OmniSwitch 2260/2360 AOS Release 5.2R1 WebView Guide

Alcatel·Lucent
Enterprise

www.al-enterprise.com

This user guide documents AOS Release 5.2R1
The functionality described in this guide is subject to change without notice.

Alcatel·Lucent
Enterprise

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505

Service & Support Contact Information
North America: 800-995-2696
Latin America : 877-919-9526
EMEA: +800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific: +65 6240 8484
Web: myportal.al-enterprise.com
Email: ebg_global_supportcenter@al-enterprise.com

Contents

BLANK PAGE

List of Figures

About This Guide

This OmniSwitch 2260,2360 AOS Release 5.2R1 WebView Guide describes basic attributes of your switch and basic switch administration tasks. The software features described in this manual are shipped standard with your OmniSwitch 2260, 2360 switches. These features are used when readying a switch for integration into a live network environment.

OmniSwitch 2260, 2360 AOS software provides rich Layer 2 and Quality of Service (QoS) functionality for switches operating in small office/home office networks. This guide describes how to configure AOS software features by using the Web-based graphical user interface (GUI).

Supported Platforms

This information in this guide applies to the following product:

• OmniSwitch 2260 Series

• OmniSwitch 2360 Series

Who Should Read this Manual?

The information in this guide is intended for any of the following individuals:

• System administrators who are responsible for configuring and operating a network using OS2260/OS2360 AOS software.

• Software engineers who are integrating OS2260/OS2360 AOS software into a switch product.

• Level 1 and/or Level 2 Support providers

To obtain the greatest benefit from this guide, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of ethernet and networking concepts.

This document is designed as a reference for you to configure your devices. It provides instructions for general scenarios, but does not cover all use cases of all product models. The examples given may differ from your use case due to differences in software versions, models, and configuration files. When configuring your device, alter the configuration depending on your use case.

What is in this Manual?

This configuration guide includes information about the following features:

- Basic switch administrative features, such as file editing utilities, and setting up system information (name of switch, date, time).

- Basic security features, such as switch access control and customized user accounts.

- SNMP

- Web-based management (WebView) of OmniSwitch 2260/2360.

Further information on WebView can be found in the context-sensitive on-line help available with that application.

How is the Information Organized?

This guide contains the following sections:

- Chapter 1, "Getting Started."contains information about performing the initial system configuration and accessing the user interfaces.

- Chapter 2, "Configure Physical Features." describes how to configure physical features such as Chassis Management, Ethernet, System Management and WLAN Configuration.

- Chapter 3, "Configure Layer 2 Features." describes how to manage and monitor the layer 2 switching features such as VALN, Spanning Tree and Link Aggregation.

- Chapter 4, "Configure Networking Features." contains information about configuring networking features such as IP, IP Multicast, Services, and DHCP.

- Chapter 5, "Configure Security Features." contains information about configuring switch security information such as port AAA, Access Guardian, Authenticated Switch Access, and Port Security settings.

- Chapter 6, "Configure QoS." describes how to manage QOS, QOS Groups, and TCAM Manager features.

- Chapter 7, "Device Management." describes how to configure device management features such as Interfaces, SNMP and Net Monitoring.

Documentation Roadmap

The OmniSwitch user documentation suite was designed to supply you with information at several critical junctures of the configuration process.The following section outlines a roadmap of the manuals that will help you at each stage of the configuration process. Under each stage, we point you to the manual or manuals that will be most helpful to you.

Stage 1: Using the Switch for the First Time

Pertinent Documentation: *OmniSwitch 2260,2360 Hardware Users Guides*
OmniSwitch 2260,2360 AOS Release 5.2R1 Release Notes

This guide provides all the information you need to get your switch up and running the first time. It provides information on unpacking the switch, rack mounting the switch, setting the switch's IP address, and setting up a password. It also includes succinct overview information on fundamental aspects of the switch, such as hardware LEDs, the software directory structure, CLI conventions, and web-based management.

At this time you should also familiarize yourself with the Release Notes that accompanied your switch. This document includes important information on feature limitations that are not included in other user guides.

Stage 2: Gaining Familiarity with Basic Switch Functions

Pertinent Documentation: *OmniSwitch 2260,2360 Hardware Users Guides*
OmniSwitch 2260,2360 AOS Release 5.2R1 WebView Guide

Once you have your switch up and running, you will want to begin investigating basic aspects of its hardware and software. Information about switch hardware is provided in the *Hardware Guide*. This guide provide specifications, illustrations, and descriptions of all hardware components, such as chassis, power supplies, Chassis Management Modules (CMMs), Network Interface (NI) modules, and cooling fans. It also includes steps for common procedures, such as removing and installing switch components.

Anytime

The *OmniSwitch 2260,2360 AOS Release 5 CLI Reference Guide* contains comprehensive information on all CLI commands supported by the switch. This guide includes syntax, default, usage, example, related CLI command, and CLI-to-MIB variable mapping information for all CLI commands supported by the switch. This guide can be consulted anytime during the configuration process to find detailed and specific information on each CLI command.

Related Documentation

The following are the titles and descriptions of all the related OmniSwitch user manuals:

- *OmniSwitch 2260,2360 AOS Release 5.2R1 Release Notes*

  Includes critical Open Problem Reports, feature exceptions, and other important information on the features supported in the current release and any limitations to their support.

- *OmniSwitch 2260, 2360 Hardware Users Guides*

  Describes the hardware and software procedures for getting an OmniSwitch up and running as well as complete technical specifications and procedures for all OmniSwitch chassis, power supplies, and fans.

- *OmniSwitch 2260,2360 AOS Release 5 CLI Reference Guide*

  Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- Technical Tips, Field Notices

  Includes information published by Alcatel-Lucent Enterprise's Customer Support group.

Technical Support

An Alcatel-Lucent Enterprise service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel-Lucent Enterprise features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners.

With 24-hour access to Alcatel-Lucent Enterprise's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel-Lucent Enterprise's technical support, open a new case or access helpful release notes, technical bulletins, and manuals.

Access additional information on Alcatel-Lucent Enterprise's Service Programs:

Web: myportal.al-enterprise.com

Phone: 1-800-995-2696

Email: ebg_global_supportcenter@al-enterprise.com

1 Getting Started

OmniSwitch AOS provides rich Layer 2 and Quality of Service (QoS) functionality for switches operating in Enterprise office networks. This guide describes how to configure OmniSwitch 2260/2360 software features by using the Web-based graphical user interface (GUI).

To obtain the greatest benefit from this guide, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of Ethernet and networking concepts.

Connecting the Switch to the Network

To enable remote management of the switch through a Web browser or SNMP, the switch must be connected to the network. The switch is preconfigured with an IP address for the device management. The switch can also be configured to acquire its address from a DHCP server on the network.

Remote Configuration Login (RCL)

Remote Configuration Load (RCL) is a feature on the switch, which automates and simplifies the deployment of large network installations eliminating the need for manual configuration of each switch. When the switch is connected in the network, RCL process is triggered to obtain IP address automatically.

When RCL process is triggered, DHCP client interface is created and it gets file server details through DHCP offer. It then downloads the configuration fiels from the file server and implements the commands. Auto Reload of the switch is based on the configuration and the switch is automatically configured.

For more information on Remote Configuration Login, see "Managing Automatic Remote Configuration Download" on page 8-1

Note. If RCL is not triggered, the switch can be configured using the default management IP addresses.

Note. The default IP address will not be removed if only image upgrade is done and not the config file download through RCL. The default IP address will not be removed if the config file is empty.

Using the Default Management IP Address

By default, the OmniSwitch is assigned the following static IP information for access to the AOS WebView:

- IP address: https://192.168.1.3

- Network mask: 255.255.255.0

1 Connect the switch to the management PC or to the network using any of the available network ports.

2 Power on the switch. Set the IP address of the management PC's network adapter to be in the same subnet as the switch.
Example: Set it to IP address 192.168.1.3, mask 255.255.255.0

3 Enter the IP address shown above in the Web browser.

Thereafter, use the Web interface to configure a different IP address or configure the basic parameters of the switch.

Using the Web Interface

Use the following procedures to log on to the Web Interface:

1 Open a Web browser and enter the IP address of the switch in the Web browser address field.

2 Type the user name and password into the fields on the login screen, and then click **Login**.

The user name and password are the same as those you use to log on to the command-line interface. By default, the user name is **admin**, and password **switch**.
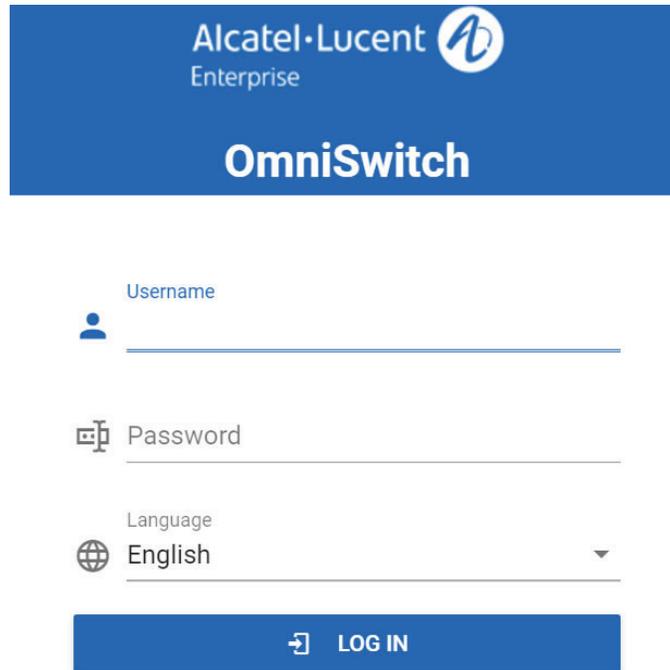
Figure 1-1 : WebView Login Page

WebView Interface

On successful login, the WebView Home Page is displayed. The Home Page displays a dashboard with application widgets that provide a quick overview of key applications. The Global tab displays CMM Utilization, System Information and Vlan Usage.
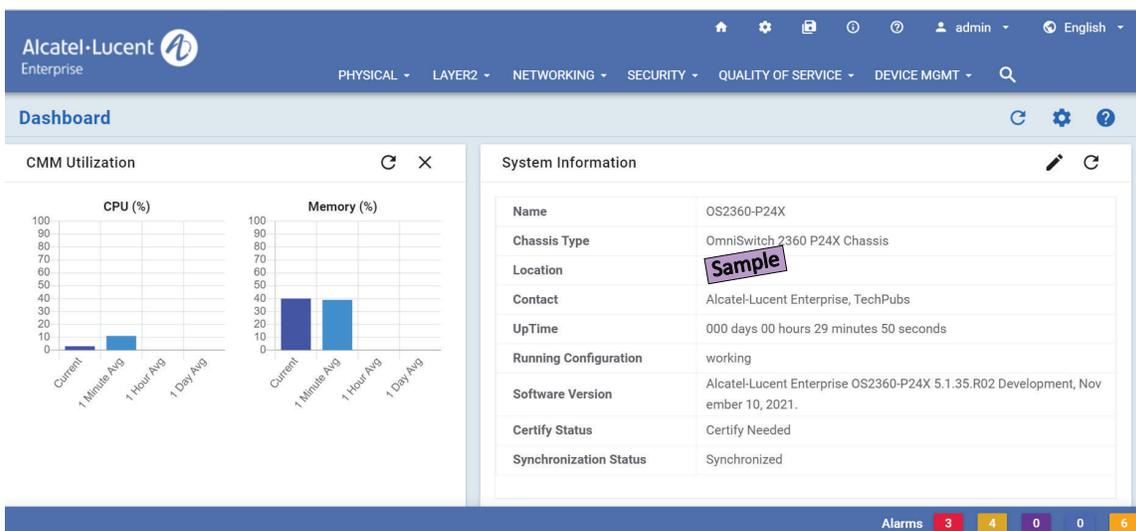
Figure 1-2 : WebView Dashboard

Navigation Buttons

OmniSwitch 2260/2360 provides standard tools for interacting with configuration screens. These buttons are typically located at the top-right of each screen and include:

Table 1-1 : Navigation Buttons

Navigation Button	Description
+	**Create/Add** Click the Create/Add button to create a new entry within the configuration screen.
	Modify To modify or edit an existing entry, select the entry in the configuration screen and click the Modify button.
	Delete To delete an entry, select the entry and click the Delete button.
ACTION ⌄	**Action** To enable or disable an existing entry, select the entry in the configuration screen and click on Action button. To clear statistics of an entry, select the entry in the configuration screen and click on Action button.
	Export To export the details of the information page to an excel file, select the entry and click the Export button.
	Refresh The Refresh button loads the latest data for an application table, chart or list.
	Help Click on the Help button to load context-sensitive help of the table or configuration screen.
	MIB Information Click on the MIB Information button to load SNMP MIB Variables used for that particular Page.
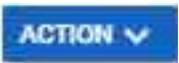
WebView Menu

The WebView page has the following areas:

- Banner

- Horizontal Menu

- Vertical Menu

- View/Configuration Area
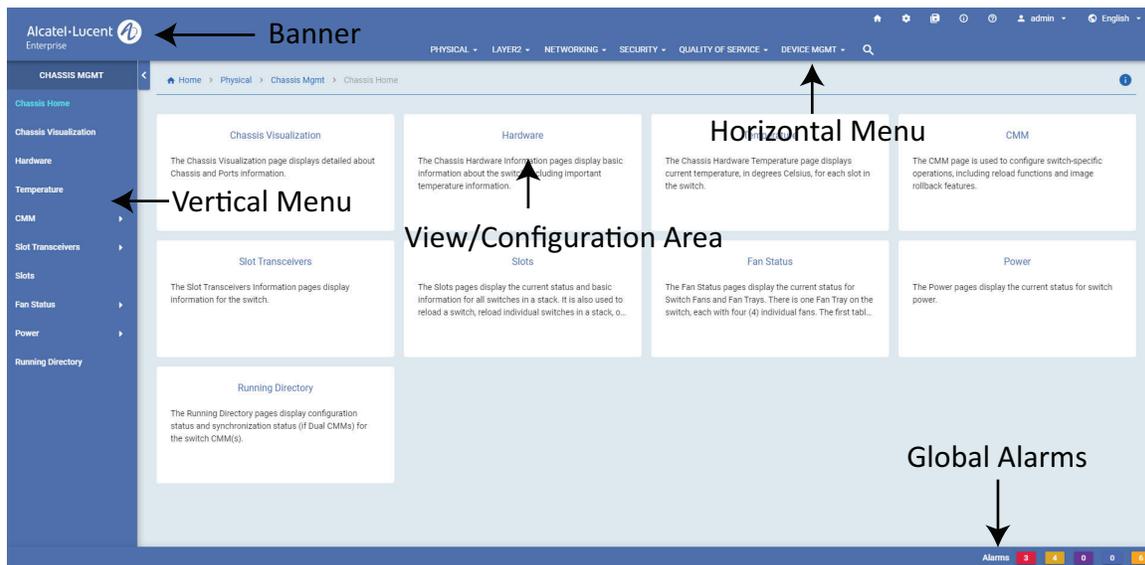
Figure 1-3 : WebView Menu

Banner

The banner contains the Company Logo, Quick Config, Write Memory, About, Help, Username, and Language.

Horizontal Menu

The horizontal menu contains the seven main configuration groups of the switch. It is Physical, Layer 2, Networking, Security, Quality of Service and Device Management.

Vertical Menu

Vertical Menu displays all the available configuration options for the selected configuration group from the horizontal menu.

View or Configuration Area

View or configuration area displays the configuration information for the selected configuration option in the vertical menu.

Global Alarm

The alarm or traps will be displayed on the bottom of the screen of the WebView 2.0 page. The alarm is displayed with the severity levels Critical, High, Medium. Low, and Warning.The alarm notification will also display the number of alarms generated for the severity level. On clicking the alarm severity, the alarm details are displayed.

Figure 1-4 : Global Alarm

Viewing System Information

After you login, the Home Page of the Switch the dashboard displays the CMM Utilization and System Information of the switch.

Table 1-1 : CMM Utilization Fields

Field	Description
CMM Utilization	Display the current, 1 minute average, 1 hour average, 1 day average CPU and Memory usage of the switch. It will auto refresh every 60s.
System Information	Showing general information of the switch
VLAN usage	Showing all VLAN for each type was created in the switch.
Port Statistic	Show general information of all port in the switch

The system information page displays basic information of the switch such as the configurable switch name, description, object ID, up time, contact details, date, time and timzone.

To update the system information configuration, Click on **Modify** button to open the system configuration dialog.

- **System Information :** Enter the switch contact details, name and location. You cannot edit the description, object ID, and Up Time of the switch.

- **System Time/Date Configuration:** Enter the date, time and timezone. Enable if Daylight Saving Time is in effect in the timezone.

Click **Apply** to implement the changes.

WebView Language Option

WebView supports multiple language. It currently supports English and Simplified Chinese.

The language can be selected from the login screen.
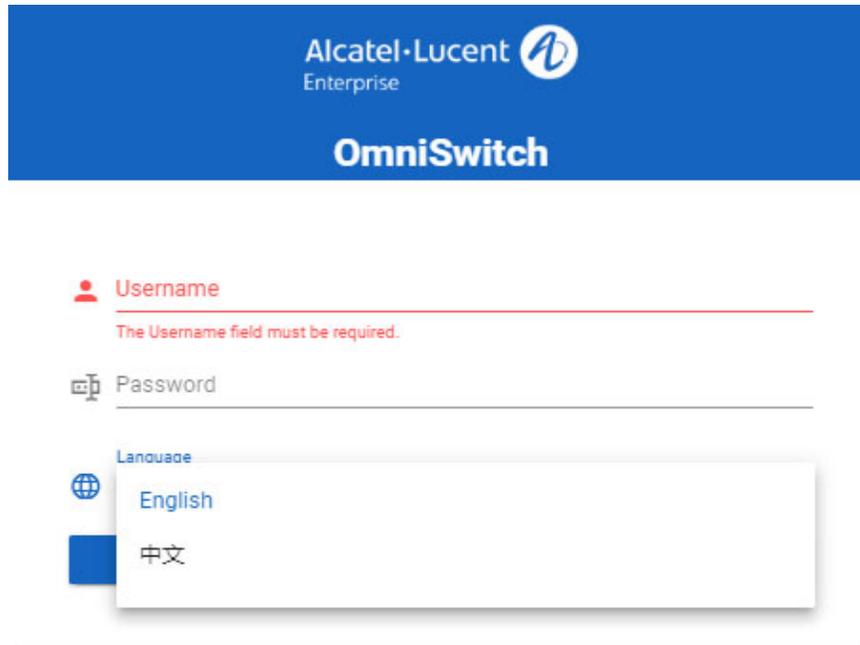
Figure 1-5 : Language Selection in Login Screen

The language can also be selected any time after login by clicking on the language displayed on the Banner from any page of WebView.
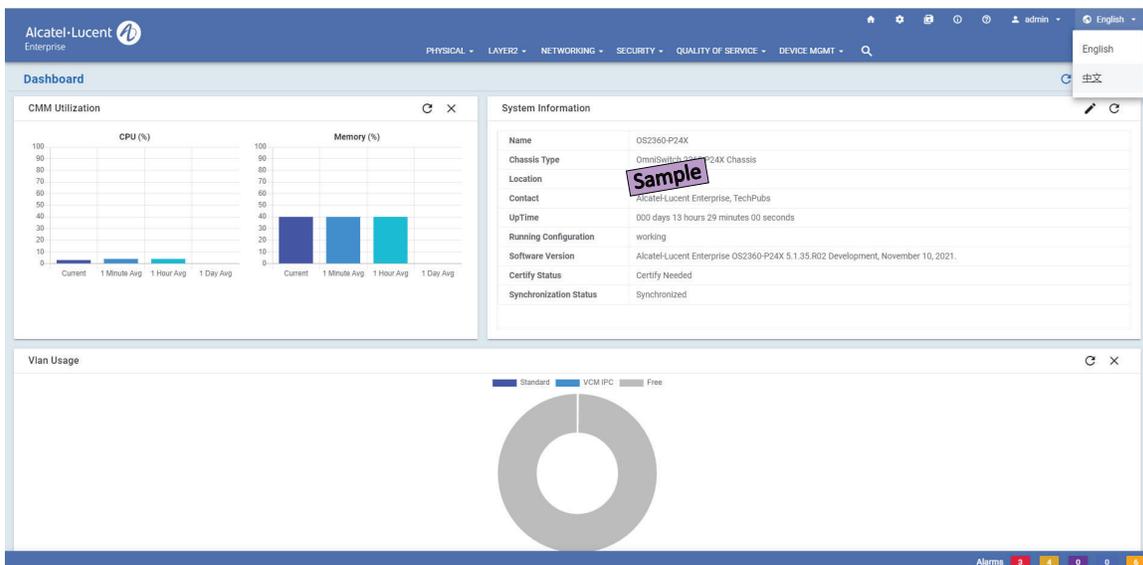
Figure 1-6 : Language Selection From Banner

A sample WebView page in Chinese
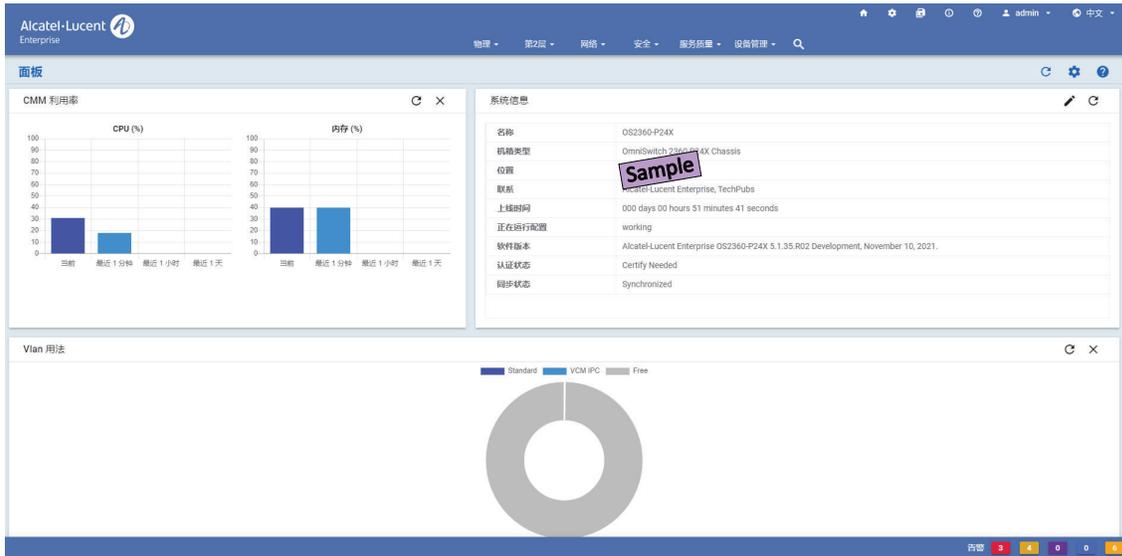
Figure 1-7 : WebView in Chinese

Help Access Page

The **Help** button is always available in the upper right corner of the active page. Click Help to open a new page that contains information about the configuration fields, status fields, and command buttons available on the active page. The online help pages are context sensitive. For example, if the VLAN page is open, the help topic for that page displays if you click Help.

