec-entities
Entity: ip 12.12.12.49
metric-name   min    max      mean     threshold   error         anomaly
Fwd pkts      126    140      133      140         2.581687      No
Rev pkts      125    140      133      140         2.637233      No
Fwd Bytes     11264  12544    11987    12544       232.692383    No
Rev bytes     14625  16380    15652    16380       308.556244    No
64B_pkt       151    168      160      168         3.108687      No
64-512B_pkt   100    112      107      112         2.109786      No
connections   25     28       26       28          0.527446      No
```

Session Indexing

When “Session Indexing” is enabled for an application, administrators can view the sessions that are uploading data to the monitoring entities. The primary use case of “Session indexing” is to make the debugging easier for the administrators.

The following topics are covered:

Session Indexing Using CLI

To enable session indexing, use the following CLI command:

```
ACOS(config)# visibility
ACOS(config-visibility)# monitor traffic dest
ACOS(config-visibility-monitor:traffic)# index-sessions
```

To enable per CPU list for session indexing, use the following CLI command:

```
ACOS(config-visibility-monitor:traffic)# index-sessions per-cpu
```

To disable session indexing, use the following CLI command:

```
ACOS(config-visibility-monitor:traffic)# no index-sessions
```

To disable per CPU list, use the following CLI command:

```
ACOS(config-visibility-monitor:traffic)# no index-sessions per-cpu
```

Multiple Port-Monitoring Mirror Ports

The following topics are covered:

Overview of Port Mirroring

Port mirroring is used to send copies of network packets (inbound, outbound, or both) from a monitored port to a separate port for monitoring. This is often used for the purpose of troubleshooting, debugging, and for analyzing traffic.

Up to four physical Ethernet data interfaces can be configured as mirror ports.

L3V port mirroring can be based on the port and optionally, the VLAN ID.

NOTE: The port mirroring and monitoring feature is supported on all A10 Thunder Series devices that are supported with this software release; it is NOT supported on vThunder platforms.

- In earlier 2.7.2.x releases, this feature is supported on A10 Thunder Series and FTA-enabled models only.
- Since mirrored packets are handled by the switching ASIC directly, not the CPU, do not use the **debug packet** command to test packet mirroring on FTA devices.
- Instead, verify that packets are received on the neighboring devices.

Configure Mirror Ports

To configure mirror ports, use the **mirror-port** command at the global configuration level:

The following commands configure four mirror ports:

```
ACOS(config)# mirror-port 1 ethernet 4
ACOS(config)# mirror-port 2 ethernet 7 output
ACOS(config)# mirror-port 3 ethernet 9
ACOS(config)# mirror-port 4 ethernet 3 input
```

The **output** and **input** parameters used in these commands must match the ones you use when configuring the monitor port. The **output** parameter enables outbound traffic on the monitored port to be copied and sent out on the mirror port. The **input** parameter enables inbound traffic on the monitored port to be copied and sent out on the mirror port.

The **show mirror** command verifies the mirror configuration:

```
ACOS(config)# show mirror
Mirror Ports 1:          Input = 4        Output = 4
Mirror Ports 2:          Input = None     Output = 7
Mirror Ports 3:          Input = 9        Output = 9
Mirror Ports 4:          Input = 3        Output = None
```

At this point, monitoring is not yet enabled on any ports. The next step is to access the configuration level for Ethernet interface 1 and enable monitoring of its traffic. For example:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# monitor input 1
```

The following command displays the mirror configuration:

```
ACOS(config-if:ethernet:1)# show mirror
Mirror Ports 1:          Input = 4        Output = 4
 Ports monitored at ingress : 1
Mirror Ports 2:          Input = None     Output = 7
Mirror Ports 3:          Input = 9        Output = 9
Mirror Ports 4:          Input = 3        Output = None
```

The output now lists the monitoring configuration on port 1, which uses mirror 1.

The following commands attempt to enable monitoring of ingress traffic on port 2, using mirror 2. However, this configuration is not valid because mirror 2 can accept egress traffic only.

```
ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# monitor input 2
Please configure mirror port first.
```

Likewise, the **both** option is not valid in this case:

```
ACOS(config-if:ethernet:2)# monitor both 2
Please configure mirror port first.
```

The following configuration is valid, since mirror 2 is configured to accept only the egress traffic of monitored ports:

```
ACOS(config-if:ethernet:2)# monitor output 2
```

