

Release Notes - Rev. A

OmniSwitch 2260, 2360

Release 5.1R1

These release notes accompany AOS Release 5.1R1. These release notes provide important information on individual software features and hardware modules. Since much of the information in these release notes is not included in the hardware and software user manuals, it is important that you read all sections of this document before installing new hardware or loading new software.

Contents

Contents 2

Related Documentation 3

System Requirements 4

Prerequisites 5

Supported Hardware 6

Supported Transceivers..... 8

Supported Software Features 9

Unsupported Software Features 13

Open Problem Reports and Feature Exceptions 14

Technical Support..... 15

Appendix A - Specifications 16

Related Documentation

These release notes should be used in conjunction with OmniSwitch AOS Release 5 User Guides. The following are the titles of the user guides that apply to this release.

- OmniSwitch 2260/2360 Hardware User Guide
- OmniSwitch 2260/2360 AOS Release 5.1R1 CLI Reference Guide
- OmniSwitch 2260/2360 AOS Release 5.1R1 WebView Guide

System Requirements

Memory Requirements

The following are the standard shipped memory configurations. Configuration files and the compressed software image, including web management software images, are stored in the flash memory.

Platform	SDRAM	Flash
OS2260	512 MB	512 MB
OS2360	1 GB	512 MB

UBoot and FPGA Requirements

The software versions listed below are the MINIMUM required, except where otherwise noted. Switches running the minimum versions, as listed below, do not require any UBoot or FPGA upgrades. Use the 'show hardware-info' command to determine the current versions.

Switches not running the minimum version required should upgrade to the latest UBoot or FPGA that is available with this release available from Service & Support.

OmniSwitch 2x60 - AOS Release 5.1.80.R01 (GA)

Hardware	Minimum UBoot	Minimum FPGA
OS2260	5.1.8.R01	0.5
OS2360	5.1.8.R01	0.6

Prerequisites

The OmniSwitch 2260/2360 products do not contain a real-time clock.

- It is recommended to use NTP to ensure time synchronization.
- When the switch is reset, the switch will boot up from an approximation of the last known good time.
- When the switch is powered off it cannot detect the time left in the powered off state. When it boots up it will have the same time as when the switch was last powered off.

Supported Hardware

The following new hardware is being introduced in this release.

OS2260-10

Fixed-configuration chassis in a 1U form factor with:

- 8 x RJ45 non-PoE ports
- 4 x SFP (1G) ports
- Internal power supply
- Fanless

OS2260-P10

Fixed-configuration chassis in a 1U form factor with:

- 8 x RJ45 PoE (802.3at) ports
- 4 x SFP (1G) ports
- Internal power supply
- Fanless

OS2260-24

Fixed-configuration chassis in a 1U form factor with:

- 24 x RJ45 non-PoE ports
- 4 x SFP (1G) ports
- Internal power supply
- Fanless

OS2260-P24

Fixed-configuration chassis in a 1U form factor with:

- 24 x RJ45 PoE (802.3at) ports
- 4 x SFP (1G) ports
- Internal power supply
- 1 Fan

OS2260-P24X (China model)

Fixed-configuration chassis in a 1U form factor with:

- 24 x RJ45 PoE (802.3at) ports
- 2 x SFP (1G) ports
- 2 x SFP+ (1G/10G) ports
- Internal power supply
- 1 Fan

OS2260-48

Fixed-configuration chassis in a 1U form factor with:

- 48 x RJ45 non-PoE ports
- 6 x SFP (1G) ports
- Internal power supply
- 1 Fan

OS2260-P48

Fixed-configuration chassis in a 1U form factor with:

- 48 x RJ45 PoE (802.3at) ports
- 6 x SFP (1G) ports
- Internal power supply
- 1 Fan

OS2260-P48X (China model)

Fixed-configuration chassis in a 1U form factor with:

- 48 x RJ45 PoE ports
- 4 x SFP (1G) ports

- 2 x SFP+ (1G/10G) ports
- Internal power supply
- 2 Fans

OS2360-24

Fixed-configuration chassis in a 1U form factor with:

- 24 x RJ45 non-PoE ports
- 2 x SFP (1G) ports
- 2 x SFP (1G) Uplink or SFP+ (10G) VFL ports
- Internal power supply
- Fanless

OS2360-P24

Fixed-configuration chassis in a 1U form factor with:

- 24 x RJ45 PoE (802.3at) ports
- 2 x SFP (1G) ports
- 2 x SFP (1G) Uplink or SFP+ (10G) VFL ports
- Internal power supply
- 1 Fan

OS2360-P24X

Fixed-configuration chassis in a 1U form factor with:

- 24 x RJ45 PoE (802.3at) ports
- 2 x SFP+ (1G/10G) ports
- 2 x SFP (1G) Uplink or SFP+ (10G) VFL ports
- Internal power supply
- 1 Fan

OS2360-48

Fixed-configuration chassis in a 1U form factor with:

- 48 x RJ45 non-PoE ports
- 4 x SFP (1G) ports
- 2 x SFP (1G) Uplink or SFP+ (10G) VFL ports
- Internal power supply
- 1 Fan

OS2360-P48

Fixed-configuration chassis in a 1U form factor with:

- 48 x RJ45 PoE (802.3at) ports
- 4 x SFP (1G) ports
- 2 x SFP (1G) Uplink or SFP+ (10G) VFL ports
- Internal power supply
- 1 Fan

OS2360-P48X

Fixed-configuration chassis in a 1U form factor with:

- 48 x RJ45 PoE ports
- 2 x SFP (1G) ports
- 2 x SFP+ (10G) ports
- 2 x SFP (1G) Uplink or SFP+ (10G) VFL ports
- Internal power supply
- 2 Fans

Supported Transceivers

Transceiver	OS2260	OS2360
SFP-GIG-T - 1000BaseT Gigabit Ethernet Transceiver (SFP MSA). SFP works at 1000 Mb/s speed and full duplex mode.	Supported	Supported
SFP-GIG-SX - 1000Base SX Gigabit Ethernet optical transceiver (SFP MSA).	Supported	Supported
SFP-GIG-LX - 1000Base LX Gigabit Ethernet optical transceiver (SFP MSA).	Supported	Supported
SFP-GIG-LH40 - 1000Base LH Gigabit Ethernet optical transceiver (SFP MSA). Typical reach of 40 km on 9/125 μ m SMF.	Supported	Supported
SFP-GIG-LH70 - 1000Base LH Gigabit Ethernet optical transceiver (SFP MSA). Typical reach of 70 km on 9/125 μ m SMF.	Supported	Supported
SFP-10G-SR - 10 Gigabit optical transceiver (SFP+). Supports multimode fiber over 850 nm wavelength (nominal) with an LC connector. Typical reach of 300 m.	Supported (X-models)	Supported
SFP-10G-ER - 10 Gigabit optical transceiver (SFP+). Supports single mode fiber over 1550 nm wavelength (nominal) with an LC connector. Typical reach of 40 km.	Supported (X-models)	Supported
OS2x60-CBL-60CM - 1/10G direct attached uplink copper cable (60 cm, SFP+).	Supported	Supported
OS2x60-CBL-1M - 1/10G direct attached uplink copper cable (1 m, SFP+).	Supported	Supported
OS2x60-CBL-3M - 1/10G direct attached uplink copper cable (3 m, SFP+)	Supported	Supported
Note: SFP-GIG-T is not supported on SFP+ ports.		

Supported Software Features

The following software features are being introduced in this release, subject to the feature exceptions and problem reports described later in these release notes.