MIB Information

The MIB information for that particular feature can be accessed from the top right corner of the WebView. Click on **i** button to view the MIB information.

2 Configure Physical Features

In This Chapter

This chapter provides an overview of the following physical menu components:

- Chassis Management (see "Chassis Management" on page 2-2)

- Virtual Chassis (see "Accessing the Virtual Chassis Menu" on page 2-3)

- Health (see "Health Monitoring" on page 2-4)

- Ethernet (see "Ethernet Configuration" on page 2-5)

- Adjacencies (see "Adjacencies Configuration" on page 2-7)

- Console Port (see "Console Port Configuration" on page 2-9)

- System Management (see "System Management Configuration" on page 2-11)

- WLAN Configuration (see "WLAN Configuration" on page 2-13)

Accessing the Physical Menu

The Physical Menu can be accessed from the WebView page by clicking on the **PHYSICAL** label on the horizontal menu bar on the home page.

The following screen displays the **PHYSICAL** menu components
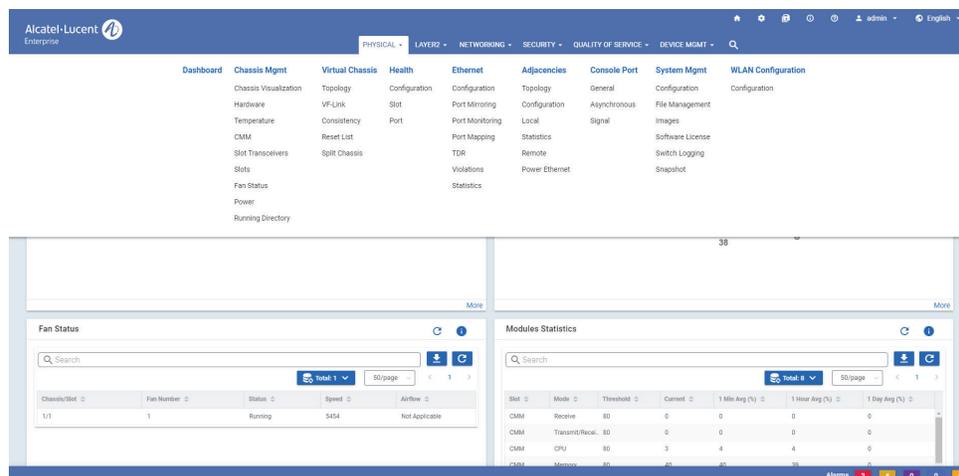
Figure 2-1 : PHYSICAL Menu Screen

Chassis Management

Chassis Management and Monitoring allow you to configure and view hardware-related operations on the switch.

Accessing Chassis Management Menu

The Chassis Management web interface can be accessed from the WebView page by clicking on the **Chassis Mgmt** label under the Physical group.

To configure the Chassis Management information, click **PHYSICAL > Chassis Mgmt** in the menu.

The following screen displays the **Chassis Management** menu components.
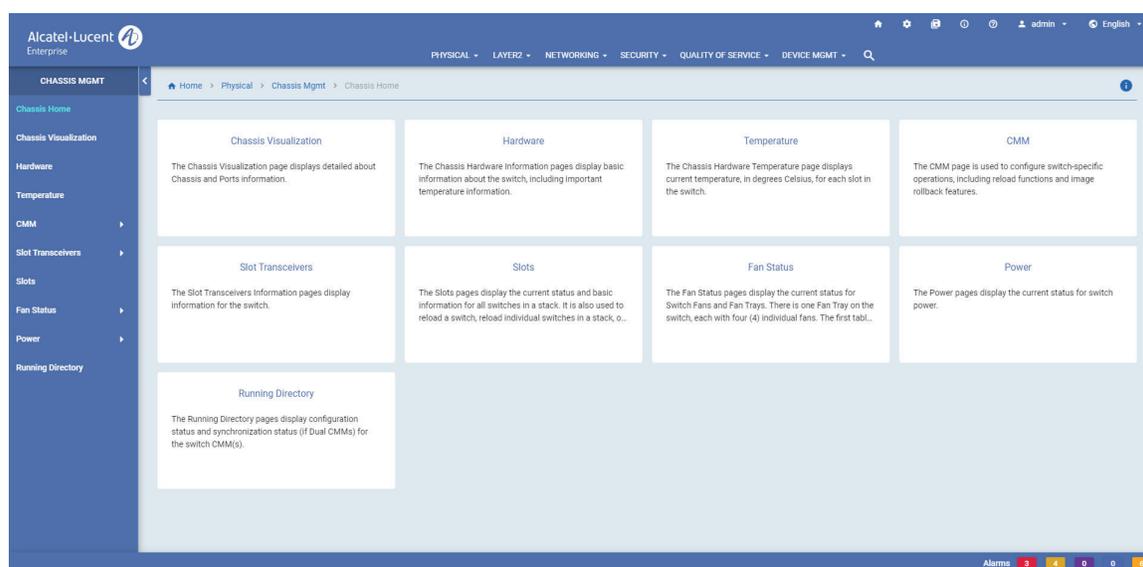
Figure 2-2 : Chassis Management Home

The Chassis Management Home page allows to configure and manage the following chassis management features:Virtual Chassis

Table 2-2 : Chassis Management Features

Features	Description
Chassis Visualization	Allows to view Chassis, slot and Port information.
Hardware	Allows to view basic information about the switch, including important temperature information.
Temperature	Allows to view current temperature, in degrees Celsius, for each slot in the switch.
CMM	Allows to: **Management:** Configure switch-specific operations, including takeover, shutdown, reload and image rollback functions. **Software:** View basic switch software information. **Hardware:** View basic hardware and status information for the switch. **Hardware Component:** View current switch hardware information.

Table 2-2 : Chassis Management Features

Features	Description
Slot Transceivers	Allows to: **Information:** View GBIC information for the switch. **DDM:** Enable or Disable DDM status and DDM trap status on the switch.
Slots	Allows to view current status and basic information for all switches in a stack.
Fan Status	Allows to view current status for switch fans and the switch fan trays.
Power	Allows to: **Power Supplies:** View current status for switch power supplies. **Power Monitor:** View hardware information and current status for chassis power supplies. **Inline Power:** View inline power settings for all Power on LAN (PoL) slots or ports in the corresponding chassis ID. **Update:** Update inline power file settings for specific Power on LAN (PoL) ports in a corresponding slot. **Policy:** Configure and view Power Policy Rules, Rule bindings and Power Rule assigned to specific ports.
Running Directory	Allows to view configuration status and synchronization status (if Dual CMMs) for the switch CMM(s).

A Virtual Chassis is a group of switches managed through a single management IP address and that behave as a single bridge or router. It provides both node level and link level redundancy for devices connecting to the aggregation layer via dual-homed standard 802.3ad link aggregation mechanisms.

Accessing the Virtual Chassis Menu

The Virtual Chassis web interface can be accessed from the WebView page by clicking on the **Virtual Chassis** label under the Physical group.

To configure the Virtual Chassis information, click **PHYSICAL > Virtual Chassis** in the menu.

The following screen displays the **Virtual Chassis** menu components.
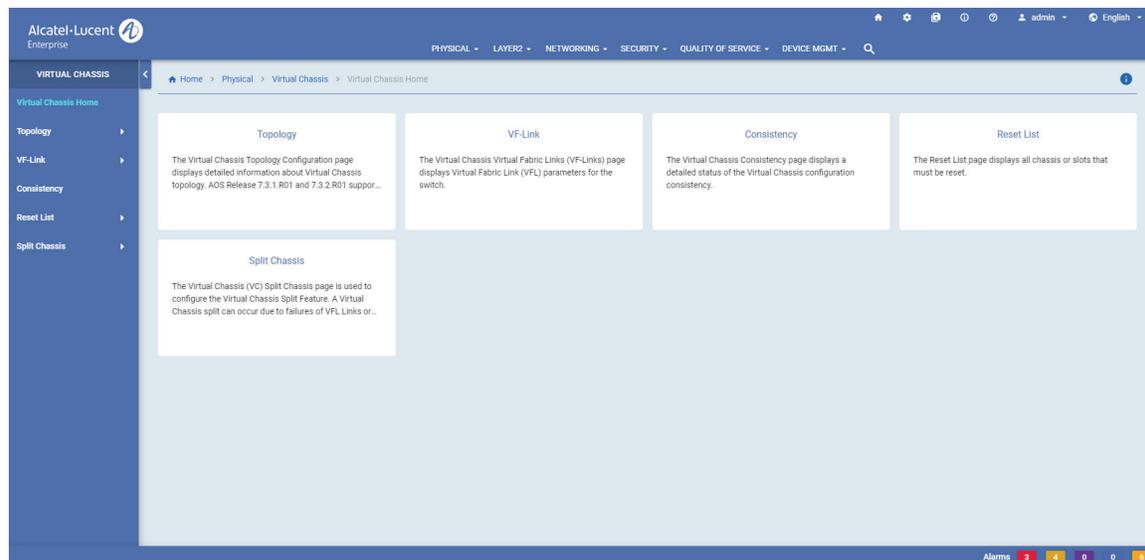
Figure 2-3 : Virtual Chassis Home

The Virtual Chassis page allows to configure and manage the following virtual chassis features:

Table 2-3 : Virtual Chassis Features

Features	Description
Topology	Allows to: **Global Configuration:** Configure and view global information about Virtual Chassis topology. **Configuration:** View detailed information about Virtual Chassis topology. **Status:** View detailed status of the Virtual Chassis topology. **Neighbors:** View information about the local switch shortest path to its neighbors.
Consistency	Allows to view detailed status of the Virtual Chassis configuration consistency.
Reset List	Allows to: **Chassis:** View chassis that must be reset along with a specified chassis, to prevent Virtual Chassis split. **Slot:** View slots that must be reset to prevent Virtual Chassis split.
VF-Link	The Virtual Chassis Fabric Links (VF-Links) page allows you to view the Virtual Fabric Link (VFL) parameters for the switch.
Split-Chassis	The Virtual Chassis (VC) Split Chassis page allows you to configure the Virtual Chassis Split Feature. A Virtual Chassis split can occur due to failures of VFL Links or Virtual Chassis resulting in the Master Chassis having the same system MAC and IP address.

Health Monitoring

The Health Monitoring function monitors the consumable resources of the switch (for example, bandwidth usage, CPU usage) and provides a single integrated resource for a Network Management System (NMS). This function monitors the switch, and at fixed intervals, collects the current values for each

resource being monitored. Users specify resource threshold limits and traps are sent to an NMS if a value falls above or below a user-specified threshold.

Accessing the Health Monitoring Menu

The Health Monitoring web interface can be accessed from the WebView page by clicking on the **Health** label under the Physical group.

To configure the Health Monitoring information, click **PHYSICAL > Health** in the menu.

The following screen displays the **Health** menu components.
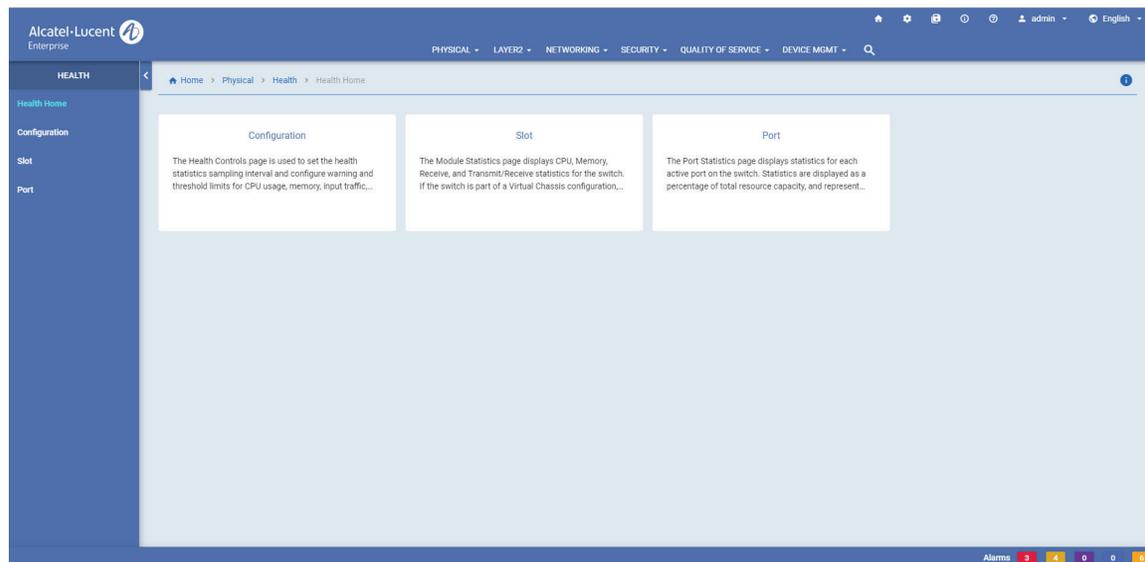
Figure 2-4 : Health Home

The Health Monitoring page allows to configure and manage the following Health Monitoring features:

Table 2-4 : Health Monitoring Features

Features	Description
Configuration	Allows to set the health statistics sampling interval and configure warning and threshold limits for CPU usage, memory, input traffic, input/output traffic, and device temperature.
Slot	Allows to view CPU, Memory, Receive, and Transmit or Receive statistics for each active slot on the switch.
Port	Allows to view statistics for each active port on the switch.

Ethernet Configuration

The Ethernet Configuration is responsible for configuring and monitoring Ethernet ports. This includes:

• Performing hardware diagnostics, loading software, and initializing hardware.

- Notifying other software modules in the system when Ethernet links become active or inactive.

- Configuring basic line parameters for Ethernet ports.

- Gathering basic line statistics for Ethernet ports and passing this information to the user interface and configuration manager.

Accessing the Ethernet Configuration Menu

The Ethernet web interface can be accessed from the WebView page by clicking on the **Ethernet** label under the Physical group.

To configure the Ethernet information, click **PHYSICAL > Ethernet** in the menu.

The following screen displays the **Ethernet** menu components.
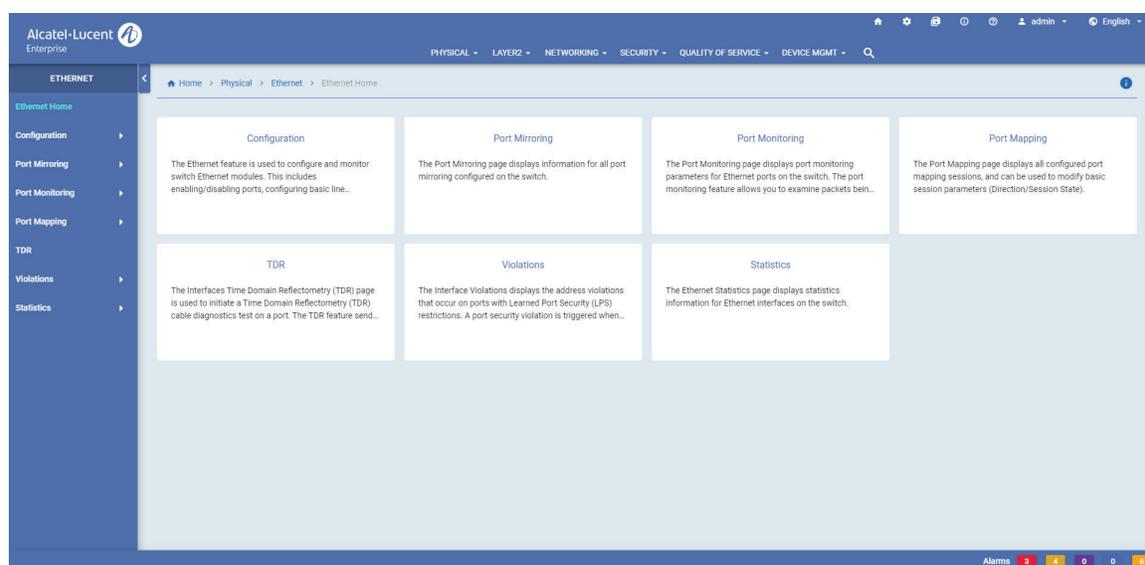
Figure 2-5 : Ethernet Home

The Ethernet configuration page allows to configure and manage the following Ethernet features:

Table 2-5 : Ethernet Features

Features	Description
Configuration	Allows to: **General:** View general configuration information for Ethernet interfaces on the switch. Also, enable or disable an interface(s), and modify interface general parameters. **Extended:** View detailed information about interfaces on the switch. **Status:** View configuration information for Ethernet interfaces on the switch. **Flood Control:** View incoming traffic level, compare it with the thresholds configured by the administrator, and drop traffic when incoming traffic level exceeds the set thresholds.

Table 2-5 : Ethernet Features

Features	Description
Port Mirroring	Allows to: **Status:** Configure and view port to mirror and the port that is to receive data from the mirrored port. Also, enable or disable remote port mirroring. **Session:** Configure and view information for all port mirroring session configured on the switch.
Port Monitoring	Allows to: **Ports:** Configure and view port monitoring parameters for Ethernet ports on the switch. Also, enable or disable port monitoring and modify the port monitoring parameters. **Sessions:** Configure and view port monitoring session. Also, enable or disable and Modify port monitoring sessions.
Port Mapping	Allows to: **Ports:** Assign Chassis/Slot/Ports into Port Mapping session. **Sessions:** Configure basic session parameters and view the status of all configured port mapping sessions.
TDR	The Interfaces Time Domain Reflectometry (TDR) page allows you to initiate a Time Domain Reflectometry (TDR) cable diagnostics test on a port. The TDR feature sends signal down a cable to determine the distance to a break or other discontinuity in the cable path. The length of time it takes for the signal to reach the break and return is used to estimate the distance to the discontinuity.
Violations	Allows to: **Global:** Configure and view global violation recovery configuration details. **Port Status:** View port security violations that occur on ports with Learned Port Security (LPS). **Recovery Ports:** View configured interface violation parameters, and modify parameters on specific ports.
Statistics	Allows to: **Input:** View switch interface input statistics. **Output:** View switch interface output statistics. **Input Counters:** View switch interface input counter statistics. **Output Counters:** View switch interface output counter statistics. **General:** View general Input and Output interface information and statistics for Ethernet interfaces on the switch. **Accounting:** View input and output accounting information for Ethernet interfaces on the switch. **Counters:** View counter statistics information for Ethernet interfaces on the switch. **Counters Errors:** View counter error statistics information for Ethernet interfaces on the switch. **Traffic:** View traffic information for Ethernet interfaces on the switch.

Adjacencies Configuration

Adjacencies build the topology map of all the adjacencies device. It allows to manage the LLDP parameters, MED network policy, and power ethernet.

Accessing the Adjacencies Menu

The Adjacencies web interface can be accessed from the WebView page by clicking on the **Adjacencies** label under the Physical group.

To configure the Adjacencies information, click **PHYSICAL > Adjacencies** in the menu.

The following screen displays the **Adjacencies** menu components.
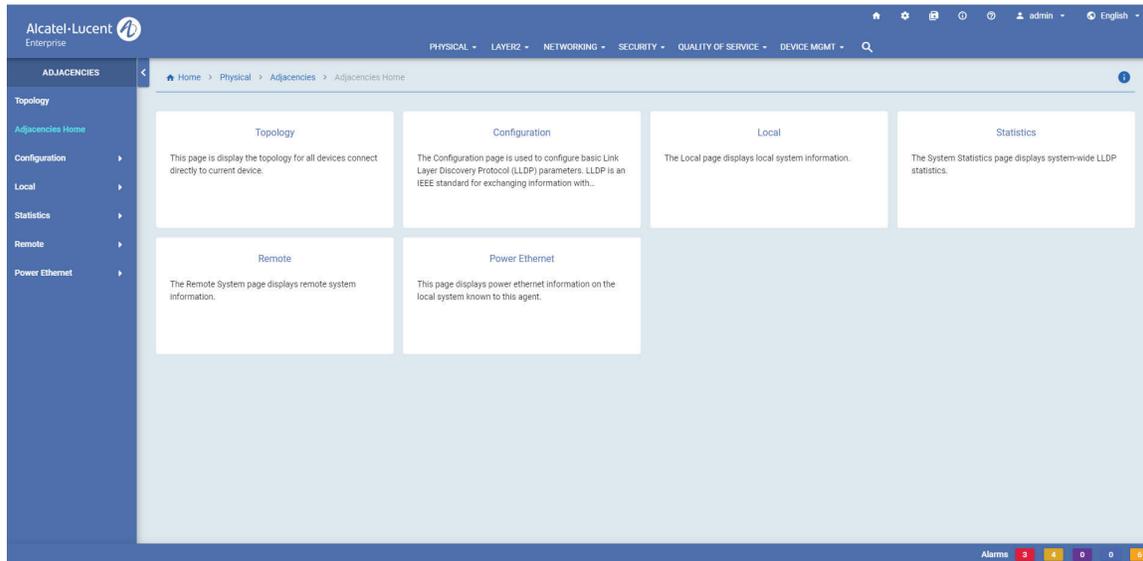
Figure 2-6 : Adjacencies Home

The Adjacencies configuration page allows to configure and manage the following Adjacencies features:

Table 2-6 : Adjacencies Features

Features	Description
Topology	Allows to view adjacencies device topology and device information that is connected to the current device.
Configuration	Allows to: **System:** Configure basic Link Layer Discovery Protocol (LLDP) parameters. **Port:** View LLDP port information. **Trust Agent:** View LLDP security mechanism globally (chassis level) or for a slot or a single port.
Local	Allows to: **System:** View local system information. **MED Network Policy:** Configure and view network policies in the local system and the network policies that are bound to ports. **Port:** View port information. **Agent Destination Address:** View the destination MAC addresses used for LLDP-DUs.
Statistics	Allows to: **System:** View system-wide LLDP statistics. **Port:** View LLDP statistics by port.

