



HPE Aruba Networking CX 5420 Switch Series

Key features

- Powerful, modular, intelligent Layer 3 chassis switch with BGP, VSX, OSPF, and robust QoS
- High performance switching up to 960 Gbps in non-blocking bandwidth and up to 714 Mpps for forwarding
- High availability VSX live upgrades, redundant power supplies, and N+1 redundant fans
- High capacity HPE Smart Rate 10GbE multi-gigabit for up to 90W Class-8 PoE
- High speed 6-line card slots with up to 160 Gb/s forwarding per slot, line rate at 64 bytes
- Intelligent monitoring, visibility, and remediation with HPE Aruba Networking Network Analytics Engine (NAE)
- Single pane of glass management with HPE Aruba Networking Central across wired, wireless, and WAN
- Support for automated configuration and verification with HPE Aruba Networking NetEdit. Secure and simple access for users and IoT devices via HPE Aruba Networking dynamic segmentation

Product overview

HPE Aruba Networking CX 5420 chassis switches are modern, flexible, intelligent, and modular making them optimal for access, small core, and aggregation deployments. Designed for operational efficiency, CX 5420 chassis switches feature built-in MACsec¹ hardware capability, analytics, and automation — providing an enterprise-class access layer solution that's easy-to-deploy, simple, secure, and resilient.

Part of the HPE Aruba Networking CX switching portfolio, CX 5420 chassis switches were built from the ground up with cutting-edge hardware, software, and analytics and automation tools, and are ideal for small and medium campus and branch networks.

CX 5420 chassis switches combine a modern, fully programmable OS with the HPE Aruba Networking Network Analytics Engine for superior monitoring and troubleshooting capabilities across the network.

A powerful HPE Aruba Networking Gen7 ASIC architecture delivers performance and feature support with flexible programmability for tomorrow's applications. The HPE Aruba Networking Virtual Switching Extension (VSX) with live upgrades provides high availability, fast, non-disruptive upgrades, and simplified management. This advanced modular 4U chassis switch offers performance up to 960 Gbps with low latency, six half-width line card slots with line rate at 64 bytes, and up to 90W Smart Rate 10 GbE PoE. The Layer 3 chassis provide BGP/OSFP/RIP/PIM support with single data-plane VRF and management VRF.

HPE Aruba Networking dynamic segmentation extends HPE Aruba Networking's wireless role-based policy capability to HPE Aruba Networking wired switches. This means the same security, user experience, and simplified IT management is uniform throughout the network.

Regardless of how users and IoT devices connect, consistent policies are enforced across wired and wireless networks, keeping traffic secure and separate.

Product differentiators

The HPE Aruba Networking CX 5420 Switch Series is based on the HPE Aruba Networking CX Operating System (AOS-CX), a modern, database-driven operating system that automates and simplifies many critical and complex network tasks.

A built-in time series database to utilize software scripts for historical troubleshooting and analysis of past trends. This helps predict and avoid future problems caused by scale, security, and performance bottlenecks.

AOS-CX is built on a modular Linux[®] architecture with a stateful database, providing it the following capabilities:

- Easy access to all network state information allows unique visibility and analytics
- REST APIs and Python scripting for fine-grained programmability of network tasks
- A microservices architecture that enables full integration with other workflow systems and services
- Continual state synchronization for superior fault tolerance and high availability
- Continuous telemetry data with WebSocket subscriptions for event-driven automation
- Software processes that communicate with the database rather than each other, ensuring near real-time state and resiliency and allowing individual software modules to be independently upgraded for higher availability

Every CX switch includes AOS-CX at no cost and an active, perpetual set of native features, providing everything needed to deploy, connect, and troubleshoot an enterprise network, including:

- Network Analytics Engine (NAE)
- Dynamic segmentation
- High availability and resiliency
- Quality of Service (QoS)
- Layer 2 switching
- Layer 3 services and routing
- IP Multicast
- Network security
- Support for NetEdit software

HPE Aruba Networking Central — unified single pane of glass management

HPE Aruba Networking Central is an AI-powered solution that simplifies IT operations, improves agility, and reduces costs by unifying management of all network infrastructure. Built for enterprise-grade resiliency and security, while simple enough for smaller businesses with limited IT staff, Central is your single point of visibility and control that spans the entire network — from branch to data center, wired and wireless LAN to WAN.

Available as a cloud-based or an on-premises solution, HPE Aruba Networking Central simplifies day 0 through day 2 operations. It offers streamlined workflows for virtual switch stack creation, automated monitoring using AI-powered insights and NAE, and a unified view of all devices and users, both wired and wireless. Comprehensive switch management capabilities include configuration, on boarding, monitoring, troubleshooting, and reporting.

An HPE Aruba Networking Central Advanced license expands these capabilities with premium security and AIOps, including the HPE Aruba Networking Central NetConductor Fabric Wizard and Policy Manager to enable dynamic segmentation.

With the HPE Aruba Networking Central Advanced license there is no need to purchase a CX Advanced license. This streamlines operational efficiency, reducing the need to keep track of multiple licenses, active terms, and renewal dates. For more information on HPE Aruba Networking Central licensing, see the [HPE Aruba Networking Central SaaS subscription ordering guide](#).

HPE Aruba Networking Network Analytics Engine — advanced monitoring and diagnostics

The HPE Aruba Networking Network Analytics Engine (NAE) automatically monitors and analyzes events that can impact network health, enhancing visibility and troubleshooting.

Advanced telemetry and automation provide easy identification and troubleshooting of network, system, application, and security related issues, using Python agents, CLI-based agents, and REST APIs.

The Time Series Database (TSDB) stores configuration and operational state data, to quickly resolve network issues. The data may also be used to analyze trends, identify anomalies, and predict future capacity requirements.

HPE Aruba Networking Central uses NAE and agents to deliver switch monitoring, analytics, and enhanced troubleshooting for wired assurance. HPE Aruba Networking NetEdit and third-party tools such as ServiceNow and Slack provide intelligence to integrate NAE alerts into IT service management processes, speeding problem resolution.

