Data sheet

HP MSR3000 TAA-Compliant Router Series

Product overview

The HP MSR3000 TAA-Compliant Router Series, the next generation of routers from HP, is a component of the HP FlexBranch solution. These routers feature a modular design that delivers unmatched application services for medium- to large-sized branch offices. Your IT personnel can benefit from reduced complexity and simplified configuration, deployment, and management.

The MSR3000 routers use the latest multicore CPUs, offer Gigabit switching, provide an enhanced PCI bus, and ship with the latest version of the HP Comware software to help ensure high performance with concurrent services. With these routers, you get a full-featured, resilient routing platform, including IPv6 and MPLS, with up to 2.6 Mp/s forwarding capacity and 1.9 Gb/s of IPSec VPN encrypted throughput. In addition, the routers support HP Open Application Platform (OAP) modules to deliver integrated industry-leading HP AllianceOne partner applications such as virtualization, unified communications and collaboration (UC&C), and application optimization capabilities.

Leveraging the MSR3000 series, you can realize an agile, flexible network infrastructure that enables you to quickly adapt to changing business requirements, while delivering integrated concurrent services on a single, easy-to-manage platform.

A summary of the highlights of the MSR3000 TAA-Compliant Router Series:

- Up to 2.6 Mp/s forwarding performance; support for multiple concurrent services
- OAP for HP AllianceOne applications such as WAN acceleration and Microsoft® Lync
- Embedded security features with hardware-based encryption, firewall, network address translation (NAT), and VPNs
- No additional licensing complexity; no cost for advanced features
- Zero-touch solution with single-pane-of-glass management capabilities

Features and benefits

Performance

- Excellent forwarding performance

  Provides forwarding performance up to 2.6 Mp/s (1.7 Gb/s); and meets the bandwidth-intensive application demands of enterprise businesses

- Powerful security capacity

  Includes an embedded hardware encryption accelerator to improve encryption performance; the IPSec encryption throughput can be up to 1.9 Gb/s with a maximum of 4,000 IPSec VPN tunnels

Product architecture

- Ideal multiservice platform

  Provides a WAN router, Ethernet switch, wireless LAN, 3G/4G WAN, firewall, VPN, and SIP/voice gateway—all in one device

- Advanced hardware architecture

  Provides multicore processors, gigabit switching, PCIE bus, external RPS or dual internal power supplies, internal and external CF cards, and support for new high-performance MIM modules (HMIM)

- New version of the operating system

  Ships with the new Comware 7 operating system, delivering the latest in virtualization and routing

- OAP architecture

  Provides unmatched application and service flexibility, with the potential to deliver the functionality of multiple devices—creating capital and operational expense savings and lasting investment protection

- Field-programmable gate array (FPGA)

  Improves the bandwidth of SIC module slots from 100 Mb/s to 1,000 Mb/s; and improves uplink performance from 1 Gb/s to 10 Gb/s

- Multi gigabit fabric (MGF)

  Eases utilization of the main processor by transmitting L2 packets directly via the MGF

Connectivity

- High-density port connectivity

  Provides up to 6 interface module slots and up to three onboard Gigabit Ethernet ports

- Multiple WAN interfaces

  Provides traditional links with E1, T1, serial, and ISDN; Offers high-density Ethernet access with WAN Gigabit Ethernet and LAN 4- and 9-port Fast Ethernet; and enables mobility access with the 3G SIC module, 3G/4G USB modems, and high-speed E3/T3 and 155 Mb/s OC3 access options

- Packet storm protection

  Protects against broadcast, multicast, or unicast storms with user-defined thresholds

- Loopback

  Supports internal loopback testing for maintenance purposes and an increase in availability; the loopback detection protects against incorrect cabling or network configurations, and it can be enabled on a per-port or per-VLAN basis for added flexibility

- 3G/4G LTE access support

  Provides 3G wireless access for primary or backup connectivity via a 3G SIC module that's certified on various cellular networks; optional carrier 3G/4G LTE USB modems are also available

- USB interface

  Uses USB memory disk to download and upload configuration/OS image files; and supports an external USB 3G/4G modem for a 3G/4G WAN uplink

- Flexible port selection

  Provides a combination of fiber and copper interface modules, 100/1000BASE-X support, 10/100/1000BASE-T auto-speed detection plus auto duplex, and MDI/MDI-X

L2 switching

- Spanning tree protocol (STP)

  Supports standard IEEE 802.1D STP, IEEE 802.1w Rapid STP (RSTP) for faster convergence and IEEE 802.1s Multiple STP (MSTP)

- Internet group management protocol (IGMP) and multicast listener discovery (MLD) protocol snooping

  Controls and manages the flooding of multicast packets in an L2 network

- Port mirroring

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

- VLANs

  Supports up to 4,094 VLANs or IEEE 802.1Q-based VLANs

- sFlow

  Allows traffic sampling

- Capability to define port as switched or routed

  Supports command switch to easily change switched ports to routed (maximum of four Fast Ethernet ports)

L3 routing

- Static IPv4 routing

  Provides simple manually configured IPv4 routing

- Routing information protocol (RIP)

  Uses a distance vector algorithm with UDP packets for route determination; supports RIPv1 and RIPv2 routing; and includes loop protection

- Open shortest path first (OSPF)

  Delivers faster convergence; and uses link-state routing with the interior gateway protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

