About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Connected Roadways System Cisco Validated Design

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1  System Overview  1-1
Connected Roadways  1-1
Policy Trends  1-3
USDoT Action Plan and Directives  1-3
European Commission Action Plan and Directives  1-3

CHAPTER 2  System Architecture  2-1
Roadside Network Design  2-2
Citywide MPLS Transport  2-3
Layer One  2-3
Layer Two  2-3
Transport Infrastructure  2-4
Unified MPLS  2-4

CHAPTER 3  Network Topology  3-1
MPLS Transport Network Model  3-1
Transport Network Model Roles  3-2
Transport Control Plane  3-2
Ethernet Access Network  3-3
Hub-and-Spoke Access Network  3-3
Per Node Active/Standby Multichassis Link Aggregation Groups  3-3
Per VLAN Active/Active Multichassis Link Aggregation Groups (Pseudo MC-LAG)  3-3
Ethernet Access Rings  3-4

CHAPTER 4  Service Infrastructure  4-1
L3VPN Services  4-2
Circuit Emulation Services  4-3
Service Control Plane  4-4
CHAPTER 5

System Components  5-1

CHAPTER 6

System Functional Considerations  6-1
  Multicast  6-1
  Quality of Service (QoS)  6-2
  Redundancy and High Availability  6-3
    Loop-Free Alternate Fast Reroute with BFD  6-3
    Microloop Avoidance in Remote LFA FRR  6-3
    BGP Fast Reroute (FRR) Edge Protection  6-4
    Pseudowire Redundancy  6-4
  Operations, Administration, and Maintenance (OAM)  6-4

CHAPTER 7

System Implementation  7-1
  Transport Network Implementation  7-1
    MPLS Transport Implementation  7-2
      MPLS Transport Gateway Configuration  7-2
      Pre-Aggregation Node Configuration  7-4
  Small Network Non-IP/MPLS Access Network Implementation  7-5
    Dual-homed Hub-and-Spoke Ethernet Access  7-5
      Per Node Active/Standby MC-LAG  7-5
      Per VLAN Active/Active MC-LAG (pseudo MC-LAG)  7-8
    Ethernet Access Rings  7-11
      Pre-Aggregation Node Configuration  7-11
      Ethernet Access Node Configuration  7-13
  L3VPN Service Implementation  7-13
    L3 MPLS VPN Service Model  7-13
      MPLS VPN Core Transport  7-14
      L3VPN over Hub-and-Spoke Access Topologies  7-17
      L3VPN over Ring Access Topologies  7-19
  Circuit Emulation Services Implementation  7-21
    CESoPSN VPWS from PAN to MTG  7-22
      Cisco ASR 903 Series Pre-Aggregation Node Configuration  7-22
    SAToP VPWS from PAN to MTG  7-24
      Cisco ASR 903 Series Pre-Aggregation Node Configuration  7-24
      Cisco ASR 9000 Series Mobile Transport Gateway Configuration  7-25
  Quality of Service Implementation  7-26
    CE QoS Configuration  7-27
      Class Maps  7-27
Contents

- NNI Classification for REP Ring Access 7-28
- REP Fiber Ring NNI QoS Policy Maps 7-29
- Pre-Aggregation Node QoS Configuration (Cisco ASR 903) 7-29
  - Class Maps 7-29
  - Fiber Ring UNI QoS Policy Maps 7-30
  - Fiber Access NNI QoS Policy Maps 7-31
  - Aggregation NNI QoS Policy Map 7-31
- Aggregation and Core Network QoS Configuration 7-31
  - Class Maps 7-31
  - NNI QoS Policy Maps 7-32
- MTG QoS Configuration 7-33
  - Ethernet UNI QoS Policy Maps 7-33
  - ATM UNI QoS Policy Maps 7-34
  - TDM UNI QoS Policy Map 7-35
- Multicast Services in Global Routing 7-35
  - MTG-9006-K1501 (Root-node/Ingress-PE) 7-35
  - Branch Node Configuration 7-36
  - AGN-9006-K1102 (Leaf-node/Egress-PE) 7-37
- High Availability Implementation 7-38
  - MPLS VPN-BGP FRR Edge Protection and VRRP 7-38
    - Mobile Transport Gateway 1 7-39
    - Mobile Transport Gateway 2 7-40
    - Core Route Reflector 7-41
    - Pre-Aggregation Node 7-41
  - Pseudowire Redundancy for TDM Services 7-42
    - TDM Services 7-42
- OAM Implementation 7-44
  - Service OAM Implementation for L3VPN 7-44
  - Service OAM Implementation for TDM Circuit Emulation 7-44
  - Transport OAM 7-45
  - IP SLA Configuration 7-45
    - IP SLA Responder Configuration on PAN 7-45
    - MPLS Transport Gateway Initiator Configuration for IP SLA 7-45

Chapter 8

Summary 8-1

Appendix A

Acronyms and Initialisms A-1
System Overview

This document defines a system architecture for Connected Roadways as part of the Cisco Connected Transportation System (CTS) portfolio. It includes design and best practice recommendations for a scalable and resilient multi-service transport infrastructure for any size and scale of deployment. Previous releases of CTS focused on Positive Train Control (PTC) in CTS 1.0, and Connected Rail in CTS 1.5.

The Connected Roadways System design is based on a proven architecture deployed by dozens of major service providers around the world: Unified MPLS Transport. This design addresses the requirements of both legacy and next-generation services in a converged, scalable, and operationally simplified design. It provides transport of any service to any location over any type of access, providing maximum flexibility. It eliminates the need for service-specific networks or protocols, optimizing both capital and operating expenditures for the network infrastructure.

Connected Roadways

The transportation industry is changing radically. As Figure 1-1 depicts, competitive pressure, innovation, and regulation require transport authorities to adopt new standards and infrastructure investments.

Figure 1-1  Today’s Transportation Challenges

- **Safety**: 33,561 highway deaths in 2012, 5,615,000 crashes in 2012. Leading cause of death for ages 4-11-27
- **Mobility**: 5.6 billion hours of travel delay, $121 billion cost of urban congestion
- **Environment**: 2.9 billion gallons of wasted fuel, 50 billion lbs. of additional CO₂
A safe, interoperable wireless communications network that links cars, buses, trucks, trains, transportation infrastructure, and personal mobile devices transforms the way we travel. Technology will fundamentally change the transportation system paradigm by giving people the tools to avoid crashes, and make travel faster, easier, more accessible, and friendlier to the environment. These investments aim to tackle some of the biggest challenges in the surface transportation industry—safety, mobility, and environment:

- **Safety**—According to USDOT, 5.6 million crashes were reported in 2012 alone, resulting in over 33,000 fatalities. While mass transit is already one of the safest modes for travel, connected vehicle technologies will give mass transit drivers tools to anticipate potential crashes and significantly reduce the number of lives lost each year.

- **Mobility**—Connected vehicle mobility applications will enable system operators and travelers to make informed decisions that reduce travel delay. In addition, communication between mass transit and traffic management infrastructures will optimize routing of vehicles, further reducing potential delays.

- **Environment**—According to the American Public Transportation Association (APTA), transit systems can collectively reduce carbon dioxide (CO\(_2\)) emissions by 16.2 million metric tons each year by reducing private vehicle miles. Connected vehicle environmental applications will give all travelers the real-time information they need to make “green” transportation choices.

The following megatrends have emerged which have a profound impact on the future of transportation:

- **Population Growth**—By 2025, an estimated 1 billion additional people will inhabit the earth, with 87% of this growth coming from Asia and Africa. The estimated impact on logistics is equally staggering. Freight transportation, measured in freight ton kilometers (ftk), is forecasted to increase by 60% between 2010 and 2025, reaching up to 31.1 trillion ftk.

- **Grand Economic Shift**—The World Economic Forum projects that by 2030 a radical change in the socioeconomic makeup of global population may occur—with a strong increase in the middle-class. This fundamental shift in demography will influence all types of middle-class expectations about mobility, automobile ownership, civil aviation, and global commerce.

- **Great Urban Shift**—By 2025, nearly half of the world’s population will live in cities of more than 1 million inhabitants. In addition, the total number of megacities—those with more than 10 million inhabitants—is projected to increase from 23 in 2011 to 37 by 2025, with nine new megacities emerging in Asia alone.

- **Global Aging**—It is another important development to consider. Individuals aged 55 or older will account for 20% of world population (or 1.6 billion out of 8 billion) in 2025. This “silver segment” is even expected to reach 35% in G7 countries by 2025, a situation that will call for age-appropriate mobility solutions.

While streamlined operations, safe travel, integrated infrastructures, and intelligent networks are of the utmost importance, the transportation industry continues to face many challenges:

- Increased government regulations, including safety mandates and requirements for driver/operator credentials and workplace standards for employees.

- Congestion on roadways and overcrowded mass transit and railway systems.

- The impact of rising fuel costs on many sectors within the transportation industry, including passenger vehicles, commercial fleets, and emergency response and public safety vehicles.

- Environmental concerns further highlight the importance of reducing pollution and carbon footprints while the demand for travel continues to rise.

Currently, infrastructure upgrades and funding lag behind the demand for travel services over roads, rail, and in the air. It is more important than ever for government agencies and transit operators to find better ways to increase capacity without having to build new infrastructures in the traditional manner.
Policy Trends

The policy initiatives to address the growing needs of transportation are well underway in both the United States and Europe. Similar initiatives are taking shape in Japan, Korea, China, and India. Intelligent Transport Systems is defined by the US Department of Transportation and the European Commission in the following way:

- **USDoT**—ITS improves transportation safety and mobility and enhances American productivity through the integration of advanced communications technologies into the transportation infrastructure and in vehicles. Intelligent transportation systems (ITS) encompass a broad range of wireless and wireline communications-based information and electronics technologies.

- **European Commission**—Intelligent Transport Systems (ITS) apply information and communications technologies to transport. Computers, electronics, satellites, and sensors are playing an increasingly important role in our transport systems. The main innovation is the integration of existing technologies to create new services. ITS as such are instruments that can be used for different purposes under different conditions. ITS can be applied in every transport mode (road, rail, air, water) and services can be used by both passenger and freight transport.

**USDoT Action Plan and Directives**

The following is a synopsis of USDoT action plan and policy directives:

- On January 8, 2001, the Final Rule on ITS Architecture and Standards Conformity (Final Rule) and the Final Policy on Architecture and Standards Conformity (Final Policy) were enacted by the FHWA and FTA, respectively. The Final Rule/Final Policy ensures that ITS projects carried out using funds from the Highway Trust Fund, including the Mass Transit Account, conform to the National ITS Architecture and applicable ITS standards. This will be accomplished through the development of regional ITS architectures and using a systems engineering process for ITS project development.

- FHWA Rule on ITS Architecture and Standards Conformity. This new rule is provided to ensure that intelligent transportation system projects carried out using funds made standards.
  - HTML: [http://www.ops.fhwa.dot.gov/its_arch_imp/policy_1.htm](http://www.ops.fhwa.dot.gov/its_arch_imp/policy_1.htm)
  - PDF: [http://www.ops.fhwa.dot.gov/its_arch_imp/docs/20010108.pdf](http://www.ops.fhwa.dot.gov/its_arch_imp/docs/20010108.pdf)

- FTA Policy on ITS Architecture and Standards Conformity. This new policy is provided to ensure that intelligent transportation system projects carried out using Mass Transit Funds from the Highway Trust Fund to conform to the National ITS Architecture and applicable standards.
  - HTML: [http://www.ops.fhwa.dot.gov/its_arch_imp/policy_2.htm](http://www.ops.fhwa.dot.gov/its_arch_imp/policy_2.htm)
  - PDF: [http://www.ops.fhwa.dot.gov/its_arch_imp/docs/fta-pol.pdf](http://www.ops.fhwa.dot.gov/its_arch_imp/docs/fta-pol.pdf)

- NHTSA Decision on V2 Communication (February 3, 2014). This decision is targeted at light vehicle drivers to be receive collision warnings prior to the crash. Decision on heavy vehicles is expected by the end of 2014.

**European Commission Action Plan and Directives**

The following is a synopsis of European Commission action plan and policy directives:
• ITS can significantly contribute to a cleaner, safer and more efficient transport system. A new legal framework (Directive 2010/40/EU) was adopted on 7 July 2010 to accelerate the deployment of these innovative transport technologies across Europe. This Directive is an important instrument for the coordinated implementation of ITS in Europe. It aims to establish interoperable and seamless ITS services while leaving Member States the freedom to decide which systems to invest in.

• Under this Directive, the European Commission has to adopt within the next seven years specifications (i.e., functional, technical, organizational, or services provisions) to address the compatibility, interoperability, and continuity of ITS solutions across the EU. The first priorities will be traffic and travel information, the eCall emergency system, and intelligent truck parking.

• The Commission already took a major step towards the deployment and use of ITS in road transport (and interfaces to the other transport modes) on 16 December 2008 by adopting an Action Plan. The Action Plan suggested a number of targeted measures and included the proposal for this Directive. The goal is to create the momentum necessary to speed up market penetration of rather mature ITS applications and services in Europe.

• The initiative is supported by five cooperating Directorates General: DG Mobility and Transport (lead), DG Information Society and Media, DG Research, DG Enterprise, and Industry and DG Climate Action.
System Architecture

This chapter includes the following major topics:

- **Roadside Network Design**, page 2-2
- **Citywide MPLS Transport**, page 2-3
- **Transport Infrastructure**, page 2-4

The Connected Roadways System design follows a layered approach. Each layer builds on the previous one by adding new functionalities and capabilities into the system. This design approach results in a network that easily scales to any deployment size, from a metro area deployment to a statewide deployment. It provides the flexibility to position the right platforms at the right locations to match specific deployment criteria.

The system design incorporates a Unified MPLS-based "core" network design for transport. To extend the reach of this transport network to smaller equipment locations, such as roadside cabinets, Ethernet access networks, and time-division multiplexing (TDM) access off of the MPLS transport network are also incorporated. This provides the flexibility to address service transport to any required location.

This chapter provides a detailed description of the Connected Roadways System architecture design and the components of which it is comprised. **Figure 2-1** illustrates the high level architecture of the Connected Roadways System.