Table 2-6 : Adjacencies Features

Features	Description
Remote	Allows to: **System:** View remote system information. **Trusted Remote Agent:** View Remote Agent Information. **MED Inventory:** View remote system MED inventory information. **MED Network Policy:** View the remote system MED network policies known to the switch. **Application TLV:** View the remote application TLV information.
Power Ethernet	Allows to: **802.3X Information:** View power ethernet information (as a part of the LLDP 802.3 organizational extension) on the local system known to this agent. **MED TLV Ext Information:** View Adjacency Power Ethernet detailed information on the local MED TLV Ext Information. **802.3 TLV Information:** View Adjacency Power Ethernet detailed information on the remote 802.3 TLV Information.

Console Port Configuration

Console port is the management port of the switch. It is used to connect the devices to the switch. The status of console port can be viewed and managed.

Accessing the Console Port Menu

The Console Port web interface can be accessed from the WebView page by clicking on the **Console Port** label under the Physical group.

To configure the Console Port information, click **PHYSICAL > Console Port** in the menu.

The following screen displays the **Console Port** menu components.
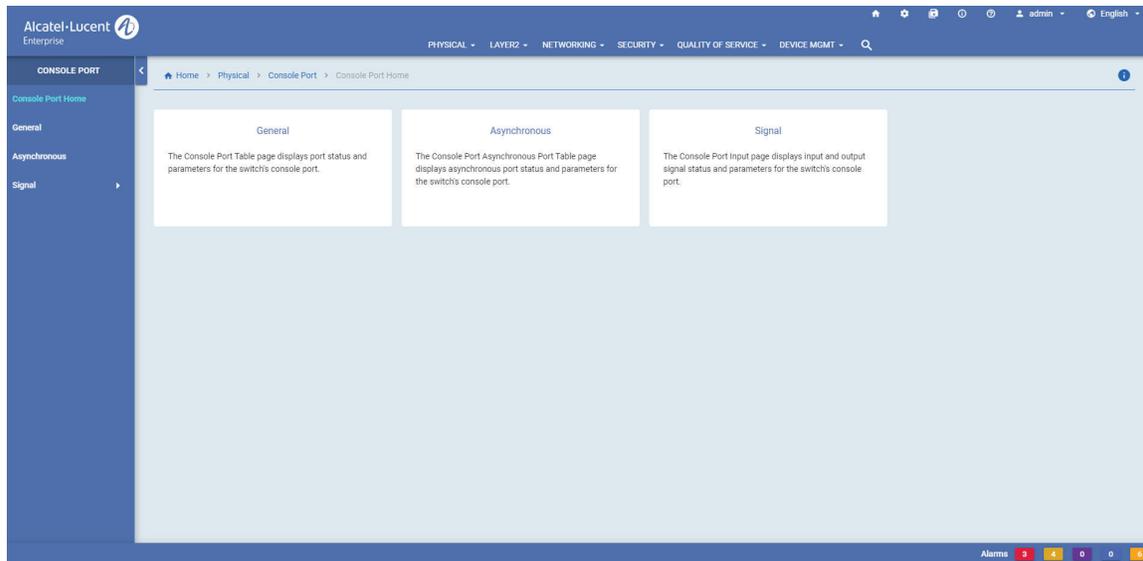
Figure 2-7 : Console Port Home

The Console Port configuration page allows to configure and manage the following Console Port features:

Table 2-7 : Console Port Features

Features	Description
General	Allows to view port status and parameters for the switch's console port.
Asynchronous	Allows to view asynchronous port status and parameters for the switch's console port.
Signal	Allows to: **Input:** View input signal status and parameters for the switch's console port. **Output:** View output signal status and parameters for the switch's console port.

System Management Configuration

The system management allows to configure and manage basic system information and logs of the switch.

Accessing the System Management Menu

The System Management web interface can be accessed from the WebView page by clicking on the **System Mgmt** label under the Physical group.

To configure the System Management information, click **PHYSICAL > System Mgmt** in the menu.

The following screen displays the **System Mgmt** menu components.

Figure 2-8 : System Management Home

The System Mgmt configuration page allows to configure and manage the following System Management features:

Table 2-8 : System Management Features

Features	Description
Configuration	Allows to view basic switch system information and set date and time.
File Management	Allows to manage and view files in the switch and application management module(s).
Images	Allows to: **Loaded Images:** View list of all software image files currently loaded on the switch. **Images in Flash:** View list of all software image files currently loaded on the switch in flash memory.

Table 2-8 : System Management Features

Features	Description
Switch Logging	Allows to: **Logging Output:** Enable or disable Switch Logging and configure Remote Sockets. **Change Logging Levels:** Set, change or restore the Severity Level settings for the Applications shown on the Log Level Settings page. **Tech Support:** Create status and statistics log files using Command Line Interface (CLI) show commands.
Snapshot	Allows to: **Create Virtual Chassis Snapshot:** Create a snapshot file of a Virtual Chassis configuration on the switch. **Apply Snapshot:** Apply a configuration file to the switch.
Software license	Allows you to view the WebView license information and to activate the WebView advanced feature license.

Updating the System Information Configuration

The system information page displays basic information of the switch such as the configurable switch name, description, object ID, up time, contact details, date, time and timzone.

To update the system information configuration, navigate to **PHYSICAL > System Mgmt> Configuration** in the menu.

- **System Information :** Enter the switch contact details, name and location. You cannot edit the description, object ID, and Up Time of the switch.

- **System Time/Date Configuration:** Enter the date, time and timezone. Enable if Daylight Saving Time is in effect in the timezone.

Click **Apply** to implement the changes.

WLAN Configuration

The WLAN feature manages the OmniAccess Stellar cluster of Access Points (AP). It also allows to access the OmniAccess Stellar APs web management interface for configuration.

Accessing the WLAN Menu

The WLAN web interface can be accessed from the WebView page by clicking on the **WLAN Configuration** label under the Physical group.

To configure the WLAN information, click **PHYSICAL > WLAN** in the menu.

The following screen displays the **WLAN** menu components.
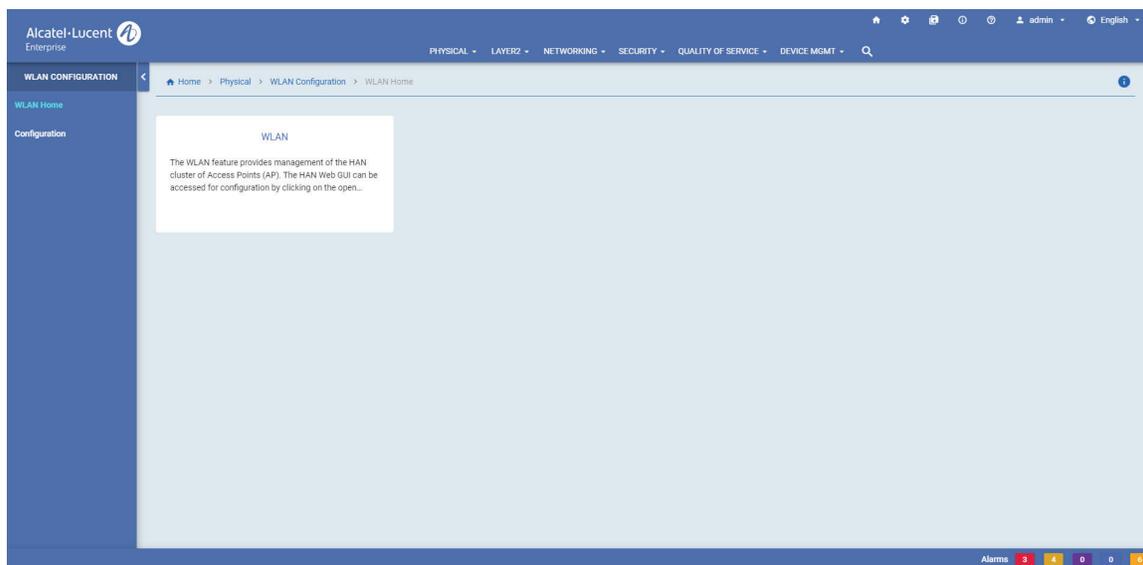
Figure 2-9 : WLAN Home

The WLAN configuration page allows to configure and manage the following WLAN features:

Table 2-9 : WLAN Features

Features	Description
Configuration	Allows to configure and view the WLAN IP Address. The OmniAccess Stellar AP web management interface can also be accessed by clicking on **Open WLAN GUI** option.

BLANK PAGE

3   Configure Layer 2 Features

In This Chapter

This chapter provides an overview of the following Layer2 menu components:

- VLAN Mgmt (see "VLAN Management" on page 3-2)

- Spanning Tree (see "Spanning Tree" on page 3-5)

- Link Aggregation (see "Link Aggregation" on page 3-6)

- ERP (see "ERP" on page 3-7)

- Loopback Detection (see "Loopback Detection" on page 3-8)

- UDLD (see "UDLD" on page 3-9)

Accessing the Layer2 Menu

The Layer2 menu can be accessed from the WebView page by clicking on the **LAYER2** label on the horizontal menu bar on the homepage.

The following screen displays the **LAYER2** menu components.
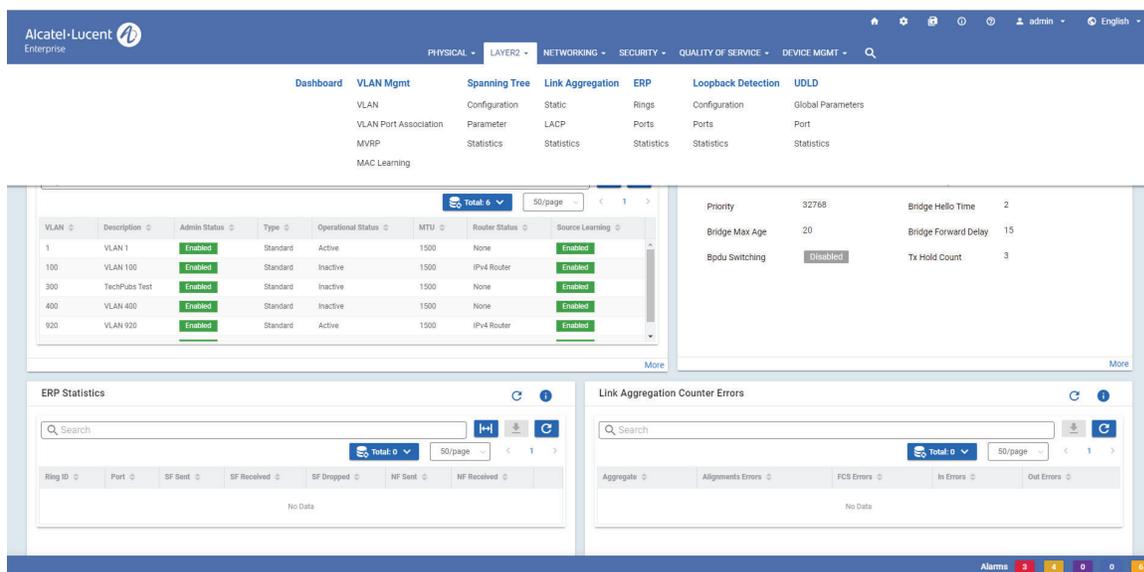
Figure 3-1: LAYER2 Menu Screen

VLAN Management

VLAN Management and Monitoring allows you to define and manage VLAN configurations on the switch.

Accessing VLAN Management Menu

The VLAN Management web interface can be accessed from the WebView page by clicking on the **VLAN Mgmt** label under the Layer2 group.

To configure the VLAN Management information, click **Layer2** > **VLAN Mgmt** in the menu.

The following screen displays the **VLAN Management** menu components.
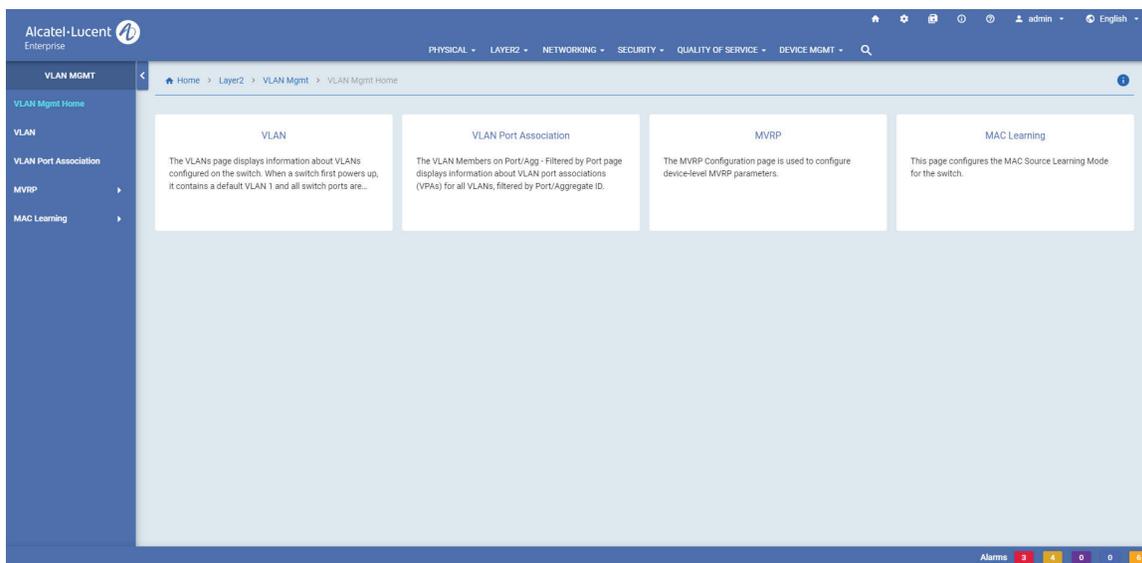
Figure 3-2 : VLAN Management Home

The VLAN Management page allows to configure and manage the following VLAN features:

Table 3-10 : VLAN Management Features

Features	Description
VLAN	Allows to view information on the Standard VLANs configured on the switch, and enable or disable VLANs or source learning on a VLAN. When a switch first powers up, it contains a default VLAN 1 and all switch ports are assigned to this VLAN. Additional VLANs can be created to logically group switch ports into their own broadcast domain. Up to 4094 VLANs per switch, including VLAN 1, can be configured.
VLAN Port Association	Allows to add new VLAN port association (VPA) and view information about the VPAs for all VLANs.
MAC Learning	Allows to: **Global Configuration**: Display and configure the MAC aging time for static and dynamically learned MAC addresses. **Port Configuration**: View the control information about the MAC learning on the ports. **Port Configuration**: View a list of MAC Address entries maintained in the Source Learning MAC Address Table that exists on each switch. (These entries include addresses that were statically assigned by the user or dynamically learned on active switch ports.) Also can add, delete, and flush MAC address table entries.
MVRP	The MVRP Configuration page allows you to configure device-level MVRP parameters. **VLAN Restriction:** Allows you to view the MVRP VLAN Restrictions on Port/ Agg. Filtered by Port page displays the VLAN Restriction configuration for MVRP on a port, filtered by Chassis/Slot/Port or Link Agg or VLAN. **Port Parameters**: MVRP Port table allows you to view the port-level MVRP parameters. It can also be used to enable/disable MVRP on a port. **Statistics:** The MVRP Statistics page allows you to view receive and transmit statistics on an MVRP enabled port.

Viewing VLAN Information and Adding a new VLAN

Use the VLAN Information page to view information on VLANs currently defined on the switch and to add new VLAN information.

To view VLAN information page, click **Layer2 > VLAN Mgmt> VLAN** in the menu.

Creating a VLAN

VLANs are created using a wizard that guides you through each of the steps needed to create the VLAN. The Add VLAN Wizard will then guide you through the process.

Click on the **Add** icon and complete the following Page in the VLAN Wizard, to create VLANs by selecting specific devices.

- **VLAN Information :** The VLAN Information Page is used to configure basic VLAN parameters to be included in the VLAN. You can add VLAN ID, Description, Admin Status, and MTU.
  When you have completed all of the parameters, click the **Next** button at the bottom of the screen or click on Default Port Association on the left side of the screen to move to the next step.

- **Default Port Association:** Select the ports that needs to be associated with the VLAN. Click the **Next** button at the bottom of the screen or click on Q Tagged Port Association on the left side of the screen to move to the next step.

- **Q Tagged Port Association:** Select the Q Tagged ports that needs to be associated with the VLAN. click the **Next** button at the bottom of the screen or click on Review on the left side of the screen to move to the next step.

- **Review and Apply:** Review VLAN configuration and click **Submit** to create a new VLAN.

Modifying a VLAN

Select a VLAN on the VLAN Information page and click on **Modify** icon to bring up the VLAN Detail Screen. Modify the required VLAN Information, Default Port Association, and Q Tagged Port Association. Review the modified VLAN configuration and click **Submit** to modify the VLAN.

Removing a VLAN

To delete an existing VLAN from the switch configuration, select a single VLAN from the VLAN Information Page and click on the **Delete** icon, then click **Yes**. The VLAN is not removed from the appropriate switch configurations until you click the **Yes** button.

Spanning Tree

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology on a network. STP helps to provide data path redundancy and network scalability. This functionality improves network robustness by providing a Spanning Tree that continues to respond to BPDUs (Bridge Protocol Data Unit) and port link up and down states in the event of a fail over to a backup management module or switch.

Accessing Spanning Tree Menu

The Spanning Tree web interface can be accessed from the WebView page by clicking on the **Spanning Tree** label under the Layer2 group.

To configure the Spanning Tree information, click **Layer2** > **Spanning Tree** in the menu.

The following screen displays the **Spanning Tree** menu components.
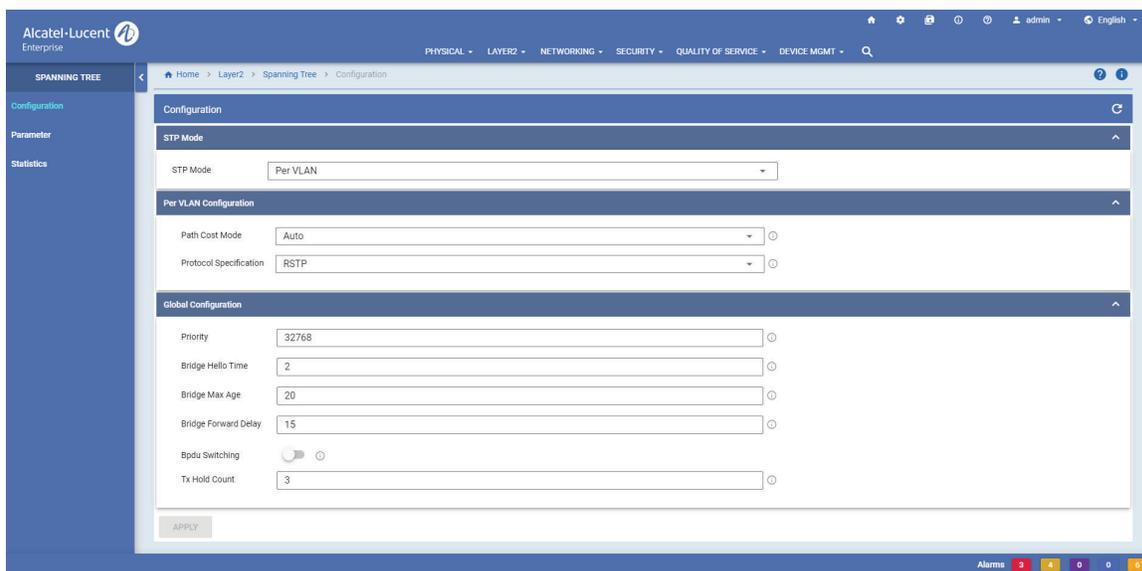
Figure 3-3 : Spanning Tree Home

The Spanning Tree page allows to configure and manage the following Spanning Tree features:

Table 3-11 : Spanning Tree Features

Features	Description
Configuration	Allows to configure spanning tree parameters such as the operating mode, bridge parameters, and port parameters.
Parameter	Allows to configure spanning tree port parameters.
Statistics	Allows to view spanning tree port statistics and bridge statistics.

Link Aggregation

Link aggregation combines multiple physical links between two switches into one logical link. The aggregate group operates within Spanning Tree as one virtual port and can provide more bandwidth than a single link. It also provides redundancy. If one physical link in the aggregate group goes down, link integrity is maintained.

There are two types of aggregate groups: static and dynamic. Static aggregate groups are manually configured on the switch with static links. Dynamic groups are set up on the switch but they aggregate links as necessary according to the Link Aggregation Control Protocol (LACP).

Accessing Link Aggregation Menu

The Link Aggregation web interface can be accessed from the WebView page by clicking on the **Link Aggregation** label under the Layer2 group.

To configure the Spanning Tree information, click **Layer2** > **Link Aggregation** in the menu.

