Release Notes

OmniSwitch 6900

Release 7.3.3.R01

These release notes accompany release 7.3.3.R01 software which is supported on the OmniSwitch 6900 platforms. 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.

NOTE: Please refer to the 7.3.3.R01 Prerequisite section for important release specific information prior to upgrading including specific build information for hardware support.

NOTE: The OmniSwitch 10K is not supported in AOS Release 7.3.3.R01.

Contents

Related Documentation

These release notes should be used in conjunction with OmniSwitch AOS Release 7 User Guides. The following are the titles and descriptions of the user manuals that apply to this release. User manuals can be downloaded at: http://enterprise.alcatel-lucent.com/?dept=UserGuides&page=Portal

> **Note**: The latest release of the OmniSwitch AOS Release 7 user guides cover AOS Release 7.3.2.R01 for the OS10K and AOS Release 7.3.3.R01 for the OS6900.

OmniSwitch 6900 Series Getting Started Guide
Describes the hardware and software procedures for getting an OmniSwitch up and running.

OmniSwitch 6900 Series Hardware User Guide
Complete technical specifications and procedures for all OmniSwitch Series chassis, power supplies, and fans

OmniSwitch AOS Release 7 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.

OmniSwitch AOS Release 7 Network Configuration Guide
Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethe rnet and VLAN configuration), Layer 3 information (routing protocols), security options (Authen¬ticated Switch Access (ASA)), Quality of Service (QoS), link aggregation.

OmniSwitch AOS Release 7 Switch Management Guide
Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, software rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

OmniSwitch AOS Release 7 Advanced Routing Configuration Guide
Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM), BGP, OSPF, and OSPFv3.

OmniSwitch AOS Release 7 Data Center Switching Guide
Includes and introduction to the OmniSwitch data center switching architecture as well as network configuration procedures and descriptive information on all the software features and protocols that support this architecture. Chapters cover Shortest Path Bridging MAC (SPBM), Data Center Bridging (DCB) protocols, Virtual Network Profile (vNP), and the Edge Virtual Bridging (EVB) protocol.

OmniSwitch AOS Release 7 Transceivers Guide
Includes SFP, SFP+, and QSFP transceiver specifications and product compatibility information.

Technical Tips, Field Notices
Contracted customers can visit our customer service website at: service.esd.alcatel-lucent.com.

System Requirements

Memory Requirements

OmniSwitch 6900 Series Release 7.3.3.R01 requires 2GB (6900X models) / 4GB (6900T models) of SDRAM and 2GB flash memory. This is the standard configuration shipped.

Configuration files and the compressed software images—including web management software (WebView) images—are stored in the flash memory.

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 the 7.3.3.R01 AOS software available from Service & Support.

The newly supported XNI-U12E in 7.3.3.R01 requires a minimum CMM FPGA version as listed in the table below.

If upgrading from 7.2.1.R02 or higher and if XNI-U12E support is not required, the Uboot and FPGA should already be at the correct versions listed below. If upgrading from a release prior to 7.2.1.R02 upgrading the Uboot and FPGA according to the table below may be required.

A separate file containing the Uboot and FPGA upgrade files is available from Service & Support.

Please refer to the Upgrade Instructions section at the end of these Release Notes for step-by-step instructions on upgrading your switch to support 7.3.3.R01.

OmniSwitch 6900-X20/X40 – AOS Release 7.3.3.384.R01(GA)

Hardware	Uboot	FPGA
CMM (if XNI-U12E support is not needed)	7.2.1.266.R02	1.3.0/1.2.0
CMM (if XNI-U12E support is needed)	7.2.1.266.R02	1.3.0/2.2.0[1]
All Expansion Modules	N/A	N/A[2]

1. FPGA 1.3.0/2.2.0 is required to support the XNI-U12E
2. Shipped from factory with correct version, no upgrade is available or required.

OmniSwitch 6900-T20/T40 – AOS Release 7.3.3.384.R01(GA)

Hardware	Uboot	FPGA
CMM (if XNI-U12E support is not needed)	7.3.2.134.R01[2]	1.4.0/0.0.0[2]
CMM (if XNI-U12E support is needed)	7.3.2.134.R01[2]	1.6.0/0.0.0[1]
All Expansion Modules	N/A	N/A[2]

1. FPGA 1.6.0 is required to support the XNI-U12E
2. Shipped from factory with correct version, no upgrade is available or required.

Use the '**show hardware-info**' command to view current versions as seen below:

```
-> show hardware-info
CPU Manufacture                 : Freescale Semiconductor
CPU Model                       : MPC 8572
Compact Flash Manufacturer      : CF 2GB
Compact Flash size              : 2097930240 bytes
RAM Manufacturer                : Other
RAM size                        : 1974828 kB
FPGA 1 version                  : 1.3.0
FPGA 2 version                  : 2.2.0
U-Boot Version                  : 7.2.1.266.R02
Power Supplies Present          : 1
NIs Present                     : 1,2,3
```

AOS Release 7.3.3.R01 Prerequisites

Prior to upgrading to AOS Release 7.3.3.R01 please note the following:

- The OmniSwitch 10K is not supported in AOS Release 7.3.3.R01.
- When upgrading a virtual chassis from an earlier AOS release to AOS release 7.3.3.R01 please refer to the Virtual Chassis Upgrade Instructions for specific steps to follow to help minimize any network disruption.

New Hardware Support in 7.3.3.R01

OS-XNI-U12E

Twelve port 10-Gigabit SFP+ Ethernet or 2/4/8 Gigabit Fibre Channel (FC) expansion module for the OS6900 series of swicthes. Data center license is required for FC/FCoE operation. **Note**: In a virtual chassis environment VFLs are supported on this module but not with the FC transceiver.

SFP-FC-SR Transceiver

SFP-FC-SR triple-speed Fibre Channel (FC) optical transceiver. Supports multimode fiber 850nm wavelength with an LC connector. Supports auto-sensing 8GFC, 4GFC and 2GFC. Please refer to the Service & Support site for a list of tested FC vendors. This transceiver is only supported on the OS-XNI-U12E but cannot be used to configure VFLs in a virtual chassis environment.

New Software Features and Enhancements

The following software features are being introduced with the 7.3.3.R01 release, subject to the feature exceptions and problem reports described later in these release notes:

Features listed as 'Base' are included as part of the base software and do not require any license installation. Features listed as 'Advanced' or "Data Center" require the installation of a license.

7.3.3.R01 New Feature/Enhancements Summary

Feature	Platform	License
Data Center Feature Support		
- FCoE/FC Gateway	6900	Data Center
- CEE DCBX Version 1.01	6900	Data Center
Layer 3 Feature Support		
- ISIS – IPv4/IPv6	6900	Advanced
- BGP 4-Octet ASN	6900	Advanced
Management		
- Virtual Chassis mesh of 6 chassis with ISSU support	6900	Advanced
Early Availability Feature Support		
- OpenFlow Agent versions 1.3.1 and 1.0 (Normal and Hybrid modes)	6900	Base
- Internal IPv4/IPv6 DHCP Server	6900	Base
- OmniSwitch Networking Plug-in for OpenStack	6900	Base
- M-ISIS	6900	Advanced

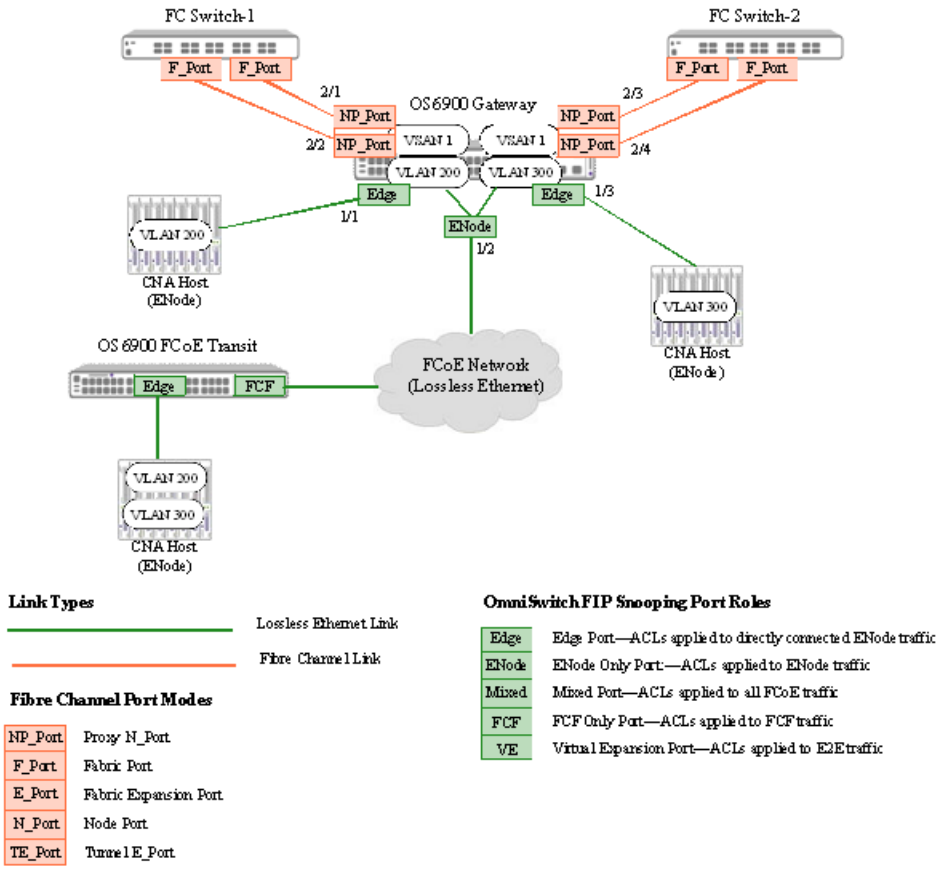
Data Center Feature Descriptions

FCoE/FC Gateway

The Alcatel-Lucent OmniSwitch provides Fibre Channel over Ethernet (FCoE) convergence solutions that facilitate the expansion of a Fibre Chanel (FC) storage area network (SAN) across an existing multi-hop Ethernet infrastructure. FCoE convergence features supported include the following:

- **FCoE transit switch—**The OmniSwitch supports the FCoE technology used to tunnel FC frames encapsulated within Ethernet MAC frames. To provide the necessary FCoE transit switch functionality, the OmniSwitch supports FCoE Initialization Protocol (FIP) snooping and Data Center Bridging (DCB) protocols for lossless Ethernet. A transit switch is basically a Layer 2 DCB switch that bridges encapsulated FCoE traffic over the Ethernet fabric between FCoE end devices.
- **FCoE gateway switch**—The OmniSwitch serves as an FCoE forwarder to connect FCoE nodes to FC switches, connect FC nodes to an FCoE forwarder, and connect native FC fabrics across an FCoE network. To provide the necessary FCoE gateway functionality, the OmniSwitch supports the following operational modes:
    - N_Port proxy operation using N_Port ID Virtualization (NPIV) to aggregate FCoE Node (ENode) logins over a single OmniSwitch FC port that is connected to an FC switch.
    - F_Port proxy operation to connect FC nodes to an FCoE forwarder or another gateway switch through an FCoE network.
    - E_Port proxy operation to provide a transparent point-to-point FC link between native E_Ports. This allows inter-switch link (ISL) tunneling between FC fabrics over an FCoE network.

An OmniSwitch FCoE transit switch can connect to an OmniSwitch FCoE gateway to access the necessary gateway services needed to transport FCoE traffic to or from the FC SAN. An OmniSwitch FCoE gateway runs FIP snooping on the 10G Ethernet FCoE ports that connect to an FCoE network. On the same switch, FC ports connect to native FC switches or nodes. Traffic is transmitted between the FCoE network and the FC SAN through the gateway switch.



OmniSwitch FCoE Example Diagram

Converged Enhanced Ethernet (CEE) DCBX Version 1.01

The OmniSwitch implementation of Data Center Bridging has been enhanced to support CEE DCBX version 1.0.1. The OmniSwitch now supports two following two versions of the DCB Exchange protocol (DCBX):

- IEEE 802.1Qaz DCBX
- Converged Enhanced Ethernet (CEE) DCBX version 1.0.1

By default, a DCB port will use the IEEE 802.1Qaz version of DCBX until the port detects the peer switch is using the CEE version. When this occurs, the switch will automatically stop 802.1Qaz DCBX on the port and start using CEE DCBX. Please contact Service & Support for a list of tested devices.

Layer 3 Feature Descriptions

ISIS IPv4/IPv6

Intermediate System-to-Intermediate System (IS-IS) is an International Organization for Standardization (ISO) dynamic routing specification. IS-IS is a shortest path first (SPF), or link state protocol. Also considered an interior gateway protocol (IGP), IS-IS distributes routing information between routers in a single Autonomous System (AS) in IP environments. IS-IS chooses the least-cost path as the best path. It is suitable for complex networks with a large number of routers by providing faster convergence where multiple. This release supports multi-VRF aware IS-IS for IPv4.

BGP 4-Octet Autonomous System Number (ASN)

This feature enhancement provides the following:

- BGP Support for 4-octet (32 bit) ASN for BGP neighbor interoperability and path attribute interoperability as per RFC 6793.
- Capabilities Advertisement with BGP-4 - The advertisement and discovery of 4-octet ASN capability by using the BGP CAPABILITY FIELDS.
- Support for two new optional transitive attributes AS4_PATH and AS4_AGGREGATE. These attribute are used while interacting with NEW BGP speaker and OLD BGP speaker.
- To establish a neighbor relationship between non-mappable BGP 4-octet ASNs with BGP 2-octet ASNs the reserved 2-octet ASN AS_TRANS 23456 is used.
- Extended Community will be used for non-mappable 4-octet ASNs with BGP 2-octet ASNs.
- The 4-octet ASN is represented in one of three ways:
    - asplain (simple decimal notation)
    - asdot+ (two 16-bit values as low-order and high-order)
    - asdot (a mixture of asplain and asdot+).

Management Feature Descriptions

Virtual Chassis Mesh of 6 Chassis

Virtual Chassis is a group of chassis managed through a single management IP address. It provides both node level and link level redundancy for layer 2 and layer 3 services and protocols acting as a single device. The use of Virtual Chassis provides node level redundancy without the need to use redundancy protocols such as STP and VRRP between the edge and the aggregation/core layer.

The following are some key points regarding Virtual Chassis configuration:

- A Virtual Chassis can now be comprised of a mesh of up to 6 OS6900 chassis
- A Virtual Chassis will consist of one master and up to 5 slave chassis. The election of a Master chassis can automatically be determined based on various chassis attributes.
- Running in Virtual Chassis mode will cause a change to the CLI requiring a chassis identifier to be used and displayed for the *slot/port* commands. (i.e. chassis/slot/port)
- A virtual chassis provides a single management IP address for a group of chassis that are acting as a single bridge or router.
- A Virtual Chassis can leverage an ISSU upgrade to help minimize network impact.
- The switches in the Virtual Chassis are created by inter-connecting them via standard single or aggregated 10G or 40G ports. (10G and 40G ports cannot be mixed within the same VFL).
- Each chassis participating in the Virtual Chassis must have a valid Advanced license to join the VC.

In-Service Software Upgrade (ISSU)

The In-Service Software Upgrade (ISSU) feature is used to upgrade the images running on an OmniSwitch 6900 VC with minimal disruption to data traffic. The images can be upgraded on a fully synchronized, certified, and redundant system running an ISSU capable build.

Note: Upgrading from an virtual chassis running an earlier AOS release to AOS release 7.3.3.R01 is supported using a modified ISSU "staggered upgrade" that will minimize data impact. Please refer to the Virtual Chassis Upgrade Instructions. Please contact Service & Support for ISSU guidelines.

Early Availability Feature Descriptions

The following software features are being introduced with the 7.3.3.R01 release as limited or early availability features. Some CLI and feature functionality may be available, however, they have not gone through the complete Alcatel-Lucent qualification process. For additional information please contact the Product Line Manager.

OpenFlow Agent

OpenFlow is a communications interface defined between the control and forwarding layers that is used in a Software Defined Network (SDN). OpenFlow separates the control plane and the data plane in the switch. Traditionally, switches and routers have made decisions on where packets should travel based on rules local to the device. With OpenFlow, only the data plane exists on the switch itself, and all control decisions are communicated to the switch from a central Controller. If the device receives a packet for which it has no flow information, it sends the packet to the Controller for inspection, and the Controller determines where that packet should be sent based on QoS-type rules configured by the user (drop the packets to create a firewall, pass the packets to a specific port to perform load balancing, prioritize packets, etc).

The OS6900 can operate in AOS or OpenFlow mode, including a modified OpenFlow mode known as Hybrid mode. AOS will designate the ports managed/controlled by AOS or by OpenFlow on a per-port basis. By default, ports are managed/controlled by AOS.

OpenFlow 1.0 and 1.3.1 are supported on OS6900 switches in standalone mode running AOS 7.3.3.R01. When the OS6900 is part of a Virtual Chassis OpenFlow commands are disabled.

The following are the key components available on an OS6900 for OpenFlow support.

- **OpenFlow Logical Switch** - An OpenFlow logical switch consists of a portion of the switch's resources that are managed by an OpenFlow Controller (or set of Controllers) via the OpenFlow Agent. Up to 3 logical switches can be configured on an OS6900, with each switch supporting up to three controllers. A logical switch has a VLAN, physical ports, and/or link aggregate ports assigned to it. All packets received on these ports are forwarded directly to the Openflow agent. Spanning tree and source learning do not operate on OpenFlow assigned ports.

- **OpenFlow Normal Mode** - In Normal Mode, the logical switch operates as per the OpenFlow standards.

- **OpenFlow Hybrid Mode** - In Hybrid mode, logical switch acts as an interface through which the Controller may insert flows. These flows are treated as QoS policy entries and offer the same functionality. A Hybrid mode logical switch operates on all ports, link aggregates, and VLANs not assigned to other OpenFlow logical switches. Only one logical switch can be active in Hybrid mode.

Internal IPv4/IPv6 DHCP Server
The OmniSwitch now supports an internal DHCP Server compliant with RFC 2131 and RFC 3315 based on Vital QIP 8.0 release. This feature can be used to provide IP addresses for small offices, management network, or local phone services. The following files are used to configure the internal DHCP server setting on the OmniSwitch:

- IPv4 Policy Files- dhcpd.conf, dhcpd.pcy
- IPv6 Configuration Files – dhcpd6.conf, dhcpd6.pcy

DHCP Policy files - The dhcpd(v6).pcy files initialize the global attributes for the DHCP server.

DHCP Configuration files - The dhcpd(v6).conf files are used to configure specific DHCP server settings on the switch such as the following:

- MAC pool allowed (for DHCPv4)
- MAC pool excluded (for DHCPv4)
- Subnet pools
- Dynamic scopes
- Static scopes
- IP range, mask, DNS, Default router, Net Bios configurations for DHCPv4.
- User class specific configs.
- Vendor class specific configs.
- DUID Pool (for DHCPv6 only).
- Excluded DUID Pool (for DHCPv6 only)
- Manual DUID mapping (for DHCPv6 only).
- Other options that need to be sent to the client.