This document focuses on the transport layers and their connections to the roadside, yard, and data center layers.
Roadside Network Design

The goal of the Connected Roadways System is to provide an infrastructure interconnecting devices deployed at the roadside with backend systems and centralized control. As nearly all roadside equipment is deployed in cabinets subject to harsh conditions, and even equipment exposed directly to the elements on poles and other locations, special considerations need to be taken when designing a transport infrastructure to accommodate this environment.

The roadside network, as depicted in Figure 2-2, design employs a hardened Cisco router, such as the ISR 819, to provide Layer 3 routing of IP traffic to and from equipment in the curbside cabinet, such as a traffic signal controller, sensor gateway, or any other IP-enabled device. This router is a "customer edge" (CE) routing device, configured to peer with the "provider edge" (PE) devices at the edge of the MPLS network, interworking with Layer 3 virtual private networking (L3VPN) transport. Utilizing L3VPN transport is what allows for a converged infrastructure to support multiple services with proper service separation.

![Figure 2-2 Roadside Network Overview](image)

If a single uplink from the roadside cabinet to the citywide MPLS transport network is desired, then the gigabit Ethernet wide area network (WAN) port Cisco router may be connected directly to the pre-aggregation node (PAN) at the edge of the MPLS network.

In many cases, redundant connectivity to the roadside cabinet equipment is desired. This may be achieved through connectivity to two PANs in a hub-and-spoke fashion from each roadside cabinet; however, having fiber runs and gigabit Ethernet ports consumed on the PANs is very expensive. A more likely network topology is to deploy fiber rings that connect several roadside cabinets to a pair of PANs. In either topology, the gigabit Ethernet WAN port of the hardened Cisco router is connected to a Cisco Industrial Ethernet switch, such as the IE2000.

The Ethernet switch has multiple uplink ports to support the redundant connectivity to the citywide MPLS transport network, and implements topology control functionality to manage traffic flow and avoid loops. For hub-and-spoke deployments, Link Aggregation Control Protocol (LACP) provides management of traffic over the redundant uplinks. For ring deployments, Cisco's Resilient Ethernet Protocol (REP) is used to manage traffic flow around the ring to avoid switching loops and manage traffic rerouting in the event of a link or node failure within the ring. In either deployment scenario, virtual local area network (VLAN) tagging is implemented to maintain service separation over the native Ethernet access network.
Citywide MPLS Transport

The Connected Roadways System design follows a layered approach for the citywide deployment of an MPLS transport network. Each layer builds on the previous one by adding new functionalities and capabilities into the system. See Figure 2-3.

**Figure 2-3   Cisco Connected Roadways System Concept**

**Layer One**

Starting from the first layer, the system's transport infrastructure provides a framework to achieve connectivity among any two or more nodes in the network, whether locations are roadside cabinets, departmental buildings, or centralized infrastructure components. It also enables the virtualization and convergence of multiple services over a common network architecture.

Based on a Unified MPLS transport design, this layer allows for the integration of any access technology and topology into the architecture to meet service requirements and operator preferences. Last mile networks supported include legacy TDM access and Ethernet access over hub-and-spoke and ring topologies made of fiber, copper, or microwave links, as described in the previous section on Roadside Network deployment.

Through automated processes and virtualization, the first layer also aims to minimize or facilitate user intervention at different stages of the network setup:
- Insertion and initial configuration of nodes in the network
- Intelligent route filtering based on route tagging and service activation events
- Optimal centralization of functions in the data center

**Layer Two**

The second layer, the service infrastructure, builds upon those capabilities to instantiate services between nodes in the architecture. This layer is concerned with the ubiquitous setup of transport services over any access and any device, supporting legacy TDM transport via circuit emulation, L2VPN transport, and L3VPN transport. This document focuses on the deployment of L3VPN transport, but it is important to note that L2VPN and circuit emulation service transport are supported concurrently on the same infrastructure.

The service infrastructure is also involved in the integration and virtualization of certain network functions to ensure their optimal placement in the network, resulting in maximized resource utilization and minimized costs, while guaranteeing stipulated service level agreements. Thus, service edge
functions are typically integrated in the network nodes, while other control plane or less performance-demanding tasks may be virtualized in computing resources centralized or distributed in the network, such as route reflectors (RRs) for implementation of Border Gateway Protocol (BGP) for L3VPN service deployment.

Transport Infrastructure

Enabled by the Unified MPLS technology, the Connected Roadways System incorporates a network architecture designed to consolidate transport of multiple services in a single network.

Such converged infrastructure must conform to the SLAs demanded by each of these services, ranging from resiliency requirements, to guaranteed bandwidth, to jitter and delay boundaries. Operations, Administration, and Maintenance (OAM) and Performance Management (PM) aspects, as well as granular QoS assurance, assume a pivotal role in these new networks and become key aspects fully integrated into the system.

Certain services may benefit or even require accurate timing distribution and synchronization across all endpoint equipment in the network. While a number of approaches are possible, including the installation of Global Positioning System (GPS) receivers at each endpoint or dedicated timing equipment in several locations throughout the network, the Connected Roadways System takes advantage of the network fabric as a timing transport infrastructure. By selecting a hybrid approach involving a combination of physical and packet-oriented technologies and a multi-layer hierarchy of clock functions optimally co-located with network equipment, the system is capable of delivering accurate frequency and time throughout the network.

Lastly, as providers convert more and more applications requiring multipoint communication to use a more efficient multicast transport, the industry expectation is that the infrastructure is capable of leveraging the intelligent replication logic built into multicast forwarding increases and becomes a requirement. The Connected Roadways System supports multicast delivered across all services supported, using a combination of multicast Label Distribution Protocol (mLDP) in the aggregation network, and Protocol Independent Multicast (PIM) in the access network.

Unified MPLS

Unified MPLS is the foundation upon which the Evolved Programmable Network (EPN) system, which serves as the basis for the Connected Roadways System, was originally developed and it continues to evolve today. It is an efficient MPLS-based transport that employs a hierarchical approach to solve scaling and convergence issues associated with a large-scale MPLS deployment, while ensuring ease of end-to-end service provisioning and monitoring. End-to-end provisioning implies that service configuration should only happen at the service edges and nowhere else in the network. Similarly, end-to-end monitoring enables the use of service OAM and PM tools to evaluate the state of service “edge-to-edge.”

MPLS is the clear winner as a technology that satisfies the requisites for convergence in Next Generation Networks (NGN) while preserving existing network investments. It supports legacy circuit (Asynchronous Transfer Mode (ATM)/TDM) and packet-based (Ethernet) access technologies and easily enables virtualization of multiple services, including Layer 2 and Layer 3 VPNs, over a single infrastructure.

In its simplest form, MPLS is a technology based on Interior Gateway Protocols (IGPs) and, as such, every node must be capable of reaching any other node in the network. Label Distribution Protocol (LDP) is used for MPLS label distribution to build label-switched paths (LSPs) based on these IGP routes for service transport. For the vast majority of Connected Roadways deployments, this is the
recommended deployment model. Only in the case of extremely large MPLS domain deployments with over 1000 MPLS nodes in the network, does this ubiquitous connectivity requirement become a limiting factor. In this case, Unified MPLS implements a divide-and-conquer strategy, partitioning the network into smaller IGP domains, and implementing RFC3017 compliant BGP to build hierarchical LSP across IGP domains for service transport. This is considered to be a corner case of deployment scenarios, and is not covered in the scope of this document. It is covered in the scope of the EPN system DIGs.

Unified MPLS also distances itself from the traditional MPLS Fast Re-Route (FRR) technologies based on Traffic Engineered (TE) tunnels, which required manual setup of the protection mode and possibly the tunnels, toward totally automated mechanisms.

For LSPs, Loop Free Alternate (LFA) and Remote LFA (rLFA) FRR are used for unicast MPLS/IP traffic in hub-and-spoke and ring topologies. LFA FRR technologies pre-calculate a backup path for every prefix in the IGP routing table, allowing the node to rapidly switch to the backup path when a failure occurs, providing recovery times on the order of 50 msec or less.

For L3VPN services configured in BGP, network re-convergence is accomplished via BGP core and edge Prefix Independent Convergence (PIC) throughout the system. This allows for deterministic network re-convergence on the order of 100 msec, regardless of the number of BGP prefixes. BGP FRR technologies pre-calculate a loop free backup path for every prefix in the BGP forwarding table, and rely on the structure and entries in the Label Forwarding Information Base (LFIB) to allow for a fast transition to the alternate paths.
Network Topology

This chapter includes the following major topics:

- **MPLS Transport Network Model**, page 3-1
- **Ethernet Access Network**, page 3-3

**MPLS Transport Network Model**

The Connected Roadways System design incorporates a native Ethernet access network, and a combined core and aggregation network that implements Unified MPLS.

The Ethernet access network supports point-to-point or ring topologies over fiber and newer Ethernet microwave-based access. Ring topologies can be Layer 3 enabled or Layer 2 only with REP protection.

The MPLS transport services are enabled by the core and aggregation network and include L3VPN, L2VPN, and CES.

The MPLS core/aggregation domain has a single physical topology with a design combining all network nodes in a single MPLS-enabled IGP/LDP region. The access domain is then integrated as a Layer 1 or a Layer 2 cloud made up of Ethernet or TDM links. Figure 3-1 depicts the case of a Layer 1 or a Layer 2 access network. Since no segmentation exists between network layers, a flat LDP LSP provides end-to-end reachability across the network. Aggregation and pre-aggregation nodes are in charge of enabling all mobile and wireline services.

**Figure 3-1**  **MPLS Transport Network Model**
The Connected Roadways System design recommends either Intermediate System to Intermediate System (IS-IS) or Open Shortest Path First (OSPF) for the IGP. The single IGP domain can be implemented as an OSPF Area 0 or as an IS-IS L2 backbone. Since there is no segmentation between network layers, a flat LDP LSP provides end-to-end reachability across the network.

**Transport Network Model Roles**

Table 3-1 lists the names of the network node roles within the Connected Roadways System design and the definition of each role.

<table>
<thead>
<tr>
<th>Network Role</th>
<th>Role Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roadside Router</td>
<td>Provides network connectivity, routing, and facilitates IP address management and network address translation (NAT) for endpoint devices. Performs CE role and peers to PE node for L3VPN service transport.</td>
</tr>
<tr>
<td>Ethernet Access Node (EAN)/Fixed Access Node (FAN)</td>
<td>Provides ruggedized, resilient access from the Roadside Router (and potentially other devices) to the edge of the MPLS network. Maintains service separation by VLANs.</td>
</tr>
<tr>
<td>Pre-Aggregation Node (PAN)</td>
<td>Connects Ethernet Access Networks and TDM circuits for transport across the MPLS network. Implements service edge functions needed for service transport, such as PE role for L3VPN services.</td>
</tr>
<tr>
<td>Core Node (CN)</td>
<td>Provides scalable and resilient transport of MPLS Label Switched Paths (LSPs) between PANs and MTGs. Typically will be the location of the route reflector for the L3VPN service deployment.</td>
</tr>
<tr>
<td>MPLS Transport Gateway (MTG)</td>
<td>Provides MPLS transport network connectivity to centralized network infrastructure and backend systems, such as data centers and Internet peering gateways. Implements service edge functions needed for service transport, such as PE role for L3VPN services to a CE device within the data center. Provides large-scale circuit emulation termination and TDM interconnects.</td>
</tr>
<tr>
<td>Route reflector (RR)</td>
<td>Control-plane only role that maintains table of all possible L3VPN service endpoints in the MPLS transport network. All endpoints within the MPLS transport network simple peer with the RR, instead of having to have all endpoints maintain all peering information with each other.</td>
</tr>
</tbody>
</table>

**Transport Control Plane**

The Connected Roadways System design implements a single IGP/LDP core/aggregation domain, and thus all control plane management is performed by the IGP and LDP protocols. The Connected Roadways System proposes the use of IS-IS or OSPF for the IGP, as these two protocols implement the necessary resiliency and filtering functions for Unified MPLS to operate properly.

BGP is only used for L3VPN service management, and thus the Connected Roadways System design only requires a single RR in the core of the network. Since BGP is not involved in the transport plane, discussion of RR implementation is in Chapter 4, “Service Infrastructure.”
Ethernet Access Network

This section describes the different designs implemented by the Connected Roadways System design for Ethernet-based access network.

Hub-and-Spoke Access Network

Hub-and-spoke topologies are the simplest way of connecting devices, or spokes, to a common aggregation node or hub. These topologies can be single or dual homed, with the latter entailing each spoke node to be connected to a pair of hub devices.

The Connected Roadways System supports the following dual-homed hub-and-spoke topologies:

- Per Node Active/Standby Multichassis Link Aggregation Groups (MC-LAG)
- Per VLAN Active/Active Multichassis Link Aggregation Groups (Pseudo mLACP)

Per Node Active/Standby Multichassis Link Aggregation Groups

Multichassis Link Aggregation Groups (MC-LAG), or Multichassis LACP (mLACP), provides a flexible redundancy mechanism emulating a single homing environment to a dual-homed access device in hub-and-spoke topologies. The access node is connected to the network via a single Ethernet bundle interface with member links terminating into two different service edge devices. These edge nodes synchronize bundle-related protocol states via Inter-Chassis Control Protocol (ICCP) in order to appear as a single entity to the access node. The ICCP protocol runs over MPLS. mLACP mandates that all the bundle members link toward a specific SE node run in either active or standby mode. See Figure 3-2.

Per VLAN Active/Active Multichassis Link Aggregation Groups (Pseudo MC-LAG)

Pseudo MC-LAG enhances standard MC-LAG by load-balancing traffic across PANs, maintaining all inter-chassis links active at the same time on a per-VLAN basis. See Figure 3-3.

The access node is connected to each service edge device via standalone Ethernet links or bundle interfaces that are part of the same bridge domain(s). All the links terminate in a common multi-chassis bundle interface at the SE nodes and are placed in active or hot-standby state based on node and VLAN. ICCP is used again for the correlation required between the PANs.
Figure 3-3  Pseudo Multichassis Link Aggregation

Ethernet Access Rings

Ring topologies allow for ubiquitous connectivity among networks nodes while achieving the highest degree of sharing of physical resources such as the links that interconnect the various nodes.

The dominant interconnection technology over ring topologies has historically been SONET, capable of delivering up to 40 Gbps speeds and sub-50ms failover time.

With the move to NGNs and the wide adoption of Ethernet as the latest interconnection technology for the delivery of cost effective network infrastructure, operators are looking into new ring fault detection mechanisms that are once again standardized, predictable, and fast. Under those premises, the Connected Roadways System design has selected REP to provide protection for Ethernet traffic in a ring topology.

