



NOT CISCO CONFIDENTIAL



UMMT 3.0 Design Guide Technical Paper

SDU-6432

Version 1.0

July 12, 2012



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

NOT CISCO CONFIDENTIAL

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE 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 THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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: 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.

UMMT 3.0 Design Guide Technical Paper © 1992-2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

Document Version and System Release	ix
Document Organization	x
Obtaining Documentation, Obtaining Support, and Security Guidelines	x
Cisco Product Security Overview	xi

CHAPTER 1

Introduction 1-1

1.1 Executive Summary	1-1
1.2 Release Notes	1-4

CHAPTER 2

Requirements 2-1

2.1 State of the Mobile Transport Industry	2-1
2.2 Next-Generation Mobile Transport Characteristics	2-2

CHAPTER 3

System Overview 3-1

3.1 System Concept	3-1
3.2 Transport Models	3-3
3.2.1 Flat LDP Core and Aggregation	3-5
3.2.2 Labeled BGP Access with Flat LDP Core and Aggregation	3-5
3.2.3 Labeled BGP Core and Aggregation	3-6
3.2.4 Labeled BGP Core, Aggregation, and Access	3-7
3.2.5 Labeled BGP Core and Aggregation with Redistribution into Access Network IGP	3-8
3.3 Service Models	3-9

CHAPTER 4

System Architecture 4-1

4.1 Transport Architecture	4-1
4.1.1 Large Network, Multi-Area IGP Design with IP/MPLS Access	4-1
4.1.2 Large Network, Inter-AS Design with IP/MPLS Access	4-5
4.1.3 Large Network, Multi-Area IGP Design with non-IP/MPLS Access	4-9
4.1.4 Large Network, Inter-AS Design with non-IP/MPLS Access	4-11
4.1.5 Small Network, Integrated Core and Aggregation with IP/MPLS Access	4-13
4.1.6 Small Network, Integrated Core and Aggregation with non-IP/MPLS Access	4-15

NOT CISCO CONFIDENTIAL

4.2	Service Architecture	4 - 15
4.2.1	L3 MPLS VPN Service Model for LTE	4 - 16
4.2.2	L2 MPLS VPN Service Model for 2G and 3G	4 - 20
4.2.3	Fixed-Mobile Convergence Use Case	4 - 21
4.3	Inter-Domain Hierarchical LSPs	4 - 23
4.3.1	Inter-Domain LSPs for Multi-Area IGP Design	4 - 23
4.3.2	Inter-Domain LSPs for Inter-AS Design	4 - 27
4.3.3	Inter-Domain LSPs for Integrated Core and Aggregation Design	4 - 31
4.4	Transport and Service Control Plane	4 - 33
4.4.1	BGP Control Plane for Multi-Area IGP Design	4 - 33
4.4.2	BGP Control Plane for Inter-AS Design	4 - 35
4.4.3	BGP Control Plane for Integrated Core and Aggregation Design	4 - 38
4.5	Prefix Filtering	4 - 39
4.6	Scale Considerations	4 - 41

CHAPTER 5

Functional Components 5 - 1

5.1	Quality of Service	5 - 1
5.2	Synchronization Distribution	5 - 5
5.3	Redundancy and High Availability	5 - 7
5.4	OAM and Performance Monitoring	5 - 9
5.5	Network Management with Cisco Prime	5 - 10

CHAPTER 6

Conclusion 6 - 1

CHAPTER 7

Related Documents 7 - 1

GLOSSARY

Glossary GL - 1



FIGURES

<i>Figure 1-1</i>	Cisco Unified MPLS for Mobile Transport System	1 - 2
<i>Figure 1-2</i>	UMMT System Components	1 - 3
<i>Figure 2-1</i>	Cisco VNI: Global Mobile Data Traffic, 2011 to 2016	2 - 3
<i>Figure 2-2</i>	Macro Cell Capacity	2 - 4
<i>Figure 2-3</i>	RAN Backhaul Architecture	2 - 5
<i>Figure 3-1</i>	Flat LDP Core and Aggregation	3 - 5
<i>Figure 3-2</i>	Labeled BGP Access with Flat LDP Core and Aggregation	3 - 6
<i>Figure 3-3</i>	Labeled BGP Core and Aggregation	3 - 6
<i>Figure 3-4</i>	Labeled BGP Core, Aggregation, and Access	3 - 7
<i>Figure 3-5</i>	Labeled BGP Core and Aggregation with Redistribution into Access Network IGP	3 - 8
<i>Figure 3-6</i>	Mobile Backhaul Services	3 - 9
<i>Figure 4-1</i>	Multi-Area IGP/LDP Domain Organization	4 - 2
<i>Figure 4-2</i>	Inter-Domain Transport for Multi-Area IGP Design with Labeled BGP Access	4 - 3
<i>Figure 4-3</i>	Inter-Domain Transport for Multi-Area IGP Design with IGP/LDP Access	4 - 4
<i>Figure 4-4</i>	Inter-AS IGP/LDP Domain Organization	4 - 6
<i>Figure 4-5</i>	Inter-Domain Transport for Inter-AS Design with Labeled BGP Access	4 - 7
<i>Figure 4-6</i>	Inter-Domain Transport for Inter-AS Design with IGP/LDP Access	4 - 8
<i>Figure 4-7</i>	Multi-Area IGP/LDP Domain Organization	4 - 10
<i>Figure 4-8</i>	Inter-Domain Transport with Hierarchical LSPs	4 - 10
<i>Figure 4-9</i>	Inter-AS IGP/LDP Domain Organization	4 - 11
<i>Figure 4-10</i>	Inter-Domain Transport with Hierarchical LSPs	4 - 12
<i>Figure 4-11</i>	Integrated Core and Aggregation with IP/MPLS Access	4 - 13
<i>Figure 4-12</i>	Inter-Domain Transport for Labeled BGP Access with Flat LDP Core and Aggregation	4 - 14
<i>Figure 4-13</i>	Single-Area IGP with Flat LDP Core and Aggregation	4 - 15
<i>Figure 4-14</i>	LTE Backhaul Service	4 - 16
<i>Figure 4-15</i>	L3 MPLS VPN Service Model	4 - 17
<i>Figure 4-16</i>	Inter-Access X2 Connectivity	4 - 19
<i>Figure 4-17</i>	ATM/TDM Transport Services	4 - 20
<i>Figure 4-18</i>	Wireline VPWS Service between CSGs across the Core Network	4 - 21
<i>Figure 4-19</i>	Scalability Control for Fixed-Mobile Converged Deployments	4 - 22
<i>Figure 4-20</i>	Hierarchical LSPs between Remote PANs for Multi-Area IGP Design	4 - 24
<i>Figure 4-21</i>	Hierarchical LSPs between CSGs and MTGs for Multi-Area IGP Design with Labeled BGP Access	4 - 25
<i>Figure 4-22</i>	Hierarchical LSPs between CSGs and MTGs for Multi-Area IGP Design with IGP/LDP Access	4 - 26
<i>Figure 4-23</i>	Hierarchical LSPs between Remote PANs for Inter-AS Design	4 - 28
<i>Figure 4-24</i>	Hierarchical LSPs between CSGs and MTGs for Inter-AS Design with Labeled BGP Access	4 - 29

NOT CISCO CONFIDENTIAL

<i>Figure 4-25</i>	Hierarchical LSPs between CSGs and MTGs for Inter-AS Design with IGP/LDP Access	4 - 30
<i>Figure 4-26</i>	Hierarchical LSPs between CSGs and MTGs for Integrated Core and Aggregation Design	4 - 32
<i>Figure 4-27</i>	BGP Control Plane for Multi-Area IGP Design with Labeled BGP Access	4 - 33
<i>Figure 4-28</i>	BGP Control Plane for Multi-Area IGP Design with IGP/LDP Access	4 - 35
<i>Figure 4-29</i>	BGP Control Plane for Inter-AS Design with Labeled BGP Access	4 - 36
<i>Figure 4-30</i>	BGP Control Plane for Inter-AS Design with IGP/LDP Access	4 - 37
<i>Figure 4-31</i>	BGP Control Plane for Integrated Core and Aggregation Design with Labeled BGP Access	4 - 38
<i>Figure 4-32</i>	BGP-Community based Coloring of Transport Prefixes	4 - 39
<i>Figure 4-33</i>	BGP Extended Community-based Coloring of Service Prefixes	4 - 41
<i>Figure 4-34</i>	UMMT Hierarchical Network	4 - 43
<i>Figure 4-35</i>	UMMT Hierarchical RR Topology	4 - 44
<i>Figure 5-1</i>	UMMT System Upstream QoS Model	5 - 2
<i>Figure 5-2</i>	UMMT System Downstream QoS Model	5 - 3
<i>Figure 5-3</i>	UMMT System DiffServ QoS Domain	5 - 4
<i>Figure 5-4</i>	Synchronization Distribution	5 - 6
<i>Figure 5-5</i>	UMMT High Availability Overview	5 - 8
<i>Figure 5-6</i>	OAM Protocol Positioning	5 - 10