HPE Aruba Networking NetEdit — automated switch configuration and management

The HPE Aruba Networking CX portfolio can orchestrate multiple switch configuration changes for smooth end-to-end service rollouts. HPE Aruba Networking NetEdit introduces automation for rapid network-wide changes and ensures policy conformance for post-network updates. Intelligent capabilities include search, edit, validation (including conformance checking), deployment, and audit features.

- Centralized configuration with validation for consistency and compliance
- Simultaneous viewing and editing of multiple configurations to save time
- Customized validation tests for corporate compliance and network change analysis
- Automated large-scale configuration deployment without programming
- Visibility into network health and topology via HPE Aruba Networking NAE integration

Note: A separate software license is required to use NetEdit.

HPE Aruba Networking CX Mobile App — true deployment convenience

This easy-to-use mobile app simplifies connecting and managing HPE Aruba Networking CX 5420 chassis switches for any size project. Switch information can also be imported into HPE Aruba Networking NetEdit for simplified configuration management and to continuously validate conformance of configurations anywhere in the network.

HPE Aruba Networking ASICs — programmable innovation

With over 30 years of continuous investment, HPE Aruba Networking's ASICs form the basis for innovative and agile software feature advancements, improved performance, and deep visibility. These programmable ASICs are purpose built for a tighter integration of switch hardware and software within campus and data center architectures to optimize performance and capacity. Flexible ASIC resources enable HPE Aruba Networking's NAE solution to inspect all data, for superior analytics capabilities. The HPE Aruba Networking CX 5420 chassis switch is based on HPE Aruba Networking Gen7 ASIC architecture.

HPE Aruba Networking dynamic segmentation — campus and branch fabric

Providing seamless mobility, consistent policy enforcement, and automated configurations, HPE Aruba Networking dynamic segmentation is ideal for wired and wireless clients for networks of all sizes. It unifies role-based access and policy enforcement across LAN, WLAN, and SD-WAN networks with centralized policy definition and dedicated enforcement points. This ensures that users and devices can only communicate with destinations consistent with their role, keeping traffic secure and separate. Dynamic segmentation establishes least privilege access to IT resources by segmenting traffic based on identity, a fundamental concept of both zero trust and SASE frameworks, which base trust on roles and policies, not on where and how a user or device connects.

The solution begins with colorless ports and role-based microsegmentation technologies. Colorless ports allow wired clients to connect to any switch port, using RADIUS-based control to automate configuration. This eliminates the need for manual onboarding of clients, including IoT devices, onto the network.

Role-based microsegmentation reduces subnet and VLAN sprawl, simplifies policy definition and employs client user roles for scalable policy enforcement. Independent of network constructs such as VLANs and VRFs, clients can be grouped into user roles based on their identity, which extends the colorless ports to the centralized overlay fabric. This enables client onboarding using automatic tunnel creation based on the associated user roles policy. The user roles policy provides a choice between microsegmentation (using centralized and unified policy enforcement for wireless and wired traffic with Layer 7 stateful firewall on gateways) or a distributed approach (using Layer 4 role-role ACL on switches).

Dynamic segmentation enables scale and flexibility in network design by stretching VLANs and subnets across the network using VXLAN overlay fabric with Group Based Policy tagging to transport source role. The CX 5420 chassis switch attaches to the VXLAN Fabric as an Extended-Edge VTEP with static VXLAN to stub VTEP.

This switch series supports VXLAN-GBP-based policies to enable role-based microsegmentation, and when used in a HPE Aruba Networking Central NetConductor Extended-Edge campus solution, forms static VXLAN-GBP tunnels to fabric edge devices.

Mobility and IoT performance

The HPE Aruba Networking CX 5420 chassis switch uses the latest HPE Aruba Networking Gen7 ASICs. This ensures very low latency, increased packet buffering, and adaptive power consumption. Wire speed switching and routing ensure the demands of bandwidth-intensive applications are met today and in the future. Each switch includes the following:

- Up to 960 Gbps non-blocking bandwidth and up to 714 Mpps for forwarding available.
- Selectable queue configurations that increase performance by defining the number of queues and buffer associated memory

HPE Aruba Networking Virtual Switching Extension (VSX)

AOS-CX maintains a synchronous state across dual-control planes to enable simplified carrier-class high availability through HPE Aruba Networking Virtual Switching Extension (VSX).

HPE Aruba Networking VSX enables high availability during upgrades or control plane events. Features include:

- Continuous configuration synchronization via AOS-CX
- Operational simplicity and usability for easy configuration
- High availability by design during upgrades, including support for VSX Live Upgrade with LACP traffic draining

Ideal for SMB and branch environments

Whether in a branch office or small to midsize environment, you can choose these 4U modular models with rear slots for hot swappable power supplies, allowing customized PoE requirements. Additional features include:

- Flexibility to mix HPE Aruba Networking 5420 modules within a single chassis switch to meet deployment requirements
- Compact 6 slot (4 RU) support a choice of line cards and redundant, half-width management modules
- Industry standard IEEE 802.3bt High Power PoE support offers up to 90W of Class 8 PoE power per port for the latest APs and IoT devices
- Always-on PoE for high availability that supplies PoE power even during scheduled reboots and firmware upgrades