The following screen displays the **Link Aggregation** menu components.
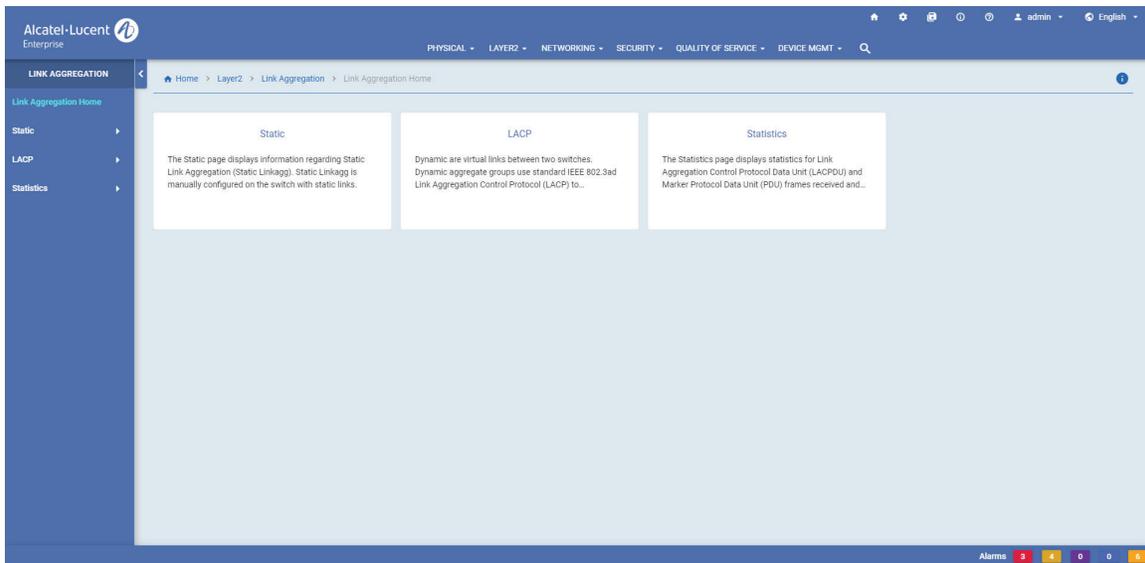
Figure 3-4 : Link Aggregation Home

The Link Aggregation page allows to configure and manage the following features:

Table 3-12 : Link Aggregation Features

Features	Description
Static	Static Linkagg is manually configured on the switch with static links. Allows to: **Aggregate** - Create and view static aggregate groups. You can create up to four aggregate groups (both Static and Dynamic combined) on a single 24-port switch, up to 8 on a single 48-port switch, and up to 128 on a stack. **Port** - Add new static port and view existing static aggregated ports. A port may belong to only one aggregate group (either Static or Dynamic).
LACP	Dynamic are virtual links between two switches. Allows to: **Aggregate** - Create and view link aggregate groups. You can create up to four aggregate groups (both Static and Dynamic combined) on a single 24-port switch, up to 8 on a single 48-port switch, and up to 32 on a stack. **Port**- Add new LACP port and view displays ports in dynamic aggregate groups. A port may belong to only one aggregate group and mobile ports cannot be aggregated.
Statistics	The statistics page displays statistics for Link Aggregation Control Protocol Data Unit (LACPDU) and Marker Protocol Data Unit (PDU) frames received and transmitted on dynamic aggregation group ports.

ERP

Ethernet Ring Protection (ERP) switching mechanism is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. ERP provides fast recovery times for Ethernet ring topologies by utilizing traditional Ethernet MAC and bridge functions.

Accessing ERP Menu

The ERP web interface can be accessed from the WebView page by clicking on the **ERP** label under the Layer2 group.

To configure the Spanning Tree information, click **Layer2** > **ERP** in the menu.

The following screen displays the **ERP** menu components.
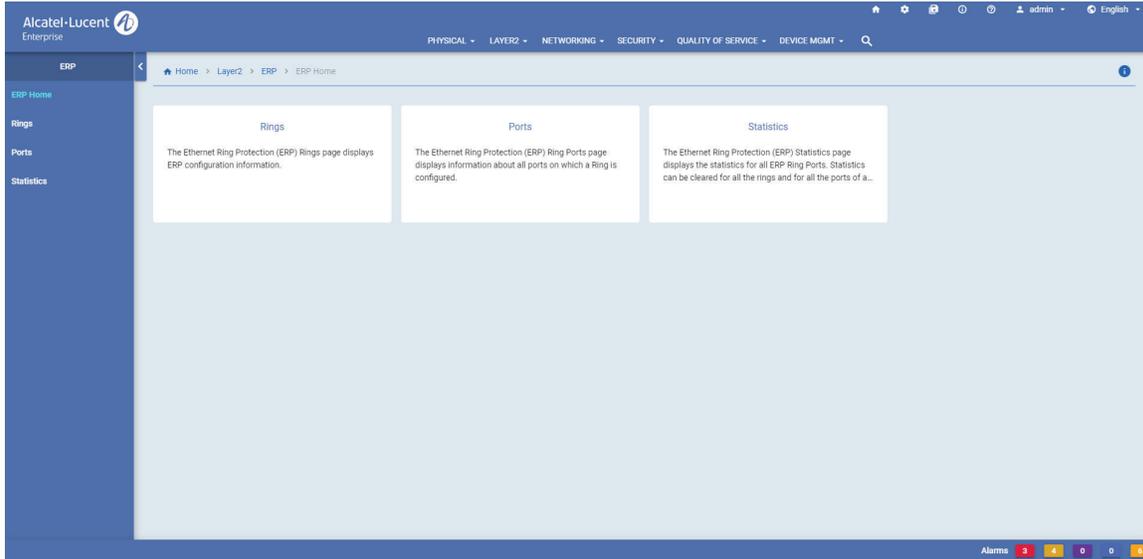
Figure 3-5 : ERP Home

The ERP page allows to configure and manage the following features:

Table 3-13 : ERP Features

Features	Description
Rings	The Ethernet Ring Protection (ERP) Rings page allows you to view ERP configuration information.
Ports	The Ethernet Ring Protection (ERP) Ring Ports page allows you to view information about all ports on which a Ring is configured.
Statistics	The Ethernet Ring Protection (ERP) Statistics page allows you to view the statistics for all ERP Ring Ports. Statistics can be cleared for all the rings and for all the ports of a ring.

Loopback Detection

Loopback Detection automatically detects the loop and shutdown the port involved in the loop. This prevents forwarding loops on ports that have forwarded network traffic which has looped back to the originating switch. Loopback Detection detects and prevents Layer 2 forwarding loops on a port either in the absence of other loop detection mechanisms such as STP/RSTP/MSTP, or when these mechanisms cannot detect it (for example, a client's equipment may drop BPDUs, or the STP protocol may be restricted to the network edge).

Accessing Loopback Detection Menu

The Loopback Detection web interface can be accessed from the WebView page by clicking on the **Loopback Detection** label under the Layer2 group.

To configure the Spanning Tree information, click **Layer2** > **Loopback Detection** in the menu.

The following screen displays the **Loopback Detection** menu components.
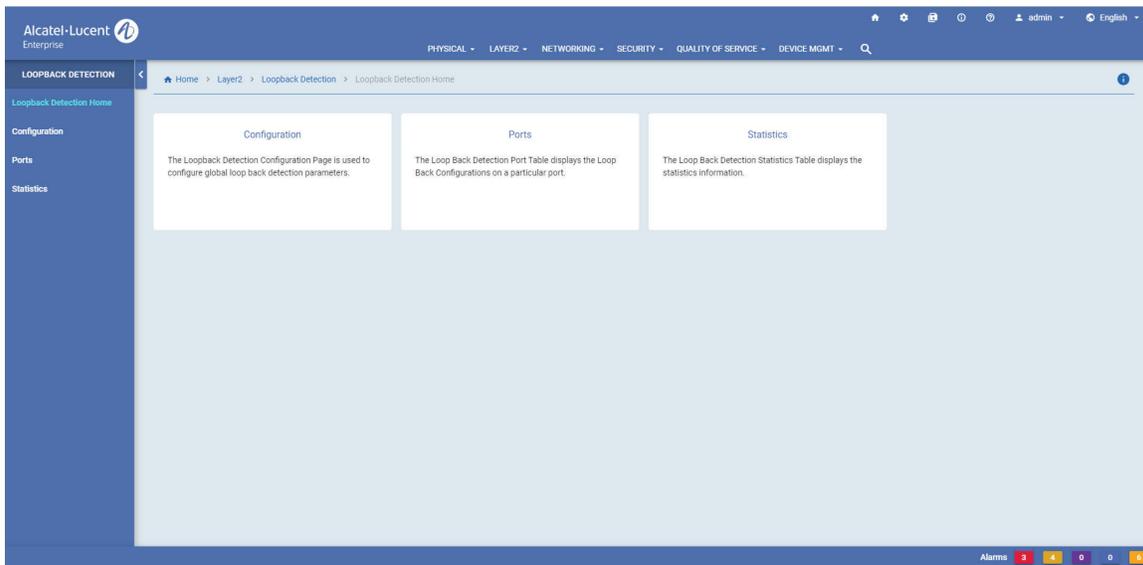
Figure 3-6 : Loopback Detection Home

The Loopback Detection page allows to configure and manage the following features:

Table 3-14 : Loopback Detection Features

Features	Description
Configuration	The Loopback Detection Configuration Page allows you to configure global loop back detection parameters.
Ports	The Loopback Detection Port Table allows you to view the Loopback configurations on a particular port.
Statistics	The Loopback Detection Statistics Table page allows you to view the statistics information.

UDLD

UniDirectional Link Detection (UDLD) is a protocol for detecting and disabling unidirectional Ethernet fiber or copper links caused by mis-wiring of fiber strands, interface malfunctions, media converter faults, and so on. The UDLD protocol operates at Layer 2 in conjunction with the IEEE 802.3 - Layer 1 fault detection mechanisms.

UDLD is a lightweight protocol that can be used to detect and disable one-way connections before they create dangerous situations such as Spanning Tree loops or other protocol malfunctions. The protocol is mainly used to advertise the identities of all the UDLD-capable devices attached to the same LAN segment and to collect the information received on the ports of each device to determine whether or not the Layer 2 communication is functioning properly. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, the protocol administratively shuts down the affected port and generates a trap to alert the user
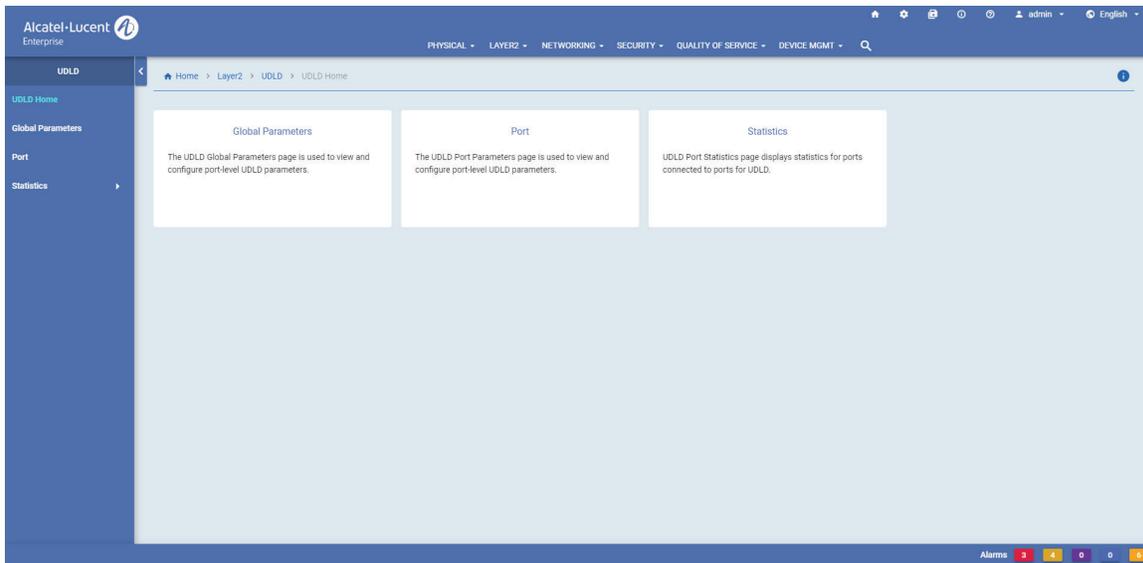
Figure 3-7 : UDLD Home Page

Accessing UDLD Menu

The Loopback Detection web interface can be accessed from the WebView page by clicking on the **Loopback Detection** label under the Layer2 group.

To configure the Spanning Tree information, click **Layer2** > **Loopback Detection** in the menu.

The UDLD page allows to configure and manage the following features:

Table 3-15 : UDLD Features

Features	Description
Global Parameters	The UDLD Global Parameters page allows you to view and configure port-level UDLD parameters.
Ports	The UDLD Port Parameters page allows you to view and configure port-level UDLD parameters.
Statistics	The UDLD Port Statistics page allows you to view the statistics for ports connected to ports for UDLD.

4 Configure Networking Features

In This Chapter

This chapter provides an overview of the following networking menu components:

- IP/IPv6 (see "IP/IPv6" on page 4-2)

- IP Multicast (see "IP Multicast" on page 4-4)

- Services (see "Services" on page 4-5)

- DHCP (see "DHCP" on page 4-7)

Accessing the Networking Menu

The Networking Menu can be accessed from the WebView page by clicking on the **NETWORKING** label on the horizontal menu bar on the home page.

The following screen displays the **NETWORKING** menu components.
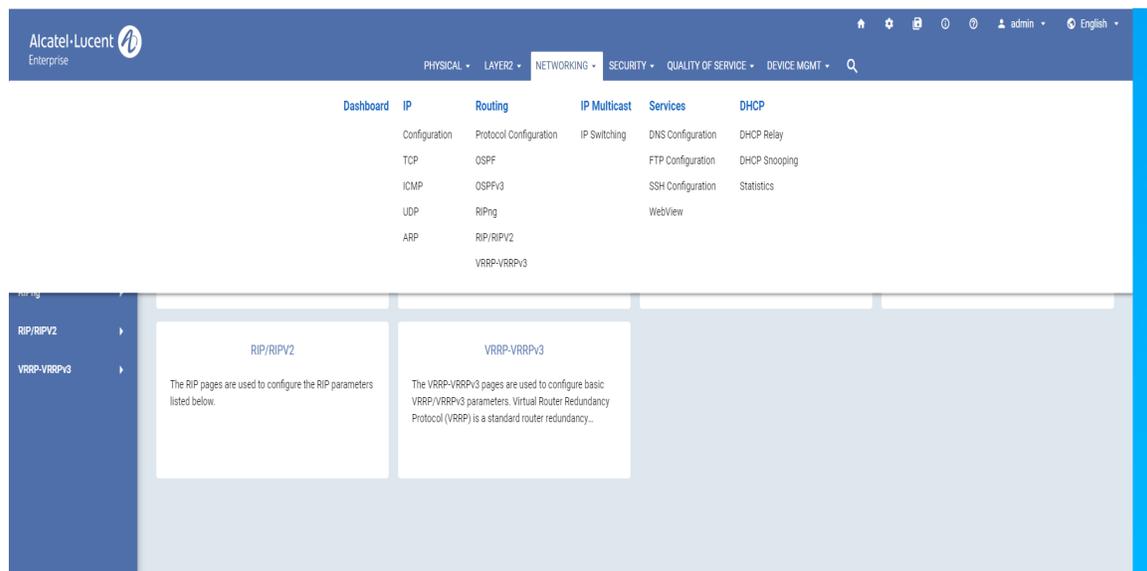
Figure 4-1 : NETWORKING Menu Screen

IP/IPv6

IP is a network-layer (Layer 3) protocol that contains addressing information and control information that enables packets to be forwarded. It allows for basic IP configuration.

Accessing IP Menu

The IP web interface can be accessed from the WebView page by clicking on the **IP** label under the Networking group.

To configure the IP information, click **NETWORKING > IP** in the menu.

The following screen displays the **IP** menu components.
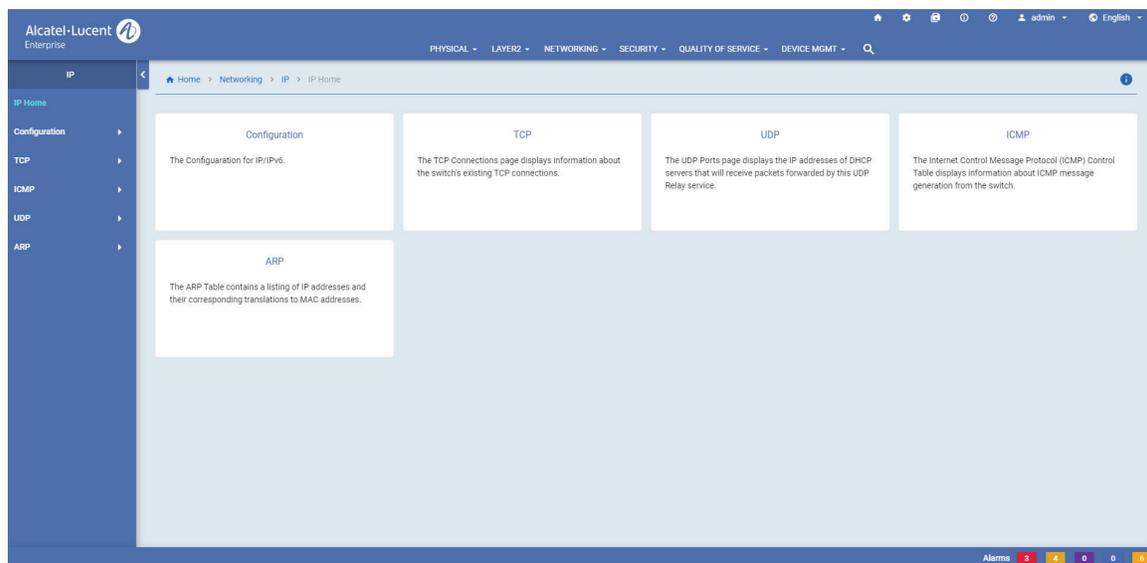
Figure 4-2 : IP Home

The IP Home page allows to configure and manage the following IP features:

Table 4-1 : IP Features

Field	Description
Configuration	Allows to: **Global:** Configure the IP Global and IP Route Preference parameters. **Interfaces:** Configure and view IP interface details. **DHCP Client:** Configure and manage the DHCP Client information on the switch. **Addresses:** View the status of all configured IP interface addresses. **Route:** Add new route static and view the number of routes and all IP routes stored in the IP Forwarding Table. **IPV4:** Configure and view the managed interface (source IP service and source IP interface). **IPV6:** Configure and view the managed interface (source IPv6 service and source IPv6 interface). **Service:** Configure and view the IP services, NTP client, NTP servers, NTP Authentication and restricted addresses. **Denial of Service:** View the DoS attack statistics, configure and view IP DoS ARP Poison Restricted Addresses, and set the configuration values for monitoring Denial of Service (DoS) attacks. **Statistics:** View IP datagram statistics and IP datagram statistics per interface.
TCP	Allows to: **Configuration:** Configure the time out interval for half open TCP connections. **Connections:** View information about the switch's existing TCP connections. **Listeners:** View information about the switch's existing applications listening for TCP connections. **Statistics:** View TCP statistics.
ICMP	Allows to: **Control:** View information about ICMP message generation from the switch. **Statistics:** View ICMP statistics and errors.
UDP	Allows to: **Ports:** View the IP addresses of DHCP servers that will receive packets forwarded by this UDP Relay service. Local UDP port numbers are also displayed. **Statistics:** View the number of packets received and transmitted by the UPD Relay service.
ARP	Allows to: **ARP Filters:** Configure and view the ARP filters for the switch. **Global Parameters:** Clear dynamic entries from the ARP Table. **View ARP Table:** View the ARP Table information. **Create Proxy ARP:** Configure and view proxy ARP entries on the switch. **ARP Configuration:** Configure and view permanent ARP table entries.

IP Multicast

IP Multicast Switching (IPMS) is a one-to-many communication technique employed by emerging applications such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, and BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic.

Accessing the IP Multicast Menu

The IP Multicast web interface can be accessed from the WebView page by clicking on the **IP Multicast** label under the Networking group.

To configure the IP Multicast information, click **NETWORKING > IP Multicast** in the menu.

The following screen displays the **IP Multicast** menu components.
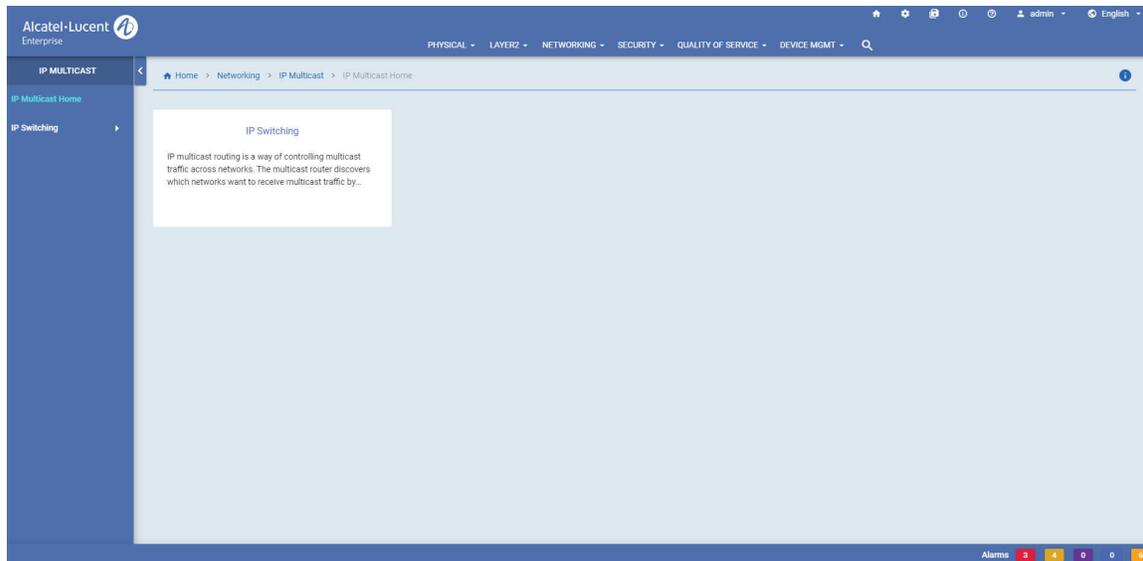
Figure 4-3 : IP Multicast Home

The IP Multicast page allows to configure and manage the following IP Multicast features:

Table 4-2 : Port Security Features

Features	Description
IP Switching	Allows to: **Configuration:** Enable and disable IPv4/IPv6 Multicast Switching (IPMS) on the switch and modify IPMS parameters. View the current IPMS configuration on a switch. Configure and view the current IPv4/IPv6 IPMS configuration profiles on the switch. **VLAN Configuration:** Configure and veiw all IPv4/IPv6 Multicast Switching (IPMS) static groups, all neighboring IPv4/IPv6 multicast static routers, all IPv4/IPv6 multicast queriers, IPv4/IPv6 Multicast Switching (IPMS) source table, IP Multicast Switching (IPMS) forwarding table. View the detected IPv4/IPv6 Multicast Switching (IPMS) groups that have members, neighboring IPv4/IPv6 multicast routers, IPv4/IPv6 multicast queriers. View the IP multicast bridging information and forwarding state for the IP multicast bridge entries. **Tunnels:** View the IPv4/IPv6 Multicast Switching (IPMS) Tunneling Table.

Services

The services allows to manage the DNS, FTP, SSH and WebView services in the switch.

Accessing the Services Menu

The Services web interface can be accessed from the WebView page by clicking on the **Services** label under the Networking group.

To configure the Services information, click **NETWORKING > Services** in the menu.