The REP protocol has been developed as a standard alternative to slow converging spanning tree protocol (STP) to achieve faster (~50ms) protection switching in ring topologies without any extensive information exchange, overprovisioning, or complex computation. Loop avoidance is achieved by guaranteeing that at any time, traffic within the ring will flow on all but one of the ring links. Under normal conditions, REP blocks this link to data traffic, only allowing traffic to pass over it if there is a Topology Change Notification (TCN).

The REP protocol allows super-imposing multiple logical rings over the same physical topology by using different instances. Each instance contains an inclusion list of VLAN IDs, thus allowing for per-VLAN load balancing on a single ring. Load sharing between PANs is achieved by implementing two REP instances for different VLAN ranges.

As shown in Figure 3-4, the system design implements a design with the PANs at the ring edges acting as the owners for two different REP instances, blocking the access ring-facing port in their respective instance.

Figure 3-4  REP-enabled Ethernet Access Ring
This chapter includes the following major topics:

- **L3VPN Services**, page 4-2
- **Circuit Emulation Services**, page 4-3
- **Service Control Plane**, page 4-4

The service infrastructure layer of the Connected Roadways System focuses on the deployment and implementation of the full set of services supported by the system. The service infrastructure layer also introduces the next level of convergence in the architecture.

From a service standpoint, the meaning of convergence is multi-fold. Convergence may happen at different levels of the service infrastructure, from the network functions to access technology agnosticism, and can be achieved by network integration.

All services supported by the Connected Roadways System are *Integrated Network Functions*, meaning those functionalities that are optimally embedded in the network transport devices to optimize traffic patterns while reducing power consumption and real estate requirements through consolidation.

The additional computing capacity and better hardware performances of today's equipment have made multi-service capabilities within a single network node possible. Consolidation of functionalities enables economies of scale by decreasing the infrastructure, either installed base or spares. By lowering the power consumption, CAPEX and OPEX are inevitably reduced. In addition, consolidation of transport and service functions within a single device allows for an optimal placement of the service edge based upon service distribution, which, in turn, results in a better use of network resources as well as an improved service experience.

All transport services are supported across a combination of access technologies that include native Ethernet and TDM access. Native Ethernet access is further segmented into hub-and-spoke and ring topologies, depending upon the requirements and deployed network topology.

The various services the Connected Roadways System supports are:

- **L3VPN Services**—Provides Layer 3 routing of IP traffic from numerous remote locations to centralized backend systems.

- **Circuit Emulation Services**—Provides both structured and unstructured emulation of legacy TDM circuits, allowing for convergence of all services into a single infrastructure.

Due to the vast majority of service scenarios being covered by these two service categories, this document focuses on only these. The system also supports:

- **L2VPN Services**—Provides Layer 2 switching of Ethernet frames, analogous to a LAN infrastructure emulated by the MPLS transport. Supports both point-to-point and multipoint deployments, as defined by the Metro Ethernet Forum (MEF).
A future version of the Connected Roadways System may include these L2VPN services as well if sufficient need is identified.

**L3VPN Services**

The vast majority of services deployed in Connected Roadways use case scenarios are supported by L3VPN service transport. Supporting both IPv4 and IPv6 transport, the L3VPN services implemented by the system design can support both existing and next-generation routed transport simultaneously. In addition, multicast transport support ensures that any multicast-reliant services are also supported. The VPN aspect of L3VPN transport services ensures proper service separation, allowing for multiple services and multitenant deployments on a converged infrastructure. An overview of the models supported for the transport of mobile services is illustrated in Figure 4-1 and Figure 4-1.

**Figure 4-1  MPLS Transport Services Architecture-TDM and Ethernet Access**

The L3VPN model allows for roadside network infrastructure to be deployed easily at any location in the network. Likewise, data centers and backend systems can be deployed in multiple locations connected to the MPLS Transport network, and have instant connectivity to each other without additional configuration overhead.

Connectivity between roadside routers associated to Ethernet access nodes and PANs providing service edge functionality for MPLS transport is based on Ethernet links in point-to-point or ring topologies over fiber connectivity. Ring topologies made of Ethernet links are secured by REP ring protection technology to ensure sub-50ms recovery from network ring failures.

Additionally, the L3VPN model provides the required transport virtualization for multiservice deployment on a converged infrastructure, and even provides for multi-tenant deployments that can support multiple departments or agencies on a single infrastructure. It is also capable of providing mesh connectivity for services that may require direct endpoint-to-endpoint communication.

Simple L3VPN route-target import/export mechanisms allow enabling multipoint connectivity while keeping the VPN route scale under control in the following ways:

- Within the local Ethernet access network, enabling communications between devices in that access network
- With adjacent Ethernet access networks, enabling communications between devices in different access networks
- With centralized infrastructure elements located behind the MTGs in the MPLS transport network

**Figure 4-2**  **MPLS Transport Service Routes Filtering Architecture**

As shown in Figure 4-2, the system defines the following route targets to satisfy all possible connectivity requirements while achieving the following optimal traffic patterns:

- A unique route target (RT) denoted as a Common RT is assigned to the transport L3VPN service. It is exported by all PANs across the core/aggregation domain and it is imported by the MTGs. This provides reachability from the centralized backend systems to all roadway endpoints in the network.

- A unique RT denoted by MTG RT is assigned to the MTG. It is imported by all PANs across the MPLS Transport network. This provides reachability from all roadside endpoints via the PANs to the centralized backend systems.

- Each aggregation region in the network is assigned a unique PAN RT. Each PAN in a given domain exports the local PAN RT and imports the PAN RT of neighboring aggregations domains. This provides direct communication between roadside infrastructures.

The rapid migration of IP networking for Connected Roadways deployments is leading to an exponential increase in IP address requirements. In order to minimize the requirements for public IPv4 address usage, the Cisco Connected Roadways System enables carrying IPv6 traffic over an IPv4 Unified MPLS Transport infrastructure, using 6VPE as defined in RFC 4659. The network endpoints can be IPv6 only or dual-stack enabled to support IPv6 for service transport while using IPv4 for network management functions, if desired. The dual-stack network endpoints connect to PANs and MTGs configured with a dual stack VRF carrying VPNv4 and VPNv6 routes. IPv6 reachability between the network endpoints is exchanged between the PANs and MTGs using the BGP MPLS VPN IPv6 address family.

Some services deployed in a Connected Roadways System may require identical data to be distributed to many endpoints. A multicast-based transport mechanism may be implemented for these services, minimizing packet duplication within the transport network.

The multicast mechanism used for transporting multicast service traffic depends upon the network location. In the MPLS transport network domains, transport happens via Label Switched Multicast (LSM) and multicast Label Distribution Protocol (mLDP)-Global in-band signaling profile, which provide efficient and resilient transport of the multicast traffic within these regions. In the Ethernet access domain, native IP Multicast is used to provide efficient and resilient transport.

**Circuit Emulation Services**

Service virtualization with MPLS-based service transport allows for legacy circuit-based transport to co-exist with L3VPNs on the same MPLS transport infrastructure. The Connected Roadways System supports customers wishing to remove, reduce, or cap investments in point-to-point TDM, SONET/SDH, and even ATM transport infrastructure by using MPLS-based circuit emulation over packet (CEoP) services. See Figure 4-3.
Service Control Plane

To optimize the network infrastructure costs, the Connected Roadways System proposes the integration of BGP Service RRs and Network Management System (NMS) as virtualized functions running over a common pool of standard server systems in the customer's data center. See Figure 4-4.
In the case of the Connected Roadways System where the MPLS Transport network is based on a single IGP/LDP core and aggregation domain, the virtual Route Reflector (vRR) design applies to the core RRs only, which provides RR connectivity to all other nodes in the network.
System Components

For each role in the Connected Roadways System architecture, the system selects devices from different Cisco product families to provide operators with the best-of-breed selection of fully interoperable products available in the market.

The various network components and their architectural role are described in Table 5-1.

Table 5-1  Connected Roadways System Components

<table>
<thead>
<tr>
<th>Architectural Role</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation node + service edge</td>
<td>ASR 9006</td>
</tr>
<tr>
<td>Pre-aggregation node</td>
<td>ASR 903 RSP1 and RSP2</td>
</tr>
<tr>
<td>Access node</td>
<td>ASR 901 and ASR 920</td>
</tr>
<tr>
<td>Business CPE</td>
<td>Small Branch—ISR G2 for enterprise and ME1200 NID for MEF transport services</td>
</tr>
<tr>
<td></td>
<td>Large Branch—ASR1000, Virtual-CSR1000V</td>
</tr>
<tr>
<td>Residential CPE</td>
<td>ME4600 RG, Virtual: Quantum virtual Broadband Network (Q-vBN)</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Prime Network Registrar</td>
</tr>
<tr>
<td>Network Management System</td>
<td>Prime Provisioning, Prime Performance Manager</td>
</tr>
</tbody>
</table>
System Functional Considerations

This chapter includes the following major topics:

- Multicast, page 6-1
- Quality of Service (QoS), page 6-2
- Redundancy and High Availability, page 6-3
- Operations, Administration, and Maintenance (OAM), page 6-4

Multicast

The Connected Roadways System supports services delivered via unicast transport as well as multicast transport for any service that requires multicast.

A citywide network may carry multiple multicast services concurrently on a single infrastructure, which requires proper transport organization in order to meet the different communication needs for the disparate services while providing the required separation at the same time.

While standard efforts exist to address transport of multicast services using multicast GRE (mGRE) tunnels and PIM, a more desirable approach aims to consolidate both unicast and multicast traffic forwarding on a common data plane based on label switched paths (LSPs). These new Label Switched Multicast (LSM) paths are created via multicast Label Distribution Protocol (mLDP), which provides extensions to LDP to enable the setup of multiprotocol LSPs (MP LSPs) without requiring additional multicast routing protocols, such as PIM, in the MPLS infrastructure.

As an example of a multicast service, contribution and distribution of broadcast video services involves a limited number of multicast groups and sources, thus only requiring a reasonably low number of LSM trees. A hierarchical approach, built upon LSP nesting to reduce the total number of LSPs and routes to multicast sources that each domain must maintain, is not required for this type of service, and a flat architecture with redistribution of multicast source addresses across all domains is thus used.

Similarly, multipoint-to-multipoint multicast VPNs have historically been centralized in the core domain, also requiring a flat LSP topology.

The scale of multicast service deployment typically encountered in a Connected Roadways System deployment focuses on enabling an end-to-end flat LSM tree across the unified MPLS domains without redistribution. RFC 6512, in particular, defines recursive mLDP behaviors to enable the creation of LSM paths when a given domain has no reachability to the multicast source or root node.

Figure 6-1 illustrates the end-to-end deployment of multicast transport implemented by the system design and based on RFC 6512.
Quality of Service (QoS)

Although congestion is more likely where statistical estimates of peak demand are conservative (that is, under-provisioned), such as in access and aggregation links, it can occur anywhere in a transport network. Therefore, all nodes in a transport network are required to implement congestion management techniques, which involve classification and proper scheduling functions.

The Connected Roadways System design applies the Differentiated Services (DiffServ) Architecture defined by the IETF in RFC 2475 across all network layers, utilizing classification mechanisms like MPLS Experimental (EXP) bits, IP Differentiated Services Code Point (DSCP), and IEEE 802.1p Class of Service (CoS) for implementing the DiffServ Per-Hop Behaviors (PHBs) in use.

Within the aggregation and core networks, where strict control over SLAs is not required, a flat QoS policy with a single-level scheduler is sufficient for the desired DiffServ functionality among the different classes of traffic, as all links are operated at full line rate transmission.

H-QoS policies are required whenever the physical bandwidth of an access link is lower than the line-rate of the interface on the node. An example of this would be a Gigabit Ethernet link transmitted over a point-to-point wireless carrier that only supports approximately 400 Mbps. In this case, a parent policy with a shaper configured to at or just below the speed of the physical bandwidth available, combined with a child policy providing per-class PHB treatments, ensures proper SLA guarantees.

Services in the Connected Roadways System are typically divided into three main categories:

- ** Expedited Forwarding (EF) **—Traffic marked as EF is grouped in a single class, serviced with priority treatment to satisfy stringent latency and delay variation requirements. The EF PHB defines a scheduling logic able to guarantee an upper limit to the per-hop delay variation caused by packets from non-EF services. Examples of these services are Voice-over-IP (VoIP), Network Timing Synchronization, and Circuit Emulation Services (CES) traffic.
Redundancy and High Availability

The Connected Roadways System architecture implements high availability at the transport network level and the service level. By utilizing a combination of several technologies throughout the network, the design is capable of meeting stringent availability SLAs.

High availability at the transport network layer is provided through the combination of several technologies:

- Loop-Free Alternate Fast Reroute (LFA FRR)
- Bidirectional Forwarding Detection (BFD) at the IGP

In addition, the following mechanisms improve resiliency in dual-homing scenarios for Ethernet access, which have been previously discussed in this document:

- Multichassis Link Aggregation Groups (MC-LAG) and pseudo MC-LAG for multi-homed Ethernet access nodes in hub-and-spoke topologies
- REP protection for Ethernet access nodes in ring topologies

Loop-Free Alternate Fast Reroute with BFD

LFA FRR pre-calculates a backup path for every prefix in the IGP routing table, allowing the node to rapidly switch to the backup path when a failure is encountered, with recovery times on the order of 50 msec. Remote LFA FRR functionality extends LFA FRR functionality to ring networks and other topologies.

Also integrated are BFD rapid failure detection and IS-IS/OSPF extensions for incremental shortest-path first (SPF) and link-state advertisement (LSA)/SPF throttling.

More information regarding LFA FRR can be found in IETF RFC 5286, 5714, and 6571.

Microloop Avoidance in Remote LFA FRR

In a network comprised of different platforms, some of which converge faster than others, this difference in convergence time can lead to a condition where a node is forwarding traffic to the same neighbor from which traffic was being received prior to the topology change. This is referred to as a microloop within the topology.