TABLES

<i>Table i-1</i>	Document Version	i - ix	
<i>Table i-2</i>	Document Organization	i - x	
<i>Table 1-1</i>	UMMT 3.0 Platforms and Software Versions		1 - 5
<i>Table 1-2</i>	UMMT 2.0 Platforms and Software Versions		1 - 6
<i>Table 1-3</i>	UMMT 1.0 Platforms and Software Versions		1 - 6
<i>Table 3-1</i>	UMMT Transport Models	3 - 5	
<i>Table 4-1</i>	Network Sizing	4 - 42	
<i>Table 4-2</i>	Route Scale	4 - 43	
<i>Table 4-3</i>	BGP Session Scale	4 - 45	



Preface

The huge growth in mobile data traffic is challenging legacy network infrastructure capabilities and forcing transformation of mobile transport networks. Until now, mobile backhaul networks have been composed of a mixture of many legacy technologies that are operationally complex and have reached the end of their useful life. The market inflection point for mobile backhaul is introduction of 4G/LTE. The majority of deployments require concurrent legacy (2G/3G radio) backhaul support while gracefully introducing long term evolution (LTE) to the service mix, along with virtualization of the packet transport to deliver multiple services.

The Unified MPLS Mobile Transport (UMMT) System is a comprehensive RAN backhaul solution that forms the foundation for LTE backhaul, while integrating components necessary for continued support of legacy 2G GSM and existing 3G UMTS transport services. The UMMT System enables a comprehensive and flexible framework that integrates key technologies from Cisco's Unified MPLS suite of technologies to deliver a highly scalable and simple-to-operate MPLS-based RAN backhaul network.

This preface includes the following major topics:

- [Document Version and System Release](#)
- [Document Organization](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)
- [Cisco Product Security Overview](#)

Document Version and System Release

This is the UMMT System Release 3.0 Design Guide.

Document Version

[Table i-1](#) lists document version information.

Table i-1. Document Version

Document Version	Date	Notes
1	7/11/2012	Initial release.

System Release

UMMT System Release 3.0 covers Unified MPLS for Mobile Transport supporting LTE and the introduction of ASR 901.

NOT CISCO CONFIDENTIAL

Document Organization

The chapters in this document are described in [Table i-2](#).

Table i-2. Document Organization

Chapter	Major Topics
Chapter 1, Introduction	Includes an executive summary of UMMT 3.0 and release notes.
Chapter 2, Requirements	Provides an overview of the state of the mobile transport industry and characteristics of next-generation mobile transport.
Chapter 3, System Overview	Provides an overview of the UMMT 3.0 concept, and transport architecture and mobile backhaul service models.
Chapter 4, System Architecture	Describes the UMMT 3.0 architectures: transport architecture, service models, inter-domain hierarchical LSPs, transport and service control plane, prefix filtering, and scale considerations.
Chapter 5, Functional Components	Describes the UMMT 3.0 functional components: QoS, synchronization distribution, redundancy and high availability, OAM and performance monitoring, and network management with Cisco Prime.
Chapter 6, Conclusion	Describes highlights and benefits summary for UMMT 3.0.
Chapter 7, Related Documents	Describes the full array of UMMT 3.0 documentation available for download.
Glossary	List of acronyms and initialisms used in this document.

Obtaining Documentation, Obtaining Support, and Security Guidelines

Specific information about UMMT can be obtained at the following locations:

- Cisco ASR 901 Series Aggregation Services Routers: <http://www.cisco.com/en/US/products/ps12077/index.html>
- Cisco ASR 903 Series Aggregation Services Routers: <http://www.cisco.com/en/US/products/ps11610/index.html>
- Cisco ME 3600X Series Ethernet Access Switches: <http://www.cisco.com/en/US/partner/products/ps10956/index.html>
- Cisco ME 3800X Series Carrier Ethernet Switch Routers: <http://www.cisco.com/en/US/products/ps10965/index.html>
- Cisco ASR 9000 Series Aggregation Services Routers: <http://www.cisco.com/en/US/products/ps9853/index.html>
- Cisco Carrier Routing System: <http://www.cisco.com/en/US/products/ps5763/index.html>

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

NOT CISCO CONFIDENTIAL

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.

NOT CISCO CONFIDENTIAL



CHAPTER 1

Introduction

This chapter includes the following major topics:

- [Section 1.1 Executive Summary](#)
- [Section 1.2 Release Notes for UMMT System Release 3.0](#)

1.1 Executive Summary

Infused with intelligence and select solutions for scalability, agile transport, security, and more, the Cisco® Unified MPLS for Mobile Transport System gives operators a proven architecture, platforms, and solutions to stay ahead of the curve for bandwidth demand and provide operational simplification, all at optimized cost points.

Cisco UMMT is a comprehensive RAN backhaul solution that forms the foundation for LTE service deployment while integrating components necessary to support legacy 2G and 3G transport services. It provides flexible cell site connectivity options, including integration of third-party microwave vendors. It supports both retail and wholesale backhaul options, and concurrent transport for residential and business services traffic over the same infrastructure.

Challenge

While voice calls and texting used to dominate the mobile network market, mobile multimedia devices such as tablet computers and smartphones are now ubiquitous, running a wide variety of bandwidth-intensive applications and creating unprecedented growth in mobile data traffic. To remain competitive, operators that supply transport for mobile traffic must continue to scale network throughput and performance, support legacy 2G/3G services and flexible any-to-any connectivity for LTE, and leverage fiber and microwave assets to the maximum extent possible.

The Cisco Visual Networking Index (VNI) Global Mobile Data Forecast 2011-2016 states that 2016 global mobile traffic will be eighteen times greater than it was in 2010. Over ten billion mobile devices will be in use by 2016, and sixty-six percent of mobile traffic will be video, with its related high bandwidth and quality of service (QoS) demands. Aggregate traffic is expected to exceed ten exabytes per month by 2016, an annual run rate of over 120 exabytes per year. This equates to roughly 30 billion DVDs or 839 quadrillion SMS text messages.

This huge growth is challenging legacy network infrastructure capabilities and forcing transformation of mobile network infrastructures. The mobile network is evolving to an all-IP network with greater cost efficiency in bandwidth scaling. New transport requirements, driven by the dramatic growth in data rates and new communication streams within the backhaul network, must be simultaneously accommodated. The key LTE interfaces that must be supported are X2 and S1:

NOT CISCO CONFIDENTIAL

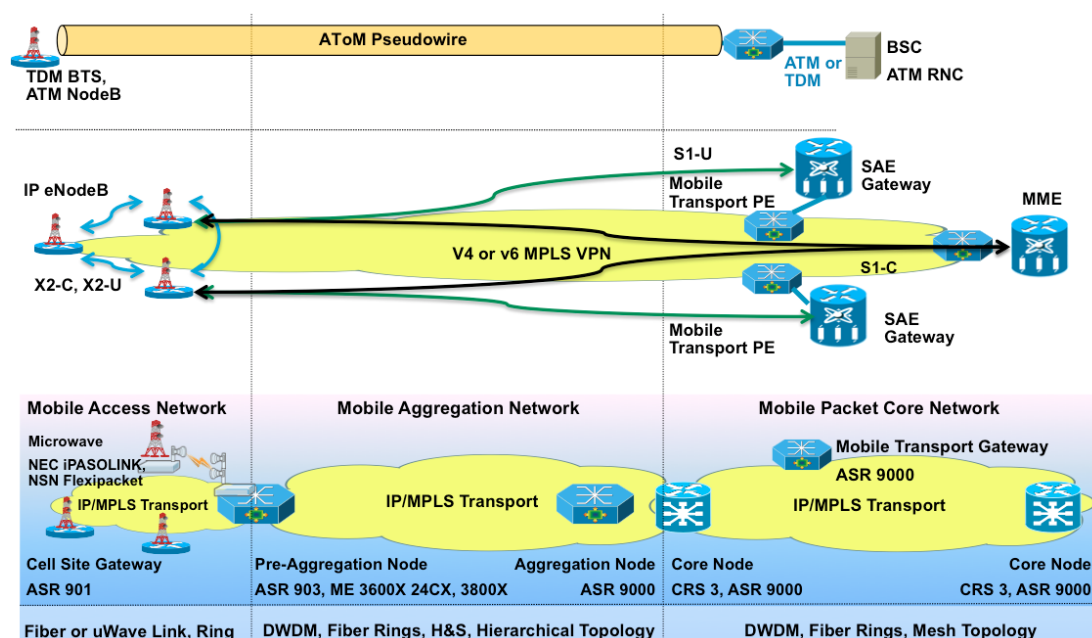
- The X2 interface requires a cell site-to-cell site communication path to support call handover for fast-moving mobile devices, for which the centralized circuit paradigms of previous RAN architectures are ill suited.
- The S1 interface requires communication from the cell site to a centralized MME for user control.

