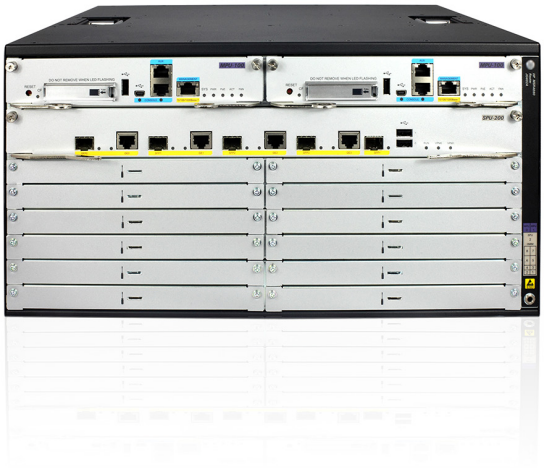
HPE MSR4000 Router Series



Key features

- Up to 36 Mpps forwarding performance; support for multiple concurrent services
- High reliability with separated hardware data and control planes, and dual main processing units (MPUs)
- HPE Open Application Platform (OAP) for HPE AllianceOne applications
- Powerful aggregation capacity; integrated 10GbE; support for up to 64 E1 or eight T3 ports
- Zero-touch solution with single-pane-of-glass management

Product overview

The HPE MSR4000 Router Series, the next generation of router from Hewlett Packard Enterprise (HPE), is a component of the HPE FlexBranch solution, which is a part of the comprehensive HPE FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for extra-large branch offices, headquarters, and campuses. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management. The MSR4000 series leverages separated data and control planes, dual main processing units (MPUs), and support for up to four power supplies, which provides outstanding performance and reliability.

The MSR4000 routers provide a full-featured, resilient routing platform with the latest multicore CPUs, offer 10 Gigabit SFP+ integrated, provide an enhanced PCI bus, and ship with the latest version of HPE Comware software to help enable high performance with concurrent services. The MSR4000 series provides a full-featured, resilient routing platform, including IPv6 and Multiprotocol Label Switching (MPLS), with up to 36 Mpps forwarding capacity and 28 Gbps of IPSec Virtual Private Networks (VPN) encrypted throughput. These routers also support HPE Open Application Platform (OAP) modules to deliver integrated industry-leading HPE AllianceOne partner applications such as virtualization, unified communications and collaboration (UC&C), and application optimization capabilities.

The MSR4000 series provides an agile, flexible network infrastructure that enables you to quickly adapt to your changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform.

Features and benefits

Performance

- Excellent forwarding performance

  Provides forwarding performance up to 36 Mpps (24.2 Gbps); meets the bandwidth-intensive application demands of enterprise businesses. Excellent full service performance (NAT + QoS + ACL Performance by Platform, IMIX Traffic), 1 Gbps for SPU-100, 3 Gbps for SPU-200, 8 Gbps for SPU-300

- Powerful security capacity

  The MSR4000 series is available with standard or high encryption, an embedded hardware encryption accelerator to improve encryption performance; IPSec encryption throughput can be up to 28 Gbps with a maximum of 10,000 IPSec VPN tunnels

Product architecture

- SDN/OpenFlow

  OpenFlow is the communications interface defined between the control and forwarding layers of a SDN (Software-Defined Networking) architecture. OpenFlow separates the data forwarding and routing decision functions. It keeps the flow-based forwarding function and employs a separate controller to make routing decisions. OpenFlow matches packets against one or more flow tables. MSR support OpenFlow 1.3.1

- Ideal multiservice platform

  Provides WAN router, Ethernet switch, stateful firewall, VPN, and Session Initiation Protocol (SIP) or voice gateway all in one device

- Advanced hardware architecture

  Provides multicore processors, Gigabit switching, and PCIe bus; dual main processing units, four internal power supplies (N+1 configuration), and internal and external CF cards are offered; new high-performance MIM modules (HMIM) supported

- New operating system version

  Ships with new Comware v7 Operating System delivering the latest in virtualization and routing

- Open Application Platform architecture

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

- Distributed architecture with separation of data and control planes

  Delivers enhanced fault tolerance and facilitates near continuous operation and zero service disruption during planned or unplanned control-plane events; service processing units (SPUs) perform data forwarding, encryption, or decryption, and analyzing or filtering of data packets; main processing units perform route calculation, forward table maintenance, and configure and monitor the SPU

- Field-programmable gate array (FPGA)

  Improves the bandwidth of I/O module slots from 100 Mbps to 1000 Mbps, and improves uplink performance from 1 Gbps to 10 Gbps

- Multi-Gigabit Fabric (MGF)

  Eases utilization of the main processor by transmitting Layer 2 packets directly via the MGF

- Main processing unit (MPU)

  Provides 1GbE management port; has default of 512 MB internal flash and 2 GB DDR3 memory

- Service processing units (SPU)

  Includes four 1000BASE-T and four SFP (combo) slots, two voice processing module slots, and 2 GB DDR3 memory; SPU 200/300 also has one 10GbE SFP+ slot; forwarding performance: 10 Mpps (SPU-100), 20 Mpps (SPU-200), 36 Mpps (SPU-300)

  SPU-100-X1 and SPU-400-X1 have ten 1000BASE-T or SFP (combo) ports

Connectivity

- Powerful aggregation capacity

  Supports integrated 10GbE LAN, and up to 64 E1 or eight T3 ports, and up to 148 Giga ports on one chassis

- High-density port connectivity

  Provides up to eight interface module slots and up to four on-board Gigabit Ethernet and one 10GbE ports

- Multiple WAN interfaces

  Provides traditional links with E1, T1, Serial, Asynchronous Transfer Mode (ATM), and ISDN; high-density Ethernet access with WAN Fast Ethernet and Gigabit Ethernet with POE/POE+; and high-speed T3, 155 Mbps OC3 access options

- Packet storm protection

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

- Ethernet Virtual Interconnect (EVI)

  EVI is a MAC-in-IP technology that provides Layer 2 connectivity between distant Layer 2 network sites across an IP routed network. It is used for connecting geographically dispersed sites of a virtualized large-scale data center that requires Layer 2 adjacency

- VXLAN (Virtual Extensible LAN)

  VXLAN (Virtual Extensible LAN, scalable virtual local area network) is an IP-based network, using the “MAC in UDP” package of Layer VPN technology. VXLAN can be based on an existing ISP or enterprise IP networks for decentralized physical site provides Layer 2 communication, and can provide service isolation for different tenants.

