Understanding JUNOS MPLS Components for EX Series Switches

JUNOS MPLS for Juniper Networks EX Series Ethernet Switches supports Layer 2 protocols and Layer 2 virtual private networks (VPNs). You can configure MPLS on your switches to increase transport efficiency in your network. MPLS services can be used to connect various sites to a backbone network or to ensure better performance for low-latency applications such as VoIP and other business-critical functions.

Provider Edge Switches

To implement MPLS on EX Series switches, you must configure two provider edge switches—that is, an ingress provider edge switch and an egress provider edge switch.

The ingress switch (the entry point to the MPLS tunnel) receives an IP packet, analyzes it, and pushes an MPLS label onto it, which places it into a forwarding equivalence class (FEC) and determines its handling and destination through the MPLS tunnel. The egress provider edge switch (the exit point from the MPLS tunnel) pops the MPLS label off of the outgoing packet.

MPLS traffic is bidirectional. So each provider edge switch is both an ingress switch and an egress switch, depending on the direction of the traffic.

EX Series switches can handle only single-label MPLS packets. If the packet has an existing MPLS label, the provider edge switch removes the label and swaps it for another MPLS label.

MPLS Protocol and Label Switched Paths

Each provider edge switch must be configured to support the MPLS protocol, and the MPLS stanza must include the configuration of a label switched path (LSP) that specifies the address of the remote provider edge switch.

JUNOS MPLS for EX Series switches supports RSVP-based LSPs.

Circuit Cross-Connect

You must configure the customer-edge interfaces of the provider edge switches as a circuit cross-connect (CCC), creating a transparent connection between two circuits. When you configure an interface as a CCC, the interface no longer belongs to a default VLAN. The interface becomes an MPLS tunnel, used exclusively for MPLS packets. You can create different CCCs for different customers or for segregating different traffic streams over different MPLS tunnels.

Using CCC, you can connect the following types of circuits:

- Local interface with remote interface or VLAN
- Local VLAN with remote interface or VLAN

NOTE: To configure a VLAN circuit as a CCC, you must enable VLAN tagging and specify a VLAN ID.

MPLS on EX Series switches does not support the following types of CCC configurations:

- Aggregated Ethernet interface (LAG)
- Q-in-Q tunneling
- Routed VLAN interface (RVI)
- Beginning and end of the CCC on the same switch

Provider Switch

You must configure one or more provider switches as transit switches within the network to support the forwarding of MPLS packets. You can add provider switches without changing the configuration of the provider edge switches.

A provider switch does not analyze the packets. It refers to an MPLS label forwarding table and swaps one label for another. The new label determines the next hop along the MPLS tunnel. A provider switch cannot perform the push or pop operations.

Components Required for All Switches in the MPLS Network

You must configure the following components on both the provider edge and the provider switches:

- OSPF Routing Protocol on page 2
- Traffic Engineering on page 3
- MPLS Protocol on page 3
- RSVP on page 3

OSPF Routing Protocol

MPLS works in coordination with the interior gateway protocol (IGP). Therefore, you must configure OSPF as the routing protocol on the loopback interface and core interfaces of both the provider edge and provider switches.

These core interfaces can be either Gigabit Ethernet or 10-Gigabit Ethernet interfaces, and they can be configured as either individual interfaces or aggregated Ethernet interfaces.

NOTE: These core interfaces cannot be configured with VLAN tagging or a VLAN ID. When you configure them to belong to family mpls, they are removed from the default VLAN. They operate as an exclusive tunnel for MPLS traffic.

Traffic Engineering

Traffic engineering maps traffic flows onto an existing physical topology and provides the ability to move traffic flow away from the shortest path selected by the IGP and onto a potentially less congested physical path across a network.

Traffic engineering enables the selection of specific end-to-end paths to send given types of traffic through your network. In order for MPLS to work properly, you must enable traffic engineering for the specified routing protocol (OSPF).

MPLS Protocol

You must enable the MPLS protocol on all switches that participate in the MPLS network and apply it to the core interface addresses of both the provider edge and provider switches. You do not need to apply it to the loopback address, because the MPLS protocol uses the framework established by the RSVP session to create LSPs. On the provider edge switches, the configuration of the MPLS protocol must also include the definition of an LSP.

RSVP

Resource Reservation Protocol (RSVP) is a signaling protocol that allocates and distributes labels throughout an MPLS network. RSVP sets up unidirectional paths between the ingress provider edge switch and the egress provider edge switch. RSVP makes the LSPs dynamic; it can detect topology changes and outages and establish new LSPs to move around a failure.

You must enable RSVP and apply it to the loopback address and the core interface addresses of both the provider edge and provider switches. The path message contains the configured information about the resources required for the LSP to be established.

When the egress switch receives the path message, it sends a reservation message back to the ingress switch. This reservation message is passed along from switch to switch along the same path as the original path message. Once the ingress switch receives this reservation message, an RSVP path is established.

The established LSP stays active as long as the RSVP session remains active. RSVP continues activity through the transmissions and responses to RSVP path and reservation messages. If the messages stop for three minutes, the RSVP session terminates and the LSP is lost.

RSVP runs as a separate software process in the Juniper Networks JUNOS Software and is not in the packet forwarding path.

Family MPLS

You must also configure the core interface addresses used for MPLS traffic to belong to family mpls.

NOTE: You can enable family mpls on either individual interfaces or aggregated Ethernet interfaces. You cannot enable it on tagged VLAN interfaces.

Related Topics

- JUNOS MPLS for EX Series Switches Overview
- Understanding MPLS and Path Protection on EX Series Switches
- Example: Configuring MPLS on EX Series Switches
- Configuring MPLS on Provider Edge Switches (CLI Procedure)
- Configuring MPLS on Provider Switches (CLI Procedure)
- Configuring Path Protection in an MPLS Network (CLI Procedure)
- *JUNOS Software MPLS Applications Configuration Guide* at http://www.juniper.net/techpubs/software/junos/junos95/index.html
- *JUNOS Software VPNs Configuration Guide* at http://www.juniper.net/techpubs/software/junos/junos95/index.html

Published: 2009-11-18