HP 10500/7500 20G Unified Wired-WLAN Module

Key features

- Enterprise-scale capacity, performance, and high reliability for wireless networks
- System-wide approach to WLAN reliability through Wi-Fi Clear Connect
- Flexible forwarding modes
- IPv4/IPv6 dual stack
- End-to-end QoS

Product overview

The HP 10500/7500 20G Unified Wired-WLAN Module delivers enterprise-scale features, capacity, and high reliability, as well as offers substantial data processing capacity for wireless networks.

The HP 10500/7500 20G Unified Wired-WLAN Module provides refined user control and management, comprehensive RF management and security mechanisms, fast roaming, QoS and IPv4/IPv6 features, and powerful WLAN access control.

Designed for the WLAN access of enterprise networks, this module provides an industry-leading WLAN solution for large enterprise networks. Working together with HP access points, the HP 10500/7500 Unified Wired-WLAN Module can be easily deployed on Layer 2 or Layer 3 networks without affecting existing configurations.
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 via advanced radio resource management and identifying rogue activity; these capabilities optimize WLAN performance by making decisions at a system-wide level
• Advanced radio resource management
  – Automatic radio power adjustments includes real-time power adjustments based on changing environmental conditions and signal coverage adjustment
  – 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 optimize AP and client throughput
• Enterprise network management is provided by HP Intelligent Management Center (IMC) Platform Software and the IMC Wireless Services Manager Software Module, 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

Quality of Service (QoS)
• End-to-end QoS the HP 10500/7500 20G Unified Wired-WLAN Module 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 support port-based and SSID-based 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
• Secure shell encrypts all transmitted data for secure remote CLI access over IP networks
• Media access control (MAC) authentication provides simple authentication based on a user’s MAC address; supports local or RADIUS-based authentication
• Integrated intrusion detection system (IDS) 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
• Secure user isolation virtual AP services enable the network administrator to provide specific services for different user groups, allowing effective resource sharing, and simplifying network maintenance and management
• 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) used to control access
• Authentication, authorization, and accounting (AAA) uses an embedded authentication server or external AAA server for local users

Connectivity
• 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 traversal helps ensure that communication between a branch office AP and the module is supported when the branch is using NAT
Performance

- **Flexible forwarding modes**
  support both centralized and distributed modes; enable all wireless traffic to be sent to the module for processing using centralized forwarding or dropped off locally using distributed mode; provide branch office survivability with distributed mode (that is, where APs are deployed at branches, authenticated clients can continue to access local resources in the event that connectivity to the controller is lost)

- **Wireless user access control and management**
  support defining settings such as Committed Access Rate (CAS), QoS profiles, and access control policies based on location for different applications

- **Fast roaming**
  supports Layer 3 roaming and fast roaming, satisfying the most demanding voice service requirements

- **Robust switching capacity and wire-speed processing**
  deliver powerful forwarding capacity to support large enterprise WLANs

Resiliency and high availability

- **High reliability**
  the module supports 1+1, N+1, and N+N backup; the 1+1 redundancy configuration of the modules supports subsecond-level failure detection; APs establish AP-module tunnel links with both modules, but only the links to the active module are active; when the active module fails, the heartbeat mechanism between the two modules help ensure that the standby module can sense the failure in subsecond level and then informs the APs to switch over to it, thus providing service continuity

Scalability

- **Ease of deployment**
  these wireless interface cards use the backplane for all network and management communications, with no need for external network power connections

- **128-access point license upgrade**
  allows you to increase support for additional access points without the need to buy additional costly hardware and use additional valuable space in a chassis; a redundant module must be provisioned with the same number of APs as the primary module

Layer 2 switching

- **VLAN support and tagging**
  supports IEEE 802.1Q with 4,094 simultaneous VLAN IDs

- **Jumbo packet support**
  supports up to 4 KB frame size to improve the performance of large data transfers

Comprehensive portfolio

- **Access point support**
  includes HP MSM430, MSM460, MSM466, MSM466-R, WA2620, WA2620E, WA2612, and WA2610E models

Warranty and support

- **1-year warranty**
  with advance replacement and 10-calendar-day delivery (available in most countries)

- **Electronic and telephone support**
  1-year limited electronic and telephone support is available from HP; to reach our support centers, refer to [www.hp.com/networking/contact-support](http://www.hp.com/networking/contact-support); for details on the duration of support provided with your product purchase, refer to [www.hp.com/networking/warrantysummary](http://www.hp.com/networking/warrantysummary)

- **Software releases**
  includes all offered software releases for as long as you own the product; to find software for your product, refer to [www.hp.com/networking/support](http://www.hp.com/networking/support); for details on the software releases available with your product purchase, refer to [www.hp.com/networking/warrantysummary](http://www.hp.com/networking/warrantysummary)
# HP 10500/7500 20G Unified Wired-WLAN Module

