Overview

HPE Networking Comware Router Series MSR2000

The HPE Networking Comware Router Series MSR2000, 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 Networking Comware architecture. These routers feature a modular design that delivers unmatched application services for small- to medium-sized branch offices. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management.

The MSR2000 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.



HPE Networking Comware MSR2003 AC Router Rear View

Key features

- Up to 1 Mpps forwarding; converged high-performance routing, switching, security, voice, mobility
- Embedded security features with hardware-based encryption, firewall, NAT, and VPNs
- Industry-leading breadth of LAN and WAN connectivity, up to 24/48 GE switching ports integrated
- No additional licensing complexity; no cost for advanced features
- Zero-touch solution, with single pane-of-glass management

Standard Features

Features and benefits

Connectivity

- **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.
- **NEMO (Network Mobility)**
  Network mobility (NEMO) enables a node to retain the same IP address and maintain application connectivity when the node travels across networks. It allows location-independent routing of IP datagrams on the Internet.
- **High-density port connectivity**
  provides 24 or 48 Giga LAN switching ports on board (all switching ports can be configured as routed ports), up to 4 interface module slots and up to 30 module options
- **Multiple WAN interfaces**
  provides a traditional link with E1, T1, Serial, ADSL over POTs, ADSL over ISDN, G.SHDSL, ATM and ISDN links; high-density Fast or Giga Ethernet access modules; mobility access with 3G (WCDMA/HSPA)/4G LTE SIC module and 3G/4G USB modems
- **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; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
- **3G/4G LTE access support**
  provides 3G/4G LTE wireless access for primary or backup connectivity via a 3G/4G LTE SIC modules certified on various cellular networks; optional carrier 3G/4G LTE USB modems are available
- **USB interface**
  uses USB memory disk to download and upload configuration and 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

Performance

- **Excellent forwarding performance**
  provides forwarding performance up to 4 Mpps; meets the bandwidth-intensive application demands of enterprise businesses
- **Powerful security capacity**
  Includes an embedded hardware encryption accelerator to improve encryption performance; encryption throughput can be up to 3 Gbps with a maximum of 1000 IPSec VPN tunnels

Ease of deployment

- **Zero-touch deployment**
  supports both USB disk auto deployment and 3G SMS auto deployment

Investment protection

- **Re-use of existing SIC modules**
  supports existing SIC modules, transceivers, and cables for investment protection

Standard Features

Layer 3 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; 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, 6to4, 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 (MP-BGP) 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 ACLs, IP prefix, AS paths, community lists, and aggregate policies

Standard Features

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 multi-service platform**
  provides WAN router, Ethernet switch, 3G/4G WAN, stateful firewall, VPN, and SIP/voice gateway on MSRs
- **Advanced hardware architecture**
  supports multicore processors, gigabit switching, and PCIE bus. Dual internal power supplies(AC or DC) supported on MSR2004-48 for higher reliability and flexibility
- **New operation system version**
  ships with new Comware v7 operating system delivering the latest in virtualization and routing

Layer 3 services

- **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.
- **NAT-PT**
  Network Address Translation – Protocol Translation (NAT-PT) enables communication between IPv4 andIPv6 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.
- **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

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 IEEE 802.1Q-based VLANs
- **sFlow**
  allows traffic sampling
- **Define port as switched or routed**
  supports command switch to easily change switched ports to routed (maximum four Fast Ethernet ports)

Standard Features

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
- **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.
- **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.
- **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, 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 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 utilizing a user/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 into a remote device; with authentication and encryption, it protects against IP spoofing and plain text password interception; increases the security of SFTP transfers
- **Attack Detection and Protection**

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 Multicast(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

Standard Features

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 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

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

Standard Features

Quality of Service (QoS)

- **Nested QoS**
  provides a built-in QoS engine that supports nested QoS (Same to hierarchical QoS) and can implement a hierarchical scheduling mechanism based on ports, user groups, users, and user services.
- **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)/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/LFI, and Control Plane Policing (CoPP).

Integration

- **Embedded NetStream**
  improves traffic distribution using powerful scheduling algorithms, including Layer 4 to 7 services; monitors the health status of servers and firewalls
- **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
- **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 Fabric (IRF)**
  Intelligent Resilient Fabric (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
- **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, 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

Warranty and support

- **1-year Warranty**
  See **http://www.hpe.com/networking/warrantysummary** for warranty and support information included with your product purchase.
- **Software releases**
  to find software for your product, refer to **http://www.hpe.com/networking/support** ; for details on the software releases available with your product purchase, refer to **http://www.hpe.com/networking/warrantysummary**

Configuration Information

Build To Order:
BTO is a standalone unit with no integration. BTO products ship standalone are not part of a CTO or Rack-Shippable solution.

