
Alcatel-Lucent Enterprise OmniSwitch 6900 (25G & 100G) GOLDEN RFP

Version 8.9R4

Contents

1. Introduction	3
2. OmniSwitch 6900 models and chassis components	5
2.1. OS6900-X24 (OS6900-X24C2)	5
2.2. OS6900-T24 (OS6900-T24C2)	6
2.3. OS6900-X48 (OS6900-X48C6)	7
2.4. OS6900-T48 (OS6900-T48C6)	8
2.5. OS6900-X48E (6900-X48C4E)	9
2.6. OS6900-V48 (OS6900-V48C8)	10
2.7. OS6900-C32 (OS6900-C32E)	11
3. Network virtualization technologies	11
4. Layer-3 IPv4 routing protocols and features	12
5. Layer-3 IPv6 routing protocols and features	13
6. IPv4/IPv6 multicast protocols and features	14
7. Layer-2 switching services	14
8. Security features	15
9. Quality of Service (QoS) features	16
10. Data Center features	17
11. Switch management and operation features	17
12. Access authentication security features	19
13. Software Defined Networking (SDN) features	19
14. Other key software features:	20
15. ITU-T recommendations	20
16. Certifications	21
17. Video surveillance	21

1. Introduction

The Alcatel-Lucent OmniSwitch® 6900 fixed Core LAN and Data Center (DC) switches are compact, high-density 10, 25, 40 and 100 Gigabit Ethernet (GigE) platforms. They offer high performance and extremely low latency Layer-2 and Layer-3 switching for campus and DC Fabric networks. They are designed for the most demanding software-defined operations in virtualized or physical networks.

OmniSwitch 6900s can be positioned as Top- of- Rack (ToR) or spine switches in DC environments, or as core and aggregation devices in campus networks. They support a wide range of protocols and programable interface (API) for building ALE's autonomous Service Defined Network or overlay networks based on Software Defined Network architectures.

The OmniSwitch 6900 product family offers a very high port density, with up to 128 x 10 GigE, 80 x 25 GigE and up to 32 x 40/100 GigE ports in a 1RU form factor. The Virtual Chassis feature extends the modularity and reliability of connectivity to address any size of virtualized, highly secured modern and autonomous networks. MACSec is also supported on specific OS6900 models for mission critical and encrypted communication networks. The OmniSwitch 6900 product family leverages an energy-efficient model with leading low power consumption, making them the most efficient and versatile switches in their class.



OmniSwitch 6900-C32



OmniSwitch 6900-X48



OmniSwitch 6900-V48



OmniSwitch 6900-T48



OmniSwitch 6900-T24



OmniSwitch 6900-X24

Alcatel-Lucent OmniSwitch 6900 25G & 100GigE models

The Alcatel-Lucent OmniSwitch 6900 family offers high-performance and very low-latency multi-layer (L2/L3), supporting speeds of 10G/25G/40G/100GigE for a multitude of application deployments. All models are 1RU form factor with redundant power supplies and fan trays for front-to-back and back-to-front airflow. Available interfaces include 100 GigE, 40 GigE, 25 GigE, 1/10 GigE, 1G/10GBase-T, and 100Base-T (supported in some models).

