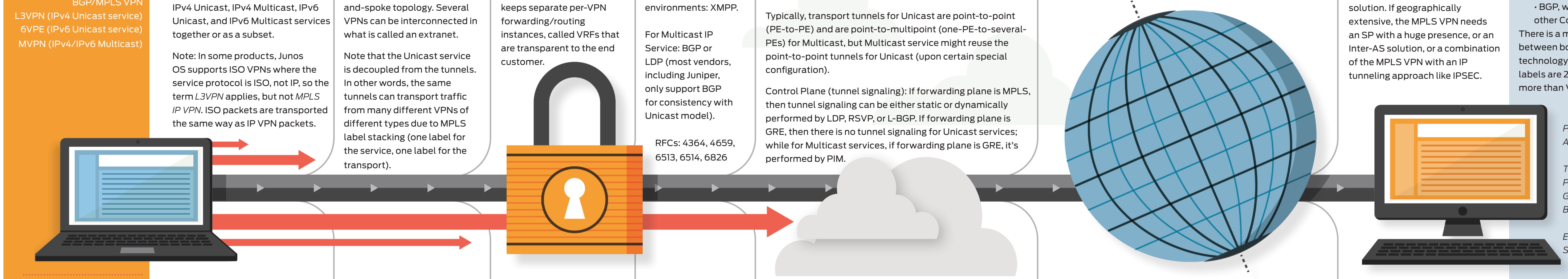
	SERVICE LAYER	TOPOLOGY	SECURITY	SERVICE PROTOCOLS	TUNNEL/ TRANSPORT PROTOCOLS	KEY ADVANTAGES	KEY LIMITATIONS
SSL TLS, HTTPS	Layer 3 (IPv4 or IPv6). (Even though SSL is a Layer 7 protocol, the service it transports is Layer 3).	Point-to-point. The tunnel is coupled to service. Hub-and-spoke and meshed topologies use point-to-point tunnels via Layer 3 routing at a hub endpoint.	Implemented by the tunnel endpoints. Has full security including certificates, identity verification, and data encryption.	N/A RFC 2246 for TLS 1.0 RFC 4346 for TLS 1.1 RFC 5246 for TLS 1.2	SSL/TLS Watch the Poster 13.2 Video for details.	Goes across Web proxies. Provides highest likelihood to get connected.	Requires endpoint software/ appliance. Tunnel is coupled to service. Scalability.
IPSEC	Layer 3 (IPv4 or IPv6)	Same as above. Also, Group Domain of Interpretation (GDOI) (RFC 6407) establishes secure associations from a centralized server, easing the creation of full mesh topologies (but each tunnel remains point-to-point).	Same as above	N/A RFC 4303, 5996, 6071	IPSEC (IP Security). The Security Associations (SAs) are typically established via IKE (Internet Key Exchange). User data traffic can be processed with ESP (Encapsulation Security Payload), or with AH (Authentication Header), or with both. Watch the Poster 13.2 Video for details.	Flexibility in terms of security options. Slightly better performance than SSL/TLS.	Same as above, but doesn't work across Web proxies. Needs GRE to support IP Multicast. Watch the Poster 13.2 Video for details.
GRE & IP/IP IP/GRE, IP-in-IP	Layer 3 (IPv4 or IPv6)	Same as above	None! Can be coupled to IPSEC (GRE over IPSEC) to get security in the tunnel.	N/A GRE = RFC 2784 IP-in-IP = RFC 1853	GRE. Note: GRE and IP-in-IP (IP/IP) are similar, except GRE is used more often because it allows encapsulation of any protocol—not just IP—on top of it.	Simplicity Watch the Poster 13.2 Video for details.	No security. Doesn't work accross Web proxies.
MPLS IP VPN BGP/MPLS VPN L3VPN (IPv4 Unicast service) 6VPE (IPv6 Unicast service) MVPN (IPv4/IPv6 Multicast)	Layer 3 (IPv4 or IPv6). Junos OS enables the same VPN to run with IPv4 Unicast, IPv4 Multicast, IPv6 Unicast, and IPv6 Multicast services together or as a subset. Note: In some products, Junos OS supports ISO VPNs where the service protocol is ISO, not IP, so the term *L3VPN* applies, but not *MPLS IP VPN*. ISO packets are transported the same way as IP VPN packets.	Can be a full mesh between PEs, a partial mesh, or a hub-and-spoke topology. Several VPNs can be interconnected in what is called an extranet. Note that the Unicast service is decoupled from the tunnels. In other words, 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, which keeps separate per-VPN forwarding/routing instances, called VRFs that are transparent to the end customer.	For Unicast IP Service: BGP. In SDN environments: XMPP. For Multicast IP Service: BGP or LDP (most vendors, including Juniper, only support BGP for consistency with Unicast model). RFCs: 4364, 4659, 6513, 6514, 6826	Forwarding Plane: MPLS (point-to-point or point-to-multipoint) or GRE (point-to-point or point-to-multipoint) Typically, transport tunnels for Unicast are point-to-point (PE-to-PE) and are point-to-multipoint (one-PE-to-several-PEs) for Multicast, but Multicast service might reuse the point-to-point tunnels for Unicast (upon certain special configuration). Control Plane (tunnel signaling): If forwarding plane is MPLS, then tunnel signaling can be either static or dynamically performed by LDP, RSVP, or L-BGP. If forwarding plane is GRE, then there is no tunnel signaling for Unicast services; while for Multicast services, if forwarding plane is GRE, it's performed by PIM.	Scalability, flexibility, maturity, redundancy, interoperability: it's the VPN solution.	Reliant on a (or on a set of) Service Provider(s). Not a self-provisioning solution. If geographically extensive, the MPLS VPN needs an SP with a huge presence, or an Inter-AS solution, or a combination of the MPLS VPN with an IP tunneling approach like IPSEC.