M-ISIS
Multi-topology (M-ISIS) support is necessary in IS-IS to support network domains in which non-dual stack IS-IS routers exist. The default protocol behavior of IS-IS is to construct shortest paths through the network using the routers' MAC addresses with no regard to the different IP address families supported. This behavior may result in black-holed routing when there are some IPv4-only or IPv6-only routers in an IS-IS routing domain, instead of all dual-stack routers. M-ISIS mechanism runs multiple, independent IP topologies within a single IS-IS network domain, using separate topology-specific SPF computation and multiple Routing Information Bases (RIBs). M-ISIS is advised in networks containing ISIS enabled routers with a combination of IPv4 and IPv6 capabilities.

OmniSwitch Networking Plug-in for OpenStack – Release 1.1
The OmniSwitch Networking Plug-in (OSNP) for OpenStack networking offers infrastructure services for OpenStack logical networks by coordinating the orchestration of Alcatel-Lucent OmniSwitches as the underlying physical network. When used in conjunction with the OpenVSwitch plug-in, end-to-end multi-tenant network provisioning through OpenStack Networking (Quantum/Nuetron) is achieved.

The plug-in is intended to be installed in existing OpenStack Grizzly environments to configure the underlying physical network for its cloud networking operations.

The following HW platforms with their respective AOS SW releases are supported.

- OS6900 and OS10K with AOS 732-R01 SW release and above
- OS68XX and OS9000E with AOS 645-R02 SW release and above

SNMP Traps

The following table provides a list of SNMP traps managed by the switch.

No.	Trap Name	Platforms	Description
0	coldStart	OS6900	The SNMP agent in the switch is reinitiating and itsk configuration may have been altered.
1	warmStart	OS6900	The SNMP agent in the switch is reinitiating itself and its configuration is unaltered.
2	linkDown	OS6900	The SNMP agent in the switch recognizes a failure in one of the communications links configured for the switch.
3	linkUp	OS6900	The SNMP agent in the switch recognizes that one of the communications links configured for the switch has come up.
4	authenticationFailure	S6900	The SNMP agent in the switch has received a protocol message that is not properly authenticated.
5	entConfigChange	OS6900	An entConfigChange notification is generated when a conceptual row is created, modified, or deleted in one of the entity tables.
6	policyEventNotification	OS6900	The switch notifies the NMS when a significant event happens that involves the policy manager.
7	chassisTrapsStr	OS6900	A software trouble report (STR) was sent by an application encountering a problem during its execution.
8	chassisTrapsAlert	OS6900	A notification that some change has occurred in the chassis.
9	chassisTrapsStateChange	OS6900	An NI status change was detected.
10	chassisTrapsMacOverlap	OS6900	A MAC range overlap was found in the backplane eeprom.
11	vrrpTrapNewMaster	OS6900	The SNMP agent has transferred from the backup state to the master state.
12	vrrpTrapAuthFailure	OS6900	This trap is not supported.
13	healthMonModuleTrap	OS6900	Indicates a module-level threshold was crossed.
14	healthMonPortTrap	OS6900	Indicates a port-level threshold was crossed.
15	healthMonCmmTrap	OS6900	This trap is sent when the Module-level rising/falling threshold is crossed.

No.	Trap Name	Platforms	Description
16	bgpEstablished	OS6900	The BGP routing protocol has entered the established state.
17	bgpBackwardTransition	OS6900	This trap is generated when the BGP router port has moved from a more active to a less active state.
18	esmDrvTrapDropsLink	OS6900	This trap is sent when the Ethernet code drops the link because of excessive errors.
19	portViolationTrap	OS6900	This trap is sent when a port violation occurs. The port violation trap will indicate the source of the violation and the reason for the violation.
20	dvmrpNeighborLoss	OS6900	A 2-way adjacency relationship with a neighbor has been lost. This trap is generated when the neighbor state changes from “active” to “one-way,” “ignoring” or “down.” The trap is sent only when the switch has no other neighbors on the same interface with a lower IP address than itself.
21	dvmrpNeighborNotPruning	OS6900	A non-pruning neighbor has been detected in an implementation-dependent manner. This trap is generated at most once per generation ID of the neighbor. For example, it should be generated at the time a neighbor is first heard from if the prune bit is not set. It should also be generated if the local system has the ability to tell that a neighbor which sets the prune bit is not pruning any branches over an extended period of time. The trap should be generated if the router has no other neighbors on the same interface with a lower IP address than itself.
22	risingAlarm	OS6900	An Ethernet statistical variable has exceeded its rising threshold. The variable’s rising threshold and whether it will issue an SNMP trap for this condition are configured by an NMS station running RMON.
23	fallingAlarm	OS6900	An Ethernet statistical variable has dipped below its falling threshold. The variable’s falling threshold and whether it will issue an SNMP trap for this condition are configured by an NMS station running RMON.
24	stpNewRoot	OS6900	Sent by a bridge that became the new root of the spanning tree.

No.	Trap Name	Platforms	Description
25	stpRootPortChange	OS6900	A root port has changed for a spanning tree bridge. The root port is the port that offers the lowest cost path from this bridge to the root bridge.
26	mirrorConfigError	OS6900	This trap is sent when any NI fails to configure mirroring. Due to this error, port mirroring session will be terminated.
27	mirrorUnlikeNi	OS6900	The mirroring configuration is deleted due to the swapping of different NI board type. The Port Mirroring session which was active on a slot cannot continue with the insertion of different NI type in the same slot.
28	slbTrapOperStatus	OS6900	A change occurred in the operational status of the server load balancing entity.
29	sessionAuthenticationTrap	OS6900	An authentication failure trap is sent each time a user authentication is refused.
30	trapAbsorptionTrap	OS6900	The absorption trap is sent when a trap has been absorbed at least once.
31	alaDoSTrap	OS6900	Indicates that the sending agent has received a Denial of Service (DoS) attack.
32	ospfNbrStateChange	OS6900	Indicates a state change of the neighbor relationship.
33	ospfVirtNbrStateChange	OS6900	Indicates a state change of the virtual neighbor relationship.
34	lnkaggAggUp	OS6900	Indicates the link aggregate is active. This trap is sent when any one port of the link aggregate group goes into the attached state.
35	lnkaggAggDown	OS6900	Indicates the link aggregate is not active. This trap is sent when all ports of the link aggregate group are no longer in the attached state.
36	lnkaggPortJoin	OS6900	This trap is sent when any given port of the link aggregate group goes to the attached state.
37	lnkaggPortLeave	OS6900	This trap is sent when any given port detaches from the link aggregate group.
38	lnkaggPortRemove	OS6900	This trap is sent when any given port of the link aggregate group is removed due to an invalid configura tion.
39	monitorFileWritten	OS6900	This trap is sent when the amount of data requested has been written by the port

No.	Trap Name	Platforms	Description
			monitoring instance.
40	alaVrrp3TrapProtoError	OS6900	Indicates that a TTL, checksum, or version error was encountered upon receipt of a VRRP advertisement.
41	alaVrrp3TrapNewMaster	OS6900	The SNMP agent has transferred from the backup state to the master state.
42	chassisTrapsPossibleDuplicateMac	OS6900	The old PRIMARY element cannot be detected in the stack. There is a possiblity of a duplicate MAC address in the network
43	lldpRemTablesChange	OS6900	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes.
44	pimNeighborLoss	OS6900	A pimNeighborLoss notification signifies the loss of an adjacency with a neighbor.
45	pimInvalidRegister	OS6900	An pimInvalidRegister notification signifies that an invalid PIM Register message was received by this device
46	pimInvalidJoinPrune	OS6900	A pimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device.
47	pimRPMappingChange	OS6900	An pimRPMappingChange notification signifies a change to the active RP mapping on this device.
48	pimInterfaceElection	OS6900	An pimInterfaceElection notification signifies that a new DR or DR has been elected on a network.
49	pimBsrElectedBSRLostElection	OS6900	This trap is sent when the current E-BSR loses an election to a new Candidate-BSR.
50	pimBsrCandidateBSRWinElection	OS6900	This trap is sent when a C-BSR wins a BSR Election.
51	lpsViolationTrap	OS6900	A Learned Port Security (LPS) violation has occurred.
52	lpsPortUpAfterLearningWindowExpiredT	OS6900	When an LPS port joins or is enabled after the Learning Window is expired, the MAC address learning on the port will be disabled, and this trap is generated as a notification.
53	lpsLearnMac	OS6900	Generated when an LPS port learns a bridged MAC.
54	gvrpVlanLimitReachedEvent	OS6900	Generated when the number of vlans learned dynamically by GVRP has reached

No.	Trap Name	Platforms	Description
			a configured limit.
55	alaNetSecPortTrapAnomaly	OS6900	Trap for an anomaly detected on a port.
56	alaNetSecPortTrapQuarantine	OS6900	Trap for an anomalous port quarantine.
57	ifMauJabberTrap	OS6900	This trap is sent whenever a managed interface MAU enters the jabber state.
58	udldStateChange	OS6900	Generated when the state of the UDLD protocol changes.
59	ndpMaxLimitReached	OS6900	This IPv6 Trap is sent when the hardware table has reached the maximum number of entries supported.
60	ripRouteMaxLimitReached	OS6900	This trap is sent when the RIP database reaches the supported maximum number of entries. When the maximum number is reached, RIP discards any new updates.
61	ripngRouteMaxLimitReached	OS6900	This trap is sent when the RIPng database reaches the supported maximum number of entries. When the maximum number is reached, RIPng discards any new updates.
62	alaErpRingStateChanged	OS6900	This trap is sent when the ERP Ring State has changed from “Idle” to “Protection”.
63	alaErpRingMultipleRpl	OS6900	This trap is sent when multiple RPLs are detected in the Ring.
64	alaErpRingRemoved	OS6900	This trap is sent when the Ring is removed dynamically.
65	ntpMaxAssociation	OS6900	This trap is generated when the maximum number of peer and client associations configured for the switch is exceeded.
66	ddmTemperatureThresholdViolated	OS6900	This trap is sent when an SFP/ XFP/SFP+ temperature has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/ XFP/SFP+ temperature.
67	ddmVoltageThresholdViolated	OS6900	This trap is sent when SFP/XFP/ SFP+ supply voltage has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/XFP/SFP+ supply voltage.
68	ddmCurrentThresholdViolated	OS6900	This trap is sent when if an SFP/ XFP/SFP+ Tx bias current has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex.