- Virtual Private LAN Service (VPLS)

  Virtual Private LAN Service (VPLS) delivers a point-to-multipoint L2VPN service over an MPLS or IP backbone. The backbone is transparent to the customer sites, which can communicate with each other as if they were on the same LAN. The following protocols support on MSRs, RFC4447, RFC4761 and RFC4762, BFD detection in VPLS, support hierarchical HOPE (H-VPLS), MAC address recovery in H-VPLS to speed up convergence

- 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

- USB interface

  Uses USB memory disk to download and upload configuration or OS image files; 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, and 10/100/1000BASE-T auto-speed detection plus auto duplex and MDI/MDI-X

Layer 2 switching

- 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)

- Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping

  Controls and manages the flooding of multicast packets in a Layer 2 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

Layer 3 routing

- Static IPv4 routing

  Provides simple manually configured IPv4 routing

- Routing Information Protocol (RIP)

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

- Open shortest path first (OSPF)

  Delivers faster convergence; uses this link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

- Border Gateway Protocol 4 (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; scales to very large networks

- Intermediate system to intermediate system (IS-IS)

  Uses a path vector Interior Gateway Protocol (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 design

- Routing Information Protocol next generation (RIPng)

  Extends RIPv2 to support IPv6 addressing

- OSPFv3

  Provides OSPF support for IPv6

- BGP+

  Extends BGP-4 to support Multiprotocol BGP (MBGP), 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; 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 Layer 2 or Layer 3 protocol, which reduces complexity and increases performance; supports graceful restart for reduced failure impact; supports LSP tunneling and multilevel stacks

- Multiprotocol Label Switching (MPLS) Layer 3 VPN

  Allows Layer 3 VPNs across a provider network; uses Multiprotocol BGP (MBGP) to establish private routes for increased security; supports RFC 2547bis multiple autonomous system VPNs for added flexibility; supports IPv6 MPLS VPN

- Multiprotocol Label Switching (MPLS) Layer 2 VPN

  Establishes simple Layer 2 point-to-point VPNs across a provider network using only MPLS Label Distribution Protocol (LDP); requires no routing and therefore decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; 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; supports access control lists (ACLs), IP prefix, AS paths, community lists, and aggregate policies

Layer 3 services

- NAT-PT

  Network Address Translation-Protocol Translation (NAT-PT) enables communication between IPv4 and IPv6 nodes by translating between IPv4 and IPv6 packets. It performs IP address translation, and according to different protocols, performs semantic translation for packets. This technology is only suitable for communication between a pure IPv4 node and a pure IPv6 node

- WAN Optimization

  MSR performs optimization using TFO and a combination of DRE, Lempel-Ziv (LZ) compression to provide the bandwidth optimization for file service and web applications. The policy engine module determines which traffic can be optimized and which optimization action should be taken. A pair of WAN optimization equipment can discover each other automatically and complete the negotiation to establish a TCP optimization session

- Address Resolution Protocol (ARP)

  Determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network

- 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 operation across subnets

Quality of Service (QoS)

- Hierarchical quality of service (HQoS) or Nested QoS

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

- Traffic policing

  Supports Committed Access Rate (CAR) and line rate

- Congestion management

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

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

  Delivers congestion avoidance capabilities through the use of queue management algorithms

- Other QoS technologies

  Supports traffic shaping, MPLS QoS, MP QoS or LFI, and Control Plane Policing (CoPP)

Security

- IPS

  Built-in Intrusion Prevention System (IPS) detects and protects the branch office from security threats. Optional HPE integration filters for client-side, branch protection from exploits and vulnerabilities

- Zone based firewall

  Zone-Based Policy Firewall changes the firewall configuration from the older interface-based model to a more flexible, more easily understood zone-based model. Interfaces are assigned to zones, and inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface

- Enhanced stateful firewall

  Application layer protocol inspection, Transport layer protocol inspection, ICMP error message check, and TCP SYN check. Support more L4 and L7 protocols like TCP, UDP, UDP-Lite, ICMPv4/ICMPv6, SCTP, DCCP, RAWIP, HTTP, FTP, SMTP, DNS, SIP, H.323, SCCP

- Auto Discover VPN (ADVPN)

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

- IPSec VPN

  Supports DES, Triple DES (3DES), and Advanced Encryption Standard (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 a Layer 2 header or a Layer 3 protocol header; 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 packet due to lack of reverse path route or incorrect inbound interface; prevents source spoofing and distributed attacks

- Network login

  Allows authentication of multiple users per port

- RADIUS

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

- Network address translation (NAT)

  Supports one-to-one NAT, many-to-many NAT, and NAT control, enabling NAPT to support multiple connections; supports deny list in NAT, a limit on the number of connections, session logs, and multi-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; increases the security of Secure File Transfer Protocol (SFTP) transfers

Convergence

- Internet Group Management Protocol (IGMP)

  Utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks; 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; 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; is used for inter-domain multicast applications

- Multicast Border Gateway Protocol (MBGP)

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

Integration

- Embedded VPN and firewall

  Provides enhanced stateful packet inspection and filtering; delivers advanced VPN services with Triple DES (3DES) and Advanced Encryption Standard (AES) encryption at high performance and low latency, URL filtering, and application prioritization and enhancement

- Embedded NetStream

  Improves traffic distribution using powerful scheduling algorithms, including Layer 4 to 7 services; monitors the health status of servers and firewalls

- 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

- Intelligent Resilient Framework (IRF)

  IRF allows the customer build an IRF stack, namely a logical device, by interconnecting multiple devices through stack ports. The customer can manage all the devices in the IRF stack by managing the logical device, which is cost-effective like a box-type device, and scalable and highly reliable like a chassis-type distributed device

- Backup center

  Acts as a part of the management and backup function to provide backup for device interfaces; 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; supports VRRP load balancing

- In-Service Software Upgrade (ISSU)

  Lowers downtime caused by planned maintenance and software upgrades

- Embedded Automation Architecture (EAA)

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

- Multiple internal power supply slots

  Delivers higher reliability with a maximum of four internal power supplies, which can be installed

- 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

- HPE Intelligent Management Center (IMC)

  Integrates fault management, element configuration, and network monitoring from a central vantage point; built-in support for third-party devices 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 configuration comparison tools, 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; offers multiple privilege levels with password protection; ACLs provide telnet and Simple Network Management Protocol (SNMP) access; local and remote syslog capabilities allow logging of all access

- SNMPv1, v2, and v3

  Provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption

- Remote monitoring (RMON)