CCC & TCC Circuit and Translational Cross-Connects, PWE, PWE3, L2.5 VPNs	Layer 2: Ethernet, Frame Relay, ATM, PPP, or HDLC	Point-to-point. The tunnel is coupled to service, and each service (or cross-connect) has a different tunnel.	Implemented by the Service Provider, which keeps separate forwarding information for each cross-connect. Transparent to the end customer.	N/A RFCs: in draft, try 3985	MPLS (point-to-point). Tunnel signaling can be performed by RSVP only.	The service interfaces at each endpoint (PE1 and PE2) for CCC must be the same type (for example, both Ethernet or both ATM). The service interfaces for TCC can be different types, and Junos OS takes care of changing the Layer 2 encapsulation without any Layer 3 routing (hence the nickname L2.5 VPN).	There are scaling issues due to the 1:1 nature of its service:tunnel mapping. And it is point-to-point as compared to, for example, VPLS.
ETHERNET PSEUDO-WIRES PWE, PWE3, L2 Circuit, L2CKT, L2VPN, VPWS (Virtual Private Wire Service)	Layer 2. Supports Unicast and Multicast Layer 2 traffic, raw Ethernet frames, as well as VLAN-tagged ones. It allows for VLAN tag manipulation at the endpoints (push, pop, swap), too.	Point-to-point. The service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs of different types.	Security is implemented by the Service Provider, which keeps separate forwarding information for each pseudowire. Transparent to the end customer.	Can be BGP or LDP. Junos can interoperate between BGP and LDP-signaled networks. RFCs: 6624 (BGP) and 4447 (LDP)	Forwarding Plane: MPLS (point-to-point) or GRE (point-to-point). Transport tunnels are point-to-point (PE-to-PE). Control Plane (tunnel signaling): If forwarding plane is MPLS, then tunnel signaling is either static, LDP, RSVP, or L-BGP. If forwarding plane is GRE, then there is no tunnel signaling.	Advantage is simplicity. Pseudowires can be internally connected in a PE to another VPN – you can stitch two pseudowires, or you can add the endpoint of a pseudowire to a VRF/VPLS/EVPN . When the service is signaled with LDP, the advantage is interoperability. When signaled with BGP, the advantage is redundancy (active-backup), and its role as MPLS's universal service protocol.	Pseudowires are point-to-point and do not implement MAC address learning, so they just emulate an extended wire, not a LAN.
VPLS Virtual Private LAN Service	Layer 2 (Ethernet only). Supports Unicast and Multicast Layer 2 traffic. VPLS supports raw Ethernet frames, as well as VLAN-tagged ones, and it allows for VLAN tag manipulation at the endpoints (push, pop, swap), too.	VPLS can be a full mesh between PEs, a partial mesh, or a hub-and-spoke topology. One key point is that the Unicast service is decoupled from the tunnels. The same tunnels can transport traffic from many different VPNs of different types.	Security is implemented by the Service Provider, which keeps separate per-VPLS forwarding instances. It's transparent to the end customer.	Can be BGP or LDP. Junos OS can interoperate between BGP and LDP-signaled networks. RFCs: 4761 (BGP) and	Forwarding Plane: MPLS (point-to-point or point-to-multipoint), or, GRE (point-to-point only), note this is different from L3VPN. Transport tunnels for L2 Unicast are point-to-point (PE-to-PE) and the tunnels for L2 Multicast can be point-to-point, or point-to-multipoint (one-PE-to-several-PEs). Control Plane (tunnel signaling): If forwarding plane is MPLS, then tunnel signaling can be static or performed by LDP, RSVP, or L-BGP. If forwarding plane is GRE, then no tunnel signaling.	Compared to a pseudowire, VPLS provides a multipoint solution with more than two sites interconnected, as well as MAC learning. Compared to an EVPN, VPLS has less control plane signaling. When service is signaled with LDP, an advantage is wider interoperability. When it's signaled with BGP, an advantage is redundancy (active-backup).	MAC learning is performed at the forwarding plane level—the whole VPLS across PEs behaves like a single Ethernet switch.
EVPN Ethernet VPN MPLS	Layer 2 (Ethernet only). Supports Unicast and Multicast Layer 2 traffic. EVPN supports raw Ethernet frames, as well as VLAN-tagged ones, and it allows for VLAN tag manipulation at the endpoints (push, pop, swap), too.	Same as above	Security is implemented by the Service Provider, which keeps separate per-EVPN forwarding instances. It's transparent to the end customer.	BGP RFCs: in draft	Same as above Note that there is BUM traffic (Broadcast, Unknown-Unicast, Multicast), treated as L2 Multicast in both VPLS and EVPN.	Compared to a pseudowire, EVPN provides a multipoint solution with more than two sites interconnected, as well as MAC learning. Compared to VPLS, an EVPN provides MAC learning at the control plane level. EVPN provides active-active redundancy, as compared to VPLS, which only does active-backup. BGP vs LDP service signaling? Only BGP. Agreed by all vendors!	There's more signaling than VPLS, due to the MAC address information exchanged via BGP.