No.	Trap Name	Platforms	Description
			It also provides the current realtime value of SFP/XFP/SFP+ Tx bias current.
69	ddmTxPowerThresholdViolated	OS6900	This trap is sent when an SFP/ XFP/SFP+ Tx output power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/XFP/SFP+ Tx output power.
70	ddmRxPowerThresholdViolated	OS6900	This trap is sent when an SFP/ XFP/SFP+ Rx optical power has crossed any threshold or reverted from previous threshold violation for a port represented by ifIndex. It also provides the current realtime value of SFP/XFP/SFP+ Rx optical power.
71	webMgtServerErrorTrap	OS6900	This trap is sent to management station(s) when the Web Management server goes into error state after becoming unreachable twice within a minute.
72	multiChassisIpcVlanUp	OS6900	This trap is sent to indicate the operational status for the multi-chassis communication VLAN is up.
73	multiChassisIpcVlanDown	OS6900	This trap is sent to indicate the operational status for the multi-chassis communication VLAN is down.
74	multiChassisMisconfigurationFailure	OS6900	This trap is sent to indicate a mis-configuration due to Chassis Id or IPC VLAN.
75	multiChassisHelloIntervalConsisFailure	OS6900	This trap is sent to indicate a hello interval consistency failure.
76	multiChassisStpModeConsisFailure	OS6900	This trap is sent to indicate an STP mode consistency failure.
77	multiChassisStpPathCostModeConsisFailure	OS6900	This trap is sent to indicate an STP path cost mode consistency failure.
78	multiChassisVflinkStatusConsisFailure	OS6900	This trap is sent to indicate a VFLink status consistency failure.
79	multiChassisStpBlockingStatus	OS6900	This trap is sent to indicate the STP status for some VLANs on the VFLink is in blocking state.
80	multiChassisLoopDetected	OS6900	This trap is sent to indicate a loop has been detected.
81	multiChassisHelloTimeout	OS6900	This trap is sent to indicate the hello timeout has occurred.
82	multiChassisVflinkDown	OS6900	This trap is sent to indicate the VFLink is

No.	Trap Name	Platforms	Description
			down.
83	multiChassisVFLMemberJoinFailure	OS6900	This trap is sent to indicate a port configured as virtual-fabric member is unable to join the virtual-fabric link.
84	alaDHLVlanMoveTrap	OS6900	When linkA or linkB goes down or comes up and both ports are are part of some vlan-map, this trap is sent to the Management Entity, with the DHL port information.
85	alaDhcpClientAddressAddTrap	OS6900	This trap is sent when a new IP address is assigned to DHCP Cli-ent interface.
86	alaDhcpClientAddressExpiryTrap	OS6900	This trap is sent when the lease time expires or when the DHCP client is not able to renew/rebind an IP address.
87	alaDhcpClientAddressModifyTrap	OS6900	This trap is sent when the DHCP client is unable to obtain the existing IP address and a new IP address is assigned to the DHCP client
88	vRtrIsisDatabaseOverload	OS6900	This notification is generated when the system enters or leaves the overload state.
89	vRtrIsisManualAddressDrops	OS6900	Generated when one of the manual area addresses assigned to this system is ignored when computing routes.
90	vRtrIsisCorruptedLSPDetected	OS6900	This notification is generated when an LSP that was stored in memory has become corrupted.
91	vRtrIsisMaxSeqExceedAttempt	OS6900	Generated when the sequence number on an LSP wraps the 32 bit sequence counter
92	vRtrIsisIDLenMismatch	OS6900	A notification sent when a PDU is received with a different value of the System ID Length.
93	vRtrIsisMaxAreaAddrsMismatch	OS6900	A notification sent when a PDU is received with a different value of the Maximum Area Addresses.
94	vRtrIsisOwnLSPPurge	OS6900	A notification sent when a PDU is received with an OmniSwitch systemID and zero age
95	vRtrIsisSequenceNumberSkip	OS6900	When an LSP is received without a System ID and different contents.
96	vRtrIsisAutTypeFail	OS6900	A notification sent when a PDU is received with the wrong authentication type field.
97	vRtrIsisAuthFail	OS6900	A notification sent when a PDU is received with an incorrent authentication information field.

No.	Trap Name	Platforms	Description
98	vRtrIsisVersionSkew	OS6900	A notification sent when a a Hello PDU is received from an IS running a different version of the protocol.
99	vRtrIsisAreaMismatch	OS6900	A notification sent when a Hello PDU is received from an IS which does not share any area address.
100	vRtrIsisRejectedAdjacency	OS6900	A notification sent when a Hello PDU is received from an IS, but does not establish an adjacency due to a lack of resources.
101	vRtrIsisLSPTooLargeToPropagate	OS6900	A notification sent when an attempt to propagate an LSP which is larger than the dataLinkBlockSize for a circuit.
102	vRtrIsisOrigLSPBufSizeMismatch	OS6900	A notification sent when a Level 1 LSP or Level 2 LSP is received which is larger than the local value for the originating L1LSP BufferSize or originating L2LSPBufferSize respectively. Also when a Level 1 LSP or Level2 LSP is received containing the originating LSPBufferSize option and the value in the PDU option field does not match the local value for originating L1LSP BufferSize or originatingL2LSP BufferSize respectively.
103	vRtrIsisProtoSuppMismatch	OS6900	A notification sent when a non-pseudonode segment 0 LSP is received that has no matching protocols supported.
104	vRtrIsisAdjacencyChange	OS6900	A notification sent when an adjacency changes state, entering or leaving state up. The first 6 bytes of the vRtrIsisTrapLSPID are the SystemID of the adjacent IS.
105	vRtrIsisCircIdExhausted	OS6900	A notification sent when ISIS cannot be started on a LAN interface because a unique circId could not be assigned due to the exhaustion of the circId space.
106	vRtrIsisAdjRestartStatusChange	OS6900	A notification sent when an adjancency's graceful restart status changes.
107	mvrpVlanLimitReachedEvent	OS6900	This trap is sent when the num-ber of VLANs learned dynamically by MVRP reaches the configured limit.
108	alaHAVlanClusterPeerMismatch	OS6900	The trap is sent when parameteras configured for this cluster ID (Level 1 check) does not match accross the MCLAG peers.

No.	Trap Name	Platforms	Description
109	alaHAVlanMCPeerMismatch	OS6900	The trap is sent when when the cluster parameters are matching on the peers, but MCLAG is not configured or clusters are not in operational state.
110	alaHAVlanDynamicMAC	OS6900	The trap is sent when the dynamic MAC is learned on non-server cluster port
111	unpMcLagMacIgnored	OS6900	This trap is sent when a MAC/User is dropped because the VLAN does not exist or UNP is not enabled on the MCLAG.
112	unpMcLagConfigInconsistency	OS6900	This trap is sent when a configuration becomes “Out of Sync".
113	multiChassisGroupConsisFailure	OS6900	This trap is sent when there is an inconsistency between local and peer chassis group.
114	multiChassisTypeConsisFailure	OS6900	This trap is sent when there is an inconsistency between local and peer chassis group.
115	alaPimNonBidirHello	OS6900	This trap is sent when a bidir-capable router has received a PIM hello from a non-bidir-capable router. It is generated whenever the counter alaPimsmNon-BidirHelloMsgsRcvd is incremented, subject to the rate limit specified by alaPimsmNonBidirHelloNotificationPeriod.
116	dot1agCfmFaultAlarm	OS6900	This trap is sent when a MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.
117	alaSaaIPIterationCompleteTrap	OS6900	This trap is sent when an IP SAA iteration is completed.
118	alaSaaEthIterationCompleteTrap	OS6900	This trap is sent when when an eth-LB or Eth-DMM SAA iteration is completed.
119	alaSaaMacIterationCompleteTrap	OS6900	This trap is sent when a MAC iteration is complete.
120	virtualChassisStatusChange	OS6900	This trap is sent when a chassis status change is detected.
121	virtualChassisRoleChange	OS6900	This trap is sent when a chassis role change is detected.
122	virtualChassisVflStatusChange	OS6900	This trap is sent when s vflink status change is detected.

