Overview

HPE VSR1000 Virtual Services Router Series

Models

HP VSR1001 Comware 7 Virtual Services Router E-LTU	JG811AAE
HP VSR1004 Comware 7 Virtual Services Router E-LTU	JG812AAE
HP VSR1008 Comware 7 Virtual Services Router E-LTU	JG813AAE

Key features

- Virtualized x86 software router with 20 Gbps+ performance
- Mainstream hypervisor support including VMware ESXi and Linux KVM
- Rich enterprise router services, no feature licensing: firewall, encryption, VPN, MPLS, QoS and HA
- Comprehensive data center and SDN features: VXLAN, OpenFlow 1.3 and IRF 2:1 virtualization
- Agile deployments across the branch office, data center and cloud

Product overview

The HPE VSR1000 Series is a routing virtualized network function (VNF) that provides similar functionality as enterprise physical routers. It enables significant operational savings as a result of its agility and ease of deployment. Like other VNFs, the VSR1000 runs in a virtual machine (either Linux KVM or VMware ESXi) on an x86 server. Resources on the VSR1000 can be dynamically allocated and upgraded on demand as performance requirements grow. The VSR1000 series is available in one, four, and eight virtual CPU versions that have no expiration date. No feature licenses are needed, avoiding hidden costs. Full-function trial version is free to download. A variety of deployment models are supported including enterprise vCPE either on premise or at PoP, and vPC gateway.

In addtion to a complete set of IPv4 and IPv6 routing features and a large routing table, the VSR1000 provides comprehensive network services such as NAT, zone-based firewall, IPSec VPN, ADVPN, MPLS VPN and QoS etc. Leveraging SR-IOV technology, the VSR1000 may achieve 20 Gbps+ network services.

Besides routing functionalities, the VSR1000 series supports IRF (Intelligent Resilient Fabric) to virtualize two VSR instances into one single VSR cluster, which simplifies the management and improves the reliability significantly. The latest datacenter and SDN technologies like VXLAN and Openflow 1.3 are also fully supported by the VSR1000, which allows customers to easily deploy the VSR in a fast-evolving and mission-critical environment.

Features and benefits

Virtualization

- **Hypervisor support**
  supports the following industry-standard hypervisors: VMware ESXi versions 4.1, 5.0, 5.1, and 5.5; Linux KVM (Linux kernel version 2.6.25 or later)
- **Recommended Linux operating systems**
  CentOS 7, Ubuntu 14.04, Red Hat Enterprise Linux (RHEL) 6.3, and SUSE Linux Enterprise Server 11 SP2
- **Recommended vNICs**

Overview

E1000 and VirtIO virtual NICs are recommended in a virtual switch environment. Intel 82599VF (SR-IOV) is recommended for best performance as it bypasses virtual switch processing.

- **Maximum of 16 vNICs supported**
  provides flexible virtual connectivity

Layer 3 routing

- **Static IPv4 routing**
  provides simple manually configured IPv4 routing
- **Static IPv6 routing**
  provides simple manually configured IPv6 routing
- **Routing Information Protocol (RIP)**
  uses a distance vector algorithm with UDP packets for route determination; supports RIPv1 and RIPv2 routing; includes loop protection
- **Routing Information Protocol next generation (RIPng)**
  extends RIPv2 to support IPv6 addressing
- **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
- **OSPFv3**
  provides OSPF support for IPv6
- **Border Gateway Protocol (BGP)**
  provides IPv4 Border Gateway Protocol routing, which is scalable, robust, and flexible
- **BGP+**
  extends BGP-4 to support Multiprotocol BGP (MBGP), including support for IPv6 addressing
- **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)
- **IS-IS for IPv6**
  extends IS-IS to support IPv6 addressing
- **ISIS Multi-Topology Routing (MTR)**
  splits a base topology into multiple topologies, which intersect or overlap with one another. Route calculation is performed on a per-topology basis
- **Policy-based routing**
  makes routing decisions based on policies set by the network administrator
- **Routing policy**
  allows custom filters of routing information for increased performance and security; supports ACLs, IP prefix, AS paths, community lists, and aggregate policies

Layer 3 services

- **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
- **Domain Name System (DNS)**
  provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server
- **Network address translation (NAT)**

Overview

supports one-to-one NAT, net-to-net NAT, NAT444, bidirectional NAT, NAT hairpin, Twice NAT, NAT load sharing, and NAT session control, enabling NAPT to support multiple connections; supports blacklist in NAT, a limit on the number of connections, session logs, and multi-instances (VRF-aware NAT)

- **Dynamic Host Configuration Protocol (DHCP)**
  simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
- **User Datagram Protocol (UDP) helper**
  redirects UDP broadcasts to specific IP subnets to prevent server spoofing
- **Additional IP services**
  delivers forwarding/fast forwarding (unicast/multicast), TCP, FTP server, FTP client, TFTP client, Telnet server, Telnet client, and NTP/SNTP
- **Wide Area Application Services (WAAS)**
  performs WAN connectivity 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
- **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
- **IPv6 tunneling**
  allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet or vice versa; supports manually configured tunnel, automatic IPv4-compatible IPv6 tunnel, 6to4 tunnel, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), IPv4 over IPv6 manual tunnel, DS-lite and IPv6 over IPv6 tunnel.
- **Address Family Translation (AFT)**
  translates an IP address of one address family into an IP address of the other address family. It enables IPv4 network and IPv6 network to communicate with each other