The following screen displays the **Services** menu components.
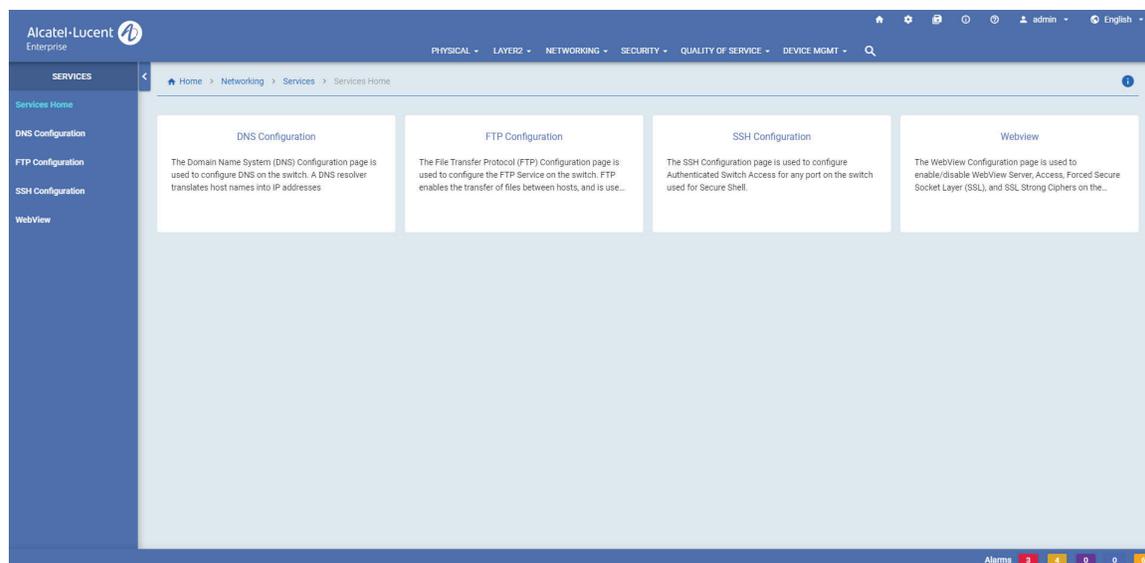
Figure 4-4 : Services Home

The Services page allows to configure and manage the following Services features:

Table 4-3 : Services Features

Features	Description
DNS Configuration	Allows to configure DNS on the switch.
FTP Configuration	Allows to configure the FTP Service on the switch.
SSH Configuration	Allows to configure Authenticated Switch Access for any port on the switch used for Secure Shell.
WebView	Allows to enable/disable WebView Server, Access, Forced Secure Socket Layer (SSL), SSL Strong Ciphers and TLS Version on the switch. It is also allows to configure the HTTP and HTTPS port configuration.

DHCP

Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets contain configuration information for network hosts. It enables to manage the DHCP relay and DHCP snooping in the switch.

Accessing the DHCP Menu

The DHCP web interface can be accessed from the WebView page by clicking on the **DHCP** label under the Networking group.

To configure the DHCP information, click **NETWORKING > DHCP** in the menu.

The following screen displays the **DHCP** menu components.
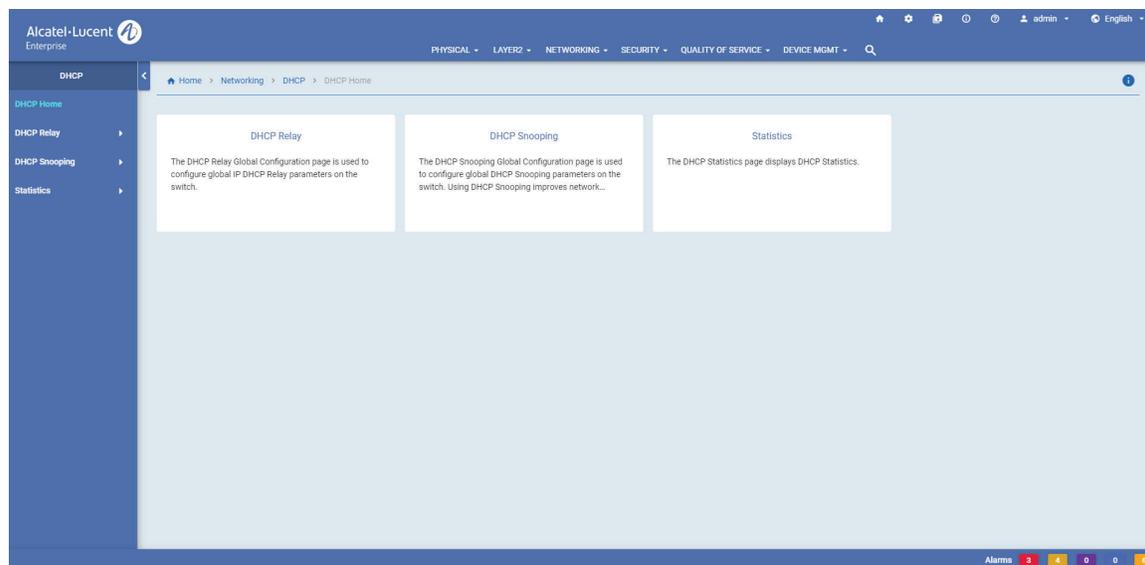
Figure 4-5 : DHCP Home

The DHCP page allows to configure and manage the following DHCP features:

Table 4-4 : DHCP Features

Features	Description
DHCP Relay	Allows to: **Configuration:** Configure global IP DHCP Relay parameters on the switch. **Destination:** Configure and view DHCP destination information. **Interface:** Configure and view DHCP Relay interface information. **Option 82:** Configure global UDP Relay Option 82 format on the switch.
DHCP Snooping	Allows to: **Configuration:** Configure global DHCP Snooping and binding database parameters on the switch. **Port:** Displays Port number. **VLAN:** DHCP Snooping VLAN **Binding:** Configure DHCP Snooping binding functionality. **Option 82 Format:** Configure global DHCP Snooping Option 82 format on the switch.

Features	Description
Statistics	Allows to: **DHCP Relay Agent:** View the DHCP Relay agent global statistics and configuration information and packet handling statistics for all enabled relay services. **Option 82:** View the list of UDP Relay Option-82 related error statistics count per port and per VLAN.

5 Configure Security Features

In This Chapter

This chapter provides an overview of the following Security menu components:

- AAA (see "AAA" on page 5-2)

- Access Guardian (see "Access Guardian" on page 5-4)

- ASA (see "ASA" on page 5-6)

- Port Security (see "Port Security" on page 5-9)

Accessing the Security Menu

The Security menu can be accessed from the WebView page by clicking on the **SECURITY** label on the horizontal menu bar on the homepage.

The following screen displays the **SECURITY** menu components.
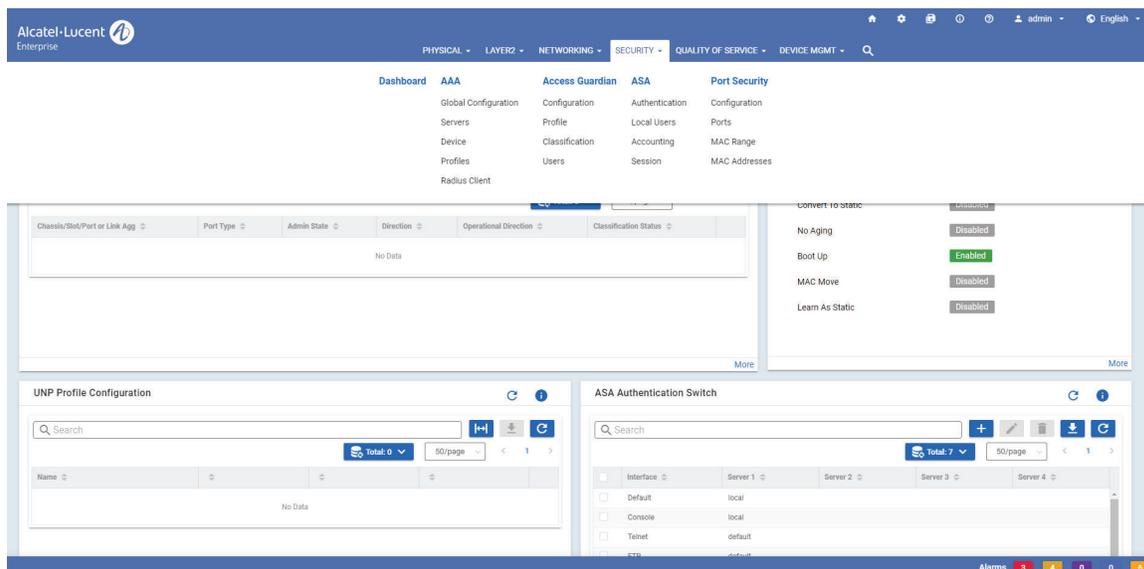
Figure 5-1: SECURITY Menu Screen

AAA

AAA allows you to define and manage authentication, authorization, and accounting (AAA) configurations.

Accessing AAA Menu

The AAA web interface can be accessed from the WebView page by clicking on the **AAA** label under the Security group.

To configure the AAA information, click **Security** > **AAA** in the menu.

The following screen displays the **AAA** menu components.
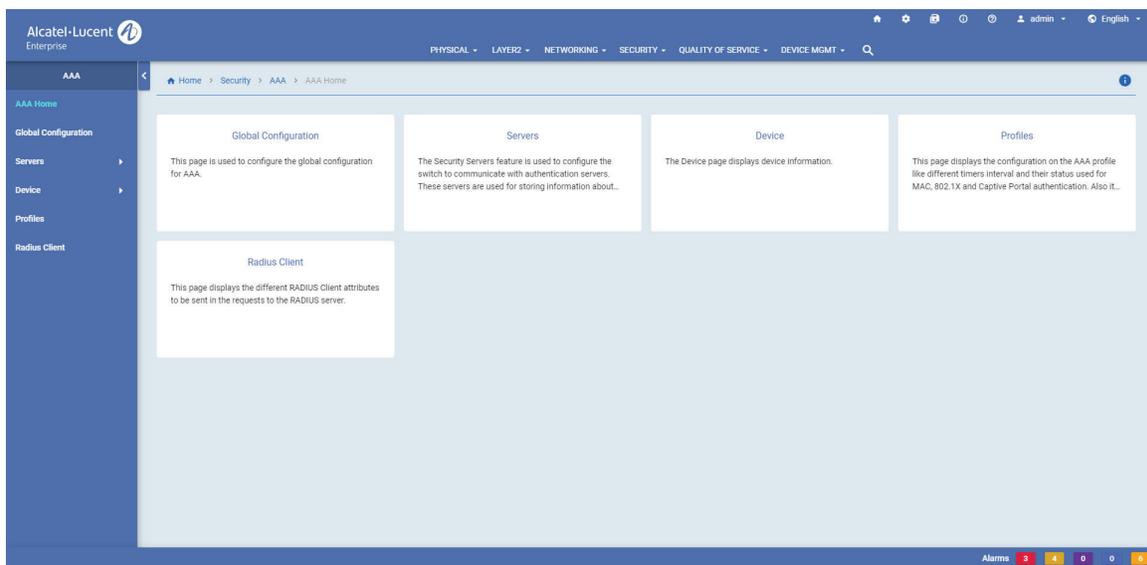
Figure 5-2 : AAA Home

The AAA page allows to configure and manage the following features:

Table 5-5 : AAA Features

Features	Description
Global Configuration	Allows to view the global configuration on the AAA, and to enable or disable the console access.
Servers	Allows to: **RADIUS:** Configure and view RADIUS server attributes for Authenticated VLANs or Authenticated Switch Access. **LDAP**: Configure and view LDAP server attributes for Authenticated VLANs or Authenticated Switch Access. **TACACS+**: Configure and view TACACS displays information about configured Terminal Access Controller Access Control System (TACACS+) servers. TACACS+ is a standard authentication and accounting protocol that employs TCP for reliable transport. **Statistics**: View AAA Server statistics and BYOD server statistics. **RADIUS Health Check**: View AAA RADIUS server status, and RADIUS server health check.
Device	Allows to: **Authentication**: Configure and view RADIUS servers. Up to three (3) backup servers can be configured. This page also allows to configure different timer intervals and their status used for 802.1X authentication. **Accounting**: Configure and view accounting servers. Up to four servers may be configured. Note: Only RADIUS or Syslog server can be used for 802.1X accounting. Configuring both RADIUS server and Syslog server is not allowed.
Profiles	Allows to configure AAA profile with different timers interval and their status used for MAC, 802.1x, and Captive Portal authentication. Also, configure the RADIUS client attributes for the AAA profile.
Radius Client	Allows to configure different RADIUS client attributes to be sent in the requests to the RADIUS server.

Access Guardian

Access Guardian refers to a set of OmniSwitch security functions that work together to provide a dynamic, proactive network security solution.

Accessing Access Guardian Menu

The Access Guardian web interface can be accessed from the WebView page by clicking on the **Access Guardian** label under the Security group.

To configure the Access Guardian information, click **Security** > **Access Guardian** in the menu.

The following screen displays the **Access Guardian** menu components.
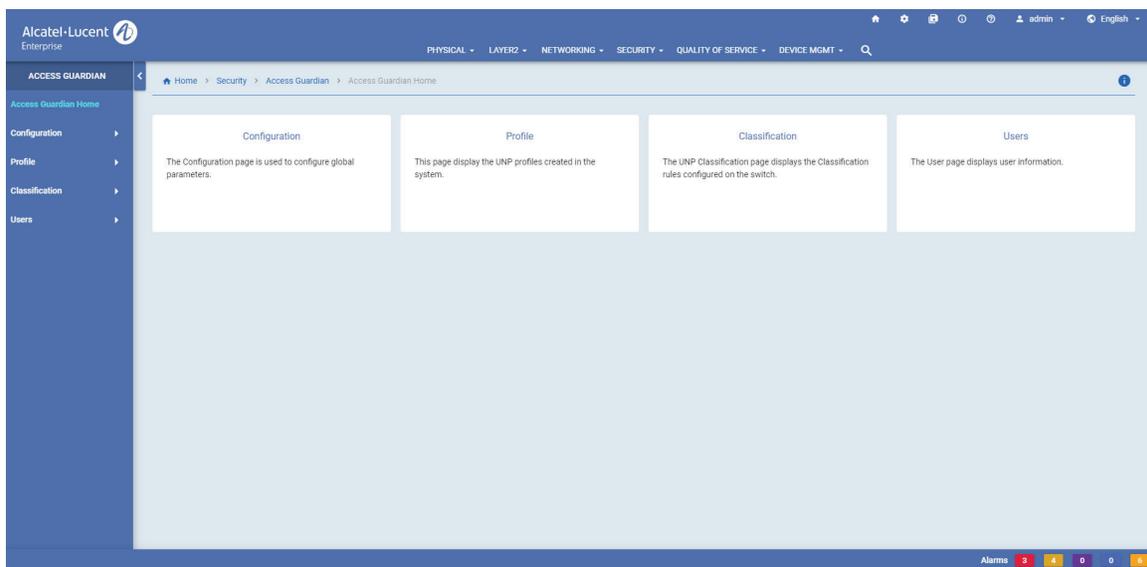
Figure 5-3 : Access Guardian Home

The Access Guardian page allows to configure and manage the following features:

Table 5-6 : Access Guardian Features

Features	Description
Configuration	Allows to: **Global**: Configure global Universal Network Profile (UNP) parameters. **Port**: Enable multiple authentication/classification policies on UNP port to arrive at an UNP Profile or UNP VLAN ID. Access-Guardian/UNP VLAN functionality can be enabled on physical Ports and Link Aggregates. **Port Template**: Attach the UNP port-template to a UNP Port/Link Aggregate or a VLAN. Port Template contains all the UNP properties to be enabled on a UNP Port or Linkagg.
Profile	Allows to: **Configuration**: Configure new UNP profile and view UNP profiles created in the system. **Mapping**: Add new UNP VLAN mapping and view the VLAN profiles in the system. The entries would be mapped to the VLAN ID that would be used by device authentication for classifying users.
Classification	Allows to configure new Atomic UNP MED End Point Classification rules and view the Atomic rules configured on the switch. If the source device, based on the LLDP TLV matches the LLDP End Point defined for the rule, the specified UNP Profile is applied to the device.
Users	Allows to: **Applications**: View configuration information for UNP based on the applications. **By Port**: View configuration information for UNP ports. **Flush**: Flush the user based on the input criteria.

ASA

ASA (Authenticated Switch Access) page displays information about interfaces for Authenticated Switch Access. By default, the switch is configured for access through the console port through the local database; authentication over other management interfaces is disabled.

Accessing ASA Menu

The ASA web interface can be accessed from the WebView page by clicking on the **ASA** label under the Security group.

To configure the Access Guardian information, click **Security** > **ASA** in the menu.

The following screen displays the **ASA** menu components.
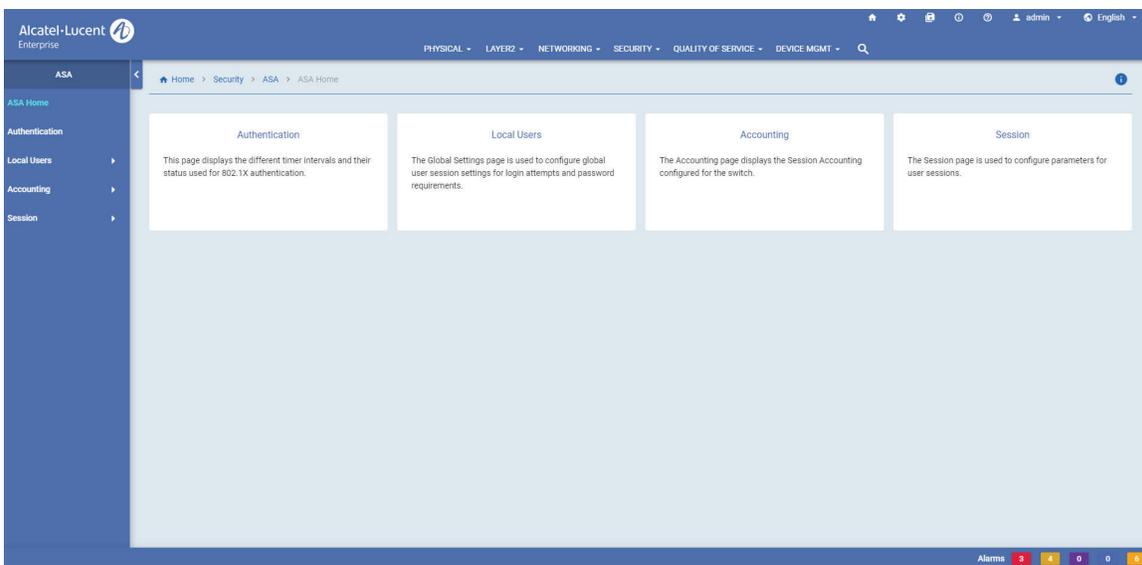
Figure 5-4 : ASA Home

The ASA page allows to configure and manage the following features:

Table 5-7 : ASA Features

Features	Description
Authentication	Allows to add an interface for switch access and/or configure servers to be associated with the interface type.
Local Users	Allows to: **Global Settings**: Configure global user session settings for login attempts and password requirements. **Password Policy**: Configure global parameters for user passwords. **User Database**: Configure new local user database and view information about user accounts in the local user database. It is also used to lock or unlock a user, modify a user family privileges, or disabled password expiration settings.
Accounting	Allows to: **Session**: Configure and view the Session Accounting Servers configured for the switch. Session Accounting Servers keep track of network resources (time, packets, bytes, etc.) and user activity. **Command**: Configure and view TACACS+ Command Accounting Servers configured for the switch. Command Accounting Servers allow users read/write access to specific command families.
Session	Allows to: **Current**: View information about users currently managing the switch. **Configuration**: Configure parameters for user sessions.

Viewing User Database and Adding a new User

The Local User Database page displays information about user accounts in the local user database. It is also used to lock or unlock a user, modify a user family privileges, or disabled password expiration settings.

Use the User Database page to view information on local users currently configured on the switch and to add new local user.

To view User Database page, click **Security > ASA> Local Users** in the menu.

Creating a User

- Click on the **Add** icon and enter the user name and password for the new user. The User Login and Password fields are mandatory. The user will use this User Login and Password to log into the switch.

- For temporary users, you can enable Password Expiration date and provide a valid date for the users validty to expire. Select one of the SNMP Access Level at the bottom of the screen to provide SNMP access level to the user. The default is no access. Other possible values are - SNMPv1-v2c-v3 without authentication, which specifies that the user has SNMP access without any required SNMP authentication and encryption protocol.

- Click on **Submit** to add a new user to the database.

Modifying a User

Click on a User on the User Database Page to bring up the User Detail Screen. Click on the **Modify** icon Edit any fields as necessary and/or edit the SNMP Access Level at the bottom of the screen to re-assign

the User to a SNMP Access. When you are done, click **Submit**. You will be returned to the User Database Screen. Note that you cannot edit the User Login field.

Deleting a User

Select a User(s) on the User Database Screen by clicking in the checkbox, click on the **Delete** icon, then click **Yes**. Note that you cannot delete the user admin.

Port Security

LPS (Learned Port Security) provides a mechanism for controlling network device communication on one or more switch ports by allowing the user to restrict source learning on a port by configuring the number of MAC addresses allowed on the port, and/or specifying a list or range of authorized MAC addresses for the port.

Accessing Port Security Menu

The ASA web interface can be accessed from the WebView page by clicking on the **Port Security** label under the Security group.

To configure the Access Guardian information, click **Security** > **Port Security** in the menu.