No.	Trap Name	Platforms	Description
123	virtualChassisVflMemberPortStatusCh	OS6900	This trap is sent when a vflink member port has a change of status.
124	virtualChassisVflMemberPortJoinFail	OS6900	This trap is sent when a port configured as virtual-fabric member is unable to join the virtual-fabric link.
125	lldpRemTablesChange	OS6900	This trap is sent when the value of lldpStatsRemTablelastChange Time changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.
126	vRtrLdpInstanceStateChange	OS6900	This trap is sent when the LDP module changes state either administratively or operationally.
127	evbFailedCdcpTlvTrap	OS6900	This trap is sent when bridge receives a CDCP packet with: - Wrong TLV type, or - Wrong OUI, or - Role is set to Bridge, or - Wrong default channel(scid), or - Incorrect channel number(scid).
128	evbFailedEvbTlvTrap	OS6900	This trap is sent when bridge receives an EVBTLV packet with: - Wrong TLV type. or - Incorrect TLV length, or - Wrong OUI.
129	evbUnknownVsiManagerTrap	N/A	This trap is sent when bridge receives a VDP packet with: - Unknown Manager ID type, or - Wrong Manager ID length.
130	evbVdpAssocTlvTrap	N/A	This trap is sent when bridge receives an ASSOC TLV in a VDP packet with: - Null VID found and number of entry field is not 1, or - Unknown filter format, - Null VID on De-Assoc TLV type, or - VSI included more than Max number of filter info entries

No.	Trap Name	Platforms	Description
131	evbCdcpLldpExpiredTrap	OS6900	This trap is sent when an LLDP Timer expired in bridge. The timer expires when LLDP doesn't not receive CDCP TLV within a specified interval.
132	evbTlvExpiredTrap	OS6900	This trap is sent when an LLDP Timer expired in bridge. The timer expires when LLDP doesn't not receive EVB TLV within a specified interval.
133	evbVdpKeepaliveExpiredTrap	N/A	This trap is sent when a VDP Keep Alive Timer expired in bridge. The timer expires when the bridge doesn't not receive VDP Keep Alive message within a specified interval.
134	smgrServiceError	OS6900	This trap is sent when there is a failure to create/delete a service.
135	smgrServiceHwError	OS6900	This trap is sent when there is a failure to allocate/de-allocate a hardware resource for a service, or to program the hardware tables for a service.
136	smgrServiceSapError	OS6900	This trap is sent when there is a failure to create/delete a Service Access Point.
137	smgrServiceSapHwError	OS6900	This trap is sent when there is a failure to allocate/de-allocate a hardware resource for a SAP, or to program the hardware tables for a SAP.
138	smgrServiceSdpError	OS6900	This trap is sent when there is a failure to create/delete a Service Distribution Point.
139	smgrServiceSdpHwError	OS6900	This trap is sent when there is a failure to allocate/de-allocate a hardware resource for an SDP, or to program the hardware tables for an SDP.
140	smgrServiceSdpBindError	OS6900	This trap is sent when there is a failure to create/delete an SDP Bind.
141	smgrServiceSdpBindHwError	OS6900	This trap is sent when there is a failure to allocate/de-allocate a hardware resource for an SDP Bind, or to program the hardware tables for an SDP Bind.
142	smgrGeneralError	OS6900	This trap is sent when there is a .general system failure detected during normal system operation.
143	smgrStatusChange	OS6900	This trap is sent when there is a status change for a group of selected services.
144	portViolationNotificationTrap	OS6900	This trap is sent when a port violation is cleared.
145	multiChassisConsisFailureRecovered	OS6900	This trap is sent when the system has recovered from a multi-chassis inconsistency between the local and peer switches

No.	Trap Name	Platforms	Description
146	alaSaaPacketLossTrap	OS6900	This trap is sent when a a packet is lost during a test.
147	alaSaaJitterThresholdYellowTrap	OS6900	This trap is sent when the Jitter Threshold crosses 90%.
148	alaSaaRTTThresholdYellowTrap	OS6900	This trap is sent when the RTT Threshold crosses 90%.
149	alaSaaJitterThresholdRedTrap	OS6900	This trap is sent when the Jitter threshold is crossed.
150	alaSaaRTTThresholdRedTrap	OS6900	This trap is sent when the RTT threshold is crossed.
151	chassisTrapsDuplicateMacClear	OS6900	This trap is sent when the old Master Chassis has rejoined the Virtual Chassis as a slave.
152	alaFipsConfigFilterResourceLimit	OS6900	The allowed maximum percentage of filter resources configured from the allocated FIPS resources is exceeded.
153	virtualChassisUpgradeComplete	OS6900	Critical trap indicates whether the software upgrade process has failed after a timeout or completed successfully. Note that if the process fails, it may be still possible for the system to recover if the process successfully completes later after the expired timeout.
154	appFPSignatureMatchTrap	OS6900	This trap is sent when a traffic flow matches an application signature.
155	virtualChassisVflSpeedTypeChange	OS6900	
156	alaSIPSnoopingACLPreemptedBySOSCall	N/A	This trap is sent when a SIP snooping RTP/RTCP ACL entry is preempted by an SOS call.
157	alaSIPSnoopingRTCPOverThreshold	N/A	This trap is sent when one or more RTCP parameters exceeds the threshold limit.
158	alaSIPSnoopingRTCPPktsLost	N/A	This trap is sent when RTCP packets are lost due to rate limiting.
159	alaSIPSnoopingSignallingLost	N/A	This trap is sent when when SIP signalling messages are lost due to rate limiting.
160	alaSIPSnoopingCallRecordsFileMoved	N/A	
161	alaIPv6NeighborLimitExceeded	OS6900	
162	alaIPv6NeighborVRFLimitExceeded	OS6900	
163	alaIPv6InterfaceNeighborLimitExceed	OS6900	

No.	Trap Name	Platforms	Description
164	alaDyingGaspTrap	OS6900	This trap is sent when a switch has lost all power.
165	alaDhcpSrvLeaseUtilizationThreshold	OS6900	This trap is sent when the lease utilization on a subnet exceeds or falls below the configured threshold value.
166	pethPsePortOnOffNotification	N/A	Indicates if power inline port is or is not delivering power to the a power inline device.
167	pethPsePortPowerMaintenanceStatus	N/A	Indicates the status of the power maintenance signature for inline power.
168	pethMainPowerUsageOnNotification	N/A	Indicates that the power inline usage is above the threshold.
169	pethMainPowerUsageOffNotification	N/A	Indicates that the power inline usage is below the threshold.
170	pethPwrSupplyConflict	OS6900	Power supply type conflict trap.
171	pethPwrSupplyNotSupported	OS6900	Power supply not supported trap.
172	alaDHCPv6SrvLeaseUtilizationThresho	OS6900	This trap is sent when the lease utilization on a subnet exceeds or falls below the configured threshold value.

Unsupported Software Features

The following CLI commands and Web Management options may be available in the switch software for the following features. These features are not supported:

Feature	Platform	License
Dual-Home Link Aggregation	OS6900	Base
NetSec	OS6900	Base

Unsupported CLI Commands

The following CLI commands may be available in the switch software for the following features. These commands are not supported:

Software Feature	Unsupported CLI Commands
Source Learning	mac-learning mode [distributed | centralized]
Chassis	reload slot
SLB	server-cluster port all

Open Problem Reports and Feature Exceptions

The problems listed here include problems known at the time of the product's release. Any problems not discussed in this section should be brought to the attention of the Alcatel-Lucent Technical Support organization as soon as possible. Please contact customer support for updates on problem reports (PRs) where no known workaround was available at the time of release.

Hardware

PR	Description	Workaround
185306	Inserting an XNI-U12E into an OS6900 that doesn't have the minimum FPGA and AOS versions installed will cause the OS6900 to crash.	Upgrade the OS6900 to the proper FPGA and AOS version prior to inserting the XNI-U12E module. Refer to the upgrade instructions.
184913	The Link-Quality field is not displayed for the XNI-U12E module.	There is no known workaround at this time.

Webview

PR	Description	Workaround
178308	After a virtual chassis takeover Webview does not display the DDM information for transceivers on the new Master chassis.	Use the 'show interfaces ddm' CLI command.
186561	Firefox 23 and previous versions can't access WebView over an IPv6 interface.	Upgrade to version 24 or higher or use Internet Explorer.

FCoE Gateway

PR	Description	Workaround
185138	After a reboot some fiber channel port statistics display a large number of receive error frames.	Clear the statistics counters using the 'clear interfaces *slot/port* l2-statistics' command. In some instances the transmit error frame statistics will slowly continue to increment after being cleared. This has no impact on functionality and there is no workaround at this time
188330	The Max-frame-size on an FC port should not be changed from the default value of 2K.	There is no known workaround at this time.

Hot Swap/Redundancy Feature Guidelines

Hot Swap Feature Guidelines

- Hot swap of like modules is supported.
- Hot swap of unlike modules is not supported.
- Hot insertion, the insertion of a module into a previously empty slot, is supported on 10-Gigabit modules (i.e. OS-XNI-U4 and OS-XNI-U12(E)).
- Hot insertion, the insertion of a module into a previously empty slot, is not supported on 40-Gigabit modules (i.e. OS-QNI-U3 and OS-HNI-U6) due to the hardware having to be reset for 40-Gigabit support. After hot-inserting a 40-Gigabit module, a reboot is required.
- For the OS6900-X40 wait for first module to become operational before adding the second module.

Hot Swap Procedure

The following steps must be followed when hot-swapping expansion modules.

1. Disconnect all cables from transceivers on module to be hot-swapped.
2. Extract all transceivers from module to be hot-swapped.
3. Extract the module from the chassis and wait approximately 30 seconds before inserting replacement.
4. Insert replacement module of same type.
5. Wait for a message similar to the following to display on the console or issue the -> show module status command and wait for operational status to show 'UP':

   ChassisSupervisor niMgr info message:

   +++ Expansion module 2 ready!
6. Re-insert all transceivers into new module.
7. Re-connect all cables to transceivers.

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
Europe Union	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484

Email: esd.support@alcatel-lucent.com

Internet: Customers with Alcatel-Lucent service agreements may open cases 24 hours a day via Alcatel-Lucent's support web page at: service.esd.alcatel-lucent.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 telnet or dial-in access, hardware configuration—module type and revision by slot, software revision, 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**.

Appendix A: Upgrading an OmniSwitch 6900 to 7.3.3.R01

Overview

These instructions document how to upgrade the following OmniSwitch products to 7.3.3.R01 AOS software. Release 7.3.3.R01 is supported on the OS6900 switches.

Prerequisites

This instruction sheet requires that the following conditions exist, or are performed, before upgrading. The person performing the upgrade must:

- be the responsible party for maintaining the switch's configuration
- be aware of any issues that may arise from a network outage caused by improperly loading this code
- understand that the switch must be rebooted and network users will be affected by this procedure
- have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port
- Read the 7.3.3.R01 GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of Uboot and FPGA on the OS6900. If they meet the minimum requirements, (i.e. they were already upgraded during a previous AOS upgrade) then only an upgrade of the AOS images is required.