- Border gateway protocol (BGP) 4

  Delivers an implementation of the Exterior Gateway Protocol (EGP), utilizing path vectors; 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

- Intermediate system to intermediate system (IS-IS)

  Uses a path-vector IGP, which is defined by the ISO organization for IS-IS routing and extended by IETF RFC 1195 to operate in both TCP/IP and the OSI reference model (integrated IS-IS)

- Static IPv6 routing

  Provides simple manually configured IPv6 routing

- Dual IP stack

  Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network

- RIP next generation (RIPng)

  Extends RIPv2 to support IPv6 addressing

- OSPFv3

  Provides OSPF support for IPv6

- BGP+

  Extends BGP-4 to support Multiprotocol BGP (MP-BGP), including support for IPv6 addressing

- IS-IS for IPv6

  Extends IS-IS to support IPv6 addressing

- IPv6 tunneling

  Allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6-to-4, and intra-site automatic tunnel addressing protocol (ISATAP) tunnels; and is an important element for the transition from IPv4 to IPv6

- Multiprotocol label switching (MPLS)

  Uses BGP to advertise routes across label switched paths (LSPs); but uses simple labels to forward packets from any L2 or L3 protocol, which reduces complexity and increases performance; supports graceful restart for reduced failure impact; and supports LSP tunneling and multilevel stacks

- MPLS L3 VPN

  Allows L3 VPNs across a provider network; uses MP-BGP to establish private routes for increased security; supports RFC2547bis multiple autonomous system VPNs for added flexibility; and supports IPv6 MPLS VPN

- MPLS L2 VPN

  Establishes simple L2 point-to-point VPNs across a provider network, using only MPLS Label Distribution Protocol (LDP); requires no routing and hence decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; and supports circuit cross connect (CCC), static virtual circuits (SVCs), Martini draft, and Kompella-draft technologies

- Routing policy

  Allows custom filters for increased performance and security; and supports ACLs, IP prefix, AS paths, community lists, and aggregate policies

L3 services

- Address resolution protocol (ARP)

  Determines the MAC address of another IP host in the same subnet; and supports static ARPs, gratuitous ARPs—allowing detection of duplicate IP addresses, and proxy ARPs—allowing normal ARP operation between subnets or when subnets are separated by an L2 network

- User datagram protocol (UDP) helper

  Redirects UDP broadcasts to specific IP subnets to prevent server spoofing

- Dynamic host configuration protocol (DHCP)

  Simplifies the management of large IP networks and supports client and server; DHCP relay enables DHCP operations across subnets

Quality of service (QoS)

- Traffic policing

  Supports the committed access rate (CAR) and line rate

- Congestion management

  Supports FIFO, PQ, CQ, WFQ, CBQ, and RTPQ

- Weighted random early detection (WRED)/random early detection (RED)

  Delivers congestion avoidance capabilities through the use of queue management algorithms

- Hierarchical QoS (HQoS)/Nested QoS

  Manages traffic uniformly; hierarchically schedules traffic by user, network service, and application; and provides more granular traffic control and quality assurance services than traditional QoS

- Other QoS technologies

  Supports traffic shaping, MPLS QoS, and MP QoS/LFI

Security

- Dynamic virtual private network (DVPN)

  Collects, maintains, and distributes dynamic public addresses through the VPN address management (VAM) protocol, making the VPN establishment available between enterprise branches that use dynamic addresses to access the public network; compared to traditional VPN technologies, the DVPN technology is more flexible and has richer features, such as NAT traversal of DVPN packets, AAA identity authentication, IPSec protection of data packets, and multiple VPN domains

- IPSec VPN

  Supports DES, 3DES, and AES 128/192/256 encryption and MD5 and SHA-1 authentication

- Access control list (ACL)

  Supports powerful ACLs for both IPv4 and IPv6; ACLs are used 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 to be forwarded; rules can be based on an L2 or L3 protocol header; and rules can be set to operate on specific dates or times

- Terminal access controller access-control system (TACACS)

  Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security

- Unicast reverse path forwarding (URPF)

  Allows normal packets to be forwarded correctly, but discards the attaching packets due to the lack of a reverse path route or incorrect inbound interface; and prevents source spoofing and distributed attacks

- Network login

  Allows authentication of multiple users per port

- RADIUS

  Eases security access administration by using a user/password authentication server

- NAT

  Supports one-to-one NAT, many-to-many NAT, and NAT control—enabling NAT-PT to support multiple connections; and also supports blacklist in NAT/NAT-PT—a limit on the number of connections, session logs, and multiple instances

- Secure shell (SSHv2)

  Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; and increases the security of SFTP transfers

Convergence

- IGMP

  Utilizes any-source multicast (ASM) or source-specific multicast (SSM) to manage IPv4 multicast networks; and supports IGMPv1, v2, and v3

- Protocol independent multicast (PIM)

  Defines modes of Internet IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; and supports PIM Dense Mode (DM), Sparse Mode (SM), and Source-Specific Mode (SSM)

- Multicast source discovery protocol (MSDP)

  Allows multiple PIM-SM domains to interoperate; and is used for inter-domain multicast applications

- Multicast BGP (MBGP)

  Allows multicast traffic to be forwarded across BGP networks and kept separate from unicast traffic

Integration

- Embedded NetStream

  Improves traffic distribution using powerful scheduling algorithms, including L4–7 services; and monitors the health status of servers and firewalls