Here is the mirror configuration now:

```
ACOS(config-if:ethernet:2)# show mirror
Mirror Ports 1:          Input = 4        Output = 4
 Ports monitored at ingress : 1
Mirror Ports 2:          Input = None     Output = 7
 Ports monitored at egress  : 2
Mirror Ports 3:          Input = 9        Output = 9
Mirror Ports 4:          Input = 3        Output = None
```

The ingress traffic received on port 2 can be monitored, if a mirror that accepts ingress traffic is used. In this example, mirrors 1, 3, and 4 can accept ingress traffic. The following command configures use of mirror 4 for ingress traffic received on port 2:

```
ACOS(config-if:ethernet:2)# monitor input 4
```

The following is the mirror configuration after this change:

```
ACOS(config-if:ethernet:2)# show mirror
Mirror Ports 1:          Input = 4        Output = 4
 Ports monitored at ingress : 1
Mirror Ports 2:          Input = None     Output = 7
 Ports monitored at egress  : 2
Mirror Ports 3:          Input = 9        Output = 9
Mirror Ports 4:          Input = 3        Output = None
 Ports monitored at ingress : 2
```

For brevity, this example does not show configuration of monitoring using mirror 3. Likewise, the example does not show that a mirror can accept monitored traffic from more than one interface, but this is supported.

Port Monitoring and Mirroring for aVCS Devices

Port mirroring and monitoring is supported in an aVCS setup. For example:

```
ACOS-11-Active-vMaster[1/1](config)# mirror-port 2 ethernet 13 ?
  device   Device
  input    Mirror incoming packets to this port
  output   Mirror outgoing packets to this port
```

The only distinction from the base command is that in an aVCS scenario, you must specify the device ID.

In the monitoring mode, you can specify the device to which the Ethernet belongs:

```
ACOS-11-Active-vMaster[1/1][p1]# show mirror ?
  active-vrid  VRRP-A vrid
  device       Device
  |            Output modifiers
```

The following output displays that Ethernet 2 resides on device 1:

```
interface ethernet 1/2
 cpu-process
 monitor both 1 vlan 3
```

NOTE: For more information about configuring aVCS, see *Configuring ACOS Virtual Chassis Systems*.

Remove Mirror Port Configuration

To properly remove mirror port configuration, you must remove both the monitor configuration at the interface configuration level, and also the mirror-port configuration. Removing one without the other does not completely remove the mirror port configuration and may cause problems if you try to re-configure mirror ports at a later time.

An example of removing the monitor configuration:

```
ACOS(config)# interface ethernet 2
ACOS(config-if:ethernet:2)# no monitor output 2
```

An example of removing the mirror port configuration:

```
ACOS(config)# no mirror-port 2 ethernet 7 output
```

sFlow

ACOS can act as an sFlow agent by sampling random packets and sending statistics in an sFlow datagram to an external sFlow collector for analysis.

Some important implementation notes:

- sFlow data collection is supported only for individual Ethernet data ports and VE interfaces. Data collection cannot be performed on trunk interfaces, loopback interfaces, or on the management interface of ACOS.
- Host resource sampling is not supported:
- Application behavior sampling is not supported
- Configuration of sFlow agent behavior using SNMP is not supported

The following topics are covered:

sFlow Sampling Types

sFlow supports two types of sampling. One type of sampling uses a time-based approach to retrieve statistics for a specific interface, while the other approach samples information from the packet header of every Nth packet.

- You can enable one or both sampling types on a single Ethernet data port – the sampling types are not mutually exclusive.
- The sFlow datagram includes information about the incoming interface but not the outgoing interface where sampling occurred.
- sFlow data can be exported to up to 4 sFlow collectors. This offers the benefit of redundancy, as well as the ability to send sFlow datagrams to different destinations.

- By default, the sFlow datagrams use the management IP of ACOS as the source address, but you can modify the exported sFlow datagrams to the source address of your choice.

The following topics are covered:

Counter Polling Interval

This is a counter sampling method that is based on time. Statistics for an interface are gathered periodically and sent to the sFlow collector. You can specify the time interval (frequency) with which the counter interfaces statistics are gathered and sent. This global configuration will apply to all interfaces where sFlow is enabled unless a more granular value is configured at the interface level. You can enter a value ranging from 1–200 seconds. By default, this interval is set to 20 seconds.

Once ACOS has sampled statistics from a target interface, the information is collected and sent in an sFlow datagram to one or more sFlow collectors. The sFlow datagrams are listed in the Received and Transmitted counter fields in **`show interface`** CLI output, or on the **Network** > **Interface** page of the GUI.

