

Chapter 22

Layer 2 Circuit Overview

A Layer 2 circuit is a point-to-point Layer 2 connection transported by means of Multiprotocol Label Switching (MPLS) or another tunneling technology on the service provider's network. A Layer 2 circuit is similar to a circuit cross-connect (CCC), except that multiple Layer 2 circuits can be transported over a single label-switched path (LSP) tunnel between two provider edge (PE) routers. In contrast, each CCC requires a dedicated LSP.

This chapter discusses the following topics:

Layer 2 Circuit Overview on page 454

Layer 2 Circuit Standards on page 454

Layer 2 Circuit Policy on page 455

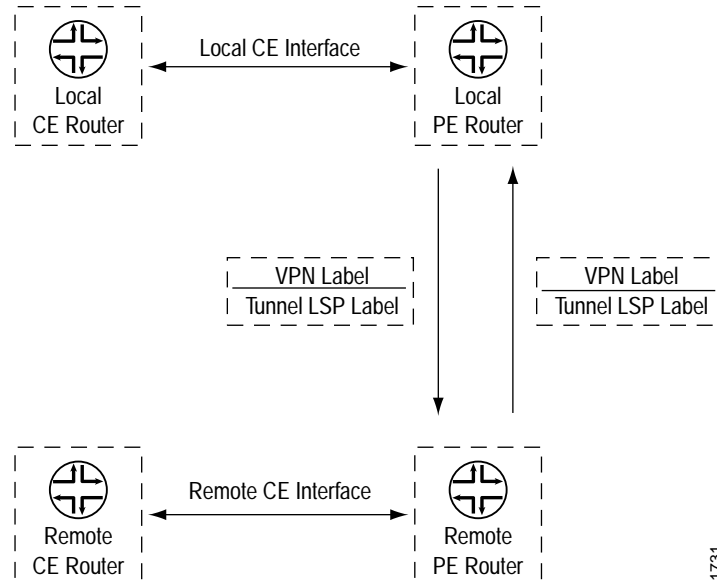
Layer 2 Circuit Bandwidth Accounting and Call Admission Control on page 455

Layer 2 Circuits Trunk Mode on page 458

Layer 2 Circuit Overview

The JUNOS software implementation of Layer 2 circuits supports only the remote form of a Layer 2 circuit; that is, a connection from a local customer edge (CE) router to a remote CE router. Figure 48 illustrates the components of a Layer 2 circuit.

Figure 48: Components of a Layer 2 Circuit



The interfaces shown in Figure 48 are logical interfaces. Packets are sent to the remote CE router by means of an egress virtual private network (VPN) label advertised by the remote PE router. The VPN label transits over either a Resource Reservation Protocol (RSVP) or a Label Distribution Protocol (LDP) LSP (or other type) tunnel to the remote PE router connected to the remote CE router. If you configure RSVP for Layer 2 circuits, you must also configure LDP.

Return traffic sent from the remote CE router to the local CE router uses an ingress VPN label advertised by the local PE router, which again transits over an RSVP and LDP LSP to the local PE router from the remote PE router. LDP is the signaling protocol used for advertising VPN labels.

Layer 2 Circuit Standards

For more information on Layer 2 circuits, see *Transport of Layer 2 Frames Over MPLS*, Internet draft draft-martini-l2circuit-trans-mpls-14.txt. This draft is available on the IETF Web site at <http://www.ietf.org/>.

Layer 2 Circuit Policy

You can configure JUNOS software routing policies to control the flow of packets over Layer 2 circuits. This capability allows you to provide different levels of service over a set of equal-cost Layer 2 circuits. For example, you can configure a circuit for high-priority traffic, a circuit for average-priority traffic, and a circuit for low-priority traffic. By configuring Layer 2 circuit policies, you can ensure that higher-value traffic has a greater likelihood of reaching its destination.

Layer 2 Circuit Bandwidth Accounting and Call Admission Control

The sections that follow discuss Layer 2 circuit bandwidth accounting and call admission control (CAC):

Bandwidth Accounting and Call Admission Control Overview on page 455

Selecting an LSP Based on the Bandwidth Constraint on page 456

LSP Path Protection and CAC on page 456

For information on how to configure bandwidth accounting and CAC for Layer 2 circuits, see “Configuring Bandwidth Allocation and Call Admission Control” on page 472.

Bandwidth Accounting and Call Admission Control Overview

Some network environments require that a certain level of service be guaranteed across the entire length of a path transiting a service provider’s network. For Layer 2 circuits transiting an MPLS core network, a customer requirement might be to assure that guarantees for bandwidth and class of service (CoS) be maintained across the core network. For example, an Asynchronous Transfer Mode (ATM) circuit can provide service guarantees for each traffic class. A Layer 2 circuit configured to transport that ATM circuit across the network could be expected to provide the same service guarantees.

Providing this type of service guarantee requires the following:

The LSPs in the MPLS core network must be able to provide service guarantees for bandwidth, rerouting, and route failures. You accomplish these guarantees by configuring multiclass LSPs. For more information on multiclass LSPs, see the *JUNOS MPLS Applications Configuration Guide*.

The service guarantee must be maintained across the entire length of the link as it transits the service provider’s network. Different Layer 2 circuits could have different bandwidth requirements. However, many Layer 2 circuits could be transported over the same E-LSP in the MPLS core network.

