IMPLEMENTING VPLS FOR DATA CENTER INTERCONNECTIVITY

Although Juniper Networks has attempted to provide accurate information in this guide, Juniper Networks does not warrant or guarantee the accuracy of the information provided herein. Third party product descriptions and related technical details provided in this document are for information purposes only and such products are not supported by Juniper Networks. All information provided in this guide is provided “as is”, with all faults, and without warranty of any kind, either expressed or implied or statutory, Juniper Networks and its suppliers hereby disclaim all warranties related to this guide and the information contained herein, whether expressed or implied of statutory including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement, or arising from a course of dealing, usage, or trade practice.
Table of Contents

Introduction .................................................................................................................. 4
Trends in the Data Center .............................................................................................. 4
Benefits of Layer 2 Data Center Interconnectivity ....................................................... 4
Scope ............................................................................................................................ 4
Target Audience .......................................................................................................... 5
Abstract ....................................................................................................................... 5
VPLS Technical Overview .......................................................................................... 5
VPLS Use Cases in the Data Center ............................................................................ 7
High Availability Clusters ......................................................................................... 7
High-Performance Computer Cluster and Grid-Based Applications ......................... 7
Control Traffic Considerations Between Data Centers .............................................. 7
Technologies to Extend VLAN Across Data Center Locations ................................ 8
Benefits of Extending VLANs Using VPLS ................................................................. 8
Low Latency and Low Latency Variation .................................................................... 8
High Availability ........................................................................................................ 9
QoS and Traffic Engineering ...................................................................................... 9
Network Segmentation ............................................................................................... 9
Design and Protocol Considerations ......................................................................... 9
VPLS Signaling Protocols ......................................................................................... 10
   Signaling for VPLS Pseudowires Using LDP ......................................................... 10
   Signaling for VPLS Pseudowires Using BGP ....................................................... 11
MPLS Signaling Protocols ......................................................................................... 11
   MPLS Signaling Using LDP .................................................................................. 11
   MPLS Signaling Using RSVP ................................................................................ 12
Enabling Routing from a VPLS Domain ................................................................... 12
Network Services Configuration for the VPLS Domain ........................................... 13
Implementation and Configuration Guidelines ......................................................... 15
   Configuring MPLS Signaling at the Core Routers ................................................. 16
   Configuring VPLS Signaling Using BGP at the Core Data Center Routers .... 17
   Configuring a VPLS Instance ............................................................................... 17
Summary ..................................................................................................................... 19
Appendix A Configuration ......................................................................................... 20
Configuration Examples ............................................................................................. 20
   Data Center Location 1 ......................................................................................... 20
   Data Center Location 2 ......................................................................................... 31
Show Commands ........................................................................................................ 42
   Verifying LDP Neighbor Status ........................................................................... 42
   Verifying Internal-BGP Neighbor Status .............................................................. 43
   Display VPLS Connections .................................................................................. 43
   Display VPLS mac-table ...................................................................................... 44
   Display VRRP Details ......................................................................................... 45
Appendix B Reference List .......................................................................................... 46
About Juniper Networks .............................................................................................. 47
Table of Figures

Figure 1: Supporting VPLS services via MPLS backbone ................................................................. 6
Figure 2: Signaling for VPLS pseudowires using LDP ........................................................................ 10
Figure 3: VPLS signaling using BGP and route reflectors in a full mesh topology .............................. 11
Figure 4: Load balancing for VPLS segment using statically split IP address space ............................ 13
Figure 5: Unified policy in firewalls for traffic from separate virtual routing instances in the network. .. 13
Figure 6: Distinct security policies in firewalls with virtual individual virtual routing instances in the network .................................................................................................................. 14
Figure 7: IP address space split across VPLS locations allowing associated distribution of firewall services .................................................................................................................... 14
Figure 8: Single IP address space distributed across VPLS locations allowing only one firewall choice. .. 15
Figure 9: Deploying VPLS services across data center locations ......................................................... 16
Figure 10: Extending VLANs across data center locations using VPLS ................................................. 20
Introduction
This implementation guide explains how to implement virtual private LAN service (VPLS) across multiple data center locations using Juniper Networks® MX Series 3D Universal Edge Routers. The design discussed in this implementation guide only uses MX Series devices for core connectivity. This design supports Juniper’s 2-tier data center network reference model as well as the generic 3-tier network connectivity models. One of the overriding themes throughout this document is that VPLS services are a key data center technology, seamlessly enabling the scalability of multiple data center locations without requiring the need to statically define affinity of applications to data centers. This allows organizations to unleash the full potential of their data center’s computing power.

Trends in the Data Center
With today’s shift toward data center consolidation, centralization of applications, and multiple initiatives to optimize resource utilization, dynamism and scale are highly prized infrastructure characteristics. Traditionally, data center infrastructures have been tightly coupled with the applications being served in each location, and application performance characteristics have been fairly well understood as they were statically defined. At the same time, modern IT organizations are striving to optimize every unit of infrastructure in order to cope with the business demands of deploying applications, supporting those applications throughout their life cycle, offering uniformity across the infrastructure, and providing scalability—all requirements of crucial importance.

Benefits of Layer 2 Data Center Interconnectivity
Today’s networks are typically built with an extremely tight Layer 3 boundary around each data center location or even around aggregation areas within data center locations. This coupling of physical network to logical L3 IP subnet truly limits the scalability and flexibility of data center operations. This last statement is particularly true for legacy applications relying on L2 connectivity between elements which are required not only to migrate to different facilities, but to support emerging applications such as virtual machine live migration, compute clusters, and other multi-node applications. All of these applications are ones that effectively require an L2 connection between multiple nodes, where the nodes are likely to be physically separate. Unfortunately, today’s networks are not built to solve this problem at scale.

Extended L2 broadcast domains provide flexibility of physical placement for the nodes participating in clusters across data center locations. With this flexibility, customers can decide the physical placement of these nodes based on business requirements such as High Availability (HA) and low latency. This enables servers to be located across geographically dispersed locations. Extending L2 domains across data center locations also addresses physical deployment constraints and offers administrators flexible deployment options to optimize space and capacity.

Juniper Networks offers a unique best-in-class solution for seamlessly providing L2 interconnectivity between data center locations, data center facilities, and data center networks over an IP network infrastructure. Juniper offers a VPLS implementation that overcomes the challenges of today’s data center network infrastructure without any security or performance implications.

Scope
The objective of this paper is to present a best practice approach, demonstrating that L2 broadcast domains can be extended reliably across multiple data center locations using VPLS in support of critical application services and business operating needs. The guidelines in this paper address an infrastructure with multiple data center locations and multiple logical network segments (functional areas) that may or may not extend across data center locations. This document covers major design considerations for the following:

- Incorporating VPLS in the core to construct inter site and intra site L2 networks
- Selecting VPLS signaling protocol (BGP/LDP) for data center applications.
- Selecting MPLS signaling protocol (LDP/RSVP).
Target Audience

This guide is intended for the following readers:

- Data center network/security architects evaluating the feasibility of new approaches in network design
- Data center network planners, engineers, and operators designing and implementing new data center networks
- Data center managers, IT managers, network and security managers planning and evaluating data center infrastructure and security requirements

Note: The reader should have a thorough understanding of MPLS technology and concepts prior to reading this document.

Abstract

In this document, we provide implementation guidelines for building a data center LAN consisting of two network tiers (access and core) at each data center location (although the design is applicable to a 3-tier network as well). We also provide guidance for extending VLANs across multiple locations using VPLS across the MPLS backbone between the core routers at each location. The servers’ default gateway, which connects to the access switch, resides on the core router at the same location or at another location across the VPLS network.

The VPLS also complements the data center’s logical network segmentation requirement for granular security policy and for network traffic separation for any compliance requirements by extending the segment across data center locations. The traffic engineering capability of the MPLS backbone helps customers meet the quality-of-service (QoS) and availability requirements for real-time applications.

Because access switches provide full fault tolerance at the uplink level, there are at least two links that connect up to the core tier from each access switching element. Each link terminates at a different core device. With this design, a core device failure will not impact the availability of a server that connects to the access element. Additionally, we provide link level redundancy using the connections from the access switching element to each core device over multiple physical links that act as the link aggregation group (LAG). Consequently, each access element supports local hosting of multiple VLANs and trunks all VLANs in the uplinks to the core network tier. The core devices act as a label edge router (LER) commonly referred to as an LER router in service provider deployments, and provides VPLS services across the MPLS backbone through the core network. The core devices connect across locations through a ring topology or through a partial/full mesh connection to address traffic and resiliency requirements.

VPLS Technical Overview

VPLS is an Ethernet-based point-to-multipoint Layer 2 VPN. This technology allows you to connect geographically dispersed data center LANs to each other across an MPLS backbone while maintaining Layer 2 connectivity. VPLS delivers an Ethernet service that can span one or more metro areas, providing connectivity between multiple sites as though these sites were attached to the same Ethernet LAN. VPLS uses the IP/MPLS core infrastructure to bridge between Ethernet networks and provide Ethernet-based services.