Packet Sampling Rate

This is a sampling method that is based on the number of incoming packets. This sampling rate value essentially means that one packet is sampled out of every N packets. When expressed as a ratio, the packet sampling rate looks like 1/N. You can enter a value for N (the denominator) ranging from 10–1000000 packets. By default, N is equal to 1000, meaning that one packet is sampled out of every 1000 packets arriving at that interface. This global configuration will apply to all interfaces where sFlow data is collected, unless a more granular value has been configured at the interface level.

Unlike the other time-based sampling method, which gathers counter statistics for an interface, this packet-volume sampling approach gathers data about specific packets arriving at an interface. Information is extracted from the first 128 bytes in the header of the sampled packet, beginning with the MAC header. Once ACOS has

sampled packets from a specified target interface, the information is collected and sent in an sFlow datagram to one or more sFlow collectors.

Information Included in sFlow Datagrams

The following information is included in sFlow datagrams:

- Discarded packets

  Information about the discarded packets is included in the sFlow datagrams.

  For a list of Destination Unreachable codes associated with discarded packets, see section "**Input/Output Port Information**" in the following RFC: http://sflow.org/sflow_version_5.txt.

- Export CPU and Memory information

  CPU and memory information are included in the "Processor information" section of the exported sFlow datagram.

sFlow Configuration

The following topics are covered:

Configure sFlow Data Collection

The following list summarizes the high-level steps involved in configuring the sFlow data collection feature on an ACOS device:

1. Specify the sFlow collector where data will be exported.
2. (Optional) Enable use of the management interface's IP as the source address for outbound sFlow packets. This may be beneficial for filtering at the collector or to maintain consistency in the source address of the sFlow packets.
3. Specify the individual Ethernet data interfaces that will be sampled.
4. (Optional) Change the default data sampling rate or polling interval.

Configure Using GUI

1. Hover over **System** in the navigation bar, and select **Monitoring**.
2. Click **sFlow** on the menu bar. The sFlow update page appears.
3. Enter an IP address for the sFlow agent. By default, the management IP of ACOS is used, but you may enter a different address if desired.

NOTE: This information will appear in the Layer 4 information section of the sFlow datagram. Although the information is "textual" and is not used for routing decisions, it may be helpful in identifying which sFlow agent a particular packet came from, particularly in complex networks that have more than one sFlow agent.

4. (Optional) Enable Source IP use mgmt if you wish to use the ACOS device's management IP as the source address for exported sFlow datagrams. This changes the source address on the sFlow datagrams but has no effect on which interface the ACOS device selects for exporting sFlow datagrams.
5. (Optional) In the **Counter Polling Interval** field, specify the time interval at which the counter of interface statistics will be sampled. (See Counter Polling Interval for more information.)
6. (Optional) In the **Packet Sampling Rate** field, alter the default value if desired. Smaller numbers increase the sampling frequency, and larger numbers decrease the sampling frequency. (See Packet Sampling Rate for more information.)
7. (Optional) In the **Max Header** field, specify the number of bytes, from 14-512, that should be copied from a sampled packet.
8. (Optional) Select **Enable** in the CPU Usage field to enable CPU utilization monitoring.

9. (Optional) Select **Enable** in the Enable HTTP field to enable sFlow counter polling on HTTP interfaces.
10. In the Collector section:
    a. Select the **IPv4** or **IPv6** radio button for Type.
    b. Enter an IPv4 or IPv6 address in the Address field, depending on which IP protocol version was selected for Type.
    c. Enter a value in the **Port** field. This is the port on the collector where sFlow traffic will be sent. By default, traffic is sent to UDP port 6343.
    d. Click **Add** to add the sFlow collector's information
11. To enable time-based sFlow sampling, specify polling interfaces in the Polling Ethernet and/or Polling VE fields.
12. To enable packet volume-based sFlow sampling, specify sampling interfaces in the Sampling Ethernet and/or Sampling VE fields.
13. Click **Configure** to save your changes.

Configure Using CLI

This section contains CLI sFlow configuration examples.

The following commands specify the sFlow collector through port 5, and enable use of the management interface's IP as the source IP for the data samples sent to the sFlow collector:

```
ACOS(config)# sflow collector ip 192.168.100.3 5
ACOS(config)# sflow setting source-ip-use-mgmt
```

The following command enables counter polling for several Ethernet data interfaces, and uses the globally configured sampling rate by default:

```
ACOS(config)# sflow polling ethernet 1 to 8
```

The following command enables packet sampling for a range of Ethernet interfaces:

```
ACOS(config)# sflow sampling ethernet 3 to 5
```

The following command displays sFlow data collection statistics:

```
ACOS(config)# show sflow statistics
Interface      Packet Sample Records      Counter Sample Records
```

```
-----------------------------------------------------------------
1               3461                            81
2               20801                           81
3               0                               81
4               0                               81
5               0                               81
6               0                               81
7               0                               81
8               0                               81
9               0                               81
10              0                               81
11              0                               81
12              0                               81
-----------------------------------------------------------------
sflow total statistics
   Packet sample records:          24262
   Counter sample records:         972
   Sflow packets sent:             16257
```

sFlow Config Snippets for GUI Support

To support GUI functionality, small blocks of sFlow CLI config snippets have been added to the config. These sFlow snippets (below) may even appear in the config for users who are NOT using sFlow.