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

- FTP, TFTP, and SFTP support

  Offers different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; trivial FTP (TFTP) is a simpler method using User Datagram Protocol (UDP); Secure File Transfer Protocol (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; 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 order of severity; outputs the network information to multiple channels based on user-defined rules

- Management interface control

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

- Network Quality Analyzer (NQA)

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

- Role-based security

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

- Standards-based authentication support for LDAP

  Integrates seamlessly into existing authentication services

Ease of deployment

- Zero-touch deployment

  Supports TR069, 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, thereby 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

- For details on Limited Lifetime warranty and software releases available with your product purchase, please refer to hpe.com/networking/support

HPE MSR4000 Router Series

Specifications	HPE MSR4060 Router Chassis (JG403A)	HPE MSR4080 Router Chassis (JG402A)
I/O ports and slots	2 MPU (Main Processing Unit) slots 1 SPU (Service Processing Unit) slot 6 HMIM slots 4 Power Supply slots	2 MPU (Main Processing Unit) slots 1 SPU (Service Processing Unit) slot 8 HMIM slots 4 Power Supply slots
Physical characteristics		
Dimensions	17.32(w) x 18.9(d) x 6.89(h) in. (44 x 48 x 17.50 cm) (4U height)	17.32(w) x 18.9(d) x 8.64(h) in. (44 x 48 x 21.95 cm) (5U height)
Weight	45.52 lb (20.65 kg)	49.93 lb (22.65 kg)
Memory and processor	MPU-100, 2 cores RISC @ 1 GHz, 512 MB flash capacity, 2 GB DDR3 SDRAM SPU-100, 8 cores RISC @ 1 GHz, 2 GB DDR3 SDRAM SPU-200, 16 cores RISC @ 1 GHz, 2 GB DDR3 SDRAM SPU-300, 32 cores RISC @ 1 GHz, 4 GB DDR3 SDRAM SPU-100-X1, 8 cores RISC @ 1.2 GHz, 2 GB DDR3 SDRAM SPU-400-X1, 16 cores RISC @ 1.5 GHz, 4 GB DDR3 SDRAM	MPU-100, 2 cores RISC @ 1 GHz, 512 MB flash capacity, 2 GB DDR3 SDRAM SPU-100, 8 cores RISC @ 1 GHz, 2 GB DDR3 SDRAM SPU-200, 16 cores RISC @ 1 GHz, 2 GB DDR3 SDRAM SPU-300, 32 cores RISC @ 1 GHz, 4 GB DDR3 SDRAM SPU-100-X1, 8 cores RISC @ 1.2 GHz, 2 GB DDR3 SDRAM SPU-400-X1, 16 cores RISC @ 1.5 GHz, 4 GB DDR3 SDRAM
Mounting and enclosure	Desktop or can be mounted in an EIA standard 19-inch telco rack when used with the rack-mount kit in the package.	Desktop or can be mounted in an EIA standard 19-inch telco rack when used with the rack-mount kit in the package.
Performance		
Throughput	SPU-100/SPU-200/SPU-300/SPU-400	SPU-100/SPU-200/SPU-300/SPU-400
Routing table size	(10 Mpps/20 Mpps/36 Mpps/60 Mpps)	(10 Mpps/20 Mpps/36 Mpps/60 Mpps)
Forwarding table size	1000000 entries (IPv4), 1000000 entries (IPv6) 1000000 entries (IPv4), 1000000 entries (IPv6)	1000000 entries (IPv4), 1000000 entries (IPv6) 1000000 entries (IPv4), 1000000 entries (IPv6)
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 90%, noncondensing	5% to 90%, 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 90%, noncondensing	5% to 90%, noncondensing
Altitude	Up to 16,404 ft (5 km)	Up to 16,404 ft (5 km)

HPE MSR4000 Router Series (continued)

Specifications	HPE MSR4060 Router Chassis (JG403A)	HPE MSR4080 Router Chassis (JG402A)
Electrical characteristics		
Frequency	50/60 Hz	50/60 Hz
Maximum heat dissipation	285/347 BTU/hr (300.67/366.09 kJ/hr), lower number is with SPU-100 module installed; higher number is for SPU-200	297/358 BTU/hr (313.33/377.69 kJ/hr), lower number is with SPU-100 module installed; higher number is for SPU-200
AC voltage	100–240 VAC	100–240 VAC
DC voltage	–36 to –75 VDC	–36 to –75 VDC
Maximum power rating	300W	300W
PoE power	450W PoE+	450W PoE+
	Note 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. 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). No default power supply is included in the chassis; a minimum of one/maximum of four power supplies should be ordered.	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. 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). No default power supply is included in the chassis; a minimum of one/maximum of four power supplies should be ordered.
Reliability		
MTBF (years)	178.66	178.66
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; AS/NZS 60950-1; GB 4943.1	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; FDA 21 CFR Subchapter J; AS/NZS 60950-1; GB 4943.1
Emissions	EN 61000-4-11:2004; ANSI C63.4-2009; AS/NZS CISPR 22:2009; CISPR 22 Ed2.0 2008-09; EN 55022:2010; EN 61000-3-3:2008; GB 9254-2008; IEC 61000-3-2 Ed3.0 (2009-02); IEC 61000-3-3 Ed2.0 (2008-06); VCCI V-4/2012.04; CISPR 24 Ed2.0 2010-08; EN 55024:2010; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-2:2009; EN 61000-4-29:2000; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; EN 61000-4-8:2010; ETSI EN 300 386 V1.6.1 (2012-09); FCC 47 CFR Part 15 (latest current version); ICES-003 Issue 5; IEC 61000-4-11 Ed2.0 (2004-03); IEC 61000-4-2 Ed2.0 (2008-12); IEC 61000-4-29 Ed1.0 (2000-08); IEC 61000-4-3 Ed3.2 (2010-04); IEC 61000-4-4 Ed3.0 (2012-04); IEC 61000-4-5 Ed2.0 (2005-11); IEC 61000-4-6 Ed3.0 (2008-10); IEC 61000-4-8 Ed2.0 (2009-09); VCCI V-3/2013.04	EN 61000-4-11:2004; ANSI C63.4-2009; AS/NZS CISPR 22:2009; CISPR 22 Ed2.0 2008-09; EN 55022:2010; EN 61000-3-3:2008; GB 9254-2008; IEC 61000-3-2 Ed3.0 (2009-02); IEC 61000-3-3 Ed2.0 (2008-06); VCCI V-4/2012.04; CISPR 24 Ed2.0 2010-08; EN 55024:2010; EN 61000-3-2:2006+A1:2009+A2:2009; EN 61000-4-2:2009; EN 61000-4-29:2000; EN 61000-4-3:2006; EN 61000-4-4:2012; EN 61000-4-5:2006; EN 61000-4-6:2009; EN 61000-4-8:2010; ETSI EN 300 386 V1.6.1 (2012-09); FCC 47 CFR Part 15 (latest current version); ICES-003 Issue 5; IEC 61000-4-11 Ed2.0 (2004-03); IEC 61000-4-2 Ed2.0 (2008-12); IEC 61000-4-29 Ed1.0 (2000-08); IEC 61000-4-3 Ed3.2 (2010-04); IEC 61000-4-4 Ed3.0 (2012-04); IEC 61000-4-5 Ed2.0 (2005-11); IEC 61000-4-6 Ed3.0 (2008-10); IEC 61000-4-8 Ed2.0 (2009-09); VCCI V-3/2013.04
Telecom	FCC part 68; CS-03	FCC part 68; CS-03

HPE MSR4000 Router Series (continued)

Specifications	HPE MSR4060 Router Chassis (JG403A)	HPE MSR4080 Router Chassis (JG402A)
Management	IMC—Intelligent Management Center; 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	IMC—Intelligent Management Center; 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 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)

BGP	RFC 1163 Border Gateway Protocol (BGP) RFC 1267 Border Gateway Protocol 3 (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 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 3107 Support BGP carry Label for MPLS RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (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 Mesh Internal BGP (IBGP) RFC 4724 Graceful Restart Mechanism for BGP RFC 4760 Multiprotocol Extensions for BGP-4 RFC 1998 An Application of the BGP Community Attribute in Multi-home Routing
Denial of service protection	CPU DoS Protection	Rate Limiting by ACLs	
Device management	RFC 1155 Structure and Management Information (SMIv1) RFC 1157 SNMPv1/v2c RFC 1305 NTPv3 RFC 1591 DNS (client) RFC 1902 (SNMPv2)	RFC 1908 (SNMPv1/2 Coexistence) RFC 1945 Hypertext Transfer Protocol—HTTP/1.0 RFC 2271 Framework RFC 2573 (SNMPv3 Applications) RFC 2576 (Coexistence between SNMPv1, v2, v3)	RFC 2578-2580 SMIv2 RFC 2579 (SMIv2 Text Conventions) RFC 2580 (SMIv2 Conformance) RFC 3416 (SNMP Protocol Operations v2) RFC 3417 (SNMP Transport Mappings)

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

General protocols

RFC 768 UDP
RFC 760 DoD standard Internet Protocol
RFC 764 Telnet Protocol specification
RFC 777 Internet Control Message Protocol
RFC 783 TFTP Protocol (revision 2)
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 813 Window and Acknowledgement Strategy in TCP
RFC 815 IP datagram reassembly algorithms
RFC 826 ARP
RFC 854 Telnet Protocol Specification
RFC 855 Telnet Option Specifications
RFC 856 Telnet Binary Transmission
RFC 857 Telnet Echo Option
RFC 858 Telnet Suppress Go Ahead Option
RFC 862 Echo Service (TCP Echo)
RFC 879 TCP maximum segment size and related topics
RFC 882 Domain names: Concepts and facilities
RFC 883 Domain names: Implementation specification
RFC 894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
RFC 896 Congestion Control in IP/TCP Internetworks
RFC 906 Bootstrap loading using TFTP (Trivial File Transfer Protocol)
RFC 917 Internet Subnets
RFC 919 Broadcasting Internet Datagrams
RFC 922 Broadcasting Internet Datagrams in the Presence of Subnets (IP_BROAD)
RFC 925 Multi-LAN Address Resolution
RFC 926 Protocol for providing the connectionless mode network services
RFC 950 Internet Standard Subnetting Procedure
RFC 951 BOOTP
RFC 958 Network Time Protocol (NTP)
RFC 959 File Transfer Protocol (FTP)
RFC 973 Domain system changes and observations
RFC 988 Host extensions for IP multicasting
RFC 1027 Proxy ARP
RFC 1034 Domain names—concepts and facilities
RFC 1035 Domain names—implementation and specification
RFC 1048 BOOTP (Bootstrap Protocol) vendor information extensions
RFC 1054 Host extensions for IP multicasting
RFC 1058 RIPv1
RFC 1059 Network Time Protocol (version 1) specification and implementation
RFC 1060 Assigned numbers
RFC 1063 IP MTU (Maximum Transmission Unit) discovery options
RFC 1071 Computing the Internet checksum
RFC 1072 TCP extensions for long-delay paths
RFC 1079 Telnet terminal speed option
RFC 1084 BOOTP (Bootstrap Protocol) vendor information extensions
RFC 1091 Telnet Terminal-Type Option
RFC 1093 NSFNET routing architecture
RFC 1101 DNS encoding of network names and other types
RFC 1119 Network Time Protocol (version 2) specification and implementation
RFC 1122 Requirements for Internet Hosts—Communication Layers
RFC 1141 Incremental updating of the Internet checksum
RFC 1142 OSI IS-IS Intra-domain Routing Protocol
RFC 1164 Application of the Border Gateway Protocol in the Internet
RFC 1166 Internet address used by Internet Protocol (IP)
RFC 1171 Point-to-Point Protocol for the transmission of multi-protocol datagrams over Point-to-Point links
RFC 1172 Point-to-Point Protocol (PPP) initial configuration options
RFC 1185 TCP Extension for High-Speed Paths
RFC 1191 Path MTU discovery
RFC 1195 OSI ISIS for IP and Dual Environments
RFC 1213 Management Information Base for Network Management of TCP/IP-based internets
RFC 1253 (OSPFv2)
RFC 1265 BGP Protocol Analysis
RFC 1266 Experience with the BGP Protocol
RFC 1268 Application of the Border Gateway Protocol in the Internet
RFC 1271 Remote Network Monitoring Management Information Base
RFC 1284 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 1286 Definitions of Managed Objects for Bridges
RFC 1294 Multiprotocol Interconnect over Frame Relay
RFC 1305 NTPv3 (IPv4 only)
RFC 1321 The MD5 Message-Digest Algorithm
RFC 1323 TCP Extensions for High Performance
RFC 1331 The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
RFC 1333 PPP Link Quality Monitoring
RFC 1334 PPP Authentication Protocols
RFC 1349 Type of Service
RFC 1350 TFTP Protocol (revision 2)
RFC 1364 BGP OSPF Interaction
RFC 1370 Applicability Statement for OSPF
RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP)
RFC 1393 Traceroute Using an IP Option
RFC 1395 BOOTP (Bootstrap Protocol) Vendor Information Extensions
RFC 1398 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 1403 BGP OSPF Interaction
RFC 1444 Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1449 Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC 1473 The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
RFC 1483 Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1490 Multiprotocol Interconnect over Frame Relay
RFC 1497 BOOTP (Bootstrap Protocol) Vendor Information Extensions
RFC 1519 CIDR
RFC 1531 Dynamic Host Configuration Protocol
RFC 1532 Clarifications and Extensions for the Bootstrap Protocol
RFC 1533 DHCP Options and BOOTP Vendor Extensions
RFC 1534 Interoperation Between DHCP and BOOTP
RFC 1541 Dynamic Host Configuration Protocol
RFC 1542 BOOTP Extensions
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1548 The Point-to-Point Protocol (PPP)
RFC 1549 PPP in HDLC Framing

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

RFC 1570 PPP LCP (Point-to-Point Protocol Link Control Protocol) Extensions
RFC 1577 Classical IP and ARP over ATM
RFC 1597 Address Allocation for Private Internets
RFC 1618 PPP over ISDN
RFC 1619 PPP over SONET/SDH (Synchronous Optical Network/ Synchronous Digital Hierarchy)
RFC 1624 Incremental Internet Checksum
RFC 1631 NAT
RFC 1650 Definitions of Managed Objects for the Ethernet-like Interface Types using SMIv2
RFC 1661 The Point-to-Point Protocol (PPP)
RFC 1662 PPP in HDLC-like Framing
RFC 1700 ASSIGNED NUMBERS
RFC 1701 Generic Routing Encapsulation
RFC 1702 Generic Routing Encapsulation over IPv4 networks
RFC 1717 The PPP Multilink Protocol (MP)
RFC 1721 RIP-2 Analysis
RFC 1722 RIP-2 Applicability
RFC 1723 RIPv2
RFC 1724 RIP Version 2 MIB Extension
RFC 1757 Remote Network Monitoring Management Information Base
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 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1884 IP Version 6 Addressing Architecture
RFC 1885 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 1886 DNS Extensions to support IP version 6
RFC 1889 RTP (Real-Time Protocol): A Transport Protocol for Real-Time Applications. Audio-Video Transport Working Group
RFC 1933 Transition Mechanisms for IPv6 Hosts and Routers
RFC 1945 Hypertext Transfer Protocol—HTTP/1.0
RFC 1962 The PPP Compression Control Protocol (CCP)
RFC 1966 BGP Route Reflection An alternative to full mesh IBGP
RFC 1970 Neighbor Discovery for IP Version 6 (IPv6)
RFC 1971 IPv6 Stateless Address Auto-configuration
RFC 1972 A Method for the Transmission of IPv6 Packets over Ethernet Networks
RFC 1981 Path MTU Discovery for IP version 6
RFC 1982 Serial Number Arithmetic
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2001 TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms
RFC 2002 IP Mobility Support
RFC 2003 IP Encapsulation within IP
RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2
RFC 2012 SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013 SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
RFC 2018 TCP Selective Acknowledgement Options
RFC 2021 Remote Network Monitoring Management Information Base Version 2 using SMIv2
RFC 2073 An IPv6 Provider-Based Unicast Address Format
RFC 2082 RIP-2 MD5 Authentication
RFC 2091 Triggered Extensions to RIP to Support Demand Circuits
RFC 2104 HMAC: Keyed-Hashing for Message Authentication
RFC 2131 DHCP
RFC 2132 DHCP Options and BOOTP Vendor Extensions
RFC 2136 Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC 2138 Remote Authentication Dial In User Service (RADIUS)
RFC 2205 Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification
RFC 2209 Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules
RFC 2210 Use of RSVP (Resource Reservation Protocol) in Integrated Services
RFC 2225 Classical IP and ARP over ATM
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 2292 Advanced Sockets API for IPv6
RFC 2309 Recommendations on queue management and congestion avoidance in the Internet
RFC 2327 SDP: Session Description Protocol
RFC 2338 VRRP
RFC 2344 Reverse Tunneling for Mobile IP
RFC 2358 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 2364 PPP Over AAL5
RFC 2365 Administratively Scoped IP Multicast
RFC 2373 IP Version 6 Addressing Architecture
RFC 2374 An IPv6 Aggregatable Global Unicast Address Format
RFC 2375 IPv6 Multicast Address Assignments
RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2427 Multiprotocol Interconnect over Frame Relay
RFC 2428 FTP Extensions for IPv6 and NATs
RFC 2433 Microsoft PPP CHAP (Challenge Handshake Authentication Protocol) Extensions
RFC 2451 The ESP CBC-Mode Cipher Algorithms
RFC 2452 IP Version 6 Management Information Base for the Transmission Control Protocol
RFC 2453 RIPv2
RFC 2454 IP Version 6 Management Information Base for the User Datagram Protocol
RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
RFC 2462 IPv6 Stateless Address Auto-configuration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 Management Information Base for IP Version 6: ICMPv6 Group
RFC 2472 IP Version 6 over PPP
RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