- Embedded VPN and firewall

  Provides enhanced stateful packet inspection and filtering; and delivers advanced VPN services with triple DES (3DES) and advanced encryption standard (AES) encryption at high performance and low latency, Web content filtering, and application prioritization and enhancement

- SIP trunking

  Delivers multiple concurrent calls on one link; the carrier authenticates only the link, rather than carrying each SIP call on the link

Resiliency and high availability

- Backup Center

  Acts as a part of the management and backup function to provide backup for device interfaces; and delivers reliability by switching traffic over to a backup interface when the primary one fails

- Virtual router redundancy protocol (VRRP)

  Allows groups of two routers to dynamically back each other up to create highly available routed environments; and supports VRRP load balancing

- Embedded automation architecture (EAA)

  Monitors the internal event and status of system hardware and software, identifying potential problems as early as possible; and collects field information and attempts to automatically repair the issues; based on the user configuration, onsite information will be sent to technical support

- Bidirectional forwarding detection (BFD)

  Detects quickly the failures of the bidirectional forwarding paths between two devices for upper-layer protocols such as routing protocols and MPLS

Management

- HP Intelligent Management Center (IMC)

  Integrates fault management, element configuration, and network monitoring from a central vantage point; has built-in support for third-party devices; and enables network administrators to centrally manage all network elements with a variety of automated tasks—including discovery, categorization, baseline configurations, and software images; the software also provides tools for configuration comparison, version tracking, change alerts, and more

- Industry-standard CLI with a hierarchical structure

  Reduces training time and expenses; and increases productivity in multivendor installations

- Management security

  Restricts access to critical configuration commands and offers multiple privilege levels with password protection; ACLs provide telnet and SNMP access; and local and remote syslog capabilities allow logging of all access

- SNMPv1, v2, and v3

  Provide complete support for SNMP and industry-standard management information base (MIB) as well as private extensions; SNMPv3 supports increased security using encryption

- Remote monitoring

  Uses standard SNMP to monitor essential network functions; and supports events, alarms, history, and a statistics group as well as a private alarm extension group

- FTP, trivial FTP (TFTP), and secure file transfer protocol (SFTP) support

  Offers different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; TFTP is a simpler method using UDP; and SFTP runs over an SSH tunnel to provide additional security

- Debug and sampler utility

  Supports ping and traceroute for both IPv4 and IPv6

- Network time protocol (NTP)

  Synchronizes timekeeping among distributed time servers and clients; and keeps timekeeping consistent among all clock-dependent devices within the network, so that the devices can provide diverse applications based on the consistent time

- Information center

  Provides a central repository for system and network information; aggregates all logs, traps, and debugging information generated by the system and maintains them in the order of severity; and sends the network information to multiple channels, based on user-defined rules

- Management interface control

  Provides management access through the modem port and terminal interface; and provides access through the terminal interface, telnet, or SSH

- Network quality analyzer (NQA)

  Analyzes network performance and service quality by sending test packets; provides network performance and service quality parameters such as jitter, TCP, or FTP connection delays; and allows the network manager to determine overall network performance as well as diagnose and locate network congestion points or failures

• Role-based security

Delivers role-based access control (RBAC); and supports 16 user levels (0–15)

• Standards-based authentication support for LDAP

Integrates seamlessly into existing authentication services

Investment protection

• Re-use of existing SIC and MIM modules

Supports existing SIC and MIM modules, transceivers, and cables for investment protection

Ease of deployment

• Zero-touch deployment

Supports both USB disk auto deployment and 3G SMS auto deployment

Additional information

• OPEX savings

Simplifies and streamlines deployment, management, and training through the use of a common operating system—cutting costs as well as reducing the risk of human errors associated with having to manage multiple operating systems across different platforms and network layers

• Faster time to market

Allows new and custom features to be brought rapidly to market through engineering efficiencies, delivering better initial and ongoing stability

• Green initiative support

Provides support for RoHS and WEEE regulations

Warranty and support

• 1-year Warranty 2.0

Advance hardware replacement with 10-calendar-day delivery (available in most countries)

• Electronic and telephone support (for Warranty 2.0)

Limited electronic and 24x7 telephone support is available from HP for the entire warranty period; to reach our support centers, refer to hp.com/networking/contact-support; for details on the duration of the support provided with your product purchase, refer to hp.com/networking/warrantysummary

• Software releases

To find software for your product, refer to hp.com/networking/support; for details on the software releases available with your product purchase, refer to hp.com/networking/warrantysummary

HP MSR3000 TAA-Compliant Router Series

Specifications

	HP MSR3024 TAA-Compliant AC Router (JG861A)
Ports	2 HMIM slots 4 SIC slots or 2 DSIC slots 1 VPM slot 3 RJ-45 1000BASE-T ports (IEEE 802.3ab Type 1000BASE-T) 1 SFP fixed Gigabit Ethernet SFP port
Physical characteristics	17.32(w) x 18.9(d) x 1.74(h) in (44 x 48 x 4.42 cm) (1U height) Weight 17.42 lb (7.9 kg)
Memory and processor	RISC, 4 cores @ 1 GHz, 256 MB flash capacity, 2 GB DDR3 SDRAM
Mounting	Desktop or can be mounted on an EIA standard 19-inch telco rack when used with the rack-mount kit in the package
Performance	
Throughput	up to 2.6 Mp/s (64-byte packets)
Routing table size	500,000 entries (IPv4), 500,000 entries (IPv6)
Forwarding table size	500,000 entries (IPv4), 500,000 entries (IPv6)
Environment	
Operating temperature	32°F to 113°F (0°C to 45°C)
Operating relative humidity	5% to 90%, noncondensing
Nonoperating/storage temperature	-40°F to 158°F (-40°C to 70°C)
Nonoperating/storage relative humidity	5% to 90%, noncondensing
Altitude	up to 16,404 ft (5 km)