Quality of Service (QoS)

- **Traffic classification**
  utilizes port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, and protocol type
- **Traffic policing**
  supports committed access rate (CAR) and line rate (LR)
- **Traffic shaping**
  supports generic traffic shaping (GTS)
- **Congestion management**
  supports FIFO, weighted fair queuing (WFQ), and class-based queuing (CBQ)
- **Congestion avoidance**
  supports tail drop and weighted random early detection (WRED)
- **Hierarchical Quality of Service (HQoS)**
  provides three levels of hierarchical QoS; manage traffic and hierarchically schedule traffic by user, network service, and application. Through multi-level child QoS policy, provides more granular traffic control and quality assurance services than traditional one-level QoS.
- **MPLS QoS**
  allows MPLS traffic classification

Virtual private network (VPN)

- **Generic Routing Encapsulation (GRE)**

Overview

transports Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site

- **IPSec**
  provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two network endpoints
- **Manual or automatic Internet Key Exchange (IKE)**
  provides both manual or automatic key exchange required for the algorithms used in encryption or authentication; auto-IKE allows automated management of the public key exchange, providing the highest levels of encryption
- **Layer 2 Tunneling Protocol (L2TP)**
  an industry standard-based traffic encapsulation mechanism supported by many common operating systems; will tunnel the Point-to-Point Protocol (PPP) traffic over the IP and non-IP networks; may use the IP/UDP transport mechanism in IP networks
- **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
- **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
- **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

Security

- **Access control list (ACL)**
  supports powerful ACLs for both IPv4 and IPv6; filters traffic to prevent unauthorized users from accessing the network, or controls network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on Layer 2 header or Layer 3 protocol header; rules can be set to operate on specific dates or times
- **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**
  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
- **Attack detection and prevention**
  detects variety of attacks by inspecting arriving packets, and protect a private network by logging, dropping packets, blacklisting

Overview

- **Remote Authentication Dial-In User Service (RADIUS)**
  eases switch security access administration by using a password authentication server
- **Terminal Access Controller Access-Control System (TACACS+)**
  delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security
- **Access control**
  supports ACL, AAA (local authentication, RADIUS, HWTACACS, LDAP), RBAC, portal, and IP source guard
- **Secure management access**
  delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv
- **Unicast Reverse Path Forwarding (URPF)**
  limits malicious traffic on a network
- **Web-based authentication (Portal)**
  similar to IEEE 802.1X, it provides a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant
- **Additional security features**
  supports SSH (v1.5 and 2.0), FIPS 140-2, PKI, session management, connection limit, and password management

Data center optimized

- **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. Supports VXLAN IP Gateway and VXLAN over IPsec
- **Ethernet Virtual Interconnect (EVI)**
  provides Layer 2 connectivity between distant Layer 2 network sites across an IP routed network using MAC-in-IP technology. Connects geographically dispersed sites of a virtualized large-scale data center that requires Layer 2 adjacency. Supports EVI over IPsec

Software-defined networking

- **OpenFlow**
  Supports OpenFlow 1.3.1, a 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.

Multicast support

- **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
- **Multicast Border Gateway Protocol (MBGP)**
  allows multicast traffic to be forwarded across BGP networks separately from unicast traffic
- **Multicast Source Discovery Protocol (MSDP)**
  allows multiple PIM-SM domains to interoperate; is used for inter-domain multicast applications
- **Protocol Independent Multicast (PIM)**
  defines modes of Internet IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of

Overview

information; PIM Dense Mode (DM), Sparse Mode (SM), and Source-Specific Mode (SSM) are supported

Resiliency and high availability

- **Intelligent Resilient Fabric (IRF)**
  allows the customer to build an IRF stack, namely a logical device, by interconnecting multiple VSRs through stack ports. The customer can manage all the VSR instances in the IRF stack by managing the single logical device, which is cost-effective like a box-type device, and scalable and highly reliable like a chassis-type distributed device. Supports cross-server IRF
- **Bidirectional Forwarding Detection (BFD)**
  supports BFD, enabling link connectivity monitoring and reduces network convergence time
- **Hitless patch upgrades**
  allows patches and new service features to be installed without restarting the equipment, increasing network uptime and facilitating maintenance
- **In-Service Software Upgrade (ISSU)**
  lowers downtime caused by planned maintenance and software upgrades
- **Load balancing**
  a cluster technology that distributes services among multiple network devices or links. Supports L4 to L7 server 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
- **Redundant Ethernet**
  helps ensure link availability through a virtual Layer 3 interface using two member interfaces. One member interface is active and the other is inactive. When the active interface fails, the inactive interface becomes active. The member interface switchover does not interrupt traffic.
- **Interface backup**
  allows the configuration of multiple backup interfaces for a Layer 3 interface to increase link availability. When the primary interface fails or is overloaded, its backup interfaces can take over or participate in traffic forwarding.