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

RFC 2507 IP Header Compression
RFC 2508 Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
RFC 2509 IP Header Compression over PPP
RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2519 A Framework for Inter-Domain Route Aggregation
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2543 SIP: Session Initiation Protocol
RFC 2548 (MS-RAS-Vendor only)
RFC 2553 Basic Socket Interface Extensions for IPv6
RFC 2570 Introduction to Version 3 of the Internet-standard Network Management Framework
RFC 2581 TCP Congestion Control
RFC 2597 Assured Forwarding PHB Group
RFC 2598 An Expedited Forwarding PHB
RFC 2615 PPP over SONET/SDH (Synchronous Optical Network/ Synchronous Digital Hierarchy)
RFC 2616 HTTP Compatibility v1.1
RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
RFC 2618 RADIUS Authentication Client MIB
RFC 2620 RADIUS Accounting Client MIB
RFC 2644 Changing the Default for Directed Broadcasts in Routers
RFC 2661 L2TP
RFC 2663 NAT Terminology and Considerations
RFC 2665 Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 2668 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 2675 IPv6 Jumbograms
RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2685 Virtual Private Networks Identifier
RFC 2686 The Multi-Class Extension to Multi-Link PPP
RFC 2694 DNS extensions to Network Address Translators (DNS_ALG)
RFC 2698 A Two Rate Three Color Marker
RFC 2702 Requirements for Traffic Engineering Over MPLS
RFC 2711 IPv6 Router Alert Option
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 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing
RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2866 RADIUS Accounting
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 2884 Performance Evaluation of Explicit Congestion Notification (ECN) in IP Networks
RFC 2894 Router Renumbering for IPv6
RFC 2917 A Core MPLS IP VPN Architecture
RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2963 A Rate Adaptive Shaper for Differentiated Services
RFC 2965 HTTP State Management Mechanism
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 2976 The SIP INFO Method
RFC 2993 Architectural Implications of NAT
RFC 3011 The IPv4 Subnet Selection Option for DHCP
RFC 3022 Traditional IP Network Address Translator (Traditional NAT)
RFC 3024 Reverse Tunneling for Mobile IP, revised
RFC 3025 Mobile IP Vendor/ Organization-Specific Extensions
RFC 3027 Protocol Complications with the IP Network Address Translator
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3036 LDP Specification
RFC 3037 LDP (Label Distribution Protocol) Applicability
RFC 3041 Privacy Extensions for Stateless Address Auto-configuration in IPv6
RFC 3046 DHCP Relay Agent Information Option
RFC 3063 MPLS Loop Prevention Mechanism
RFC 3097 RSVP (Resource Reservation Protocol) Cryptographic Authentication—Updated Message Type Value
RFC 3115 Mobile IP Vendor/Organization-Specific Extensions
RFC 3137 OSPF Stub Router Advertisement
RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP
RFC 3176 InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks
RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP-Tunnels
RFC 3215 LDP State Machine
RFC 3220 IP Mobility Support for IPv4
RFC 3246 Expedited Forwarding PHB
RFC 3261 SIP: Session Initiation Protocol
RFC 3262 Reliability of Provisional Responses in Session Initiation Protocol (SIP)
RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3270 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
RFC 3273 Remote Network Monitoring Management Information Base for High Capacity Networks
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 3306 Unicast-Prefix-based IPv6 Multicast Addresses
RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses
RFC 3311 The Session Initiation Protocol (SIP) UPDATE Method
RFC 3319 Dynamic Host Configuration Protocol v6 (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

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

RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
RFC 3344 IP Mobility Support for IPv4
RFC 3345 Border Gateway Protocol (BGP) Persistent Route Oscillation Condition
RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System
RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
RFC 3392 Support BGP capabilities advertisement
RFC 3410 Introduction to Version 3 of the Internet-standard Network Management Framework
RFC 3442 The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4
RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 3478 Graceful Restart Mechanism for Label Distribution Protocol
RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP)
RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
RFC 3493 Basic Socket Interface Extensions for IPv6
RFC 3495 Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration
RFC 3509 OSPF ABR Behavior
RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
RFC 3515 The Session Initiation Protocol (SIP) Refer Method
RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3527 Link Selection sub-option for the Relay Agent Information Option for DHCPv4
RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6
RFC 3547 The Group Domain of Interpretation
RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering
RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC 3569 An Overview of Source-Specific Multicast (SSM)
RFC 3584 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 3587 IPv6 Global Unicast Address Format
RFC 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC 3596 DNS Extensions to Support IP Version 6
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 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3621 Power Ethernet MIB
RFC 3623 Graceful OSPF Restart
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 3636 Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
RFC 3704 Unicast Reverse Path Forwarding (URPF)
RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3711 The Secure Real-time Transport Protocol (SRTP)
RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3737 IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB (Management Information Base) modules
RFC 3768 Virtual Router Redundancy Protocol (VRRP)
RFC 3782 The NewReno Modification to TCP's Fast Recovery Algorithm
RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3809 Generic Requirements for Provider Provisioned Virtual Private Networks (VPNs)
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management
RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
RFC 3814 Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)
RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC 3847 Restart signaling for IS-IS
RFC 3879 Deprecating Site Local Addresses
RFC 3898 Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
RFC 3916 Requirements for Pseudo-wire Emulation Edge-to-Edge (PWE3)
RFC 3917 Requirements for IP Flow Information Export (IPFIX)
RFC 3942 Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options
RFC 3948 UDP Encapsulation of IPSec ESP Packets
RFC 3954 Cisco Systems NetFlow Services Export Version 9
RFC 3973 Protocol Independent Multicast—Dense Mode (PIM-DM): Protocol Specification (Revised)
RFC 3985 Pseudo-wire Emulation Edge-to-Edge (PWE3) Architecture
RFC 4022 Management Information Base for the Transmission Control Protocol (TCP)
RFC 4023 Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
RFC 4026 Provider Provisioned VPN terminology
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

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

RFC 4075 Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
RFC 4105 Requirements for Inter-Area MPLS Traffic Engineering
RFC 4109 Algorithms for Internet Key Exchange version 1 (IKEv1)
RFC 4113 Management Information Base for the User Datagram Protocol (UDP)
RFC 4124 Protocol Extensions for Support of DiffServ-aware MPLS Traffic Engineering
RFC 4125 Maximum Allocation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering
RFC 4127 Russian Dolls Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering
RFC 4133 Entity MIB (Version 3)
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4221 Multiprotocol Label Switching (MPLS) Management Overview
RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance
RFC 4242 Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 4244 An Extension to the Session Initiation Protocol (SIP) for Request History Information
RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers
RFC 4251 The Secure Shell (SSH) Protocol Architecture
RFC 4252 The Secure Shell (SSH) Authentication Protocol
RFC 4253 The Secure Shell (SSH) Transport Layer Protocol
RFC 4254 The Secure Shell (SSH) Connection Protocol
RFC 4272 BGP Security Vulnerabilities Analysis
RFC 4291 IP Version 6 Addressing Architecture
RFC 4292 IP Forwarding Table MIB
RFC 4293 Management Information Base for the Internet Protocol (IP)
RFC 4294 IPv6 Node Requirements
RFC 4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4306 Internet Key Exchange v2 (IKEv2) Protocol
RFC 4308 Cryptographic Suites for IPSec
RFC 4361 Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4365 Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4377 Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks
RFC 4381 Analyses of the Security of BGP/MPLS IP VPNs
RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base
RFC 4384 BGP Communities for Data Collection
RFC 4385 Pseudo-wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 4419 Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 4444 Management Information Base for Intermediate System to Intermediate System (IS-IS)
RFC 4446 IANA Allocations for Pseudo-wire Edge to Edge Emulation (PWE3)
RFC 4447 Pseudo-wire 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 4502 Remote Network Monitoring Management Information Base Version 2
RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4552 Authentication/Confidentiality for OSPFv3
RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 4561 Definition of a Record Route Object (RRO) Node-Id sub-Objects
RFC 4562 MAC-Forced Forwarding: A Method for Subscriber Separation on an Ethernet Access Network
RFC 4568 Session Description Protocol (SDP) Security Descriptions for Media Streams
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 Protocol Independent Multicast—Sparse Mode (PIM-SM): Protocol Specification (Revised)
RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC 4605 Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")
RFC 4607 Source-Specific Multicast for IP
RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
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 Multiprotocol Label Switching (MPLS) Networks
RFC 4632 Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
RFC 4649 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option
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 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
RFC 4741 NETCONF Configuration Protocol
RFC 4742 Using the NETCONF Configuration Protocol over Secure Shell (SSH)
RFC 4743 Using NETCONF over the Simple Object Access Protocol (SOAP)
RFC 4750 OSPF Version 2 Management Information Base