## Specifications

**HP 10500/7500 20G Unified Wired-WLAN Module (JG639A)**

### Ports
- 1 RJ-45 serial console port (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only
- 1 RJ-45 out-of-band management port (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only

### Physical characteristics
- 15.71(w) x 13.98(d) x 1.57(h) in (39.9 x 35.5 x 4.0 cm) (1U height)
- Weight: 7.98 lb (3.62 kg)

### Memory and processor
- Processor: Eight core @ 950 MHz, 1 GB compact flash, 2 GB DDR2 DIMM

### Performance
- Switch fabric speed: 10 Gbps
- MAC address table size: 24000 entries

### Environment
- Operating temperature: 32°F to 113°F (0°C to 45°C)
- Operating relative humidity: 5% to 95%, noncondensing
- Nonoperating/Storage temperature: -40°F to 158°F (-40°C to 70°C)
- Nonoperating/Storage relative humidity: 5% to 95%, noncondensing

### Electrical characteristics
- Maximum heat dissipation: 512 BTU/hr (540.16 kJ/hr)
- Maximum power rating: 150 W
- Notes: Power consumption: 118 W-150 W

### Safety
- UL 60950-1; CAN/CSA 22.2 No. 60950-1; IEC 60950-1; FDA 21 CFR Subchapter J

### Emissions
- EN 55022 Class A; CISPR 22 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

### Immunity
- EN 55024, CISPR24 & ETSI EN 300 386

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

### Features
- For use in HP 10500 Switch Series and HP 7500 Switch Series
- Default supported APs: 128
- Maximum supported APs: 1,024 (via the optional purchase of the 128-Access Point E-LTU)
- Maximum supported users: 20,000
- Maximum supported users via local portal authentication: 4,000
- Maximum supported users via local authentication: 1,000
- Maximum supported configured SSIDs: 512
- Maximum supported ACLs: 32,000
- Supported MSM APs are automatically discovered, Comware firmware is loaded, and the APs can be fully managed.

### Services
- Refer to the HP website at [www.hp.com/networking/services](http://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.
HP 10500/7500 20G Unified Wired-WLAN Module
Specifications (continued)