To allow for growth in LTE adoption, users and cell site locations will need to be moved from heavily utilized gateways (e.g., mobility management entity (MME) and system architecture evolution (SAE)) to new, less centralized gateways. UMMT provides the capabilities for these changes to happen without re-architecting the underlying transport network.

Solution

UMMT provides reliable, scalable, high-density packet processing that addresses mass market adoption while reducing the operator's total cost of operation (TCO). It also handles the complexities of multiple access technologies, including seamless handover and mobility between access networks (2G, 3G, 4G LTE, and WiFi) to meet demands for convergence, product consolidation, and a common end user service experience.

Figure 1-1. Cisco Unified MPLS for Mobile Transport System



UMMT introduces key technologies from Cisco's Unified MPLS suite of technologies to deliver highly scalable and simple-to-operate MPLS-based IP RAN backhaul networks. For RAN backhaul of LTE services, operators are adopting MPLS over pure IP for two main reasons:

- Investment in packet-based networks delivers an economic solution to the exponential growth in packet traffic that needs transport. While the future lies with LTE, the present only offers 2G and 3G cell site connectivity. Support for asynchronous transfer mode (ATM) and time-division multiplexing (TDM) traffic inherent in legacy networks must exist in order to move traffic to the new higher-capacity LTE networks. The MPLS pseudowire is the industry choice for achieving this over a packet infrastructure.
- Layer 3 (L3) multi-protocol label switching (MPLS) VPNs in the RAN backhaul, which facilitate virtualization of the transport infrastructure, are becoming common in LTE designs. This is

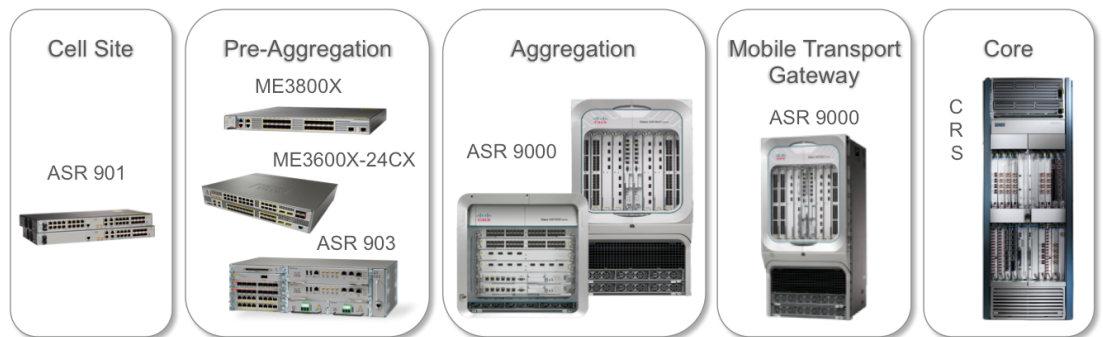
NOT CISCO CONFIDENTIAL

useful when offering wholesale transport. It also leverages the RAN backhaul network for transport to other services for business and residential consumers.

Unified MPLS resolves legacy challenges such as scaling MPLS to support tens of thousands of end nodes, which provides the required MPLS functionality on cost-effective platforms, and the complexity of technologies like traffic engineering fast reroute (TE-FRR) to meet transport SLAs.

By addressing the scale, operational simplification, and cost of the MPLS platform, UMMT resolves the immediate need to deploy an architecture that is suitable for LTE deployment.

Figure 1-2. UMMT System Components



UMMT Highlights

- **Decoupling of transport and service layers.** Enables end-to-end MPLS transport for any service, at any scale. Optimal service delivery to any location in the network is unrestricted by physical topological boundaries.
- **Scaling of the MPLS infrastructure using RFC 3107 hierarchical LSPs.** RFC 3107 procedures define the use of Border Gateway Protocol (BGP) to distribute labels such that BGP can split up large routing domains to manageable sizes, yet still retain end-to-end connectivity.
- **Improved high availability.** Multi-Router Automatic Protection Switching (MR-APS), pseudowire redundancy, remote Loop-Free Alternate (LFA) to support arbitrary topologies in access and aggregation to delivery zero configuration 50msec convergence and labelled BGP Prefix-Independent Convergence (PIC) for edge and core.
- **Simplified provisioning of mobile and wireline services.** New service activation requires only end point configuration.
- **Highly-scaled MPLS VPNs support transport virtualization.** This enables a single fiber infrastructure to be re-utilized to deliver transport to multiple entities, including mobile for retail and wholesale applications, residential, and business services. This enables the one physical infrastructure to support multiple VPNs for LTE and wireline services.
- **TDM circuit support.** Addition of TDM transport over packet for the Global System for Mobile Communications (GSM) Abis interface.
- **ATM circuit support.** Addition of ATM transport over packet for 3g Iub support.
- **Microwave support.** Full validation and deployment recommendations for Cisco's two main microwave partners: NEC (with their iPASOLINK product) and NSN (with their Flexipacket offering).
- **Synchronization distribution.** A comprehensive synchronization scheme is supported for both frequent and phase synchronization. Synchronous Ethernet is used in the core, aggregation, and access domains where possible. Where SyncE may not be possible, based on the transmission

NOT CISCO CONFIDENTIAL

medium, a hybrid mechanism is deployed converting SynchE to IEEE 1588v2 timing. IEEE 1588v2 Boundary Clock (BC) function in the aggregation to provide greater scalability. UMMT now supports Hybrid SyncE and Precision Time Protocol (PTP) with 1588 BC across all network layers.

- **QoS.** UMMT leverages DiffServ QoS for core and aggregation, H-QoS for microwave access and customer-facing SLAs, and support for LTE QoS class identifier (QCIs) and wireline services, to deliver a comprehensive QoS design.
- **OAM and Performance Monitoring.** Operation, Administration, and Maintenance (OAM) and Performance Management for Label-Switched Protocol (LSP) Transport, MPLS VPN, and virtual private wire service (VPWS) services are based on IP SLA, PW OAM, MPLS and MPLS OAM, and future Internet Engineering Task Force (IETF) MPLS PM enhancements.
- **LFA for FRR capabilities.** The required 50ms convergence time inherent in Synchronous Optical Networking/Synchronous Digital Hierarchy (SONET/SDH) operations used to be achieved in packet networks with MPLS TE-FRR. This has been successfully deployed in core networks, but not in access networks due to the complexity of additional required protocols and overall design. LFA delivers the same fast convergence for link or node failures without any new protocols or explicit configuration on a network device. Hub-and-spoke topologies are currently supported, with a later release extending LFA coverage to arbitrary topologies.

Until now, mobile network infrastructures have been composed of a mixture of many legacy technologies that have reached the end of their useful life. The UMMT system architecture provides the first integrated, tested, and validated mobile network architecture, meeting all the demands of legacy and highly scaled any-to-any connectivity for LTE networks.

