HPE 830 Unified Wired-WLAN Switch Series

Key features

• Unified wired and wireless services for branch offices

• System-wide approach to WLAN reliability through Wi-Fi Clear Connect

• Flexible forwarding modes

• PoE+ capability

• 8-port and 24-port versions available

Product overview

The HPE 830 Unified Wired-WLAN Switch Series integrates both wireless controller and 1000 Mb/s Ethernet switch functions. The 830 Unified Wired-WLAN Switch Series supports up to 60 APs (depending on the model and through optional licensing) and provides 1000 Mb/s Ethernet ports, with each supporting a maximum of up to 30 W PoE+ power and IEEE 802.11a/b/g/n and IEEE 802.11ac APs and access devices while delivering unified wired and wireless access control functions. The HPE 830 24-Port PoE+ Unified Wired-WLAN Switch provides up to two 10GbE links via the optional Uplink Module modules on the rear panel to relieve transmission bottlenecks at the core of the WLAN network.

This series provides edge-to-core unified access and consistent WLAN services to the small and medium branch offices of enterprises that are deploying the HPE 10500/7500 20G Unified Wired-WLAN Module or HPE 870 Unified Wired-WLAN Appliance at their central (or main) offices.

The HPE 830 Unified Wired-WLAN Switch Series is part of the Hewlett Packard Enterprise Mobility solution.

Features and benefits

Management

• Wi-Fi Clear Connect

Provides a system-wide approach to help ensure WLAN reliability by proactively determining and adjusting to changing RF conditions and by identifying rogue activity and enforcing prevention policies, and optimizing WLAN performance by detecting interference from Wi-Fi and non-Wi-Fi sources using spectrum analysis capabilities built into specific HPE access points (refer to the HPE Access Point—Controller Compatibility Matrix)

• Advanced radio resource management

– Automatic radio power adjustments

Include real-time power adjustments based on changing environmental conditions and signal coverage adjustments

– Automatic radio channel

Provides intelligent channel switching and real-time interference detection

– Intelligent client load balancing

Balances the number of clients across multiple APs to improve AP and client throughput

– Airtime fairness

Helps ensure equal RF transmission time for wireless clients

• Spectrum analysis

– Signal detection/classification

Identifies source of RF interference, for example, Bluetooth®, cordless phones, and microwave ovens

– Evaluation of channel quality

Helps detect severe channel degradation and improves the reporting of poor RF performance

• Band Navigation

Enables automatic redirection of 5 GHz–capable clients to the less-congested 5 GHz spectrum

• Enterprise network management

Is provided by HPE Intelligent Management Center (IMC) platform software and the HPE IMC Wireless Services Manager Software Module, which effectively integrate traditionally disparate management tools into one easy-to-use interface

• Secure controller management

Manages the controller securely from a single location with IMC or any other SNMP management station; controller supports SNMPv3 as well as SSHv2 and SSL for secure CLI and Web management; console port is available as a pass-through to the switch console function

• Support for environments using Bonjour services

– Gateway: Allows discovery of Bonjour services located in a different layer-3 network

– HPE Zerocast: Eliminates Bonjour multicast traffic from the WLAN enabling scalable deployment of Apple devices with no performance impact on the Wi-Fi network

– Access control: Enables filters to be applied inbound and outbound (on the AP) to SSIDs, groups of or specific APs. User based filtering can block Bonjour traffic until the user is authenticated

- VLAN pooling

  Enables wireless clients to be dynamically assigned to different VLANs so administrators can assign different subnets to different clients in the same SSID. A VLAN pool can bind to multiple SSIDs

- Unified network visibility

  Provides visibility between a wired and wireless network using IEEE 802.1AB Link Layer Discovery Protocol (LLDP) and sFlow®

- AP Plug and Play (PnP)

  Provides zero-configuration capability. An AP without a predefined configuration file can connect to the WLAN controller and the WLAN Controller will provision it with the correct wireless configuration

- Policy based forwarding

  Simplifies the deployment of centralized or local forwarding. The policy-based mode allows user to classify data traffic based on ACL and choose local or centralized forwarding policy can be applied on a SSID or a specific user or a group of users