- Quick PoE provides PoE power to powered devices as soon as the switch is plugged into AC power, allowing the device to initialize at same time the switch OS boots up
- Support for pre-standard PoE detection to power legacy PoE devices
- Support for Energy Efficient Ethernet IEEE 802.3az to reduce power consumption during low network traffic periods
- Auto-MDIX for automatic adjustments to straight- through or crossover cables on 10/100/1000, Smart Rate, and 10GBASE-T ports
- Unsupported Transceiver Mode (UTM) to insert and enable all unsupported 100M through 25G transceivers and cables. (No warranty or support for the transceiver/cable is provided when this feature is used)
- IPv6 capabilities include:
 - IPv6 host to manage switches in an IPv6 network
 - Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols
 - MLD snooping to forward IPv6 multicast traffic to the appropriate interface
 - IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic
 - IPv6 routing supports Static, MP-BGP, RIPng, and OSPFv3 protocols
 - Security for RA guard, DHCPv6 protection, dynamic IPv6 lockdown, ND snooping, IPv6 Destination Guard, IPv6 DHCP Guard, and IPv6 Router Advertisement Guard
- Jumbo frames for high performance backups and disaster-recovery systems with a maximum frame size of 9198 bytes
- Packet storm protection against broadcast and multicast storms with user-defined thresholds
- Smart link for simple, fast-converging link redundancy and load balancing with dual uplinks to avoid Spanning Tree complexities
- Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops in STP-based networks
- IEEE 802.3ad LACP supports up to 144 LAGs, each with up to 16 links per LAG, providing support for static or dynamic groups and a user-selectable hashing algorithm
- IEEE 802.1s Multiple Spanning Tree for high link availability in VLAN environments (where multiple Spanning Trees are required) and legacy support for IEEE 802.1d and IEEE 802.1w
- IEEE 802.3ad Link Aggregation Control protocol (LACP) and port trunking supports static and dynamic trunks, with each trunk supporting up to sixteen links (ports) per static trunk
- Hot-patching support for standalone.

Quality of Service (QoS) features

The HPE Aruba Networking CX 5420 Series includes the following to support congestion actions and traffic prioritization:

- Strict priority (SP) queuing and Deficit Weighted Round Robin (DWRR)
- Traffic prioritization (IEEE 802.1p) for real-time classification
- Class of Service (CoS) to set IEEE 802.1p priority tags based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums
- Per-queue limiting of transmission rates for egressing frames using Egress Queue Shaping (EQS)
- Large buffers for graceful congestion management

Simplified configuration and management

In addition to HPE Aruba Networking Central, the HPE Networking CX Mobile App, HPE Aruba Networking NetEdit and HPE Aruba Networking Network Analytics Engine, the 5420 Switch Series offers the following:

- Built-in programmable and easy to use REST API interface
- Simple day 0 provisioning
- Scalable ASIC-based wire speed network monitoring and accounting with no impact on network performance, allowing network operators to gather a variety of network statistics and information for capacity planning and real-time network monitoring
- Management interface control enables or disables each of the following depending on security preferences, console port, or reset button

High availability and resiliency

To maximize uptime, we offer high availability and multicast features for Layer 3 deployments, including:

- Hot swappable power supplies
 - N+1 and N+N redundancy for high reliability in case of power line or supply failure
 - Up to 4 power supplies to increase total available PoE power
- Virtual Router Redundancy Protocol (VRRP) allows groups of two routers to dynamically create highly available routed environments in IPv4 and IPv6 networks

- Industry-standard CLI with a hierarchical structure for reduced training time and expense and increased productivity in multivendor environments
- Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access
- sFlow® (RFC 3176) ASIC-based wire speed provides network monitoring and accounting with no impact on network performance, so network operators can gather a variety of statistics and information for capacity planning and real-time network monitoring
- Supports SNMP (v2c/v3) and a wide range of read, write, and trap capabilities for industry-standard Management Information Base (MIB), private extensions, and common use cases, such as system, port, PoE, and VLAN management
- Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group. RMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events
- Support for TFTP and SFTP provides different mechanisms for configuration updates. Trivial FTP (TFTP) allows bidirectional transfers over a TCP/IP network. Secure File Transfer Protocol (SFTP) runs over an SSH tunnel for additional security
- Debug and sampler utility supports ping and traceroute for IPv4 and IPv6
- Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients so timekeeping remains consistent among all network clock-dependent devices so devices can provide diverse applications based on the consistent time
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications
- Dual flash images provide independent primary and secondary operating system files for backup while upgrading
- Multiple configuration files can be stored to a flash image
- Ingress and egress port monitoring enable more efficient network problem solving
- Unidirectional link detection (UDLD) monitors links between two switches and blocks the ports on both ends of the link if the link goes down at any point
- IP SLA for Voice monitors quality of voice traffic using the UDP Jitter and UDP Jitter for VoIP tests

Layer 2 switching

The following layer 2 services are supported:

- VLAN support and tagging for IEEE 802.1Q (4094 VLAN IDs)
- Jumbo packet for improved large data transfer performance; supports frame size of up to 9198 bytes
- IEEE 802.1v protocol VLANs isolate select non-IPv4 protocols automatically into their own VLANs
- Rapid Per-VLAN Spanning Tree (RPVST+) allows each VLAN to build a separate Spanning Tree to improve link bandwidth usage and is compatible with PVST+
- MVRP allows automatic learning and dynamic assignment of VLANs
- Bridge Protocol Data Unit (BPDU) tunnelling Transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs
- Port mirroring duplicates port traffic (ingress and egress) to a monitoring port; supports 4 mirroring groups
- VXLAN encapsulation tunneling protocol for overlay network that enables a more scalable virtual network deployment
- STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- Internet Group Management Protocol (IGMP) controls and manages the flooding of multicast packets in a Layer 2 network
- QinQ improves VLAN utilization by adding another 802.1Q tag to tagged packets

Layer 3 services

The following layer 3 services are supported:

- Bidirectional Forwarding Detection (BFD) enables link connectivity monitoring and reduces network convergence time for static route, OSPFv2 and VRRP
- Address Resolution Protocol (ARP) determines the MAC address of another IP host in the same subnet and supports static ARP; Gratuitous ARP allows detection of duplicate IP addresses. Proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network
- Dynamic Host Configuration Protocol (DHCP) simplifies the management of large IP networks and supports clients. DHCP Relay enables DHCP operation across subnets
- DHCP server centralizes and reduces the cost of IPv4 address management
- Domain Name System (DNS) provides a distributed database that translates domain names and IP addresses, simplifying network design and supporting client and server

- Internal loopback testing for maintenance and increased availability. Loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
- Route maps provide more control during route redistribution and allow filtering and altering of route metrics

Layer 3 routing

The following layer 3 routing services are supported:

- Border Gateway Protocol (BGP) provides IPv4 and IPv6 routing, which is scalable, robust, and flexible
- Border Gateway Protocol 4 (BGP 4) delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors. It uses TCP for enhanced reliability for the route discovery process, reduces bandwidth consumption by advertising only incremental updates, supports extensive policies for increased flexibility and scales to very large networks with graceful restart capability
- Multi protocol BGP (MP BGP) enables sharing of IPv6 routes using BGP and connections to BGP peers using IPv6
- Routing Information Protocol version 2 (RIPv2) provides an easy-to-configure routing protocol for small networks while RIPng provides support for small IPv6 networks
- Open Shortest Path First (OSPF) delivers faster convergence. It uses link-state routing Interior Gateway Protocol (IGP), which supports NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery
- OSPF provides OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing
- Static IP routing provides manually configured routing; includes ECMP capability
- Static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routes
- Policy-based routing uses a classifier to select traffic that can be forwarded based on policy set by the network administrator
- IP performance optimization provides a set of tools to improve IPv4 network performance. It includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities
- Dual IP stack maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
- mDNS (Multicast Domain Name System) Gateway enables discovery of mDNS groups across L3 boundaries
- Equal-Cost Multipath (ECMP) enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth

Security

The HPE Aruba Networking CX 5420 Switch Series comes with an integrated trusted platform module (TPM) for platform integrity. This ensures the boot process starts from a trusted combination of HPE Aruba Networking AOS-CX switches. Other security features include:

- AOS-CX uses FIPS 140-2 validated cryptography for protection of sensitive information
- Access control list (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network or for controlling network traffic to save resources. Rules can either deny or permit traffic forwarding and can be based on a Layer 2 header or a Layer 3 protocol header
- ACLs also provide filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN, per-port, or global basis
- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS+) is an authentication tool using TCP with encryption of the full authentication request, providing additional security
- Management access security for both on- and off- box authentication for administrative access.
- RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization service
- Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks
- Multiple user authentication methods with an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
- Web based authentication using Captive Portal on HPE Aruba Networking ClearPass is supported for use cases such as Guest Access and for devices that don't support 802.1x or MAC Auth.
- Supports MAC-based client authentication
- Concurrent IEEE 802.1X, web, and MAC authentication schemes per switch port accept up to 32 sessions of IEEE 802.1X, web, and MAC authentications
- Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3
- Switch CPU protection provides automatic protection against malicious network traffic attempts to shut down the switch

- ICMP throttling defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic
- Identity-driven ACL enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user
- STP BPDU port protection blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
- Dynamic IP lockdown works with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing
- Dynamic ARP protection blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data
- STP root guard protects the root bridge from malicious attacks or configuration mistakes
- Port security allows access only to specified MAC addresses, which can be learned or specified by the administrator
- MAC address lockout prevents specifically configured MAC addresses from connecting to the network
- Source-port filtering allows only specified ports to communicate with each other
- Secure shell encrypts all transmitted data for secure remote CLI access over IP networks
- Secure Sockets Layer (SSL) encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch
- Secure FTP allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file
- Critical Authentication Role ensures that important infrastructure devices such as IP phones are allowed network access even in the absence of a RADIUS server
- MAC pinning allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the client logs off or gets disconnected
- Security banner displays a customized security policy when users log in to the switch
- RadSec enables RADIUS authentication and accounting data to be passed safely and reliably across insecure networks
- Private VLAN (PVLAN) provides traffic isolation between users on the same VLAN. Typically, a switch port can only communicate with other ports in the same community and/or an uplink port, regardless of VLAN ID or destination MAC address. This extends network security by restricting peer-peer communication to prevent a variety of malicious attacks.
- Auto VLAN Creation automates VLAN creation on access switches for authenticated clients
- DHCP smart relay allows the DHCP relay agent to use secondary IP addresses when the DHCP server does not reply to the DHCP-OFFER message
- Supports device fingerprinting to identify a device based on collected attributes and analyze information using ClearPass Device Insight. This provides better visibility and informs network access control decisions
- IEEE 802.1AE MACsec¹ provides switch-to-switch and switch-to-host security on a link between two ports using standard encryption and authentication, available on uplink and downlink ports

Multicast

- IGMP Snooping allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN
- Multicast Listener Discovery (MLD) enables discovery of IPv6 multicast listeners; supports MLD v1 and v2
- Protocol Independent Multicast (PIM) defines modes of IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information. Support for PIM Sparse Mode (SM), Source-Specific Multicast (SSM), and Dense Mode (DM) for both IPv4 and IPv6
- Internet Group Management Protocol (IGMP) utilizes Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3

Convergence

- IP multicast routing includes PIM Sparse, Source-Specific Multicast, and Dense modes to route IP multicast traffic
- IP multicast snooping (data-driven IGMP) prevents flooding of IP multicast traffic
- Protocol Independent Multicast for IPv6 supports one-to-many and many-to-many media casting use cases such as IPTV over IPv6 networks
- LLDP-MED (Media Endpoint Discovery) defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- PoE allocations supports multiple methods (allocation by usage or class, with LLDP and LLDP-MED to allocate PoE power for more efficient power management and energy savings)
- Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones

¹ Hardware capable. Software support available in future releases.

Additional information

- Green initiative support for RoHS (EN 50581:2012) and WEEE regulations
- TAA compliant models available

Customer first, customer last support

When your network is important to your business, then your business needs the backing of HPE Aruba Networking Support Services. Partner with HPE Aruba Networking product experts to increase your team productivity, keep pace with technology advances, software releases, and obtain break-fix support.

- Foundational Care for HPE Aruba Networking support services include priority access to HPE Aruba Networking Technical Assistance Center (TAC) engineers 24x7x365, flexible hardware and on-site support options, and total coverage for HPE Aruba Networking products. HPE Aruba Networking switches with assigned HPE Aruba Networking Central subscriptions also have an option for additional hardware support only.
- HPE Aruba Networking Pro Care adds fast access to senior TAC engineers, who are assigned as a single point of contact for case management, reducing the time spent addressing and resolving issues.