UMMT Benefits

- **Flexible deployment options for multiple platforms** to optimally meet size and throughput requirements of differing networks.
- **High-performance solution**, utilizing the highest capacity Ethernet aggregation routers in the industry. The components of this system can be in service for decades to come.
- **Tested and validated reference architecture** that allows operators to leverage a pre-packaged framework for different traffic profiles and subscriber services.
- Promotes **significant capital savings** from various unique features such as pre-tested solutions, benchmarked performance levels, and robust interoperability, all of which are validated and pre-packaged for immediate deployment.
- Enables **accelerated time-to-market** based on a pre-validated, turnkey LTE RAN backhaul system.
- **Complementary system support**, with mobile video transport optimization integration; I-WLAN untrusted offload support on the same architecture; Mobile Packet Core (MPC); and cost-optimized performance for Voice over LTE (VoLTE), plus additional services such as Rich Communication Suite (RCS).
- **Cisco's IP expertise is available to operators deploying UMMT through Cisco Services.** These solutions include physical tools, applications, and resources plus training and annual assessments designed to suggest improvements to the operator's network.

1.2 Release Notes

These release notes outline the hardware and software versions validated as part of the UMMT System effort and the key advancements of each system release.

UMMT 3.0

Release 3.0 of the Cisco UMMT system architecture further builds upon the architecture defined in the first two releases with the addition of the following improvements:

- New Unified MPLS models;
 - Labeled BGP Access. Provides highest scalability plus wireline coexistence.
 - v6VPN for LTE transport.
- IEEE 1588v2 Boundary Clock and SyncE/1588v2 Hybrid models:
 - Greater scalability and resiliency for packet-based timing in access and aggregation.
- ATM/TDM transport end-to-end:
 - ATM provides transport for legacy 3G services.
 - PW redundancy with MR-APS.
- New network availability models:
 - Remote LFA FRR.
 - Labeled BGP PIC core and edge.
 - MPLS VPN BGP PIC edge.
 - Most comprehensive resiliency functionality.
- ME3600X-24CX platform:
 - 2RU fixed-configuration 40Gb/s platform.
 - Supports Ethernet and TDM interfaces.
- Network Management, service management, and assurance with Prime.

Table 1-1. UMMT 3.0 Platforms and Software Versions

Architectural Role	Hardware	Software Revision
Core Node	ASR 9000	XR 4.2.1 / 4.3.0
	CRS-3	XR 4.2.1
Aggregation Node	ASR 9000	XR 4.2.1 / 4.3.0
Pre-Aggregation Node	ASR 903	XE 3.7 / 3.8
	ME 3600X-24CX	15.2(2)S1
Cell Site Gateway (CSG)	ASR 901	15.2(2)SNG
Mobile Transport Gateway (MTG)	ASR 9000	XR 4.2.1 / 4.3.0
Network Management	PRIME Management Suite	1.1

UMMT 2.0

Release 2.0 of the Cisco UMMT system architecture continues to build upon the baseline established by release 1.0 by implementing the following improvements:

- Introduction of ASR 903 modular platform as a pre-aggregation node.

NOT CISCO CONFIDENTIAL

- Any Transport over MPLS (AToM): Complete TDM transport capabilities in access and aggregation domains with Circuit Emulation over Packet Switching Network (CESoPSN) and Structure Agnostic Transport over Packet (SAToP) TDM Circuit Emulation over Packet (CEoP) services on the ASR 903 and ASR 9000 platforms.
- 200Gbps/Slot line cards and new supervisor cards for the ASR 9000, which bring increased scalability, 100G Ethernet support, and synchronization enhancements with 1588 BC support.
- BGP PIC edge and core on ASR 9000 for labeled Unicast.
- Microwave partnerships with NEC and NSN.

Table 1-2. UMMT 2.0 Platforms and Software Versions

Architectural Role	Hardware	Software Revision
Core Node	ASR 9000	XR 4.2
	CRS-3	XR 4.2
Aggregation Node	ASR 9000	XR 4.2
Pre-Aggregation Node	ASR 903	XE 3.5.1.S
	ME3800X	15.1(2.0.47)EY0
Cell Site Gateway (CSG)	ASR 901	15.1(2)SNH
Mobile Transport Gateway (MTG)	ASR 9000	XR 4.2
Packet Microwave	NSN FlexiPacket	2.4
Hybrid Microwave	NEC iPASOLINK	2.02.29

UMMT 1.0

The first release of the Cisco UMMT System architecture formed the baseline for a highly-scalable and operationally-simplified system architecture to deliver mobile backhaul services:

- Introduction of RFC3107-compliant labeled BGP control plane in the access, aggregation, and core network domains.
- Introduction of hierarchical LSP functionality to provide abstraction between transport and service layers.
- MPLS L3VPN-based backhaul of S1 and X2 interfaces for LTE deployment.
- Simplified provisioning of mobile backhaul services enabled by BGP-based control plane. Only endpoint configuration needed for service enablement.
- LFA functionality provides FRR capabilities in a greatly operationally-simplified manner.
- End-to-end OAM and PM functionality for mobile backhaul services and transport layer.

Table 1-3. UMMT 1.0 Platforms and Software Versions

Architectural Role	Hardware	Software Revision
Core Node	ASR 9000	IOS-XR 4.1.1

NOT CISCO CONFIDENTIAL

Architectural Role	Hardware	Software Revision
	CRS	IOS-XR 4.1.1
Aggregation Node	ASR 9000	IOS-XR 4.1.1
Pre-Aggregation Node	ME3800X	IOS 15.1(2)EY1
Cell Site Gateway (CSG)	MWR2941	IOS 15.1(1)MR
	ASR 901	IOS 15.1(2)SNG
Mobile Transport Gateway (MTG)	ASR 9000	XR 4.1.1

NOT CISCO CONFIDENTIAL



Requirements

This chapter includes the following major topics:

- [Section 2.1 State of Mobile Transport Industry](#)
- [Section 2.2 Next-Generation Mobile Transport Characteristics](#)

2.1 State of the Mobile Transport Industry

The shift from the dominance of mobile voice calls to mobile data has led to a fundamental change in the mobile service mix. As mobile standards evolved from 2G to 3G and now to 4G, mobile operators are under constant pressure to improve mobile backhaul speed, scale, and QoS, while having the difficult task of controlling and reducing the cost per bit in the transport network. Legacy 2G and 3G transport is mostly synchronous digital hierarchy (SDH) based using dedicated T1/E1 circuits for GSM (TDM) and Universal Mobile Telecommunications System (UMTS) (ATM) backhaul. However, the rollout of mobile broadband standards such as High Speed Packet Access (HSPA) and Evolution Data Only Optimized (EV-DO) made it clear that the underlying SDH infrastructure could no longer cost effectively scale at the increased traffic volumes, and triggered the migration of mobile backhaul to packet networks. The debate between circuit versus packet transport has been laid to rest as packet transport is universally accepted as the best solution for next generation mobile transport. As a result, all new 3G rollout has been based on IP transport over Ethernet interfaces, and mobile operators are transitioning their backhaul infrastructure to packet networks.

Current industry solutions for RAN backhaul built on packet transport face the following issues:

Operational Complexity

Mobile standards have evolved over different transport technologies. While L3 packet transport has been predominant in the core and to a large extent in the aggregation domains of the network, the access network buildout has largely been based on Layer 2 (L2) transport. Consequently, industry solutions for RAN backhaul have been based on mixed packet transport technologies across the access, aggregation, and core layers of the network. These solutions typically involve a combination of L2 and L3 transport, with a L2 access and aggregation interfacing with a L3 core, or a L2 access interfacing with a L3 aggregation and core. Such architectures intrinsically couple the transport and service layers of the network and are consequently plagued with both control and management plane translations at the boundaries of these network domains:

- In mixed L2/L3 environments, increased complexity occurs in the control plane when MPLS RAN transport that uses pseudowire emulation (CESoPSN, SAToP, and ATM virtual channel and virtual path) for 2G/3G services is built over bridged infrastructures that rely solely on the L2 topology protection.

NOT CISCO CONFIDENTIAL

- Often interworking functions like multi-segment pseudowire (MSPW) stitching, VLAN to pseudowire (PW) XConnect, VLAN into VPLS VFI, spoke PW into H-VPLS VFI hub, or spoke PW into MPLS VPN virtual routing and forwarding (VRF) are required at the boundaries of these domains to provide the end-to-end services. These interworking entities are essentially touchpoints for the service that consume resources on the network device deployed at this boundary.
- These intermediate touchpoints introduce management complexity and require repeated provisioning as new services are added to the network.
- The intermediate touchpoints also complicate the operation and management of the service since they do not allow for simple end-to-end service monitoring and require separate L2 and L3 OAM technologies to be used in the respective segments of the service.

