Overview

Models

HP 9500 Access Controller Module for 128–640 Access Points   JD442A

Key features

- Flexible forwarding modes
- Carrier-class wireless user access control
- High reliability
- IPv4/IPv6 dual stack
- End-to-end QoS

Product overview

The HP 9500 Access Controller Module (ACM) features large capacity, high reliability, and rich services and offers strong wireless data processing capacity. The 9500 ACM provides refined user control and management, comprehensive RF management and security mechanisms, fast roaming, strong QoS and IPv4/IPv6 features, and powerful WLAN access control capability. Designed for WLAN access of enterprise networks and metropolitan area networks (MANs), the 9500 ACM provides the most ideal access control solutions for WLAN access of large enterprise campus networks, wireless MAN coverage, and hot-spot coverage.

Features and benefits

Quality of Service (QoS)

- **End-to-end QoS**: based on the Comware V5 platform, the 9500 ACMs support not only the DiffServ standard but also the IPv6 QoS; the QoS DiffServ model includes traffic classification and traffic policing, completely implementing the six groups of services—EF, AF1 through AF4, and BE; this enables ISPs to provide differentiated services for users, making the Internet a true integrated network carrying data, voice, and video services at the same time
- **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

Management

- **Automatic radio power adjustment**: automatic AP power adjustment features analyze user access status in real time, adapting power requirements based on environmental changes and providing high-quality user access signal coverage
- **Automatic radio channel adjustment**: intelligent channel switching and real-time interference detection provide the allocation of a high-quality channel to each AP, reducing adjacent channel interference
- **Load balancing**: intelligent load-sharing analyzes the locations of wireless clients in real time, providing high-quality client throughput regardless of location or number of online sessions
- **Rogue AP detection**: regular scans for rogue APs help confirm that the network is secure
- **Enterprise network management**: is supported by the Web-based, enterprise-class HP Intelligent Management Center (IMC) network management platform and Wireless Service Management (WSM), which effectively integrate traditionally disparate management tools into one easy-to-use interface
- **Secure controller management**: securely manages the controller from a single location with IMC or any other SNMP management station; controller supports SNMPv3 as well as SSH and SSL for secure CLI and Web management
- **AAA**: use embedded AAA server or use external AAA server for local users

Connectivity

Overview

- **IPv6**:
  - IPv6 host: enables controllers to be managed and deployed at the IPv6 network's edge
  - Dual stack (IPv4 and IPv6): transitions from IPv4 to IPv6, supporting connectivity for both protocols
  - MLD snooping: IPv6 multicast traffic to the appropriate interface, preventing traffic flooding
  - IPv6 ACL/QoS: supports ACL and QoS for IPv6 network traffic
- **IEEE 802.11h International Telecommunication Union** (ITU) **compliant**: employs Dynamic Frequency Selection (DFS) to automatically select another channel and adjust transmit power to reduce interference with systems such as radar, if detected on that same channel

Performance

- **Flexible forwarding modes**: the 9500 access controller module supports both distributed forwarding mode and centralized forwarding mode; you can set SSID-based forwarding type as needed; in a wireless network of centralized forwarding mode, all wireless traffic is sent to an AC for processing; if there is a wireless network where APs are deployed at branches, ACs are deployed at the headquarters, and APs and ACs are connected over a WAN, the distributed mode will be necessary
- **Carrier-class wireless user access control**: user-based access control is a feature of the 9500 ACM; for different application scenarios, you can configure different items in a user profile, such as Committed Access Rate (CAR) and QoS policies
- **Fast roaming**: supports Layer 3 roaming and fast roaming, satisfying the most demanding voice service requirements
- **High performance**: robust switching capacity and wire-speed processing provide powerful forwarding capacity for medium and large enterprise-size wireless LANs (WLANs)