5.1R1 New Feature Summary

Feature	Platform
Power Over Ethernet	OS2260/OS2360
Fast/Perpetual PoE	OS2260/OS2360
VLAN Management	OS2260/OS2360
Spanning Tree	OS2260/OS2360
Source Learning	OS2260/OS2360
Link Aggregation (Static and LACP)	OS2260/OS2360
802.1AB	OS2260/OS2360
IPv4 / Static Routing	OS2260/OS2360
DHCP Relay and Snooping	OS2260/OS2360
IP Multicast Switching	OS2260/OS2360
Quality of Service	OS2260/OS2360
AAA (Authentication, Authorization, and Accounting)	OS2260/OS2360
UNP	OS2260/OS2360
Learned Port Security	OS2260/OS2360
Port Mirroring/Monitoring	OS2260/OS2360
RMON	OS2260/OS2360
Switch Logging	OS2260/OS2360
Health Monitoring	OS2260/OS2360
Chassis Management and Monitoring	OS2260/OS2360
Network Time Protocol	OS2260/OS2360
Session Management	OS2260/OS2360
File Management	OS2260/OS2360
Web Management	OS2260/OS2360
Configuration File Manager	OS2260/OS2360
SNMP	OS2260/OS2360
OmniVista Cirrus	OS2260/OS2360
DNS	OS2260/OS2360
Automatic Remote Configuration Download (RCL)	OS2260/OS2360

Power Over Ethernet

Power over Ethernet (PoE) provides inline power directly from the switch's Ethernet ports. Powered Devices (PDs) such as IP phones, wireless LAN stations, Ethernet hubs, and other access points can be plugged directly into the Ethernet. From these RJ-45 the devices receive both electrical power and data flow.

Fast/Perpetual PoE

Fast PoE can be used to provide PoE power within a few seconds after powering on the chassis. Perpetual PoE allows the switch to provide uninterrupted power to connected power devices (PD) even when the switch is rebooting or reloading, such as on a soft reset.

VLAN Management

VLAN management software handles VLAN configuration and the reporting of VLAN configuration changes to other switch tasks. A VLAN defines a broadcast domain that contains physical ports and can span across multiple switches. All switches contain a default VLAN 1.

Spanning Tree

The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability.

Source Learning

The Source Learning capability of OmniSwitch is responsible for creating, updating, and deleting source and destination MAC Address entries in the MAC Address Table.

Link Aggregation (Static and LACP)

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).

802.1AB

802.1AB is an IEEE standard for exchanging information with neighboring devices and maintaining a database of it. The information is exchanged as an LLDPDU (Link Layer Discovery Protocol Data Unit) in TLV (Time, Length, Value) format.

IPv4 / Static Routing

IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be forwarded. It is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

DHCP Relay and Snooping

Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets contain configuration information for network hosts. DHCP Relay enables forwarding of BOOTP/DHCP packets between networks. This allows routing of DHCP traffic between clients and servers. DHCP Snooping is used to snoop the DHCP packets between the server and clients and dynamically learn the IP address.

IP Multicast Switching

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

Quality of Service

The OmniSwitch QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation or Quality of Service (QoS) may be as simple as allowing/denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

AAA (Authentication, Authorization, and Accounting)

AAA is used for configuring the type of authentication as well as the AAA servers and the local user database on the switch. It can be used to authenticate users into the switch to manage the switch. User information is stored on a RADIUS, TACACS+, LDAP or information may be stored locally in the switch user database. The local may be configured for Authenticated Switch Access. For functional management access, users may be allowed to access specific command families or domains.

UNP (Access Guardian)

Universal Network Profile (UNP) Access Guardian is configured and applied through the framework of the UNP feature. UNP is enabled on switch ports to activate Access Guardian functionality that is used to authenticate and classify users into UNP profiles.

Learned Port Security

Learned Port Security (LPS) provides a mechanism for controlling network device communication on one or more switch ports. Configurable LPS parameters allow the user to restrict source learning on a port to various criteria such as the maximum number of learned source MAC addresses, a specific amount of time in which source MAC addresses are learned, an individual learned source MAC address or a range of learned source MAC addresses.