For complete details on Foundational Care and HPE Aruba Networking Pro Care, please visit:

hpe.com/us/en/networking/hpe-aruba-networking-support-services.html

Warranty, services, and support

- Limited Lifetime Warranty, see arubanetworks.com/support-services/product-warranties for warranty and support information included with your product purchase
- For more detailed information on HPE Aruba Networking AOS-CX software release and features, please visit the [HPE Aruba Networking CX Operating System Switch Software Documentation Portal](https://hpe.com/us/en/networking/aos-cx/operating-system-switch-software-documentation-portal)
- Explore and compare switch features for each platform and software release on the [HPE Aruba Networking Switch Feature Navigator](https://hpe.com/us/en/networking/switch-feature-navigator)
- For software releases and documentation, refer to the [AOS-CX Switch Software Documentation Portal](https://hpe.com/us/en/networking/aos-cx/switch-software-documentation-portal)
- For support and services information, visit [HPE Aruba Networking Support Services](https://hpe.com/us/en/networking/support-services)

Technical specifications

HPE Aruba Networking 5420 6-slot Switch (SOU59A)	
Description	1 x 5420 6-slot Chassis (SOU60A) 1 x 5420 Management Module (SOU55A) 1 x Fan Tray (SOU54A) 1 open management slot 6 open line card module slots Supports the management card in the open management slots: SOU55A, SOU58A Supports any of the following line cards in the open slots: SOU62A, SOU66A, SOU65A, SOU61A, SOU67A, SOU63A, SOU64A, SOU68A SOU72A, SOU76A, SOU75A, SOU71A, SOU77A, SOU73A, SOU74A, SOU78A Supports PoE Standards IEEE 802.3af, 802.3at, 802.3bt (up to 90W)
Power supplies	Supports 4 field replaceable and hot-swappable power supply slots Supported power supplies: SOU53A PoE availability is dependent on the number of management modules, line cards, fan trays and the number of power supplies used. Power supplies are not included; order separately.
Fans	1 field-replaceable and hot-swappable system fan tray
Dimensions	(H) 17.41 cm x (W) 44.25 cm x (D) x 44.74 cm (6.85" x 17.42" x 17.6")
Configuration weight	15.73 kg (34.7 lb)
Additional specifications	
CPU	Management Module: AMD Ryzen Quad Core V1500B x86 processor @ 2.2GHz
Memory and flash	Management Module: 16GB DDR4 SODIMM with ECC, 32GB eMMC Flash Memory

Technical specifications (continued)

HPE Aruba Networking 5420 6-slot Switch (SOU59A)	
Packet buffer	64MB packet buffer memory shared dynamically among ports
Performance	
Model switching capacity	960 Gbps (480 Gbps in + 480 Gbps out)
Model throughput capacity	714 Mpps
Average latency (LIFO-64-bytes packets)	2.5 micro sec
Switch Virtual Interface (SVI) (dual stack)	512
IPv4 host table (ARP)	25,600
IPv6 host table (ND)	25,600
IPv4 unicast routes	16,384
IPv6 unicast routes	8,192
MAC table capacity	32,768
IGMP groups	2,048
MLD groups	2,048
IPv4/IPv6/MAC ACL entries (ingress)	MAC – 10,233 IPv4 – 10,233 IPv6 – 2,558 (1/4 of scale)
IPv4/IPv6/MAC ACL entries (egress)	MAC – 5,113 IPv4 – 5,113 IPv6 – 1,278 (1/4 of scale)
Environment	
Operating temperature	32°F to 113°F (0°C to 45°C), up to 5,000 feet Derate 1°C every 1,000 feet from 5,000 feet to 10,000 feet Can support excursion to 131°F (55°C) for short periods of time
Operating relative humidity	5% to 95% relative humidity at 113°F (45°C), non-condensing
Non-operating	–40°F to 158°F (–40°C to 70°C) up to 15,000 feet
Non-operating storage relative humidity	5% to 95% relative humidity at 149°F (65°C), non-condensing
Max operating altitude	Up to 10,000 feet (3 km)
Max non-operating altitude	Up to 15,000 feet (4.5 km)

Technical specifications (continued)

HPE Aruba Networking 5420 6-slot Switch (SOU59A)	
Acoustics	Sound power (LWAd): 4.7 Bel, Sound pressure (LpAm, Bystander): 44.6 dB when tested with 2x SOU53A power supply at low voltage line, loaded with 2 x SOU55A, 3 x SOU67A, 3 x SOU68A with a loading of 50% traffic on all ports Sound power (LWAd): 5.5 Bel, Sound pressure (LpAm, Bystander): 52.1 dB when tested with 4x SOU53A power supply at low voltage line, loaded with 2 x SOU55A, 6 x SOU66A and drawing a total of 2000W PoE, with a loading of 50% traffic on all ports
Primary airflow	Front to back
Electrical characteristics	
Frequency	50Hz/60Hz
AC voltage	SOU53A PSUs: 100-127/200-240VAC
Current	11.6A @ 100-127VAC 9A @ 200VAC 8A @ 208-240VAC
Power output	SOU53A: 1600W @ 200-240VAC, 1000W @ 100-127VAC
80plus.org certification	Platinum for SOU53A PSU
Safety	
	IEC 62368-1:2014 2nd Ed with all known national deviations IEC 62368-1:2018 3rd Ed with all known national deviations EN 62368-1:2014 +A11:2017 2nd Ed. EN IEC 62368-1:2020 +A11:2020 3rd Ed. UL 62368-1 3rd Ed./ CAN/CSA C22.2 No. 62368-1:19 CNS 15598-1:2020
Emissions	
	EN 55032:2015+A11:2020 Class A, CISPR 32:2015+A1:2019 Class A, FCC Part 15B Class A, VCCI 32-1 Class A, ICES-003 Class A, AS/NZS CISPR 32 Class A, CNS 15936:2016
Lasers	
	IEC 60825-1:2014/EN 60825-1:2014+A11:2021 Class 1 Laser
Immunity	
Generic	Directive 2014/35/EU
EN	CISPR 35:2016/EN 55035:2017+A11:2020
ESD	IEC 61000-4-2
Radiated	IEC 61000-4-3
EFT/Burst	IEC 61000-4-4

Technical specifications (continued)