With remote LFA-FRR activated, the backup path is used until the computing node learns about the topology change and reinstalls new paths for the prefix. If the computing node converges before its neighbors, microloops can occur. To prevent this from happening, a microloop avoidance mechanism is provided to postpone the protected prefixes by an additional delay to allow for convergence in its neighbors.
BGP Fast Reroute (FRR) Edge Protection

For L3VPN services, BGP Edge protection and BGP FRR Edge protection mechanisms are supported, and VRRP is enabled on the MTGs for redundant connectivity to the data center infrastructure. The combination of these technologies combined with the transport layer mechanisms ensures a recovery time on the order of sub-200 milliseconds for all L3VPN services due to any node or link failure within the network.

Pseudowire Redundancy

For TDM pseudowire-based services, pseudowire redundancy is supported for protection across the MPLS Transport network. For redundant connectivity to TDM headend connections, Multirouter Automatic Protection Switching (MR-APS) is enabled. This provides a similar recovery target time of sub-200 milliseconds for any infrastructure failure encountered.

Operations, Administration, and Maintenance (OAM)

For transport services, the Connected Roadways System design uses a combination of protocols to provide the required service and transport OAM and PM functionality between the PAN and the MTG. The details of the required mechanism are highlighted in Figure 6-2.

At a high level, for Service OAM, the Connected Roadways System employs:

- MPLS VPN OAM and MPLS VCCV PW OAM for services carried over MPLS VPNs or pseudowires, respectively. Specifically MPLS VPN OAM is used for IP-based services, while MPLS VCCV PW OAM applies to Non-IP services, such as TDM circuit emulation.
- Cisco IP SLA tools for any service configured between IP-enabled end points

For transport OAM, the system design employs MPLS LSP OAM to monitor the health of the Unified MPLS Transport. Performance monitoring is based on Cisco IP SLA tools running between service end points or between any two points in the unified MPLS domain to find performance bottlenecks.
System Implementation

This chapter includes the following major topics:

- Transport Network Implementation, page 7-1
- Small Network Non-IP/MPLS Access Network Implementation, page 7-5
- L3VPN Service Implementation, page 7-13
- Circuit Emulation Services Implementation, page 7-21
- Quality of Service Implementation, page 7-26
- Multicast Services in Global Routing, page 7-35
- High Availability Implementation, page 7-38
- OAM Implementation, page 7-44

Transport Network Implementation

In this model, the core and aggregation networks are integrated with a flat IGP and LDP control plane from the core to the PANs in the aggregation domain. See Figure 7-1.

Figure 7-1 Flat IGP/LDP Network with Ethernet Access

All nodes (MTG, Core, AGN, and PAN) in the combined core-aggregation domain make up the IS-IS Level-2 domain or OSPF backbone area.

In this model, the access network could be one of the following options:
• Routers configured as Customer Edge (CE) devices in point-to-point or ring topologies over fiber Ethernet running native IP transport, supporting L3VPN services. In this case, the CEs pair with PANs configured as L3VPN PEs, enabling Layer 3 backhaul. Any TDM circuits connected directly to the PANs, which provide circuit emulation services via pseudowire-based circuit emulation to the MTG.

• Ethernet Access Nodes in point-to-point and REP-enabled ring topologies over fiber access running native Ethernet. In this case, the PANs provide service edge functionality for the services from the access nodes and connect the services to the proper L2VPN or L3VPN service backhaul mechanism. The MPLS services are always enabled by the PANs in the aggregation network.

MPLS Transport Implementation

MPLS Transport Gateway Configuration

This section shows the IGP/LDP configuration required to build the LSPs to the PANs. See Figure 7-2.

![Figure 7-2 MPLS Transport Gateway (MTG)](image)

Interface Configuration

```snippet
interface Loopback0
   description Global Loopback
   ipv4 address 100.111.15.1 255.255.255.255
!
!***Core-facing Interface***
interface TenGigE0/0/0/0
   description To CN-K0201 Ten0/0/0/0
      cdp
      service-policy output PMAP-NNI-E
      ipv4 address 10.2.1.9 255.255.255.254
      carrier-delay up 2000 down 0
      load-interval 30
      transceiver permit pid all
!
!***Core-facing Interface***
interface TenGigE0/0/0/1
   description To CN-K0401 Ten0/0/0/1
      cdp
      service-policy output PMAP-NNI-E
      ipv4 address 10.4.1.5 255.255.255.254
      carrier-delay up 2000 down 0
      load-interval 30
      transceiver permit pid all
!
```

IGP Configuration

```snippet
router isis core-agg
   set-overload-bit on-startup 250
```
net 49.0100.1001.1101.5001.00
nsf cisco
log adjacency changes
lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
lsp-refresh-interval 65000
max-lsp-lifetime 65535
address-family ipv4 unicast
  metric-style wide
  ispf
  spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200

interface Loopback0
  passive
  point-to-point
  address-family ipv4 unicast
!

interface TenGigE0/0/0/0
  circuit-type level-2-only
  bfd minimum-interval 15
  bfd multiplier 3
  bfd fast-detect ipv4
  point-to-point
  address-family ipv4 unicast
    fast-reroute per-prefix level 2
    metric 10
    mpls ldp sync
!

interface TenGigE0/0/0/1
  circuit-type level-2-only
  bfd minimum-interval 15
  bfd multiplier 3
  bfd fast-detect ipv4
  point-to-point
  address-family ipv4 unicast
    fast-reroute per-prefix level 2
    metric 10
    mpls ldp sync
!
!
mpls ldp
  router-id 100.111.15.1
  discovery targeted-hello accept
  nsr
  graceful-restart
  session protection
  igp sync delay 10
  log
  neighbor
  graceful-restart
  session-protection
  nsr
!
interface TenGigE0/0/0/0
!
interface TenGigE0/0/0/1
!
Pre-Aggregation Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs. Minimal BGP configuration is shown as the basis for building the transport MPLS VPN. The actual service configuration is in L3VPN Service Implementation, page 7-13. See Figure 7-3.

![Figure 7-3 Pre-Aggregation Node (PAN)](image)

Interface Configuration

```plaintext
interface Loopback0
  ip address 100.111.14.3 255.255.255.255
!
***Redundant PAN interface***
interface TenGigabitEthernet0/0/0
  description To PAN-K1404 Ten0/0/0
  ip address 10.14.3.0 255.255.255.254
  ip router isis core
  load-interval 30
  carrier-delay msec 0
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
cdp enable
  isis network point-to-point
  isis metric 10
  isis csnp-interval 10
  service-policy output PMAP-NNI-E
  hold-queue 1500 in
  hold-queue 2000 out
!
***Uplink interface***
interface TenGigabitEthernet0/1/0
  description To AGN-K1102 Ten0/0/0/1
  ip address 10.11.2.1 255.255.255.254
  ip router isis core
  load-interval 30
  carrier-delay msec 0
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
cdp enable
  isis circuit-type level-2-only
  isis network point-to-point
  isis metric 10
  service-policy output PMAP-NNI-E
  hold-queue 1500 in
  hold-queue 2000 out
!
***Interface toward native IP CE device in MPLS VPN VRFS***
! ***Shown here for reference. Not part of Unified MPLS config.***
interface GigabitEthernet0/4/2
  description To CE Router
  vrf forwarding RFS
```
ip address 10.13.14.1 255.255.255.254
ip ospf network point-to-point load-interval 30
negotiation auto
bfd interval 50 min_rx 50 multiplier 3 no bfd echo
hold-queue 350 in
hold-queue 2000 out
!

IGP/LDP Configuration

router isis core-agg
net 49.0100.1001.1101.4003.00
!***PAN is a IS-IS Level-1-2 node***
ispf level-1-2
metric-style wide
fast-flood
set-overload-bit on-startup 180
max-lsp-lifetime 65535
lsp-refresh-interval 65000
spf-interval 5 50 200
prc-interval 5 50 200
lsp-gen-interval 5 5 200
no hello padding
log-adjacency-changes
nsf cisco
passive-interface Loopback0
bfd all-interfaces
mpls ldp sync
!
mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force

Small Network Non-IP/MPLS Access Network Implementation

Dual-homed Hub-and-Spoke Ethernet Access

Dual-homed topologies for hub-and-spoke access have been implemented in the following modes:

- Per Node Active/Standby MC-LAG
- Per VLAN Active/Active MC-LAG (pseudo mLACP)

Per Node Active/Standby MC-LAG

Figure 7-4 illustrates the implementation of hub-and-spoke Ethernet access with MC-LAG operating in Per Node Active and Standby Mode.
The Ethernet access node is dual-homed to the AGN nodes using a bundle interface. The AGN node establishes an inter-chassis bundle and correlates the states of the bundle member ports using ICCP.

At steady state, links connected to AGN1 are selected as active, while links to AGN2 are kept in standby state ready to take over in case of a failure.

The following configuration shows the implementation of the AGN nodes, AGN-K1101 and AGN-K1102, and the Ethernet Access Node.

### Aggregation Node Configuration

**AGN1: Active Point-of-Attachment (PoA) AGN-K1101: ASR9000**

**NNI Interfaces**

For reference throughout this document, the following is a list of settings used for MC-LAG configuration. The access-facing virtual bundle interface is configured as follows:

- Suppress-flaps timer set to 300 ms. This prevents the bundle interface from flapping during a LACP failover.
- Associated with ICCP redundancy group 300
- Lowest possible port-priority (to ensure node serves as active point of attachment (PoA) initially)
- MAC address for bundle interface. This needs to match the MAC address configured on the other PoA’s bundle interface.
- Wait-while timer set to 100 ms to minimize LACP failover time
- Maximum links allowed in the bundle limited to 1. This configuration ensures that the access node will never enable both links to the PoAs simultaneously if ICCP signaling between the PoAs fails.

```plaintext
!*** Interface configuration towards the OLT ***
interface TenGigE0/2/0/1
  bundle id 102 mode active
! interface Bundle-Ether102
  mlacp iccp-group 102
  mlacp switchover type revertive
  mlacp switchover recovery-delay 300
  mlacp port-priority 10
  mac-address 0.1101.1102
!
```

**ICCP and Multichasssis LACP**

For reference throughout this document, the following is a list of settings used for ICCP configuration. The ICCP redundancy group is configured as follows:

- Group ID
- mLACP node ID (unique per node)
- mLACP system MAC address and priority (same for all nodes). These two values are concatenated to form the system ID for the virtual LACP bundle.

- ICCP peer address. Since ICCP works by establishing an LDP session between the PoAs, the peer’s LDP router ID should be configured.

- Backbone interfaces. If all interfaces listed go down, core isolation is assumed and a switchover to the standby PoA is triggered.

```plaintext
!*** ICCP configuration ***
redundancy
iccp
group 102
mlacp node 1
mlacp system mac 0000.1101.1111
mlacp system priority 20
member
    neighbor 100.111.11.2
!
backbone
    interface TenGigE0/0/0
    interface TenGigE0/0/2
!

AGN2: Active Point-of-Attachment (PoA) AGN-A9K-K1102: ASR9000

NNI Interfaces

interface Bundle-Ether300
!*** Interface configuration towards the OLT ***
interface TenGigE0/1/1/1
    bundle id 102 mode active
!
interface Bundle-Ether102
    mlacp iccp-group 102
    mlacp switchover type revertive
    mlacp switchover recovery-delay 300
    mlacp port-priority 20
    mac-address 0.1101.1102
!

ICCP and Multichassis LACP
The ICCP redundancy group is configured as follows:

- Group ID
- mLACP node ID (unique per node)
- mLACP system MAC address and priority (same for all nodes). These two values are concatenated to form the system ID for the virtual LACP bundle.
- ICCP peer address. Since ICCP works by establishing an LDP session between the PoAs, the peer’s LDP router ID should be configured.
- Backbone interfaces. If all interfaces listed go down, core isolation is assumed and a switchover to the standby PoA is triggered.

```plaintext
!*** ICCP Configuration ***
redundancy
iccp
group 102
mlacp node 2
```
Ethernet Access Node Configuration

The following configuration is taken from a Cisco router running IOS. Configurations for Ethernet switches and other access nodes can be easily derived from the following configuration.

**NNI Interfaces**

```plaintext
mlacp system mac 0000.1101.1111
mlacp system priority 20
member
    neighbor 100.111.11.1
!
backbone
    interface TenGigE0/0/0/0
    !
    !
```

**Per VLAN Active/Active MC-LAG (pseudo MC-LAG)**

*Figure 7-5* illustrates the implementation of hub-and-spoke Ethernet access with MC-LAG operating in per VLAN active/active load balancing.
The Ethernet access node connects to each AGN via standalone Ethernet links or Bundle interfaces that are part of a common bridge domain(s). All the links terminate in a common multi-chassis bundle interface at the AGN and are placed in active or hot-standby state based on node and VLAN via ICCP-SM negotiation.

In steady state conditions, each AGN node forwards traffic only for the VLANs it is responsible for, but takes over forwarding responsibility for all VLANs in case of peer node or link failure.

The following configuration shows the implementation of active/active per VLAN MC-LAG for VLANs 100 and 101, on the AGN nodes, AGN-K1101 and AGN-K1102, and the FAN, ME-K0904.

**Aggregation Nodes Configuration**

**AGN1: Active Point-of-Attachment (PoA) AGN-A9K-K1101: ASR9000**

**NNI Interfaces**

```plaintext
interface Bundle-Ether1

interface Bundle-Ether1.100 l2transport
  encapsulation dot1q 100

interface Bundle-Ether1.101 l2transport
  encapsulation dot1q 101

interface GigabitEthernet0/0/1/1
  bundle id 1 mode on
```

**ICCP and ICCP-SM and Multichassis LACP**

For reference throughout this document, here is a list of settings used for ICCP-SM configuration. The ICCP-SM redundancy group is configured as follows:

- Group ID
- Multi-homing node ID (1 or 2 unique per node)
- ICCP peer address. Since ICCP works by establishing an LDP session between the PoAs, the peer’s LDP router ID should be configured.
- Backbone interfaces. If all interfaces listed go down, core isolation is assumed and a switchover to the standby PoA is triggered.