- AP grouping

  Enables an admin to easily apply AP-based or radio-based configurations to all the AP that are in the same group

- Staged Firmware Upgrades

  Enables an admin to selectively upgrade APs, typically a group of APs, to minimize the impact of upgrading large deployments of APs to a new version of firmware

- Custom antenna settings

  Allow the admin to select a custom antenna gain

Quality of Service (QoS)
- End-to-end QoS

  – Supports the DiffServ standard and IPv6 QoS; the QoS DiffServ model includes traffic classification and traffic policing, and fully implements six groups of services—EF, AF1 through AF4, and BE

- IEEE 802.1p prioritization

  Delivers data to devices based on the priority and type of traffic

- Class of Service (CoS)

  Sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ

Security
- Web-based authentication

  provides a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant

- IEEE 802.1X and RADIUS network logins

  supports port-based and SSID-based IEEE 802.1X authentication and accounting

- WEP, WPA2, or WPA encryption

  can be deployed at the AP to lock out unauthorized wireless access by authenticating users prior to granting network access; robust Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) encryption secures the data integrity of wireless traffic

- Integrated Wireless Intrusion Detection System (WIDS) support

  Provides support for hybrid and dedicated modes; detects flood, spoofing, and weak IV attacks; displays statistics (events) and history; supports configuration of detection policies

- Integrated Wireless Intrusion Prevention System (WIPS)

  Automatically identifies and classifies all APs and stations; enables packet-trigger containment via knowledge-based heuristics; protects against honeypot attacks and enforces STA security; detects Denial of Service (DoS) attacks via predefined DoS attacks, and provides a Signature mechanism, which allows admins to define custom rules; enables Virtual Service Domains to deploy security policies by department or location for example

- Media access control (MAC) authentication

  Provides simple authentication based on a user's MAC address; supports local or RADIUS-based authentication

- Secure user isolation

  Virtual AP services enable network administrators to provide specific services for different user groups, allowing effective resource sharing, and simplifying network maintenance and management

- Secure access by location

  AP location-based user access control helps ensure that wireless users can access and authenticate only to preselected APs, enabling system administrators to control the locations where a wireless user can access the network

- Endpoint Admission Defense

  Integrated wired and wireless Endpoint Admission Defense (EAD) helps ensure that only wireless clients who comply with mandated enterprise security policies can access the network, reducing threat levels caused by infected wireless clients and improving the overall security of the wireless network

- Public Key Infrastructure (PKI)

  Is used to control access

- Authentication, authorization, and accounting (AAA)

  Uses an embedded authentication server or external AAA server for local users

- Intelligent Application Aware Feature (WIAA)

  Provides a user role based or SSID based firewall embedded in WLAN Controller via ACL-based packet filter firewall and ASPF firewall. Protect clients from outside attacks Restrict specific users from accessing specific network resources

- Source Address Validation Improvement (SAVI)

  Records the wireless client's IP address and MAC address and at the next data traffic forwarding stage, SAVI will validate the client's IP address to prevent attacker spoofing other client's IP address

Connectivity

- IEEE 802.3at Power over Ethernet (PoE+)

  Provides 30 W of support per port for PoE+-capable devices such as IP phones, wireless access points, and security cameras, as well as any IEEE 802.3af-compliant end device; eliminates the cost of additional electrical cabling that would be needed in IP phone and WLAN deployments; the HPE 830 8-Port PoE+ Unified Wired-WLAN Switch supports up to 5 ports at 30 W; the 24-port model can support up to 24 ports at up to 30 W depending on the power source

- Loopback

  Supports internal loopback testing for maintenance purposes and an increase in 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

- IPv6

  – IPv6 host

    Enables controllers to be managed and deployed at the IPv6 network's edge

  – Dual stack (IPv4 and IPv6)

    Transitions customers from IPv4 to IPv6, supporting connectivity for both protocols

  – MLD snooping

    Directs IPv6 multicast traffic to the appropriate interface, preventing traffic flooding