Do not proceed until all the above prerequisites have been met. Any deviation from these upgrade procedures will result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

Note: The examples below use the '**working'** directory as the upgrade directory, however any user-defined directory can be used for the upgrade.

OmniSwitch 6900 – Upgrade Instructions

Upgrading OS6900 Switches to 7.3.3.R01 consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go the to Alcatel-Lucent Service and Support Website and download and unzip the 7.3.3.R01 upgrade files for the OS6900. The archive contains the following:

Image Files **-** Tos.img (7.3.3.R01)

U-Boot File - u-boot.7.2.1.R02.266.tar.gz (if required)

CMM FPGA Kit – fpga_kit (if required) – this kit contains the proper files for performing an FPGA upgrade for both the OS6900X and OS6900T models to support the OS-XNI-U12E.

2. FTP the Upgrade Files to the Switch

FTP the upgrade files to the following directories of the switch you are upgrading:

- Image File - Tos.img - **/flash/working** directory
- U-Boot File - u-boot.7.2.1.R02.266.tar.gz - /**flash** directory (if required)
- CMM FPGA File - tor_fpgas.vme - /**flash** directory (if required)

3. Upgrading the U-Boot File (if required)

Execute the following CLI command to update the U-Boot File on the switch.

OS6900-> update uboot cmm 1 file u-boot.7.2.1.R02.266.tar.gz

Sample output for "update uboot cmm 1”

u-boot.bin

u-boot.bin.md5sum

u-boot.bin: OK

Erasing blocks: 4/4 (100%)lease wait.

Writing data: 0k/512k (100%)

Verifying data: 0k/512k (100%)

U-boot successfully updated

Update successfully completed

WARNING: DO NOT INTERRUPT the upgrade process until it is complete (“Update success¬fully completed”). Interruption of the process will result in an unrecoverable failure condition.

4. Upgrading the FPGA (if required)

Execute the following CLI command to update the CMM FPGA File on the switch.

OS6900-> update fpga cmm 1 file tor_fpgas.vme

Sample output for "update fpga cmm 1"

Wed Feb 8 11:27:59 : ChassisSupervisor MipMgr info message:

+++ Starting CMM FPGA Upgrade

OS6900 system and expansion fpga update

Please wait.....Update successfully completed

After the FPGA upgrade has successfully completed ("Update successfully completed"), delete the U-Boot and the FPGA Files from the /flash directory by entering the following CLI commands:

OS6900-> rm u-boot.7.2.1.R02.266.tar.gz

OS6900-> rm tor_fpgas.vme

5. Upgrade the image file

Follow the steps below to upgrade the image file:

OS6900-> reload from working no rollback-timeout

After the switch finishes rebooting, log into the switch.

Copy the image files from the Working Directory to the Certified Directory by entering the following command:

OS6900-> copy running certified

6. Verify the Software Upgrade

To verify that the software was successfully upgraded to 7.3.3.R01, use the **show microcode** command as shown below:

OS6900-> show microcode

```
Package        Release         Size       Description
---------------+---------------+------------+-------------------
Tos.img        7.3.3.384.R01   106031376  Alcatel-Lucent OS
```

Appendix B: Upgrading an OmniSwitch Virtual Chassis to 7.3.3.R01

Overview

These instructions document how to upgrade a VC of two OS6900 switches to AOS release 7.3.3.R01. Due to the software difference between AOS 7.3.2 and 7.3.3.R01 an ISSU upgrade is not supported, however the following procedure can be used to minimize any network interruptions.

Prerequisites

This instruction sheet requires that the following conditions exist, or are performed, before upgrading. The person performing the upgrade must:

- be the responsible party for maintaining the switch's configuration
- be aware of any issues that may arise from a network outage caused by improperly loading this code
- understand that the switch must be rebooted and network users will be affected by this procedure
- have a working knowledge of the switch to configure it to accept an FTP connection through the EMP or Network Interface (NI) Ethernet port
- Read the 7.3.3.R01 GA Release Notes prior to performing any upgrade for information specific to this release.
- Ensure there is a current certified configuration on the switch so that the upgrade can be rolled-back if required.
- Verify the current versions of Uboot and FPGA versions on the OS6900 and ensure they meet the minimum requirements.

Do not proceed until all the above prerequisites have been met. Any deviation from these upgrade procedures will result in the malfunctioning of the switch. All steps in these procedures should be reviewed before beginning.

Note: The examples below use the '**newversion** directory as the upgrade directory, however any user-defined directory can be used for the upgrade.

OmniSwitch 6900 – Virtual Chassis Upgrade Instructions

Upgrading a VC of OS6900 Switches to 7.3.3.R01 consists of the following steps. The steps should be performed in order:

1. Download the Upgrade Files

Go the to Alcatel-Lucent Service and Support Website and download and unzip the 7.3.3.R01 upgrade files for the OS6900. The archive contains the following files:

Image Files **-** Tos.img (7.3.3.R01)

Upgrade Script – vcof2-upgrade

2. Create a directory to hold the 7.3.3.R01 upgrade files on both Master and Slave chassis

OS6900-> mkdir /flash/newversion

3. FTP the Files to the Slave chassis and execute the script

Tos.img – FTP this file to the **/flash/newversion** directory on the Slave chassis

vcof2-upgrade – FTP this file to the **/flash** directory on the Slave chassis

Execute the script by enter the following:

-> chmod a+x /flash/vcof2-upgrade

-> /flash/vcof2-upgrade part1-on-slave newversion

The above command sequence copies the vcboot.cfg and vcsetup.cfg from the current running-directory to **/flash/newversion** directory and creates the special upgrade helper file "vcupgrade.cfg", which coordinates the Staggered Upgrade of VC-of-2 process.

4. FTP the Files to the Master chassis and execute the script

Tos.img – FTP this file to the **/flash/newversion** directory on the Slave chassis

vcof2-upgrade – FTP this file to the **/flash** directory on the Slave chassis

Execute the script by enter the following:

-> chmod a+x /flash/vcof2-upgrade

-> /flash/vcof2-upgrade part2-on-master newversion

The above command sequence copies the vcboot.cfg and vcsetup.cfg from the current running-directory to **/flash/newversion** directory and then initiates a reload on the Slave with the new software which begins the upgrade process.

5. Summary of Upgrade process

The Slave chassis loads the new software, it notes the presence of the vcupgrade.cfg file indicating it is in the process of upgrading.

After rebooting the Slave chassis becomes the Master as soon as its VFL comes up.

The old Master then reboots and loads the new software, becoming the new Slave chassis.

Appendix C: Previous Release Feature Summary

Existing Hardware - AOS 7.3.2.R01

OmniSwitch 6900-T20

10-Gigabit Ethernet (10GBase-T) fixed configuration chassis in a 1U form factor with 20 10-gigabit copper ports, one optional module slot, redundant AC or DC power and front-to-rear or rear-to-front cooling. The switch includes:

- 1 – Console Port (USB Form Factor - RS-232)
- 1 – USB Port (For use with Alcatel-Lucent OS-USB-FLASHDR USB flash drive)
- 1 – EMP Port
- 20 – 10-Gigabit copper ports
- 1 Slot– Optional module
- 1 Slot – Fan Tray
- 2 Slots – Power Supplies (AC or DC)
- Energy Efficient Ethernet
- CAT 5e/6 = 55 meters; CAT 6a/7 = 100 meters
- 100mbps/1G/10G support

OmniSwitch 6900-T40

10-Gigabit Ethernet (10GBase-T) fixed conguration chassis in a 1U form factor with 40 10-gigabit copper ports, two optional module slots, redundant AC or DC power and front-to-rear or rear-to-front cooling. The switch includes:

- 1 – Console Port (USB Form Factor - RS-232)
- 1 – USB Port (For use with Alcatel-Lucent OS-USB-FLASHDR USB flash drive)
- 1 – EMP Port
- 40 – 10-Gigabit copper ports
- 2 Slots– Optional Modules
- 1 Slot – Fan Tray
- 2 Slots – Power Supplies (AC or DC)
- Energy Efficient Ethernet
- CAT 5e/6 = 55 meters; CAT 6a/7 = 100 meters
- 100mbps/1G/10G support

OS-XNI-T8

10-Gigabit Ethernet module for the OS6900 series of swicthes with eight 1G/10G copper ports.

Existing Hardware - AOS 7.3.1.R01

OS10K-XNI-U16L
OS10K network interface card includes 8 unpopulated 10G SFP+ ports (1-8) and 8 unpopulated 1G SFP+ ports (9-16). 1G ports can be updated to 10G through license upgrade. Supports standard tables for L2, L3 and ACL policies, MPLS ready.

OS10K-XNI-U16E
OS10K network interface card includes 16 unpopulated 10G SFP+ ports. Supports standard tables for L2, L3 and ACL policies, MPLS ready.

OS10K-XNI-U32E
OS10K network interface card includes 32 unpopulated 10G SFP+ ports. Supports standard tables for L2, L3 and ACL policies, MPLS ready.

OS10K-QNI-U4E
OS10K network interface card includes 4 unpopulated 40G QSFP+ ports. Supports standard tables for L2, L3 and ACL policies, MPLS ready.

OS10K-QNI-U8E
OS10K network interface card includes 8 unpopulated 40G QSFP+ ports. Supports standard tables for L2, L3 and ACL policies, MPLS ready.

QSFP-40G-LR Transceiver
Four channel 40 Gigabit optical transceiver (QSFP+). Supports single mode fiber over 1310nm wavelength with a typical reach 10 km. Note: Supports the DDM parameters of Voltage (V), Temperature (T), Current (mA) and Input (dBm). If the threshold values of the transceiver are '0' then NS (Not supported) will be displayed in the DDM output display.