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

RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
RFC 4765 Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks
RFC 4781 Graceful Restart Mechanism for BGP with MPLS
RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
RFC 4797 Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
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 Pseudo-wire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service
RFC 4818 RADIUS Delegated-IPv6-Prefix Attribute
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 Auto-configuration
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 Auto-configuration in IPv6
RFC 5004 Avoid BGP Best Path Transitions from One External to Another
RFC 5007 DHCPv6 Leasequery
RFC 5015 Bidirectional Protocol Independent Multicast (BIDIR-PIM)
RFC 5036 LDP Specification
RFC 5060 Protocol Independent Multicast MIB
RFC 5065 Autonomous System Confederations for BGP
RFC 5072 IP Version 6 over PPP
RFC 5082 The Generalized TTL Security Mechanism (GTSM)
RFC 5085 Pseudo-wire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudo-wire
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 5120 M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)
RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags
RFC 5132 IP Multicast MIB
RFC 5187 OSPFv3 Graceful Restart
RFC 5214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 5240 Protocol Independent Multicast (PIM) Bootstrap Router MIB
RFC 5254 Requirements for Multi-Segment Pseudo-wire 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 5281 Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)
RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates
RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudo-wires in MPLS Networks
RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
RFC 5302 Domain-Wide Prefix Distribution with Two-Level IS-IS
RFC 5303 Three-Way Handshake for IS-IS Point-to-Point Adjacencies
RFC 5304 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC 5305 IS-IS Extensions for Traffic Engineering
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 5310 IS-IS Generic Cryptographic Authentication
RFC 5359 Session Initiation Protocol Service Examples
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 5415 Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
RFC 5416 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
RFC 5443 LDP IGP Synchronization
RFC 5492 Capabilities Advertisement with BGP-4
RFC 5496 The Reverse Path Forwarding (RPF) Vector TLV
RFC 5508 NAT Behavioral Requirements for ICMP
RFC 5539 NETCONF over Transport Layer Security (TLS)
RFC 5601 Pseudo-wire (PW) Management Information Base (MIB)
RFC 5602 Pseudo-wire (PW) over MPLS PSN Management Information Base (MIB)
RFC 5613 OSPF Link-Local Signaling
RFC 5659 An Architecture for Multi-Segment Pseudo-wire Emulation Edge-to-Edge
RFC 5681 TCP Congestion Control
RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
RFC 5833 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Base MIB
RFC 5834 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding MIB for IEEE 802.11
RFC 5880 Bidirectional Forwarding Detection
RFC 5881 BFD for IPv4 and IPv6 (Single Hop)
RFC 5881 Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)
RFC 5882 Generic Application of BFD
RFC 5883 BFD for Multihop Paths
RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
RFC 5969 IPv6 Rapid Deployment on IPv4 Infrastructures (6RD)—Protocol Specification
RFC 6037 Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs
RFC 6085 Address Mapping of IPv6 Multicast Packets on Ethernet

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

IP multicast	RFC 1112 IGMP RFC 2362 PIM Sparse Mode RFC 2710 Multicast Listener Discovery (MLD) for IPv6	RFC 2934 Protocol Independent Multicast MIB for IPv4 RFC 3376 IGMPv3 RFC 3376 IGMPv3 (host joins only)	RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
IPv6	RFC 2080 RIPng for IPv6 RFC 2460 IPv6 Specification RFC 2473 Generic Packet Tunneling in IPv6 RFC 2475 IPv6 DiffServ Architecture RFC 2529 Transmission of IPv6 Packets over IPv4	RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2740 OSPFv3 for IPv6 RFC 2893 Transition Mechanisms for IPv6 Hosts and 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
MIBs	RFC 1213 MIB II RFC 1493 Bridge MIB RFC 1724 RIPv2 MIB RFC 1850 OSPFv2 MIB RFC 1907 SNMPv2 MIB RFC 2011 SNMPv2 MIB for IP	RFC 2012 SNMPv2 MIB for TCP RFC 2013 SNMPv2 MIB for UDP RFC 2096 IP Forwarding Table MIB RFC 2233 Interfaces MIB RFC 2273 SNMP-NOTIFICATION-MIB RFC 2571 SNMP Framework MIB	RFC 2572 SNMP-MPD MIB RFC 2573 SNMP-Notification MIB RFC 2574 SNMP USM MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2737 Entity MIB (Version 2) RFC 2863 The Interfaces Group MIB RFC 3813 MPLS LSR MIB
Network management	IEEE 802.1D (STP) RFC 1098 Simple Network Management Protocol (SNMP) RFC 1158 Management Information Base for network management of TCP/IP-based internets: MIB-II RFC 1212 Concise MIB definitions RFC 1215 Convention for defining traps for use with the SNMP RFC 1389 RIPv2 MIB Extension RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2) RFC 1450 Management Information Base (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 RFC 1904 SNMPv2 Conformance	RFC 1905 SNMPv2 Protocol Operations RFC 1906 SNMPv2 Transport Mappings RFC 1908 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC 1918 Private Internet Address Allocation RFC 2037 Entity MIB using SMIv2 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) RFC 2272 SNMPv3 Management Protocol	RFC 2273 SNMPv3 Applications RFC 2274 USM for SNMPv3 RFC 2275 VACM for SNMPv3 RFC 2575 SNMPv3 View-based Access Control Model (VACM) RFC 3164 BSD syslog Protocol RFC 3411 An Architecture for Describing Simple Network 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) RFC 3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