Router Chassis

Remarks	Description	SKU
1, 2, 3, 6, 7	HPE FlexNetwork MSR2003X AC Router	S0P10A
	• 2 RJ-45 autosensing 10/100/1000 Combo WAN ports • 8 RJ-45 autosensing 10/100/1000 LAN ports • 2 SFP Fibre Combo ports (min=0 \ max=2 SFP Transceivers) • 3 SFP+ Fibre ports (min=0 \ max=3 SFP+ Transceivers) • 1 USB 2.0 port • 1 Console port • 4GB DDR4 included (default=4GB \ max=4GB DDR4) • AC Power Supply included • 1U - Height	
	HPE FlexNetwork MSR2003X AC Router	S0P10A#B2B
	• C15 PDU Jumper Cord (NA/MEX/TW/JP)	
	HPE FlexNetwork MSR2003X AC Router	S0P10A#B2C
	• C15 PDU Jumper Cord (ROW)	
	HPE FlexNetwork MSR2003X AC Router	S0P10A#B2E
	• NEMA L6-20P Cord (NA/MEX/JP/TW)	
	HPE FlexNetwork MSR2003X AC Router	S0P10A#AC3
	• No Localized Power Cord Selected	
	Configuration Rules:	
Rule #	**Description**	**SKU**
1	AC Power Supply included	
2	Localization required on orders without #B2B, #B2C or #B2E options.	
3	#B2E is Offered only in NA, Mexico, Taiwan, and Japan.	
6	The following Transceivers install into this Router:	
	HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
	HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
	HPE X120 1G SFP LC LH100 Transceiver	JD103A
	HPE X120 1G SFP RJ45 T Transceiver	JD089B
7	The following Transceivers install into this Router	
	HPE X130 10G SFP+ LC ER 40km Transceiver	JG234A
	HPE X130 10G SFP+ LC LH 80km Transceiver	JG915A
	HPE X130 10G SFP+ LC LR Transceiver	JD094B
	HPE X130 10G SFP+ LC SR Transceiver	JD092B
	HPE X130 10G SFP+ LC BiDi 10km-Uplink Transceiver	JL737A
	HPE X130 10G SFP+ LC BiDi 10km-Downlink Transceiver	JL738A
	HPE X130 10G SFP+ LC BiDi 40km-Uplink Transceiver	JL739A
	HPE X130 10G SFP+ LC BiDi 40km-Downlink Transceiver	JL740A

Configuration Information

SIC Modules

System (std 0 // max 4, 3, 2 or 1) User Selection (min 0 // max 4, 3, 2 or 1) per Host (See Modules for Port information)

Rule #	Description	SKU
1, 11	HPE FlexNetwork MSR 1-port Enhanced Serial SIC Module	JD557A
	• min=0 \ max=1 Serial Port Cable	
1, 11	HPE FlexNetwork MSR 4-port Enhanced Sync/Async Serial SIC Module	JG737A
	• min=0 \ max=4 Serial Port Cable	
18	HPE FlexNetwork MSR 4-port Gig-T Switch SIC Module	JG739A
18	HPE FlexNetwork MSR 4-port GbE Combo SIC Module	R8V29A
	Configuration Rules:	
Rule #	**Description**	**SKU**
1	These Modules can install directly to the Routers (S0P10A), min=0\ max=2 per enclosure (only supported in Slots 2 and 3)	
11	The following Cables install into this Module:	
	HPE FlexNetwork X200 V.24 DTE 3m Serial Port Cable	JD519A
	HPE FlexNetwork X200 V.35 DTE 3m Serial Port Cable	JD523A
	HPE FlexNetwork X200 V.35 DCE 3m Serial Port Cable	JD525A
	HPE FlexNetwork X200 V.24 DCE 3m Serial Port Cable	JD521A
18	These Modules can install directly to the Routers (S0P10A), min=0\ max=1 per enclosure (only supported in Slot 2)	
19	The following E1/T1 Cables install into this Module:	
	HPE FlexNetwork X260 E1 RJ45 to 2xBNC 75ohm 3m Router Cable	JH294A
	HPE FlexNetwork X260 E1 RJ45 120 ohm 2m Router Cable	JC156A
	HPE FlexNetwork X260 T1 Router Cable	JD518A
Notes:	PoE Module JG740A can be used as non-POE module on chassis without PoE power supplies.	