Short-Reach of Legacy RAN Backhaul

Existing industry solutions have been tailored to meet the immediate needs of 2G or 3G transport, which entails connectivity from the base transceiver station (BTS)/NodeB to the base station controller (BSC)/radio network controller (RNC). Therefore, the focus of backhaul thus far has been restricted to providing connectivity from the cell site to the controller located somewhere in the aggregation network, without considering implications to the MPC. While the limited reach of these backhaul designs suits the hierarchical nature of legacy 2G and 3G mobile standards, they have significant shortcomings for LTE deployments. The transition from a hierarchical 3G network architecture to a flat all-IP LTE/evolved packet core (EPC) network architecture has profound implications to the mobile transport network. LTE mandates reachability from the cell site all the way to the EPC gateways located deep in the core network. Extending the existing backhaul designs with interworking functions to provide reachability into the packet core will only introduce operational complexity and defeats the benefit that the flattened all-IP LTE/EPC architecture brings to mobile backhaul. These designs handicap the flexible placement of mobile gateways across the core network to address the gradual uptake in 4G scale as subscribers move from existing 2G and 3G services.

Lack of Consideration for Fixed Mobile Convergence

The biggest cost challenge facing MSPs today is the backhaul network. With circuit-to-packet migration being well under way, mobile operators are making huge investments in the rollout of packet-based networks. To this end, operators wanting to capitalize on their return on investment are looking to provide additional services on a converged network. In many cases, SPs are exploring the option of deploying fixed wireline services alongside 4G RAN backhaul in order to achieving fixed mobile convergence. The transport architecture plays a critical role in attaining this goal. However, existing industry solutions, which have been purpose built for legacy RAN backhaul with the transport architecture essentially following the circuit-switched paradigm of hub-and-spoke connectivity from cell sites to centrally located radio controllers, are not conducive to meeting the active convergence of packet transport in fixed mobile operations.

2.2 Next-Generation Mobile Transport Characteristics

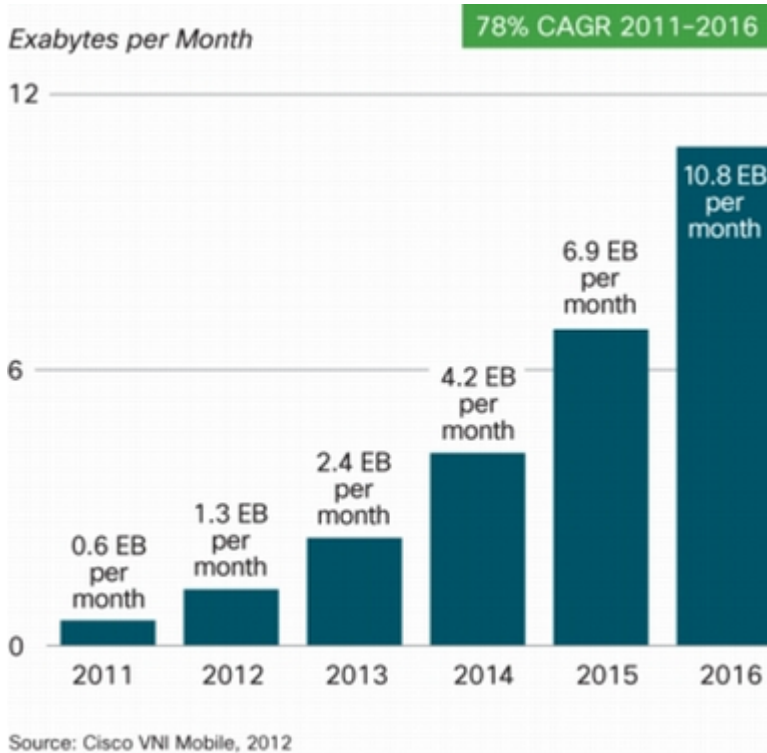
The next-generation mobile backhaul infrastructure has the following characteristics:

High Capacity Requirements from Edge to Core

The mobile landscape is changing with consumer behavior. Powerful new mobile devices, increasing use of mobile Internet access, and a growing range of data-hungry applications for music, video, gaming, and social networking are driving huge increases in data traffic. The 2012 Cisco VNI states that global mobile data traffic grew 2.3-fold in 2011, more than doubling for the fourth year in a row. Global mobile data traffic in 2011 was over eight times greater than the total global Internet traffic in 2000, and mobile network connection speeds grew 66 percent, with a 4G connection generating 28 times more traffic on average than a non-4G connection. The VNI forecasts that mobile data traffic is set to increase 18-fold globally between 2011 and 2016. These exploding bandwidth requirements

are driving high capacity requirements from the edge to the core with typical rates of 100Mbps per eNodeB, 1Gbps access, 10Gbps aggregation, and future 100Gbps core networks.

Figure 2-1. Cisco VNI: Global Mobile Data Traffic, 2011 to 2016

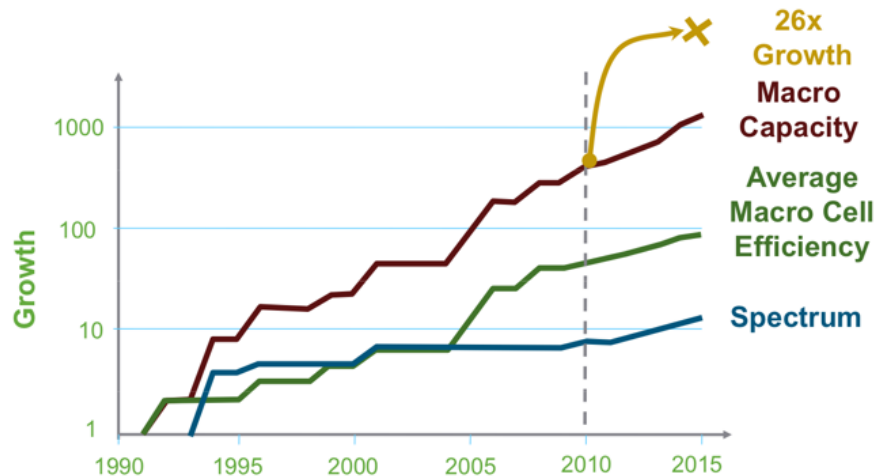


Exponential Increase in Scale Driven by LTE Deployments

LTE will drive ubiquitous mobile broadband with its quantum leap in uplink and downlink transmission speeds.

- In denser populations, the **increased data rates** delivered to each subscriber will force division of the cell capacity among fewer users. Because of this, cells must be much smaller than they are today.
- Another factor to consider is the **macro cell capacity**. The spectrum allotted to mobile networks has been increasing over the years, roughly doubling over a five year period. With advancements in radio technology, a corresponding increase in average macro cell efficiency has occurred over the same period. As a result, the macro cell capacity, which is a product of these two entities, will see a four-fold increase over a five year period. This increase, however, is nowhere close to the projected 26-fold increase in mobile data (as stated above), and will force mobile operators to deploy a small-cell network architecture.

These two factors will force operators to adopt small cell architectures, resulting in an exponential increase in cell sites deployed in the network. In large networks covering large geographies, the scale is expected to be in the order of several tens of thousands to a few hundred thousands of LTE eNodeBs and associated CSGs.

Figure 2-2. Macro Cell Capacity

Source: Agilent

Support for Multiple and Mixed Topologies

Many options exist for physical topologies in the RAN transport network, with hub-and-spoke and ring being the most prevalent. Capacity requirements driven by subscriber density, CAPEX of deploying fiber in large geographies, and physical link redundancy considerations could lead to a combination of fiber and microwave rings in access, fiber rings, and hub-and-spoke in aggregation and core networks, etc. The transport technology that implements the RAN backhaul must be independent of the physical topology, or combination thereof, used in various layers of the network, and must cost-effectively scale to accommodate the explosive increase in bandwidth requirements imposed by the mobile growth.

Seamless Interworking with the Mobile Packet Core

As mentioned in the previous section, the flattened all-IP LTE/EPC architecture is a significant departure from previous generations of mobile standards and should be an important consideration in designing the RAN backhaul for 4G mobile transport.