The following screen displays the **Port Security** menu components.
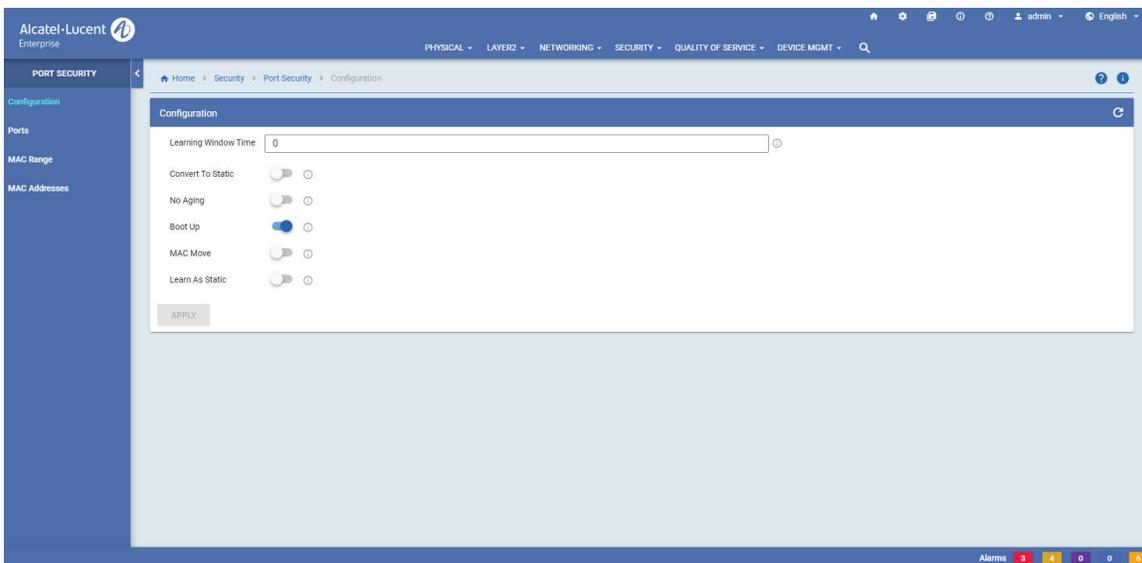
Figure 5-5 : Port Security Home

The Port Security page allows to configure and manage the following features:

Table 5-8 : Port Security Features

Features	Description
Learning Window Time	Allows you to set the amount of time in minutes to allow source learning on all LPS ports.
Convert To Static	Allows you to enable or disable a device-wide restriction that facilitates the handling of dynamic MAC addresses when LPS source learning time window expires.
No Aging	Allows you to enable or disable a device-wide restriction that facilitates the handling of aging of all MAC addresses. • Enabled - all MAC addresses learned are deferred from aging. • Disabled - all MAC addresses are allowed to age.
Boot Up	Allows you to enable or disable a device-wide restriction that determines when the LPS Learning Window Time begins.
MAC Move	When MAC Move is enabled, all the pseudo static MAC addresses will be subject to MAC move.
Learn As Static	When Learn As Static is enabled, all the MAC addresses learnt on the port would be directly converted to static.

6   Configure QoS

In This Chapter

This chapter provides an overview of the following physical menu components:

- QoS Configuration (see "QoS Configuration" on page 6-2)

- QoS Groups (see "QoS Groups" on page 6-3)

- TCAM Manager (see "TCAM Manager" on page 6-5)

- LDAP Policies (see "LDAP Policies" on page 6-2)

- VFC (see "VFC" on page 6-6)

Accessing the Quality of Service Menu

The following screen displays the **Quality of Service** menu components

The Quality of Service Menu can be accessed from the WebView page by clicking on the **Quality of Service** label on the horizontal menu bar on the home page.
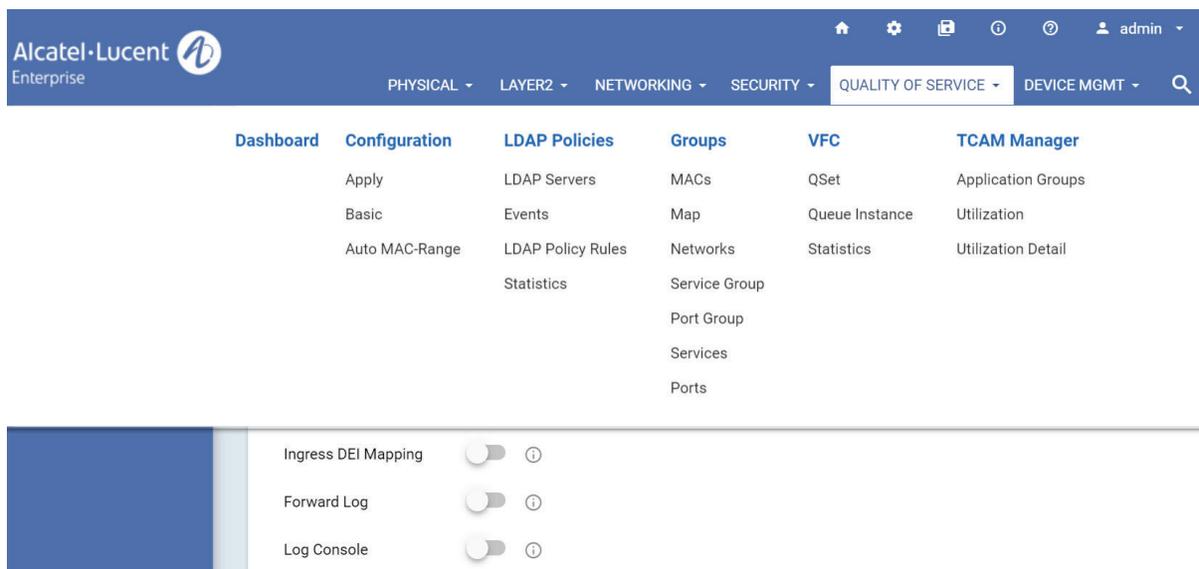
Figure 6-1 : Quality of Service Menu Screen

QoS Configuration

This section gives an overview of Quality of Service (QoS) and explains the QoS features available from the Quality of Service navigation menu.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given "special treatment" in a QoS capable network. With this in mind, all elements of the network must be QoS capable.

The Quality of Service Menu can be accessed from the WebView page by clicking on the Quality of Service label on the horizontal menu bar on the home page.

To configure the QoS Basic information, click **Quality of Service > Configuration** page in the menu.
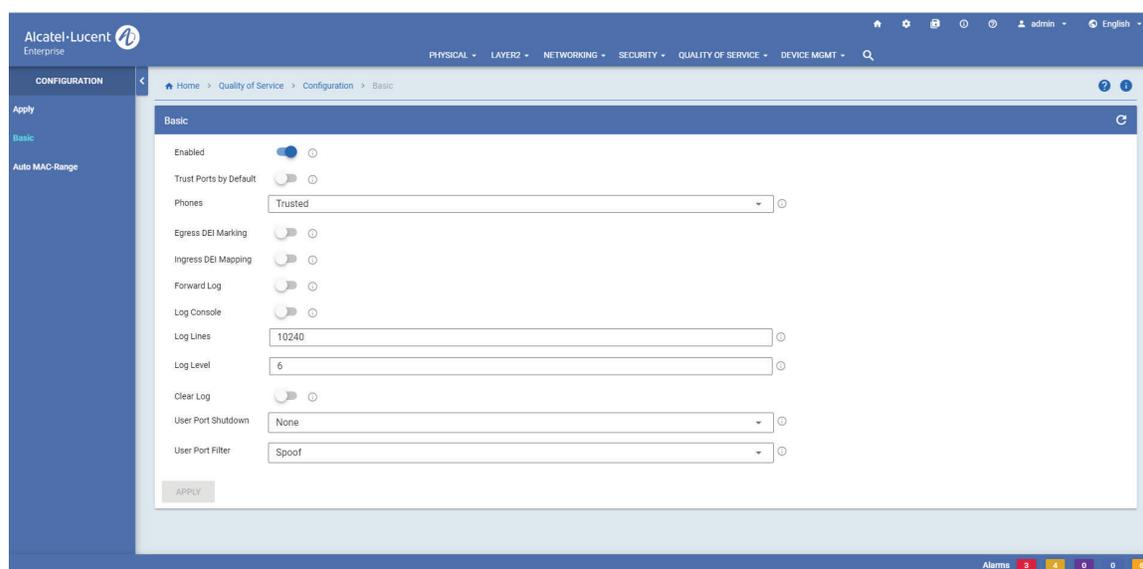
Figure 6-1 : QoS Configuration

The Quality of Service page allows to configure and manage the following QoS features:

Table 6-1 : QoS Configuration Fields

Field	Description
Basic Configuration	The QoS Configuration page allows to configure global QoS parameters. Additional global QoS parameters are configures using the QoS Advanced Configuration page.
Auto Mac-Range	The MAC Address Ranges page displays the QoS auto MAC address ranges. **Start MAC Address:** The first MAC address in the corresponding range. **End MAC Address**: The last MAC address in the corresponding range.

LDAP Policies

LDAP directory servers are used with the switch for policy management. There is no required configuration on the switch. When policies are created on the directory server through PolicyView, the PolicyView application automatically configures the switch to communicate with the server.

To view the LDAP Server information, click **Quality of Service > LDAP Policies** page in the menu.

The LDAP server page displays displays information about Server Address, Port, Preference, Admin State, and the Operational Status.

QoS Groups

The QoS Groups page displays the QOS Group Home page. The QOS Group Home page displays QoS parameters for ports. Note that port settings override settings configured globally for QoS ports on the QoS Configuration and QoS Advanced Configuration pages.

Accessing QoS Groups Menu

The QoS Groups web interface can be accessed from the WebView page by clicking on the **Groups** label under the Security group.

To view the QoS Ports information, click **Quality of Service > Groups** page in the menu.

The following screen displays the **QoS Groups** menu components.
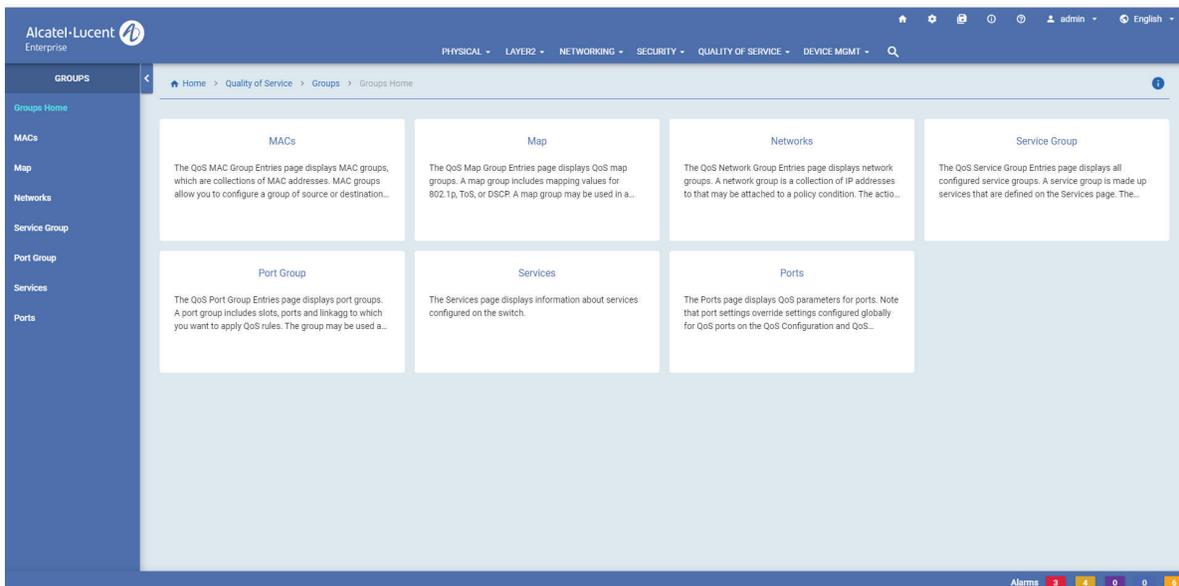
Figure 6-2 : QoS Groups menu

The QoS Groups page allows to manage the following features:

Table 6-2 : Port Security Features

Features	Description
MACs	The QoS MAC Group Entries page allows you to view MAC groups, which are collectios of MAC addresses. MAC groups allow you to configure a group of source or destination MAC addresses to which you want to apply QoS rules. Rather than create a condition for each MAC address, create a single MAC group.
Map	The QoS Map Group Entries page allows you to view QoS map groups. A map group includes mapping values for 802.1p, ToS or DSCP. A map group may be used in a policy action.
Networks	The QoS Network Group page allows you to view network groups. A network group is a collection of IP addresses to that may be attached to a policy condition. The associated with that policy will be applied to all members of the network group.
Service Group	The QoS Service Entries page allows you to view all configured service groups. A service group is made up services that are defined on the Services page. The service group may then be attached to a policy condition. The action associated with that policy will be applied to all members of the service group.
Port Group	The QoS port Group Entries page displays port groups. A port group includes slots, ports and linkagg to which you want to apply QoS rules. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the port group.
Services	The Services page allows you to view information about services configured on the switch.
Ports	The Ports page allows you to view QoS parameters for ports. Note that port settings override settings configured globally for QoS Ports on the QoS Configuration and QoS Advanced Configuration pages.

TCAM Manager

Displays runtime information about the Ternary Content Addressable Memory (TCAM) utilization for each stage of each TCAM on each slot of the switch. The utilization is represented in terms of the minimum-sized entry supported by the TCAM.

To view TCAM groups, click **Quality of Service > TCAM Manager** page in the menu.
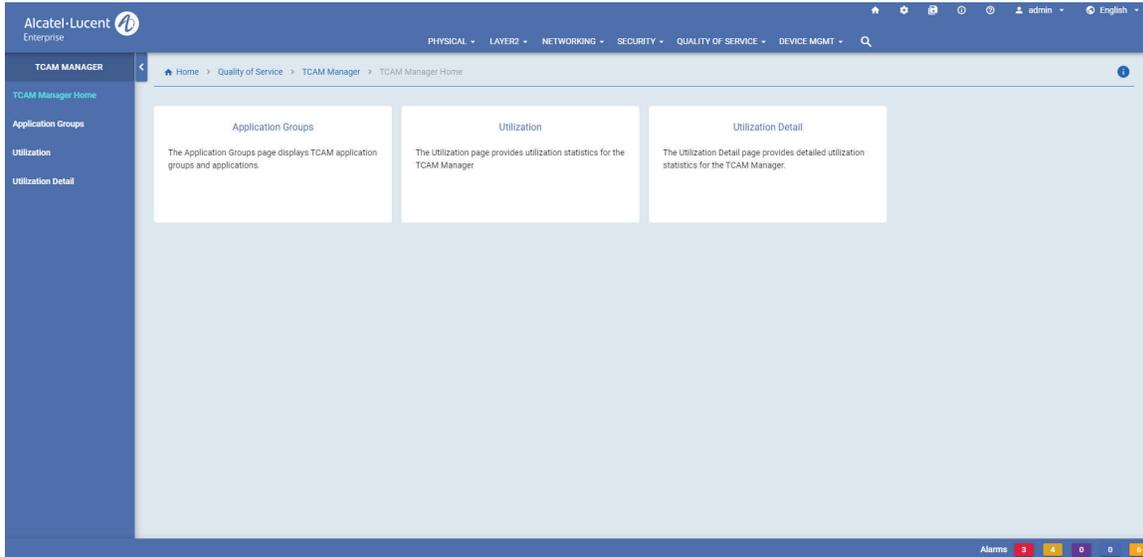
Figure 6-3 : TCAM Manager Home

Table 6-3 : TCAM Manager Fields

Field	Description
Application Groups	The Application Groups page displays TCAM application groups and applications.
Utilization	The utilization page allows utilization statistics for the TCAM Manager.
Utilization Detail	The utilization detail page provides detailed utilization statistics for the TCAM Manager.

VFC

The VFC page displays information about Virtual Fibre Channel (VFC).

To view VFC click **Quality of Service > VFC** page in the menu.
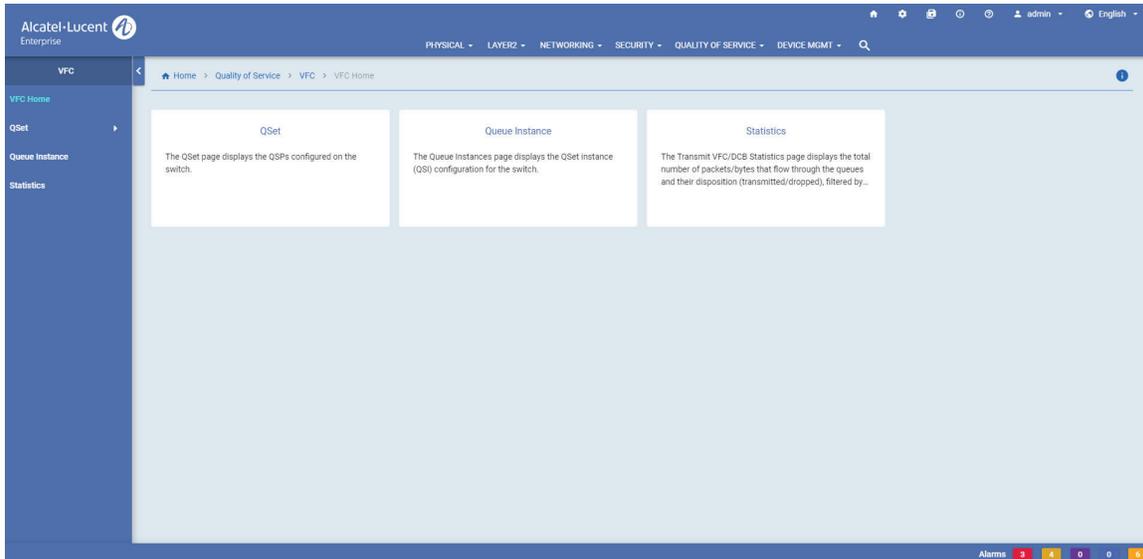
Figure 6-4 : VFC Home

Table 6-4 : VFC Fields

Field	*Description*
QSet	The QSet page displays the QSPs configured on the switch.
Queue Instance	The Queue Instance page displays the QSet Instance (QSI) configuration for the switch.
Statistics	The Transmit VFC/DCB Statistics page displays the total number of packets/bytes that flow through the queues and their disposition (transmitted/dropped), filtered by port.

7 Device Management

In This Chapter

This chapter provides an overview of the following Device Management menu components:

- Interfaces (see "Interfaces Page" on page 7-2)

- SNMP (see "SNMP Home Page" on page 7-2)

- Net Monitoring (see "Net Monitoring Home Page" on page 7-3)

Accessing the Device Management Menu

This section gives an overview of Device Management and explains the Device Management features available from the Device Management menu.

The Devie Management Menu can be accessed from the WebView page by clicking on the **Device Mgmt** label on the horizontal menu bar on the home page.

The following screen displays the **Device Management** menu components.
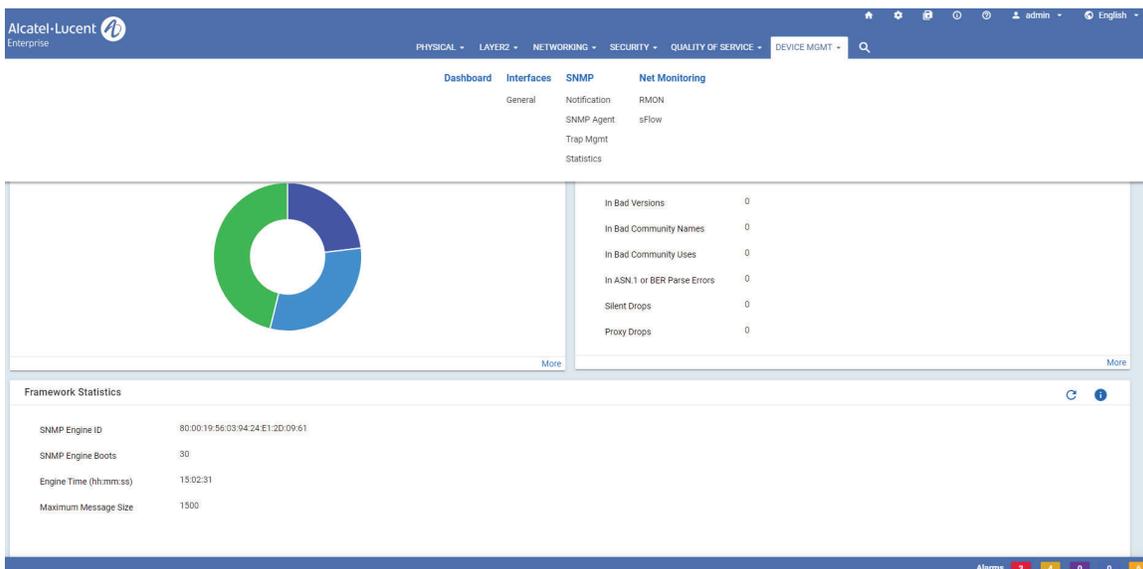
Figure 7-1 : Device Management Home

Interfaces Page

To view the **Interfaces** page, click **Device Mgmt > Interfaces** page in the menu. Use the Down Arrow button to export the data to Excel.

The General Information page is used to enable, disable, and view general information about each interface on the switch.

SNMP Home Page

The SNMP Home Page can be accessed from the WebView page by clicking on the **Device Mgmt** label under the Device Management group.

To configure the Device Management information, click **Device Mgmt** > **SNMP** in the menu.

The following screen displays the **SNMP Home** menu components.
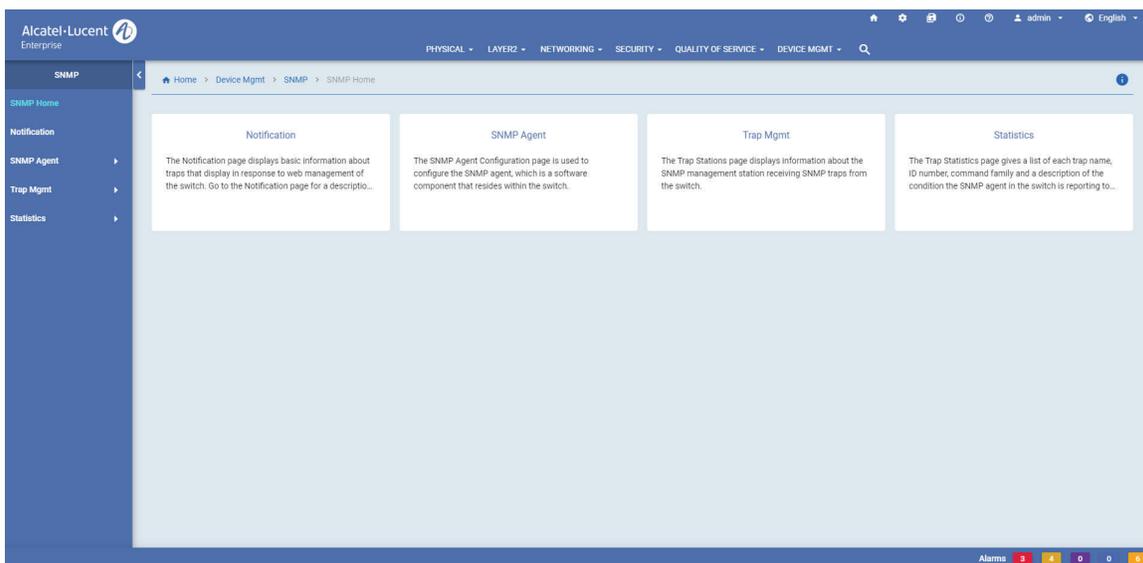
Figure 7-2 : SNMP Home

The SNMP Management page allows to configure and manage the following SNMP features:

Table 7: SNMP Management Features

Features	Description
Notification	The Notification page displays basic information about traps that display in response to web management of the switch. Go to the Trap Definitions page for a description of each SNMP trap..