Resiliency and high availability

- **High reliability**: the 9500 access controller modules support 1+1, N+1 and N+N backup; the 1+1 redundancy configuration of the 9500 ACMs support subsecond level failover; fit APs establish CAPWAP links with both ACs, but only the links to the active AC are active; when the active AC fails, the heartbeat mechanism between the two ACs ensures that the standby AC can sense the failure within 100 ms and then inform APs to use links to it, thus ensuring service continuity

Manageability

- **Web interface**: allows configuration of the switch from any Web browser on the network

Layer 2 switching

- **VLAN support and tagging**: support up to 64 port-based VLANs and dynamic configuration of IEEE 802.1Q VLAN tagging, providing security between workgroups
- **GARP VLAN Registration Protocol** (GVRP): allows automatic learning and dynamic assignment of VLANs
- **Spanning Tree**: fully supports standard IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol
- **Jumbo packet support**: supports up to 4 KB frame size to improve performance of large data transfers

Standards

- **Latest high-speed wireless standards**: when used with IEEE 802.11n-based APs, provides wireless access six times that of traditional IEEE 802.11a/b/g networks, resulting in expanded coverage and more efficient support for wireless multimedia applications

Security

- **IEEE 802.1X and RADIUS network logins**: control port-based access for authentication and accountability
- **Web-based authentication**: similar to IEEE 802.1X, it provides a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant
- **Choice of IEEE 802.11i, Wi-Fi Protected Access 2** (WPA2)**, or WPA**: locks 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 the wireless traffic

- **Secure Shell** (SSHv2): encrypts all transmitted data for secure, remote command-line interface (CLI) access over IP networks
- **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 the network administrator to provide specific services for different user groups, improving bandwidth and system resources and simplifying network maintenance and management
- **Secure access by location**: location AP-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
- **Secure access control by user**: media access control (MAC)-based and IEEE 802.1X network access control centralize wireless security through existing Remote Authentication Dial-In User Service (RADIUS) servers to protect the network from unauthorized user access
- **Endpoint Admission Defense** (EAD): integrated wired and wireless EAD helps ensure that only wireless clients who comply with mandated enterprise security policies access the network, reducing threat levels by infected wireless clients and improving the overall security of the wireless network
- **Guest VLAN**: similar to IEEE 802.1X, it provides a browser-based environment to authenticated clients via the IMC component
- **HTTPS management**: provides secure Web management
- **Public Key Infrastructure** (PKI): used to control access

Scalability

- **Pay as you grow**: license upgrades allow you to increase support for additional access points without the need to buy additional costly hardware and use additional valuable space in a chassis
- **Ease of deployment**: these wireless interface cards use the backplane for all network and management communications; there is no need for external network power connections

Warranty and support

- **1-year warranty**: with advance replacement and 10-calendar-day delivery (available in most countries)
- **Electronic and telephone support**: limited electronic and telephone support is available from HP; refer to: www.hp.com/networking/warranty for details on the support provided and the period during which support is available
- **Software releases**: refer to: www.hp.com/networking/warranty for details on the software releases provided and the period during which software releases are available for your product(s)

Technical Specifications

HP 9500 Access Controller Module for 128–640 Access Points (JD442A)

Ports	1 RJ-45 serial console port	
	1 RJ-45 out-of-band management port	
	2 USB 1.0 12 Mbps ports	
Physical characteristics	Dimensions	14.45(d) x 13.39(w) x 1.6(h) in. (36.7 x 34 x 4.06 cm) (1U height)
	Weight	7.89 lb. (3.58 kg)
Memory and processor	Processor	Eight core @ 950 MHz, 256 MB compact flash, 1 GB DDR2 DIMM
Performance	Switch fabric speed	20 Gbps
	MAC address table size	24,000 entries
Environment	Operating temperature	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	5% to 95%, non-condensing
	Non-operating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Non-operating/Storage relative humidity	5% to 95%, non-condensing
Electrical characteristics	Maximum heat dissipation	358 BTU/hr (377.69 kJ/hr)
	Maximum power rating	105 W

Safety   UL 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; Anatel; GOST; C-Tick; NOM; IEC 60950-1(with CB report)

