What You Need to Know About VPNs

JUNIPER NETWORKS

VPN Name	Service Layer	Topology	Security	Service Protocols	Tunnel/Transport Protocols	Key Advantages	Key Limitations
SSL/OpenVPN Secure Sockets Layer	Layer 3 (IPv4 or IPv6) Note: Although SSL is a Layer 7 protocol, it transports service at Layer 3.	P2P. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VXLANs.	Implemented by tunnel endpoints. Offers full security including certificates, identity verification, and data encryption.	RFC 2246 for SSL	SSL	Travels across Web proxies and provides greatest connection potential.	Requires endpoint software or appliance. Tunnel is coupled to service, and difficult to scale.
IPsec Internet Protocol Security	Layer 3 (IPv4 or IPv6).	Same as above.	Same as above.	RFCs: 4302, 4303, 5996, and 6071	IPsec AH (Authentication Header) IPsec ESP (Encapsulating Security Payload)	Offers flexibility with security options.	Same as above. Additionally, does not connect across Web proxies, and needs GRE to support IP Multicast.
GRE/IP-in-IP Generic Routing Encapsulation	Layer 3 (IPv4 or IPv6).	Same as above.	None! To implement security in tunnel, couple to IPsec using GRE over IPsec.	RFC 2890 for GRE RFC 1853 for IP-in-IP	GRE. Note: GRE and IP-in-IP (IP/IP) are similar. However, GRE is used more often because it allows encapsulation of any protocol on top of it.	Offers simplicity.	Provides no security and does not connect across Web proxies.
MPLS IP VPN Multiprotocol Label Switching	Layer 3 (IPv4 or IPv6). Junos OS enables the same VPN with IPv4/Unicast, IPv4 Multicast, IPv6 Unicast, and IPv6 Multicast services, together, or as a subset. In some products, Junos OS supports ISO VPNs, where the service protocol is ISO, not IP, so L3VPN applies but not MPLS IP VPN. ISO packets are transported, just like IP VPN packets.	Can be full mesh between PEs, partial mesh, or a hub-and-spoke topology. You can connect several VPNs in an extranet. Note: The Unicast service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs of different types due to MPLS label stacking (one label for the service, one label for the transport).	Implemented by the Service Provider. Maintains separate per-VPN forwarding/routing instances, called VRFs (transparent to customer).	For Unicast IP Service: BGP only. For Multicast IP Service: BGP or PIM. (Juniper Networks, Nokia, and Huawei only support BGP for consistency with Unicast model.) RFCs: 4364, 4659, 6513, 6514, and 6826	Forwarding Plane: MPLS (P2P, or P2MP) or GRE (P2P, or P2MP). Transport tunnels for Unicast are P2P (PE-to-PE) and for Multicast are P2MP (one-PE-to-several-PEs). Multicast service may reuse the P2P tunnels for Unicast (with special configuration). Control Plane (tunnel signaling): If forwarding plane = MPLS, then LDP, RSVP, or L-BGP can perform tunnel signaling. You can use IGP with SPRING to establish MPLS forwarding path. If forwarding plane = GRE, then no tunnel signaling exists for Unicast services; and tunnel signaling is performed by PIM for Multicast services.	Scalability, flexibility, maturity, redundancy, and interoperability.	Depends on a Service Provider (or set of Service Providers). This is not a self-provisioning solution. If geographically vast, then the MPLS VPN needs a Service Provider with a huge presence, or an Inter-AS solution, or a combination of the MPLS VPN with an IP tunneling approach like IPsec.
CCC and TCC Circuit and Translational Cross-Connects	Layer 2: Ethernet, Frame Relay, ATM, PPP or HDLC.	P2P. The tunnel is coupled to service and each service, or cross-connect, has a different tunnel.	Implemented by the Service Provider. Maintains separate forwarding information for each cross-connect (transparent to customer).	RFC: In draft. Refer to 3985.	MPLS (P2P). Tunnel signaling is performed by RSVP only.	Service interfaces at each endpoint (PE1, PE2) for CCC must be the same type (for example, both Ethernet or both ATM). Service interfaces for TCC can be different types. Junos OS changes Layer 2 encapsulation without any Layer 3 routing (also known as L2.5 VPN).	Scaling issues because of the 1:1 (service:tunnel) mapping, and it is P2P.
Ethernet Pseudowires	Layer 2. Supports Unicast and Multicast Layer 2 traffic, raw Ethernet frames, and VLAN-tagged frames. Allows for VLAN tag manipulation at the endpoints (push, pop, and swap).	P2P. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs.	Implemented by the Service Provider. Maintains separate forwarding information for each pseudowire (transparent to customer).	Protocols can be BGP or LDP. Junos OS interoperates between BGP and LDP signaled networks. RFC 6625 for BGP RFC 4447 for LDP	Forwarding Plane: MPLS (P2P) or GRE (P2P). Transport tunnels are P2P (PE-to-PE). Control Plane (tunnel signaling): If forwarding plane = MPLS tunnel signaling is either LDP, RSVP, or L-BGP. You can use IGP with SPRING to establish MPLS forwarding path. If forwarding plane = GRE, then there is no tunnel signaling.	Simplicity. You can internally connect pseudowires in a PE to another VPN. For example, you can stitch two pseudowires, or add the endpoint of a pseudowire to a VPLS/EVPN instance. When the service is signaled with LDP, advantage = wider interoperability; with BGP, advantage = better scalability and using BGP as MPLS service protocol.	Same as above. Pseudowires are P2P and do not implement MAC address learning. They emulate an extended wire, not a LAN.
VXLAN Virtual Extensible LAN	Layer 2. Supports Unicast and Multicast Layer 2 traffic.	P2P. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VXLANs.	Implemented by the Data Center/operator. Maintains separate forwarding information for each VXLAN (transparent to customer).	RFC 7348 Note: You can use EVPN as the control plane for VXLAN.	UDP Ethernet frames are encapsulated in UDP with an additional VXLAN header.	Extends the limitation of 4095 VLANs to 16 million VNI (VXLAN Network Identifiers) logical networks. Typically used in a Data Center environment.	No control plane (could use EVPN as control plane). Limited entropy for ECMP/Hashing (only source UDP port).
VPLS Virtual Private LAN Service	Layer 2 (Ethernet only). Supports Unicast and Multicast Layer 2 traffic. VPLS supports raw Ethernet frames, VLAN tagged frames. Allows for VLAN tag manipulation at the endpoints (push, pop, and swap).	VPLS can be a full-mesh between PEs, a partial-mesh, or a hub-and-spoke (tree) topology. Unicast service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs.	Implemented by the Service Provider. Maintains separate per-VPLS forwarding instances (transparent to customer).	Protocols can be BGP or LDP. Junos OS interoperates BGP and LDP signaled networks. RFC 4761 for BGP RFC 4762 for LDP RFC 6074 for BGP and LDP	Forwarding Plane: MPLS (P2P or P2MP) or GRE (P2P). Transport tunnels for Layer 2: Unicast are P2P (PE-to-PE). Multicast are P2MP (one-PE-to-several-PEs). Control Plane (tunnel signaling): If forwarding plane = MPLS tunnel signaling is either LDP, RSVP, or L-BGP. You can use IGP with SPRING to establish MPLS forwarding path. If forwarding plane = GRE, then there is no tunnel signaling.	Compared to a pseudowire, VPLS provides a multipoint solution with more than two sites interconnected and MAC learning. Compared to EVPN, VPLS has less control plane signaling. When service is signaled with LDP, advantage = wider interoperability. With BGP, advantage = redundancy (active-backup), auto-discovery, and better scalability.	MAC learning is performed at the forwarding plane level. The entire VPLS traveling across the PEs functions as a single Ethernet switch.
EVPN Ethernet VPN	Same as above.	Same as above.	Implemented by the Service Provider. Maintains separate per-EVPN forwarding instances (transparent to customer).	RFC 7432 for BGP	Forwarding Plane: MPLS/MPLSoUDP/MPLSoGRE (P2P or P2MP), VXLAN, GRE (P2P). Transport tunnels for Layer 2: Unicast are P2P (PE-to-PE). Multicast are P2P, or P2MP (one-PE-to-several-PEs). Control Plane (tunnel signaling): If forwarding plane = MPLS tunnel signaling is either LDP, RSVP, or L-BGP. You can use IGP with SPRING extensions to establish MPLS forwarding path. If forwarding plane = GRE, then there is no tunnel signaling. BUM traffic (broadcast, unknown unicast, multicast) is treated as Layer 2 Multicast.	Compared to a pseudowire, EVPN provides a multipoint solution with more than two sites interconnected and MAC learning. Compared to VPLS, EVPN provides MAC learning at the control plane level. EVPN provides active-active redundancy, whereas VPLS only provides active-backup redundancy. All vendors agreed to use BGP signaling.	More signaling than VPLS due to the MAC address information exchanged through BGP.