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
- **Local management**
  supports CLI, automatic configuration, and file system
- **Industry-standard CLI with a hierarchical structure**
  reduces training time and expenses, and increases productivity in multivendor installations
- **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
- **Role-based security (RBAC)**
  delivers role-based access control (RBAC); supports 16 user levels (0~15)
- **Information center**
  provides a central repository for system and network information; aggregates all logs, traps, and debugging information

Overview

generated by the system and maintains them in order of severity; outputs the network information to multiple channels based on user-defined rules

- **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
- **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
- **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

Monitor and diagnostics

- **Debug and sampler utility**
  supports ping and traceroute for both IPv4 and IPv6
- **Remote monitoring (RMON)**
  uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- **sFlow® (RFC 3176)**
  provides high-speed traffic accounting and monitoring
- **Embedded NetStream**
  improves traffic distribution using powerful scheduling algorithms, including Layer 4 to 7 services; monitors the health status of servers and firewalls
- **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

Warranty and support

- **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**

Technical Specifications

HPE VSR1001 Comware 7 Virtual Services Router E-LTU (JG811AAE)

Management	IMC - Intelligent Management Center; command-line interface; SNMP Manager; Telnet; RMON1; FTP; IEEE 802.3 Ethernet MIB
Notes	(1) Number of virtual CPUs supported: 1 (2) Minimum hardware requirements: • CPU: 2.0 GHz • Memory: 1 GB • Disk space: 8 GB • Network interfaces: 2 virtual NICs (3) Performance numbers: • IPv4 forwarding performance: up to 2.9Mpps@64byte or 9Gbps@IMIX for VMware hypervisor; up to 3.6Mpps@64byte or 10.1Gbps@IMIX for KVM hypervisor • IPSec performance: up to 331Mbps@IMIX or 594Mbps@1400byte with VMware hypervisor; up to 801Mbps@IMIX or 1.1Gbps@1400byte with KVM hypervisor • Performance results with x86 Server (CPU **E5-2680@2.8** GHz + Intel 82599EB NIC with SR-IOV enabled); VMware hypervisor: ESXi 5.5.0; KVM Hypervisor: CentOS7 KVM; IPSec with Intel AES-NI engine enabled
Services	Refer to the Hewlett Packard Enterprise website at **http://www.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.

HPE VSR1004 Comware 7 Virtual Services Router E-LTU (JG812AAE)

Management	IMC - Intelligent Management Center; command-line interface; SNMP Manager; Telnet; RMON1; FTP; IEEE 802.3 Ethernet MIB
Notes	(1) Number of virtual CPUs supported: 4 (2) Minimum hardware requirements: • CPU: 2.0 GHz • Memory: 2 GB • Disk space: 8 GB • Network interfaces: 2 virtual NICs (3) Performance numbers: • IPv4 forwarding performance: up to 4.7Mpps@64byte or 13.4Gbps@IMIX for VMware hypervisor; up to 4.7Mpps@64byte or 13.8Gbps@IMIX for KVM hypervisor • IPSec performance: up to 1.1Gbps@IMIX or 1.8Gbps@1400byte with VMware hypervisor; up to 1.3Gbps@IMIX or 2.0Gbps@1400byte with KVM hypervisor • Performance results with x86 Server (CPU **E5-2680@2.8** GHz + Intel 82599EB NIC with SR-IOV enabled); VMware hypervisor: ESXi 5.5.0; KVM Hypervisor: CentOS7 KVM; IPSec with Intel AES-NI engine enabled.
Services	Refer to the Hewlett Packard Enterprise website at **http://www.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.

HPE VSR1008 Comware 7 Virtual Services Router E-LTU (JG813AAE)

Management	IMC - Intelligent Management Center; command-line interface; SNMP Manager; Telnet; RMON1; FTP;

Technical Specifications

IEEE 802.3 Ethernet MIB

Notes

(1) Number of virtual CPUs supported: 8
(2) Minimum hardware requirements:
• CPU: 2.0 GHz
• Memory: 4 GB
• Disk space: 8 GB
• Network interfaces: 2 virtual NICs
(3) Performance numbers:
• IPv4 forwarding performance: up to 8.8Mpps@64byte or 21.5Gbps@IMIX for VMware hypervisor; up to 11.2Mpps@64byte or 31.4Gbps@IMIX for KVM hypervisor
• IPSec performance: up to 2.6Gbps@IMIX or 4.2Gbps@1400byte with VMware hypervisor; up to 3.7Gbps@IMIX or 5.3Gbps@1400byte with KVM hypervisor
• Performance results with x86 Server (CPU **E5-2680@2.8** GHz + Intel 82599EB NIC with SR-IOV enabled); VMware hypervisor: ESXi 5.5.0; KVM Hypervisor: CentOS7 KVM; IPSec with Intel AES-NI engine enabled

Services

Refer to the Hewlett Packard Enterprise website at **http://www.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.

Date	Version History	Action	Description of Change
05-Feb-2016	From Version 1 to 2	Changed	Overview, Features and Benefits and Technical Specifications updated.

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

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

c04111377 - 14677 - Worldwide – V2 - 05-February-2016