Features	Description
SNMP Agent	The SNMP Agent Configuration page is allows to configure the SNMP agent, which is a software component that resides within the switch. It maintains the management data about a particular network device and reports these data, as needed, to the management station. The authentication failure trap is sent when an SNMP authentication failure is detected. This trap is a signal to the management station that the switch received a message from an unauthorized protocol entity.
Trap Management	The Trap Stations page displays information about the SNMP management station receiving SNMP traps from the switch.
Statistics	The SNMP Statistics page displays SNMP Statistics.

Net Monitoring Home Page

The Net Monitoring Home Page can be accessed from the WebView page by clicking on the **Net Monitoring** label under the Device Management group.

To configure the Device Management information, click **Device Mgmt** > **Net Monitoring** in the menu.

The following screen displays the **Net Monitoring Home** menu components.
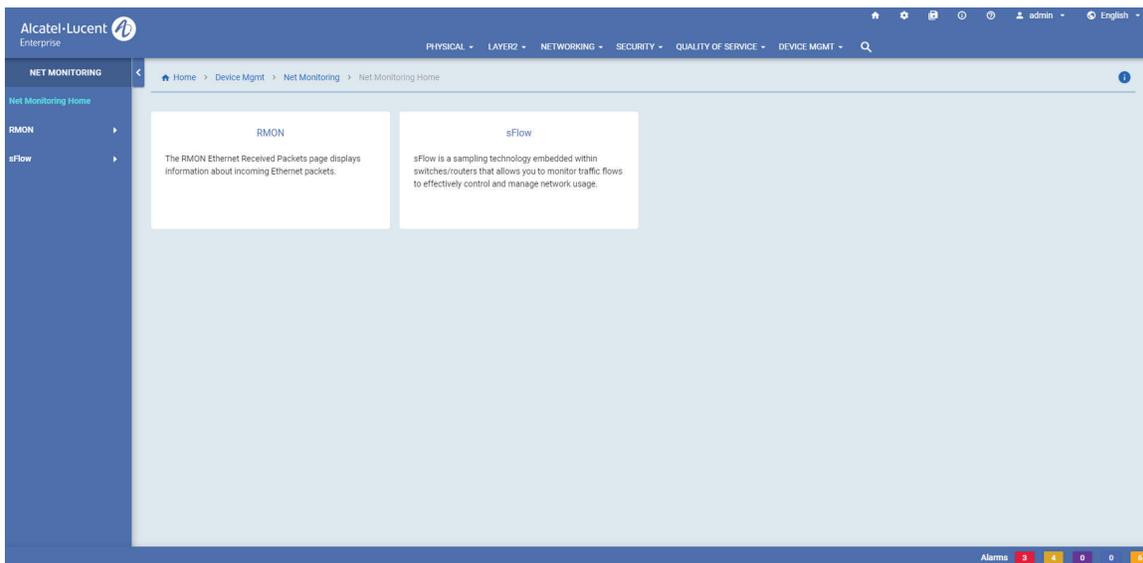
Figure 7-3 : Net Monitoring Home

The Net Monitoring Home page allows to configure and manage the following SNMP features:

Table 8: Net Monitoring Features

Features	Description
RMON	The RMON Ethernet Received Packets page displays information about incoming Ethernet packets.
sFLOW	sFlow is a sampling technology embedded within switches that allows you to monitor traffic flows to effectively control and manage network usage.

BLANK PAGE

8 Managing Automatic Remote Configuration Download

The Automatic Remote Configuration (RCL) capability automates and simplifies the deployment of large network installations eliminating the need for manual configuration of each switch. It also ensures that each switch is compliant with the centrally controlled switch configuration policies and firmware revisions.The Automatic Remote Configuration feature enables:

- the automatic upgrade of firmware and/or configuration of a standalone switch without user intervention.

- the automatic upgrade of firmware and/or configuration of a switch without user intervention.

- the automated configuration of the switch on bootup, when the switch is connected to the network for the first time.

- the automatic download and installation of the critical configuration bootup and image files.

In This Chapter

This chapter describes Automatic Remote Configuration on the OmniSwitch. The sections in this chapter are:

Automatic Remote Configuration Defaults

Figure 8-1 : Automatic Remote Configuration Defaults

Description	Default
DHCP Interface	VLAN 1
Instruction file	Location: TFTP Server File name: ***.alu** (* represents any instruction filename) Download location: **/flash** directory Downloaded as a temporary file.
Configuration file	File name: **Any name** Location: FTP/SFTP/TFTP Server Download location: **/flash/working** directory
Debug configuration file	File name: **AlcatelDebug.cfg** Location: FTP/SFTP/TFTP Server Download location: **/flash/working** directory
Script file	File name: **Any name** Location: FTP/SFTP/TFTP Server Download location: **/flash/working** directory
Firmware version	**Taos_*_*_R01** (*_* represents version number)
Firmware or image files	File name extension: ***.img** (* represents image filename) Location: FTP/SFTP/TFTP Server Download location: **/flash/working** directory
File download server	Primary FTP/SFTP/TFTP Server
Backup server for file download	Secondary FTP/SFTP/TFTP Server
Password for FTP/SFTP Server	Same as username

Quick Steps for Automatic Remote Configuration

1 Configure the DHCP server in the network to provide IP address, gateway, and TFTP server addresses to the OmniSwitch DHCP client.

2 Store the instruction file on the TFTP server.

3 Store the configuration, image, and script files on the primary and/or secondary FTP/SFTP servers.

4 When the OmniSwitch is integrated in to the network as a new device with no **vcboot.cfg** file the automatic remote configuration process is initiated.

5 A DHCP client is automatically configured on the OmniSwitch (see "DHCP Server Preference" on page 8-13). The OmniSwitch obtains IP address information, TFTP server address, instruction file name, and location from the DHCP server through the DHCP client.

6 The OmniSwitch downloads the instruction file from the TFTP server. The instruction file contains the file names and file locations of the configuration, image, and script files.

7 The OmniSwitch downloads the image files from the FTP/SFTP server if necessary.

8 The OmniSwitch downloads the configuration file from the FTP/SFTP server, if available, and saves it as the **vcboot.cfg** file in the **/flash/working/** directory. If no script file is downloaded, the switch reboots applying the downloaded configuration file and the automatic configuration process is complete.

9 The OmniSwitch downloads the script file, if available, from the FTP/SFTP server and runs the commands in the script file.

Notes.

- If the script file is not specified in the instruction file, or if it is not properly downloaded, then the Remote Configuration Manager software automatically initiates a **reload from working no rollback-timeout** command after firmware or bootup configuration files are downloaded.

- The script file does not support the **reload** command. If the command is included in the script file, a 'command not supported' error will be displayed.

- If a **write memory** command is used in the script file, then it overwrites the **vcboot.cfg** file. Hence, if the script file is downloaded along with the bootup configuration file, then the script file must not contain the **write memory** command.

- If a **vcboot.cfg** is already present on the switch, Automatic Remote Configuration Download does not occur.

Overview

The Automatic Remote Configuration feature provides the advantage of automatic download and installation of critical configuration and image files at initial bootup or when firmware upgrade is required for the OmniSwitch.

Automatic Remote Configuration download occurs when:

- There is no bootup configuration file (**vcboot.cfg**) on the switch.

- During a takeover or reboot on the new Primary unit or CMM.

- The initialization process of the switch is complete and the network interfaces or ports are ready.

- There is connectivity with a DHCP server through the default VLAN 1.

- There is connectivity with TFTP file server.

The following sections provide more information about the automatic configuration and download process.

Basic Operation

Automatic remote configuration process is initialized on the OmniSwitch if the **vcboot.cfg** file is not found on the switch.

The following illustration shows the basic setup required for Automatic Remote Configuration Download operation.
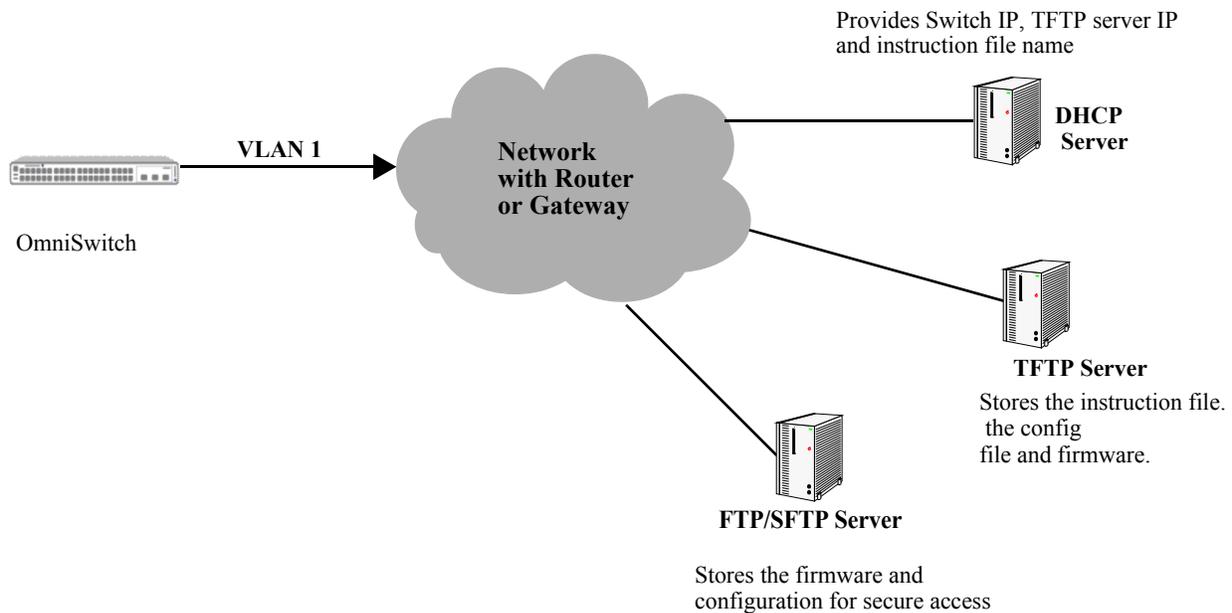
Figure 8-1 : Basic Network Components for Automatic Remote Configuration Download

Network Components

The network components required for the Automatic Remote Configuration download process are:

- DHCP server (mandatory)

- TFTP file server (mandatory)

- Primary FTP/SFTP server (mandatory)

- Secondary FTP/SFTP server (optional)

Information Provided by DHCP Server

When the network interfaces or ports on the switch are ready, a DHCP client is automatically configured on VLAN 1. The following information is acquired from the DHCP server, after a connection is established:

- IP address of the Network Gateway or Router.

- TFTP file server address.

- Instruction file name and location.

- Dynamic IP address for the OmniSwitch (valid only for initial bootup process).

Information Provided by Instruction File

The TFTP server address information is received from the DHCP server. The OmniSwitch downloads the instruction file from the TFTP server. The instruction file provides the following information:

- Firmware version and file location.

- Configuration file name and location.

- Debug configuration file name and location.

- Script file name and location.

- License file name and location.

- Primary FTP/SFTP file server address / type / username.

- Secondary FTP/SFTP file server address / type / username.

For more details on all the component files downloaded during the automatic remote configuration download process, see - .

File Servers and Download Process

The download process from the file servers is as follows:

1   The username required to connect to the FTP/SFTP enabled servers is provided in the instruction file. The password required to connect to the servers is same as the username.

2   The required files mentioned in the instruction file are downloaded from the primary FTP/SFTP file server.

3   If the configuration, debug and script file names are specified in the instruction file, then they are downloaded to the **/flash/working** directory of the switch.

4   The Remote Configuration Manager now compares the current firmware version on the switch to the one mentioned in the instruction file. If the firmware version is different, then firmware upgrade is performed.

5   The new firmware or image files are downloaded to the *working* directory of the switch.

Notes. If the primary server is down or if there is any failure in downloading the files from the primary file server, then a connection is established with the secondary file server. The secondary file server is used for file download.

---

6   All the required files are downloaded.

Notes. If a specific filename (for firmware and **configuration/debug/script** files) is not found, an error is logged. The download process continues with the next available file. File transfer is tried three times and if file transfer still fails, an error is logged, and download process is stopped. In such instances, the *working* folder of the switch will contain an incomplete set of image files, configuration, debug, or script files. For details on troubleshooting under such instances, see "Troubleshooting" on page 8-14.

---

7   Now, the DHCP client configured on the related VLAN is removed.

8   The script file is downloaded and the commands in the script file are run. All the commands in the script file are implemented on the switch in the order specified.

For other detailed steps that are part of the automatic remote configuration download process, see "Automatic Remote Configuration Download Process" on page 8-7

LED Status

The LED status during different stages of the Automatic Remote Configuration download process is as follows:

• DHCP phase: OK1 LED is flashing green

• DHCP lease obtained: OK1 LED is solid green

• DHCP phase stopped by console login: OK1 LED is solid green.

• Automatic Remote Configuration in process: OK1 LED is flashing amber.

Automatic Remote Configuration Download Process

The automatic remote configuration process is initialized when an OmniSwitch is integrated in to the network as a new device or when a firmware and configuration upgrade is required.

If the automatic configuration download process is not performed completely on the switch, manual intervention is required. For details on troubleshooting techniques under such instances, see "Troubleshooting" on page 8-14

The detailed process of Automatic Remote Configuration Download performed on the OmniSwitch is as follows:

1 When the switch is integrated in to the network as a new device with no **vcboot.cfg** file, then Automatic Remote Configuration is performed on the switch.

2 A DHCP client is automatically configured on VLAN 1 at switch boot up.

3 The DHCP client looks for the OV Cirrus DHCP server response to provide preference to the desired OV Cirrus DHCP server. For details, see the following section "DHCP Server Preference" on page 8-13

4 The DHCP client obtains the switch IP address information from the DHCP server.

5 The DHCP client obtains the TFTP server IP address from the DHCP server using Option (66).

6 The DHCP client obtains the instruction file name and location from the DHCP server using Option (67).

7 SSH access is automatically enabled to allow remote access in case the automatic configuration process fails.

8 The instruction file with the **.alu** extension is downloaded from the TFTP server to the **/flash/working** directory of the OmniSwitch.

9 If available, the configuration, script, and images files are downloaded from the FTP or SFTP servers. The password used to connect to the FTP/SFTP servers is same as the username.

10 If available, the switch compares the firmware version available on the switch with the firmware version in the instruction file. If the firmware versions are different, then the new firmware is downloaded in to the **/flash/working** directory.

11 If available, the downloaded configuration file is saved as the **vcboot.cfg** file in the **/flash/working** directory and the switch is rebooted completing the auto configuration process (a reboot occurs only if no script file is downloaded).

12 The RCL process will not work if the **/flash/working** directory is deleted before RCL is started.

13 If available, commands in the script file are run and the DHCP client configuration is automatically removed.

14 Manual intervention in RCL process is allowed only if there are any issues in completing the RCL process automatically.

15 The switch is automatically reloaded once the RCL process is successfully completed.

Additional Process Notes

1   Once the switch obtains an IP interface from the DHCP server, remote access through SSH is automatically configured to allow remote access in case of any download errors during the Auto Configuration process.

Notes. It is not recommended to have the **write memory** command in the script file if a configuration file is downloaded. This causes the **vcboot.cfg** file to be overwritten with the commands in the script file.

---

2   After the successful download of the script file, the DHCP IP interface is automatically deleted. However, SSH access remains enabled. Use the **no aaa authentication ssh** command to disable SSH connectivity if desired.

3   The Automatic Remote Configuration process can be stopped using the **auto-config-abort** command.

Download Component Files

This section provides the details of the files downloaded and how they are utilized during the automatic configuration process. The main component files are:

- **Instruction file**—The instruction file is the initial file required for the automatic remote configuration process to occur. The instruction file is stored in the TFTP server with the **.alu** extension. For further details, see "Instruction File" on page 8-9

- **Firmware upgrade files**—The firmware files or image files differ for different OmniSwitch platforms. These image files contain executable code, which provides support for the system, Ethernet ports, and network functions. For further details, see "Firmware Upgrade Files" on page 8-11

- **Bootup configuration file**—The file contains bootup configuration information for the switch. The bootup configuration file stores the network configuration parameters. For further details, see "Bootup Configuration File" on page 8-11

- **Debug Configuration file**—The debug configuration file stores the default debug configuration information. For further details, see "Debug Configuration File" on page 8-11

- **Script file**—The script file consists of commands to be performed on the switch so that appropriate actions can be taken on the downloaded files. For further details, see "Script File" on page 8-12

Instruction File

The instruction file is the initial file required for automatic remote configuration process to occur. The instruction file is stored in the TFTP server with the **.alu** extension.

The instruction file contains user information such as switch ID, file version, firmware version, image file names and location, configuration file (**vcboot.cfg**) name and location, script file name and location, and FTP/SFTP server IP address to connect to the FTP/SFTP server.

The TFTP server IP address and instruction filename details are received from the DHCP server by the DHCP client on the OmniSwitch.

The instruction file is downloaded from the TFTP server and stored in the **/flash** directory of the switch.

Notes.

- If an error or failure occurs during the file transfer, the transfer process is retried up to three times. If file transfer and download are not successful, the automatic remote configuration process is halted and the switch is made available remotely using SSH.

- All contents of the instruction file are stored in the switch log (**swlog.log**) file as evidence of the last Automatic Remote Configuration download.

Instruction File Syntax

The instruction file is a text file containing the following information:

Header	Contains user information such as switch ID, file version, and so on. Header text is a type of comment.
Comments	Comments provide additional information for better user readability. These lines are ignored during the remote configuration download process.

Firmware version and file location	Image files required for firmware upgrade. A firmware location can have only one entry. It cannot be copied to certified or to instruction file with multiple directory.
Configuration file name and location	The file containing the configuration for the switch, this file is saved as the **vcboot.cfg** file in the **/flash** directory.
Debug file name and location	The **AlcatelDebug.cfg** containing additional debug configuration commands.
Script file name and location	The script file containing commands to be implemented on the switch.
License file name and location	The license file containing the licensing information.
Primary file server address/ protocol/username	The primary file server from which the required files are downloaded. The specified protocol and username is used for the download.
Secondary file server address/ protocol/username	The secondary file server from which the required files are downloaded if the connection to primary file server fails. The specified protocol and username are used for the download.

Example

The instruction file has the Keyword:Value format as shown below:

```
! Alcatel-Lucent OmniSwitch OS2x60 – Instruction file version 1.2.1
! Firmware version
Firmware version:OS_5.1R01
Firmware location:/home/ftpboot/firmware
! Configuration file
Config filename:boot_OS2x60.cfg
Config location:/home/ftpboot/config
! Debug file
Debug filename:AlcatelDebug.cfg
Debug location:/home/ftpboot/debug
! Script File
Script filename:OS2x60_script.txt
Script location:/home/ftpboot/scripts
! License File
License filename:swlicense.dat
License location:/home/ftpboot/license
! Primary file Server
Primary server:10.200.100.112
Primary protocol:FTP
Primary user:admin
! Secondary file Server
Secondary server:10.200.110.111
Secondary protocol:SFTP
Secondary user:admin
```

Instruction File Usage Guidelines

- The instruction file is case sensitive and can contain only the keywords provided in the instruction file output example.

- The keywords can be placed in any order.

- If the Keyword:Value format is incorrect, the information on that line is discarded.

- Firmware version must be provided in the format as specified in the example.

- Pathnames provided must contain the complete path to the file location.

- If any file is not required, the value is provided as "None". For example, if a debug configuration file is not required to be downloaded, the instruction file syntax is as follows:

```
Debug filename:None
Debug location:None
```

- The header line is the first line of the instruction file and begins with "!" character.

- Header line contents are logged to the switch log along with the other contents of the instruction file.

- The header and comment lines begin with "!" character.

Firmware Upgrade Files

Firmware files are also known as image files. These files have the **.img** extension.

Firmware files may be different based on the OmniSwitch platform. The relevant firmware files are downloaded from the location mentioned in the instruction file. The filenames of the firmware files must exactly match the files which are to be downloaded. The filenames are in the ***.img** format. Modified filenames are not recognized.

Firmware files are downloaded only when the firmware version in the instruction file is higher than the firmware version present on the switch.

Bootup Configuration File

The bootup configuration file (**vcboot.cfg**) is not present during the initial bootup process when a new OmniSwitch is integrated in to the network. The **vcboot.cfg** file is automatically generated and stored in the **/flash/working** directory when a **write memory** command is issued.

During the automatic remote configuration process, the bootup configuration file is downloaded from the FTP/SFTP server and stored as **vcboot.cfg** in the **/flash/working** directory of the switch.

If no script file is downloaded, the switch boots up normally according to the configurations specified in the **vcboot.cfg** file when the remote configuration download process is completed.

Debug Configuration File

The debug configuration file is used for setting specific OmniSwitch settings and must only be used as directed by Service and Support. During the automatic remote configuration process, the debug configuration file is downloaded with the filename **AlcatelDebug.cfg**.

Script File

The script file is downloaded and stored with the same name in the **/flash/working** directory. The script file contains the commands to be implemented on the switch after running the configuration file.

If a configuration file is not available, the script file can be used to configure the switch dynamically without a **vcboot.cfg** file.

Script File Example

```
vlan 100 enable name "VLAN 100"
vlan 100 members port 1/1/1 untagged
write memory
```

Script File Usage Guidelines

- It is recommended to create the script file with a Unix / Linux type text editor. Creating the script file in a Windows environment can result in hidden control characters that may cause issues with script file parsing.

- After the script file is downloaded the switch does not automatically reboot.

- If a **write memory** command is used in the script file, then it overwrites the **vcboot.cfg** file. Hence, the script file must not contain the **write memory** command if it is downloaded along with the configuration file.