Transceivers

SFP Transceivers	
HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
HPE X120 1G SFP LC LH100 Transceiver	JD103A
HPE X120 1G SFP RJ45 T Transceiver	JD089B
SFP+ Transceivers	
HPE X130 10G SFP+ LC ER 40km Transceiver	JG234A
HPE X130 10G SFP+ LC LH 80km Transceiver	JG915A
HPE X130 10G SFP+ LC LR Transceiver	JD094B
HPE X130 10G SFP+ LC SR Transceiver	JD092B
HPE X130 10G SFP+ LC BiDi 10km-Uplink Transceiver	JL737A
HPE X130 10G SFP+ LC BiDi 10km-Downlink Transceiver	JL738A
HPE X130 10G SFP+ LC BiDi 40km-Uplink Transceiver	JL739A
HPE X130 10G SFP+ LC BiDi 40km-Downlink Transceiver	JL740A

Configuration Information

Cables

Remarks	Description	SKU
	HPE FlexNetwork X260 Mini D-28 to 4-RJ45 0.3m Router Cable	JG263A
	HPE FlexNetwork X200 V.24 DTE 3m Serial Port Cable	JD519A
	HPE FlexNetwork X200 V.24 DCE 3m Serial Port Cable	JD521A
	HPE FlexNetwork X200 V.35 DTE 3m Serial Port Cable	JD523A
	HPE FlexNetwork X200 V.35 DCE 3m Serial Port Cable	JD525A
	HPE FlexNetwork X260 E1 (2) BNC 75 ohm 3m Router Cable	JD175A
	HPE FlexNetwork X260 E1 RJ45 BNC 75-120 ohm Conversion Router Cable	JD511A
	HPE FlexNetwork X260 T1 Router Cable	JD518A
	HPE FlexNetwork X260 E1 RJ45 to 2xBNC 75ohm 3m Router Cable	JH294A
	HPE FlexNetwork X260 E1 RJ45 120 ohm 2m Router Cable	JC156A
Notes:	The following cable is used for RJ45 BNC Conversion -	
	HPE FlexNetwork X260 E1 RJ45 BNC 75-120 ohm Conversion Router Cable	JD511A

Technical Specifications

HPE MSR2003X AC Router (S0P10A)		
I/O ports and slots	3 fixed 10GbE SFP+ ports, 2 combo ports (SFP or RJ45) and 8 RJ-45 autosensing 10/100/1000 LAN ports	
Additional ports and slots	1 RJ45 console port and 1 USB port 2.0 or 3.0	
Physical characteristics	**Dimensions (w x d x h)**	360x300x44.2 mm
	Weight	3.1 kg
	Memory and processor	Marvell ARM64 @ 2.2 GHz, 4 GB DRAM, 4 GB eMMC Flash
	Mounting and enclosure	Mounts in an EIA standard 19-inch telco rack or equipment cabinet
Performance	**Throughput**	4 Mpps
	Routing table size	300000 entries (IPv4), 300000 entries (IPv6)
	Forwarding table size	300000 entries (IPv4), 300000 entries (IPv6)
Environment	**Operating temperature**	0~45 ˚C
	Operating relative humidity	5~95% no dew
	Non-operating/storage temp	–40°C~70°C
	Non-operating/storage relative humidity	5~95% no dew
	Acoustic	37dBA
	Altitude	Up to 5,000 ft (1.5 km)
Electrical characteristics	**Frequency**	2.2 GHz
	Voltage	100~240 VAC; ~50/60 Hz
	Maximum power rating	54W
	Reliability—MTBF (years)	130 years
	Safety	IKE/IP SecVPN, ADVPN, GDVPN, L2TP VPN, GRE VPN NAT/NAPT, PKI, RSA, URPF DDoS attack prevention, ARP attack prevention EAD FIPS, N ETCONF, OpenFlow, telemetry, VXLAN, EVPN
Specifications	HPE MSR2003X AC Router (S0P10A)	
Electrical characteristics	**EMC**	CISPR 24 EN 55024 EN 61000–3–2 EN 61000–3–3 EN 61000–6–1 ETSI EN 300 386 EN 301 489–1 EN 301 489–17 UL 60950–1 CAN/CSA C22.2 No 60950–1 IEC 60950–1 EN 60950–1/A11
Telecom	EN 301 511; EN 301 908-1; EN 300 328; EN 62311; FCC Part 22	
Management	IMC—Intelligent Management Center; Command-line interface; SNMP manager; Telnet; RMON1; FTP; 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.	