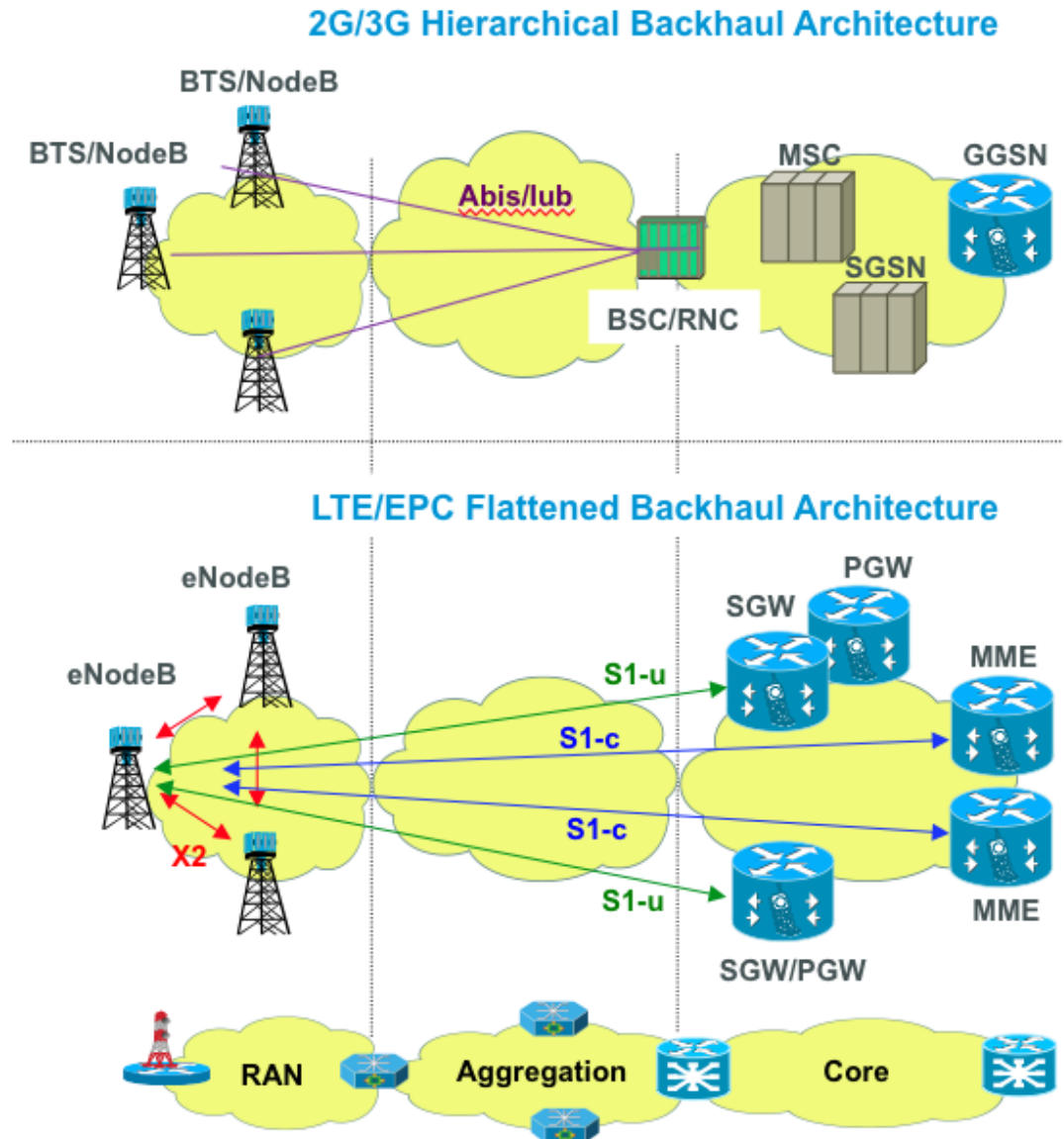
The 2G, 3G hierarchical architecture consists of a logical hub-and-spoke connectivity between BSC/RNC and the BTS/NodeBs. This hierarchical architecture lent itself naturally to the circuit-switched paradigm of having point-to-point connectivity between the cell sites and controllers. The reach of the RAN backhaul was also limited in that it extended from the radio access network to the local aggregation/distribution location where the controllers were situated.

In contrast, the flat LTE architecture does away with the hierarchy by getting rid of the intermediate controller like the BSC/RNC and lets the eNodeB communicate directly with the EPC gateways. It also does away with the point-to-point relationship of 2G, 3G architectures and imposes multipoint connectivity requirements at the cell site. This multipoint transport requirement from the cell site not only applies to the LTE X2 interface, which introduces direct communication between eNodeBs requiring any-to-any mesh network connectivity, but also applies to the LTE S1 interface, which requires a one-to-many relationship between the eNodeB and multiple EPC gateways. While the serving gateways (SGWs) may be deployed in a distributed manner closer to the aggregation network, the MMEs are usually fewer in number and centrally located in the core. This extends the reach of the RAN backhaul from the cell site deep into the core network.

Important consideration also needs to be given to SAE concepts like MME pooling and SGW pooling in the EPC that allow for geographic redundancy and load sharing. The RAN backhaul service model

must provide for eNodeB association to multiple gateways in the pool and migration of eNodeB across pools without having to re-architect the underlying transport architecture.

Figure 2-3. RAN Backhaul Architecture



Transport of Multiple Services from All Locations

LTE has to co-exist with other services on a common network infrastructure that could include:

- Existing mobile services:
 - 3G UMTS IP/ATM
 - 2G GSM and SP WiFi in a mobile-only deployment
- A myriad of other services:
 - Residential broadband triple play

NOT CISCO CONFIDENTIAL

- Metro Ethernet Forum (MEF) E-Line and E-LAN
- L3VPN business services
- RAN sharing, wireline wholesale in a converged mobile and wireline deployment

In these scenarios, the network has to not only support multiple services concurrently, but also support all these services across disparate endpoints. Typical examples are:

- L3 transport for LTE and Internet-High Speed Packet Access (I-HSPA) controller-free architectures: from RAN to SAE gateways in the core network.
- L3 transport for 3G UMTS/IP: from RAN to BSC in the aggregation network.
- L2 transport for 2G GSM and 3G UMTS/ATM: from RAN to RNC/BSC in the aggregation network.
- L2 transport for residential wireline: from access to broadband network gateways (BNG) in the aggregation network.
- L3/L2 transport for business wireline: from access to remote access networks across the core network.
- L2 transport for wireline wholesale: from access to retail wireline SP peering point.
- L3 transport for RAN sharing: from RAN to retail mobile SP peering point.

The transport technology used in the RAN backhaul and the network architecture must be carefully engineered to be scalable and flexible enough to meet the requirements of various services being transported across a multitude of locations in the network.



System Overview

This chapter includes the following major topics:

- [Section 3.1 Concept](#)
- [Section 3.2 Transport Models](#)
- [Section 3.3 Service Models](#)

3.1 System Concept

UMMT provides the architectural baseline for creating a scalable, resilient, and manageable mobile backhaul infrastructure that is optimized to seamlessly interwork with the Mobile Packet Core (MPC). The system is designed to concurrently support multiple generations (2G/3G/4G) of mobile services on a single converged network infrastructure. The system supports graceful introduction of LTE with existing 2G/3G services with support for pseudowire emulation (PWE) for 2G GSM and 3G UMTS/ATM transport, L2VPNs for 3G UMTS/IP, and L3VPNs for 3G UMTS/IP and 4G LTE transport. It supports essential features like network synchronization (physical layer and packet based), H-QoS, OAM, performance management, and fast convergence. It is optimized to cater to advanced 4G requirements like IPSec and authentication, direct eNodeB communication through the X2 interface, multicast for optimized video transport, virtualization for RAN sharing, capability of distributing the EPC gateways, and traffic offload.

The UMMT System meets the NGMN requirements for next-generation mobile backhaul, and innovates on the Broadband Forum TR-221 specification for MPLS in mobile backhaul networks by unifying the MPLS transport across the access, aggregation, and core domains. The architecture is also extensible to a converged mobile and wireline deployment and supports wireline residential, business, retail/wholesale L2VPNs and L3VPNs, and IP services.

The key aspects of the UMMT concept are described in this section.