As shown in Figure 1, VPLS allows administrators to extend VLANs across data center locations. Administrators can configure all or some of the VLANs to extend across the MPLS backbone to other data center locations. The traffic from the access network traverses through the MPLS label-switched path (LSP) across the MPLS backbone to the other sites in the VPLS topology. The ingress router for the VPLS service pushes the appropriate labels to the Ethernet packet and forwards them on the appropriate LSP. The transit router examines the label of the incoming packet and swaps with the outgoing label based on the label information base and forwards the labeled packet to the outgoing interface. The egress core router removes the label from the packet and forwards the Ethernet frame to the appropriate network based on the label information. This entire packet forwarding mechanism is transparent in the access network. Hence, it does not require any special configuration on access switches.
In this topology, the devices support the following MPLS architectural roles, as indicated in the diagram and described in multiple industry MPLS references.

**Label edge router (LER):** The label edge router is located at the edge of the MPLS domain. The LER receives the native Ethernet frame and is responsible for inserting the appropriate label before forwarding the packet to the MPLS domain (ingress LER). The egress end router (egress LER) is responsible for examining the incoming label, removing the label, and forwarding the Ethernet frame to the access network. These routers are also referred to as provider edge (PE) routers. The core routers at data center locations function as LERs. In this case, the data center core routers serve the LER function.

**Label-switching router (LSR):** The transit router examines the incoming packet's label and swaps with the outgoing label based on the label information. It then forwards the labeled packet to the outgoing interface. This router is called the LSR or provider (P) router. In this case, the provider routers act as the LSRs that form the Metro Area Network (MAN) and are positioned between the data centers.

**Customer edge (CE) devices:** Customer edge devices are known as routers or switches that connect to the LERs. In the data center environment, the access layer switches function as CE devices. Core routers and the wider MPLS backbone provide the VPLS functionality, and therefore the access switches do not require any special configuration to benefit from VPLS.

In the data center, VPLS capabilities as defined in IETF VPLS and MPLS standards exist in the core data center routers. One or more VLANs are associated with each core router for VPLS. The VPLS service provided by the core routers is referred to as the VPLS domain. Each VPLS domain consists of a number of LERs, each running a VPLS instance that participates in that VPLS domain. A full mesh of LSPs is built between the VPLS instances on each of the LERs in a VPLS domain to ensure full connectivity of the LAN segments wanting to participate in the extended domain. Once the LSP mesh is built, the VPLS instance on a given LER can receive Ethernet frames from the access tier (customer edge), and based on media access control (MAC) address, switch those frames into the appropriate LSP. This switching is possible because VPLS enables the LER to act as a learning bridge with one MAC address table per VPLS instance on each LER. In other words, the VPLS instance on the label edge router has a MAC table populated by learning the MAC addresses as Ethernet frames enter on physical or logical ports, exactly the same way an Ethernet switch works to construct its LAN/VLAN topologies.
Once an Ethernet frame enters through an ingress port from the access tier, the destination MAC address is looked up in the MAC table and the frame is sent unaltered into the LSP (as long as the MAC table contains the MAC address). The LSP then delivers the frame to the correct LER at the remote site. If the MAC address is not in the MAC address table, the Ethernet frame is replicated and flooded to all logical ports associated with that VPLS instance, except for the ingress port where the frame just entered. Once the host that owns the MAC address on a specific port communicates to the LER, the MAC table is updated in the LER. As in a normal Ethernet switch, the MAC addresses that have not been used for a certain amount of time are aged out to control the MAC table size.

**VPLS Use Cases in the Data Center**

Here we outline various use cases for VPLS in data center networks. The primary purpose of VPLS is to extend Layer 2 broadcast domains across WANs/MANs using an MPLS backbone. As clarified in Juniper's Enterprise Data Center Reference Architecture, a VLAN represents a single Layer 2 broadcast domain. Without VPLS (or any other technology used to extend a VLAN), a broadcast domain is limited to a single data center location and all traffic beyond this domain is routed at Layer 3. This mandates placing server nodes (requiring Layer 2 connectivity) in a single data center location without a solution to the multi-site extension problem.

Applications that require Layer 2 connectivity among server nodes for various reasons are indicated below:

- High availability clusters
- Data replication and backup
- Server virtualization deployments using live migration
- High-performance computer cluster and grid-based applications

**High Availability Clusters**

High availability clusters are deployed to provide availability in case of server hardware failures. Nodes in the cluster provide application services in active/passive mode. Nodes check the availability of an active node using a heartbeat mechanism. In addition to heartbeat, the nodes also require real-time data replication for HA. Some data replication applications require a Layer 2 connection between source and target nodes. Live migration technologies such as Vmotion™ require a Layer 2 connection between the two connected server interfaces. This allows user sessions to migrate over to another node without disruption. Being able to place the nodes in more than one site ensures availability of the services, even if a data center becomes unavailable or when maintenance is required.

**High-Performance Computer Cluster and Grid-Based Applications**

A high-performance computer cluster environment consists of a large number of nodes that participate in the cluster, and each node is assigned a task from the central manager. Certain high-performance computer cluster applications require Layer 2 connectivity among nodes. Extending a cloud computing environment across data center locations provides a large centralized resource pool of nodes and facilitates efficient resource utilization.

**Control Traffic Considerations Between Data Centers**

When nodes in a high availability cluster or high-performance computer cluster environment are placed across WANs by extending VLANs, the HA cluster nodes check the availability of other nodes using a heartbeat mechanism. A split brain situation may occur if both nodes are up and heartbeat communication is broken during a network failure. This places some challenges in terms of resiliency and network convergence to meet the time-out requirements of heartbeat communications. The heartbeat communication not only requires a Layer 2 connection but also expects LAN-like network connection characteristics such as low latency, low jitter, fast convergence, and high throughput with QoS guarantees.
Technologies to Extend VLAN Across Data Center Locations

A range of technologies can be considered for extending Layer 2 domains across data center sites.

Dense wavelength-division multiplexing (DWDM): DWDM is a physical layer architecture which uses a fiber link between data center locations and transmits multiple data channels over a single fiber link. This requires a dedicated fiber connection between data center locations, and it requires special hardware to support DWDM in order to provide LAN-like connectivity. However, dedicated long-haul fiber connections are expensive and difficult to scale.

Ethernet Q in Q: In Ethernet Q in Q technology, an additional VLAN tag is added to the Ethernet frame. This additionally tagged frame traverses across a core network. At the destination, the original VLAN tag is retrieved and the Ethernet frame is forwarded to a local VLAN. Ethernet Q in Q requires Layer 2 loop avoidance techniques such as Spanning Tree Protocol (STP), and hence convergence time may vary. In general, Q in Q is a less scalable solution than VPLS.

Ethernet pseudowire over MPLS: Using an Ethernet pseudowire over an MPLS network extends a VLAN across two locations via a point-to-point “wire” in each direction. It utilizes MPLS and can provide fast convergence and QoS using traffic engineering. Because pseudowire requires a point-to-point connection, it also requires a full mesh of pseudowires across all sites. Resulting in Ethernet pseudowire over MPLS being a resource intensive solution that won’t scale in large deployments.

Virtual private LAN service (VPLS) over MPLS: VPLS over MPLS uses the MPLS capability of the core to extend VLANs to one or more data center locations. The high availability features defined in VPLS standards (such as LER dual homing) and topology autodiscovery features using BGP signaling make VPLS scalable and easy to deploy. Because VPLS uses MPLS as its core, it provides low latency variation and statistically bound low convergence times within the MPLS network. It also supports QoS using the traffic engineering capabilities of the MPLS network.

Table 1 compares these technologies, showing how they can be used to extend VLANs between data center sites.

### Table 1: Technology Summary for Extending VLANs Across Data Center Locations

<table>
<thead>
<tr>
<th></th>
<th>DWDM TRANSPORT</th>
<th>ETHERNET Q IN Q</th>
<th>ETHERNET PW OVER MPLS</th>
<th>VPLS OVER MPLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scalability</strong></td>
<td>Low—requires direct fiber connections</td>
<td>Low—extended L2 core network</td>
<td>Low—requires point-to-point connection</td>
<td>High—shared core, point-to-multipoint</td>
</tr>
<tr>
<td></td>
<td>between sites</td>
<td></td>
<td>between sites</td>
<td>connection</td>
</tr>
<tr>
<td><strong>Convergence</strong></td>
<td>Low</td>
<td>High—L2 convergence across network</td>
<td>Medium—L2 convergence with multiple</td>
<td>Low—MPLS backbone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sites</td>
<td></td>
</tr>
<tr>
<td><strong>Latency</strong></td>
<td>Low</td>
<td>High—L2 forwarding across core</td>
<td>Low—forwarding across LSP connection</td>
<td>Low—forwarding across LSP connection</td>
</tr>
<tr>
<td><strong>Latency Variation</strong></td>
<td>Low</td>
<td>High—L2 forwarding across core</td>
<td>Low—forwarding across LSP connection</td>
<td>Low—forwarding across LSP connection</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>High</td>
<td>Low—shared core infrastructure</td>
<td>Low—shared core infrastructure</td>
<td>Low—shared core infrastructure</td>
</tr>
<tr>
<td><strong>Provisioning operations</strong></td>
<td>Complex—requires direct fiber connections between sites</td>
<td>Complex—L2 core network</td>
<td>Complex—requires point-to-point connection mesh between site</td>
<td>Simple—shared core infrastructure, autodiscovery support</td>
</tr>
</tbody>
</table>

Benefits of Extending VLANs Using VPLS

Low Latency and Low Latency Variation

Because VPLS uses MPLS as its underlying transport, Ethernet packets forwarded in a VPLS domain are label switched across pre-established LSPs between the LER/core data center routers at each location. This label switching mechanism, using defined paths across the backbone, provides low latency as packets do not require route lookup across the WAN backbone. All packets for a given VPLS connection follow the same path, and hence provide low latency variation.
High Availability

VPLS signaling using BGP supports LER dual homing for high availability of the VLANs using the VPLS service. With LER dual homing, VLANs accessing the VPLS domain can connect to it using two different LERs within the data center. LER dual homing has an internal mechanism to avoid a Layer 2 loop, and hence does not require STP for loop prevention. In case one LER router fails, the backup LER becomes active and forwards the traffic.