<table>
<thead>
<tr>
<th>Standards and protocols</th>
<th>General protocols</th>
<th>IP multicast</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 168 UDLP</td>
<td>RFC 246 IPv6 Neighbor Discovery</td>
<td>RFC 1112 IGMP</td>
<td>RFC 1350 TFTP</td>
</tr>
<tr>
<td>RFC 792 ICMP</td>
<td>RFC 2463 ICMPv6</td>
<td>RFC 2934 Protocol Independent Multicast MB for IPv4</td>
<td></td>
</tr>
<tr>
<td>RFC 793 TCP</td>
<td>RFC 2464 Transmission of IPv6 over Ethernet Networks</td>
<td></td>
<td>RFC 1981 IPv6 Path MTU Discovery</td>
</tr>
<tr>
<td>RFC 826 ARP</td>
<td>RFC 2455 Management Information Base for IP Version 6: Textual Conventions and General Group [partially support, only &quot;IPv6 Interface Statistics table&quot;]</td>
<td></td>
<td>RFC 2292 Advanced Sockets API for IPv6</td>
</tr>
<tr>
<td>RFC 854 TELNET</td>
<td>RFC 2466, Management Information Base for IP Version 6 - ICMPv6</td>
<td></td>
<td>RFC 2373 IPv6 Addressing Architecture</td>
</tr>
<tr>
<td>RFC 855 Telnet Option Specification</td>
<td>RFC 2526 Reserved IPv6 Subnet Anycast Addresses</td>
<td>RFC 2375 IPv6 Multicast Address Assignments</td>
<td>RFC 2375 IPv6 Protocol (revision 2)</td>
</tr>
<tr>
<td>RFC 858 Telnet Suppress Go-Ahead Option</td>
<td>RFC 2553 Basic Socket Interface Extensions for IPv6</td>
<td></td>
<td>RFC 3513 IPv6 Addressing Architecture</td>
</tr>
<tr>
<td>RFC 894 IP over Ethernet</td>
<td>RFC 2582 ICMPv6</td>
<td>RFC 3542 Advanced Sockets API for IPv6</td>
<td>RFC 3587 IPv6 Global Unicast Address Format</td>
</tr>
<tr>
<td>RFC 900 Internet Standard Subnetting Procedure</td>
<td>RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only)</td>
<td>RFC 4193, Unique Local IPv6 Unicast Addresses</td>
<td>RFC 4863 IPv6 Stateless Address Auto-configuration</td>
</tr>
<tr>
<td>RFC 959 File Transfer Protocol (FTP)</td>
<td>RFC 3315 DHCPv6 (client and relay)</td>
<td>RFC 5095 Deprecation of Type O Routing Headers in IPv6</td>
<td>RFC 5095 Deprecation of Type O Routing Headers in IPv6</td>
</tr>
<tr>
<td>RFC 1122 Host Requirements</td>
<td>RFC 3363 DNS support</td>
<td>RFC 3749 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3749 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 1141 Incremental updating of the Internet checksum</td>
<td>RFC 3484 Default Address Selection for IPv6</td>
<td>RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm</td>
<td>RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm</td>
</tr>
<tr>
<td>RFC 1144 Compressing TCP/IP headers for low-speed serial links</td>
<td>RFC 3493 Basic Socket Interface Extensions for IPv6</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 1256 ICMP Router Discovery Protocol (RDP)</td>
<td>RFC 3513 IPv6 Addressing Architecture</td>
<td>Access Control Lists (ACLs)</td>
<td>Access Control Lists (ACLs)</td>
</tr>
<tr>
<td>RFC 1321 The MDS Message-Digest Algorithm</td>
<td>RFC 3542 Advanced Sockets API for IPv6</td>
<td>Guest VLAN for BO2.1x</td>
<td>Guest VLAN for BO2.1x</td>
</tr>
<tr>
<td>RFC 1350 TFTP Protocol (revision 2)</td>
<td>RFC 3596 DNS Extension for IPv6</td>
<td>SSHv2 Secure Shell</td>
<td>SSHv2 Secure Shell</td>
</tr>
<tr>
<td>RFC 1812 IPv4 Routing</td>
<td>RFC 4193, Unique Local IPv6 Unicast Addresses</td>
<td>Web Authentication</td>
<td>Web Authentication</td>
</tr>
<tr>
<td>RFC 1844 Benchmarking Methodology for Network Interconnect Devices</td>
<td>RFC 4443 ICMPv6</td>
<td>WPA (Wi-Fi Protected Access)</td>
<td>WPA (Wi-Fi Protected Access)</td>
</tr>
<tr>
<td>RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)</td>
<td>RFC 4541 GMP &amp; MLD Snooping Switch</td>
<td>IKEv1</td>
<td>IKEv1</td>
</tr>
<tr>
<td>RFC 2246 The TLS Protocol Version 1.0</td>
<td>RFC 5095 Deprecation of Type O Routing Headers in IPv6</td>
<td>Mobility</td>
<td>Mobility</td>
</tr>
<tr>
<td>RFC 2284 EAP over LAN</td>
<td>RFC 3749 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>IEEE 802.11a High Speed Physical Layer in the 5 GHz Band</td>
<td>IEEE 802.11a High Speed Physical Layer in the 5 GHz Band</td>
</tr>
<tr>
<td>RFC 2644 Directed Broadcast Control</td>
<td>RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm</td>
<td>IEEE 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band</td>
<td>IEEE 802.11b Higher-Speed Physical Layer Extension in the 2.4 GHz Band</td>
</tr>
<tr>
<td>RFC 2864 The Inverted Stack Table Extension to the Interfaces Group MB</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>IEEE 802.11d Global Harmonization</td>
<td>IEEE 802.11d Global Harmonization</td>
</tr>
<tr>
<td>RFC 2865 RADIUS Accounting</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>IEEE 802.11e QoS enhancements</td>
<td>IEEE 802.11e QoS enhancements</td>
</tr>
<tr>
<td>RFC 2869 RADIUS Extensions</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>IEEE 802.11f Further Higher Data Rate Extension in the 2.4 GHz Band</td>
<td>IEEE 802.11f Further Higher Data Rate Extension in the 2.4 GHz Band</td>
</tr>
<tr>
<td>RFC 2658 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>IEEE 802.11h Dynamic Frequency Selection</td>
<td>IEEE 802.11h Dynamic Frequency Selection</td>
</tr>
<tr>
<td>RFC 2519 CipherSuites for Transport Layer Security (TLS)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>Network management</td>
<td>Network management</td>
</tr>
<tr>
<td>RFC 3019 Ethernet Automatic Protection Switching (EAPS)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 1155 Structure of Management Information</td>
<td>RFC 1155 Structure of Management Information</td>
</tr>
<tr>
<td>RFC 3266 The Inverted Stack Table Extension to the Interfaces Group MB</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 1905 SNMPv2 Protocol Operations</td>
<td>RFC 1905 SNMPv2 Protocol Operations</td>
</tr>
<tr>
<td>RFC 3269 RADIUS Extensions</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 2573 SNMPv3 Applications</td>
<td>RFC 2573 SNMPv3 Applications</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 2575 VACM for SNMP</td>
<td>RFC 2575 VACM for SNMP</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
<tr>
<td>RFC 3269 Advanced Encryption Standard (AES)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
<td>RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP)</td>
</tr>
</tbody>
</table>
License

**NEW** HP 10500/7500 Unified Wired-WLAN Module 128-Access Point E-LTU (JG649AAE)