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

OSPF	RFC 1245 OSPF protocol analysis RFC 1246 Experience with OSPF RFC 1583 OSPFv2	RFC 1587 OSPF NSSA RFC 1765 OSPF Database Overflow RFC 1850 OSPFv2 Management Information Base (MIB), traps	RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option RFC 3101 OSPF NSSA
QoS/CoS	IEEE 802.1P (CoS) RFC 2474 DS Field in the IPv4 and IPv6 Headers RFC 2475 DiffServ Architecture RFC 2597 DiffServ Assured Forwarding (AF)	RFC 2598 DiffServ Expedited Forwarding (EF) RFC 2697 A Single Rate Three Color Marker RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP	RFC 3247 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior) RFC 3260 New Terminology and Clarifications for DiffServ
Security	IEEE 802.1X Port Based Network Access Control RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication RFC 2138 RADIUS Authentication RFC 2139 RADIUS Accounting	RFC 2408 Internet Security Association and Key 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 2865 RADIUS Authentication 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 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	RFC 2405 The ESP DES-CBC Cipher Algorithm With 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 3948—UDP Encapsulation of IPSec ESP Packets 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

HPE MSR4000 Router Series accessories

Transceivers	HPE X110 100M SFP LC FX Transceiver (JD102B) HPE X110 100M SFP LC LX Transceiver (JD120B) HPE X110 100M SFP LC LH40 Transceiver (JD090A) HPE X110 100M SFP LC LH80 Transceiver (JD091A) HPE X120 1G SFP LC SX Transceiver (JD118B) HPE X120 1G SFP LC LX Transceiver (JD119B) HPE X120 1G SFP LC LH100 Transceiver (JD103A) HPE X120 1G SFP LC BX 10-U Transceiver (JD098B) HPE X120 1G SFP LC BX 10-D Transceiver (JD099B) HPE X120 1G SFP RJ45 T Transceiver (JD089B) HPE X130 10G SFP+ LC SR Transceiver (JD092B) HPE X130 10G SFP+ LC LR Transceiver (JD094B) HPE X130 10G SFP+ LC ER 40km Transceiver (JG234A) HPE X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable (JD095C) HPE X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable (JD096C) HPE X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable (JD097C) HPE X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable (JG081C)
Cables	HPE X200 V.24 DTE 3m Serial Port Cable (JD519A) HPE X200 V.24 DCE 3m Serial Port Cable (JD521A) HPE X200 V.35 DTE 3m Serial Port Cable (JD523A) HPE X200 V.35 DCE 3m Serial Port Cable (JD525A) HPE X260 Auxiliary Router Cable (JD508A) HPE X260 E1 RJ45 20m Router Cable (JD517A) HPE X260 E1 (2) BNC 75 ohm 3m Router Cable (JD175A) HPE X260 E1 BNC 20m Router Cable (JD514A) HPE X260 E1/2 BNC 75 ohm 40m Router Cable (JD516A) HPE X260 E1 RJ45 BNC 75-120 ohm Conversion Router Cable (JD511A) HPE X260 T1 Router Cable (JD518A) HPE X260 8E1 BNC 75 ohm 3m Router Cable (JD512A) HPE X260 T3/E3 Router Cable (JD531A) HPE X260 E1 RJ45 to 2xBNC 75ohm 3m Router Cable (JH294A) HPE X260 E1 RJ45 120 ohm 2m Router Cable (JC156A) HPE X260 E1 RJ45 120 ohm 15m Router Cable (JC151A) HPE X260 E1 RJ45 120 ohm 30m Router Cable (JC152A)

HPE MSR4000 Router Series accessories (continued)

Power supply	HPE X351 300W 100–240VAC to 12VDC Power Supply (JG527A) HPE X351 300W -48/-60VDC to 12VDC Power Supply (JG528A)
Router modules	HPE MSR4000 MPU-100-X1 Main Processing Unit (JM045A) HPE MSR4000 SPU-400-X1 Service Processing Unit (JM046A) HPE MSR4000 SPU-200 Service Processing Unit (JG414A) HPE MSR4000 SPU-100-X1 Service Proc Unit (R8V30A) HPE MSR 4p Gig-T HMIM-V2 Module (S0W32A) HPE MSR 16p Enhanced Async Serial HMIM-V2 Module (S0W35A) HPE MSR 1-port E1 Voice HMIM Module (JG429A) HPE MSR 2-port E1 Voice HMIM Module (JG431A) HPE MSR 1-port T1 Voice HMIM Module (JG430A) HPE MSR 4-port FXS HMIM Module (JG446A) HPE MSR 4-port FXO HMIM Module (JG447A) HPE MSR 4-port E and M HMIM Module (JG448A) HPE MSR 4-port Enhanced Sync/Async Serial HMIM Module (JG442A) HPE MSR 8-port Enhanced Sync/Async Serial HMIM Module (JG443A) HPE MSR 1p E3/CE3/FE3 HMIM Module (JG436A) HPE MSR 1-port OC-3c/STM-1c POS HMIM Module (JG438A) HPE MSR 0.5U HMIM Adapter Module (JG415A) HPE MSR 1U HMIM Adapter Module (JG416A) HPE MSR 8-port 10/100/1000BASE-T/2-port 1000BASE-X (Combo) Switch HMIM Module (JG741A) HPE MSR 2-port Gig-T HMIM Module (JG420A) HPE MSR 4-port Gig-T HMIM Module (JG421A)* HPE MSR 8-port Gig-T HMIM Module (JG422A) HPE MSR 2-port 1000BASE-X HMIM Module (JG423A) HPE MSR 4-port 1000BASE-X HMIM Module (JG424A) HPE MSR 8-port 1000BASE-X HMIM Module (JG425A) HPE MSR 16p Enhanced Async Serial HMIM Module (JG445A)* HPE MSR 24-port Gig-T Switch HMIM Module (JG426A) HPE MSR 1-port OC-3/STM-1 CPOS HMIM Module (JG428A) HPE MSR 8-port 100BASE-FX/1000BASE-X/4-port 1000BASE-T (Combo) L2/L3 HMIM Module (JH238A) HPE MSR 16-port Enhanced Async Serial HMIM Module (JG445A) HPE MSR 8-port E1/CE1/T1/CT1/PRI HMIM Module (JH169A) HPE MSR 8-port E1/Fractional E1/T1/Fractional T1 HMIM Module (JH172A)
Memory	HPE X600 1G Compact Flash Card (JC684A) HPE X610 2GB DDR3 SDRAM UDIMM Memory (JG529A) HPE X610 4GB DDR3 SDRAM UDIMM Memory (JG530A)

*JG421A and JG445A are now obsolete

Learn more at

hpe.com/networking

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Visit **HPE GreenLake**

4AA4-8842ENW, Rev. 9

Hewlett Packard Enterprise