NOTE: If you see the sFlow config snippets below, it is recommended that you do NOT delete them, as deleting them may block access to the statistics that the GUI needs to generate certain charts.

Starting with the 4.1.4 release, the following sFlow configuration snippets may appear in the shared partition:

```
sflow setting local-collection
sflow collector ip 127.0.0.1 6343
```

And starting with the 4.1.4-P2 release, the following config snippet may appear in an L3V partition:

```
sflow collector ip 127.0.0.1 6343
```

The GUI requires presence of these sFlow snippets to display statistics in the charts that appear in the Dashboards panels (for example, FW Dashboard and SSLi Dashboard).

ACOS automatically adds these snippets to provide a better user-experience. The sFlow snippets enable local statistics collection, without which the charts in the GUI would appear blank.

Other Details

- These sFlow snippets are configured on a per-partition basis. If they are not already present, they will be automatically configured each time a user logs into the GUI and switches to that partition.
- If these sFlow config snippets are manually removed, they will be automatically added the next time a user logs into the GUI.
- The reason that the shared partition has one more command than the L3V is that the additional command “sflow setting local-collection” is only supported in the shared partition by design.

Call Home

Call Home enables ACOS devices to send diagnostic information securely to the A10 Product Research team. The diagnostic information includes configuration and environmental data such as the ACOS device, it's form factor, deployment location, number of interfaces, L3V partitions, VLANs, and more. It also collects information on the ACOS licenses activated on the device. All the information collected is used to improve the quality of the product.

NOTE: Call Home is enabled by default from ACOS 5.2.1-P8 and 6.0.2 versions onwards. You can choose to manually disable the Call Home feature on your ACOS device.

For Call Home to work, the following conditions must be met:

- **Internet Connection** — The ACOS device must be able to reach the internet for Call Home to send diagnostic data to the A10 end-point. This feature does not work with proxy server configuration.
- **Port** — The Call Home data from your ACOS device is sent over TLS protocol using port 443 by default.

The following topics are covered:

Enable Call Home

To enable Call Home, verify the internet connectivity and configure the call-home profile on the ACOS device.

```
ACOS(config)# call-home profile
ACOS(config-profile)# register
```

The `register` command enables the Call Home service. Once enabled, the Call Home data is collected from the ACOS device every 24 hours at midnight.

Disable Call Home

To disable Call Home, enter the following commands and save your configurations:

```
ACOS(config)# call-home profile
ACOS(config-profile)# deregister
```

The `deregister` command disables the Call Home service and stops the ACOS device from sending data to A10.

Verify Call Home Registration

To verify if Call Home is enabled successfully, run the following command:

```
ACOS(config)# show run call-home
!Section configuration: 33 bytes
!
call-home profile
register
!
```

Information Collected Using Call Home

The following Table 9 lists the diagnostic information collected using Call Home:

Table 9 : Diagnostic Information Collected Using Call Home

Parameter	Description
Registration Data	
Host Name	Unique name configured on the device.
UUID/Host-ID	Unique number to identify the device.
Hardware Platform	Device hardware platform such as Thunder 3350S, Thunder 7655S, vThunder, Thunder Container, and so on.

Table 9 : Diagnostic Information Collected Using Call Home

Parameter	Description
Product Model/Series-name	Model or series name provided to the device.
Platform Info	Device form factor such as hardware, Virtual Machine (VM), Bare Metal, or Container.
Virtualization Type	Device VM hypervisor type such as KVM, VMware, and so on.
Environmental Data	
CPUs	Number of physical cores.
Data CPUs	Number of data CPUs.
CPU Utilization	Each CPU average utilization. For example, {cpu1 – 50%, cpu2 – 60%, cpu3 – 40%}.
Deployment Location	Device deployment location such as on-prem, public, or private.
Public Cloud Type	Device deployed public cloud type such as AWS, Azure, OCI, and so on.
Memory Usage	Total memory utilization in the device.
SSL Cards	Number of SSL cards on the device.
GLM License Module	Information on the configured GLM license on the device such as SLB, GSLB, NGWAF, and so on.
Configuration Data	
Number of interfaces	Number of interfaces in the device.
Number of L3V partitions	Number of L3V partitions configured on the device.
Number of VLANs	Number of VLANs configured on the device.
Number of trunks	Number of trunks configured on the device.
VRRP-A state	VRRP-A state of the device.
VCS state	VCS state of the device.
Number of GLIDs	Number of GLIDs configured on the device.
Harmony Controller	Number of Harmony Controllers configured on the device.