HPE Aruba Networking 5420 6-slot Switch (SOU59A)	
Surge	IEC 61000-4-5
Conducted	IEC 61000-4-6
Power frequency magnetic field	IEC 61000-4-8
Voltage dips and interruptions	IEC 61000-4-11
Harmonics	EN IEC 61000-3-2
Flicker	EN IEC 61000-3-3
Mounting and enclosure	
Cable management kit and 2-post rack mounting kit included. 4-post rack mounting kit available separately	

Standards and protocols

- ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
- CPU DoS Protection
- Bootstrap Router (BSR) Mechanism for PIM, PIM WG draft-ietf-savi-mix
- IEEE 802.1AB-2005
- IEEE 802.1ak-2007
- IEEE 802.1AX-2008 Link Aggregation
- IEEE 802.1D MAC Bridges
- IEEE 802.1p Priority
- IEEE 802.1Q VLANs
- IEEE 802.1s Multiple Spanning Trees
- IEEE 802.1t-2001
- IEEE 802.1v VLAN classification by Protocol and Port
- IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae 10-Gigabit Ethernet
- IEEE 802.3af Power over Ethernet
- IEEE 802.3at Power over Ethernet
- IEEE 802.3az Energy Efficient Ethernet (EEE)
- IEEE 802.3bt Power over Ethernet
- IEEE 802.3z 1000BASE-X
- RFC 1122 Requirements for Internet Hosts — Communications Layers
- RFC 1215 Convention for defining traps for use with the SNMP
- RFC 1256 ICMP Router Discovery Messages
- RFC 1350 TFTP Protocol (revision 2)
- RFC 1393 Traceroute Using an IP Option
- RFC 1403 BGP OSPF Interaction
- RFC 1519 CIDR
- RFC 1542 BOOTP Extensions
- RFC 1583 OSPF Version 2
- RFC 1591 Domain Name System Structure and Delegation
- RFC 1657 Definitions of Managed Objects for BGP-4 using SMIv2
- RFC 1772 Application of the Border Gateway Protocol in the Internet
- RFC 1812 Requirements for IP Version 4 Router
- RFC 1918 Address Allocation for Private Internet
- RFC 1997 BGP Communities Attribute
- RFC 1998 An Application of the BGP Community Attribute in Multi-home Routing
- RFC 2131 DHCP
- RFC 2132 DHCP Options and BOOTP Vendor Extensions
- RFC 2236 IGMP
- RFC 2328 OSPF Version 2
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2402 IP Authentication Header
- RFC 2439 BGP Route Flap Damping
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2464 Transmission of IPv6 over Ethernet Networks
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2576 (Coexistence between SNMP V1, V2, V3)
- RFC 2579 (SMIv2 Text Conventions)
- RFC 2580 (SMIv2 Conformance)
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)
- RFC 2934 Protocol Independent Multicast MIB for IPv4
- RFC 3019 MLDv1 MIB
- RFC 3046 DHCP Relay Agent Information Option
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3065 Autonomous System Confederation for BGP
- RFC 3068 An Anycast Prefix for 6to4 Relay Route
- RFC 3137 OSPF Stub Router Advertisement sFlow
- RFC 3376 IGMPv3
- RFC 3417 (SNMP Transport Mappings)
- RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3484 Default Address Selection for IPv6
- RFC 3509 Alternative Implementations of OSPF Area Border Routers
- RFC 3575 IANA Considerations for RADIUS
- RFC 3623 Graceful OSPF Restart
- RFC 3768 VRRP

- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 3973 PIM Dense Mode
- RFC 4022 MIB for TCP
- RFC 4113 MIB for UDP
- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4251 The Secure Shell (SSH) Protocol
- RFC 4252 SSHv6 Authentication
- RFC 4253 SSHv6 Transport Layer
- RFC 4254 SSHv6 Connection
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4273 Definitions of Managed Objects for BGP-4
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4292 IP Forwarding Table MIB
- RFC 4293 Management Information Base for the Internet Protocol (IP)
- RFC 4360 BGP Extended Communities Attribute
- RFC 4419 Key Exchange for SSH
- RFC 4443 ICMPv6
- RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4541 IGMP & MLD Snooping Switch
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM Sparse Mode
- RFC 4607 Source-Specific Multicast for IP
- RFC 4675 RADIUS VLAN & Priority
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4861 IPv6 Neighbor Discovery
- RFC 4862 IPv6 Stateless Address Auto-configuration
- RFC 4940 IANA Considerations for OSPF
- RFC 5065 Autonomous System Confederation for BGP
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5340 OSPFv3 for IPv6
- RFC 5424 Syslog Protocol
- RFC 5492 Capabilities Advertisement with BGP-4
- RFC 5519 Multicast Group Membership Discovery MIB (MLDv2 only)
- RFC 5701 IPv6 Address Specific BGP Extended Community Attribute
- RFC 5722 Handling of Overlapping IPv6 Fragments
- RFC 5798 VRRP (exclude Accept Mode and sub-sec timer)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 6620 FCFS SAVI
- RFC 6987 OSPF Stub Router Advertisement
- RFC 7047 The Open vSwitch Database Management Protocol
- RFC 7313 Enhanced Route Refresh Capability for BGP-4
- RFC 768 User Datagram Protocol
- RFC 783 TFTP Protocol (revision 2)
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 813 Window and Acknowledgement Strategy in TCP
- RFC 815 IP datagram reassembly algorithms
- RFC 8201 Path MTU Discovery for IP version 6
- RFC 3065 Autonomous System Confederation for BGP
- RFC 3068 An Anycast prefix for 6to4 Relay Route
- RFC 3137 OSPF Stub Router Advertisement sFlow
- RFC 3376 IGMPv3
- RFC 3417 (SNMP Transport Mappings)
- RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3484 Default Address Selection for IPv6
- RFC 3509 Alternative Implementations of OSPF Area Border Routers
- RFC 3575 IANA Considerations for RADIUS
- RFC 3623 Graceful OSPF Restart
- RFC 3768 VRRP
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 3973 PIM Dense Mode
- RFC 4022 MIB for TCP
- RFC 4113 MIB for UDP
- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4251 The Secure Shell (SSH) Protocol
- RFC 4252 SSHv6 Authentication
- RFC 4253 SSHv6 Transport Layer
- RFC 4254 SSHv6 Connection
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4273 Definitions of Managed Objects for BGP-4
- RFC 4291 IP Version 6 Addressing Architecture
- RFC 4292 IP Forwarding Table MIB
- RFC 4293 Management Information Base for the Internet Protocol (IP)