CAC ensures that the LSP has sufficient bandwidth to accommodate the Layer 2 circuit. If there is not enough bandwidth over a particular LSP, the Layer 2 circuit is prevented from using that LSP.

Selecting an LSP Based on the Bandwidth Constraint

CAC of Layer 2 circuits is based on the bandwidth constraint. You must configure this constraint for each Layer 2 circuit interface. If there is a bandwidth constraint configured for a Layer 2 circuit, CAC bases the final selection of which LSP-forwarding next hop to use on the following:

If multiple LSPs meet the bandwidth requirements, the first LSP found that can satisfy the bandwidth requirements for the Layer 2 circuit is selected.

If there is more than one next hop mapped to the same LSP, then all the next hops that map to that LSP and pass CAC constraints are installed. This allows the Layer 2 circuit routes to restore themselves quickly in case of failure.

The available bandwidth on the selected LSP is decremented by the bandwidth required for each Layer 2 circuit. Similarly, when the Layer 2 circuit route is changed or deleted (for example, when the route is disassociated from that particular LSP), the bandwidth on the corresponding LSP is incremented.

There are no priorities among different Layer 2 circuits competing for the same LSP next hop in the core network.

When an LSP's bandwidth changes, the Layer 2 circuits using that LSP repeat the CAC process again.

If the LSP bandwidth increases, some Layer 2 circuits that were not established might now successfully resolve over the LSP. Similarly, if the bandwidth of the LSP decreases, some Layer 2 circuits that were previously up might now be declared down because of insufficient bandwidth on the LSP.

When no LSP is found to meet the bandwidth requirements of the Layer 2 circuit, it is considered to be a CAC failure, and an error is reported.

LSP Path Protection and CAC

CAC can take into account LSPs that have been configured with an MPLS path protection feature, such as secondary paths, fast reroute, or node and link protection. CAC can consider the bandwidth available on these auxiliary links and can accept the backup connection as valid if the main connection fails. However, there are limitations on how the path protection feature must be configured to prevent CAC from taking down the Layer 2 circuit when the LSP it is using is switched to a backup route.

For more information on MPLS path protection features, see the *JUNOS MPLS Applications Configuration Guide*.

The sections that follow discuss the path protection features that can be used in conjunction with CAC and how they must be configured:

Secondary Paths and CAC on page 457

Fast Reroute and CAC on page 457

Link and Node Protection and CAC on page 457

Secondary Paths and CAC

The following describes the ways in which secondary paths would interact with Layer 2 circuit CAC:

If an LSP is configured with both primary and secondary paths, if the paths have the same bandwidth, and if this bandwidth is enough to accommodate the Layer 2 circuit, the Layer 2 circuit route installs both next hops in the forwarding table.

CAC allows the Layer 2 circuit to be switched to the secondary path if the primary path fails.

If the LSP has primary and secondary paths configured with different bandwidths, each path must run through CAC independently. If the active path for that LSP passes CAC constraints successfully, then that next hop is installed and the corresponding LSP is selected to transport the Layer 2 circuit traffic. The LSP's secondary paths are then checked for CAC, and installed if there is sufficient bandwidth.

However, if the active path for the LSP fails to meet the CAC constraints, then that LSP is not selected and the system looks for a different LSP to transport the Layer 2 circuit.

For example, an LSP has an active primary path with 30 megabits of bandwidth and a secondary path with 10 megabits of bandwidth. The Layer 2 circuit requires 15 megabits of bandwidth. The secondary path fails CAC, and only the next hop corresponding to the primary path is installed for the Layer 2 circuit route. The path protection originally provided by the secondary path is no longer available.

Fast Reroute and CAC

No CAC is done for fast reroute detours. However, as long as the protected path satisfies the CAC bandwidth constraints, the detour next hop is also selected and installed.

Link and Node Protection and CAC

CAC cannot select or install the bypass route for a bandwidth-constrained Layer 2 circuit using an LSP that has link and node protection configured. Link and node protection is not available for these routes. If the protected LSP path goes down, even if the LSP switches to the bypass, CAC no longer uses that path for the Layer 2 circuit route. CAC reevaluates the Layer 2 circuit route and updates it either to use a different LSP or, if no LSP with sufficient bandwidth is found, the Layer 2 circuit is taken down and an error is reported.

Layer 2 Circuits Trunk Mode

Using Layer 2 circuit trunk mode, you can configure Layer 2 circuits to carry ATM trunks, providing a way to link ATM switches over an MPLS core network.

Layer 2 circuit trunk mode allows you to configure the following CoS features:

CoS queues in Layer 2 circuit trunk mode—For ATM2 IQ interfaces, you can configure ATM CoS queues for Layer 2 circuit trunk mode.

Layer 2 circuit trunk mode scheduling—For ATM2 IQ interfaces configured to use Layer 2 circuit trunk mode, you can share a scheduler among 32 trunks on an ATM port.

Two early packet discard (EPD) thresholds per queue—For ATM2 IQ interfaces configured to use Layer 2 circuit trunk mode, you can set two EPD thresholds that depend on the packet-loss priorities (PLPs) of the packets.

For a detailed overview and configuration documentation, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.