Simplification of the End-to-End Mobile Transport and Service Architecture

A founding principle of UMMT is the simplification of the mobile backhaul architecture by eliminating the control and management plane translations that are inherent in legacy designs. As described in [Section 2.1 State of the Mobile Transport Industry](#), traditional backhaul architectures relying on L2 transport are not optimized for 4G all-IP flat LTE architecture, and backhaul architectures built over mixed L2 and L3 transport are inherently complex to operate. The UMMT System enables a unified L3 MPLS/IP transport extending end-to-end from the mobile core all the way to the RAN access. It simplifies the control plane by providing seamless MPLS LSPs across access, pre-aggregation, aggregation/distribution, and core domains of the network. In doing so, a fundamental attribute of decoupling the transport and service layers of the network and eliminating intermediate touchpoints in the backhaul is achieved. By eliminating intermediate touchpoints, it simplifies the

operation and management of the service. Service provisioning is restricted only at the edges of the network where it is required: namely at the CSGs in the access and the provider edge (PE) (hereby referred to as MTG) connecting the mobile gateways in the MPC. Simple carrier class operations with end-to-end OAM, performance monitoring of the GSM, UMTS, and LTE services are made possible.

Flexible Placement of L3 and L2 Transport Virtualization Functions for GSM, UMTS, and LTE

The hierarchical RAN backhaul architecture of 2G and 3G releases involved an intermediate agent like the BSC/RNC, which mostly resided at the aggregation/distribution layer of the transport network. This simplified the requirements on the transport in that it only required connectivity between the RAN access and aggregation network layers. In comparison, 4G LTE imposes many new requirements on the backhaul:

- Because of the any-to-any relationship between eNodeBs for the X2 interface and the one-to-many relationship between eNodeBs and EPC gateways (SGWs, MMEs) for the S1-u/c interface, the eNodeBs and associated CSGs in the RAN access need both local connectivity and direct connectivity to the EPC gateways in the MPC.
- The stringent latency requirements of the X2 interface requires a logical mesh connectivity between CSGs that introduces the minimum amount of delay that is in the order of 30ms. The minimum delay is expected to reduce further to around 10ms for features such as collaborative multiple input multiple output (MIMO) in the future with 3GPP LTE Release 10 and beyond.
- The Evolved Universal Terrestrial Radio Access Network (E-UTRAN)/EPC architecture supports MME pooling and SGW pooling to enable geographic redundancy, capacity increase, load sharing, and signaling optimization. This requires the transport infrastructure to provide connectivity from eNodeBs in the RAN access to multiple MME and SGWs within these pools in the core network.
- The introduction of LTE into a existing 2G/3G network has to be graceful and the transition will take time. During this period, it is natural for a few centralized EPC gateways to be initially deployed and shared across different regions of the network. As capacity demands and subscriber densities increase, it is expected that new gateways will be added closer to the regions and subscribers will have to be migrated. While the migration across gateways within the packet core could be done seamlessly based on gateway pooling, it is imperative that the underlying transport infrastructure requires minimal to no provisioning changes to allow the migration.

In 2G and 3G releases, the hub-and-spoke connectivity requirement between the BSC/RNC and the BTS/NodeB makes L2 transport using Ethernet bridging with VLANs or P2P PWs with MPLS PWE3 appealing. In contrast, a L3 transport option is much better suited to meet the myriad of connectivity requirements of 4G LTE. The UMMT architecture provides both L2 and L3 MPLS VPN transport options that provide the necessary virtualization functions to support the coexistence of LTE S1-u/c, X2, interfaces with GSM Abis TDM, and UMTS IuB ATM backhaul. The decoupling of the transport and service layers of the network infrastructure and the seamless connectivity across network domains makes the system a natural fit for the flat all-IP LTE architecture by allowing for the flexible placement of 2G/3G/4G gateways in any location of the network to meet all the advance backhaul requirements listed above.

Deliver New Levels of Scale for MPLS Transport with RFC-3107 Hierarchical-Labeled BGP LSPs

As described in [Section 2.2 Next-Generation Mobile Transport Characteristics](#), LTE deployments will introduce unprecedented levels of scale in terms of eNodeBs and associated network elements like CSGs into the network. While L2 and L3 MPLS VPNs are well suited to provide the required virtualization functions to transport 2G/3G/4G mobile services, LTE's requirement to have inter-domain connectivity from the RAN access all the way to the core network in order to reach the EPC gateways, however, presents challenges of scale to the transport infrastructure. This is because IP aggregation with route summarization usually performed between (access, aggregation, core) regions of the network does not work for MPLS as MPLS is not capable of aggregating Forwarding

NOT CISCO CONFIDENTIAL

Equivalency Class (FEC). In MPLS deployments, the FEC is typically the PE's /32 loopback IP address. Exposing the loopback addresses of all the nodes (10k -100k) across the network introduces two main challenges:

1. Large flat routing domains adversely affect the stability and convergence time of the IGP.
2. The sheer size of the routing and MPLS label information control plane and forwarding plane state will easily overwhelm the technical scaling limits on the smaller nodes (CSGs, pre-aggregation nodes) involved in the network.

Unified MPLS elegantly solves this problem with a divide-and-conquer strategy of isolating the access, aggregation, and core network layers into independent and isolated Interior Gateway Protocol (IGP) domains. Label Distribution Protocol (LDP) is used for setting up LSPs within these domains, and RFC-3107 BGP-labeled unicast is used for setting up LSPs across domains. This BGP-based inter-domain hierarchical LSP approach helps scale the network to hundreds of thousands of LTE cell sites without overwhelming any of the smaller nodes in the network. At the same time, the stability and fast convergence of the small isolated IGP domains corresponding to various network layers are maintained.

Facilitate Fixed-Mobile Convergence

The UMMT System addresses all of the needs of next-generation mobile backhaul while concurrently supporting transport legacy 2G and 3G mobile services. The concept of Unified MPLS, however, is not restricted to mobile transport. By decoupling the transport and service layers on the network, Unified MPLS enables end-to-end MPLS transport for any service, at any scale. The architecture is allows extensions for wireline residential, business, retail/wholesale L2 and L3 VPNs and IP services on the common network infrastructure supporting mobile backhaul.

3.2 Transport Models

The ubiquitous mobile broadband adoption driven by LTE will introduce unprecedented levels of scale in terms of eNodeBs and CSGs into the RAN backhaul network. This factor, combined with the flattened LTE/EPC architecture requiring connectivity from the RAN access all the way to the core network, introduces challenges in scaling the MPLS network. The endpoint identifier in MPLS is the PE's /32 loopback IP address, and since MPLS is not capable of aggregating FEC, IP aggregation with route summarization cannot be performed between the access, aggregation, and core regions of the network. All network technologies meet a scale challenge at some point, and the solution is always some form of hierarchy to scale. The UMMT System uses this hierarchical approach to solve the scaling problem in MPLS-based LTE deployments.

Unified MPLS adopts a divide-and-conquer strategy where the core, aggregation, and access networks are partitioned in different MPLS/IP domains. The network segmentation between the core and aggregation domains could be based on a single AS multi-area design or inter-AS organization. Regardless of the type of segmentation, the unified MPLS transport concept involves partitioning the core, aggregation, and access layers of the network into isolated IGP/LDP domains. Partitioning these network layers into such independent and isolated IGP domains helps reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence. LDP is used for label distribution to build LSPs within each independent IGP domain. This enables a device inside an access, aggregation, or core domain to have reachability via intra-domain LDP LSPs to any other device in the same domain. Reachability across domains is achieved using RFC 3107 procedures whereby BGP-labeled unicast is used as an inter-domain label distribution protocol to build hierarchical LSPs across domains. This allows the link state database of the IGP in each isolated domain to remain as small as possible while all external reachability information is carried via BGP, which is designed to scale to the order of millions of routes.

- In single AS multi-area designs, interior Border Gateway Protocol (iBGP)-labeled unicast is used to build inter-domain LSPs.

NOT CISCO CONFIDENTIAL

- In inter-AS designs, iBGP-labeled unicast is used to build inter-domain LSPs inside the AS and exterior Border Gateway Protocol (eBGP)-labeled unicast is used to extend the end-to-end LSP across the AS boundary.

In both cases, the Unified MPLS transport across domains will use hierarchical LSPs that rely on a BGP-distributed label that is used to transit the isolated MPLS domains, and on a LDP-distributed label used within the AS to reach the inter-domain area border router (ABR) or autonomous system boundary router (ASBR) corresponding to the labeled BGP next hop.

The UMMT System integrates key technologies from Cisco's Unified MPLS suite of technologies to deliver a highly scalable and simple-to-operate MPLS-based RAN backhaul network. It enables a comprehensive and flexible transport framework structured around the most common layers in SP networks: the radio access network, the aggregation network, and the core network. The transport architecture structuring takes into consideration the type of access and the size of the network.