  – IPv6 ACL/QoS

    Supports ACL and QoS for IPv6 network traffic

- NAT support

  – NAT traversal

    Helps ensure that communication between a branch office AP and HPE 830 is supported when the branch uses NAT

  – Integrated NAT support

    Replaces the private source IP address with a public address; enables multiple internal addresses to be mapped to the same public IP address; permits only certain internal IP addresses to be NAT'ed, and provides an Application Layer Gateway that supports specific application protocols without requiring the NAT platform to be modified

- IEEE 802.3ad Link Aggregation Control Protocol (LACP)

  – Supports a total of 12 (24-port) or 4 trunk groups (8-port) with each group supporting 8 active ports. Ports must be of the same type (that is, all 100/1000 ports or 10GbE ports)

Performance

- Flexible forwarding modes

  Supports both distributed and centralized forwarding mode; in a wireless network using centralized forwarding, all wireless traffic is sent to the HPE 830 Unified Wired-WLAN Switch for processing; if the distributed mode is configured, authenticated clients can continue to access local resources in the event that connectivity to the HPE 830 Unified Wired-WLAN Switch is lost

- Fast roaming

  Supports Layer 3 roaming and fast roaming, satisfying the most demanding voice service requirements

- Flexible forwarding modes

  – Enable distributed and centralized traffic forwarding

    Centralized forwarding, wireless traffic is sent to the HPE 830 for processing. With distributed mode wireless traffic is dropped off locally. In the event that connectivity to the HPE 830 is lost, authenticated clients can continue to access local resources

  – Support local drop off or centralization of data traffic

    After an HTML authentication using the built-in portal server or IMC portal authentication

Resiliency and high availability

- High reliability

  Supports N+1 and N+N backup

Layer 2 switching

- VLAN support and tagging

  Supports IEEE 802.1Q with 4,094 simultaneous VLAN IDs

- Spanning Tree Protocol (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)

- Port mirroring

  Duplicates port traffic (ingress and egress) to a local or remote monitoring port

- Jumbo packet support

  Supports frame sizes up to 9K byte (switch) and up to 4K byte (controller) to improve the performance of large data transfers

Layer 3 routing

- Routing Information Protocol (RIP)

  Provides RIPv1 and RIPv2 routing

- Static IP routing

  Provides manually configured routing for both IPv4 and IPv6 networks

Scalability

- Pay as you grow

  12 AP license upgrades allow you to increase support for additional access points without the need to buy additional costly hardware.

Comprehensive portfolio

- Access point support

  Refer to the HPE Access Point—Controller Compatibility Matrix
  h20195.www2.hpe.com/V2/GetDocument.aspx?docname=4AA5-0345ENW&cc=us&lc=en

Warranty and support

- Limited Lifetime Warranty 2.0

  See hpe.com/networking/warrantysummary for warranty and support information included with your product purchase.

- Software releases

  Includes all offered software releases for as long as you own the product; to find software for your product, refer to hpe.com/networking/support; for details on the software releases available with your product purchase, refer to hpe.com/networking/warrantysummary

HPE 830 Unified Wired-WLAN Switch Series

SPECIFICATIONS	HPE 830 24-Port PoE+ Unified Wired-WLAN Switch (JG640A)	HPE 830 8-Port PoE+ Unified Wired-WLAN Switch (JG641A)
I/O ports and slots	24 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP dual-personality ports; Duplex: full only; (4 10/100/1000BASE-T and 1000BASE-X Gigabit Ethernet combination) 2 extended module slots	8 RJ-45 auto-negotiating 10/100/1000 PoE+ ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T, IEEE 802.3af PoE, IEEE 802.3at); Media Type: Auto-MDIX; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 2 SFP dual-personality 1000 Mb/s ports
Additional ports and slots	1 RJ-45 serial console port	1 RJ-45 serial console port
Physical characteristics Dimensions Weight	17.32(w) x 16.89(d) x 1.72(h) in. (44 x 42.9 x 4.36 cm) (1U height) 15.87 lb (7.2 kg)	17.32(w) x 10.63(d) x 1.72(h) in. (44 x 27 x 4.36 cm) (1U height) 8.82 lb (4 kg)
Memory and processor Processor	Dual core @ 750 MHz, 1 GB flash, 512 MB DDR2 SDRAM	Dual core @ 750 MHz, 1 GB compact flash, 512 MB DDR2 SDRAM
Mounting and enclosure	EIA standard 19-inch Telco rack or equipment cabinet (hardware included)	EIA standard 19-inch Telco rack or equipment cabinet (hardware included)
Performance Switch fabric speed MAC address table size	88 Gb/s 8000 entries	20 Gb/s 8000 entries