```plaintext
redundancy iccp
  group 1
  member
    neighbor 100.111.11.2
  !
  backbone
    interface TenGigE0/0/0/0
    interface TenGigE0/0/0/2
```
ICCP and Multichassis LACP

The ICCP redundancy group is configured as follows:

```
redundancy
  iccp
group 1
  member
    neighbor 100.111.11.1

  backbone
    interface TenGigE0/0/0
    interface TenGigE0/0/2

*** ICCP-SM configuration ***
```

```
l2vpn redundancy
  iccp group 1
  multi-homing node-id 2
  interface Bundle-Ether1
    primary vlan 101
    secondary vlan 100

!  
!  
```
Ethernet Access Node

In this example, the Ethernet access node is a Cisco Ethernet switch running IOS. Configurations for other access node devices can be easily derived from this configuration example, given that it shows a simple Ethernet trunk configuration for each interface.

NNI Interfaces

interface GigabitEthernet0/13
  port-type nni
  switchport trunk allowed vlan 100-101
  switchport mode trunk
  load-interval 30

interface GigabitEthernet0/14
  port-type nni
  switchport trunk allowed vlan 100-101
  switchport mode trunk
  load-interval 30

Ethernet Access Rings

In addition to hub-and-spoke access deployments, the Connected Roadways System design supports native Ethernet access rings off of the MPLS Transport domain. These Ethernet access rings are comprised of Cisco Industrial Ethernet switches, providing ruggedized and resilient connectivity to many trackside devices.

The Ethernet access switch provides transport of traffic from the roadside CE router and other roadside components. To provide segmentation between services over the Ethernet access network, the access switch implements 802.1q VLAN tags to transport each service. Ring topology management and resiliency for the Ethernet access network is enabled by implementing Cisco REP segments in the network.

The Ethernet access ring is connected to a pair of PANs at the edge of the MPLS Transport network. The PAN maps the service transport VLAN from the Ethernet access network to a transport MPLS L3VPN Virtual Routing and Forwarding (VRF) instance, which provides service backhaul across the Unified MPLS transport network. The REP segment from the access network is terminated on the pair of access nodes, providing closure to the Ethernet access ring.

If the endpoint equipment being connected at the roadside only supports a single default gateway IP address, Virtual Router Redundancy Protocol (VRRP) is implemented on the pair of PANs to provide a single virtual router IP address while maintaining resiliency functionality.

Pre-Aggregation Node Configuration

The following configurations are the same for both access nodes.

VRF Configuration

RT constrained filtering is used to minimize the number of prefixes learned by the PANs. In this example, RT 100:100 is the common transport RT which has all prefixes. While all nodes in the transport network export any connected prefixes to this RT, only the MTG nodes providing connectivity to the data center infrastructure and backend systems will import this RT. These nodes will also export the prefixes of the data center infrastructure with RT 1001:1001. The PAN nodes import this RT, as only connectivity with the data center infrastructure is required.

ip vrf DC
Ethernet Access Ring NNI Configuration

interface GigabitEthernet0/0

description to Ethernet access ring

no ip address

negotiation auto

!***REP segment configuration***

rep segment 1 edge
cdp enable

!***Transport VLAN***

service instance 100 ethernet

encapsulation dot1q 100

rewrite ingress tag pop 1 symmetric

bridge-domain 100

! end

IP/MPLS Access Ring NNI Configuration

This interface has two service instances configured. The untagged service instance provides the L3 connectivity for the MPLS transport. The tagged service instance closes the Ethernet access ring and REP segment with the other access node.

interface GigabitEthernet0/11

description to IP/MPLS Access Ring

no ip address

load-interval 30

carrier-delay msec 0

negotiation auto

rep segment 1 edge

synchronous mode
cdp enable

ethernet oam

!***VLAN for IP/MPLS transport***

service instance 11 ethernet

encapsulation untagged

bridge-domain 11

!

!***VLAN to close Ethernet access ring REP segment***

service instance 100 ethernet

encapsulation dot1q 100

rewrite ingress tag pop 1 symmetric

bridge-domain 100

! end

VRRP Configuration

The following configuration example shows how VRRP is implemented on each access node to enable a single gateway IP address for an endpoint device.

PAN-1

interface Vlan100

ip vrf forwarding DC

ip address 15.0.0.2 255.255.255.0

vrrp 1 ip 15.0.0.1

vrrp 1 timers advertise 2
Ethernet Access Node Configuration

The identical configuration is used for each Ethernet access switch in the ring. Only one switch configuration is shown here.

Ethernet Ring NNI Configuration

UNI to Base Station Configuration

L3VPN Service Implementation

L3 MPLS VPN Service Model

This section describes the implementation details and configurations for the core transport network required for the Layer 3 MPLS VPN service model. See Figure 7-6.

This section is organized into the following sections:

- MPLS VPN Core Transport, which gives the implementation details of the core transport network that serves all the different access models.
- L3VPN Hub-and-Spoke Access Topologies, which describes direct endpoint connectivity at the PAN.
- L3VPN Ring Access Topologies, which provides the implementation details for REP-enabled Ethernet access rings.
Connected Roadways System

Chapter 7      System Implementation

L3VPN Service Implementation

Note
ASR903 RSP1 and RSP2 support L3VPN Services with Non-MPLS access.

Figure 7-6  MPLS VPN Service Implementation

MPLS VPN Core Transport

This section describes the L3VPN PE configuration on the PANs connecting to the access network, the L3VPN PE configuration on the MTGs in the core network, and the RR required for implementing the L3VPN transport services.

This section also describes the BGP control plane aspects of the L3VPN service backhaul. See Figure 7-7.

Figure 7-7  BGP Control Plane for MPLS VPN Service

MPLS Transport Gateway MPLS VPN Configuration

This is a one-time MPLS VPN configuration done on the MTGs. No modifications are made when additional access nodes or other MTGs are added to the network.

Data Center UNI

interface TenGigE0/0/2.1100
  description Connected to Data Center.
  vrf DC102
  ipv4 address 115.1.102.3 255.255.255.0
  ipv6 nd dad attempts 0
  ipv6 address 2001:115::1:102::3/64
  encapsulation dot1q 1100

### VRF Definition

```conf
vrf DC102
  address-family ipv4 unicast
    !***Common Access RT imported by MTG***
    import route-target 10:10
    !
    !***Export MSE RT.***
    !***Imported by every PAN in entire network.***
    export route-target 1001:1001
    !
  address-family ipv6 unicast
    import route-target 10:10
   !
    export route-target 1001:1001
    !
```

### MTG 1 VPNv4/v6 BGP Configuration

```conf
router bgp 1000
  bgp router-id 100.111.15.1
  bgp update-delay 360
  !
  vrf DC102
    rd 1001:1001
    address-family ipv4 unicast
      redistribute connected
    !
    address-family ipv6 unicast
      redistribute connected
    !
```

### MTG 2 VPNv4/v6 BGP Configuration

```conf
router bgp 1000
  bgp router-id 100.111.15.2
  !
  vrf DC102
    rd 1001:1002
    address-family ipv4 unicast
      redistribute connected
    !
    address-family ipv6 unicast
      redistribute connected
    !
```

---

**Note**

Each MTG has a unique RD for the MPLS VPN VRF to properly enable BGP FRR Edge functionality.

A more detailed explanation is given in *High Availability Implementation*, page 7-38.
PAN VPNv4 PE Configuration

```plaintext
router bgp 1000
  bgp router-id 100.111.14.1
  ! ***CN-RR***
  neighbor 100.111.15.50 peer-group cn-rr
  !
  address-family vpnv4
  bgp next-hop trigger delay 3
  ! ***CN-RR***
  neighbor cn-rr send-community both
  neighbor 100.111.15.50 activate
  exit-address-family
  !
  address-family vpnv6
  bgp next-hop trigger delay 3
  ! ***CN-RR***
  neighbor cn-rr send-community both
  neighbor 100.111.15.50 activate
  exit-address-family
  !
  ! ***RT Constrained Route Distribution towards CN-RR***
  address-family rtfILTER unicast
  neighbor cn-rr send-community extended
  neighbor 100.111.15.50 activate
  exit-address-family
  !
```

Centralized CN-RR Configuration

The BGP configuration requires the small change of activating the neighborship when a new PAN is added to the core/aggregation network.

Centralized vCN-RR Configuration

```plaintext
router bgp 1000
  bgp router-id 100.111.15.50
  !
  address-family vpnv4 unicast
  next-hop trigger-delay critical 2000
  !
  address-family vpnv6 unicast
  next-hop trigger-delay critical 2000
  !
  ! ***Peer group for all nodes***
  session-group intra-as
  remote-as 1000
  !
  ! ***Neighbor Group for MTGs***
  neighbor-group mtg
  use session-group intra-as
  !
  ! ***MTGs are Route-Reflector Clients***
  address-family vpnv4 unicast
  route-reflector-client
  !
  address-family vpnv6 unicast
  route-reflector-client
  !
  ! ***Neighbor Group for PANs
```
neighbor-group pan
  use session-group intra-as

  !***PANs are Route-Reflector Clients***
  address-family vpnv4 unicast
    route-reflector-client
  !
  address-family vpnv6 unicast
    route-reflector-client
  !
  exit-address-family

  !***MTGs***
  neighbor 100.111.15.1
    use neighbor-group mtg
  !
  neighbor 100.111.15.2
    use neighbor-group mtg
  !
  !***PANs***
  neighbor 100.111.14.1
    use neighbor-group pan
  !
  neighbor 100.111.14.2
    use neighbor-group pan
  !
  end-policy

MTG VPNv4/v6 PE Configuration

router bgp 1000
  nsr
  bgp router-id 100.111.15.1
  !
  session-group intra-as
  !
  neighbor-group cn-rr
    use session-group intra-as
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  !
  !***CN-RR***
  neighbor 100.111.15.50
    use neighbor-group cn-rr
  !

L3VPN over Hub-and-Spoke Access Topologies

This section describes the implementation details of direct endpoint connectivity at the PAN over hub-and-spoke access topologies.

Direct Endpoint Connectivity to PAN Node

This section shows the configuration of PAN K1401 to which the endpoint is directly connected.
MPLS VPN PE Configuration on PAN K1401

Directly-attached endpoint UNI

interface GigabitEthernet0/3/6
vrf forwarding VPN224
ip address 114.1.224.1 255.255.255.0
load-interval 30
negotiation auto
ipv6 address 2001:114:1:224::1/64

VRF Definition

vrf definition VPN224
rd 10:104
!
address-family ipv4
  export map ADDITIVE
  route-target export 10:104
  route-target import 10:104
  route-target import 1001:1001
  route-target import 236:236
  route-target import 235:235
exit-address-family
!
address-family ipv6
  export map ADDITIVE
  route-target export 10:104
  route-target import 10:104
  route-target import 1001:1001
  route-target import 235:235
exit-address-family
!

!***Route map to export Global RT 10:10 in addition to Local RT 10:203***
route-map ADDITIVE permit 10
set extcommunity rt 10:10 additive

!***VPN BGP Configuration***
router bgp 1000
  neighbor pan peer-group
  neighbor pan remote-as 1000
  neighbor pan password lab
  neighbor pan update-source Loopback0
!
address-family vpnv4
  bgp nexthop trigger delay 2
  neighbor pan send-community extended
!
address-family vpnv6
  bgp nexthop trigger delay 2
  neighbor pan send-community extended
!
address-family ipv4 vrf VPN224
  !***For Directly Connected endpoint***
  redistribute connected
exit-address-family
!
address-family ipv6 vrf VPN224
  !***For Directly Connected endpoint***
  redistribute connected
exit-address-family
L3VPN over Ring Access Topologies

L3VPN transport over ring access topologies are implemented for REP-enabled Ethernet access rings. This section shows the configuration for the pre-aggregation nodes terminating the service from the Ethernet access ring running IOS-XR and a sample router access node. Configuration of the access ring itself with Ethernet switches, as well as PANs running IOS-XE, has been covered in Transport Network Implementation, page 7-1.

PAN dual homing is achieved by a combination of VRRP, routed PW, and REP providing resiliency and load balancing in the access network. In this example, the PANs, AGN-K0301 and AGN-K0302, implement the SE for the Layer 3 MPLS VPN transporting traffic to the data center behind the MTG. A routed BVI interface acts as the service endpoint. The Ethernet access network is implemented as a REP access ring and carries a dedicated VLAN to Layer 3 MPLS VPN-based service. A PW running between the SE nodes closes the service VLAN providing full redundancy on the ring.

VRRP is configured on the Routed BVI interface to ensure the endpoints have a common default gateway regardless of the node forwarding the traffic.

AGN K0302 Configuration

interface TenGigE0/2/1/3.302 l2transport
  encapsulation dot1q 302
  rewrite ingress tag pop 1 symmetric
!
  l2vpn
  bridge group L2VPN
  bridge-domain L3VPN-302
    interface TenGigE0/2/1/3.302
    !

  !*** Routed PW configured to other SE Node 100.111.3.1***
    neighbor 100.111.3.1 pw-id 302
    !
    routed interface BVI302
    !
    !
  !***VRF Definition***
    vrf VPN224
      address-family ipv4 unicast
        import route-target
    !***Local RT***
      10:104
      235:235
      236:236
      1001:1001
      !
      export route-policy ADDITIVE
      export route-target
      10:104
      !
    !
    address-family ipv6 unicast
      import route-target
      10:104
      235:235
      236:236
      1001:1001
      !
      export route-policy ADDITIVE
      export route-target
      10:104
      !
**L3VPN Service Implementation**

---

**Chapter 7  System Implementation**

**L3VPN Service Implementation**

---

**AGN K0301 Configuration**

```
interface TenGigE0/2/1/3.302 l2transport
  encapsulation dot1q 302
  rewrite ingress tag pop 1 symmetric

l2vpn
  bridge group L2VPN
    bridge-domain L3VPN-302
      interface TenGigE0/2/1/3.302