- The **OmniSwitch 6900-X24C2** supports 10Gigabit/100Gigabit Ethernet L3 fixed in a 1RU form factor with 26 SFP+ ports and 2 QSFP28 ports. SFP+ ports operate as 1/10GE. QSFP28 ports operate as 100/40GE.
- The **OmniSwitch 6900-T24C2** supports 10Gigabit/100Gigabit Ethernet L3 fixed in a 1RU form factor with 24 10GBaseT, 2 SFP+ ports and 2 QSFP28 ports. SFP+ and 10GBaseT ports operate as 1/10GE. QSFP28 ports operate as 100/40GE.
- The **OmniSwitch 6900-X48C6** supports 1G/10G/25G/40G/100Gigabit Ethernet L3 fixed configuration chassis in a 1RU form factor with 48 1/10G SFP+ ports and six 40G/100G QSFP28 ports. QSFP28 ports operate as single 40/100GE port or Quad-10/25GigE ports.
- The **OmniSwitch 6900-T48C6** supports 10Gigabit/100Gigabit Ethernet L3 fixed configuration chassis in a 1RU form factor with 48 1G/10G BaseT and six 40G/100GigE QSFP28 ports. QSFP28 ports operate as single 40G/100GigE port or Quad-10G/25GigE.
- The **OmniSwitch 6900-X48C4E** supports 10Gigabit/100Gigabit Ethernet L3 fixed configuration chassis in a 1RU form factor with 40 (ports 1-40) 1G/10G SFP+ ports, 8 (ports 41-48) 1G/10G/25G SFP28 ports and four 40G/100G QSFP28 ports. The QSFP28 ports operate as single 40G/100GE port or Quad 10G/25GE ports. Supports **MACsec** in hardware on all ports.
- The **OmniSwitch 6900-V48C8** supports 10Gigabit/25Gigabit L3 fixed configuration chassis in a 1RU form factor with 48 1/10/25G SFP28 ports and 8 QSFP28 ports. The QSFP28 ports operate as single 40G/100GE port or Quad 10G/25GE ports.
- The **OmniSwitch 6900-C32E** supports 100 Gb Ethernet L3 fixed configuration chassis in a 1RU form factor with 32 QSFP28 ports. Ports operate as single 40/100GigE port or Quad-10/25GigE.

Links to supporting documentation:

[OmniSwitch 6900 Family Data Sheet](#)

For the most recent Common Criteria EAL2 and NDcPP certificates go to fvm.se.

2. OmniSwitch 6900 models and chassis components

2.1.OS6900-X24 (OS6900-X24C2)

The switch must support the following characteristics:

2.1.1.	Non-blocking architecture	C/PC/NC
2.1.2.	Total RU: 1 RU maximum	C/PC/NC
2.1.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.1.4.	Minimum of 26 1/10G SFP+ ports	C/PC/NC
2.1.5.	Minimum of 2 40/100G QSFP28 ports	C/PC/NC
2.1.6.	Minimum 2 QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.1.7.	Support for hot swappable SFPs	C/PC/NC
2.1.8.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.1.9.	Minimum switching capacity of 1.12Tbps	C/PC/NC
2.1.10.	Maximum latency of 650 ns	C/PC/NC
2.1.11.	Maximum power consumption under full L2 traffic load includes two power supplies of 219W	C/PC/NC
2.1.12.	Minimum MTBF with AC PS of 384,636h	C/PC/NC
2.1.13.	Minimum MTBF with DC PS of 385,000h	C/PC/NC
2.1.14.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.1.15.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

2.2.OS6900-T24 (OS6900-T24C2)

The switch must support the following characteristics:

2.2.1.	Non-blocking architecture	C/PC/NC
2.2.2.	Total RU: 1 RU maximum	C/PC/NC
2.2.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.2.4.	Minimum of 24 1/10G Base-T ports	C/PC/NC
2.2.5.	Minimum of 2 1/10G SFP+ ports	C/PC/NC
2.2.6.	Minimum of 2 40/100G QSFP28 ports	C/PC/NC
2.2.7.	Minimum 2 QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.2.8.	Support for hot swappable SFPs	C/PC/NC
2.2.9.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.2.10.	Minimum switching capacity of 1.12 Tbps	C/PC/NC
2.2.11.	Maximum latency of 650 ns	C/PC/NC
2.2.12.	Maximum power consumption under full L2 traffic load includes two power supplies of 222W	C/PC/NC
2.2.13.	Minimum MTBF with AC PS of 384,636h	C/PC/NC
2.2.14.	Minimum MTBF with DC PS of 385,000h	C/PC/NC
2.2.15.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.2.16.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

2.3.OS6900-X48 (OS6900-X48C6)

The switch must support the following characteristics:

2.3.1.	Non-blocking architecture	C/PC/NC
2.3.2.	Total RU: 1 RU maximum	C/PC/NC
2.3.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.3.4.	Minimum of 48 1/10G SFP+ ports	C/PC/NC
2.3.5.	Minimum of 6 40/100G QSFP28 ports	C/PC/NC
2.3.6.	Minimum 2 QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.3.7.	Support for hot swappable SFPs	C/PC/NC
2.3.8.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.3.9.	Minimum switching capacity of 2.16Tbps	C/PC/NC
2.3.10.	Maximum latency of 650 ns	C/PC/NC
2.3.11.	Maximum power consumption under full L2 traffic load includes two power supplies of 356W	C/PC/NC
2.3.12.	Minimum MTBF with AC PS of 384,636h	C/PC/NC
2.3.13.	Minimum MTBF with DC PS of 385,000h	C/PC/NC
2.3.14.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.3.15.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

2.4.OS6900-T48 (OS6900-T48C6)

The switch must support the following characteristics:

2.4.1.	Non-blocking architecture	C/PC/NC
2.4.2.	Total RU: 1 RU maximum	C/PC/NC
2.4.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.4.4.	Minimum of 48 1/10GBase-T ports	C/PC/NC
2.4.5.	Minimum of 6 40/100G QSFP28 ports	C/PC/NC
2.4.6.	Minimum 2 QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.4.7.	Support for hot swappable SFPs	C/PC/NC
2.4.8.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.4.9.	Minimum switching capacity of 2.16Tbps	C/PC/NC
2.4.10.	Maximum latency of 650 ns	C/PC/NC
2.4.11.	Maximum power consumption under full L2 traffic load includes two power supplies of 323W	C/PC/NC
2.4.12.	Minimum MTBF with AC PS of 372,562h	C/PC/NC
2.4.13.	Minimum MTBF with DC PS of 385,000h	C/PC/NC
2.4.14.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.4.15.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

2.5.OS6900-X48E (6900-X48C4E)

The switch must support the following characteristics:

2.5.1.	Non-blocking architecture	C/PC/NC
2.5.2.	Total RU: 1 RU maximum	C/PC/NC
2.5.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.5.4.	Minimum of 40 1/10G SFP+ ports	C/PC/NC
2.5.5.	Minimum of 8 1G/10G/25G SFP28 ports	C/PC/NC
2.5.6.	Minimum of 4 40/100G QSFP28 ports	C/PC/NC
2.5.7.	QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.5.8.	Supports MACsec on all ports	C/PC/NC
2.5.9.	MACsec is supported between two directly connected Service Access Ports or network ports for service type SPB/VXLAN/L2GRE to provide MACsec security on the tunneled traffic.	C/PC/NC
2.5.10.	Support for hot swappable SFPs	C/PC/NC
2.5.11.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.5.12.	Minimum switching capacity of 2 Tbps	C/PC/NC
2.5.13.	Maximum latency of 600 ns	C/PC/NC
2.5.14.	Maximum power consumption under full L2 traffic load includes two power supplies of 460W	C/PC/NC
2.5.15.	Minimum MTBF with AC PS of 208,000h	C/PC/NC
2.5.16.	Minimum MTBF with DC PS of 210,000h	C/PC/NC
2.5.17.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.5.18.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

2.6.OS6900-V48 (OS6900-V48C8)

The switch must support the following characteristics:

2.6.1.	Non-blocking architecture	C/PC/NC
2.6.2.	Total RU: 1 RU maximum	C/PC/NC
2.6.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.6.4.	Minimum of 48 1G/10G/25G SFP28 ports	C/PC/NC
2.6.5.	Minimum of 8 40/100G QSFP28 ports	C/PC/NC
2.6.6.	QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.6.7.	Support for hot swappable SFPs	C/PC/NC
2.6.8.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.6.9.	Minimum switching capacity of 4 Tbps	C/PC/NC
2.6.10.	Maximum latency of 600 ns	C/PC/NC
2.6.11.	Maximum power consumption under full L2 traffic load includes two power supplies of 550W	C/PC/NC
2.6.12.	Minimum MTBF with AC PS of 208,000h	C/PC/NC
2.6.13.	Minimum MTBF with DC PS of 210,000h	C/PC/NC
2.6.14.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.6.15.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