- If any script file command fails, it is logged in to a file ***.err** (* is the script file name) in the **/flash** directory and the remaining commands are implemented.

- If the script file name mentioned in the instruction file is incorrect, then an error is logged in the switch log or **swlog.log** file.

DHCP Server Preference

When RCL is running and the DHCP client is created, the following steps are followed in order to provide preference to different DHCP servers. When server-preference is enabled, the following precedence order is followed for the VLAN 1 DHCP client.

    1.OXO DHCP Server:"alcatel.a4400.0"

    2.OVCirrus Server:"alenterprise"

    3.OVClient Server:"alcatel.nms.ov2500"

    4.Others : Identified by absence of VSI string

The following describes the DHCP client preference operation:

1   If a DHCP response is received on the VLAN 1 DHCP client from a non-preferred DHCP server it will be stored during the 30 second window allowing time for a DHCP response from a higher preference server. Subsequent responses from non-preferred DHCP servers will be dropped.

2   If a DHCP response is received on the VLAN 1 DHCP client from an OXO DHCP server it will overwrite any non-preferred DHCP response. The response will be stored during the 30 second window allowing time for a DHCP response from an high preference server. Subsequent responses from any OXO DHCP servers or non-preferred DHCP servers will be dropped.

3   If a DHCP response is received on the VLAN 1 DHCP client from an OmniVista DHCP server it will overwrite any non-preferred DHCP response. The response will be stored during the 30 second window allowing time for a DHCP response from an OVCloud server. Subsequent responses from any OmniVista /OXO DHCP servers/non-preferred DHCP servers will be dropped.

4   If a DHCP response is received on the VLAN 1 DHCP client from an OVCloud DHCP server it will overwrite any existing DHCP responses and be applied immediately.

Note:
- A DHCP server should be configured and have connectivity to the switch during the initial boot-up.

 - The RCL process may be delayed while waiting for a preferred server.

Troubleshooting

Due to errors during download, the automatic configuration process can halt, or the file download process can be incomplete. The errors that occur during the automatic remote configuration download process are displayed on the switch command prompt and also stored in switch log or the **swlog.log** file.

The following section provides information on some of the common errors that can occur during the configuration download process and troubleshooting techniques to resolve these errors.

Error Resolution

If there are any issues downloading the required files for the auto configuration process the switch can be reached using the DHCP client IP address and the SSH protocol for manual intervention or configuration.

Server Connection Failure and File Download Errors

Manual download of component files is required when there is a failure in connecting to the servers or when all the component files are not downloaded during the automatic remote configuration download process.

Server connection failures can occur when:

- DHCP server is not reachable.

- TFTP server is not reachable.

- Primary and secondary servers are not reachable.

File download errors can occur when:

- Files are corrupted.

- File locations or names listed in the instruction file are incorrect.

Error Description Table

The following table provides information on the common server connection failures and file download errors that can occur during Automatic Remote Configuration:

Error Type	Error	Description
User Auto-Config Abort	`Automatic Remote Config Abort received.`	User manually aborted the process using the auto-config-abort command
TFTP Response Timeout	`Instruction File not Downloaded and the Max try 3 For TFTP reached.`	Instruction file not downloaded due to TFTP not reachable.

Primary/ Secondary Server Connection	`Download of file: <File name and pathname> from Primary Server Failed`
	
	`Starting download of file: <File name and pathname> from Secondary Server`
		File download failure from primary server.

	`Download Failed - <File name and pathname> using both Pri & Sec IP`	File download failure from both primary and secondary server.
File Download and File Location Errors	`Transfer error <File name and pathname>`	File transfer failure.
	`Download failed for configuration file <File name and pathname>`	Configuration file download failure.
	`Not all image files are downloaded`	Some of the image files are not downloaded.

	`Unable to download the firmware version`
	
	`Unable to download boot config file`
	
	`Unable to download AlcatelDebug.cfg`
	
	`Unable to download script file`
		File location errors occur when the corresponding files are not available in the locations as mentioned in the instruction file.

Script File Errors

The different types of script file errors and the troubleshooting techniques for such errors are as follows:

- If any script file command fails, it is logged in to a file ***.err** (* is the script file name) in the **/flash** directory and the remaining commands are implemented. In such an instance, check the ***.err** file. The script file commands can be manually implemented and debugged in the order specified in the script file.

- If the script file name mentioned in the instruction file is incorrect, then an error is logged in the switch log or **swlog.log** file. In such an instance, check the **swlog.log** file. The script file can be downloaded manually from the FTP/SFTP servers and implemented onto the OmniSwitch.

Error Description Table

The following error description table provides information about some of the common script file errors that occur during Automatic Remote Configuration:

Error Type	Error	Description
Script File Download	Download of Script file from Primary Server Failed	Script file cannot be downloaded from the primary server.
	Starting download of Script file: *<File name and pathname>* from Secondary Server	
	Download failed - *<File name and pathname>* using Pri and Sec IP	Script file cannot be downloaded from both primary and secondary server.
Script File Command Failure	Unable to remove Instruction file *<File name and pathname>*	Instruction file cannot be removed from flash due to error in running the script file commands.
	Error in executing the downloaded script file	The downloaded script file cannot be run.

A Software License and Copyright Statements

This appendix contains Alcatel-Lucent and third-party software vendor license and copyright statements.

Alcatel-Lucent License Agreement

ALE USA, Inc. SOFTWARE LICENSE AGREEMENT

IMPORTANT. Please read the terms and conditions of this license agreement carefully before opening this package.

By opening this package, you accept and agree to the terms of this license agreement. If you are not willing to be bound by the terms of this license agreement, do not open this package. Please promptly return the product and any materials in unopened form to the place where you obtained it for a full refund.

1. **License Grant.** This is a license, not a sales agreement, between you (the "Licensee") and Alcatel-Lucent Alcatel-Lucent hereby grants to Licensee, and Licensee accepts, a non-exclusive license to use program media and computer software contained therein (the "Licensed Files") and the accompanying user documentation (collectively the "Licensed Materials"), only as authorized in this License Agreement. Licensee, subject to the terms of this License Agreement, may use one copy of the Licensed Files on the Licensee's system. Licensee agrees not to assign, sublicense, transfer, pledge, lease, rent, or share their rights under this License Agreement. Licensee may retain the program media for backup purposes with retention of the copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Licensed Materials or any portions thereof may be made by Licensee and Licensee shall not modify, decompile, disassemble, reverse engineer, or otherwise attempt to derive the Source Code. Licensee is also advised that Alcatel-Lucent products contain embedded software known as firmware which resides in silicon. Licensee may not copy the firmware or transfer the firmware to another medium.

2. **ALE USA, Inc.'s Rights.** Licensee acknowledges and agrees that the Licensed Materials are the sole property of Alcatel-Lucent and its licensors (herein "its licensors"), protected by U.S. copyright law, trademark law, and are licensed on a right to use basis. Licensee further acknowledges and agrees that all rights, title, and interest in and to the Licensed Materials are and shall remain with Alcatel-Lucent and its licensors and that no such right, license, or interest shall be asserted with respect to such copyrights and trademarks. This License Agreement does not convey to Licensee an interest in or to the Licensed Materials, but only a limited right to use revocable in accordance with the terms of this License Agreement.

3. **Confidentiality.** Alcatel-Lucent considers the Licensed Files to contain valuable trade secrets of Alcatel-Lucent, the unauthorized disclosure of which could cause irreparable harm to Alcatel-Lucent. Except as expressly set forth herein, Licensee agrees to use reasonable efforts not to disclose the Licensed Files to any third party and not to use the Licensed Files other than for the purpose authorized by this License Agreement. This confidentiality obligation shall continue after any termination of this License Agreement.

4. **Indemnity.** Licensee agrees to indemnify, defend and hold Alcatel-Lucent harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation Alcatel-Lucent's reasonable United States and local attorneys' and expert witnesses' fees and costs) arising out of or in connection with the unauthorized copying, marketing, performance or distribution of the Licensed Files.

5. **Limited Warranty.** Alcatel-Lucent warrants, for Licensee's benefit alone, that the program media shall, for a period of ninety (90) days from the date of commencement of this License Agreement (referred to as the Warranty Period), be free from defects in material and workmanship. Alcatel-Lucent further warrants, for Licensee benefit alone, that during the Warranty Period the Licensed Files shall operate substantially in accordance with the functional specifications in the User Guide. If during the Warranty Period, a defect in the Licensed Files appears, Licensee may return the Licensed Files to Alcatel-Lucent for either replacement or, if so elected by Alcatel-Lucent, refund of amounts paid by Licensee under this License Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE LICENSED MATERIALS ARE LICENSED "AS IS" AND ALE USA, Inc. AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS WARRANTY GIVES THE LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

6. **Limitation of Liability.** Alcatel-Lucent's cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the license fee paid to Alcatel-Lucent for the Licensed Materials. IN NO EVENT SHALL ALE USA, Inc. BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF ALE USA, Inc. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION TO INCIDENTAL OR CONSEQUENTIAL DAMAGES MAY NOT APPLY TO LICENSEE.

7. **Export Control.** This product is subject to the jurisdiction of the United States. Licensee may not export or reexport the Licensed Files, without complying with all United States export laws and regulations, including but not limited to (i) obtaining prior authorization from the U.S. Department of Commerce if a validated export license is required, and (ii) obtaining "written assurances" from licensees, if required.

8. **Support and Maintenance.** Except as may be provided in a separate agreement between Alcatel-Lucent and Licensee, if any, Alcatel-Lucent is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and Alcatel-Lucent has no obligation to furnish Licensee with any further assistance, documentation or information of any nature or kind.

9. **Term.** This License Agreement is effective upon Licensee opening this package and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Licensed Materials and all copies thereof and extracts therefrom to Alcatel-Lucent and certifying to Alcatel-Lucent in writing that all Licensed Materials and all copies thereof and extracts therefrom have been returned or erased by the memory of Licensee's computer or made non-readable. Alcatel-Lucent may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by

Alcatel-Lucent, Licensee agrees to return to ALE USA, Inc.ALE USA, Inc. or destroy the Licensed Materials and all copies and portions thereof.

10. **Governing Law.** This License Agreement shall be construed and governed in accordance with the laws of the State of California.

11. **Severability.** Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms herein.

12. **No Waiver.** The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13. **Notes to United States Government Users.** Software and documentation are provided with restricted rights. Use, duplication or disclosure by the government is subject to (i) restrictions set forth in GSA ADP Schedule Contract with ALE USA, Inc.'s reseller(s), or (ii) restrictions set forth in subparagraph (c) (1) and (2) of 48 CFR 52.227-19, as applicable.

14.**Third Party Materials.** Licensee is notified that the Licensed Files contain third party software and materials licensed to ALE USA, Inc. by certain third party licensors. Some third party licensors (e.g., Wind River and their licensors with respect to the Run-Time Module) are third part beneficiaries to this License Agreement with full rights of enforcement. Please refer to the section entitled "Third Party Licenses and Notices" on page A-4 for the third party license and notice terms.

Third Party Licenses and Notices

The licenses and notices related only to such third party software are set forth below:

A. Booting and Debugging Non-Proprietary Software

A small, separate software portion aggregated with the core software in this product and primarily used for initial booting and debugging constitutes non-proprietary software, some of which may be obtained in source code format from ALE USA, Inc. for a limited period of time. ALE USA, Inc. will provide a machine-readable copy of the applicable non-proprietary software to any requester for a cost of copying, shipping and handling. This offer will expire 3 years from the date of the first shipment of this product.

B. The OpenLDAP Public License: Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1 Redistributions of source code must retain copyright statements and notices.

2 Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3 Redistributions must contain a verbatim copy of this document.

4 The names and trademarks of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission.

5 Due credit should be given to the OpenLDAP Project.

6 The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use the Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATIO OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenLDAP is a trademark of the OpenLDAP Foundation.

Copyright 1999-2000 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distributed verbatim copies of this document is granted.

C. Linux

Linux is written and distributed under the GNU General Public License which means that its source code is freely-distributed and available to the general public.

D. GNU GENERAL PUBLIC LICENSE: Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0 This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either

verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1 You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

> **b** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

> **c** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4 You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6 Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on

consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8 If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9 The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10 If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

    <one line to give the program's name and a brief idea of what it does.> Copyright (C)
    19yy <name of author>

    This program is free software; you can redistribute it and/or modify it under the terms of
    the GNU General Public License as published by the Free Software Foundation; either
    version 2 of the License, or (at your option) any later version.

    This program is distributed in the hope that it will be useful, but WITHOUT ANY
    WARRANTY; without even the implied warranty of MERCHANTABILITY or
    FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License
    for more details.

    You should have received a copy of the GNU General Public License along with this
    program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge,
    MA 02139, USA.

 Also add information on how to contact you by electronic and paper mail.

 If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with
    ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software,
    and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

    Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision'
    (which makes passes at compilers) written by James Hacker.

    <signature of Ty Coon>, 1 April 1989
    Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

    URLWatch:
        For notice when this page changes, fill in your email address.

Maintained by: Webmaster, Linux Online Inc.
Last modified: 09-Aug-2000 02:03AM.
Views since 16-Aug-2000: 177203.

Material copyright Linux Online Inc.
Design and compilation copyright (c)1994-2002 Linux Online Inc.
Linux is a registered trademark of Linus Torvalds
Tux the Penguin, featured in our logo, was created by Larry Ewing
Consult our privacy statement

URLWatch provided by URLWatch Services.
All rights reserved.

E. University of California

Provided with this product is certain TCP input and Telnet client software developed by the University of California, Berkeley.

Copyright (C) 1987. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

F. Carnegie-Mellon University

Provided with this product is certain BOOTP Relay software developed by Carnegie-Mellon University.

G. Random.c

PR 30872 B Kesner created May 5 2000
PR 30872 B Kesner June 16 2000 moved batch_entropy_process to own task iWhirlpool to make code more efficient

random.c -- A strong random number generator

Version 1.89, last modified 19-Sep-99

Copyright Theodore Ts'o, 1994, 1995, 1996, 1997, 1998, 1999. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. ALTERNATIVELY, this product may be distributed under the terms of the GNU Public License, in which case the provisions of the GPL are required INSTEAD OF the

above restrictions. (This clause is necessary due to a potential bad interaction between the GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROF-ITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABIL-ITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

H. Apptitude, Inc.

Provided with this product is certain network monitoring software ("MeterWorks/RMON") licensed from Apptitude, Inc., whose copyright notice is as follows: Copyright (C) 1997-1999 by Apptitude, Inc. All Rights Reserved. Licensee is notified that Apptitude, Inc. (formerly, Technically Elite, Inc.), a California corporation with principal offices at 6330 San Ignacio Avenue, San Jose, California, is a third party bene-ficiary to the Software License Agreement. The provisions of the Software License Agreement as applied to MeterWorks/RMON are made expressly for the benefit of Apptitude, Inc., and are enforceable by Apptitude, Inc. in addition to ALE USA, Inc.. IN NO EVENT SHALL APPTITUDE, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES, INCLUDING COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES, LOST PROFITS, OR ANY SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, ARISING IN ANY WAY OUT OF THIS AGREEMENT.

I. Agranat

Provided with this product is certain web server software ("EMWEB PRODUCT") licensed from Agranat Systems, Inc. ("Agranat"). Agranat has granted to ALE USA, Inc. certain warranties of performance, which warranties [or portion thereof] ALE USA, Inc. now extends to Licensee. IN NO EVENT, HOWEVER, SHALL AGRANAT BE LIABLE TO LICENSEE FOR ANY INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES OF LICENSEE OR A THIRD PARTY AGAINST LICENSEE ARIS-ING OUT OF, OR IN CONNECTION WITH, THIS DISTRIBUTION OF EMWEB PRODUCT TO LICENSEE. In case of any termination of the Software License Agreement between ALE USA, Inc. and Licensee, Licensee shall immediately return the EMWEB Product and any back-up copy to ALE USA, Inc., and will certify to ALE USA, Inc. in writing that all EMWEB Product components and any copies of the software have been returned or erased by the memory of Licensee's computer or made non-readable.

J. RSA Security Inc.

Provided with this product is certain security software ("RSA Software") licensed from RSA Security Inc. RSA SECURITY INC. PROVIDES RSA SOFTWARE "AS IS" WITHOUT ANY WARRANTY WHAT-SOEVER. RSA SECURITY INC. DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STAT-UTORY, AS TO ANY MATTER WHATSOEVER INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

K. Sun Microsystems, Inc.

This product contains Coronado ASIC, which includes a component derived from designs licensed from Sun Microsystems, Inc.

L. Wind River Systems, Inc.

Provided with this product is certain software ("Run-Time Module") licensed from Wind River Systems, Inc. Licensee is prohibited from: (i) copying the Run-Time Module, except for archive purposes consistent with Licensee's archive procedures; (ii) transferring the Run-Time Module to a third party apart from the product; (iii) modifying, decompiling, disassembling, reverse engineering or otherwise attempting to derive the source code of the Run-Time Module; (iv) exporting the Run-Time Module or underlying technology in contravention of applicable U.S. and foreign export laws and regulations; and (v) using the Run-Time Module other than in connection with operation of the product. In addition, please be advised that: (i) the Run-Time Module is licensed, not sold and that ALE USA, Inc. and its licensors retain ownership of all copies of the Run-Time Module; (ii) WIND RIVER DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, (iii) The SOFTWARE LICENSE AGREEMENT EXCLUDES LIABILITY FOR ANY SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL AND CONSEQUENTIAL DAMAGES; and (iv) any further distribution of the Run-Time Module shall be subject to the same restrictions set forth herein. With respect to the Run-Time Module, Wind River and its licensors are third party beneficiaries of the License Agreement and the provisions related to the Run-Time Module are made expressly for the benefit of, and are enforceable by, Wind River and its licensors.

M. Network Time Protocol Version 4

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
***********************************************************************
*                                                                     *
* Copyright (c) David L. Mills 1992-2003                              *
*                                                                     *
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose and without fee is hereby         *
* granted, provided that the above copyright notice appears in all    *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name        *
* University of Delaware not be used in advertising or publicity      *
* pertaining to distribution of the software without specific,        *
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
* warranty.                                                           *
*                                                                     *
***********************************************************************
```

N. Remote-ni

Provided with this product is a file (part of GDB), the GNU debugger and is licensed from Free Software Foundation, Inc., whose copyright notice is as follows: Copyright (C) 1989, 1991, 1992 by Free Software Foundation, Inc. Licensee can redistribute this software and modify it under the terms of General Public License as published by Free Software Foundation Inc.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

O. GNU Zip

GNU Zip -- A compression utility which compresses the files with zip algorithm.

Copyright (C) 1992-1993 Jean-loup Gailly.

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

P. FREESCALE SEMICONDUCTOR SOFTWARE LICENSE AGREEMENT

Provided with this product is a software also known as DINK32 (Dynamic Interactive Nano Kernel for 32-bit processors) solely in conjunction with the development and marketing of your products which use and incorporate microprocessors which implement the PowerPC (TM) architecture manufactured by Motorola. The licensee comply with all of the following restrictions:

1. This entire notice is retained without alteration in any modified and/or redistributed versions.

2. The modified versions are clearly identified as such. No licenses are granted by implication, estoppel or otherwise under any patents or trademarks of Motorola, Inc.

The SOFTWARE is provided on an "AS IS" basis and without warranty. To the maximum extent permitted by applicable law, MOTOROLA DISCLAIMS ALL WARRANTIES WHETHER EXPRESS OR IMPLIED, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST INFRINGEMENT WITH REGARD TO THE SOFTWARE (INCLUDING ANY MODIFIED VERSIONS THEREOF) AND ANY ACCOM-PANYING WRITTEN MATERIALS.To the maximum extent permitted by applicable law, IN NO EVENT SHALL MOTOROLA BE LIABLE FOR ANY DAMAGES WHATSOEVER.

Copyright (C) Motorola, Inc. 1989-2001 All rights reserved.

Version 13.1

Q. Boost C++ Libraries

Provided with this product is free peer-reviewed portable C++ source libraries.

Version 1.33.1

Copyright (C) by Beman Dawes, David Abrahams, 1998-2003. All rights reserved.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

R. U-Boot

Provided with this product is a software licensed from Free Software Foundation Inc. This is used as OS Bootloader; and located in on-board flash. This product is standalone and not linked (statically or dynamically) to any other software.

Version 1.1.0

Copyright (C) 2000-2004. All rights reserved.

S. Solaris

Provided with this product is free software; Licensee can redistribute it and/or modify it under the terms of the GNU General Public License.

Copyright (C) 1992-1993 Jean-loup Gailly. All rights reserved.

T. Internet Protocol Version 6

Copyright (C) 1982, 1986, 1990, 1991, 1993. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE. FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL. DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS. OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION). HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT. LIABIL-ITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The copyright of the products such as crypto, dhcp, net, netinet, netinet6, netley, netwrs, libinet6 are same as that of the internet protocol version 6.

U. CURSES

Copyright (C) 1987. The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

V. ZModem

Provided with this product is a program or code that can be used without any restriction.

Copyright (C) 1986 Gary S. Brown. All rights reserved.

W. Boost Software License

Provided with this product is reference implementation, so that the Boost libraries are suitable for eventual standardization. Boost works on any modern operating system, including UNIX and Windows variants.

Version 1.0

Copyright (C) Gennadiy Rozental 2005. All rights reserved.

X. OpenLDAP

Provided with this software is an open source implementation of the Lightweight Directory Access Protocol (LDAP).

Version 3

Copyright (C) 1990, 1998, 1999, Regents of the University of Michigan, A. Hartgers, Juan C. Gomez. All rights reserved.

This software is not subject to any license of Eindhoven University of Technology.Redistribution and use in source and binary forms are permitted only as authorized by the OpenLDAP Public License.

This software is not subject to any license of Silicon Graphics Inc.or Purdue University. Redistribution and use in source and binary forms are permitted without restriction or fee of any kind as long as this notice is preserved.

Y. BITMAP.C

Provided with this product is a program for personal and non-profit use.

Copyright (C) Allen I. Holub, All rights reserved.

Z. University of Toronto

Provided with this product is a code that is modified specifically for use with the STEVIE editor. Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.

2.The origin of this software must not be misrepresented, either by explicit claim or by omission.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

Version 1.5

Copyright (C) 1986 by University of Toronto and written by Henry Spencer.

AA.Free/OpenBSD

Copyright (c) 1982, 1986, 1990, 1991, 1993 The Regents of University of California. All Rights Reserved.