*** Routed PW configured to other SE Node 100.111.3.2***
  neighbor 100.111.3.2 pw-id 302

routed interface BVI302

***VRF Definition***

vrf VPN224
  address-family ipv4 unicast
  import route-target

***Local RT ***
  10:104
  235:235
  236:236
  1001:1001

  export route-policy ADDITIVE
  export route-target
  10:104

address-family ipv6 unicast
import route-target

10:104
235:235
236:236
1001:1001

export route-policy ADDITIVE
```
export route-target
10:104
!
!

!***BVI Interface Configuration***
interface BVI302
vrf VPN224
ipv4 address 30.2.1.3 255.255.255.0
ipv6 nd dad attempts 0
ipv6 address 2001:13:2:102::3/64
!

!***VRRP Configuration***
router vrrp
interface BVI302
   address-family ipv4
   vrrp 2
!***Highest Priority value to be active***
   priority 252
   address 30.2.1.1
   bfd fast-detect peer ipv4 30.2.1.2
!
!

Sample Access Node Configuration

interface GigabitEthernet0/5
!***connection to endpoint***
   service instance 302 ethernet
   encapsulation dot1q 302
   rewrite ingress tag pop 1 symmetric
   bridge-domain 302
!
interface TenGigabitEthernet0/1
!*** NNI port***
   service instance 302 ethernet
   encapsulation dot1q 302
   rewrite ingress tag pop 1 symmetric
   bridge-domain 302
interface TenGigabitEthernet0/0
!*** NNI port***
   service instance 302 ethernet
   encapsulation dot1q 302
   rewrite ingress tag pop 1 symmetric
   bridge-domain 302

Circuit Emulation Services Implementation

Layer 2 MPLS VPN service models provide TDM CES for legacy TDM circuit transport. The following models are shown in this section:

- TDM backhaul from the PAN to the MTG, utilizing the structured CESoPSN mechanism
- TDM backhaul from the PAN to the MTG, utilizing the unstructured SAToP mechanism
Circuit Emulation Service over Packet Switched Network (CESoPSN) provides structured transport of TDM circuits down to the DS0 level across an MPLS-based backhaul architecture. The configurations for the PAN and MTGs are outlined in this section, including an illustration of basic backup pseudowire configuration on the PAN in order to enable transport to redundant MTGs. See Figure 7-8.

Regarding CESoPSN Service Implementation:

- The Cisco ASR 903 Series router uses a 16-port T1/E1 Interface Module (A900-IMA16D) for TDM interfaces.
- Both Cisco ASR 9000 Series MTGs use 1-port channelized OC3/STM-1 ATM and circuit emulation SPA (SPA-1CHOC3-CE-ATM) in a SIP-700 card for the TDM interfaces.
- CESoPSN encapsulates T1/E1 structured (channelized) services. Structured mode (CESoPSN) identifies framing and sends only payload, which can be channelized T1s within DS3 and DS0s within T1. DS0s can be bundled to the same packet. This mode is based on IETF RFC 5086.
- mpls ldp discovery targeted-hello accept is required because the LDP session is tunneled via PW between the PEs, since they are not directly connected. Since targeted-hello response is not configured, both sessions will show as passive.

Cisco ASR 903 Series Pre-Aggregation Node Configuration

```bash
card type t1 0 5
! controller T1 0/5/1
  framing esf
  clock source internal
  linecode b8zs
  cablelength short 110
  forward-alarm ais
  forward-alarm rai
  cem-group 0 timeslots 1-24
! pseudowire-class CESoPSN
capsulation mpls
control-word
!
! interface CEM0/5/1
no ip address
load-interval 30
cem 0
  xconnect 100.111.15.1 1401150113 encapsulation mpls pw-class CESoPSN
  backup peer 100.111.15.2 1401150213 pw-class CESoPSN
!
hold-queue 4096 in
hold-queue 4096 out
```
interface Loopback0
  ip address 100.111.14.1 255.255.255.255
  
router isis agg-acc
  passive-interface Loopback0

!*** ISIS and BGP related configuration needed to ensure MPLS LDP binding with remote PE so as to establish AToM PW***
  mpls ldp discovery targeted-hello accept

Cisco ASR 9000 Series MPLS Transport Gateway Configuration

The other MTG configuration is identical, except with a Loopback 0 IP address of 100.111.15.2 and pw-ids ending in 1502 instead of 1501.

hw-module subslot 0/2/1 cardtype sonet
  
controller SONET0/2/1/0
  description To ONS15454-K1410 OC3 port 4/1
  ais-shut
  report lais
  report lrdi
  sts 1
  mode vt15-t1
  delay trigger 250
  
controller T1 0/2/1/0/1/1/3
  cem-group framed 0 timeslots 1-24
  forward-alarm AIS
  forward-alarm RAI
  clock source internal
  
interface CEM0/2/1/0/1/3:0
  load-interval 30
  l2transport
  
interface Loopback0
  description Global Loopback
  ipv4 address 100.111.15.1 255.255.255.255
  
l2vpn
  pw-class CESoPSN
  encapsulation mpls
  control-word
  
xconnect group TDM-K1401
  p2p T1-CESoPSN-01
  interface CEM0/2/1/0/1/3:0
  neighbor ipv4 100.111.14.1 pw-id 1401150113
  pw-class CESoPSN
  
router isis core
  interface Loopback0
  passive
point-to-point
address-family ipv4 unicast
!
!
router bgp 1000
bgp router-id 100.111.15.1
address-family ipv4 unicast
   network 100.111.15.1/32 route-policy MTG_Community
!
mpls ldp
   router-id 100.111.15.1
   discovery targeted-hello accept
!
*** ISIS and BGP related configuration needed to ensure MPLS LDP binding with remote PE so as to establish AToM PW***
!

SAToP VPWS from PAN to MTG

Structure-Agnostic Transport over Packet (SAToP) provides unstructured transport of TDM circuits across an MPLS-based backhaul architecture. The configurations for the PAN and MTGs are outlined in this section, including an illustration of backup pseudowire configuration on the PAN in order to enable transport to redundant MTGs. See Figure 7-9.

Figure 7-9 SAToP VPWS Implementation

Regarding SAToP VPWS implementation:
- The Cisco ASR 903 Series router uses a 16-port T1/E1 Interface Module (A900-IMA16D) for TDM interfaces.
- Both Cisco ASR 9000 Series MTGs use 1-port channelized OC3/STM-1 ATM and circuit emulation SPA (SPA-1CHOC3-CE-ATM) in a SIP-700 card for the TDM interfaces.
- SAToP encapsulates T1/E1 services, disregarding any structure that may be imposed on these streams, in particular the structure imposed by the standard TDM framing. This mode is based on IETF RFC 4553.
- mpls ldp discovery targeted-hello accept is required because the LDP session is tunneled via PW between the PEs, since they are not directly connected. Since targeted-hello response is not configured, both sessions will show as passive.

Cisco ASR 903 Series Pre-Aggregation Node Configuration

card type t1 0 5
!
controller T1 0/5/0
   framing unframed
clock source internal
   linecode b8zs
Cisco ASR 9000 Series Mobile Transport Gateway Configuration

The other MTG configuration is identical, except with a Loopback 0 IP address of 100.111.15.2 and pw-ids ending in 1502 instead of 1501.

```plaintext
cablelength short 110
cem-group 0 unframed
!
pseudowire-class SAToP
encapsulation mpls
control-word
!
interface CEM0/5/0
no ip address
load-interval 30
cem 0
xconnect 100.111.15.1 14011501 encapsulation mpls pw-class SAToP
backup peer 100.111.15.2 14011502 pw-class SAToP
!
hold-queue 4096 in
hold-queue 4096 out
!
interface Loopback0
ip address 100.111.14.1 255.255.255.255
!
router isis agg-acc
passive-interface Loopback0
!
mpls ldp discovery targeted-hello accept

hw-module subslot 0/2/1 cardtype sonet
!
controller SONET0/2/1/0
description To ONS15454-K1410 OC3 port 4/1
ais-shut
report lais
report lrdi
sts 1
mode vt15-t1
delay trigger 250
!
controller T1 0/2/1/0/1/2

cem-group unframed
forward-alarm AIS
forward-alarm RAI
clock source line
!
interface CEM0/2/1/0/1/2
load-interval 30
12transport
!
!
interface Loopback0
description Global Loopback
ipv4 address 100.111.15.1 255.255.255.255
!
12vpn
```
Quality of Service Implementation

The Connected Roadways System design uses a DiffServ QoS model across all network layers of the transport network in order to guarantee proper treatment of all services being transported. This QoS model guarantees the SLA requirements of all services across the transport network. QoS policy enforcement is accomplished with flat QoS policies with DiffServ queuing on all network-to-network interfaces (NNI), and H-QoS policies with parent shaping and child queuing on the user-network interfaces (UNIs) and interfaces connecting to microwave access links.

This section covers the aggregate QoS policies implemented on the NNI interfaces in the transport network, illustrating the treatment of all services traversing the transport network. It also covers QoS policies for UNI interfaces on both the access network as well as MTG for proper service treatment.

The classification criteria used to implement the DiffServ PHBs is covered in Figure 7-10.
**Figure 7-10  Differentiated Service QoS Domain**

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>PHB</th>
<th>Unified MPLS Transport</th>
<th>Ethernet/TDM/ATM UNI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DSCP</td>
<td>EXP</td>
</tr>
<tr>
<td>Network Management</td>
<td>AF</td>
<td>56</td>
<td>7</td>
</tr>
<tr>
<td>Network Control Protocols</td>
<td>AF</td>
<td>48</td>
<td>6</td>
</tr>
<tr>
<td>Real-Time Traffic Voice over IP</td>
<td></td>
<td>EF</td>
<td>5</td>
</tr>
<tr>
<td>Network Sync (1588 PTP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobility &amp; Signaling traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Distribution</td>
<td>AF</td>
<td>32</td>
<td>4</td>
</tr>
<tr>
<td>Video Surveillance Control</td>
<td>AF</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>Business Critical</td>
<td>AF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committed Information Rate (CIR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permitted Information Rate (PIR)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Best Effort</td>
<td>BE</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

In Figure 7-11, the following elements are called out:

- (a) H-QoS policy map on CE UNIs
- (1) (2) Flat QoS policy map on CSG and pre-aggregation NNIs in fiber access network
- (3) Flat QoS policy map on aggregation and core network NNIs
- (4) Flat QoS policy map on ingress for Circuit Emulation UNIs

**Figure 7-11  QoS Enforcement Points**

**CE QoS Configuration**

Class maps used for UNI classification are included here for reference. As stated above, the service-specific policies utilizing these class maps are covered in the service-specific design and implementation guides.

**Class Maps**

- QoS classification at the UNI in the ingress direction for upstream traffic is based on IP differentiated services code point (DSCP), with the marking done by the connected device for Layer 3 services.

```plaintext
!***Network management traffic***
class-map match-any CMAP-NMgmt-DSCP
```
Quality of Service Implementation

Chapter 7      System Implementation

match dscp cs7
!
!***Voice/Real-Time traffic***
class-map match-all CMAP-RT-DSCP
  match dscp ef
!
!*** Video traffic***
class-map match-any CMAP-Video-DSCP
  match dscp cs4

- QoS classification at the UNI in the ingress direction for upstream traffic is based on 802.1p class of service (CoS) markings, with the marking done by the connected device for Layer 2 services.

!***Voice/Real-Time traffic***
class-map match-any CMAP-RT-COS
  match cos 5
!
!***Video conferencing and TelePresence traffic***
class-map match-any CMAP-BC-Tele-COS
  match cos 3
!
!***Business critical traffic***
class-map match-any CMAP-BC-COS
  match cos 1 2

- QoS classification at the UNI in the egress direction for downstream traffic is based on QoS groups with the QoS group mapping being done at the ingress NNI.

- QoS classification at the NNI in the egress direction is based on QoS groups, with:
  - QoS group mapping for upstream traffic being done at the ingress UNI.
  - QoS group mapping for traffic transiting the access ring being done at the ingress NNI.

!***Network management traffic***
class-map match-any CMAP-NMgmt-GRP
  match qos-group 7
!
!***Network control traffic***
class-map match-any CMAP-CTRL-GRP
  match qos-group 6
!
!***Voice/Real-Time traffic***
class-map match-all CMAP-RT-GRP
  match qos-group 5
!
!***Broadcast Video traffic***
class-map match-any CMAP-Video-GRP
  match qos-group 4

- QoS classification at the NNI in the ingress direction is based on MPLS EXP for MPLS access and based on CoS for G.8032 access.

NNI Classification for REP Ring Access

!***Network management traffic***
class-map match-any CMAP-NMgmt-COS
  match cos 7
!
!***Network control traffic***
class-map match-any CMAP-CTRL-COS
  match cos 6
!
!***Voice/Real-Time traffic***
class-map match-all CMAP-RT-COS
  match cos 5
!
!***Broadcast Video traffic***
class-map match-any CMAP-Video-COS
  match cos 4
!
!***Video conferencing and TelePresence traffic***
class-map match-any CMAP-BC-Tele-EXP
  match cos 3
!
!***Business critical traffic***
class-map match-any CMAP-BC-COS
  match cos 1 2

REP Fiber Ring NNI QoS Policy Maps

- For downstream and transit traffic, a flat QoS policy map with group mapping applied in the ingress direction is used.
- For upstream and transit traffic, a flat QoS policy map with DiffServ queuing applied in the egress direction is used.

!*** QoS enforcement point (E)***
!***Interface connecting to REP Fiber Access Ring.***
interface TenGigabitEthernet0/0
  service-policy input PMAP-NNI-I
  service-policy output PMAP-NNI-E

! policy-map PMAP-NNI-E
!*** Egress policy on NNI PORT ***
class CMAP-RT-GRP
  priority percent 20
class CMAP-BC-GRP
  bandwidth percent 5
class CMAP-BC-Tele-GRP
  bandwidth percent 10
class class-default
!
! policy-map PMAP-NNI-I
!*** Ingress Policy on NNI Port ***
class CMAP-BC-COS
  set qos-group 2
class CMAP-RT-COS
  set qos-group 5
police rate 1000000
class CMAP-BC-Tele-COS
  set qos-group 3
!

Pre-Aggregation Node QoS Configuration (Cisco ASR 903)

Class Maps

- QoS classification for any local UNI connections in the ingress direction for upstream traffic is based on IP DSCP with the marking done by the connected device for residential and mobile services.
Quality of Service Implementation

- **QoS classification for any local UNI connections in the ingress direction for upstream traffic is based on 802.1p CoS markings, with the marking done by the connected device for business services.**

```diff
!!***Network management traffic***
class-map match-any CMAP-NMgmt-DSCP
  match dscp cs7
!
!!***Voice/Real-Time traffic***
class-map match-all CMAP-RT-DSCP
  match dscp ef
!
!!***Broadcast Video traffic***
class-map match-any CMAP-Video-DSCP
  match dscp cs4
```

- **QoS classification at the NNI in the ingress and egress directions is based on MPLS EXP.**

```diff
!!***Network management traffic***
class-map match-any CMAP-NMgmt-EXP
  match mpls experimental topmost 7
!
!!***Network control traffic***
class-map match-any CMAP-CTRL-EXP
  match mpls experimental topmost 6
!
!!***Voice/Real-Time traffic***
class-map match-all CMAP-RT-EXP
  match mpls experimental topmost 5
!
!!***Broadcast Video traffic***
class-map match-any CMAP-Video-EXP
  match mpls experimental topmost 4
!
!!***Video conferencing and TelePresence traffic***
class-map match-any CMAP-BC-Tele-EXP
  match mpls experimental topmost 3
!
!!***Business critical traffic***
class-map match-any CMAP-BC-COS
  match cos 1 2
```

**Fiber Ring UNI QoS Policy Maps**

The ingress and egress QoS service policies on the UNI are service-specific and thus are covered in Chapter 4, “Service Infrastructure.”
Fiber Access NNI QoS Policy Maps

- For downstream traffic, a flat QoS policy map with DiffServ queuing is applied in the egress direction on the pre-aggregation NNI that is facing the 1-G fiber access network.