SFP-10G-24DWD80 Transceiver
10 Gigabit DWDM optical tranceiver with an LC connector. Supports single mode fiber over 1558.17nm with a typical reach of 80 km. Note: Only supported on XNI (10G) modules.

SFP-10G-GIG-SR Transceiver
Dual-speed SFP+ optical transceiver. Supports multimode fiber over 850nm wavelength (nominal) with an LC connector. Supports 1000BaseSX and 10GBASE-SR.

Existing Hardware - AOS 7.2.1.R02

NOTE: The hardware described below requires the GA build 7.2.1.323.R02.

OmniSwitch 6900 Rear-to-Front Cooling
The OmniSwitch 6900 now supports a rear-to-front cooling option with the rear-to-front fantray and power supply combination. Note the following:

- The airflow direction of the power supplies and fantray must be the same.
- The switch must be upgraded to the latest UBoot version 7.2.1.266.R02 to support rear-to-front cooling.

OS-QNI-U3 Module
40-Gigabit Ethernet module for the OS6900 series of swicthes with 3 QSFP+ ports that support 40-Gigabit transceivers. Note: Refer to the hot-swap section for hot-swap and module insertion requirements.

OS-HNI-U6 Module
10/40-Gigabit Ethernet module for the OS6900 series of swicthes with 4 SFP+ ports that support 1-Gigabit and 10-Gigabit transceivers and 2 QSFP+ ports that support 40-Gigabit transceivers. Note: Refer to the hot-swap section for hot-swap and module insertion requirements.

QSFP-40G-SR Transceiver
Four channel 40 Gigabit optical transceiver (QSFP+). Supports link lengths of 100m and 150m respectively on OM3 and OM4 multimode fiber cables. Note: Supports the required DDM parameters of Voltage (V) and Temperature (T) only.

QSFP-40G-C Transceiver
40-Gigabit direct attached copper cable available in 1/3/7 meter lengths.

OS6900-BP-R (YM-2451F) Power Supply
450W modular AC power supply with rear-to-front cooling.
Note: This power supply is differentiated from the front-to-rear power supplies by purple coloring.

OS6900-BPD-R (YM-2451P) Power Supply
450W modular DC power supply with rear-to-front cooling.
Note: This power supply is differentiated from the front-to-rear power supplies by purple coloring.

OS6900-FT-R FanTray
Contains 4 individual variable-speed fans per tray with rear-to-front cooling.
Note: This fan tray is differentiated from the front-to-rear fan tray by an R->F label and purple coloring.

Existing Hardware - AOS 7.2.1.R01

The following hardware was introduced in AOS Release 7.2.1.R01 for the OmniSwitch 6900.

OmniSwitch 6900-X20

10-Gigabit Ethernet fixed configuration chassis in a 1U form factor with 20 SFP+ ports, one optional module slot, redundant AC or DC power and front-to-rear cooling. The switch includes:

1 – Console Port (USB Form Factor - RS-232)

1 – USB Port (For use with Alcatel-Lucent **OS-USB-FLASHDR** USB flash drive)

1 – EMP Port

20 – SFP+ Ports

1 Slot– Optional module

1 Slot – Fan Tray

2 Slots – Power Supplies (AC or DC)

OmniSwitch 6900-X40

10-Gigabit Ethernet fixed conguration chassis in a 1U form factor with 40 SFP+ ports, two optional module slots, redundant AC or DC power and front-to-rear cooling. The switch includes:

1 – Console Port (USB Form Factor - RS-232)

1 – USB Port (For use with Alcatel-Lucent **OS-USB-FLASHDR** USB flash drive)

1 – EMP Port

40 – SFP+ Ports

2 Slots– Optional Modules

1 Slot – Fan Tray

2 Slots – Power Supplies (AC or DC)

OS-XNI-U4

10-Gigabit Ethernet module for the OS6900 series of swicthes with 4 SFP+ ports that support 1-Gigabit and 10-Gigabit transceivers.

OS-XNI-U12

10-Gigabit Ethernet module for the OS6900 series of swicthes with 12 SFP+ ports that support 1-Gigabit and 10-Gigabit transceivers.

OS6900-BP-F (YM-2451C) Power Supply
450W modular AC power supply with front-to-rear cooling.

OS6900-BPD-F (YM-2451D) Power Supply

450W modular DC power supply with front-to-rear cooling.

OS6900-FT-F FanTray

Contains 4 individual variable-speed fans per tray with front-to-rear cooling.

Existing Hardware - AOS 7.1.1.R01

The following hardware was introduced with AOS Release 7.1.1.R01 for the OmniSwitch 10K.

OmniSwitch 10K Chassis

The OmniSwitch 10K is a high performance chassis accomodating high-density Gigabit Ethernet and 10-Gigabit Ethernet Network Interface (NI) modules.

8 Slots – Network Interface Modules

2 Slots – Chassis Management Modules (Integrated Management and Chassis Fabric Module)

2 Slots – Chassis Fabric Modules

2 Slots – Fan Trays (Two fan trays required)

4 Slots – Power Supplies

OS10K-CMM

The Chassis Management Module (CMM) provides both management and switching fabric for the OmniSwitch chassis. The CMM provides key system services and backup system services when a secondary CMM is present.

OS10K-CFM

The Chassis Fabric Module (CFM) provides the switching fabric for the chassis. Additional CFMs provide increased switching throughput, as well as redundancy.

OS10K-GNI-C48E

Provides 48 wire-rate RJ-45 1000Base-T ports and large table support for L2, L3, and ACL policies.

OS10K-GNI-U48E

Provides 48 wire-rate 1000BaseX SFP ports and large table support for L2, L3, and ACL policies.

OS10K-XNI-U32S

Provides 32 10-Gigabit SFP+ ports as well as support for 1-Gigabit SFP transceivers. Supports standard tables for L2, L3 and ACL policies.

OS10K-PS-25A

AC power supply auto-ranging from 110VAC-240VAC providing 1250W at 110VAC and 2500W at 240VAC.

OS10K-PS-24D

DC power supply providing up to 2400 watts of power with 36-72VDC input.

OS10K-Fan-Tray

Contains 12 individual variable-speed fans per tray.

Existing Software Features Summary – AOS 7.3.2.R01

Feature	Platform	License
Data Center Feature Support		
- FIP Snooping	OS10K/6900	Data Center
- Virtual Maching Performance Monitoring	OS10K/6900	Data Center
Layer 2 Feature Support		
- Dynamic Auto Fabric	OS10K/6900	Base
Layer 3 Feature Support		
- IPv4 over SPBM	OS10K/6900	Advanced
- Interop between PIM & DVMRP	OS10K/6900	Base
- Non-Contiguous Mask and IPv6 Gateway Support	OS10K/6900	Base
- Increase VRF Instances	OS10K/6900	Base
Management/Additional Feature Support		
- Command Abbreviation	OS10K/6900	Base
- Web Services & CLI Scripting	OS10K/6900	Base
- Enhanced Server & Session Limits	OS10K/6900	Base
Additional Feature Support		
- Application Fingerprinting	OS10K/6900	Base
- Fault Propagation and Link Flapping - Wait to Shutdown	OS10K/6900	Base

Existing Software Features Summary – AOS 7.3.1.R01

Feature	Platform	License

Feature	Platform	License
Data Center Feature Support		
Shortest Path Bridging (SPB)	OS10K/6900	Advanced
Data Center Bridging • DCBX • ETS • PFC	 OS10K/6900 OS10K/6900 OS10K/6900	 Data Center Data Center Data Center
Edge Virtual Briding (EVB)	OS10K/6900	Data Center
Virtual Network Profiles • SAP/SPB-M Services • Customer Domains (Multi-tenancy) • Dynamic SAP • UNP over MC-LAG on OS10K	 OS10K/6900 OS10K/6900 OS10K/6900 OS10K/6900	 Base Base Base Base
Layer 2 Feature Support		
Ethernet Ring Protection v2 (ERPv2)	OS10K/6900	Base
Layer 3 Feature Support		
VRF Management	OS10K/6900	Base
VRF Route Leak	OS10K/6900	Base
Management Feature Support		
Virtual Chassis	OS10K/6900	Advanced
SFP+ Line Diags & Enhanced Port Performance (EPP)	OS10K/6900	Base
License Management	OS10K/6900	Base
Ethernet OAM • ITU Y1731 and 802.1ag	OS10K/6900 OS10K/6900	Base
Service Assurance Agent	OS10K/6900	Base

Note: The SAP/SPB-M Services, Customer Domains, Dynamic SAP, and Virtual Chassis features were introduced in AOS Release 7.3.1.632.R01. The remaining features in this section were introduced in AOS Release 7.3.1.519.R01.