Table 9 : Diagnostic Information Collected Using Call Home

Parameter	Description
State	
Number of class-lists	Number of class-lists configured on the device.
Number of access-lists	Number of access-lists configured on the device.
Number of routes	Number. of IP routes configured on the device
Number of LIFs	Number of Logical Interfaces (LIFs) configured on the device.
DNS Configured	DNS configured on the device.
Number of NTP server	Number of NTP server configured on the device.
Number of health monitors	Number of health monitors configured on the device.
Time zones	Time zone information configured on the device.
Number of IPv4 NAT pools	Number of IPv4 NAT pools configured on the device.
Number of IPv6 NAT pools	Number of IPv6 NAT pools configured on the device.
Number of real serv-ers	Number of SLB real serves configured on the device.
Number of virtual severs	Number of SLB virtual serves configured on the device.
Number of virtual ports	Number of SLB virtual ports configured on the device.
Number of templates	Number of SLB templates configured on the device.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol or SNMP, is a commonly used protocol for managing and monitoring network devices. It provides a standard way to collect network information, set configurations, and receive alerts about network devices. Thus, SNMP helps maintain network reliability and performance.

For more information on Simple Network Management Protocol, see SNMP MIB Reference.

ACL on Interface Monitoring

Access Control Lists (ACLs) are used to permit or deny incoming traffic on interfaces. They can be applied to both data and management interfaces. ACL provides visibility through the following capabilities:

- Logging – Logs are generated whenever an ACL is hit.
- Hit count – Tracks the number of times an ACL rule (permit or deny) is hit.

The management hit count is displayed only when:

- The ACL is bound to the management interface.
- The `enable-management` command is used to bind the ACL to the management interface.

NOTE:

- Ethernet information is only retrieved from the `enable-management` service and not from the access-list.
- For access-list configurations, only the `eq` operator is supported for IP ports. Currently, operators such as `lt` or `gt` are not supported and will be ignored.

Handling ACLs on Data and Management Interfaces

ACLs applied on data and management interfaces support logging and hit count. The logs can be viewed using the `show log` command and the hit count can be viewed using the `show access-list` command. For more information, see *Command Line Interface Reference*.

Example of `show log` for data interface:

```
ACOS(config)#show log
Sep 24 2024 11:30:13 Notice       [ACOS]:[eth 2] ICMP type 3 code 3
66.66.66.105 > 66.66.66.96  ACL rule permitted this packet (ACL 5)
Sep 24 2024 11:30:13 Notice       [ACOS]:[eth 2] ICMP type 8 code 0
66.66.66.105 > 66.66.66.96  ACL rule permitted this packet (ACL 5)
```

Example of `show access-list` for data interface:

```
ACOS(config)#show access-list
access-list 5 4 permit host 66.66.66.105 log Data plane hits: 37
```

When ACLs are applied to the management interface, the hit counts are generated. This helps to monitor both permitted and denied traffic, track the total number of hits, and evaluate the effectiveness of ACLs.

Example of `show log` for management interface:

```
ACOS(config)#show log
Sep 24 2024 11:27:53 Notice      [ACOS]: TCP 192.30.8.183:54420 >
10.64.19.96:22  ACL rule permitted this packet (ACL team_1)
Sep 24 2024 11:27:52 Notice      [ACOS]: TCP 192.30.8.183:54420 >
10.64.19.96:22  ACL rule permitted this packet (ACL team_1)
Sep 24 2024 11:27:52 Notice      [ACOS]: TCP 192.30.8.183:54420 >
10.64.19.96:22  ACL rule permitted this packet (ACL team_1)
Sep 24 2024 11:27:51 Notice      [ACOS]: TCP 192.30.8.183:54420 >
10.64.19.96:22  ACL rule permitted this packet (ACL team_1)
```

Example of `show access-list` for management interface:

```
ACOS# show access-list ipv4 50
Management hit count: 175
access-list 50 permit 198.162.12.0 0.0.0.255 Data plane hits:
0, Management plane hits: 175
```

Contact Us