```
!***QoS enforcement point (2).***
!***Interface connecting Fiber Access Network.***
interface GigabitEthernet0/2
  service-policy output PMAP-NNI-Access-E
!
policy-map PMAP-NNI-Access-E
  class CMAP-RT-EXP
    priority
    police cir 200000000
  class CMAP-CTRL-EXP
    bandwidth 15000
  class CMAP-NMgmt-EXP
    bandwidth 50000
  class CMAP-Video-EXP
    bandwidth 200000
  class CMAP-BC-EXP
    bandwidth 100000
  class CMAP-BC-Tele-EXP
    bandwidth 100000
```

Aggregation NNI QoS Policy Map

- For upstream and transit traffic, a flat QoS policy map with DiffServ queuing is applied in the egress direction on the pre-aggregation NNI facing the 10-G aggregation network.

```
!***QoS enforcement point (3).***
!***Interface connecting Aggregation Network.***
interface TenGigabitEthernet0/1
  service-policy output PMAP-NNI-E
!
policy-map PMAP-NNI-E
  class CMAP-RT-EXP
    priority
    police cir 1000000000
  class CMAP-CTRL-EXP
    bandwidth 150000
  class CMAP-NMgmt-EXP
    bandwidth 500000
  class CMAP-Video-EXP
    bandwidth 2000000
  class CMAP-BC-EXP
    bandwidth 1000000
  class CMAP-BC-Tele-EXP
    bandwidth 1000000
```

Aggregation and Core Network QoS Configuration

Class Maps

- QoS classification at the NNIs is based on MPLS EXP.

```
class-map match-any CMAP-BC-EXP
  match mpls experimental topmost 1 2
end-class-map
```
class-map match-any CMAP-BUS-Tele-EXP  
match mpls experimental topmost 3  
end-class-map  

class-map match-any CMAP-Video-EXP  
match mpls experimental topmost 4  
end-class-map  

class-map match-any CMAP-RT-EXP  
match mpls experimental topmost 5  
end-class-map  

class-map match-any CMAP-CTRL-EXP  
match mpls experimental topmost 6  
end-class-map  

class-map match-any CMAP-NMgmt-EXP  
match mpls experimental topmost 7  
end-class-map  

NNI QoS Policy Maps

- Flat QoS policy map with DiffServ queuing is applied at all NNIs.

***10Gbps NNI***

policy-map PMAP-NNI-E  
class CMAP-RT-EXP  
priority level 1  
police rate 1 gbps  
!  
class CMAP-CTRL-EXP  
bandwidth 200 mbps  
!  
class CMAP-NMgmt-EXP  
bandwidth 500 mbps  
!  
class CMAP-Video-EXP  
bandwidth 2 gbps  
!  
class CMAP-BC-EXP  
bandwidth 1 gbps  
***Random Detect preserves CIR over PIR traffic***  
random-detect exp 2 80 ms 100 ms  
random-detect exp 1 40 ms 50 ms  
!  
class CMAP-BUS-Tele-EXP  
bandwidth 2 gbps  
!  
class class-default  
!  
end-policy-map  

***100Gbps NNI***

policy-map PMAP-NNI-100GE-E  
class CMAP-RT-EXP  
priority level 1  
police rate 10 gbps  
!  
!  
class CMAP-CTRL-EXP  
bandwidth 2 gbps
MTG QoS Configuration

This section includes the UNI configuration for Ethernet, ATM, and TDM services on the MPLS Transport Gateway.

Ethernet UNI QoS Policy Maps

The following configurations show the simple class maps and policy maps for interconnecting service transport to and from the MPLS transport network at the MTG.

```plaintext
class-map match-all CMAP-RT-DSCP
  match dscp ef
end-class-map
!
class-map match-any CMAP-NMgmt-DSCP
  match dscp cs7
end-class-map
!
class-map match-any CMAP-Video-DSCP
  match dscp cs3
end-class-map
!
policy-map PMAP-UNI-E
  class CMAP-RT-DSCP
    priority level 1
    police rate 10000 kbps
  !
  class CMAP-NMgmt-DSCP
    bandwidth 50000 kbps
  !
  class CMAP-Video-DSCP
    bandwidth 200000 kbps
  !
  class class-default
  !
end-policy-map
!
policy-map PMAP-UNI-I
```
class CMAP-RT-DSCP
  priority level 1
  police rate 10000 kbps
  set mpls experimental imposition 5
!

class CMAP-NMgmt-DSCP
  bandwidth 50000 kbps
  set mpls experimental imposition 7
!

class CMAP-HVideo-DSCP
  bandwidth 200000 kbps
  set mpls experimental imposition 3
!

class class-default
!
end-policy-map

ATM UNI QoS Policy Maps

The only ingress marking to match is the ATM Cell Loss Priority (CLP) bit on ATM UNIs, which indicates a discard preference for marked cells within a particular ATM CoS. This can be utilized to offer a bursting capability in a particular ATM CoS.

class-map match-any CMAP-ATM-CLP0-UNI-I
  match atm clp 0
end-class-map
!

class-map match-any CMAP-ATM-CLP1-UNI-I
  match atm clp 1
end-class-map

Two ATM policy maps are shown. The first corresponds to an ATM Variable Bit Rate-Real Time (VBR-rt) service where cells are marked with a CLP of 1 above a certain cell rate. The second corresponds to an ATM Unspecified Bit Rate (UBR) service, again where cells are marked with a CLP of 1 above a certain cell rate. The proper map is applied to an ATM PVC which corresponds to the ATM CoS carried on that PVC.

policy-map PMAP-ATM-UNI-I
  class CMAP-ATM-CLP0-UNI-I
    set mpls experimental imposition 5
  !
  class CMAP-ATM-CLP1-UNI-I
    set mpls experimental imposition 4
  !
  class class-default
  !
end-policy-map
!
	policy-map PMAP-ATM-UNI-DATA-I
  class CMAP-ATM-CLP0-UNI-I
    set mpls experimental imposition 4
  !
  class CMAP-ATM-CLP1-UNI-I
    set mpls experimental imposition 0
  !
  class class-default
  !
end-policy-map
interface ATM0/2/3/0
load-interval 30

interface ATM0/2/3/0.100 l2transport
pvc 100/4011
  service-policy input PMAP-ATM-UNI-I
  encapsulation aal0
  shape vbr-rt 20000 14000 7000
!

interface ATM0/2/3/0.101 l2transport
pvc 100/4012
  service-policy input PMAP-ATM-UNI-DATA-I
  shape ubr 40000
!

TDM UNI QoS Policy Map

The TDM UNI policy map simply marks all traffic on a CEM interface with an MPLS EXP of 5 to ensure that all traffic associated with the CEM interface is given EF treatment. This ensures that the emulated TDM circuit is transported with minimum packet delay variation (PDV) in order to guarantee the quality of the TDM circuit.

policy-map PMAP-TDM-UNI-I
  class class-default
    set mpls experimental imposition 5
  end-policy-map

interface CEM0/2/1/0/1/4/4
  service-policy input PMAP-TDM-UNI-I
  load-interval 30
  l2transport
!

Multicast Services in Global Routing

This section describes the implementation of multicast in global routing using Label-Switched Multicast (LSM) with Multicast Label Distribution Protocol (MLDP) Global in-band signaling to support Multicast service transport over the MPLS transport network. The MPLS Multicast domain is based on LSM, which is a solution that enables forwarding of IP multicast traffic over MPLS, thus allowing the MPLS infrastructure to provide a common data plane (based on label switching) for both unicast and multicast traffic.

In the configuration examples in this section, multicast sources are attached to each of the MPLS Transport Gateways, MTG-1501 and MTG-1502, respectively, and AGN K1101 and AGN K1102 mark the end of aggregation/core to where the mLDP domain extends.

MTG-9006-K1501 (Root-node/Ingress-PE)

***Advertise the network prefix where the Multicast source is located***
router bgp 1000
  bgp router-id 100.111.15.1
****Advertising the IPv4 multicast source prefixes****
address-family ipv4 unicast
    network 200.15.12.0/24 route-policy MSE_IGN_Community
    network 200.15.1.0/24 route-policy MSE_IGN_Community

****Advertising the IPv6 multicast source prefixes****
address-family ipv6 unicast
    network 2001:100:111:15::1/128
    network 2001:100:192:10::/64
    allocate-label all

****Enable MLDP****
mlps ldp
    mldp
        logging notifications
        interface TenGigE0/0/0/0
        interface TenGigE0/0/0/1
        interface TenGigE0/0/0/2

****Disable mLDP on interfaces that don't need mLDP****
    mldp disable

****Configure route-policy to set the type of MLDP core tree****
    route-policy MLDP-Inband
        set core-tree mldp-inband

****Set mLDP-Inband signaling****
    end-policy

****Assign the configured MLDP route-policy under router PIM****
    router pim
        address-family ipv4
            rpff topology route-policy MLDP-Inband
        address-family ipv6
            rpff topology route-policy MLDP-Inband

****Configure Multicast-routing to enable Multicast interfaces, MDT source, and MLDP in-band signaling****
    multicast-routing
        address-family ipv4
            mdt source Loopback0
            mdt mldp in-band-signaling ipv4
            rate-per-route
        !
        address-family ipv6
            mdt source Loopback0
            mdt mldp in-band-signaling ipv4
            rate-per-route

****Enable multicast on all interfaces****
    interface all enable
    accounting per-prefix

****Configure Multicast-routing to enable Multicast interfaces, MDT source, and MLDP in-band signaling****

Branch Node Configuration

The branch node configuration is illustrated here for larger deployments that may require multiple nodes between the edges of the MPLS transport network. It essentially shows that the only configuration needed is to enable MLDP on the node.

**** In the BRANCH-node/P-routers, the only configuration needed is MLDP****
AGN-9006-K1102 (Leaf-node/Egress-PE)

This node is a Cisco ASR 9000 Series router acting as the service edge (SE) node and used as the Leaf-node/Egress-PE of the Multicast distribution tree. The native IP Multicast (v4 & v6) coming from the access network terminates here, and then LSM MLDP-Global starts from this node towards the ROOT-node/Ingress-PE passing through the MPLS transport network.

```config
!***Enable MLDP***
mpls ldp
!***Enables mLDP***
mldp
logging notifications
!***Needed for faster LSM convergence***
make-before-break delay 0 0
!
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
interface TenGigE0/0/0/2
interface TenGigE0/0/0/3
interface GigabitEthernet0/2/0/0
!***Disable mLDP on CN-RR interface***
 mldp disable
!
interface TenGigE0/0/0/0
interface TenGigE0/0/0/2
!***mLDP uses the LDP interfaces by default.***
!***Disable mLDP on interfaces facing the Access Network***
mldp disable
!
!***Configure route-policy to set the type of MLDP core tree***!
route-policy MLDP-Inband
!***Set mLDP-Inband signaling***
 set core-tree mldp-inband
!***Assign the configured MLDP route-policy under router PIM***
 router pim
  address-family ipv4
    rpf topology route-policy MLDP-Inband
  !
  address-family ipv6
    rpf topology route-policy MLDP-Inband
  !
!***Configure Multicast-routing to enable Multicast interfaces, MDT source, and MLDP in-band signaling***
multicast-routing
  address-family ipv4
    mdt source Loopback0
    mdt mldp in-band-signaling ipv4
    rate-per-route
    accounting per-prefix
    !***Enable multicast on all IPv4 interfaces***
    interface all enable
    accounting per-prefix
    !
    address-family ipv6
```

This node is a Cisco ASR 9000 Series router acting as the service edge (SE) node and used as the Leaf-node/Egress-PE of the Multicast distribution tree. The native IP Multicast (v4 & v6) coming from the access network terminates here, and then LSM MLDP-Global starts from this node towards the ROOT-node/Ingress-PE passing through the MPLS transport network.
High Availability Implementation

This section focuses on the implementation details of high availability functionality at the service level. Transport level resiliency has been previously covered in Transport Network Implementation, page 7-1.

- For MPLS VPN services, BGP Edge protection and BGP FRR Edge protection mechanisms are supported, and VRRP is enabled on the MTGs for redundant connectivity to the data center infrastructure.
- For TDM pseudowire-based services, pseudowire redundancy is supported, and MR-APS is enabled for redundant connectivity to the TDM-connected headend equipment.

### MPLS VPN-BGP FRR Edge Protection and VRRP

BGP FRR provides deterministic network reconvergence in the Connected Roadways System design. BGP FRR edge functionality is supported at the MPLS VPN service level. The following example illustrates how to configure BGP FRR edge from the MTG to the PAN across the MPLS Transport infrastructure.
The VRF configuration under the BGP process uses a unique route distinguisher (RD) per MTG. This unique RD configuration in each MTG, combined with the BGP and VRRP timer adjustments in MTG 1, enables the ability for the rest of the transport infrastructure to optimize MPLS VPN protection via BGP FRR. This RD does not have to match the route target defined for the MPLS VPN VRF. The need for this unique RD will be eliminated once support for BGP additional-paths received is implemented for BGP VPNv4 address-family configuration in IOS, thus allowing for multiple MTG information to be propagated for the MPLS VPN.

### Mobile Transport Gateway 1

#### VRF Configuration

```plaintext
vrf VPN102
  address-family ipv4 unicast
    import route-target 10:10
    export route-target 1001:1001

  address-family ipv6 unicast
    import route-target 10:10
    export route-target 1001:1001

interface TenGigE0/0/0/2.1100
  vrf VPN102
  ipv4 address 115.1.102.3 255.255.255.0
  ipv6 address 2001:115:1:102::3/64
  encapsulation dot1q 1100
```

#### VRRP Configuration