VPLS also supports fast convergence times to recover from any failures in the MPLS core by supporting traffic protection mechanisms such as link protection, node protection, and active/standby label-switched paths.

QoS and Traffic Engineering

Because VPLS runs over MPLS between sites, the core can support traffic engineering using a protocol such as Resource Reservation Protocol – Traffic Engineering (RSVP-TE). Using this approach, VPLS segments can be mapped to different network paths (LSPs) based on QoS and failure recovery requirements. Prioritization of traffic over LSPs allows traffic on different VLAN segments to be handled according to performance goals, supporting both availability and service-level agreements (SLAs) for services being provided. This is essential for high availability clusters and real-time applications such as high rate transaction processing and voice and video services.

Network Segmentation

VPLS also supports logical network segmentation in support of granular security policies and compliance requirements by extending segmentation across data centers. As described in Juniper’s Enterprise Data Center Network Reference Architecture, data center networks typically need to be divided into logical segments for traffic protection, integrity, and enforcement of granular security policies. Thus, VPLS is helpful in extending this architecture between multiple sites.

Traffic segmentation for these purposes typically has the following characteristics:
- Consists of one or more VLAN/subnets.
- One segment’s traffic usually is not forwarded through stateful firewall or intrusion prevention system (IPS).
- Inter segment traffic is forwarded through firewall policy and/or IPS services.
- Can have different QoS or application acceleration requirements for intra and inter segment traffic.
- Requires a common group of network-based services such as load balancing, caching, and network address server (NAS) storage.

Because Juniper’s data center networks already provide strong segmentation capabilities within data center sites and complement application server clustering strategies, the fact that VPLS allows extension of this complementary architecture between sites creates an extremely robust design option in the hands of network managers to provide this segmentation in a scalable, resilient, and high-performance manner.

Design and Protocol Considerations

This section describes design considerations and protocol choices available for implementing VPLS in data center networks. We discuss design considerations in the following major areas:
- VPLS signaling protocols (LDP and BGP).
- MPLS signaling protocols (RSVP-TE and LDP).
- Enabling routing from the VPLS domain.
- Network services configuration for the VPLS domain.
VPLS Signaling Protocols

For VPLS to provide its services to VLANs in different data center sites, VPLS must establish a Layer 2 transport plane across the backbone network between the various nodes participating in the VPLS service so that the VLAN transport capabilities that are expected can be enabled. The L2 transports that are enabled between the different nodes participating in the VPLS service are called pseudowires. The pseudowires are established across the MPLS backbone using the VPLS control plane. The VPLS control plane has two primary functions:

- Autodiscovery
- Signaling

**Autodiscovery**—In general, autodiscovery refers to finding all LER routers that participate in a VPLS instance. An LER router can be manually configured with the identities of all other LER routers in a VPLS instance, or the LER router can use a protocol to discover the other LER routers involved. This latter method is called autodiscovery and, when used, greatly simplifies the administration of the service.

**Signaling**—After discovery occurs, each pair of LER routers in a VPLS network must establish pseudowires to each other in order to create the fully connected L2 domain required by the participating VLANs and endpoints. In the event of a change in membership in the VPLS service by an LER router, the LER must tear down the established pseudowires. This process of establishing and tearing down the pseudowires in the topology is known as signaling.

An administrator can choose either LDP or BGP for VPLS signaling, as described further in the sections below.

**Signaling for VPLS Pseudowires Using LDP**

VPLS implemented with an LDP control plane provides signaling but not autodiscovery. In this approach, LDP is used to signal the pseudowires used to interconnect VPLS instances on the LER routers. In the absence of autodiscovery, the identities of all remote LER routers that are part of the VPLS instance must be configured on each LER router. As the number of LER routers in the network increases, scaling this configuration process becomes burdensome; clearly an automated discovery process would be helpful.

In the LDP case, to exchange signaling information, the administrator must set up a full mesh of LDP sessions between each pair of LER routers that has at least one VPLS instance in common (see Figure 2). As the size of the VPLS network grows, the number of LDP targeted sessions increases exponentially on the order of $O(N^2)$, where $N$ is the number of LDP-VPLS LER routers in the network.

![Figure 2: Signaling for VPLS pseudowires using LDP](image-url)
**Signaling for VPLS Pseudowires Using BGP**

The BGP-VPLS control plane defines a means for an LER router to discover which remote LER routers are members of a given VPLS instance (autodiscovery), and for an LER router to know which pseudowire label a given remote LER router will use when sending the data to the local LER router (signaling). In the BGP-VPLS control plane, BGP carries sufficient information to provide autodiscovery and signaling functions simultaneously.

Unlike LDP VPLS, the exchange of VPLS signaling information in BGP VPLS does not require a full mesh of control sessions among all LER routers. Instead, the BGP-VPLS control plane, including its signaling component, can use a route reflector (RR) hierarchy in which only the RRrs are fully meshed (see Figure 4). Each BGP router then establishes a BGP session to one or more RRrs. Using RRrs also makes the provisioning task of adding or deleting an LER router simpler because only the BGP peering with the RR requires change.

Route reflectors are a proven technology used extensively in networks where BGP is deployed for Internet routing or for other types of VPNs. Furthermore, BGP-VPLS RRrs can be placed anywhere in the network; that is, they do not need to be on the data path of the VPLS domains that they host. This arrangement offers flexibility in deploying new RRrs when needed for even greater scaling.

![Figure 3: VPLS signaling using BGP and route reflectors in a full mesh topology](image)

**MPLS Signaling Protocols**

VPLS services run over an MPLS backbone. MPLS backbones establish LSPs that run from ingress LERs to egress LERs. VPLS requires LSPs that run from the ingress router to the egress router. For a fully meshed MPLS network, administrators must ensure that LSPs exist from every ingress router (LER router) to other LER routers. The MPLS LSPs can be signaled using RSVP or LDP. For VPLS services to function properly, administrators must enable an MPLS signaling protocol (RSVP or LDP) on the core routers that will function as LERrs at each data center location. In this way, MPLS and VPLS will work in an integrated manner.

**MPLS Signaling Using LDP**

LDP distributes MPLS labels in non traffic engineering MPLS applications. LDP allows routers to establish LSPs through a network by mapping network layer routing information directly to data link layer switched paths.

LDP creates LSP trees rooted at each egress router for the router IP address that is the subsequent BGP next hop. The ingress point is at every router running LDP. In Juniper Networks Junos® operating system, this process provides an inet.3 route to every egress router. If BGP is running, it tries to resolve next hops by first using the inet.3 table, which binds most if not all of the BGP routes to MPLS tunnel next hops.

Two adjacent routers running LDP become neighbors. When LDP routers become neighbors, they establish an LDP session to exchange label information. The LDP operates in conjunction with a unicast routing protocol. The LDP installs LSPs only when both LDP and the routing protocol are enabled. For this reason, you must enable both LDP and the routing protocol on the same set of interfaces to establish LSPs between each egress router and all ingress routers. Otherwise, loss of BGP-routed traffic may occur.
**MPLS Signaling Using RSVP**

RSVP provides not only support for dynamic signaling of MPLS LSPs but for traffic engineering support as well. RSVP must be configured on all interfaces on the path of LSPs along with an interior gateway protocol (OSPF or IS-IS) with traffic engineering support. With RSVP, administrators initiate LSP configuration at the ingress router, and the LSP is dynamically signaled across all transit routers to the egress router. RSVP supports defining all or some of the transit routers in the LSP configuration, a process referred to as either strict or loose path configuration.

RSVP supports traffic engineering with bandwidth allocation and administrative groups. RSVP also supports setting up LSPs using MPLS traffic protection mechanisms, including MPLS fast reroute, link protection, node protection, and standby LSP in case of LSP failure.

The following provides a brief description of the three types of traffic protection that can be used for preventing an LSP failure.

- **Fast Reroute**: You can configure fast reroute on an LSP to minimize an LSP failure. Fast reroute enables an upstream router to route around the failure quickly to the router that is downstream of the failure. The upstream router then signals the outage to the ingress router, thereby maintaining connectivity before a new LSP is established.

- **Link Protection**: Link protection helps ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. When link protection is configured for an interface and for an LSP that traverses this interface, a bypass LSP is created to handle traffic if the interface fails. The bypass LSP uses a different interface and path to reach the same destination. If a link protected interface fails, traffic is quickly switched to the bypass LSP.