Electrical characteristics	
Maximum heat dissipation	168 BTU/hr (177.24 kJ/hr)
Voltage	100-120/200-240 VAC
Maximum power rating	100 W
Frequency	50/60 Hz
	Notes Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.
Reliability	MTBF (years) 49.61
Safety	UL 60950-1; AS/NZS 60950; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1-03; EN 60950-1/A11; FDA 21 CFR Subchapter J
Emissions	EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; ETSI EN 300 386 V1.3.3; AS/NZS CISPR 22 Class A; EN 61000-4-2; EN 61000-4-3; EN 61000-4-4; EN 61000-4-5; EN 61000-4-6; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A; EN 55024:1998+ A1:2001 + A2:2003; EN61000-4-11:2004; EN 61000-4-8:2001
Telecom	FCC part 68; CS-03
Management	IMC; command-line interface; limited command-line interface; configuration menu; out-of-band management (RJ-45 Ethernet); SNMP Manager; Telnet; RMON1; FTP; in-line and out-of-band; modem interface; out-of-band management (serial RS-232C or Micro USB); IEEE 802.3 Ethernet MIB
Services	Refer to the HP website at 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
(applies to all products in series)

BGP	RFC 1163 BGP RFC 1267 BGP-3 RFC 1657 Definitions of Managed Objects for BGPv4 RFC 1771 BGPv4 RFC 1772 Application of the BGP RFC 1773 Experience with the BGP-4 Protocol RFC 1774 BGP-4 Protocol Analysis RFC 1965 BGP-4 confederations RFC 1997 BGP Communities Attribute RFC 3107 Support BGP carry Label for MPLS Mesh Internal BGP (IBGP) RFC 4724 Graceful Restart Mechanism for BGP	RFC 1998 PPP Gandalf FZA Compression Protocol RFC 2439 BGP Route Flap Damping RFC 2547 BGP/MPLS VPNs RFC 2796 BGP Route Reflection RFC 2842 Capability Advertisement with BGP-4 RFC 2858 BGP-4 Multi-Protocol Extensions RFC 2918 Route Refresh Capability RFC 3065 Autonomous System Confederations for BGP RFC 3392 Capabilities Advertisement with BGP-4	RFC 4271 A BGP-4 RFC 4273 Definitions of Managed Objects for BGP-4 RFC 4274 BGP-4 Protocol Analysis RFC 4275 BGP-4 MIB Implementation Survey RFC 4276 BGP-4 Implementation Report RFC 4277 Experience with the BGP-4 Protocol RFC 4360 BGP Extended Communities Attribute RFC 4456 BGP Route Reflection: An Alternative to Full
Denial of service protection	CPU DoS Protection Rate Limiting by ACLs		
Device management	RFC 1155 Structure and Mgmt Information (SMIv1) RFC 1902 (SNMPv2) RFC 2576 (Coexistence between SNMP V1, V2, V3) RFC 1157 SNMPv1/v2c RFC 1908 (SNMP v1/2 Coexistence) RFC 2578-2580 SMIv2 RFC 1305 NTPv3 RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0 RFC 2579 (SMIv2 Text Conventions) RFC 1591 DNS (client) RFC 2271 Framework RFC 2580 (SMIv2 Conformance) RFC 2573 (SNMPv3 Applications) RFC 3416 (SNMP Protocol Operations v2)		

Standards and protocols (continued)
(applies to all products in series)

General protocols	RFC 768 UDP RFC 2993 Architectural Implications of NAT RFC 4419 Diffie-Hellman Group Exchange for the Secure RFC 783 TFTP Protocol (revision 2) RFC 3011 The IPv4 Subnet Selection Option for DHCP RFC 791 IP RFC 3022 Traditional IP Network Address Translator Shell (SSH) Transport Layer Protocol RFC 4446 IANA Allocations for Pseudowire Edge to Edge RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 896 Congestion Control in IP/TCP Internetworks RFC 917 Internet Subnets RFC 925 Multi-LAN Address Resolution RFC 950 Internet Standard Subnetting Procedure RFC 951 BOOTP RFC 959 File Transfer Protocol (FTP) RFC 1027 Proxy ARP RFC 1048 BOOTP (Bootstrap Protocol) vendor information extensions RFC 1058 RIPv1 RFC 1091 Telnet Terminal-Type Option RFC 1093 NSFNET routing architecture RFC 1141 Incremental updating of the Internet checksum RFC 1142 OSI IS-IS Intra-domain Routing Protocol RFC 1166 Internet address used by Internet Protocol (IP) RFC 1191 Path MTU discovery RFC 1195 OSI ISIS for IP and Dual Environments RFC 1213 MIB for Network Management of TCP/IP-based internets RFC 1253 (OSPF v2) RFC 1305 NTPv3 (IPv4 only) RFC 1321 The MD5 Message-Digest Algorithm RFC 1323 TCP Extensions for High Performance RFC 1349 Type of Service RFC 1350 TFTP Protocol (revision 2) RFC 1449 Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1519 CIDR RFC 1542 BOOTP Extensions