HPE 830 Unified Wired-WLAN Switch Series

SPECIFICATIONS (CONTINUED)	HPE 830 24-Port PoE+ Unified Wired-WLAN Switch (JG640A)	HPE 830 8-Port PoE+ Unified Wired-WLAN Switch (JG641A)
Environment		
Operating temperature	32°F to 113°F (0°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing
Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Nonoperating/Storage relative humidity	5% to 95%, noncondensing	5% to 95%, noncondensing
Electrical characteristics		
Frequency	50/60 Hz	50/60 Hz
Maximum heat dissipation	307 BTU/hr (323.89 kJ/hr)	130 BTU/hr (137.15 kJ/hr)
AC voltage	100–240 VAC	100–240 VAC
Maximum power rating	90 W	38 W
Idle power	53 W	28 W
PoE power	370 W	180 W
	Notes	
	Idle power is the actual power consumption of the device with no ports connected. PoE power is the power supplied by the internal power supply. It is dependent on the type and quantity of power supplies and may be supplemented with the use of an external power supply (EPS).	Idle power is the actual power consumption of the device with no ports connected. PoE power is the power supplied by the internal power supply. It is dependent on the type and quantity of power supplies and may be supplemented with the use of an external power supply (EPS).
	Internal power supply delivers PoE+ to a maximum of 11 ports. PoE+ can be delivered to all 24 ports with the use of an optional redundant power system.	Internal power supply delivers PoE+ to a maximum of five ports.
Safety	UL 60950-1; CAN/CSA 22.2 No. 60950-1; IEC 60950-1; EN 60950-1; FDA 21 CFR Subchapter J	UL 60950-1; CAN/CSA 22.2 No. 60950-1; IEC 60950-1; EN 60950-1; FDA 21 CFR Subchapter J
Emissions	EN 55022 Class A; CISPR 22 Class A; ICES-003 Class A; AS/NZS CISPR 22 Class A; EN 61000-3-2; EN 61000-3-3; VCCI-3 CLASS A; VCCI-4 CLASS A; ETSI EN 300 386; FCC Part 15 (CFR 47) CLASS A	EN 55022 Class A; CISPR 22 Class A; ICES-003 Class A; AS/NZS CISPR 22 Class A; EN 61000-3-2; EN 61000-3-3; VCCI-3 CLASS A; VCCI-4 CLASS A; ETSI EN 300 386; FCC Part 15 (CFR 47) CLASS A

HPE 830 Unified Wired-WLAN Switch Series

SPECIFICATIONS (CONTINUED)	HPE 830 24-Port PoE+ Unified Wired-WLAN Switch (JG640A)	HPE 830 8-Port PoE+ Unified Wired-WLAN Switch (JG641A)
Immunity EN	EN 55024, CISPR 24 & ETSI EN 300 386	EN 55024, CISPR 24 & ETSI EN 300 386
Management	IMC—Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; RMON1; FTP; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB	IMC—Intelligent Management Center; command-line interface; Web browser; SNMP Manager; Telnet; HTTPS; RMON1; FTP; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB
Features	Default supported APs: 24 Maximum supported APs: 60 (via the optional purchase of the 12-access point E-LTU) Maximum supported users: 1,000 Maximum supported users via local portal authentication: 1,000 Maximum supported users via local authentication: 1,000 Maximum supported configured SSIDs: 64 Maximum supported ACLs: 2,000 Supported MSM APs are automatically discovered, Comware firmware is loaded, and the APs can be fully managed. Centralized wireless throughput is up to 2GbE.	Default supported APs: 12 Maximum supported APs: 36 (via the optional purchase of the 12-access point E-LTU). the 36 AP capacity requires R3507P37 or later. Prior releases support a maximum 24 AP capacity. Maximum supported users: 1,000 Maximum supported users via local portal authentication: 1,000 Maximum supported users via local authentication: 1,000 Maximum supported configured SSIDs: 64 Maximum supported ACLs: 2,000 Supported MSM APs are automatically discovered, Comware firmware is loaded, and the APs can be fully managed. Centralized wireless throughput is up to 2GbE.
Services	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.	Refer to the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services, and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