Port Mirroring/Monitoring

The Port Mirroring feature allows to have all the inbound and outbound traffic of an Ethernet port sent to another port on the switch. When it's enabled the active, or "mirrored," port transmits and receives network traffic normally and the "mirroring" port receives a copy of all transmit and receive traffic to the active port. A probe or network analysis device can be connected to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

The Port Monitoring feature allows you to capture and examine the data traffic to and from a monitored Ethernet port.

RMON

Remote Network Monitoring (RMON) probes can be used to monitor, manage, and compile statistical data about network traffic from designated active ports in a LAN segment without negatively impacting network performance.

Switch Logging

Switch logging allows for the viewing of the history of various switch activities in a text format.

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.

Chassis Management and Monitoring

Chassis Management and Monitoring commands allow you to configure and view hardware-related operations on the switch. Topics include basic system information, as well as Network Interface (NI) module and chassis management.

Network Time Protocol

The Network Time Protocol (NTP) is used to synchronize the time of the switch to another server or reference time source. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

Session Management

Session Management commands are used to monitor and configure operator sessions including FTP, Telnet, HTTP (WebView), console, Secure Shell, and Secure Shell FTP on the switch.

File Management

File management is used to create, move, and delete both files and directories in the OmniSwitch flash directory as well as allow for the changing of command privileges and to monitor the storage usage on the switch.

Web Management

The switch can be configured and monitored using WebView, which is a web-based device management tool. Web Management CLI commands allow you to enable/disable web-based management and configure certain WebView parameters, such as Secure Socket Layer (SSL).

Configuration File Manager

The Configuration Manager feature allows you to configure your switch using an ASCII-based text file. CLI commands may be typed into a text document—referred to as a configuration file—and then uploaded and applied to the switch.

SNMP

Simple Network Management Protocol (SNMP)—Allows communication between SNMP managers and SNMP agents on an IP network. Network administrators use SNMP to monitor network performance and manage network resources. SNMP stations can be configured, traps can be configured, replayed and filtered and the SNMP agent can be configured with multiple levels of security.

OmniVista Cirrus

OmniVista Cirrus is a network management solution to deliver zero touch provisioning using cloud. OmniVista Cirrus solution provides reduced costs, ease of devices provisioning and a unified wired/wireless management from the cloud. The solution also provides an ability to identify each device uniquely and provide a freemium/premium solution based on the user policy. Deployment of OmniVista Cirrus provides easy to use management and monitoring tools in a network and the ability to manage the network using devices ranging from workstations to smart phones.

DNS

A Domain Name System resolver is an internet service that translates host names into IP addresses. Every time a host name is used, a DNS service must resolve the name to an IP address. Multiple DNS servers can be configured and queried until the name is resolved.

Automatic Remote Configuration Download (RCL)

The Automatic Remote Configuration 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.

Unsupported Software Features

Commands for these features may exist on the switch but are currently not supported. Support in an upcoming release is planned.

5.1R1 Unsupported Feature Summary

Feature	Platform
UDLD	OS2260/OS2360
Loopback Detection	OS2260/OS2360
MVRP	OS2260/OS2360
sFlow	OS2260/OS2360
VRRP	OS2260/OS2360
Port Mapping	OS2260/OS2360
IPv6 Multicast Switching	OS2260/OS2360
ERP	OS2260/OS2360
MVRP	OS2260/OS2360
IPv6	OS2260/OS2360
QoS - ACLs	OS2260/OS2360
BYOD - Captive Portal	OS2260/OS2360
Virtual Chassis	OS2260/OS2360

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release.