- **Node Protection**: Node protection extends the capabilities of link protection. Link protection helps ensure that traffic traveling over a specific interface to a neighboring router can continue to reach that router if the interface fails. Node protection ensures that traffic from an LSP, traversing a neighboring router, can continue to reach its destination even if the neighboring router fails. When you enable node protection for an LSP, you must also enable link protection.

**Enabling Routing from a VPLS Domain**

Servers hosted within the same VPLS domain communicate with each other over an L2 network. The communication to servers in other VLAN/VPLS domains or to outside clients requires L3 routing to be provided for the VPLS domain. Administrators can configure an integrated routing and bridging (IRB) interface at the core tier node and associate it as the routing interface to the VPLS instance. The IRB interface is also associated with the virtual router instance representing the logical forwarding domain for granular forwarding and security policy controls.

For inbound/outbound load balancing, an administrator can choose to subnet the assigned network to the VPLS domain per location. The servers at each location can choose the gateway interface that is local on that interface for outbound load balancing. The inbound load balancing can be achieved by advertising more specific routes assigned to the location for the VPLS domain. This is illustrated in Figure 4 as load balancing for the VPLS segment uses statically split IP address space. The VPLS domain (VLAN 2106) is assigned IP network address 172.16.24.0/22 across two data center locations. The hosts in data center location left are assigned an IP address in the range 172.16.24.2 to 172.16.25.255 with a mask of 22 bits and default gateway of 172.16.24.1 which is configured on core routers. Similarly, the hosts in data center right are assigned an IP address in the range 172.16.26.2 to 172.16.27.254 with a mask of 22 bits and default gateway of 172.16.26.1 which is configured on core routers. For inbound load balancing, the core routers on the left can advertise route 172.16.24.0/23 and the core routers on the right can advertise route 172.16.26.0/23.

Administrators can configure Virtual Router Redundancy Protocol (VRRP) on the IRB interface to support high availability of L3 routing for endpoints in the VPLS domain.

VRRP can be configured among the core routers at the same location. An administrator can also choose to run VRRP across locations and use VRRP group functionality to load balance inbound/outbound traffic to and from the VPLS domain.
Network Services Configuration for the VPLS Domain

Network services such as firewalls, IPS, and application acceleration are often optimally provided in the core tier of the data center network. As described earlier, the routing interface of the VPLS instance can be part of a virtual router instance at the Ethernet services router in the core tier, representing a distinct logical L3 forwarding domain at the Ethernet services router. Multiple virtual router instances at the Ethernet services router can be used to support separated traffic flows in support of multiple service goals. This virtual router can also maintain a routing adjacency with the firewall at the core tier.

In such configurations, the firewall offers a variety of policy implementation choices relative to traffic arriving from two or more virtual routing instances in the core tier routers:

1. In the first option, all virtual routers on a core tier router connect over their own logical interfaces on the core tier firewall through 802.1q trunk interfaces. The logical interfaces are configured in separate policy zones on the firewall to maintain the forwarding integrity of the virtual routing instances. However, for efficiency in applying security policies, the separate zones can be supported in the firewall by a common, trusted virtual router policy boundary, allowing security policies to be applied consistently to traffic from all of the virtual routing domains aggregated into the firewall. This enables the application of a unified policy set to the traffic in the multiple virtual routing instances.
2. Alternatively, traffic from each virtual routing instance in the network can belong to a distinct zone and virtual router combination on the firewall. This creates multiple routing domains between the core router and the firewall per functional area. This design choice provides more granular policy control in addition to establishing a security policy between zones.

![Distinct security policies in firewalls with virtual individual virtual routing instances in the network](image)

Figure 6: Distinct security policies in firewalls with virtual individual virtual routing instances in the network

When VPLS services are extended across data center locations, IP subnets (and their address ranges) in a virtual routing instance are also shared across locations. In this configuration, we recommend allocating IP addresses between data center locations, so that a more specific subnet route can be defined at each location and a more specific route can be advertised by the associated virtual routers at each location. This approach provides traffic path optimization for inbound and outbound traffic to/from the VPLS domain, at the same time that security policies are applied in the appropriate associations, as illustrated in Figure 7.

![IP address space split across VPLS locations allowing associated distribution of firewall services](image)

Figure 7: IP address space split across VPLS locations allowing associated distribution of firewall services
If it is not possible to define a more specific subnet in the VPLS domain per location, then all inbound/outbound traffic to the VPLS domain must select a firewall on one of the locations. The traffic from other locations traverses through the VPLS network to the single gateway of the VPLS domain and is forwarded to the firewall for outbound communication. Inbound traffic is also forwarded through the same firewall and virtual router for all servers in the VPLS domain. Figure 8 shows this configuration.

Figure 8: Single IP address space distributed across VPLS locations allowing only one firewall choice

Implementation and Configuration Guidelines

In this section, we will review important implementation steps for deploying VPLS across data center locations. The primary implementation and configuration guidelines discussed in this section include the following:

- Configuring MPLS signaling at the core routers
- Configuring VPLS signaling at the core routers
- Configuring VPLS instance

The following bulleted list outlines the network setup details for lab validation of the implementation steps. Refer to Figure 9 when reviewing these steps.

- In the data center network, multiple VLANs can be configured on each access element. These VLANs are used by separate servers that connect to the access switching tier, and all are trunked from that access layer to the core network tier. We deployed the Juniper Networks EX4200 Ethernet Switch with Virtual Chassis technology as our access layer devices, but this design is also valid for any other switching platform at access tier.

- Each access tier device connects to a pair of Juniper Networks MX960 Ethernet Services Routers which act as core devices for resiliency purposes. We have used redundant trunk group (RTG) for L2 loop prevention and convergence.

- The connections from the access tier to the core are identical trunk links and are associated with VPLS instances on the MX960 routers using the same VLAN IDs. This allows the VLANs to be extended over the VPLS service.

- The core network has a redundant configuration of MX960s. Each of the Ethernet services routers is associated with the same networks and VPLS instances for high availability purposes.

- The core tier connects to the network services tier (firewalls, load balancers, caching systems, and application acceleration devices) and manages all connectivity between the server networks and other infrastructure using routing or policies.

- Both core MX960s connect to each other over VPLS LSPs, keeping the networks segmented and the access tier VLANs interconnected.

- Both core MX960s are configured to provide the default gateway IP address to the servers with high availability running the VRRP over IRB interfaces. The IRB interfaces are associated with all of the appropriate bridge domains and VPLS instances involved in the access-to-core Layer 2 services of the network.
Figure 9 illustrates the deployment of VPLS services across data center locations.

**Configuring MPLS Signaling at the Core Routers**

For MPLS to function, you must enable a signaling protocol on the core (LER) routers. For validation purposes, we have used LDP as the MPLS signaling protocol. To enable signaling using LDP, perform the following steps:

1. Configure an IGP on all the core routers. The example below shows a list of commands to configure OSPF as the IGP between the core data center routers. OSPF must be configured on all interfaces towards the MPLS backbone from the core routers, as well as on the core routers’ loopback interfaces.

   ```
   set protocols ospf traffic-engineering # enables traffic engineering support
   set protocols ospf area 0.0.0.0 interface ae0.2000 interface-type p2p # Interface to MX960-D
   set protocols ospf area 0.0.0.0 interface lo0.0 passive
   set protocols ospf area 0.0.0.0 interface ge-11/2/5.0 # Interface to MX960-A
   ```

2. Configure LDP only on the interfaces between the LER routers or between the LER routers and the P routers of the backbone. You can think of these as the “core facing” interfaces. You do not need to configure LDP on the interface between the core and access layer.

   ```
   set protocols ldp interface ge-11/2/5.0 # Interface to MX960-A
   set protocols ldp interface ae0.2000 # Interface to MX960-D
   ```

3. Configure the MPLS address family on the interfaces where you enabled LDP (the interfaces you configured in Step 2) by including the following statements:

   ```
   set protocols mpls interface ge-11/2/5.0 # Interface to MX960-A
   set protocols mpls interface ae0.2000 # Interface to MX960-D
   set interfaces ae0 unit 2000 family mpls
   set interfaces ge-11/2/5 unit 0 family mpls
   ```
Configuring VPLS Signaling Using BGP at the Core Data Center Routers

For validation purposes, we have used BGP for VPLS signaling because it is more scalable than LDP as described in the design considerations. You must configure an internal BGP (IBGP) session between the core (LER) routers to allow the LER routers to exchange information about routes originating and terminating in the VPLS network. The LER routers rely on this information to determine which labels to use for traffic destined for remote sites.

1. Configure an IBGP session for the VPLS signaling using the following commands:

```
set protocols bgp group VPLS-iBGP type internal
set protocols bgp group VPLS-iBGP local-address 172.32.252.14
set protocols bgp group VPLS-iBGP family Layer 2vpn signaling
set protocols bgp group VPLS-iBGP local-as 65010
set protocols bgp group VPLS-iBGP neighbor 172.32.252.12
set protocols bgp group VPLS-iBGP neighbor 172.32.252.13
set protocols bgp group VPLS-iBGP neighbor 172.32.252.15
```

The IP address in the local-address statement is the address of the loopback interface (lo0) on the local LER router. The IBGP session for VPLS runs through the loopback address.

**NOTE:** You must also configure the lo0 interface at the [edit interfaces] hierarchy level.

The IP address in the neighbor statement is the loopback address of the neighboring core (LER) router.

The family statement allows you to configure the IBGP session for Layer 2 VPNs and VPLS or for L3 VPNs.

2. Configure an IBGP session for VPLS using the following statement:

```
set protocols bgp group VPLS-iBGP family Layer 2vpn signaling
```

Configuring a VPLS Instance

A VPLS instance is configured on the core router to map the VLAN on the access tier which will be extended using VPLS services to the other data center locations.

1. Each VPLS is configured under a routing instance of type vpls. A VPLS routing instance can carry Ethernet traffic transparently across the MPLS backbone.

```
set routing-instances VPLS2106 [VPLS instance name] instance-type vpls
```

When you enable BGP signaling for each VPLS routing instance, you must configure a site range. The site range specifies the total number of sites in the VPLS.

2. Configure a site range for VPLS instance using the following command:

```
set routing-instances VPLS2106 [VPLS instance name] protocols vpls site-range 20 [range value]
```

When you configure BGP signaling for the VPLS routing instance, you must configure each VPLS site that has a connection to the LER router on each LER router.

3. You must configure a site name and site identifier for each VPLS site using the following command:

```
set routing-instances VPLS2106 protocols vpls site FA-NetworkMgmt [site name] site-identifier 3 [site id]
```

Each routing instance that you configure on an LER router must have a unique route distinguisher associated with it. VPN and VPLS routing instances need a route distinguisher to help BGP distinguish between potentially identical network layer reachability information (NLRI) messages received from different VPNs.

4. To configure a route distinguisher on an LER router, use the following command:

```
set routing-instances VPLS2106 route-distinguisher 65010:2106 [route-distinguisher value]
```
5. Configuring a VPN routing and forwarding (VRF) target community using the vrf-target statement causes default VRF import and export policies to be generated that accept and tag routes with the specified target community. You can still create more complex policies by explicitly configuring VRF import and export policies. These policies override the default policies generated when you configure the vrf-target statement.

If you do not configure the import and export options of the vrf-target statement, the specified community string is applied in both directions. The import and export keywords offer more flexibility, allowing you to specify a different community for each direction.

```txt
set routing-instances VPLS2106 vrf-target target:65010:2106
```

6. All logical interfaces belonging to a VPLS routing instance are listed under that instance using the following commands:

```txt
set routing-instances VPLS2106 interface xe-10/0/0.2106
set routing-instances VPLS2106 interface xe-10/1/0.2106
```

7. You can configure VPLS without a Tunnel Services PIC. To do so, you use a labels-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the LER router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance.

By default, VPLS requires a Tunnel Services PIC. To configure VPLS on a router without a Tunnel Services PIC, include the no-tunnel-services statement:

```txt
set routing-instances VPLS2106 protocols vpls no-tunnel-services
```

8. To enable routing from the VPLS domain to other networks, you need to assign the routing interface. An IRB interface is configured with the VLAN associated for VPLS using the following commands. This example also shows configuration of VRRP for redundancy purposes.

```txt
set interfaces irb unit 2106 family inet address 172.16.26.2/22 vrrp-group 0 virtual-address 172.16.26.1
set interfaces irb unit 2106 family inet address 172.16.26.2/22 vrrp-group 0 priority 200
set interfaces irb unit 2106 family inet address 172.16.26.2/22 vrrp-group 0 accept-data
```

9. You can associate the routing interface to a VPLS instance using the following commands. You must assign a vlan-id to the VPLS instance when the routing interface is associated with the instance.

```txt
set routing-instances VPLS2106 vlan-id 2106
set routing-instances VPLS2106 routing-interface irb.2106
```

10. The routing interface associated with a VPLS instance can be part of the main routing table, or it can be used to separate the routing table using the routing instance type “virtual router.” Support for a virtual router provides logical network segmentation for granular routing and forwarding policy control. As shown in the following command, the IRB interface is associated with the virtual router.

```txt
set routing-instances FA-WEB [routing-instance name] instance-type virtual-router
set routing-instances FA-WEB interface irb.2106
```
11. If the IRB interface is configured as an active interface for OSPF, it will establish adjacency across the VPLS domain to other sites. To avoid this, the IRB interface is configured as a passive OSPF interface. The virtual routers at the same data center locations are connected through another logical interface (ae0.2106) to provide L3 redundancy.

```plaintext
set routing-instances FA-WEB interface ae0.2106
set routing-instances FA-WEB protocols ospf area 0.0.0.0 interface irb.2106
passive
set routing-instances FA-WEB protocols ospf area 0.0.0.0 interface irb.2106
metric 500
set routing-instances FA-WEB protocols ospf area 0.0.0.0 interface ae0.2106
interface-type p2p
set routing-instances FA-WEB protocols ospf area 0.0.0.0 interface ae0.2106
metric 500
```

Summary

In this paper, we have described in detail the incredible potential for implementing VPLS to support emerging applications, as well as for easily migrating applications from legacy infrastructures to more modern infrastructures. Through this process, we have briefly described the VPLS technology umbrella and capabilities, we have examined a variety of design considerations to the MPLS backbone and VPLS transport signaling, and we have covered a set of considerations related to L3 boundaries in the data center, QoS implementation, high availability, and security enforcement.

The ultimate goal of any network designer is to create a network infrastructure that is scalable, reliable, and flexible in such a way that new applications and new business processes do not mandate significant overhaul to the network infrastructure. Throughout this document, we have described the implementation details for building a single/unified logical network across multiple data center locations. Implementing such technology relieves network engineers and architects from the constant challenge of knowing how to most efficiently install an application server into the data center network given the specific requirements of that application. With the adoption of VPLS, the advantages are enormous—server connectivity decisions can be made by a physical resource allocation manager within the data center, and application support decisions can be made by an application developer, allowing the network to implement these easily by a network policy configuration! Beyond solving a tactical problem of locating servers in different locations, we are now solving an operational business challenge by proposing a fresh and open approach to managing data center compute resources.

As a proven provider of MPLS/VPLS technology, supported by its newly-designed MX Series 3D Universal Edge Routers, Juniper remains committed to enabling network designers to enhance their current data center infrastructures to create state-of-the-art, ultra low latency networks that offer scalability and efficiency.

Demonstrating and establishing this support comes with Juniper’s 2009 recently-awarded contract from NYSE Euronext (NYX) which will allow Euronext to leverage the high-performance switching and routing technologies of the MX Series. “Juniper’s simplified data center approach will allow us to deploy a complete 10-Gigabit Ethernet network with ultra low latency at a substantial cost savings,” said Steve Rubinow, executive vice president and co-global CIO of NYSE Euronext. “Juniper has developed truly unique and innovative technologies that help us to deploy a very high capacity, low latency network that meets the stringent demands of the new data center. With Juniper, we are able to dramatically cut the cost and complexity of managing our data center network today, while continuing to enhance our competitive position with a next-generation data center fabric that will enable us to scale to tens of thousands of 10GbE ports. With such an elastic and efficient infrastructure, we can provide enhanced functionality to our customers at unmatched scale while minimizing total cost of ownership.”
IMPLEMENTATION GUIDE - Implementing VPLS for Data Center Interconnectivity

Appendix A Configuration

Figure 10 illustrates the network topology to extend VLANs across datacenter locations using VPLS followed by configuration details and commands for functional verification.

![Network Topology Diagram](image)

**Figure 10: Extending VLANs across data center locations using VPLS**

Configuration Examples

Below are configuration snippets for relevant configuration sections for extending VLAN across data center locations using Virtual Private LAN services.

**NOTE:** All devices are running Junos OS release 9.5.

Data Center Location 1

**MX960-A**

```
root@MX960-A> show configuration
version 9.5R1.8;

chassis {
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
}

interfaces {
    ge-0/1/5 {
        unit 0 {
            family inet {
                address 172.16.16.1/30;
            }
            family mpls;
        }
    }
```
xe-1/3/0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 600 {
        vlan-id 600;
        family inet {
            address 172.16.15.1/30;
        }
        family mpls;
    }
}
xe-10/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
xe-10/1/0 {
    gigether-options {
        802.3ad ae0;
    }
}
xe-10/2/0 {
    gigether-options {
        802.3ad ae1;
    }
}
xe-10/3/0 {
    gigether-options {
        802.3ad ae1;
    }
}
}
ae0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 10 {
        encapsulation vlan-vpls;
        vlan-id 10;
        family vpls;
    }
    unit 20 {
        encapsulation vlan-vpls;
        vlan-id 20;
        family vpls;
    }
}
ae1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 10 {

encapsulation vlan-vpls;
  vlan-id 10;
  family vpls;
}
unit 20 {
  encapsulation vlan-vpls;
  vlan-id 20;
  family vpls;
}
}
irb {
  unit 0;
  unit 10 {
    family inet {
      address 172.16.10.2/23 {
        vrrp-group 0 {
          virtual-address 172.16.10.1;
          priority 200;
          accept-data;
        }
      }
    }
  }
  unit 20 {
    family inet {
      address 172.16.20.2/23 {
        vrrp-group 0 {
          virtual-address 172.16.20.1;
          priority 250;
          accept-data;
        }
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.10.16.32/32;
    }
  }
}
}
routing-options {
  autonomous-system 65100;
}
protocols {
  mpls {
    interface all;
  }
  bgp {
    local-address 10.10.16.32;
    local-as 65100;
    group VPLS-IBGP {
      type internal;
      family 12vpn {
        signaling;
      }
    }
  }
}
neighbor 10.10.17.32;
neighbor 10.10.8.32;
neighbor 10.10.19.32;
}
}
ospf {
    area 0.0.0.0 {
        interface ge-0/1/5.0;
        interface lo0.0;
        interface xe-1/3/0.600;
    }
}
}
ldp {
    interface ge-0/1/5.0;
    interface xe-1/3/0.600;
    interface lo0.0;
}
}
routing-instances {
    VPLS10 {
        instance-type vpls;
        vlan-id 10;
        interface ae0.10;
        interface ae1.10;
        routing-interface irb.10;
        route-distinguisher 10.10.16.32:10;
        vrf-target target:65100:10;
        protocols {
            vpls {
                site-range 20;
                no-tunnel-services;
                site VPLS10 {
                    site-identifier 1;
                }
            }
        }
    }
    VPLS20 {
        instance-type vpls;
        vlan-id 20;
        interface ae0.20;
        interface ae1.20;
        routing-interface irb.20;
        route-distinguisher 10.10.16.32:20;
        vrf-target target:65100:20;
        protocols {
            vpls {
                site-range 20;
                no-tunnel-services;
                site VPLS20 {
                    site-identifier 1;
                }
            }
        }
    }
}
root@MX960-B> show configuration
version 9.5R1.8;

chassis {
  aggregated-devices {
    ethernet {
      device-count 2;
    }
  }
}

interfaces {
  ge-0/1/5 {
    unit 0 {
      family inet {
        address 172.16.17.1/30;
      }
      family mpls;
    }
  }
  xe-1/3/0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 600 {
      vlan-id 600;
      family inet {
        address 172.16.15.2/30;
      }
      family mpls;
    }
  }
  xe-10/0/0 {
    gigether-options {
      802.3ad ae0;
    }
  }
  xe-10/1/0 {
    gigether-options {
      802.3ad ae0;
    }
  }
  xe-10/2/0 {
    gigether-options {
      802.3ad ae1;
    }
  }
  xe-10/3/0 {
    gigether-options {
      802.3ad ae1;
    }
  }
  ae0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
      minimum-links 2;
      link-speed 10g;
    }
  }
}
Implementing VPLS for Data Center Interconnectivity

UNIT 10
encapsulation vlan-vpls;
vlan-id 10;
family vpls;

UNIT 20
encapsulation vlan-vpls;
vlan-id 20;
family vpls;

AE1
flexible-vlan-tagging;
encapsulation flexible-ethernet-services;
aggregated-ether-options {
  minimum-links 2;
  link-speed 10g;
}
UNIT 10
encapsulation vlan-vpls;
vlan-id 10;
family vpls;
UNIT 20
encapsulation vlan-vpls;
vlan-id 20;
family vpls;

IRB
UNIT 10
family inet {
  address 172.16.10.3/23 {
    vrrp-group 0 {
      virtual-address 172.16.10.1;
      priority 100;
      accept-data;
    }
  }
}
UNIT 20
family inet {
  address 172.16.20.3/23 {
    vrrp-group 0 {
      virtual-address 172.16.20.1;
      priority 200;
      accept-data;
    }
  }
}

LO0
UNIT 0
family inet {
  address 10.10.17.32/32;


} } 
} 

routing-options { autonomous-system 65100; } 

protocols { 
  mpls { 
    interface all; 
  } 
  bgp { 
    local-address 10.10.17.32; 
    local-as 65100; 
    group VPLS-IBGP { 
      type internal; 
      family 12vpn { 
        signaling; 
      } 
      neighbor 10.10.8.32; 
      neighbor 10.10.16.32; 
      neighbor 10.10.19.32; 
    } 
  } 
  ospf { 
    area 0.0.0.0 { 
      interface ge-0/1/5.0; 
      interface lo0.0; 
      interface xe-1/3/0.600; 
    } 
  } 
  ldp { 
    interface ge-0/1/5.0; 
    interface xe-1/3/0.600; 
    interface lo0.0; 
  } 
} 

routing-instances { 
  VPLS10 { 
    instance-type vpls; 
    vlan-id 10; 
    interface ae0.10; 
    interface ae1.10; 
    routing-interface irb.10; 
    route-distinguisher 10.10.17.32:10; 
    vrf-target target:65100:10; 
    protocols { 
      vpls { 
        site-range 20; 
        no-tunnel-services; 
        site VPLS10 { 
          site-identifier 2; 
        } 
      } 
    } 
  } 
  VPLS20 { 
    instance-type vpls; 
  }
vlan-id 20;
interface ae0.20;
interface ae1.20;
routing-interface irb.20;
route-distinguisher 10.10.17.32:20;
vrf-target target:65100:20;
protocols {
    vpls {
        site-range 20;
        no-tunnel-services;
        site VPLS20 {
            site-identifier 2;
        }
    }
}
}

EX4200-C

root@EX4200-C> show configuration
version 9.5R2.7;
    system {
        host-name EX4200-C;
    }
    chassis {
        aggregated-devices {
            ethernet {
                device-count 2;
            }
        }
        interfaces {
            xe-0/1/0 {
                ether-options {
                    802.3ad ae0;
                }
            }
            xe-0/1/1 {
                ether-options {
                    802.3ad ae0;
                }
            }
            xe-2/1/0 {
                ether-options {
                    802.3ad ae1;
                }
            }
            xe-2/1/1 {
                ether-options {
                    802.3ad ae1;
                }
            }
            ae0 {
                aggregated-ether-options {
                    minimum-links 2;
                }
            }
        }
    }
link-speed 10g; }
unit 0 {
  family ethernet-switching {
    port-mode trunk;
    vlan {
      members [ HR Engg Sales ];
    }
  }
}
ae1 {
  aggregated-ether-options {
    minimum-links 2;
    link-speed 10g;
  }
  unit 0 {
    family ethernet-switching {
      port-mode trunk;
      vlan {
        members [ HR Sales Engg ];
      }
    }
  }
}
vlan {
  unit 10 {
    family inet {
      address 172.16.10.10/23;
    }
  }
  unit 20 {
    family inet {
      address 172.16.20.10/23;
    }
  }
}
vme {
  unit 0 {
    family inet {
      address 192.168.3.192/24;
    }
  }
}
eternet-switching-options {
  redundant-trunk-group {
    group RTG3 {
      interface ae0.0 {
        primary;
      }
      interface ae1.0;
    }
  }
}
vlans {
  Engg {
    vlan-id 20;
l3-interface vlan.20;
}
HR {
  vlan-id 10;
  l3-interface vlan.10;
}
Sales {
  vlan-id 30;
}
}
virtual-chassis {
  member 1 {
    mastership-priority 255;
  }
  member 0 {
    mastership-priority 255;
  }
  member 2 {
    mastership-priority 128;
  }
}

EX4200-D

root@EX4200-D> show configuration
version 9.5R2.7;
system {
  host-name EX4200-D;
}
chassis {
  redundancy {
    graceful-switchover;
  }
  aggregated-devices {
    ethernet {
      device-count 2;
    }
  }
}
interfaces {
  xe-0/1/0 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-0/1/1 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-2/1/0 {
    ether-options {
      802.3ad ae1;
    }
  }
  xe-2/1/1 {
    ether-options {
802.3ad ael;
}
}

ae0 {
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ HR Engg Sales ];
            }
        }
    }
}

ae1 {
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ HR Engg Sales ];
            }
        }
    }
}

vlan {
    unit 10 {
        family inet {
            address 172.16.10.11/23;
        }
    }
    unit 20 {
        family inet {
            address 172.16.20.11/23;
        }
    }
}

vme {
    unit 0 {
        family inet {
            address 192.168.3.193/24;
        }
    }
}

ethernet-switching-options {
    voip;
    redundant-trunk-group {
        group RTG4 {
            interface ae0.0 {
                primary;
            }
        }
    }
}
interface ae1.0;
}

vlans {
  Engg {
    vlan-id 20;
    l3-interface vlan.20;
  }
  HR {
    vlan-id 10;
    l3-interface vlan.10;
  }
  Sales {
    vlan-id 30;
  }
}

virtual-chassis {
  member 1 {
    mastership-priority 255;
  }
  member 0 {
    mastership-priority 128;
  }
  member 2 {
    mastership-priority 128;
  }
}

Data Center Location 2

MX960-C

root@MX960-C> show configuration
version 9.5R1.8;

chassis {
  aggregated-devices {
    ethernet {
      device-count 2;
    }
  }
}

interfaces {
  ge-0/1/5 {
    unit 0 {
      family inet {
        address 172.16.18.1/30;
      }
      family mpls;
    }
  }
  xe-1/3/0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 500 {
      vlan-id 500;
    }
  }
}

Copyright © 2011, Juniper Networks, Inc.
family inet {
    address 172.16.21.1/30;
}
family mpls;
}
xe-10/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
xe-10/1/0 {
    gigether-options {
        802.3ad ae0;
    }
}
xe-10/2/0 {
    gigether-options {
        802.3ad ae1;
    }
}
xe-10/3/0 {
    gigether-options {
        802.3ad ae1;
    }
}
ae0 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 10 {
        encapsulation vlan-vpls;
        vlan-id 10;
        family vpls;
    }
    unit 20 {
        encapsulation vlan-vpls;
        vlan-id 20;
        family vpls;
    }
}
ae1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 10 {
        encapsulation vlan-vpls;
        vlan-id 10;
        family vpls;
    }
    unit 20 {
        encapsulation vlan-vpls;
vlan-id 20;
family vpls;
}
)

irb {
    unit 10 {
        family inet {
            address 172.16.11.2/23 {
                vrrp-group 0 {
                    virtual-address 172.16.11.1;
                    priority 200;
                    accept-data;
                }
            }
        }
    }
    unit 20 {
        family inet {
            address 172.16.20.4/23 {
                vrrp-group 0 {
                    virtual-address 172.16.20.1;
                    priority 150;
                    accept-data;
                }
            }
        }
    }
}

lo0 {
    unit 0 {
        family inet {
            address 10.10.8.32/32;
        }
    }
}

routing-options {
    autonomous-system 65100;
}

protocols {
    mpls {
        interface all;
    }
    bgp {
        local-address 10.10.8.32;
        local-as 65100;
        group VPLS-IBGP {
            type internal;
            family 12vpn {
                signaling;
            }
            neighbor 10.10.17.32;
            neighbor 10.10.16.32;
            neighbor 10.10.19.32;
        }
    }
    ospf {
area 0.0.0.0 {
  interface ge-0/1/5.0;
  interface lo0.0;
  interface xe-1/3/0.500;
}

ldp {
  interface ge-0/1/5.0;
  interface xe-1/3/0.500;
  interface lo0.0;
}

routing-instances {
  VPLS10 {
    instance-type vpls;
    vlan-id 10;
    interface ae0.10;
    interface ae1.10;
    routing-interface irb.10;
    route-distinguisher 10.10.8.32:10;
    vrf-target target:65100:10;
    protocols {
      vpls {
        site-range 20;
        no-tunnel-services;
        site VPLS10 {
          site-identifier 3;
        }
      }
    }
  }
  VPLS20 {
    instance-type vpls;
    vlan-id 20;
    interface ae0.20;
    interface ae1.20;
    routing-interface irb.20;
    route-distinguisher 10.10.8.32:20;
    vrf-target target:65100:20;
    protocols {
      vpls {
        site-range 20;
        no-tunnel-services;
        site VPLS20 {
          site-identifier 3;
        }
      }
    }
  }
}
root@MX960-D> show configuration
version 9.5R1.8;

chassis {
    aggregated-devices {
        ethernet {
            device-count 2;
        }
    }
}

interfaces {
    ge-0/1/5 {
        unit 0 {
            family inet {
                address 172.16.19.1/30;
            }
            family mpls;
        }
    }
    xe-1/3/0 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 500 {
            vlan-id 500;
            family inet {
                address 172.16.21.2/30;
            }
            family mpls;
        }
    }
    xe-10/0/0 {
        gigether-options {
            802.3ad ae0;
        }
    }
    xe-10/1/0 {
        gigether-options {
            802.3ad ae0;
        }
    }
    xe-10/2/0 {
        gigether-options {
            802.3ad ae1;
        }
    }
    xe-10/3/0 {
        gigether-options {
            802.3ad ae1;
        }
    }
    ae0 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        aggregated-ether-options {
            minimum-links 2;
            link-speed 10g;
        }
    }
}
unit 10 {
    encapsulation vlan-vpls;
    vlan-id 10;
    family vpls;
}
unit 20 {
    encapsulation vlan-vpls;
    vlan-id 20;
    family vpls;
}

ae1 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 10 {
        encapsulation vlan-vpls;
        vlan-id 10;
        family vpls;
    }
    unit 20 {
        encapsulation vlan-vpls;
        vlan-id 20;
        family vpls;
    }
}

irb {
    unit 10 {
        family inet {
            address 172.16.11.3/23 {
                vrrp-group 0 {
                    virtual-address 172.16.11.1;
                    priority 100;
                    accept-data;
                }
            }
        }
    }
    unit 20 {
        family inet {
            address 172.16.20.5/23 {
                vrrp-group 0 {
                    virtual-address 172.16.20.1;
                    priority 100;
                    accept-data;
                }
            }
        }
    }
}

lo0 {
    unit 0 {
        family inet {
            address 10.10.19.32/32;
        }
    }
}


```plaintext
routing-options {
    autonomous-system 65100;
}
protocols {
    mpls {
        interface all;
    }
    bgp {
        local-address 10.10.19.32;
        local-as 65100;
        group VPLS-IBGP {
            type internal;
            family 12vpn {
                signaling;
            }
            neighbor 10.10.17.32;
            neighbor 10.10.16.32;
            neighbor 10.10.8.32;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface ge-0/1/5.0;
            interface lo0.0;
            interface xe-1/3/0.500;
        }
    }
    ldp {
        interface ge-0/1/5.0;
        interface xe-1/3/0.500;
        interface lo0.0;
    }
}
routing-instances {
    VPLS10 {
        instance-type vpls;
        vlan-id 10;
        interface ae0.10;
        interface ae1.10;
        routing-interface irb.10;
        route-distinguisher 10.10.9.32:10;
        vrf-target target:65100:10;
        protocols {
            vpls {
                site-range 20;
                no-tunnel-services;
                site VPLS10 {
                    site-identifier 4;
                }
            }
        }
    }
    VPLS20 {
        instance-type vpls;
    }
}```
```
vlan-id 20;
interface ae0.20;
interface ae1.20;
routing-interface irb.20;
route-distinguisher 10.10.9.32:20;
vrf-target target:65100:20;
protocols {
  vpls {
    site-range 20;
    no-tunnel-services;
    site VPLS20 {
      site-identifier 4;
    }
  }
}
}
}

EX4200-E

root@EX4200-E> show configuration
version 9.5R2.7;
system {
  host-name EX4200-E;
}
chassis {
  redundancy {
    graceful-switchover;
  }
  aggregated-devices {
    ethernet {
      device-count 2;
    }
  }
}
interfaces {
  xe-0/1/0 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-0/1/1 {
    ether-options {
      802.3ad ae0;
    }
  }
  xe-2/1/0 {
    ether-options {
      802.3ad ae1;
    }
  }
  xe-2/1/1 {
    ether-options {
      802.3ad ae1;
    }
  }
}
ae0 {
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ Engg HR Sales ];
            }
        }
    }
}

ea1 {
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ Engg HR Sales ];
            }
        }
    }
}

vlan {
    unit 10 {
        family inet {
            address 172.16.11.10/23;
        }
    }
    unit 20 {
        family inet {
            address 172.16.21.10/23;
        }
    }
}

route-options {
    graceful-restart;
}

ethernet-switching-options {
    redundant-trunk-group {
        group RTG1 {
            interface ae0.0;
            interface ae1.0 {
                primary;
            }
        }
    }
}

vlans {
    Engg {
        Engg {
```yaml
vlan-id 20;
l3-interface vlan.20;
}
HR {
vlan-id 10;
l3-interface vlan.10;
}
Sales {
vlan-id 30;
}
}
virtual-chassis {
    member 0 {
        mastership-priority 128;
    }
    member 1 {
        mastership-priority 250;
    }
    member 2 {
        mastership-priority 128;
    }
}
{master:1}

EX4200-F

root@EX4200-F> show configuration
version 9.5R2.7;
system {
host-name EX4200-F;
}
chassis {
    aggregated-devices {
        ethernet {
            device-count 2;
            }
        }
    }
}
interfaces {
xe-0/1/0 {
    ether-options {
        802.3ad ae0;
    }
}
xe-0/1/1 {
    ether-options {
        802.3ad ae0;
    }
}
xe-2/1/0 {
    ether-options {
        802.3ad ae1;
    }
}
xe-2/1/1 {
```
ether-options {
    802.3ad ae1;
}

ae0 {
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ HR Engg Sales ];
            }
        }
    }
}

ae1 {
    aggregated-ether-options {
        minimum-links 2;
        link-speed 10g;
    }
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members [ HR Engg Sales ];
            }
        }
    }
}

vlan {
    unit 10 {
        family inet {
            address 172.16.11.11/23;
        }
    }
    unit 20 {
        family inet {
            address 172.16.21.11/23;
        }
    }
}

vme {
    unit 0 {
        family inet {
            address 192.168.3.195/24;
        }
    }
}

routing-options {
    graceful-restart;
}

ethernet-switching-options {
    redundant-trunk-group {
IMPLEMENTATION GUIDE - Implementing VPLS for Data Center Interconnectivity

group RTG2 {
    interface ae0.0 {
        primary;
    }
    interface ae1.0;
}
vlans {
    Engg {
        vlan-id 20;
        l3-interface vlan.20;
    }
    HR {
        vlan-id 10;
        l3-interface vlan.10;
    }
    Sales {
        vlan-id 30;
    }
}
virtual-chassis {
    member 1 {
        mastership-priority 255;
    }
    member 0 {
        mastership-priority 128;
    }
    member 2 {
        mastership-priority 128;
    }
}
{master:1}

Show Commands
Below are several show commands for verification of VPLS services across the data center location.

Verifying LDP Neighbor Status

```
root@MX960-B> show ldp session
Address           State        Connection     Hold time
10.10.16.32         Operational  Open             21
172.31.254.4        Operational  Open             28
```
Verifying Internal-BGP Neighbor Status

root@MX960-B> show bgp summary

Groups: 1  Peers: 3  Down peers: 0

Table       Tot Paths  Act Paths  Suppressed  History  Damp  State     Pending
inet.0       0          0          0          0         0         0           0
bgp.l2vpn.0   6          6          0          0         0         0           0

Peer         AS  InPkt  OutPkt  OutQ  Flaps  Last Up/Dwn
State      #Active/Received/Accepted/Damped...
10.10.8.32  65100  75345  75386  0       1     1:05:48
          Establ
bgp.l2vpn.0: 2/2/2/0
VPLS10.l2vpn.0: 1/1/1/0
VPLS20.l2vpn.0: 1/1/1/0
10.10.16.32 65100  75354  75384  0       0     3w2d17h
          Establ
bgp.l2vpn.0: 2/2/2/0
VPLS10.l2vpn.0: 1/1/1/0
VPLS20.l2vpn.0: 1/1/1/0
10.10.19.32 65100  75402  75385  0       1     1:05:55
          Establ
bgp.l2vpn.0: 2/2/2/0
VPLS10.l2vpn.0: 1/1/1/0
VPLS20.l2vpn.0: 1/1/1/0

Display VPLS Connections

root@MX960-A2> show vpls connections
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <- -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not available
BK -- Backup connection         ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy

Legend for interface status
Up -- operational
Dn -- down

Instance: VPLS10
Local site: VPLS10 (1)

<table>
<thead>
<tr>
<th>connection-site</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>rmt</td>
<td>Up</td>
<td>Aug 10 00:54:02 2009</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote PE: 10.10.17.32, Negotiated control-word: No
Incoming label: 262162, Outgoing label: 262161
Local interface: lsi.1048845, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS10 local site 1 remote site 2
   rmt  Up    Aug 12 00:06:31 2009  1
Remote PE: 10.10.8.32, Negotiated control-word: No
Incoming label: 262163, Outgoing label: 262161
Local interface: lsi.1048850, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS10 local site 1 remote site 3
   rmt  Up    Aug 12 00:06:22 2009  1
Remote PE: 10.10.19.32, Negotiated control-word: No
Incoming label: 262164, Outgoing label: 262177
Local interface: lsi.1048848, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS10 local site 1 remote site 4

Instance: VPLS20
Local site: VPLS20 (1)
   connection-site  Type  St    Time last up  # Up trans
   2                   rmt  Up    Aug 10 00:54:02 2009  1
Remote PE: 10.10.17.32, Negotiated control-word: No
Incoming label: 262170, Outgoing label: 262169
Local interface: lsi.1048844, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS20 local site 1 remote site 2
   rmt  Up    Aug 12 00:06:31 2009  1
Remote PE: 10.10.8.32, Negotiated control-word: No
Incoming label: 262171, Outgoing label: 262169
Local interface: lsi.1048851, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS20 local site 1 remote site 3
   rmt  Up    Aug 12 00:06:22 2009  1
Remote PE: 10.10.19.32, Negotiated control-word: No
Incoming label: 262172, Outgoing label: 262169
Local interface: lsi.1048849, Status: Up, Encapsulation: VPLS
Description: Intf - vpls VPLS20 local site 1 remote site 4

Display VPLS mac-table

root@MX960-B1> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC,
       SE -Statistics enabled, NM -Non configured MAC)

Routing instance : VPLS10
Bridging domain : __VPLS10__, VLAN : 10
   MAC       MAC    Logical
   address   flags  interface
  00:00:5e:00:01:00  D  lsi.1048595
  00:19:e2:54:3e:c0  D  lsi.1048589
  00:19:e2:b1:bf:f0  D  lsi.1048589
  00:19:e2:b7:7f:f0  D  lsi.1048595
  00:1f:12:32:11:80  D  ae0.10

MAC flags (S -static MAC, D -dynamic MAC,
       SE -Statistics enabled, NM -Non configured MAC)

Routing instance : VPLS20
Bridging domain : __VPLS20__, VLAN : 20
   MAC       MAC    Logical
   address   flags  interface
  00:00:5e:00:01:00  D  lsi.1048585
  00:19:e2:54:3e:c0  D  lsi.1048585
00:1f:12:32:03:80  D  lsi.1048596
00:1f:12:32:07:80  D  lsi.1048596

root@MX960-C1> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC,
SE -Statistics enabled, NM -Non configured MAC)

Routing instance : VPLS10
Bridging domain : __VPLS10__, VLAN : 10
MAC               MAC      Logical
address             flags    interface
00:19:e2:54:3e:c0   D        lsi.1048597
00:19:e2:b1:bf:f0   D        lsi.1048597
00:19:e2:b6:5f:f0   D        lsi.1048586
00:1f:12:32:07:80   D        ae1.10
00:1f:12:32:11:80   D        lsi.1048595

MAC flags (S -static MAC, D -dynamic MAC,
SE -Statistics enabled, NM -Non configured MAC)

Routing instance : VPLS20
Bridging domain : __VPLS20__, VLAN : 20
MAC               MAC      Logical
address             flags    interface
00:00:5e:00:01:00   D        lsi.1048598
00:19:e2:54:3e:c0   D        lsi.1048598
00:19:e2:b1:bf:f0   D        lsi.1048598
00:1f:12:32:03:80   D        ae0.20
00:1f:12:32:07:80   D        ae1.20

Display VRRP Details

root@MX960-A2> show vrrp detail
Physical interface: irb, Unit: 10, Address: 172.16.10.2/23
  Index: 74, SNMP ifIndex: 324, VRRP-Traps: enabled
  Interface state: up, Group: 0, State: master
  Priority: 200, Advertisement interval: 1, Authentication type: none
  Delay threshold: 100, Computed send rate: 0
  Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 172.16.10.1
  Advertisement Timer: 0.833s, Master router: 172.16.10.2
  Virtual router uptime: 02:20:29, Master router uptime: 02:20:23
  Virtual Mac: 00:00:5e:00:01:00
  Tracking: disabled

Physical interface: irb, Unit: 20, Address: 172.16.20.2/23
  Index: 90, SNMP ifIndex: 560, VRRP-Traps: enabled
  Interface state: up, Group: 0, State: master
  Priority: 250, Advertisement interval: 1, Authentication type: none
  Delay threshold: 100, Computed send rate: 0
  Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 172.16.20.1
  Advertisement Timer: 0.936s, Master router: 172.16.20.2
  Virtual router uptime: 00:46:45, Master router uptime: 00:46:40
  Virtual Mac: 00:00:5e:00:01:00
  Tracking: disabled
root@MX960-C1> show vrrp detail
Physical interface: irb, Unit: 10, Address: 172.16.11.2/23
   Index: 77, SNMP ifIndex: 355, VRRP-Traps: enabled
   Interface state: up, Group: 0, State: master
   Priority: 200, Advertisement interval: 1, Authentication type: none
   Delay threshold: 100, Computed send rate: 0
   Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 172.16.11.1
   Advertisement Timer: 0.148s, Master router: 172.16.11.2
   Virtual router uptime: 02:16:30, Master router uptime: 02:16:25
   Virtual Mac: 00:00:5e:00:01:00
   Tracking: disabled

Physical interface: irb, Unit: 20, Address: 172.16.20.4/23
   Index: 94, SNMP ifIndex: 358, VRRP-Traps: enabled
   Interface state: up, Group: 0, State: backup
   Priority: 150, Advertisement interval: 1, Authentication type: none
   Delay threshold: 100, Computed send rate: 0
   Preempt: yes, Accept-data mode: yes, VIP count: 1, VIP: 172.16.20.1
   Dead timer: 3.003s, Master priority: 250, Master router: 172.16.20.2
   Virtual router uptime: 00:42:52
   Tracking: disabled

Appendix B Reference List

Table 2 lists additional publications that can be used as references.

<table>
<thead>
<tr>
<th>PUBLICATIONS</th>
<th>PUBLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS</td>
<td>Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network. See “Junos Internet Software Network Operations Guides” at <a href="http://www.juniper.net/techpubs/software/junos/junos81/swcmdref81-protocols/html/about-protocols7.html">www.juniper.net/techpubs/software/junos/junos81/swcmdref81-protocols/html/about-protocols7.html</a>.</td>
</tr>
<tr>
<td>MPLS log reference</td>
<td>Describes MPLS status and error messages that appear in the output of the show mpls lsp extensive command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network. See “Junos Internet Software Network Operations Guides” at <a href="http://www.juniper.net/techpubs/en_US/junos9.6/information-products/topic-collections/syslog-messages/syslog-messages.pdf">www.juniper.net/techpubs/en_US/junos9.6/information-products/topic-collections/syslog-messages/syslog-messages.pdf</a>.</td>
</tr>
</tbody>
</table>
About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.