Technical Specifications

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
- RFC1998 An Application of the BGP Community Attribute in Multi-home Routing

Device Management

- RFC 1155 Structure and Mgmt Information (SMIv1)
- RFC 1157 SNMPv1/v2c
- RFC 1305 NTPv3
- RFC 1591 DNS (client)
- RFC 1902 (SNMPv2)
- RFC 1908 (SNMP v1/2 Coexistence)
- RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0
- RFC 2271 Framework
- RFC 2573 (SNMPv3 Applications)
- RFC 2576 (Coexistence between SNMP V1, 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)

Technical Specifications

Denial of service protection

- CPU DoS Protection
- Rate Limiting by ACLs

General Protocols

- RFC 2385 BGP Session Protection via TCP MD5
- 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 (OSPF v2)
- 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 Ethernetlike 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)

Technical Specifications

- 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
- 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 RIP v2
- 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

Technical Specifications

- 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 Autoconfiguration
- 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



Technical Specifications

- RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- 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
- 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



Technical Specifications

- 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

16-Oct-2023

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)

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)

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)



Technical Specifications

- 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)

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

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



Technical Specifications

- RFC 2737 Entity MIB (Version 2)
- RFC 2863 The Interfaces Group MIB
- RFC 3813 MPLS LSR MIB

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

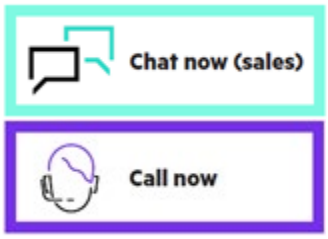


Summary of Changes

Date	Version History	Action	Description of Change:
04-Dec-2023	Version 27	Changed	Series name was updated.
06-Mar-2023	Version 25	Changed	Standard Features, Configuration Information and Technical Specifications sections were updated. Obsolete SKUs were also removed in Configuration Information section.
04-Apr-2021	Version 24	Changed	Configuration Information section was updated.
16-Aug-2021	Version 23	Changed	Configuration Information section was updated.
18-Jan-2021	Version 22	Changed	Overview, Standard Features, Configuration Information, and Technical Specifications sections were updated
02-Dec-2019	Version 21	Changed	Overview, Configuration Information, Related Options and Technical Specifications sections were updated. Obsolete SKUs were removed.
06-Feb-2017	Version 20	Changed	Adding MSR #A59 option on Configuration section
05-Sep-2016	Version 19	Changed	SKU added: JG742B Features and benefits and Technical Specifications updated
01-Aug-2016	Version 18	Changed	Adding #AC3 Option on Configuration section
06-Jun-2016	Version 17	Changed	Document name changed to HPE Networking Comware Router Series MSR2000. Product description updated.
08-Apr-2016	Version 16	Changes	Changes made on Configuration section, SKU descriptions updated on all the document.
31-Mar-2016	Version 15	Changed	SKUs added: JH240A, JH225AAE, JH229AAE Product overview, Features and benefits updated
01-Dec-2015	Version 14	Changed	Overview and Technical Specifications updated
07-Oct-2015	Version 13	Changed	Minor change made on Technical Specifications
17-Aug-2015	Version 12	Changed	SKUs added: JG929A Features and Benefits, Technical Specifications and Accessories updated.
06-Oct-2014	Version 11	Changed	Removed SKU JD572A Configuration section updated
18-Aug-2014	Version 10	Added	2 new models: JG734A, JG735A 7 new accessories: JG736A, JG737A, JG738A, JG739A, JG740A, JG745A, JG746A
10-Jun-2014	Version 9	Added	4 new accessories: JG604A, JG742A, JG743A, JG744A
10-Feb-2014	Version 8	Added	GRE tunnels was added to Performance.
22-Nov-2013	Version 7	Changed	SIC Modules and Cables were revised in Configuration.
11-Nov-2013	Version 6	Changed	Router Chassis and Box Level Integration CTO Models were revised in Configuration.
07-Oct-2013	Version 5	Changed	Corrected the callout table in the Overview section (formatting).
04-Oct-2013	Version 4	Added	Added 2 images in the Overview section.
30-Sep-2013	Version 3	Changed	Minor edits were made throughout Configuration.
27-Sep-2013	Version 2	Added	Configuration was added.
19-Aug-2013	Version 1	New	New QuickSpecs

Copyright

Make the right purchase decision.
Contact our presales specialists.



Get updates

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett Packard Enterprise

To learn more, visit: **http://www.hpe.com/networking**

c04123120 - 14642 - Worldwide - V26 - 04-December-2023