Related Protocols/VPNs

SSL: TLS, HTTP

GRE/IP-in-IP: IP/GRE, IP/IP

MPLS IP VPN: BGP/MPLS VPN, L3VPN (for IPv4 Unicast), 6VPE (for IPv6 Unicast), MVPN (for IPv4/IPv6 Multicast)

CCC and TCC: PWE (Pseudowire Emulation) (refers to Layer 2 payloads at the endpoints), PWE3 (Pseudowire Emulation Edge-to-Edge), L2.5 VPNs often refer to TCC

Ethernet Pseudowires: PWE and PWE3. L2 Circuit, L2CKT, or L2VPN (for LDP-signaled service use L2 Circuit and L2CKT. For BGP-signaled service, use L2VPN.

E-Line: MEF (Metro Ethernet Forum), VPWS (Virtual Private Wire Service), VLL (Virtual Leased Line), EVPL (Ethernet Virtual Private Line), EVC (Ethernet Virtual Circuit).

VPLS: E-LAN: MEF (Metro Ethernet Forum), Multipoint-to-Multipoint EVC (Ethernet Virtual Circuit).

Legend

P2P = point-to-point
P2MP = point-to-multipoint

Poster concept

Susan McCoy
Krzysztof Szarkowicz
Antonio Sánchez-Monge

https://www.juniper.net/documentation/en_US/junos/topics/concept/vpn-security-overview.html

http://www.juniper.net/techpubs/en_US/learn-about/secure-vpns.pdf

DAY ONE POSTER

What You Need to Know About VPNs

Juniper Networks Information and Learning Experience (iLX)

www.juniper.net/posters