JUNIPer NETWORKS

The Junos® OS release for 13.2 is supported on EX Series, M Series, MX Series, PTX Series, and T Series.

New 13.2 Features Related to VPNs:
- Subscriber interfaces over MPLS pseudowires
- BGP PIC edge for MPLS VPN
- FEC 129 BGP autodiscovery for VPWS

Visit **www.juniper.net/techpubs/software/junos** for more on Junos 13.2.

Juniper Contrail SDN extends the MPLS IP VPN concept to Cloud Services. The Control Node uses two protocols to exchange VPN route information:
- XMPP, with the Compute Nodes hosting the Tenant VMs
- BGP, with Gateway Nodes, or to other Control Nodes.

There is a mapping of messages between both protocols. The tunneling technology is MPLS over GRE. MPLS labels are 20-bit, so they scale much more than VLANs, which are 12-bit.

Poster text and video:
Antonio Sanchéz-Monge

Technical reviewers: Eddie Parra, Kaliraj Vairavakkalai, Gonzalo Gómez Herrero, Bruno Rijsman

Editing and proofing:
Susan McCoy, Nancy Koerbel

Scan for an instructional video on SSL and IPSEC VPNs, at http://youtu.be/oUpmthrkQIM

ISBN: 978-1-936779-68-0 234567

NET DATE

JUNOS 13.2

DAY ONE POSTER:

VPNs

www.juniper.net/posters