Standards and protocols (continued)
(applies to all products in series)

General protocols (Continued)

RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1624 Incremental Internet Checksum
RFC 1631 NAT
RFC 1701 Generic Routing Encapsulation
RFC 1702 Generic Routing Encapsulation over IPv4 networks
RFC 1721 RIP-2 Analysis (Traditional NAT)
RFC 3027 Protocol Complications with the IP Network Address Translator
RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3036 LDP Specification
RFC 3037 LDP (Label Distribution Protocol) Applicability
RFC 3046 DHCP Relay Agent Information Option
RFC 3063 MPLS Loop Prevention Mechanism
RFC 3137 OSPF Stub Router Advertisement
RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP
RFC 3215 LDP State Machine
RFC 3246 Expedited Forwarding PHB
RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3277 IS-IS Transient Blackhole Avoidance
RFC 3279 Algorithms and Identifiers for the Internet
X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3319 DHCPv6 Options for Session Initiation Protocol (SIP) Servers
RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in IS-IS
RFC 3392 Support BGP capabilities advertisement
RFC 3443 Time To Live (TTL) Processing in
Multi-Protocol Label Switching (MPLS) Networks
RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP)
RFC 3509 OSPF ABR Behavior
RFC 3526 More Modular Exponential (MODP)
Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
RFC 3567 IS-IS Cryptographic Authentication
RFC 3584 Coexistence between Version 1 and Version 2
Emulation (PWE3)
RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
RFC 4486 Subcodes for BGP Cease Notification Message
RFC 4541 Considerations for Internet Group
Management Protocol (IGMP) and Multicast Listener
Discovery (MLD) Snooping Switches
RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 4562 MAC-Forced Forwarding: A Method for Subscriber Separation on an Ethernet Access Network
RFC 4576 Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4594 Configuration Guidelines for DiffServ Service Classes
RFC 4601 PIM - Sparse Mode (PIM-SM): Protocol Specification (Revised)
RFC 4618 Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks
RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks
RFC 4632 Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4664 Framework for Layer 2 Virtual Private Networks (L2VPNs)
RFC 4665 Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks
RFC 4741 NETCONF Configuration Protocol
RFC 4742 Using the NETCONF Configuration Protocol over SSH
RFC 4743 Using NETCONF over the Simple Object Access Protocol (SOAP)
RFC 4765 Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks
RFC 4781 Graceful Restart Mechanism for BGP with
RFC 1722 RIP-2 Applicability
RFC 1723 RIP v2
RFC 1724 RIP Version 2 MIB Extension

Standards and protocols (continued)
(applies to all products in series)

General protocols (Continued)

RFC 1777 Lightweight Directory Access Protocol
RFC 1812 IPv4 Routing
RFC 1825 Security Architecture for the Internet Protocol
RFC 1826 IP Authentication Header
RFC 1827 IP Encapsulating Security Payload (ESP)
RFC 1829 The ESP DES-CBC Transform
RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0
RFC 1966 BGP Route Reflection An alternative to full mesh IBGP
RFC 1981 Path MTU Discovery for IP version 6
RFC 2003 IP Encapsulation within IP
RFC 2018 TCP Selective Acknowledgement Options
RFC 2082 RIP-2 MD5 Authentication
RFC 2104 HMAC: Keyed-Hashing for Message Authentication
RFC 2131 DHCP
RFC 2132 DHCP Options and BOOTP Vendor Extensions
RFC 2138 Remote Authentication Dial In User Service (RADIUS)
RFC 2236 IGMP Snooping
RFC 2246 The TLS Protocol Version 1.0
RFC 2251 Lightweight Directory Access Protocol (v3)
RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
RFC 2283 MBGP
RFC 2309 Recommendations on queue management and congestion avoidance in the Internet
RFC 2338 VRRP
RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2453 RIPv2
RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2519 A Framework for Inter-Domain Route Aggregation
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2548 (MS-RAS-Vendor only)
RFC 2581 TCP Congestion Control
RFC 2597 Assured Forwarding PHB Group
RFC 2598 An Expedited Forwarding PHB
RFC 2616 HTTP Compatibility v1.1
RFC 2661 L2TP
RFC 2663 NAT Terminology and Considerations
RFC 2694 DNS extensions to Network Address Translators (DNS_ALG)
RFC 2698 A Two Rate Three Color Marker
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2747 RSVP Cryptographic Authentication
RFC 2763 Dynamic Name-to-System ID mapping
RFC 2784 Generic Routing Encapsulation (GRE)
RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2866 RADIUS Accounting
RFC 2868 RADIUS Attributes for Tunnel Protocol Support of the Internet-standard Network Management Framework
RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec
RFC 3612 Applicability Statement for Restart Mechanisms for the Label Distribution Protocol (LDP)
RFC 3623 Graceful OSPF Restart
RFC 3646 DNS Configuration options for DHCP for IPv6 (DHCPv6)
RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
RFC 3704 URPF RFC 3706 A Traffic-Based Method of Detecting Dead
Internet Key Exchange (IKE) Peers
RFC 3719 Recommendations for Interoperable Networks using IS-IS
RFC 3736 Stateless DHCPv6
RFC 3768 VRRP RFC 3782 The NewReno Modification to TCP's Fast
Recovery Algorithm
RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
RFC 3787 Recommendations for Interoperable IP Networks using IS-IS
RFC 3810 MLD Version 2 (MLDv2) for IPv6
RFC 3812 MPLS Traffic Engineering (TE) MIB
RFC 3815 Definitions of Managed Objects for the MPLS, Label Distribution Protocol (LDP)
RFC 3847 Restart signaling for IS-IS