Existing Software Features Summary – AOS 7.2.1.R02

Feature	Platform	License
Layer 2 Feature Support		
High Availability VLAN • Added support for OS10K • HA-VLAN with MCLAG	 OS10K OS10K/6900	 Base Base
Multi-Chassis Link Aggregation • Configurable Chassis Group ID (Multiple MC-LAG Domains) • Standalone Port in VIP VLAN • SLB Over MC-LAG	 OS10K/6900 OS10K/6900 OS10K/6900	 Base Base Base
MVRP • Added support for OS10K	 OS10K	 Base
Universal Network Profiles • UNP with Dynamic Profiles • UNP with Link-Aggregation • UNP with MC-LAG • UNP with Learned Port Security	 OS6900 OS6900 OS6900 OS6900	 Base Base Base Base
Layer 3 Feature Support		
16 ECMP routes for IPv6	OS10K/6900	Base
Qos		
VFC/VoQ Profiles • Added support for profiles 2-4 • Added support for WRED	 OS10K/6900 OS6900	 Base Base
Security		
Learned Port Security Enhancements	OS10K/6900	Base

Existing Software Features Summary – AOS 7.2.1.R01

Feature	Platform	License
Manageability Feature Support		
CLI	OS6900	Base
Ethernet Interfaces	OS6900	Base
License Management	OS6900	Base
Multiple VRF Routing and Forwarding	OS6900	Advanced
Network Time Protocol (NTP)	OS6900	Base
Pause Control(RX) /Flow Control	OS6900	Base
Remote Access FTP SCP SSH/SFTP Telnet TFTP	OS6900	Base
Resiliency Features Hot Swap Expansion Modules Power Supply Redundancy Fan Redundancy	OS6900	Base
SNMP	OS6900	Base
Software Rollback – Multi-Image/Multi-Config	OS6900	Base
Storm Control	OS6900	Base
Text File Configuration	OS6900	Base
UDLD	OS6900	Base
USB Support	OS6900	Base
Web-Based Management (WebView)	OS6900	Base
Layer 2 Feature Support		
802.1AB with MED Extensions	OS6900	Base
802.1Q	OS6900	Base
Configurable Hash Mode	OS6900	Base
HA-VLAN	OS6900	Base
Link Aggregation –Static and LACP	OS6900	Base

Feature	Platform	License
(802.3ad)		
Multi-Chassis Link Aggregation	OS6900	Base
MVRP	OS6900	Base
Source Learning	OS6900	Base
Spanning Tree • 802.1d and 802.1w • Multiple Spanning Tree Protocol • PVST+ • Root Guard	OS6900	Base
Universal Network Profiles (UNP)	OS6900	Base
VLANs	OS6900	Base
IPv4 Feature Support		
Bi-Directional Forwarding Detection (BFD)	OS6900	Base
DHCP / UDP DHCP Relay/Option-82 Per-VLAN UDP Relay	OS6900	Base
BGP4 with Graceful Restart	OS6900	Advanced
DNS Client	OS6900	Base
GRE	OS6900	Base
IP Multicast Routing	OS6900	Advanced
IP Multicast Switching (IGMP)	OS6900	Base
IP Multicast Switching (Proxying)	OS6900	Base
IP Multinetting	OS6900	Base
IP Route Map Redistribution	OS6900	Base
IP-IP Tunneling	OS6900	Base
OSPFv2	OS6900	Advanced
RIPv1/v2	OS6900	Base
Routing Protocol Preference	OS6900	Base
Server Load Balancing	OS6900	Base
VRRPv2	OS6900	Advanced

Feature	Platform	License
IPv6 Feature Support		
BGP4 BGP IPv6 Extensions	OS6900	Advanced
IPSec IPv6 OSPFv3 RIPng	OS6900	Advanced
IPv6 Client and/or Server Support	OS6900	Base
IPv6 Multicast Routing	OS6900	Advanced
IPv6 Multicast Switching (MLD v1/v2)	OS6900	Base
IPv6 Routing	OS6900	Advanced
IPv6 Scoped Multicast Addresses	OS6900	Base
IPv6 Neighbor Discovery Support	OS6900	Base
OSPFv3	OS6900	Advanced
RIPng	OS6900	Advanced
VRRPv3	OS6900	Advanced
QoS Feature Support		
Auto-Qos Prioritization of NMS Traffic	OS6900	Base
Ingress and egress bandwith shaping	OS6900	Base
Policy Based Routing	OS6900	Advanced
Tri-Color Marking	OS6900	Base
Multicast Feature Support		
DVMRP	OS6900	Advanced
IGMP Multicast Group Configuration Limit	OS6900	Base
IGMP Relay	OS6900	Base
IPv4/IPv6 Multicast Switching (IPMS)	OS6900	Base
L2 Static Multicast Address	OS6900	Base
PIM / PIM-SSM (Source-Specific Multicast)	OS6900	Advanced

Feature	Platform	License
Monitoring/Troubleshooting Feature Support		
DDM - Digital Diagnostic Monitoring	OS6900	Base
Health Statistics	OS6900	Base
Ping and Traceroute	OS6900	Base
Policy Based Mirroring	OS6900	Base
Port Mirroring	OS6900	Base
Port Monitoring	OS6900	Base
Remote Port Mirroring	OS6900	Base
Rmon	OS6900	Base
sFlow	OS6900	Base
Switch Logging and Syslog	OS6900	Base
Metro Ethernet Feature Support		
ERP G.8032 – Shared VLAN	OS6900	Base
Ethernet Services	OS6900	Base
L2 Control Protocol Tunneling (L2CP)	OS6900	Base
Security Feature Support		
Access Control Lists (ACLs) for IPv4/IPv6	OS6900	Base
Account & Password Policies	OS6900	Base
Admin User Remote Access Restriction Control	OS6900	Base
ARP Defense Optimization	OS6900	Base
ARP Poisoning Detect	OS6900	Base
Authenticated Switch Access	OS6900	Base
IP DoS Filtering	OS6900	Base
Learned Port Security (LPS)	OS6900	Base
Policy Server Management	OS6900	Base

AOS 7.1.1. R01 Feature Summary Table

Feature	Platform	Software Package
Manageability Feature Support		
CLI	OS10K	Base
Ethernet Interfaces	OS10K	Base
ISSU	OS10K	Base
Multiple VRF Routing and Forwarding	OS10K	Base
Network Time Protocol (NTP)	OS10K	Base
Pause Control/Flow Control	OS10K	Base
Remote Access FTP SCP SSH/SFTP Telnet TFTP	OS10K	Base
Smart Continuous Switching Hot Swap Management Module Failover Power Monitoring Redundancy	OS10K	Base
SNMP	OS10K	Base
Software Rollback – Multi-Image/Multi-Config	OS10K	Base
Storm Control	OS10K	Base
Text File Configuration	OS10K	Base
UDLD	OS10K	Base
USB Support	OS10K	Base
Web-Based Management (WebView)	OS10K	Base
Layer 2 Feature Support		
802.1AB with MED Extensions	OS10K	Base
802.1Q	OS10K	Base
Configurable Hash Mode	OS10K	Base
Link Aggregation –Static and LACP (802.3ad)	OS10K	Base

Feature	Platform	Software Package
Multi-Chassis Link Aggregation	OS10K	Base
Source Learning	OS10K	Base
Spanning Tree • 802.1d and 802.1w • Multiple Spanning Tree Protocol • PVST+ • Root Guard	OS10K	Base
VLANs	OS10K	Base
IPv4 Feature Support		
Bi-Directional Forwarding Detection (BFD)	OS10K	Base
DHCP / UDP DHCP Relay/Option-82 Per-VLAN UDP Relay	OS10K	Base
BGP4 with Graceful Restart	OS10K	Base
DNS Client	OS10K	Base
GRE	OS10K	Base
IP Multicast Routing	OS10K	Base
IP Multicast Switching (IGMP)	OS10K	Base
IP Multicast Switching (Proxying)	OS10K	Base
IP Multinetting	OS10K	Base
IP Route Map Redistribution	OS10K	Base
IP-IP Tunneling	OS10K	Base
OSPFv2	OS10K	Base
RIPv1/v2	OS10K	Base
Routing Protocol Preference	OS10K	Base
Server Load Balancing	OS10K	Base
VRRPv2	OS10K	Base
IPv6 Feature Support		
BGP4	OS10K	Base

Feature	Platform	Software Package
BGP IPv6 Extensions		
IPSec IPv6 OSPFv3 RIPng	OS10K	Base
IPv6 Client and/or Server Support	OS10K	Base
IPv6 Multicast Routing	OS10K	Base
IPv6 Multicast Switching (MLD v1/v2)	OS10K	Base
IPv6 Routing	OS10K	Base
IPv6 Scoped Multicast Addresses	OS10K	Base
IPv6 Neighbor Discovery Support	OS10K	Base
OSPFv3	OS10K	Base
RIPng	OS10K	Base
VRRPv3	OS10K	Base
QoS Feature Support		
Auto-Qos Prioritization of NMS Traffic	OS10K	Base
Ingress and egress bandwith shaping	OS10K	Base
Policy Based Routing	OS10K	Base
Tri-Color Marking	OS10K	Base
Multicast Feature Support		
DVMRP	OS10K	Base
IGMP Multicast Group Configuration Limit	OS10K	Base
IGMP Relay	OS10K	Base
IPv4/IPv6 Multicast Switching (IPMS)	OS10K	Base
L2 Static Multicast Address	OS10K	Base
PIM / PIM-SSM (Source-Specific Multicast)	OS10K	Base
Monitoring/Troubleshooting Feature Support		
DDM - Digital Diagnostic Monitoring	OS10K	Base
Health Statistics	OS10K	Base

Feature	Platform	Software Package
Ping and Traceroute	OS10K	Base
Policy Based Mirroring	OS10K	Base
Port Mirroring	OS10K	Base
Port Monitoring	OS10K	Base
Remote Port Mirroring	OS10K	Base
Rmon	OS10K	Base
sFlow	OS10K	Base
Switch Logging and Syslog	OS10K	Base
Metro Ethernet Feature Support		
ERP G.8032 – Shared VLAN	OS10K	Base
Ethernet Services	OS10K	Base
L2 Control Protocol Tunneling (L2CP)	OS10K	Base
Security Feature Support		
Access Control Lists (ACLs) for IPv4/IPv6	OS10K	Base
Account & Password Policies	OS10K	Base
Admin User Remote Access Restriction Control	OS10K	Base
ARP Defense Optimization	OS10K	Base
ARP Poisoning Detect	OS10K	Base
Authenticated Switch Access	OS10K	Base
IP DoS Filtering	OS10K	Base
Learned Port Security (LPS)	OS10K	Base
Policy Server Management	OS10K	Base