Emissions   EN 55022; VCCI; ICES-003; AS/NZS CISPR 22; EN 300 386; FCC Part 15; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC

Immunity	EN	EN 61000-4-2:1995+A1:1998+A2:2001; EN 61000-4-3:2006; EN 61000-4-4:2004; EN 61000-4-5:2006; EN 61000-4-6: 1996 +A1:2001:A2:2007; EN 61000-4-8:2001; EN 61000-4-11:2004; EN 55024:1998+ A1:2001 + A2:2003

Management   IMC - Intelligent Management Center; command-line interface; Web browser; configuration menu; SNMP Manager; Telnet; HTTPS; RMON1; FTP; in-line and out-of-band; IEEE 802.3 Ethernet MIB; Ethernet Interface MIB

Features   9500 ACM License system

- The 9500 ACM is an access controller module for the HP 9500 series Ethernet switches. It supports 128 APs by default. After license upgrade, the access controller module can support up to 640 APs.

Notes   Max. number of users: 20K. Max. number of users that are supported by local authentication: 1K. Max. number of SSIDs that can be configured: 512. Max. number of users that are supported by local portal authentication: 4K. Number of ACLs: 32K.

Services   Refer to the HP website at: www.hp.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 HP sales office.

Standards and protocols	General protocols	MIBs
	RFC 768 UDP	RFC 1229 Interface MIB Extensions
	RFC 791 IP	RFC 1643 Ethernet MIB
	RFC 792 ICMP	RFC 1757 Remote Network Monitoring MIB
	RFC 793 TCP	RFC 2011 SNMPv2 MIB for IP

Technical Specifications

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 1321 The MD5 Message-Digest Algorithm
RFC 1334 PPP Authentication Protocols (PAP)
RFC 1350 TFTP Protocol (revision 2)
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 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3619 Ethernet Automatic Protection Switching (EAPS)
draft-ietf-capwap-protocol-specification-00.txt:CAPW
AP Protocol Specification
draft-ohara-capwap-lwapp-03.txt:Light Weight Access Point Protocol

IP multicast
RFC 1112 IGMP
RFC 2236 IGMPv2
RFC 2934 Protocol Independent Multicast MIB for IPv4

IPv6
RFC 1350 TFTP
RFC 1881 IPv6 Address Allocation Management
RFC 1887 IPv6 Unicast Address Allocation Architecture

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 2863 The Interfaces Group MIB
RFC 2932IP (Multicast Routing MIB)
RFC 2933 IGMP MIB

Mobility
IEEE 802.11a High Speed Physical Layer in the 5 GHz Band
IEEE 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band
IEEE 802.11d Global Harmonization
IEEE 802.11g Further Higher Data Rate Extension in the 2.4 GHz Band
IEEE 802.11i Medium Access Control (MAC) Security Enhancements
IEEE 802.11n WLAN Enhancements for Higher Throughput

Network 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

Security
IEEE 802.1X Port Based Network Access Control
RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm
RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)
Access Control Lists (ACLs)
Guest VLAN for 802.1x
MAC Authentication
Secure Sockets Layer (SSL)
SSHv1.5 Secure Shell
SSHv2 Secure Shell
Web Authentication
WPA (Wi-Fi Protected Access)/WPA2

Technical Specifications

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 2526 Reserved IPv6 Subnet Anycast Addresses
RFC 2563 ICMPv6
RFC 2925 Definitions of Managed Objects for
Remote Ping, Traceroute, and Lookup Operations
(Ping only)
RFC 3484 Default Address Selection for IPv6
RFC 3587 IPv6 Global Unicast Address Format
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

IKEv1
RFC 3748 - Extensible Authentication Protocol
(EAP)

Accessories

HP 9500 Access Controller Module for 128–640 Access Points accessories	Licenses	
	HP WX Blade 128 Access Point License Upgrade	JD464A
	HP WX Blade 128 AP License Upgrade	JD464B

To learn more, visit: www.hp.com/networking

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.