Standards and protocols (continued)
(applies to all products in series)

General protocols (Continued)

RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 3948 UDP Encapsulation of IPsec ESP Packets
RFC 3973 PIM - Dense Mode (PIM-DM): Protocol Specification (Revised)
RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
RFC 4061 Benchmarking Basic OSPF Single Router Control Plane Convergence
RFC 4062 OSPF Benchmarking Terminology and Concepts
RFC 4063 Considerations When Using Basic OSPF Convergence Benchmarks
RFC 4109 Algorithms for Internet Key Exchange version 1 (IKEv1)
RFC 4133 Entity MIB (Version 3)
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
RFC 4214 ISATAP
RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance
RFC 4250 The SSH Protocol Assigned Numbers
RFC 4251 The SSH Protocol Architecture
RFC 4252 The SSH Authentication Protocol
RFC 4253 The SSH Transport Layer Protocol
RFC 4254 The SSH Connection Protocol
RFC 4291 IP Version 6 Addressing Architecture
RFC 4305 Cryptographic Algorithm Implementation MPLS
RFC 4787 NAT Behavioral Requirements for Unicast UDP
RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
RFC 4811 OSPF Out-of-Band Link State Database (LSDB) Resynchronization
RFC 4812 OSPF Restart Signaling
RFC 4813 OSPF Link-Local Signaling
RFC 4816 Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service
RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
RFC 4862 IPv6 Stateless Address Autoconfiguration
RFC 4878 “Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on
RFC 4893 BGP Support for Four-octet AS Number Space
RFC 4940 IANA Considerations for OSPF
RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 5007 DHCPv6 Leasequery
RFC 5036 LDP Specification
RFC 5065 Autonomous System Confederations for BGP
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags
RFC 5187 OSPFv3 Graceful Restart
RFC 5214 ISATAP
RFC 5254 Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3)
RFC 5277 NETCONF Event Notifications
RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates
RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks
RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
RFC 5302 Domain-Wide Prefix Distribution with Two-Level IS-IS
RFC 5304 IS-IS Cryptographic Authentication
RFC 5306 Restart Signaling for IS-IS RFC 5308 Routing IPv6 with IS-IS
RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols
RFC 5381 Experience of Implementing NETCONF over SOAP
RFC 5382 The IP Network Address Translator (NAT)
RFC 5398 Autonomous System (AS) Number Reservation for Documentation Use
RFC 5492 Capabilities Advertisement with BGP-4
RFC 5508 NAT Behavioral Requirements for ICMP
RFC 5539 NETCONF over Transport Layer Security (TLS)
RFC 5613 OSPF Link-Local Signaling
RFC 5659 An Architecture for Multi-Segment Pseudowire

Standards and protocols (continued)
(applies to all products in series)

General protocols (Continued)	RFC 2869 RADIUS Extensions Requirements for Encapsulating Security Payload (ESP) Emulation Edge-to-Edge RFC 2884 Performance Evaluation of Explicit Congestion and Authentication Header (AH) RFC 5798 VRRP Notification (ECN) in IP Networks. RFC 2963 A Rate Adaptive Shaper for Differentiated RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4365 Applicability Statement for BGP/MPLS IP Version 3 for IPv4 and IPv6 RFC 5880 BFD Services RFC 2966 Domain-wide Prefix Distribution with Virtual Private Networks (VPNs) RFC 5881 BFD for IPv4 and IPv6 (Single Hop) RFC 4381 Analyses of the Security of BGP/MPLS IP VPNs RFC 5882 Generic Application of BFD Two-Level IS-IS RFC 2973 IS-IS Mesh Groups RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN RFC 5883 BFD for Multihop Paths RFC 5905 NTP version 4: Protocol and Algorithms Specification RFC 854 Telnet Protocol Specification RFC 856 Telnet Binary Transmission
IP multicast	RFC 1112 IGMP RFC 2710 MLD for IPv6 RFC 3376 IGMPv3 (host joins only) RFC 2362 PIM Sparse Mode RFC 2934 PIM MIB for IPv4 RFC 5059 Bootstrap Router (BSR) Mechanism for RFC 3376 IGMPv3 PIM
IPv6	RFC 2080 RIPng for IPv6 RFC 2529 Transmission of IPv6 Packets over IPv4 RFC 2893 Transition Mechanisms for IPv6 Hosts and RFC 2460 IPv6 Specification RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2473 Generic Packet Tunneling in IPv6 RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2475 IPv6 DiffServ Architecture RFC 2740 OSPFv3 for IPv6 Routers RFC 3056 Connection of IPv6 Domains via IPv4 Clouds RFC 3162 RADIUS and IPv6 RFC 3315 DHCPv6 (client and relay) RFC 5340 OSPF for IPv6

Standards and protocols (continued)
(applies to all products in series)