STANDARDS AND PROTOCOLS
(applies to all products in series)

General protocols	RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 855 Telnet Option Specification RFC 858 Telnet Suppress Go Ahead Option RFC 894 IP over Ethernet RFC 950 Internet Standard Subnetting Procedure RFC 959 File Transfer Protocol (FTP) RFC 1122 Host Requirements RFC 1141 Incremental updating of the Internet checksum RFC 1144 Compressing TCP/IP headers for low-speed serial links	RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1305 NTPv3 (IPv4 only) RFC 1321 the MD5 Message-Digest Algorithm RFC 1334 PPP Authentication Protocols (PAP) RFC 1350 TFTP Protocol (revision 2) RFC 1519 CIDR RFC 1812 IPv4 Routing RFC 1944 Benchmarking Methodology for Network Interconnect Devices RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2104 HMAC: Keyed-Hashing for Message Authentication RFC 2246 the TLS Protocol Version 1.0	RFC 2284 EAP over LAN RFC 2644 Directed Broadcast Control RFC 2864 the Inverted Stack Table Extension to the Interfaces Group MIB RFC 2866 RADIUS Accounting RFC 2869 RADIUS Extensions RFC 3164 Syslog RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) RFC 3619 Ethernet Automatic Protection Switching (EAPS) RFC 3636 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
IP multicast	RFC 1112 IGMP RFC 2236 IGMPv2	RFC 2934 Protocol Independent Multicast MIB for IPv4	RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
IPv6	RFC 1350 TFTP RFC 1881 IPv6 Address Allocation Management RFC 1887 IPv6 Unicast Address Allocation Architecture RFC 1981 IPv6 Path MTU Discovery RFC 2292 Advanced Sockets API for IPv6 RFC 2373 IPv6 Addressing Architecture RFC 2375 IPv6 Multicast Address Assignments RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2462 IPv6 Stateless Address Auto-configuration RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks	RFC 2466, Management Information Base for IP Version 6—ICMPv6 RFC 2526 Reserved IPv6 Subnet Anycast Addresses RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2563 ICMPv6 RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only) RFC 3315 DHCPv6 (client and relay) RFC 3363 DNS support RFC 3484 Default Address Selection for IPv6 RFC 3493 Basic Socket Interface Extensions for IPv6	RFC 3513 IPv6 Addressing Architecture RFC 3542 Advanced Sockets API for IPv6 RFC 3587 IPv6 Global Unicast Address Format RFC 3596 DNS Extension for IPv6 RFC 4193, Unique Local IPv6 Unicast Addresses RFC 4443 ICMPv6 RFC 4541 IGMP & MLD Snooping Switch RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
MIBs	RFC 1213 (MIB-II) RFC 1229 Interface MIB Extensions RFC 1643 Ethernet MIB RFC 1757 Remote Network Monitoring MIB RFC 2011 SNMPv2 MIB for IP	RFC 2012 SNMPv2 MIB for TCP RFC 2013 SNMPv2 MIB for UDP RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB RFC 2613 SMON MIB RFC 2665 Ethernet-Like-MIB	RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions RFC 2863 The Interfaces Group MIB RFC 2932IP (Multicast Routing MIB) RFC 2933 IGMP MIB

STANDARDS AND PROTOCOLS (CONTINUED)
(applies to all products in series)