```plaintext
router vrrp
  interface TenGigE0/0/0/2.1100
    delay minimum 1 reload 240
    address-family ipv4
      vrrp 110
      priority 254
      timer msec 100 force
      address 115.1.102.1
    
  address-family ipv6
    vrrp 110
    priority 254
    timer msec 100 force
    address global 2001:115:1:102::1
    address linklocal autoconfig
```

BGP FRR Edge Configuration

router bgp 1000
  address-family vpnv4 unicast
  additional-paths receive
  additional-paths send
  additional-paths selection route-policy add-path-to-ibgp

vrf VPN102
  rd 1001:1001
  address-family ipv4 unicast
    redistribute connected
  !
  address-family ipv6 unicast
    redistribute connected
  !
  route-policy add-path-to-ibgp
  set path-selection backup 1 install
end-policy

Mobile Transport Gateway 2

VRF Configuration

vrf VPN102
  address-family ipv4 unicast
    import route-target
    10:10
    export route-target
    1001:1001
  !
  address-family ipv6 unicast
    import route-target
    10:10
    export route-target
    1001:1001
  !
  !
  interface TenGigE0/0/0/2.1100
    vrf VPN102
    ipv4 address 115.1.102.4 255.255.255.0
    ipv6 address 2001:115:1:102::4/64
    encapsulation dot1q 1100

VRRP Configuration

router vrrp
  interface TenGigE0/0/0/2.1100
  delay minimum 1 reload 240
  address-family ipv4
  vrrp 110
  priority 253
  timer msec 100 force
  address 115.1.102.1
Connected Roadways System

Chapter 7      System Implementation

High Availability Implementation

! address-family ipv6
   vrrp 110
   priority 253
   timer msec 100 force
   address global 2001:115:1:102::1
   address linklocal autoconfig

! BGP FRR Edge Configuration

router bgp 1000
  address-family vpnv4 unicast
  additional-paths receive
  additional-paths send
  additional-paths selection route-policy add-path-to-ibgp

! vrf VPN102
  rd 1001:1002
  address-family ipv4 unicast
  redistribute connected

! address-family ipv6 unicast
  redistribute connected

! route-policy add-path-to-ibgp
  set path-selection backup 1 install
end-policy

Core Route Reflector

router bgp 1000
  address-family vpnv4 unicast
  additional-paths receive
  additional-paths send
  additional-paths selection route-policy add-path-to-ibgp

! address-family vpnv6 unicast

! route-policy add-path-to-ibgp
  set path-selection backup 1 advertise install
end-policy

Pre-Aggregation Node

router bgp 1000
  address-family vpnv4
  bgp additional-paths install
  !***Enable CEF recursion for BGP host routes***
  bgp recursion host

! address-family vpnv6
  !***Enable CEF recursion for BGP host routes***
  bgp recursion host
Pseudowire Redundancy for TDM Services

High availability for TDM services transported via CEoP PWs is achieved through PW redundancy over the transport network, where a backup PW pointing to an alternate MTG is configured for each primary PW. Corresponding to these redundant PWs is MR-APS functionality on the TDM side of the MTGs, which provides redundant TDM connectivity to the headend equipment.

TDM Services

Figure 7-12 and the example that follows illustrate TDM services.

Pre-Aggregation Node Configuration

The only difference between CESoPSN and SAToP configuration is the lack of “control-word” in the pseudowire-class for SAToP configs.

```plaintext
pseudowire-class CESoPSN
  encapsulation mpls
  control-word
!
interface CEM0/0
  cem 0
  xconnect 100.111.15.1 13261501 encapsulation mpls pw-class CESoPSN
  backup peer 100.111.15.2 13261502 pw-class CESoPSN
!
interface Loopback0
  ip address 100.111.13.26 255.255.255.255
!
```

MPLS Transport Gateway 1 Configuration

```plaintext
aps group 1
  timers 10 15
  channel 0 remote 100.111.15.2
  channel 1 local SONET0/2/1/0
!
controller SONET0/2/1/0
  description To BSC
  ais-shut
  report lais
  report lrdi
  sts 1
  mode vt15-t1
  delay trigger 250
```
clock source line
!
controller T1 0/2/1/0/1/2/2
cem-group framed 0 timeslots 1-24
forward-alarm AIS
forward-alarm RAI
!
interface Loopback0
description Global Loopback
ipv4 address 100.111.15.1 255.255.255.255
!
l2vpn
!
pw-class CESoPSN
encapsulation mpls
control-word
!
! xconnect group TDM-K1326
p2p T1-CESoPSN-01
interface CEM0/2/1/0/1/2/0
neighbor ipv4 100.111.13.26 pw-id 13261501
pw-class CESoPSN
!
!
!

MPLS Transport Gateway 2 Configuration

aps group 1
revert 8
timers 10 15
channel 0 local SONET0/2/1/0
channel 1 remote 100.111.15.1
signaling sonet
!
controller SONET0/2/1/0
description To ONS15454-K1410 OC3 port 4/1
ais-shut
report lais
report lrdi
sts 1
mode vt15-t1
delay trigger 250
!
clock source line
!
controller T1 0/2/1/0/1/1/3
cem-group framed 0 timeslots 1-24
forward-alarm AIS
forward-alarm RAI
!
interface Loopback0
description Global Loopback
ipv4 address 100.111.15.2 255.255.255.255
!
l2vpn
!
pw-class CESoPSN
encapsulation mpls
control-word
OAM Implementation

This section describes the implementation of Operations, Administration, and Maintenance (OAM) protocols and Performance Management (PM) protocols in the Connected Roadways System design. These mechanisms enable the system to monitor the health of the transport infrastructure and the services transported over that infrastructure, and to alert the network administrator to any issues that arise.

Service OAM Implementation for L3VPN

The OAM and PM functions are configured between the PAN and MTG to monitor the end-to-end network performance of L3VPN services across the MPLS transport network.

The following OAM and PM functions are enabled on the initiator and responder in each case:

- IP ping and traceroute operations for MPLS Transport monitoring
- VRF-aware IP ping operations for connectivity check for traffic within MPLS VPNs
- IP SLA responder enabled on responder only for both native IP/MPLS and MPLS VPN deployments
- IP SLA User Datagram Protocol (UDP) echo probes configured on initiator for round-trip time (RTT) measurement
- IP SLA UDP jitter probe configured on initiator for one-way latency, packet loss, and packet delay variation measurement

Service OAM Implementation for TDM Circuit Emulation

The OAM and PM functions are configured between the PAN and MTG to monitor the end-to-end network performance of TDM CES across the MPLS transport network.

The following OAM and PM functions are enabled on the initiator and responder in each case:

- MPLS pseudowire ping and traceroute operations for connectivity check for TDM PWs
- IP SLA responder enabled on responder for TDM PW deployments. Loopback address of node is used for IP SLA measurements.
- IP SLA UDP echo probes configured on initiator for round-trip time (RTT) measurement
- IP SLA UDP jitter probe configured on initiator for one-way latency, packet loss, and packet delay variation measurement
Transport OAM

The following OAM and PM functions between the PAN and MTG allow for monitoring the transport network health and performance.

- IP ping and traceroute operations for verifying the data plane against control plane and for isolating faults within the MPLS transport network between the PANs and the MTG
- MPLS LSP ping and traceroute operations for verifying the data plane against control plane and for isolating faults within the core/aggregation domain

IP SLA Configuration

IP SLA Responder Configuration on PAN

The PAN act as IP SLA responders for different measurement scenarios. Minimal configuration is required for enabling the responder function.

```
ip sla responder
```

MPLS Transport Gateway Initiator Configuration for IP SLA

The MTG is configured with IP SLA probes for initiating measurement of packet loss, packet delay, and packet delay variation (for example, jitter) towards the PAN.

```
Note
The ToS values in IOS-XR are equal to four times the desired DSCP value.
```

VPN: Jitter Probes

```
ipsla
operation 6
type udp jitter
vrf VPN102
destination address 114.1.224.1
packet count 100
!***tos 184 = DSCP 46 (EF)***
tos 184
destination port 918
frequency 30
!
!
schedule operation 6
start-time now
life forever
!
!***Enabled IP SLA Responder***
responder
!
!```
Reaction Configuration

The reaction configuration defines the thresholds for the previously configured probes, and it defines the corresponding actions to be taken when those thresholds are exceeded. The following configuration shows a single example of a jitter probe reaction and an echo probe reaction.

```bash
ipsla
reaction operation 6
react connection-loss
action logging
action trigger
threshold type immediate
!
react jitter-average dest-to-source
action logging
action trigger
threshold type immediate
threshold lower-limit 10 upper-limit 15
!
react jitter-average source-to-dest
action logging
action trigger
threshold type immediate
threshold lower-limit 10 upper-limit 15
!
react packet-loss dest-to-source
action logging
action trigger
threshold type immediate
threshold lower-limit 3 upper-limit 5
!
!
```
Summary

This CVD has defined and described in detail a system architecture for Connected Roadways as part of the Cisco Connected Transportation System (CTS) portfolio. It includes design and best practice recommendations for a scalable and resilient multiservice transport infrastructure for any size and scale of deployment.

The Connected Roadways System design is based on a proven architecture deployed by dozens of major service providers around the world: Unified MPLS Transport. This design addresses the requirements of both legacy and next-generation services in a converged, scalable, and operationally simplified design. It provides transport of any service to any location over any type of access, providing maximum flexibility. It eliminates the need for service-specific networks or protocols, optimizing both capital and operating expenditures for the network infrastructure.
### Acronyms and Initialisms

Table A-1 lists the acronyms and initialisms used in this document.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>Assured Forwarding</td>
</tr>
<tr>
<td>APTA</td>
<td>American Public Transportation Association</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BE</td>
<td>Best Effort</td>
</tr>
<tr>
<td>BFD</td>
<td>Bidirectional Forwarding Detection</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>CE</td>
<td>customer edge</td>
</tr>
<tr>
<td>CEoP</td>
<td>circuit emulation over packet</td>
</tr>
<tr>
<td>CES</td>
<td>Circuit Emulation Services</td>
</tr>
<tr>
<td>CESoPSN</td>
<td>Circuit Emulation Services over Packet Switched Networks</td>
</tr>
<tr>
<td>CN</td>
<td>Core Node</td>
</tr>
<tr>
<td>CoS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>CoW</td>
<td>carbon dioxide</td>
</tr>
<tr>
<td>CTS</td>
<td>Connected Transportation System</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>EAN</td>
<td>Ethernet access node</td>
</tr>
<tr>
<td>EF</td>
<td>Expedited Forwarding</td>
</tr>
<tr>
<td>EPN</td>
<td>Evolved Programmable Network</td>
</tr>
<tr>
<td>EXP</td>
<td>Experimental</td>
</tr>
<tr>
<td>FAN</td>
<td>Fixed Asset Node</td>
</tr>
<tr>
<td>FRR</td>
<td>Fast Reroute</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>H-QoS</td>
<td>Hierarchical Quality of Service</td>
</tr>
<tr>
<td>ICCP</td>
<td>Inter-Chassis Control Protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System to Intermediate System</td>
</tr>
<tr>
<td>L2VPN</td>
<td>Layer 2 Virtual Private Network</td>
</tr>
<tr>
<td>L3VPN</td>
<td>Layer 3 Virtual Private Network</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDP</td>
<td>Label Distribution Protocol</td>
</tr>
<tr>
<td>LFA</td>
<td>Loop Free Alternate</td>
</tr>
<tr>
<td>LFIB</td>
<td>Label Forwarding Information Base</td>
</tr>
<tr>
<td>LSA</td>
<td>link-state advertisement</td>
</tr>
<tr>
<td>LSM</td>
<td>Label Switched Multicast</td>
</tr>
<tr>
<td>LSP</td>
<td>Label Switched Path</td>
</tr>
<tr>
<td>MC-LAG</td>
<td>Multi-Chassis Link Aggregation Group</td>
</tr>
<tr>
<td>MEF</td>
<td>Metro Ethernet Forum</td>
</tr>
<tr>
<td>mGRE</td>
<td>multicast Generic Route Encapsulation</td>
</tr>
<tr>
<td>mLACP</td>
<td>multi-chassis Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>mLDP</td>
<td>multicast Label Distribution Protocol</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MR-APS</td>
<td>Multirouter Automatic Protection Switching</td>
</tr>
<tr>
<td>MTG</td>
<td>MPLS Transport Gateway</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NGN</td>
<td>Next Generation Network</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
</tr>
<tr>
<td>NNI</td>
<td>network-to-network interface</td>
</tr>
<tr>
<td>OAM</td>
<td>Operations, Administration, and Maintenance</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>PAN</td>
<td>Pre-Aggregation Node</td>
</tr>
<tr>
<td>PE</td>
<td>Provider Edge</td>
</tr>
<tr>
<td>PHB</td>
<td>Per Hop Behavior</td>
</tr>
<tr>
<td>PIC</td>
<td>Prefix-Independent Convergence</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>PoA</td>
<td>Point-of-Attachment</td>
</tr>
<tr>
<td>PTC</td>
<td>Positive Train Control</td>
</tr>
<tr>
<td>PWE3</td>
<td>Pseudowire Emulation Edge to Edge</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>REP</td>
<td>Resilient Ethernet Protocol</td>
</tr>
<tr>
<td>rLFA</td>
<td>Remote Loop Free Alternate</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>RR</td>
<td>Route Reflector</td>
</tr>
<tr>
<td>RT</td>
<td>Route Target</td>
</tr>
<tr>
<td>RTT</td>
<td>round-trip time</td>
</tr>
<tr>
<td>SAToP</td>
<td>Structure Agnostic Transport over Packet</td>
</tr>
<tr>
<td>SDH</td>
<td>Synchronous Digital Hierarchy</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Networking</td>
</tr>
<tr>
<td>SPF</td>
<td>shortest-path first</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>TCN</td>
<td>Topology Change Notification</td>
</tr>
<tr>
<td>TDM</td>
<td>time-division multiplexing</td>
</tr>
<tr>
<td>TE</td>
<td>Traffic Engineering</td>
</tr>
<tr>
<td>TLV</td>
<td>time-length-value</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UNI</td>
<td>user network interface</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VRF</td>
<td>Virtual Routing and Forwarding</td>
</tr>
<tr>
<td>vRR</td>
<td>virtual route reflector</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
</tbody>
</table>