MIBs	RFC 1213 MIB II RFC 2012 SNMPv2 MIB for TCP RFC 2573 SNMP-Notification MIB RFC 1493 Bridge MIB RFC 2013 SNMPv2 MIB for UDP RFC 2574 SNMP USM MIB RFC 1724 RIPv2 MIB RFC 2096 IP Forwarding Table MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 1850 OSPFv2 MIB RFC 2233 Interfaces MIB RFC 2737 Entity MIB (Version 2) RFC 1907 SNMPv2 MIB RFC 2273 SNMP-NOTIFICATION-MIB RFC 2863 The Interfaces Group MIB RFC 2011 SNMPv2 MIB for IP RFC 2571 SNMP Framework MIB RFC 3813 MPLS LSR MIB RFC 2572 SNMP-MPD MIB
Network management	IEEE 802.1D (STP) RFC 1904 SNMPv2 Conformance RFC 2272 SNMPv3 Management Protocol RFC 1098 Simple Network Management Protocol (SNMP) RFC 1905 SNMPv2 Protocol Operations RFC 2273 SNMPv3 Applications RFC 1158 MIB for network RFC 1906 SNMPv2 Transport Mappings RFC 2274 USM for SNMPv3 management of TCP/IP-based internets: MIB-II RFC 1212 Concise MIB definitions RFC 1215 Convention for defining traps for use with the RFC 1908 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC 2275 VACM for SNMPv3 RFC 2575 SNMPv3 View-based Access Control Model (VACM) SNMP RFC 1918 Private Internet Address Allocation RFC 1389 RIPv2 MIB Extension RFC 2037 Entity MIB using SMIv2 RFC 3164 BSD syslog Protocol RFC 3411 An Architecture for Describing Simple Network RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1450 MIB for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1902 Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1903 SNMPv2 Textual Conventions
Network management (Continued)	RFC 2261 An Architecture for Describing SNMP Management Frameworks RFC 2262 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) RFC 2263 SNMPv3 Applications RFC 2264 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC 2265 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) Management Protocol (SNMP) Management Frameworks RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) RFC 3413 Simple Network Management Protocol (SNMP) Applications RFC 3414 SNMPv3 User-based Security Model (USM) RFC 3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

Standards and protocols (continued)
(applies to all products in series)

OSPF	RFC 1245 OSPF protocol analysis RFC 1583 OSPFv2 RFC 1850 OSPFv2 MIB, RFC 1246 Experience with OSPF RFC 1587 OSPF NSSA RFC 1765 OSPF Database Overflow traps RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option
QoS/CoS	IEEE 802.1P (CoS) RFC 2597 DiffServ Assured Forwarding (AF) RFC 3168 The Addition of Explicit Congestion RFC 2474 DS Field in the IPv4 and IPv6 Headers RFC 2598 DiffServ Expedited Forwarding (EF) RFC 2475 DiffServ Architecture RFC 2697 A Single Rate Three Color Marker Notification (ECN) to IP RFC 3247 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)
Security	IEEE 802.1X Port Based Network Access Control RFC 2408 Internet Security Association and Key RFC 2865 RADIUS Authentication RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication RFC 2138 RADIUS Authentication RFC 2139 RADIUS Accounting Management Protocol (ISAKMP) RFC 2409 The Internet Key Exchange (IKE) RFC 2412 The OAKLEY Key Determination Protocol RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile RFC 2818 HTTP Over TLS RFC 2866 RADIUS Accounting RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP) RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
VPN	RFC 1828 IP Authentication using Keyed MD5 RFC 2405 The ESP DES-CBC Cipher Algorithm With RFC 3948 - UDP Encapsulation of IPSec ESP Packets RFC 1853 IP in IP Tunneling RFC 2401 Security Architecture for the Internet Protocol RFC 2402 IP Authentication Header 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 Explicit IV RFC 2406 IP Encapsulating Security Payload (ESP) RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP RFC 2410 The NULL Encryption Algorithm and Its Use With IPSec RFC 2411 IP Security Document Roadmap RFC 4301 - Security Architecture for the Internet Protocol RFC 4302 - IP Authentication Header (AH) RFC 4303 - IP Encapsulating Security Payload (ESP) RFC 4305 - Cryptographic Algorithm Implementation Requirements for ESP and AH