2.7.OS6900-C32 (OS6900-C32E)

The switch must support the following characteristics:

2.7.1.	Non-blocking architecture	C/PC/NC
2.7.2.	Total RU: 1 RU maximum	C/PC/NC
2.7.3.	Support for redundant and hot swappable AC & DC power supplies	C/PC/NC
2.7.4.	Minimum of 32 40/100G QSFP28 ports	C/PC/NC
2.7.5.	QSFP28 ports support splitter mode to 4x10GE or 4x25GE	C/PC/NC
2.7.6.	Support for hot swappable SFPs	C/PC/NC
2.7.7.	Virtual chassis up to 6 elements (manageable with single IP address) with dedicated ports to build stack or virtual chassis	C/PC/NC
2.7.8.	Minimum switching capacity of 6.4 Tbps	C/PC/NC
2.7.9.	Maximum latency of 600 ns	C/PC/NC
2.7.10.	Maximum power consumption under full L2 traffic load includes two power supplies of 360W	C/PC/NC
2.7.11.	Minimum MTBF with AC PS of 195,000h	C/PC/NC
2.7.12.	Minimum MTBF with DC PS of 210,000h	C/PC/NC
2.7.13.	Operating temperature between 0°C to 45°C (32°F to 113°F)	C/PC/NC
2.7.14.	Storage Temperature -10°C to 70°C (14°F to 158°F)	C/PC/NC

3. Network virtualization technologies

The switch must support the following:

3.1.	Multiple units can be stacked to create a Virtual Chassis (VC) for configuration and management as a single logical entity, supporting high resiliency software and hardware features for multi-home backbone connectivity using standard link aggregation protocol (LACP) for enabling a non-blocking network backbone architecture	C/PC/NC
3.2.	Virtualization technology must support a unified data and management plane with a single IP address for management and communications.	C/PC/NC
3.3.	Virtualization technology must support the SPB-M protocol with or without using VRRP or Link Aggregation protocols to run it.	C/PC/NC

3.4.	Support for up six switches to be virtualized into a single virtual switch unit or Virtual Chassis (VC)*. (<i>Virtual Chassis (VC) support in the OS6900X48C4E is scheduled to be supported in AOS release 8.8R1</i>)	C/PC/NC
3.5.	Must be able to support End-of-Row (EoR) and Top-of-Rack (ToR) applications where the switch must be able to serve as a master switch in a Virtual Chassis (VC) configuration to provide centralized management via a single IP	C/PC/NC
3.6.	Must support split-chassis mechanisms to maintain network integrity when unit(s) in a Virtual Chassis (VC) fail to minimize network outages.	C/PC/NC
3.7.	When operating in Virtual Chassis (VC) environments, the switches must be able to be upgraded individually without requiring every unit in the VC to reboot simultaneously.	C/PC/NC
3.8.	Must support In-Service Software Upgrade (ISSU).	C/PC/NC
3.9.	The switch must support MAC Retention, this allows a system in a Virtual Chassis or also known as, stackable switches to retain the MAC address of the primary switch for a fixed or indefinite time, even after multiple takeovers. This minimizes the recalculation of protocols, such as Spanning Tree and Link Aggregation.	C/PC/NC

4. Layer-3 IPv4 routing protocols and features

The switch must support the following:

4.1.	Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information	C/PC/NC
4.2.	VRF-aware Policy-based Routing	C/PC/NC
4.3.	Static routing with route labeling	C/PC/NC
4.4.	Routing Information Protocol (RIP) v1 and v2, RIPng	C/PC/NC
4.5.	Open Shortest Path First (OSPF) v2 with Graceful Restart	C/PC/NC
4.6.	Intermediate System to Intermediate System (IS-IS) with Graceful Restart	C/PC/NC
4.7.	Border Gateway Protocol (BGP) v4 with Graceful Restart	C/PC/NC
4.8.	Generic Routing Encapsulation (GRE) and IP/IP tunneling	C/PC/NC
4.9.	Maximum number of L2 GRE tunnel is 8000	C/PC/NC