- RFC 4360 BGP Extended Communities Attribute
- RFC 4419 Key Exchange for SSH
- RFC 4443 ICMPv6
- RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4541 IGMP & MLD Snooping Switch
- RFC 4552 Authentication/Confidentiality for OSPFv3
- RFC 4601 PIM Sparse Mode
- RFC 4607 Source-Specific Multicast for IP
- RFC 4675 RADIUS VLAN & Priority
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4861 IPv6 Neighbor Discovery
- RFC 4862 IPv6 Stateless Address Auto-configuration
- RFC 4940 IANA Considerations for OSPF
- RFC 5065 Autonomous System Confederation for BGP
- RFC 5095 Deprecation of Type O Routing Headers in IPv6
- RFC 5187 OSPFv3 Graceful Restart
- RFC 5340 OSPFv3 for IPv6
- RFC 5424 Syslog Protocol
- RFC 5492 Capabilities Advertisement with BGP-4
- RFC 5519 Multicast Group Membership Discovery MIB (MLDv2 only)
- RFC 5701 IPv6 Address Specific BGP Extended Community Attribute
- RFC 5722 Handling of Overlapping IPv6 Fragments
- RFC 5798 VRRP (exclude Accept Mode and sub-sec timer)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 6620 FCFS SAVI
- RFC 6987 OSPF Stub Router Advertisement
- RFC 7047 The Open vSwitch Database Management Protocol
- RFC 7313 Enhanced Route Refresh Capability for BGP-4
- RFC 768 User Datagram Protocol
- RFC 783 TFTP Protocol (revision 2)
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 813 Window and Acknowledgement Strategy in TCP
- RFC 815 IP Datagram Reassembly Algorithms
- RFC 8201 Path MTU Discovery for IP version 6
- RFC 826 ARP
- RFC 879 TCP Maximum Segment Size and Related Topics
- RFC 896 Congestion Control in IP/TCP Internetworks
- RFC 917 Internet subnets
- RFC 919 Broadcasting Internet Datagrams
- RFC 922 Broadcasting Internet Datagrams in the Presence of Subnets (IP_BROAD)
- RFC 925 Multi-LAN Address Resolution
- RFC 951 BOOTP
- RFC 1027 Proxy ARP
- SNMPv1/v2c/v3
- RFC 4861 IPv6 Neighbor Discovery
- RFC 4862 IPv6 Stateless Address Auto-configuration
- ITU-T Rec G.8032/Y.1344 Mar. 2010
- RFC 1757 Remote Network Monitoring Management Information Base
- 2.5G/5GBASE-T (IEEE 802.3bz-2016), 2.5G/5G NBASE-T
- 10GBASE-T (IEEE 802.3an-2006)
- 25-Gigabit Ethernet (IEEE 802.3by-2016, 802.3cc-2017)
- RFC 3101 OSPF Not-so-stubby-area Option
- RFC 4750 OSPFv2 MIB Partial Support no SetMIB

HPE Aruba Networking CX 5420 switches and accessories

Switch models

- HPE Aruba Networking 5420 6-slot TAA Switch (SOU69A)
- HPE Aruba Networking 5420 6-slot Switch (SOU59A)
- HPE Aruba Networking 5420 6-slot TAA Chassis (SOU70A)
- HPE Aruba Networking 5420 6-slot Chassis (SOU60A)

Modules

- HPE Aruba Networking 5420 TAA Management Module (SOU58A)
- HPE Aruba Networking 5420 Management Module (SOU55A)
- HPE Aruba Networking 5420 8p Smart Rate 1G/2.5G/5G/10G Class8 PoE TAA Module (SOU75A)
- HPE Aruba Networking 5420 8p Smart Rate 1G/2.5G/5G/10G Class8 PoE Module (SOU65A)
- HPE Aruba Networking 5420 8p SFP+ 1G/10G LRM TAA Module (SOU78A)
- HPE Aruba Networking 5420 8p SFP+ 1G/10G LRM Module (SOU68A)
- HPE Aruba Networking 5420 24p 10M/100M/1G TAA Module (SOU71A)

- HPE Aruba Networking 5420 24p SFP 1G TAA Module (SOU77A)
- HPE Aruba Networking 5420 24p SFP 1G Module (SOU67A)
- HPE Aruba Networking 5420 24p 10M/100M/1G Module (SOU61A)
- HPE Aruba Networking 5420 24p 10M/100M/1G Class4 PoE TAA Module (SOU72A)
- HPE Aruba Networking 5420 24p 10M/100M/1G Class4 PoE Module (SOU62A)
- HPE Aruba Networking 5420 20p 10M/100M/1G Class4 PoE 4p SFP+ 1G/10G TAA Module (SOU73A)
- HPE Aruba Networking 5420 20p 10M/100M/1G Class4 PoE 4p SFP+ 1G/10G Module (SOU63A)
- HPE Aruba Networking 5420 20p 10M/100M/1G Class4 PoE 2p SFP28 1G/10G/25G TAA Module (SOU74A)
- HPE Aruba Networking 5420 20p 10M/100M/1G Class4 PoE 2p SFP28 1G/10G/25G Module (SOU64A)
- HPE Aruba Networking 5420 16p Smart Rate 1G/2.5G/5G Class6 PoE TAA Module (SOU76A)
- HPE Aruba Networking 5420 16p Smart Rate 1G/2.5G/5G Class6 PoE Module (SOU66A)

Power supplies

- HPE Aruba Networking 5420 1600W AC Power Supply (SOU53A)

Accessories

- HPE Aruba Networking 5420 6-Slot Fan Tray (SOU54A)
- HPE Aruba Networking 5420 6-Slot Accessory Kit (SOU57A)
- HPE Aruba Networking 5420 2-post 6-slot Rack Kit (SOU56A)
- HPE Aruba Networking 5420 4-post 6-slot Rack Kit (S1T82A)