HP MSR3000 TAA-Compliant Router Series accessories

Transceivers	HP X110 100M SFP LC FX Transceiver (JD102B) HP X110 100M SFP LC LX Transceiver (JD120B) HP X110 100M SFP LC LH40 Transceiver (JD090A) HP X110 100M SFP LC LH80 Transceiver (JD091A) HP X120 1G SFP LC SX Transceiver (JD118B) HP X120 1G SFP LC LX Transceiver (JD119B) HP X125 1G SFP LC LH40 1310nm Transceiver (JD061A) HP X120 1G SFP LC LH40 1550nm Transceiver (JD062A) HP X125 1G SFP LC LH70 Transceiver (JD063B) HP X120 1G SFP LC LH100 Transceiver (JD103A) HP X120 1G SFP LC BX 10-U Transceiver (JD098B) HP X120 1G SFP LC BX 10-D Transceiver (JD099B)
Cables	HP X200 V.24 DTE 3m Serial Port Cable (JD519A) HP X200 V.24 DCE 3m Serial Port Cable (JD521A) HP X200 V.35 DTE 3m Serial Port Cable (JD523A) HP X200 V.35 DCE 3m Serial Port Cable (JD525A) HP X200 X.21 DTE 3m Serial Port Cable (JD527A) HP X200 X.21 DCE 3m Serial Port Cable (JD529A) HP X260 RS449 3m DTE Serial Port Cable (JF825A) HP X260 RS449 3m DCE Serial Port Cable (JF826A) HP X260 RS530 3m DTE Serial Port Cable (JF827A) HP X260 RS530 3m DCE Serial Port Cable (JF828A) HP X260 Auxiliary Router Cable (JD508A) HP X260 E1 RJ45 3m Router Cable (JD509A) HP X260 E1 RJ45 20m Router Cable (JD517A) HP X260 E1 (2) BNC 75 ohm 3m Router Cable (JD175A) HP X260 E1 BNC 20m Router Cable (JD514A) HP X260 E1 2 BNC 75 ohm 40m Router Cable (JD516A) HP X260 E1 RJ45 BNC 75-120 ohm Conversion Router Cable (JD511A) HP X260 2E1 BNC 3m Router Cable (JD643A) HP X260 8E1 BNC 75 ohm 3m Router Cable (JD512A) HP X260 T1 Router Cable (JD518A) HP X260 T1 Voice Router Cable (JD535A) HP X260 SIC-8AS RJ45 0.28m Router Cable (JD642A) HP X260 mini D-28 to 4-RJ45 0.3m Router Cable (JG263A) HP X260 T3/E3 Router Cable (JD531A) HP X260 E3-30 E3/T3 Router Cable (JD533A) HP X200 Transit Plug D25F MP8(S) Single Cable (JD636A) HP X200 Transit RJ45 0.5m Single Cable (JD641A)
Power supply	HP RPS 800 Redundant Power Supply (JD183A) **NEW** HP X351 300W 100-240VAC to 12VDC Power Supply (JG527A)

Router modules	HP MSR 9-port 10/100Base-T Switch DSIC Module (JD574B) HP MSR 4-port 10/100Base-T Switch SIC Module (JD573B) HP MSR 1-port 10/100Base-T SIC Module (JD545B) HP MSR 1-port 100Base-X SIC Module (JF280A) HP MSR 1-port GbE Combo SIC Module (JD572A) HP MSR 2-port FXO SIC Module (JD558A) HP MSR 1-port FXO SIC Module (JD559A) HP MSR 2-port FXS SIC Module (JD560A) HP MSR 1-port FXS SIC Module (JD561A) HP MSR 1-port E1 Voice SIC Module (JD575A) HP MSR 1-port T1 Voice SIC Module (JD576A) HP MSR 2-port FXS/1-port FXO SIC Module (JD632A) HP MSR 4-port FXS / 1-port FXO DSIC Module (JG189A) HP MSR 2-port ISDN-S/T Voice SIC Module (JF821A) HP MSR 1-port E1/Fractional E1 (75ohm) SIC Module (JD634B) HP MSR 2-port E1/Fractional E1 (75ohm) SIC Module (JF842A) HP MSR 1-port T1/Fractional T1 SIC Module (JD538A) HP MSR 1-port Enhanced Sync/Async Serial SIC Module (JD557A) HP MSR 1-port ISDN-S/T SIC Module (JD571A) HP MSR 8-port Async Serial SIC Module (JF281A) HP MSR 16-port Async Serial SIC Module (JG186A) HP MSR HSPA/WCDMA SIC Module (JG187A) **NEW** HP MSR 1-port E1 Voice HMIM Module (JG429A) **NEW** HP MSR 1-port T1 Voice HMIM Module (JG430A) **NEW** HP MSR 2-port E1 Voice HMIM Module (JG431A) **NEW** HP MSR 4-port FXS HMIM Module (JG446A) **NEW** HP MSR 4-port FXO HMIM Module (JG447A) **NEW** HP MSR 4-port E and M HMIM Module (JG448A) **NEW** HP MSR 4-port Enhanced Sync/Async Serial HMIM Module (JG442A) **NEW** HP MSR 8-port Enhanced Sync/Async Serial HMIM Module (JG443A) **NEW** HP MSR 2-port E1/CE1/PRI HMIM Module (JG450A) **NEW** HP MSR 4-port E1/CE1/PRI HMIM Module (JG451A) **NEW** HP MSR 4-port E1/Fractional E1 HMIM Module (JG453A) **NEW** HP MSR 8-port E1/CE1/PRI (75ohm) HMIM Module (JG452A) **NEW** HP MSR 2-port T1/CT1/PRI HMIM Module (JG456A) **NEW** HP MSR 4-port T1/Fractional T1 HMIM Module (JG457A) **NEW** HP MSR 1-port E3/CE3/FE3 HMIM Module (JG436A) **NEW** HP MSR 1-port T3/CT3/FT3 HMIM Module (JG435A) **NEW** HP MSR 1-port OC-3c/STM-1c POS HMIM Module (JG438A) **NEW** HP MSR G2 128-channel Voice Processing Module (JG417A) **NEW** HP MSR 1U HMIM Adapter Module (JG416A) **NEW** HP MSR 0.5U HMIM Adapter Module (JG415A)
Power cords	HP X290 MSR30 1m RPS Cable (JD637A)
Memory	HP X600 1G Compact Flash Card (JC684A) HP X600 512M Compact Flash Card (JC685A) HP X600 256M Compact Flash Card (JC686A) **NEW** HP X610 2GB DDR3 SDRAM UDIMM Memory (JG529A) **NEW** HP X610 4GB DDR3 SDRAM UDIMM Memory (JG530A)

Learn more at
hp.com/networking

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-9529ENW, November 2013