4.10.	Virtual Router Redundancy Protocol (VRRPv2)	C/PC/NC
4.11.	DHCP relay (including generic UDP relay)	C/PC/NC
4.12.	Address Resolution Protocol (ARP)	C/PC/NC
4.13.	Policy-based routing and server load balancing (SLB)	C/PC/NC
4.14.	DHCP V4 server	C/PC/NC

5. Layer-3 IPv6 routing protocols and features

The switch must support the following:

5.1.	Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information.	C/PC/NC
5.2.	VRF-aware Policy-based Routing	C/PC/NC
5.3.	Internet Control Message Protocol version 6 (ICMPv6)	C/PC/NC
5.4.	Static routing	C/PC/NC
5.5.	Routing Information Protocol Next Generation (RIPng)	C/PC/NC
5.6.	Open Shortest Path First (OSPF) v3 with Graceful Restart	C/PC/NC
5.7.	Intermediate System to Intermediate System (IS-IS) with Graceful Restart	C/PC/NC
5.8.	Multi-Topology IS-IS	C/PC/NC
5.9.	BGP v4 multiprotocol extensions for IPv6 routing (MP-BGP)	C/PC/NC
5.10.	Graceful Restart extensions for OSPF and BGP	C/PC/NC
5.11.	Virtual Router Redundancy Protocol version 3 (VRRPv3)	C/PC/NC
5.12.	Neighbor Discovery Protocol (NDP)	C/PC/NC
5.13.	Policy-based routing and server load balancing (SLB)	C/PC/NC
5.14.	DHCPv6 server	C/PC/NC

6. IPv4/IPv6 multicast protocols and features

The switch must support the following:

6.1.	IGMPv1/v2/v3 snooping and Multicast Listener Discovery (MLD) v1/v2 for fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors	C/PC/NC
6.2.	Protocol Independent Multicast - Sparse- Mode (PIM-SM), Source Specific Multicast (PIM-SSM)	C/PC/NC
6.3.	Protocol Independent Multicast - Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir)	C/PC/NC
6.4.	Distance Vector Multicast Routing Protocol (DVMRP)	C/PC/NC
6.5.	Multicast Listener Discovery (MLD) v1/v2 snooping	C/PC/NC
6.6.	PIM to DVMRP gateway support	C/PC/NC

7. Layer-2 switching services

The switch must support the following:

7.1.	Ethernet services using IEEE 802.1ad Provider Bridges (also known as Q-in-Q or VLAN stacking)	C/PC/NC
7.2.	Fabric virtualization services IEEE802.1aq Shortest Path Bridging (SPB-M)	C/PC/NC
7.3.	Fabric virtualization services VXLAN	C/PC/NC
7.4.	In-band management for IEEE 802.1aq (SPB-M)	C/PC/NC
7.5.	AOS functionality of advertising SPB L3VPN routes is extended to exchange and inject the route-tag field to be carried across the SPB-ISIS network.	C/PC/NC
7.6.	Ethernet network-to-network interface (NNI) and user network interface (UNI)	C/PC/NC
7.7.	Service VLAN (SVLAN) and Customer VLAN (CVLAN) support	C/PC/NC
7.8.	VLAN translation and mapping including CVLAN to SVLAN	C/PC/NC
7.9.	Service Access Point (SAP) profile identification (ID) defining values for ingress bandwidth sharing, rate limiting, CVLAN tag processing (translate or preserve), and priority mapping (inner to outer tag or fixed value).	C/PC/NC

7.10.	Classification of different untagged users to the same UNP dynamic untagged SAP, which can be associated to different services (like SPB, L2GRE, and VXLAN). The untagged SAP creation on different services is supported only for UNP dynamic SAPs.	C/PC/NC
7.11.	Hybrid access port feature allows a single port to function both as an access port and a bridging port. Hybrid configured port can be understood as a bridge port with a default VLAN and tagged VLAN for bridging and the user can configure SAPs for services with mapped tagged VLANs.	C/PC/NC
7.12.	Port Mapping controlling communication between peer users	C/PC/NC
7.13.	DHCP Option 82: Configurable relay agent information	C/PC/NC
7.14.	Multiple VLAN Registration Protocol (MVRP)	C/PC/NC
7.15.	High Availability (HA) -VLAN allowing for sending traffic to send traffic intended for a single destination MAC address to multiple switch ports for Layer 2 clusters such as MS-NLB and active-active Firewall clusters	C/PC/NC
7.16.	Private VLANs	C/PC/NC
7.17.	Jumbo frame	C/PC/NC
7.18.	Bridge Protocol Data Unit (BPDU) blocking	C/PC/NC
7.19.	Ethernet OAM (802.1ag): Connectivity Fault Management (L2 ping & Link trace)	C/PC/NC

8. Security features

The switch must support the following:

8.1.	Autosensing IEEE 802.1X multiclient, multi-VLAN support for SPB-M & VXLAN	C/PC/NC
8.2.	Autosensing IEEE 802.1X multiclient, multi-VLAN support for bridging services	C/PC/NC
8.3.	MAC-based authentication for non-IEEE 802.1X hosts	C/PC/NC
8.4.	Secure Shell (SSH) with public key infrastructure (PKI) support	C/PC/NC
8.5.	Terminal Access Controller Access- Control System Plus (TACACS+) client	C/PC/NC
8.6.	Centralized Remote Access Dial- In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication	C/PC/NC
8.7.	Learned Port Security (LPS) or MAC address lockdown	C/PC/NC
8.8.	Learned Port Security (LPS) on Service Access Port (SAP) ports mapped to SPB service	C/PC/NC

8.9.	Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)	C/PC/NC
8.10.	DHCP v4 & v6 Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection	C/PC/NC
8.11.	DHCP v4 Snooping Support over SPB/VxLAN/L2GRE/VPLS services	C/PC/NC
8.12.	DHCPv6 guard and DHCPv6 Client Guard	C/PC/NC
8.13.	ARP poisoning detection	C/PC/NC
8.14.	IP v4 & v6 Source Filtering as a protective and effective mechanism against ARP attacks	C/PC/NC
8.15.	Layer 2 ACLs—for filtering traffic at the MAC layer	C/PC/NC
8.16.	Layer 3/4 ACLs—for filtering traffic at the network layer including IPv6 ACL	C/PC/NC
8.17.	Multicast ACLs—for filtering IGMP traffic.	C/PC/NC
8.18.	Security ACLs—for improving network security	C/PC/NC
8.19.	User profile (UNP) time-based policy network authorization	C/PC/NC
8.20.	User profile (UNP) location-based policy network authorization	C/PC/NC
8.21.	The minimum password size range is 1-30 characters.	C/PC/NC
8.22.	Allows the switch to be authenticated as a supplicant device using X.509 certificates.	C/PC/NC

9. Quality of Service (QoS) features

The switch must support the following:

9.1.	Eight hardware-based queues per port for flexible QoS management	C/PC/NC
9.2.	Traffic prioritization - Flow-based QoS	C/PC/NC
9.3.	Flow-based traffic policing and bandwidth management	C/PC/NC
9.4.	32-bit IPv4/128-bit IPv6 non-contiguous mask classification	C/PC/NC
9.5.	Egress traffic shaping	C/PC/NC
9.6.	DiffServ architecture	C/PC/NC
9.7.	Lossless Virtual Output Queuing (VOQ) with configurable scheduling algorithms	C/PC/NC
9.8.	Congestion avoidance: IEEE 802.3x Flow Control (FC)	C/PC/NC
9.9.	Standard 802.1p CoS and DSCP field classification provided, using marking and reclassification on a per-packet basis by source and	C/PC/NC

	destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number.	
9.10.	Automatic QoS that simplifies QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect IP phones, classify traffic, and help enable egress queue configuration.	C/PC/NC

10. Data Center features

The switch must support the following:

10.1.	Dynamic Virtual Network Profiles (vNP) defining network access based on profile criteria (instead of mac address, IP address or port)	C/PC/NC
10.2.	IEEE 802.1aq Shortest Path bridging (SPB-M)	C/PC/NC
10.3.	Virtual eXtensible Local Area Network (VXLAN)	C/PC/NC
10.4.	Support seamless VM mobility by classifying the incoming server traffic based on MAC address, IP address or VLAN tag and assign an appropriate profile to the servers. The profile will determine the VLAN, priority, security and rate limiting parameters of that servers	C/PC/NC

11. Switch management and operation features

The switch must support the following:

11.1.	Fully programmable RESTful web services interface with XML and JSON support. The API enables access to Command Line Interface (CLI) and individual management information base (MIB) objects.	C/PC/NC
11.2.	File upload using USB, Trivial File Transfer Protocol (TFTP), FTP, SFTP or secure copy (SCP) over IPv4/IPv6	C/PC/NC
11.3.	Multiple microcode/OS image support with fallback recovery	C/PC/NC
11.4.	Support seamless VM mobility by classifying the incoming server traffic based on MAC address, IP address or VLAN tag and assign an appropriate profile to the servers. The profile will determine the VLAN, priority, security and rate limiting parameters of that servers	C/PC/NC
11.5.	Loopback IP address support for management-per-service	C/PC/NC
11.6.	Intuitive CLI in a scriptable BASH environment via console, Telnet, or Secure Shell (SSH) v2 over IPv4/IPv6	C/PC/NC
11.7.	Powerful WebView Graphical Web Interface via HTTP and HTTPS over IPv4/IPv6	C/PC/NC

11.8.	This feature allows for a USB-to-Ethernet interface for switches that lack an OOB management port. This interface is treated just like an OOB interface. All functions and CLIs related to an OOB management port are applicable to the USB-to-Ethernet dongle.	C/PC/NC
11.9.	This feature allows for applying an ACL on the EMP port of the switch. It enables policy-based routing on the EMP ports. The configuration is enabled using the empacl policy-list type.	C/PC/NC
11.10.	Policy- and port-based mirroring	C/PC/NC
11.11.	Remote port mirroring	C/PC/NC
11.12.	sFlow v5 and Remote Network Monitoring (RMON)	C/PC/NC
11.13.	SFLOW can be configured on non-default VRF. The OmniSwitch allows configuration of non-default VRF on SFLOW receiver, sampler, and poller.	C/PC/NC
11.14.	Integrated with Alcatel-Lucent OmniVista® products for network management	C/PC/NC
11.15.	Cloud ready with Alcatel-Lucent OmniVista® Cirrus to offer a secure, resilient and scalable cloud-based network management	C/PC/NC
11.16.	The equipment can work in a “thin client” mode. In this mode no configuration can be saved in the “Running” directory of the switch. A basic configuration with minimal network reachability configuration is stored on the switch running directory. The final configuration of a thin client is pushed by a Network Management System (NMS).	C/PC/NC
11.17.	Dynamic Host Configuration Protocol (DHCP) relay for IPv4/IPv6	C/PC/NC
11.18.	IEEE 802.1AB Link Layer Discover Protocol (LLDP) with Media Endpoint Discover (MED) extensions	C/PC/NC
11.19.	Network Time Protocol (NTP)	C/PC/NC

12. Access authentication security features

The switch must support the following:

12.1.	Restricts access to the switch only for certain IP addresses (configured as management station).	C/PC/NC
12.2.	Bans those IP addresses permanently from further access on invalid authentication attempts reaching threshold limit.	C/PC/NC
12.3.	Provides option to configure privileges for all access types, align IP services dynamically with AAA authentication configuration	C/PC/NC
12.4.	Restricts only one session per user.	C/PC/NC
12.5.	Option to configure with user passwords SHA-224/256 (SHA-2) or SHA-2+AES encryption	C/PC/NC
12.6.	SSH/SSL Pub Key hashed with SHA2	C/PC/NC
12.7.	Separate user password for SNMPv3 frame authentication/encryption.	C/PC/NC
12.8.	Support for both DSA 1024 and RSA 2048 public key algorithms for SSH private and SSH public keys	C/PC/NC
12.9.	Provide option to verify the integrity of the images in each directory, matching with the SHA-2 (SHA256 or 512 key) shared along with the image file	C/PC/NC
12.10.	Process Self-Test functional commands to view the major hardware and software process status	C/PC/NC
12.11.	Support of TLS 1.2 version for TLS connections	C/PC/NC
12.12.	Valid ASA credentials need to be provided to access SWLOG content	C/PC/NC

13. Software Defined Networking (SDN) features

The switch must support the following:

13.1.	Programmable AOS RESTful API	C/PC/NC
13.2.	Fully programmable OpenFlow 1.3.1 and 1.0 agent for control of native OpenFlow and hybrid ports	C/PC/NC
13.3.	OpenStack networking plug-in compatible with Grizzly or higher	C/PC/NC
13.4.	Software-controlled VXLAN hardware VTEP gateway (Verify model support based on the AOS 8.7R2, 8.7R3, 8.8R1, or 8.9R1 releases) *	C/PC/NC

14. Other key software features:

The switch must support the following:

14.1.	The switch must support out-of-band management and monitoring capability that bypasses the network modules and offer remote management to the management module directly	C/PC/NC
14.2.	The switch must support intuitive CLI in a scriptable Python and Bash environment through console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6	C/PC/NC
14.3.	The switch must support high availability hardware Virtual eXtensible LAN (VXLAN) Virtual Tunnel End Point (VTEP) gateway to support layer 2 overlay networks that are used to segment and tunnel device traffic through a data center or cloud network infrastructure (Verify model support based on the releases)	C/PC/NC
14.4.	The switch must support built-in cloud agent which will perform a call home and offer the capability to be managed by a cloud-based management service. The same switch must also be able to be managed by on-premises management server as a back-up.	C/PC/NC
14.5.	The switch must support a fabric technology to enable self-configuration, self-attachment, and self-healing of the network. This Auto-Fabric functionality helps eliminate many manual tasks and human errors during the deployment processes.	C/PC/NC
14.6.	The switch must come with IoT Device Profiling which uses DHCP finger printing and MAC OUI (device vendors) to identify IoT devices	C/PC/NC
14.7.	The switch must have the capability to propagate switch configurations, such as user profiles or device profiling signature across the network to other AOS switches.	C/PC/NC

15. ITU-T recommendations

The switch must support the following:

15.1.	ITU-T G.8032/Y.1344 2010: Ethernet Ring Protection (ERPV2)	C/PC/NC
-------	--	---------

16. Certifications

The switch must support the following:

16.1.	The switch proposed must possess a Common Criteria certification, ensuring compliance with internationally recognized security standards such as EAL2+ and NDcPP for network devices.	C/PC/NC
16.2.	The switch proposed must hold a valid Federal Information Processing Standards (FIPS) certification, meeting the designated FIPS publication 140-2.	C/PC/NC
16.3.	The switch proposed must hold a valid interoperability test certification, in line with standards set by Joint Interoperability Test Command (JITC) test agency to ensure the switch is certified for military uses.	C/PC/NC
16.4.	The switch proposed must comply with specified Trade Agreement Act (TAA) to be in accordance with valid applicable commercial law	C/PC/NC

17. Video surveillance

The switch must support the following:

17.1.	The switch support plugins that enable remote troubleshooting for common camera issues directly from the video surveillance management system.	C/PC/NC
-------	--	---------