Cables

- HPE Aruba Networking 10G SFP+ to SFP+ 1m Direct Attach Copper Cable (J9281D)
- HPE Aruba Networking 10G SFP+ to SFP+ 3m Direct Attach Copper Cable (J9283D)
- HPE Aruba Networking 10G SFP+ to SFP+ 7m Direct Attach Copper Cable (J9285D)
- HPE Aruba Networking 25G SFP28 to SFP28 0.65m Direct Attach Copper Cable (JL487A)
- HPE Aruba Networking 25G SFP28 to SFP28 3m Direct Attach Copper Cable (JL488A)

- HPE Aruba Networking 25G SFP28 to SFP28 5m Direct Attach Copper Cable (JL489A)
- HPE Aruba Networking 25G SFP28 to SFP28 3m AOC (ROM44A)
- HPE Aruba Networking 25G SFP28 to SFP28 7m AOC (ROM45A)
- HPE Aruba Networking 25G SFP28 to SFP28 15m AOC (ROZ21A)

Transceivers¹

- HPE Aruba Networking 1G SFP LC SX 500m MMF Transceiver (J4858D)
- HPE Aruba Networking 1G SFP LC LX 10km SMF Transceiver (J4859D)
- HPE Aruba Networking 1G SFP LC LH 70km SMF Transceiver (J4860D)
- HPE Aruba Networking 1G SFP RJ45 T 100m Cat5e Transceiver (J8177D)
- HPE Aruba Networking 1G SFP RJ45 T 100m Cat5e Transceiver (J8177E)
- HPE Aruba Networking 100M SFP LC FX 2km MMF Transceiver (J9054D)²
- HPE Aruba Networking 10G SFP+LC SR 300m MMF Transceiver (J9150D)
- HPE Aruba Networking 10G SFP+LC LR 10km SMF Transceiver (J9151E)
- HPE Aruba Networking 10G SFP+LC LRM 220m MMF Transceiver (J9152D)
- HPE Aruba Networking 10G SFP+LC ER 40km SMF Transceiver (J9153D)
- HPE Aruba Networking 25G SFP28 LC SR 100m MMF Transceiver (JL484A)
- HPE Aruba Networking 25G SFP28 LC eSR 400m MMF Transceiver (JL485A)
- HPE Aruba Networking 25G SFP28 LC LR 10km SMF Transceiver (JL486A)
- HPE Aruba Networking 10GBASE-T SFP+RJ-45 30m Transceiver (JL653C)
- HPE Aruba Networking 1G SFP LC SX 500m MMF TAA Transceiver (JL745A)
- HPE Aruba Networking 1G SFP LC LX 10km SMF TAA Transceiver (JL746A)
- HPE Aruba Networking 1G SFP RFP45 100m Cat5e TAA Transceiver (JL747A)
- HPE Aruba Networking 10G SFP+ LC SR 300m MMF TAA Transceiver (JL748A)

¹ Consult the HPE Aruba Networking Operating System Switch and HPE Aruba Networking CX Operating System Transceiver Guides in the HPE Aruba Networking Support Portal for the minimum required software releases to support these transceivers. Guide also provides certain limitations for specific transceivers for use on switch models.

² J9054D 100FX transceiver is only supported in modules SOU63A/SOU73A, SOU67A/SOU77A, SOU68A/SOU78A.

- HPE Aruba Networking 10G SFP+ LC LR 10km SMF TAA Transceiver (JL749A)
- HPE Aruba Networking 10G LC BiDi 40km-D 1330/1270 XCVR (R9X54A)
- HPE Aruba Networking 10G LC BiDi 40km-U 1270/1330 XCVR (R9X55A)
- HPE Aruba Networking 25G ER LC 40km SMF Transceiver (SOV69A)
- HPE Aruba Networking 25G BiDi 10km-D 1330/1270 Transceiver (S1C96A)
- HPE Aruba Networking 25G BiDi 10km-U 1270/1330 Transceiver (S1C98A)

- HPE Aruba Networking Central On-Premises 64xx or 54xx Switch Foundational 5-Year Subscription E-STU (R8M12AAE)
- HPE Aruba Networking Central On-Premises 64xx or 54xx Switch Foundational 7-Year Subscription E-STU (R8M13AAE)
- HPE Aruba Networking Central On-Premises 64xx or 54xx Switch Foundational 10-Year Subscription E-STU (R8M14AAE)

For details and a complete listing of HPE Aruba Networking Central licensing options, please refer to the [HPE Aruba Networking Central data sheet](#).

Software

- HPE Aruba Networking NetEdit Single Node: 1-Year (JL639AAE)
- HPE Aruba Networking NetEdit Single Node: 3-Years (JL640AAE)

HPE Aruba Networking Central Foundational licenses

- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 1-Year Subscription E-STU (R8L80AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 3-Year Subscription E-STU (R8L81AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 5-Year Subscription E-STU (R8L82AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 7-Year Subscription E-STU (R8L83AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 10-Year Subscription E-STU (R8L84AAE)
- HPE Aruba Networking Central On-Premises 64xx or 54xx Switch Foundational 1-Year Subscription E-STU (R8M10AAE)
- HPE Aruba Networking Central On-Premises 64xx or 54xx Switch Foundational 3-Year Subscription E-STU (R8M11AAE)

HPE Aruba Networking Central advanced licenses

- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 1-Year Subscription E-STU (R8L80AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 3-Year Subscription E-STU (R8L81AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 5-Year Subscription E-STU (R8L82AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 7-Year Subscription E-STU (R8L83AAE)
- HPE Aruba Networking Central 64xx or 54xx Switch Foundational 10-Year Subscription E-STU (R8L84AAE)

Support

For HPE Aruba Networking Central hardware only support, 24x7 TAC support, and many other support options, go to the [Support Services Central SKU lookup tool](#).

Visit [HPE.com](#)

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

AMD is a trademark of Advanced Micro Devices, Inc. sFlow is a registered trademark of InMon Corp. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. All third-party marks are property of their respective owners.

a00143490ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