System / General / Display

CR	Description	Workaround
CRVA-395	UDP ports are not always displayed correctly in WebView.	Use the 'show udp ports' command.
CRVA-563	When using the SFP-GIG-T transceiver, the peer end link sometimes remains up when the port is administratively disabled.	There is no known workaround at this time.
CRVA-564	A fake link-up may be observed when inserting the SFP-GIG-T transceiver without a cable.	There is no known workaround at this time.
CRVA-568	Controlled directed broadcast are not supported.	There is no known workaround at this time.
CRVA-579	<p>During the initial boot or a reboot of an OS2260/2360 the following error may be seen which prevents AOS from being fully initialized resulting in a second reboot.</p> <pre>[ERR] port 0, 0x0 0x100 0x100 [1][dal] dal_mango_port_init Failed! [2][init] !rtkErr: RT_MAPPER(unit)- >_init Failed!! *** [RT_ERR] drivers/net/switch/rtk/dal/dal_mg mt.c:364: In function 'dal_mgmt_initDevice' Error Code: 0xF01E</pre>	There is no known workaround at this time, the switch will recover after the second reboot. This is a software issue which will be fixed in an upcoming release.

Technical Support

Alcatel-Lucent technical support is committed to resolving our customer's technical issues in a timely manner. Customers with inquiries should contact us at:

Region	Phone Number
North America	800-995-2696
Latin America	877-919-9526
European Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: ebg_global_supportcenter@al-enterprise.com

Internet: Customers with service agreements may open cases 24 hours a day via the support web page at: businessportal.al-enterprise.com. Upon opening a case, customers will receive a case number and may review, update, or escalate support cases on-line. Please specify the severity level of the issue per the definitions below. For fastest resolution, please have hardware configuration, module types and version by slot, software version, and configuration file available for each switch.

Severity 1 - Production network is down resulting in critical impact on business—no workaround available.

Severity 2 - Segment or Ring is down or intermittent loss of connectivity across network.

Severity 3 - Network performance is slow or impaired—no loss of connectivity or data.

Severity 4 - Information or assistance on product feature, functionality, configuration, or installation.

Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: **/flash/foss**.

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein.

Appendix A - Specifications

Login Specifications		
	OS2260	OS2360
Login Methods	Telnet, SSH, HTTP, SNMP	
Number of concurrent Telnet sessions	6	
Number of concurrent SSH sessions	8	
Number of concurrent HTTP (WebView) sessions	4	
CMM Specifications		
	OS2260	OS2360
Compact Flash Memory	512MB	512MB
RAM Memory	512MB	1GB
Maximum Length of File Names (in Characters)	255	
Maximum Length of Directory Names (in Characters)	255	
Maximum Length of System Name (in Characters)	32	
User Database Specifications		
	OS2260	OS2360
Maximum number of alphanumeric characters in a username	63	
Maximum number of alphanumeric characters in a user password	30	
Maximum number of local user accounts	50	
NTP Specifications		
	OS2260	OS2360
Maximum number of NTP servers per client	12	
Maximum number of associations	512	
Source Learning Specifications		
	OS2260	OS2360
Maximum number of learned MAC addresses	8K	16K
VLAN Specifications		
	OS2260	OS2360
Maximum VLANs per Switch	64	1024
Spanning Tree Specifications		

	OS2260	OS2360
Maximum VLAN Spanning Tree instances	100	100
Maximum VLAN Spanning Tree instances (MSTI)	4	8
Static / Dynamic Link Aggregation Specifications		
	OS2260	OS2360
Maximum number of link aggregation groups	8	16
Maximum number of ports per link aggregate group	4	8
IPv4 Specifications		
	OS2260	OS2360
Maximum router interfaces per system	8	24
Maximum router interfaces per VLAN	8	8
Maximum Static Routes	2	32
UNP Specifications		
	OS2260	OS2360
Number of 802.1x or UNP users per chassis	128	
Learned Port Security		
	OS2260	OS2360
Minimum number of learned MAC addresses allowed per LPS port	1	
Maximum number of learned MAC addresses allowed per LPS port	1000	
Maximum number of filtered MAC addresses allowed per LPS port	100	
Maximum number of configurable MAC address ranges per LPS port	1	
Port Mirroring / Monitoring		
	OS2260	OS2360
Mirroring Sessions Supported	3	
Monitoring Sessions Supported	1	