Mobility	IEEE 802.11a High Speed Physical Layer in the 5 GHz Band IEEE 802.11ac WLAN Enhancements for Very High Throughput IEEE 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band IEEE 802.11d Global Harmonization IEEE 802.11e QoS enhancements IEEE 802.11g Further Higher Data Rate Extension in the 2.4 GHz Band	IEEE 802.11h Dynamic Frequency Selection IEEE 802.11i Medium Access Control (MAC) Security Enhancements IEEE 802.11n WLAN Enhancements for Higher Throughput IEEE 802.11s D1.06 draft	Hotspot 2.0 Release 1 per the Wi-Fi Alliance Hotspot 2.0 (Release 1) Technical Specification Package v1.0.0 (refer to the HPE Access Point—Controller Compatibility Matrix for certified APs) **Note** Some of the above standards are now included in IEEE 802.11-2012
Network management	IEEE 802.11k-2008 (beacon measurement functionality used as part of radio resource management) RFC 1155 Structure of Management Information	RFC 1905 SNMPv2 Protocol Operations RFC 2573 SNMPv3 Applications RFC 2574 SNMPv3 User-based Security Model (USM)	RFC 2575 VACM for SNMP SNMPv1/v2c
QoS/CoS	RFC 2474 DS Field in the IPv4 and IPv6 Headers RFC 2475 DiffServ Architecture	RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP	Call Admission Control (CAC): supports client-based and channel utilization based call admission policies Wi-Fi Multimedia (WMM), IEEE 802.11e
Security	IEEE 802.11w Protected Management Frames IEEE 802.1X Port Based Network Access Control RFC 1851 ESP Triple DES Transform RFC 2246 Transport Layer Security (TLS) RFC 2401 Security Architecture for the Internet Protocol RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)	RFC 2409 The Internet Key Exchange (IKE) RFC 2548 Microsoft® Vendor-specific RADIUS Attributes RFC 2716 PPP EAP TLS Authentication Protocol RFC 2865 RADIUS Authentication RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm	RFC 3576 Dynamic Authorization Extensions to RADIUS (Disconnect Message and Session-time renewal) RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP) RFC 3580 IEEE 802.1X RADIUS Guidelines Access Control Lists (ACLs) Guest VLAN for 802.1x Secure Sockets Layer (SSL) SSHv2 Secure Shell Web Authentication WPA (Wi-Fi Protected Access)/WPA2
VPN	RFC 2403 The Use of HMAC-MD5-96 within ESP and AH RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH	RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV	RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP RFC 2451 The ESP CBC-Mode Cipher Algorithms
IPSec	RFC 1829 The ESP DES-CBC Transform	RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec	
IKEv1		RFC 3748—Extensible Authentication Protocol (EAP)	
PKI		RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	

HPE 830 Unified Wired-WLAN Switch Series accessories

HPE 830 24-Port PoE+ Unified Wired-WLAN Switch (JG640A)	HPE 830 Unified Wired-WLAN Switch Uplink Module (JG643A) HPE X130 10G XFP LC SR Transceiver (JD117B) HPE X135 10G XFP LC ER Transceiver (JD121A) HPE X125 1G SFP LC LH40 1310nm Transceiver (JD061A) HPE X120 1G SFP LC LH40 1550nm Transceiver (JD062A) HPE X125 1G SFP LC LH70 Transceiver (JD063B) HPE X120 1G SFP LC SX Transceiver (JD118B) HPE X120 1G SFP LC LX Transceiver (JD119B) HPE X130 10G XFP LC LR Transceiver (JD108B) HPE RPS1600 1600W AC Power Supply (JG137A) HPE 830 Unified Wired-WLAN Switch 12-Access Point E-LTU (JG648AAE)
HPE 830 8-Port PoE+ Unified Wired-WLAN Switch (JG641A)	HPE X120 1G SFP LC LH40 1550nm Transceiver (JD062A) HPE X125 1G SFP LC LH70 Transceiver (JD063B) HPE X120 1G SFP LC SX Transceiver (JD118B) HPE X120 1G SFP LC LX Transceiver (JD119B) HPE X125 1G SFP LC LH40 1310nm Transceiver (JD061A) HPE 830 Unified Wired-WLAN Switch 12-Access Point E-LTU (JG648AAE)

Learn more at
hpe.com/networking

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise