Configuring ATM MPLS and VPN

This chapter describes Multiprotocol Label Switching (MPLS) and Virtual Private Network (VPN) features used with the Route Processor Module (RPM-PR) in the MGX 8850 and MGX 8950 switch and covers the following topics:

- MPLS Overview
- Configuring MPLS for MGX 8850 and MGX 8950
- VPN Overview
- How VPNs Work
- Configuring a VPN
- Support for LDP
- Support for Multi-VC on the RPM-PR
- LSC Redundancy
- Multiprotocol Label Switching (MPLS) over ATM using VC Merge

This chapter focuses solely on configuring the RPM-PR for cell-based ATM MPLS as an Edge Label Switch Router (ELSR) on the MGX 8850 Release 2 shelf and as a Label Switch Controller (LSC) on both the MGX 8850 and MGX 8950 shelf.

Note

In the MGX 8950, the RPM-PR supports only the MPLS Label Switch Controller (LSC) functionality.

For information on MPLS, refer to the *Cisco MPLS Controller Software Configuration Guide*. For MPLS and VPN commands, refer to the *Cisco MPLS VPN Feature Guide*.

MPLS Overview

This section describes MPLS and the role of the RPM-PR as an ELSR within the MGX 8850 switch or as an LSC within MGX 8850 and MGX 8950 switches.

The labels used to forward packets are negotiated using Label Distribution Protocol (LDP) or Tag Distribution Protocol (TDP). In this context, the RPM-PR functions as an Edge LSR to receive and label IP packets.

There are two different modes of MPLS operation.

- Frame-based
ATM cell-based.
The RPM-PR supports both of them. This chapter focuses on ATM cell-based MPLS operations with the RPM-PR.

ATM MPLS

Numerous VCs, known as MPLS Label Virtual Circuits (LVCs) are used to connect a pair of ATM MPLS devices. The LVCs are established under the direct control of MPLS signaling, and each LVC corresponds to a distinct MPLS label value.

MGX 8850 and MGX 8950 supports the Label Switch Controller (LSC) function that enables you to set up LVCs directly on ATM interfaces within an ATM switch.

The RPM supports MPLS VPNs. In MPLS VPN operation, the RPM-PR will act as a Provider Edge (PE) router. PE router function is a combination of the MPLS Edge LSR function and the use of the Border Gateway Protocol (BGP) v4 with Multiprotocol Extensions to carry routing information for the VPNs.

MPLS in the MGX 8850 or MGX 8950 Switch

On the MGX 8850 and MGX 8950 platform, MPLS provides an IP solution without the cost of Layer 2 management. In contrast to IP over ATM, MPLS reduces the customer’s network management and operational costs. Also, MPLS provides the same level of privacy as does Frame Relay or ATM.

For a description of how the RPM-PR acts as an Edge LSR to support MPLS feeder functionality in the MGX 8850, see the “System Block Diagram,” on page 7-3.

Features

The RPM-PR supports the following features:

- RPM-PR switch interface can support 3774 PVCs, 3777 LVCs, and 255 PVPs.
- ATM MPLS support without the use of PVPs.
- LSC functionality in the RPM-PR on both the MGX 8850 and MGX 8950 shelf.
- Edge LSR functionality in the RPM-PR on the MGX 8850 shelf.
- Ability to have up to two RPM-PRs acting as LSCs and multiple RPM-PRs acting as an ELSR on the same MGX 8850 shelf.
- Ability to run MPLS traffic over a PVC between RPM-PR Edge LSRs or between an RPM-PR and routers such as the Cisco 7500, configured as an external ELSR.
- Ability to run MPLS traffic over a PVP between RPM-PR Edge LSRs or from an RPM-PR Edge LSR to an MGX 8850 or MGX 8950 switch with an LSC.
- Ability to run frame-based MPLS traffic over the RPM-PR Ethernet and Fast Ethernet port adaptor ports, as well as ATM point-to-point subinterfaces.
- Ability to support ~2000 Interface Descriptor Blocks (IDBs).

Note

If an interface does not contain any sub-interfaces, then it constitutes one sub-interface for the purpose of this limit.
- MPLS PVC or PVP connections limits that fall within the established connection limits for the software release.

These connection limits stem from the MGX 8850 and MGX 8950 platforms, and not the MPLS feature. However, if the platform imposes the limit, the MPLS feature does not support any capacity beyond them.

- MPLS VPN feature.

- 1:N redundancy based on RPM-PR changeovers or dual-homing of CPE to two active RPM-PRs.

- Protocol support provided by IGP-OSPF, RIP, EIGRP, IS-IS.

- VPN addition provided by BGP, RIPv2, OSPF, and static routes for PE–CE links.

**System Block Diagram**

In the system block diagram (see Figure 7-1), an edge LSR connected to an MGX 8850 Release 1 using a PVP connection can also be connected to a Label Switch Controlled MGX 8850 Release 2.1. This ELSR is referred to as ELSR A in the diagram and in subsequent text. The ELSR and the LSC cannot coexist on the same RPM. The system block diagram shows an LSC and ELSR coexisting on an MGX 8850 Release 2. This ELSR is referred to as ELSR B in the diagram and in subsequent text.

*Figure 7-1  MGX 8850s with ELSR and LSC Configured RPMs*
MPLS Class of Service Support

This section discusses the mapping of the MPLS Class of Service (CoS) to the service class templates (SCT). The SCT is part of the VSI slave task, and is responsible for providing “default” VC parameters and “default” CoS Buffer parameters to other modules in VSI slave. SCT is used in setting up the cross-connect on the PXM-45 but is not used in programming the RPM-PR. SCTs are created from SCT configuration files downloaded from PXM-45 disk. The file is configurable to the user through Cisco WAN Manager (CWM) when it is available.

Service class templates 4 or 5 need to be loaded on the AXSM card and SCT 3 on the AXSM-E card before you can configure the MGX 8850 or MGX 8950 for MPLS support.

Configuring MPLS for MGX 8850 and MGX 8950

This section describes procedures needed to configure the RPM-PR, the PXM-45, and AXSM cards to support MPLS on the MGX 8850 and MGX 8950 switches.

To support MPLS, you need to

- Add an MPLS controller to the PXM-45
- Add and Partition an AXSM port for MPLS
- Map the AXSM port to an XTagATM Interface on the LSC
- Connect MPLS services between PXM-45 and PXM1
- Configure an RPM as an Edge Label Switch Router

Adding an MPLS Controller to the PXM-45

The first task in establishing MPLS services with the RPM-PR is to add an MPLS controller on the PXM-45. This is similar to adding the PNNI controller to the PXM-45. (See Chapter 6.) To add the MPLS controller, follow these steps.

Step 1  Access the switch CLI and enter the addcontroller command.

```
MGX8850.7.PXM.a>addcontroller <cntrlrId> i <cntrlrType> <slot> [cntrlrName]
```

Parameter | Description
---|---
`cntrlrId` | Range is from 1 through 20. 1 is reserved for PAR, 2 is reserved for PNNI, and 3 is reserved for LSC.
`i` | Internal
`cntrlrType` | 1 is reserved for PAR, 2 is reserved for PNNI, and 3 is reserved for LSC.
`slot` | RPM-PR slot, 1 through 16.
`cntrlrName` | An optional field that specifies the name of the controller.

For example:

```
MGX8850.7.PXM.a>addcontroller 5 i 3 5 LSC1
```
Configuring ATM MPLS and VPN

Chapter 7 Configuring ATM MPLS and VPN

Cisco MGX Route Processor Module (RPM-PR) Installation and Configuration Guide

Release 2.1, Part Number 78-12510-02 Rev. C1, August 31, 2004

7-5

Configuring MPLS for MGX 8850 and MGX 8950

cntrlrId = 5
i = internal
cntrlrType = 3 for LSC
slot = RPM-PR inserted in slot 5
cntrlrName = LSC1

Step 2 Enter the cc command to change to the RPM card, then configure the RPM as an LSC by entering the commands shown in this example:

```
RPM-PR> enable
Password: 
RPM-PR# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RPM-PR(config)# ip cef
RPM-PR(config)# interface loopback0
RPM-PR(config-if)# ip address 28.28.28.28 255.255.255.255
RPM-PR(config-if)# interface switch1
RPM-PR(config-if)# no ip address
RPM-PR(config-if)# tag-control-protocol vsi id 5
RPM-PR(config-if)# switch partition vcc 2 5
RPM-PR(config-if-swpart)# ingress-percentage-bandwidth 0 100
RPM-PR(config-if-swpart)# egress-percentage-bandwidth 0 100
RPM-PR(config-if-swpart)# vpi 0 0
RPM-PR(config-if-swpart)# vci 32 3808
```

Note The VSI Controller ID must match the addcontroller command ID entered in the previous step.

Adding and Partitioning an AXSM NNI Port for MPLS

Next, follow these steps to add and then partition a NNI port on an AXSM card for MPLS.

Step 1 Enter the cc command to change to an AXSM card.

```
MGX8850.7.a> cc 1
```

Step 2 Enter the cnfcdsct command as shown in the following example, to configure the AXSM card service class template (SCT) for PNNI and MPLS.

```
MGX8850.1.AXSM.a> cnfcdsct 4
```

Note 4 = policing on and 5 = policing off (for ATM Forum service types)

Step 3 Bring up the line where you want to add the port by entering the upln command.

```
MGX8850.1.AXSM.a> upln 1.1
```

Step 4 Enter the addport command to add the port.

```
addport <ifNum> <bay.line> <guaranteedRate> <maxRate> <sctID> <ifType> [vpiNum]
```

---

---
Configuring ATM MPLS and VPN

### Chapter 7

**Configuring MPLS for MGX 8850 and MGX 8950**

**Step 5**

Enter the `addpart` command to partition the port you have just added.

```
addpart <ifNum> <partId> <cntlrId> <egrminbw> <egrmaxbw> <ingminbw> <ingmaxbw> <minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifNum</td>
<td>A number between 1 and 60.</td>
</tr>
<tr>
<td>partId</td>
<td>Partition identifier; a number from 1 through 5.</td>
</tr>
<tr>
<td>cntlrId</td>
<td>Controller identifier; a number from 1 through 20. 1 is reserved for PAR, 2 is reserved for PNNI, and 3 is reserved for LSC.</td>
</tr>
<tr>
<td>egrminbw</td>
<td>Egress guaranteed % bandwidth in units of 0.0001% of interface bandwidth.</td>
</tr>
<tr>
<td>egrmaxbw</td>
<td>Egress maximum % bandwidth in units of 0.0001% of interface bandwidth.</td>
</tr>
<tr>
<td>ingminbw</td>
<td>Ingress guaranteed % bandwidth in units of 0.0001% of interface bandwidth.</td>
</tr>
<tr>
<td>ingmaxbw</td>
<td>Ingress maximum % bandwidth in units of 0.0001% of interface bandwidth.</td>
</tr>
<tr>
<td>minVpi</td>
<td>Minimum VPI value, which is a number between 0 and 4095. (0 to 255 for UNI interface)</td>
</tr>
<tr>
<td>maxVpi</td>
<td>Maximum VPI value, which is a number between 0 and 4095. (0 to 255 for UNI interface)</td>
</tr>
<tr>
<td>minVci</td>
<td>Minimum VCI value, which is a number between 32 and 65535.</td>
</tr>
<tr>
<td>maxVci</td>
<td>Maximum VCI value, which is a number between 32 and 65535.</td>
</tr>
</tbody>
</table>

**Note**

`<guaranteedRate>` must equal `<maxRate>`

For example,

```
MGX8850.1.AXSM.a>addport 1.1 353207 353207 4 2
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifNum</td>
<td>A number between 1 and 60.</td>
</tr>
</tbody>
</table>
| bay.line  | Port location designating back card bay; 1 for top and 2 for bottom.  
line is back card specific. |
| guaranteedRate | Virtual rates in cells per second. |
| maxRate   | Maximum rate depends on connection, as follows:  
OC48—between 50 and 5651320  
OC12—between 50 and 1412830  
OC3—between 50 and 353207  
T3—between 50 and 96000(PLCP), 104268(ADM)  
E3—between 50 and 80000 |
| sctID     | Port SCT ID, between 0 and 255. For default file use 0. |
| ifType    | 1 for uni; 2 for nni; 3 for vnni |
| vpiNum    | Used for configuring interface as virtual trunk, between 1 and 4095. |
Configuring MPLS for MGX 8850 and MGX 8950

Parameter | Description
---|---
minConns | Guaranteed number of connections, which is a number between 0 and the maximum number of connections in portgroup (see dspcd for portgroup information.)
maxConns | Maximum number of connections, which is a number between 0 and the maximum number of connections in portgroup (see dspcd for portgroup information.)

For example,

MGX8850.1.AXSM.a>`addpart 1 2 5 500000 500000 500000 500000 0 1500 32 65535 4000 4000

**Step 6** Enter the `dspparts` command to view the newly-added partition and verify its settings.

MGX8850.1.AXSM.a > dspparts

<table>
<thead>
<tr>
<th>Num</th>
<th>ID</th>
<th>ID</th>
<th>GuarBw</th>
<th>MaxBw</th>
<th>GuarBw</th>
<th>MaxBw</th>
<th>vpi</th>
<th>vpi</th>
<th>vci</th>
<th>vci</th>
<th>conn</th>
<th>conn</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>500000</td>
<td>500000</td>
<td>500000</td>
<td>500000</td>
<td>0</td>
<td>1500</td>
<td>32</td>
<td>65535</td>
<td>4000</td>
</tr>
</tbody>
</table>

Mapping an AXSM Port to an XTagATM Interface on the LSC

Enter the following commands into the RPM to map the AXSM ports created in the previous procedure to this LSC.

**Step 1** Enter the `cc` command to switch to the RPM card.

**Step 2** Enter `enable` and your password.

RPMLSC>enable
Password:

**Step 3** Enter `config t` to enter global configuration mode.

RPMLSC#config t

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Enter the `interface XTagATM`, `ip`, `extended-port`, and `mpls` commands to map connections to AXSM ports, as shown in the following example for AXSM ports 1.1 and 1.4.

RPMLSC(config)#interface XTagATM111
RPMLSC(config-if)#ip unnumbered Loopback0
RPMLSC(config-if)#extended-port Switch1 descriptor "1:1.1:1"
RPMLSC(config-if)#ip unnumbered Loopback0
RPMLSC(config-if)#extended-port Switch1 descriptor "1:1.4:4"

where descriptor format is x:y.y:z
  x = slot where AXSM is
  y.y = line 
  z = port # (this is a logical port)

RPMLSC(config-if)# mpls ip

**Step 5** Enter the `interface XTagATM`, `ip`, `extended-port`, and `mpls` commands for the Edge Label Switch Router, as shown in the following example.
Chapter 7 Configuring ATM MPLS and VPN

Configuring MPLS for MGX 8850 and MGX 8950

NY_9(config)#interface XTagATM41
NY_9(config-if)#ip unnumbered loopback0
NY_9(config-if)#extended-port Switch1 descriptor “4.1”
NY_9(config-if)#mpls ip

Note
The extended port switch 1 descriptor “4.1” identifies that the Xtag you created is bound to the VSI partition for an RPM in slot 4, and .1 designates the logical port. The RPM-PR has two logical ports. (“.1” is for VCCs and “.2” is for VPCs.) Therefore, all Xtags for the LER point to “<slot>.1”.

The extended port descriptor must contain a space between RPM and the port and must be in quotes.

Creating the VNNI Port on the AXSM Card

Next, create the VNNI port on the AXSM card residing on the PXM-45 shelf, by performing the following steps.

Step 1 Enter the cc command to go to an AXSM card.

Step 2 Enter the cnfcdsc 4 command to invoke the correct service class template.

Step 3 Enter the upln command to add a new line to the AXSM card.

Step 4 Enter the addport command to add the VNNI port as shown in this example.

addport <ifNum> <bay.line> <guaranteedRate> <maxRate> <sctID> <ifType>[vpiNum]

Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifNum</td>
<td>A number between 1 and 60.</td>
</tr>
<tr>
<td>bay.line</td>
<td>Port location designating back card bay; 1 for top and 2 for bottom. line is back card specific.</td>
</tr>
<tr>
<td>guaranteedRate</td>
<td>Virtual rates in cells/sec</td>
</tr>
<tr>
<td>maxRate</td>
<td>Maximum rate depends on connection, as follows:</td>
</tr>
<tr>
<td></td>
<td>OC48—between 50 and 5651320</td>
</tr>
<tr>
<td></td>
<td>OC12—between 50 and 1412830</td>
</tr>
<tr>
<td></td>
<td>OC3—between 50 and 353207</td>
</tr>
<tr>
<td></td>
<td>T3—between 50 and 96000(PLCP), 104268(ADM)</td>
</tr>
<tr>
<td></td>
<td>E3—between 50 and 80000</td>
</tr>
<tr>
<td>sctID</td>
<td>Port SCT ID, between 0 and 255. For default file use 0.</td>
</tr>
<tr>
<td>ifType</td>
<td>1 for uni; 2 for nni; 3 for vnni</td>
</tr>
<tr>
<td>vpiNum</td>
<td>Used for configuring interface as virtual trunk, between 1 and 4095.</td>
</tr>
</tbody>
</table>
Step 5

Enter the `addpart` command to apply the MPLS partition to the VNNI port.

```
MGX8850.1.AXSM.a> addport 12 1.2 353207 353207 4 3 11
```

```
MGX8850.1.AXSM.a> addpart addrscpnrn <ifNum> <partId> <cntlrId> <egrminbw> <egrmaxbw> <ingminbw> <ingmaxbw> <minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

For example,

```
MGX8850.1.AXSM.a> addport 12 1.2 353207 353207 4 3 11
```

### Parameter Description

- **ifNum**: A number between 1 and 60
- **partId**: Partition identifier; a number from 1 through 5.
- **cntlrId**: Controller identifier; a number from 1 through 20. 1 is reserved for PAR, 2 is reserved for PNNI, and 3 is reserved for LSC.
- **egrminbw**: Egress guaranteed % bandwidth in units of 0.0001% of interface bandwidth
- **egrmaxbw**: Egress maximum % bandwidth in units of 0.0001% of interface bandwidth
- **ingminbw**: Ingress guaranteed % bandwidth in units of 0.0001% of interface bandwidth
- **ingmaxbw**: Ingress maximum % bandwidth in units of 0.0001% of interface bandwidth
- **minVpi**: Minimum VPI value, which is a number between 0 and 4095 (0 to 255 for UNI interface)
- **maxVpi**: Maximum VPI value, which is number between 0 and 4095 (0 to 255 for UNI interface)
- **minVci**: Minimum VCI value, which is a number between 32 and 65535
- **maxVci**: Maximum VCI value, which is a number between 32 and 65535
- **minConns**: Guaranteed number of connections, which is a number between 0 and the maximum number of connections in portgroup (see `dspcd` for portgroup information.)
- **maxConns**: Maximum number of connections, which is a number between 0 and the maximum number of connections in portgroup (see `dspcd` for portgroup information.)

Step 6

Enter the `dspparts` command to view the MPLS partition on the VNNI port and verify that its settings are correct. For example,

```
MGX8850.1.AXSM.a> dspparts
```

```
if part Ctrl egr egr ingr ingr min max min max min max min max
Num ID ID GuarBw MaxBw GuarBw MaxBw vpi vpi vci vci conn conn
1 3 5 500000 500000 500000 500000 0 4095 32 65535 10000 10000
12 3 5 250000 250000 250000 250000 11 11 32 65535 10000 10000
```

Adding an XTagATM Interface on the LSC

Add an XTagATM interface on the Label Switch Controller for this VNNI port by performing the following steps.
Configuring an RPM-PR as an Edge Label Switch Router

To configure the RPM-PR as an Edge Label Switch Router (ELSR) on the MGX 8850 shelf as shown as ELSR A in Figure 7-1 on page 7-3, follow these steps.

Note
MGX 8950 does not support the RPM-PR configured as an ELSR.

Step 1
With the RPM-PR in the global configuration operating mode, enter the following commands.

   RPMELSR(config)#ip cef
   RPMELSR(config)#interface Loopback0
   RPMELSR(config-if)#ip address 192.168.2.11 255.255.255.255

Step 2
Enter the following commands at the global configuration level to configure the PNNI partition for the PVP.

   RPMELSR(config-if)#switch partition vcc 1 2
   RPMELSR(config-if)#ingress-percentage-bandwidth 50 100
   RPMELSR(config-if)#egress-percentage-bandwidth 50 100
   RPMELSR(config-if)#vpi 0 0
   RPMELSR(config-if)#vci 1601 3808
Chapter 7  Configuring ATM MPLS and VPN

Configuring MPLS for MGX 8850 and MGX 8950

Step 3  Enter the following commands to create a Virtual Path tunnel and configure Virtual Private Network (VPN) information.

```
RPMELSR(config)#interface Switch1.11 mpls
RPMELSR(config-if)#ip unnumbered Loopback0
RPMELSR(config-if)#no ip directed-broadcast
RPMELSR(config-if)#pvc 11/0
RPMELSR(config-if)#vbr-nrt 20000 20000
RPMELSR(config-if)#encapsulation aal5snap
RPMELSR(config-if)#mpls atm vp-tunnel 11
RPMELSR(config-if)#mpls ip
RPMELSR(config-if)#switch connection vpc 11 master remote
```

Step 4  Enter the following commands to configure VPN information into the ELSR and to add VPNs.

```
NY_9(config)#ip vrf vpn1
NY_9(config)#rd 65001:1
NY_9(config)#route-target export 65001:1
NY_9(config)#route-target import 65001:1
NY_9(config)#ip vrf vpn2
NY_9(config)#rd 65001:2
NY_9(config)#route-target export 65001:2
NY_9(config)#route-target import 65001:2
```

Configuring an Additional RPM-PR as an Edge Label Switch Router

You can also configure the RPM-PR as an Edge Label Switch Router (ELSR) on the MGX 8850 Release 2 shelf where you have installed the Label Switch Controller. This is shown in Figure 7-1 as ELSR B. Follow these steps to configure this function.

---

Step 1  With the RPM-PR in the global configuration operating mode, enter the following commands.

```
RPMELSR(config)#ip cef
RPMELSR(config)#interface Loopback0
RPMELSR(config-if)#ip address 192.168.3.11 255.255.255.255
```

Step 2  Enter the following commands to configure the MPLS partition.

```
RPMELSR(config)#int Switch1
RPMELSR(config-if)#switch partition vcc 2 5
RPMELSR(config-if)#ingress-percentage-bandwidth 50 100
RPMELSR(config-if)#egress-percentage-bandwidth 50 100
RPMELSR(config-if)#vpi 0 0
RPMELSR(config-if)#vci 32 1600
```

Step 3  Enter the following commands to create a Virtual Path tunnel.

```
RPMELSR(config)#interface Switch1.11 mpls
RPMELSR(config-if)#ip unnumbered Loopback0
RPMELSR(config-if)#no ip directed-broadcast
RPMELSR(config-if)#pvc 11/0
RPMELSR(config-if)#vbr-nrt 20000 20000
RPMELSR(config-if)#encapsulation aal5snap
RPMELSR(config-if)#mpls atm vp-tunnel 11
RPMELSR(config-if)#mpls ip
RPMELSR(config-if)#switch connection vpc 11 master remote
```

Step 4  Enter the following commands to configure VPN information into the ELSR and to add VPNs.
Virtual Private Networks (VPNs) provide the appearance, functions, and usefulness of a dedicated private network. The VPN feature for MPLS allows a Cisco IOS network to deploy scalable IPv4 Layer 3 VPN backbone service with private addressing, controlled access, and service-level guarantees between sites.

VPNs are supported by service provider networks over which labeled packets are forwarded from RPM Edge LSRs to other RPM Edge LSRs. A VPN service creates multiple private network environments within the public infrastructure. Service providers can use VPNs to target a given clientele and deliver individualized private network services to that clientele in a secure IP environment by using the public infrastructure.

**Requirements**

The requirements for an effective VPN are

- **Privacy**—All IP VPN services offer privacy over a shared (public) network infrastructure, the most well known solution of which is an encrypted tunnel. An IP VPN service must offer private addressing, where addresses within a customer private network do not need to be globally unique.

- **Scalability**—IP VPN services must scale to serve hundreds of thousands of sites and users. An IP VPN service should also serve as a management tool for service providers to control access to services, such as closed user groups for data and voice services. Controlled access places performance limits upon authorized programs, processes, or other systems in a network.

- **Flexibility**—IP VPN services must accommodate any-to-any traffic patterns and be able to accept new sites quickly, connect users over different media, and meet transport and bandwidth requirements of new intranet applications.

- **Predictable Performance**—Intranet applications supported by an IP an IP VPN service require different classes of service. The service level performance between customer sites must be guaranteed. Examples include widespread connectivity required by remote access for mobile users and sustained performance required by interactive intranet applications in branch offices.

**MPLS VPN Features**

Beyond the functions of an IP VPN, the VPN features for MPLS allow a Cisco IOS network to deploy the following scalable IPv4 Layer 3 VPN backbone services:

- **Connectionless Service**—MPLS VPNs are connectionless. They are less complex because they do not require tunnels or encryption to ensure network privacy.
Centralized Service—VPNs in Layer 3 privately connect users to intranet services and allow flexible delivery of customized services to the user group represented by a VPN. VPNS deliver IP services such as multicast, QoS, and telephony support within a VPN, and centralized services like content and web hosting. Combinations of services can be customized for individual customers.

Scalability—MPLS based VPNS use Layer 3 connectionless architecture and are highly scalable.

Security—MPLS VPNS provide the same security level as connection-based VPNS. Packets from one VPN cannot accidentally go to another VPN. At the edge of a provider network, incoming packets go to the correct VPN. On the backbone, VPN traffic remains separate.

Note Spoofing of a PER is nearly impossible because incoming packets are IP packets and must be received on an interface or subinterface uniquely identified with a VPN tag.

Easy to Create—MPLS VPNS are connectionless. It is easy to add sites to intranets and extranets and to form closed user groups. A given site can have multiple memberships.

Flexible Addressing—MPLS VPNS provide a public and private view of addresses, enabling customers to use their own unregistered or private addresses. Customers can freely communicate across a public IP network without network address translation (NAT).

Straightforward Migration—MPLS VPNS can be built over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks. There is no requirement to support MPLS on the customer edge (CE) router.

Supported Platforms

All Cisco routers, including the Cisco 3600 Series, the MGX 8850 series equipped with RPMs, and the Cisco 6400 Series, as well as several other devices, support VPNS. Any LSR-capable platform can serve in the backbone. In addition to devices already mentioned, the LS 1010 ATM Switch, 8540 MSR, and the BPX 8650 Switch also support VPNS. Non-MPLS capable ATM switches can also be used, as they can carry MPLS over PVCs or PVPs.

How VPNS Work

Each VPN is associated with one or more VPN routing/forwarding instances (VRFs), which defines a VPN at a customer site attached to a PE router. A VRF table consists of the following components.

- IP routing table
- Derived Cisco Express Forwarding table
- Set of interfaces that use the forwarding table
- Set of rules and routing protocol variables that determine what goes into the forwarding table

VPNS for MPLS

A customer site can be a member of multiple VPNS. However, a site can be associated with only one VRF. A customer site’s VRF contains all routes available to the site from the associated VPNS.
How VPNs Work

The IP routing table and CEF table for each VRF store packet forwarding information. (Together, these tables are analogous to the forwarding information base [FIB] used in MPLS.) A logically separate set of routing and CEF tables is constructed for each VRF. These tables prevent packets from being forwarded outside a VPN and prevent packets outside a VPN from being forwarded to a router within the VPN.

VPN Route-Target Communities and Export and Import Lists

The distribution of VPN routing information is controlled through the use of VPN route-target communities, implemented by Border Gateway Protocol (BGP) extended communities. Distribution works as follows:

- When a VPN route is injected into BGP, it is associated with a list of VPN route-target communities. This list is set through an export list associated with the VRF from which the route was learned.
- Associated with each VRF is an import list of route-target communities, which defines values to be verified by the VRF table before a route is deemed eligible for import into the VPN routing instance. For example, if a given VRF’s import list includes community-distinguishers A, B, and C, then any VPN route carrying A, B, or C is imported into the VRF.

iBGP Distribution of VPN Routing Information

A PER learns an IP prefix from a CE router through static configuration, a BGP session, RIP, or OSPF. The PER then generates a VPN-IPv4 (vpnv4) prefix by linking an 8-byte route distinguisher to the IP prefix. The VTN-IPv4 address uniquely identifies hosts within each VPN site, even if the site uses globally non-unique (unregistered private) IP addresses. The route distinguisher used to create the VTN-IPv4 prefix is specified by a configuration command on the PER.

BGP uses VTN-IPv4 addresses to distribute network reachability information for each VPN within a service provider network. In building and maintaining routing tables, BGP sends routing messages within (interior BGP or iBGP) or between IP domains (exterior BGP or eBGP).

BGP propagates vpnv4 information using BGP multiprotocol extensions for handling extended addresses. Refer to RFC 2283, *Multiprotocol Extensions for BGP-4*. BGP propagates reachability information (expressed as VTN-IPv4 addresses) among PE routers; reachability information for a given VPN is propagated only to members of that VPN. BGP multiprotocol extensions identify valid recipients of VPN routing information.

Label Forwarding

Based on the routing information stored in each VRF’s IP routing and CEF tables, MPLS uses extended VTN-IPv4 addresses to forward packets to their destinations.

To achieve this, an MPLS label is associated with each customer route. The PE router assigns the route originator’s label and directs data packets to the correct CE router. Tag forwarding across the provider backbone is based on dynamic IP paths or Traffic Engineered paths.

A customer data packet has two levels of labels attached when it is forwarded across the backbone.

- The top label directs the packet to the correct PE router.
- The second label indicates how that PE router should forward the packet.
The PE router associates each CE router with a forwarding table that contains only the set of routes that are available to that CE router.

### Examples of VPN Topologies

A VPN contains customer devices attached to CE routers. These customer devices use the VPN to exchange data. Only the PE routers are aware of the VPN.

An example of a VPN with a service provider (P) backbone network, service provider edge routers (PE), and CE routers is shown in Figure 7-2.

**Figure 7-2  VPN with a Service Provider (P) Backbone Network**

Three VPNs communicating with five customer sites are shown in Figure 7-3. Notice that sites 1, 3, and 4 are members of two VPNs.

**Figure 7-3  VPNs Communicate with Customer Sites**
Configuring a VPN

This section explains how to configure the RPM-PR for VPN operation. It begins by listing the prerequisites for VPN configuration, then gives the configuration steps.

Prerequisites for VPN Operation

The network must be running the following Cisco IOS services before you can configure VPN operation:

- CEF switching in every tag-enabled router
- MPLS connectivity among all provider edge (PE) routers with VPN service or MPLS in all provider backbone (P) routers
- MPLS with VPN code in all provider routers with a VPN edge service (PE) routers
- BGP in all routers providing a VPN service

Complete the following tasks before you configure VPN operation:

- Turn on Cisco Express Forwarding (CEF).
- Configure MPLS.
- Turn on BGP between provider routers for distribution of VPN routing information.

Configuring VPN Operation

This section describes how to configure routing protocols and create VRFs for a VPN. See the “MPLS Class of Service Support” section for the commands used in the tasks. Perform the following four tasks to configure and verify VPNs in your network:

1. Configure VRFs and associate interfaces with VRFs.
2. Configure BGP between provider routers for distribution of VPN routing information.
3. Configure import and export routes to control the distribution of routing information.
4. Verify VPN operation.

Configuring VRFs

To create a VRF, perform the following steps on the provider edge router.

Step 1

Enter VRF configuration mode and specify the VRF to which subsequent commands apply.

\[ \text{RPM(config)} \# \text{ip vrf vrf-name} \]

Step 2

Define the instance by assigning a name and an 8-byte route distinguisher.

\[ \text{RPM(config-vrf)} \# \text{rd route-distinguisher} \]

Step 3

Associate interfaces with the VRF.

\[ \text{RPM(config-if)} \# \text{ip vrf forwarding vrf-name} \]

Step 4

If BGP is used between the PE and a VRF CE, configure BGP parameters for the VRF CE session.

\[ \text{RPM(config-router)} \# \text{address-family ipv4 vrf name} \]
Chapter 7  Configuring ATM MPLS and VPN

Configuring a VPN

RPM(config-router-af)# aggregate-address
RPM(config-router-af)# auto-summary
RPM(config-router-af)# default-information originate
RPM(config-router-af)# default-metric ...
RPM(config-router-af)# distance ...
RPM(config-router-af)# distribute-list ...
RPM(config-router-af)# network ...
RPM(config-router-af)# neighbor ...
RPM(config-router-af)# redistribute ...
RPM(config-router-af)# synchronization
RPM(config-router-af)# table-map...

Note  To ensure that addresses learned from CE routers via BGP are properly treated as VPN IPv4 addresses on a PE router, enter the command no bgp default ipv4-activate before configuring any CE neighbors. See Step 2 and Step 3 in the next section, “Configuring BGP.”

Step 5  If RIP is used between the PE and VRF CEs, configure RIP parameters (in a VRF address-family submode).

Note  The default for auto-summary and synchronization in VRF address-family submode is off.

RPM(config-router)# address-family ipv4 vrf name
RPM(config-router-af)# auto-summary
RPM(config-router-af)# default-information originate
RPM(config-router-af)# default-metric ...
RPM(config-router-af)# distance ...
RPM(config-router-af)# network ...
RPM(config-router-af)# offset-list ...
RPM(config-router-af)# redistribute ...

Step 6  Exit from the address family config mode.
RPM(config-router-af)# exit-address-family

Step 7  Configure static routes for the VRF.
RPM(config)# ip route [vrf vrf-name] destination <interface> ip_address

Configuring BGP

To configure router address families, define sessions, and set global variables for routing protocols, perform the following steps with the PE router in configuration mode.

Step 1  Configure BGP address families.
RPM(config-router)# address-family {ipv4 | vpnv4}{unicast | multicast}

Step 2  Define BGP sessions.
RPM(config-router-af)# neighbor address | peer-group) remote-as as-number
RPM(config-router-af)# neighbor address | peer-group) update-source interface
RPM(config-router-af)# neighbor peer-group peer-group
RPM(config-router-af)# neighbor address peer-group peer-group
Step 3
Activate a BGP session by entering the `no bgp default ipv4-activate` command to prevent automatic advertisement of address family IPv4 for every neighbor.

This command is required on a PE that establishes BGP sessions with CE routers. To enable advertisement of IPv4 prefixes for a particular neighbor, enter address-family mode for IPv4 then enter the `neighbor...activate` command for the neighbor.

```
RPM(config-router)# no bgp default ipv4-activate
```

For a particular address family, enter `neighbor... activate`.

```
RPM(config-router-af)# [no] neighbor address | peer-group) activate
```

Step 4
Execute optional BGP global commands that affect all address families.

```
RPM(config-router)# bgp always-compare-med
RPM(config-router)# bgp bestpath ...
RPM(config-router)# bgp client-to-client reflection
RPM(config-router)# bgp cluster-id ...
RPM(config-router)# bgp confederation ...
RPM(config-router)# bgp default local-preference ...
RPM(config-router)# bgp deterministic-med ...
RPM(config-router)# bgp fast-external-fallover ...
RPM(config-router)# bgp log-neighbor-changes
RPM(config-router)# bgp redistribute-internal
RPM(config-router)# bgp router-id ...
RPM(config-router)# timers bgp ...
```

Step 5
Execute BGP configuration commands for address family IPv4.

All BGP configuration commands supported in previous versions of IOS are valid for address family IPv4 unicast. These commands affect either all IPv4 instances or the default IPv4 routing table. For backward compatibility, these commands can be entered in either router config mode or in address family mode for ipv4 unicast. See Step 3 for information on the command `no bgp default ipv4-activate`.

```
RPM(config-router)# bgp ...
```

Step 6
Execute BGP configuration commands for address family VPNv4.

```
RPM(config-router)# bgp dampening ...
RPM(config-router)# neighbor ...
RPM(config-router)# neighbor address | peer-group)activate
```

Step 7
To configure iBGP to exchange VPNv4 Network Layer Reachability Information (NLRI) (between PE router and route reflector or between PE routers), first define an iBGP BGP session.

```
Note

To ensure that VPN packets are properly tag forwarded between the PE routers, specify loopback addresses for the neighbor address and the update-source interface.
```

```
RPM(config-router)# neighbor address remote-as as-number
RPM(config-router)# neighbor address update-source interface
```

Step 8
Activate the advertisement of VPNv4 NLRI.

```
RPM(config-router)# address-family vpnv4
RPM(config-router-af)# neighbor address activate
```
Configure Import and Export Routes

To configure VRF route target extended communities and import route maps, perform the following steps with the PE router in configuration mode.

Step 1  Enter VRF configuration mode and specify a VRF.
        RPM(config)# ip vrf vrf-name

Step 2  Import routing information from the specified extended community.
        RPM(config-vrf)# route-target import community-distinguisher

Step 3  Export routing information to the specified extended community.
        RPM(config-vrf)# route-target export community-distinguisher

Step 4  Associate the specified route map with the VRF being configured.
        RPM(config-vrf)# import map route-map

Checking the VRFs

Perform the following steps to verify the VPN configuration.

Step 1  Display the set of defined VRFs and the interfaces associated with each one.
        RPM# show ip vrf

Step 2  Display detailed information about configured VRFs, including the import and export community lists.
        RPM# show ip vrf detail

Step 3  Display the IP routing table for VRF.
        RPM# show ip route vrf vrf-name

Step 4  Display the routing protocol information associated with a VRF.
        RPM# show ip protocols vrf vrf-name

Step 5  Display the CEF forwarding table associated with a VRF.
        RPM# show ip cef vrf vrf-name

Step 6  Display the VRF table associated with an interface. Use either of the following commands:
        RPM# show ip interface interface-number
        RPM# show cef interface interface-number

Step 7  Display VPNv4 NLRI information.
        The keyword all displays the entire database. The keyword rd displays NLRIIs that match the specified route distinguisher. The keyword vrf displays NLRIIs with the specified VRF. Add the keyword tags after any of the other keywords and arguments to list the tags distributed with the VPNv4 NLRIIs.
        RPM # show ip bgp vpnv4 all [tags]
        RPM # show ip bgp vpnv4 rd route-distinguisher [tags]
        RPM # show ip bgp vpnv4 vrf vrf-name [tags]
Step 8  Display tag forwarding entries that correspond to VRF routes advertised by this router.

RPM # show mpls forwarding vrf vrf-name [prefix mask/length] [detail]

Step 9  You can also use ping or traceroute.

RPM # ping vrf vpn 1.1.1.1

where 1.1.1.1 is the destination address

Step 10 Enter the following telnet command to check the VRFs.

telnet 1.1.1.1 /vrf vpn

---

Support for LDP

MPLS label distribution protocol (LDP) allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services. LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement Cisco's MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

LDP is a superset of the prestandard Tag Distribution Protocol (TDP) from Cisco, which also supports MPLS forwarding along normally routed paths. For those features that LDP and TDP share in common, the pattern of protocol exchanges between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages.

This release of the Cisco IOS, which supports both the LDP and TDP protocols, provides the means for transitioning an existing network from a TDP operating environment to an LDP operating environment. Thus, you can run LDP and TDP simultaneously on any given router platform. The routing protocol that you select can be configured on a per-interface basis for directly-connected neighbors and on a per-session basis for nondirectly connected (targeted) neighbors. In addition, LSP across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

For more information, including configuration tasks, transitioning a network from TDP to LDP, and command reference, refer to the Cisco IOS Release 12.2T “MPLS Label Distribution Protocol” documentation at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ldp_221t.htm#xtocid212130.

---

Note

There is no CWM support planned for LDP or TDP.
Support for Multi-VC on the RPM-PR

This feature enables support for initiation of multiple label switched paths (LSPs) per destination on the RPM. Different label switched paths are established for different class of services. This feature enables interface level queueing rather than per-vc level on the RPM based on MPLS class of service policy.

MPLS quality of service (QoS) functionality enables network administrators to satisfy a wide range of requirements in transmitting IP packets through an MPLS-enabled network. The three primary MPLS QoS offerings made available to customers are:

- Packet classification
- Congestion avoidance
- Congestion management


Note

There is no CWM support for Multi-LVC.

LSC Redundancy

Switches take time to reroute traffic when a failure occurs. Switch connection routing software, such as AutoRoute, PNNI, and MPLS, calculate routes and reprogram hardware for each connection. This enables router networks to reroute large aggregates of traffic more quickly than most connection-oriented networks.

Cisco LSC redundancy recognizes that the LSC is the single point of failure for an IP+ATM network. Whether an LSC is an external router such as the 7204 or an internal Routing Processor Module (RPM) in a BPX or MGX switch, an LSC is in the critical path for network reliability. If the LSC fails or if the LSC’s port adapter goes down, the ATM-LSR also goes down and the entire connected MPLS network loses connections. As a critical component of IP+ATM networks, label switch controllers must be robust, providing continued service despite equipment or software failures, and do so quickly.

LSC redundancy basically consists of

- Two controllers, such as two MPLS controllers
- Virtual Switch Interface (VSI)
- Equal-cost multipath IP routing

In essence, two independent MPLS controllers, via VSI, control separate partitions in the IP+ATM switch, creating a set of two identical subnetworks. Multipath IP routing chooses to use both subnetworks equally, leading to identical connections in both subnetworks. If a controller in one subnetwork fails, then multipath IP routing very quickly diverts traffic to the other subnetwork.

LSC redundancy differs from hot standby redundancy in that the LSCs do not need copies of each other’s internal state or database, thus increasing reliability. LSC redundancy is simpler than hot standby redundancy because it is not necessary to set up new connections when a controller fails. The LSC redundancy architecture requires the same amount of equipment as a network with hot standby controllers, except that the controllers act independently, rather than in hot standby mode.

For information on LSC redundancy, refer to the feature note, LSC Redundancy for IP + ATM Networks.
How the LSC, ATM Switch, and VSI Work Together

The LSC and slave ATM switch have the following characteristics:

- LSC runs all of the control protocols
- ATM switch forwards the data
- Each physical interface on the slave ATM switch maps to an XtagATM interface on the LSC. Each XtagATM interface has a dedicated LDP session with a corresponding interface on the edge. The XtagATM interfaces are mapped in the routing topology and the ATM switch behaves as a router.
- LSC can also function as an edge LSR. The data for the edge LSR passes through the control interface of the router.

If a component on the LSC fails, the ATM switch’s IP switching function is disabled. The stand-alone LSC is the single point of failure.

The VSI implementation includes the following characteristics:

- VSI allows multiple, independent control planes to control a switch. The VSI ensures that the control processes (SS7, MPLS, PNNI, and so on) can act independently of each other by using a VSI slave process to control the resources of the switch and apportion them to the correct control planes.
- In MPLS, each physical interface on the slave ATM switch maps to an XtagATM interface on the LSC through the VSI. In other words, physical interfaces are mapped to their respective logical interfaces.
- Routing protocol on the LSC generates route tables entries. The master sends connection requests and connection release requests to the slave.
- Slave sends the configured bandwidth parameters for the ATM switch interface to the master in the VSI messages. The master includes the bandwidth information in the link state topology. You can override these bandwidth values by manually configuring the bandwidth on the XtagATM interfaces.

Implementing LSC Redundancy

To make an LSC redundant, perform the following functions, which are described below:

- Partition the resources of the ATM switch
- Implement a parallel VSI model
- Add interface redundancy
- Implement hot LSC redundancy
- Implement warm LSC redundancy

Partitioning the Resources of the ATM Switch Interface

In the LSC redundancy model, two LSCs control different partitions of the ATM switch. When you partition the ATM switch for LSC redundancy, follow these guidelines:

- Make the MPLS partitions identical. If you create two partitions, make sure both partitions have the same amount of resources. (You can have two MPLS VSI partitions per switch.) Enter the `addpart` command to configure the partitions.
• If the partitions are on the same switch card, perform the following:
  – Create different control VCs for each partition.
    For example, there can be only one (0, 32) control VC on the XtagATM interface. To map two
    XtagATM interfaces on the same ATM switch interface, use a different control VC for the
    second LSC. Enter the `mpls atm control-vc` command.
  – Create the LVC on the XtagATM interfaces using nonintersecting VPI ranges.
    Enter the `mpls atm vpi` command.
• Specify the bandwidth information on the XtagATM interfaces. Normally, this information is read
  from the slave ATM switch. When you specify the bandwidth on the XtagATM interface, the value
  you enter takes precedence over the switch-configured interface bandwidth.
• Configure the logical channel number (LCN) ranges for each partition according to the expected
  number of connections.

Implementing the Parallel VSI Model

The parallel VSI model means that the physical interfaces on the ATM switch are shared by more than
one LSC. For example,
• LSC1 maps VSI slave interfaces 1 to N to the ATM switch’s physical interfaces 1 to N.
• LSC2 maps VSI slave interfaces 1 to N to the ATM switch’s physical interfaces 1 to N.
• LSC1 and LSC2 share the same physical interfaces on the ATM switch.
With this mapping, you achieve fully-meshed independent masters.

Figure 7-4 shows four ATM physical interfaces mapped as four XtagATM interfaces at LSC1 and LSC2.
Each LSC is not aware that the other LSC is mapped to the same interfaces. Both LSCs are active all the
time. The ATM switch runs the same VSI protocol on both partitions.

Figure 7-4  XtagATM Interfaces
Adding Interface Redundancy

To ensure reliability throughout the LSC redundant network, you can also implement:

- Redundant interfaces between the edge LSR and the ATM-LSR.
  Most edge LSRs are co-located with the LSCs. Creating redundant interfaces between the edge LSRs and the ATM LSRs reduces the chance of a disruption in network traffic by providing parallel paths.

- Redundant virtual trunks and VP tunnels between slave ATM switches.
  To ensure hot redundancy between the ATM switches, you can create redundant virtual trunks and VP tunnels. (See Figure 7-5.)

![Figure 7-5 Interface Redundancy](image)

Implementing Hot LSC Redundancy

Hot redundancy provides instant failover to the other path when an LSC fails. When you set up hot redundancy, both LSCs are active and have the same routing costs on both paths. To ensure that the routing costs are the same, run the same routing protocols on the redundant LSCs.

In hot redundancy, the LSCs run parallel and independent Label Distribution Protocols (LDPs). At the edge LSRs, when the LDP has multiple routes for the same destination, it requests multiple labels. It also requests multiple labels when it needs to support class of service (CoS). When one LSC fails, the labels distributed by that LSC are removed.

To achieve hot redundancy, you can implement these redundant components:

- Redundant physical interfaces between the edge LSR and the ATM-LSR to ensure reliability in case one physical interface fails.

- Redundant interfaces or redundant VP tunnels between the ATM switches.

- Slave AXSM or AXSM-E cards can have redundancy configured. If redundancy is configured, and the primary card fails, the secondary or redundant card takes over.

- Redundant LSCs.

- The same routing protocol running on both LSCs. (You can have different tag and label distribution protocols.)
Implementing Warm LSC Redundancy

Virtually any configuration of switches and LSCs that provides hot redundancy can also provide warm redundancy. You can also switch from warm to hot redundancy with little or no change to the links, switch configurations, or partitions.

To achieve warm redundancy, you need only redundant LSCs. You do not necessarily need to run the same routing protocols or distribution protocols on the LSCs.

Note

You can use different routing protocols on parallel LSCs. However, you do not get instant failover. The failover time includes the time it takes to reroute the traffic, plus the LDP bind request time. If the primary routing protocol fails, the secondary routing protocol finds new routes and creates new label virtual circuits (LVCs). An advantage to using different routing protocols is that the ATM switch uses fewer resources and offers more robust redundancy.

If you run the same routing protocols, you specify a higher cost for the interfaces on the backup LSC. This causes the data to use only the lower-cost path. This also saves resources on the ATM switch, because the edge LSR requests LVCs only through the lower-cost LSC. When the primary LSC fails, the edge LSR uses the backup LSC and creates new paths to the destination. Creating new paths requires rerouting time and LDP negotiation time.

Using LSC Redundancy in Dedicated LSC Mode

Normally, LSCs include edge LSR functionality. In the “dedicated” LSC mode, the LSC removes edge LSR functionality. In RPM-PR-based LSCs, the dedicated LSC mode of operation enables the LSC to be scaled. To achieve the edge LSR functionality, the LSC creates a label switch path (LSP) for each destination in the route table.

With LSC redundancy, if 400 destinations exist in the network, each redundant LSC adds 400 head-end VCs. In hot redundancy mode, 800 head-end VCs are created for the LSCs. If the LSCs are not edge LSRs, then 800 LVCs are wasted.

The number of LVCs increases as the number of redundant LSCs increases. In the case of a VC-merged system, the number of LVCs can be low. However, in non-VC-merged system, using the dedicated LSC mode is recommended.

Multiprotocol Label Switching (MPLS) over ATM using VC Merge

The virtual circuit (VC) merge facility allows a switch to aggregate multiple incoming flows with the same destination address into a single outgoing flow. Wherever VC merge occurs, several incoming labels are mapped to one single outgoing label. Cells from different virtual channel identifiers (VCIs) going to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections. This sharing of labels reduces the total number of VCs required for label switching.

Without VC merge, each path consumes one label VC on each interface along the path. VC merge reduces the label space shortage by sharing labels for different flows with the same destination. Therefore, VC-Merge connections are unidirectional, and furthermore, all merged connections must be of the same service type.
To support VC-merge, the ATM switch requires that AXSM cards allow multiple VC frames to be merged into a single VC without interleaving cells inside AAL5 frames. The RPM is the control point, where LSC resides.

VC Merge is enabled by default when the MPLS over ATM network is configured and is only used when the RPM is used as an LSC (Label Switch Controller). Because it is enabled by default, the only commands necessary are:

- `no tag-switching atm vc-merge` to disable VC Merge
- `tag-switching atm vc-merge` to enable VC Merge

For more information, see MPLS Label Switch Controller and Enhancements at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftlsc.htm#xtocid15