Access Type:

- MPLS Packet Access:
 - MPLS-based packet access covers point-to-point links, rings, and hierarchical topologies.
 - Applies to both fiber and newer Ethernet microwave-based access technologies with the MPLS access network enabled by the CSGs.
 - The services include both mobile and wireline services and can be enabled by the CSGs in the access network and the pre-aggregation or aggregation nodes in the aggregation network.
- IP/Ethernet/TDM Access:
 - Includes native IP or Ethernet links in point-to-point or ring topologies over fiber and newer Ethernet microwave-based access.
 - Covers point-to-point TDM+Ethernet links over hybrid microwave access.
 - The MPLS services are enabled by the aggregation network and includes GSM Abis, ATM IuB, IP IuB, and IP S1/X2 interfaces aggregated in MPLS pre-aggregation or aggregation nodes.

Network Size:

- Small Network:
 - Applies to network infrastructures in small geographies where the core and aggregation network layers are integrated in a single domain.
 - The single IGP/LDP domain includes less than 1000 core and aggregation nodes.
- Large Network:
 - Applies to network infrastructures built over large geographies.
 - The core and aggregation network layers have hierarchical physical topologies that enable IGP/LDP segmentation.

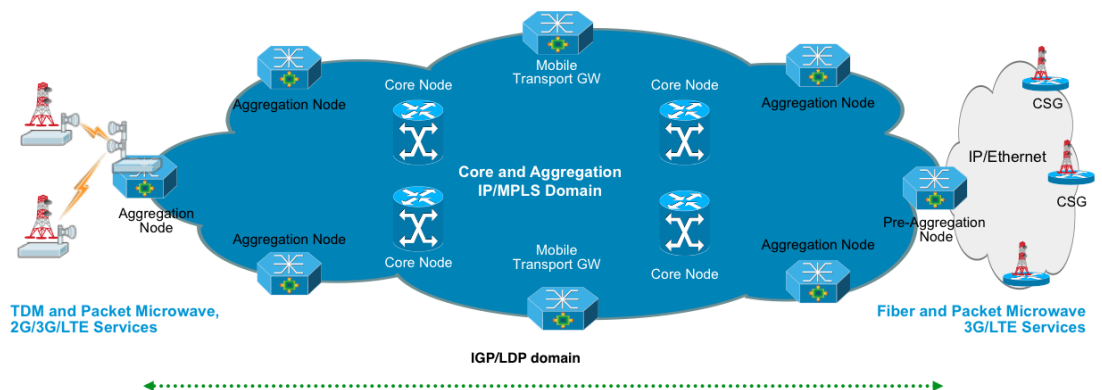
This transport architecture structuring based on access type and network size leads to five architecture models that fit various customer deployments and operator preferences as shown in [Table 3-1](#), and described in the sections below.

NOT CISCO CONFIDENTIAL**Table 3-1. UMMT Transport Models**

	Small Network	Large Network
Ethernet/TDM Access	Flat LDP Core and Aggregation Network	Labeled BGP Core and Aggregation
MPLS Access	Labeled BGP Access with Flat LDP Core and Aggregation	Labeled BGP Core, Aggregation, and Access
		Labeled BGP Core and Aggregation with Redistribution into Access Network IGP

3.2.1 Flat LDP Core and Aggregation

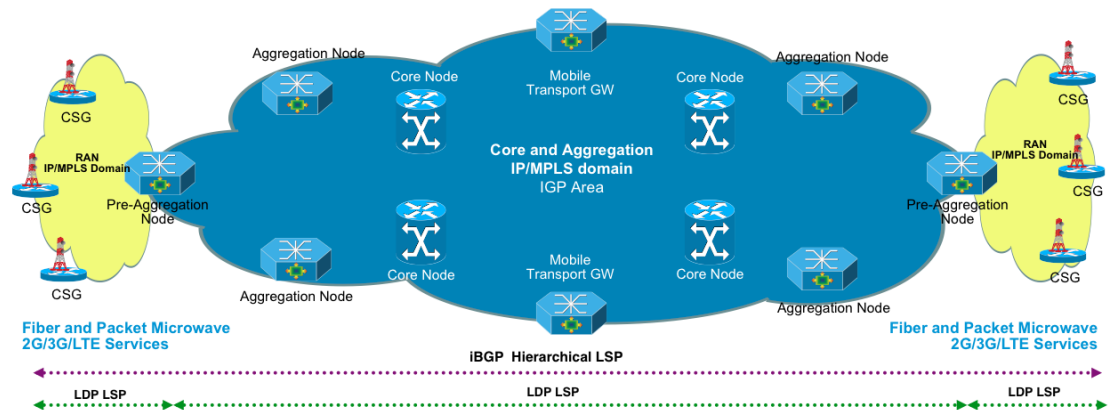
This architecture model applies to small geographies where core and aggregation networks may not have distinct physical topologies, are integrated under common operations and network segmentation is not required for availability reasons. It assumes an non-MPLS IP/Ethernet or TDM access being aggregated in a small scale network.

Figure 3-1. Flat LDP Core and Aggregation

The small scale aggregation network is assumed to be comprised of core and aggregation nodes that are integrated in a single IGP/LDP domain consisting of less than 1000 nodes. Since no segmentation between network layers exists, a flat LDP LSP provides end-to-end reachability across the network. All mobile (and wireline) services are enabled by the aggregation nodes. The mobile access is based on TDM and packet microwave links aggregated in aggregation nodes that provide TDM/ATM/Ethernet VPWS and MPLS VPN transport.

3.2.2 Labeled BGP Access with Flat LDP Core and Aggregation

This architecture model applies to small geographies. It assumes an MPLS-enabled access network with fiber and packet microwave links being aggregated in a small scale network.

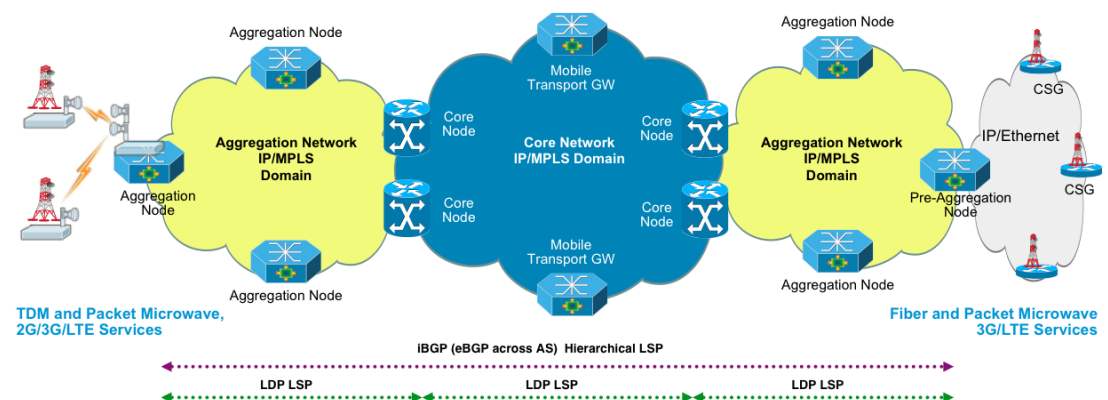
NOT CISCO CONFIDENTIAL**Figure 3-2. Labeled BGP Access with Flat LDP Core and Aggregation**

The small scale aggregation network is assumed to be comprised of core and aggregation nodes that are integrated in a single IGP/LDP domain consisting of less than 1000 nodes. The RAN access network is comprised of a separate IGP domain. The separation can be enabled by making the access network part of a different IGP area from the aggregation and core nodes, or by running a different IGP process on the pre-aggregation nodes corresponding to the aggregation/core and RAN access networks. LDP is used to build intra-area LSP within each segmented domain. The aggregation/core and RAN access networks are integrated with labeled BGP LSPs, with the pre-aggregation nodes acting as ABRs performing BGP next-hop-self (NHS) function to extend the iBGP hierarchical LSP across the two domains. The mobile 2G/3G/LTE (and wireline) services can be enabled by the CSGs in the access as well as the pre-aggregation/aggregation nodes.

BGP community-based egress filtering is performed towards the RAN access at the pre-aggregation node ABRs so that the CSGs only learn required remote destinations and all unwanted prefixes are dropped so as to keep their BGP tables small and prevent unnecessary updates.

3.2.3 Labeled BGP Core and Aggregation

This architecture model applies to networks deployed in medium to large geographies. It assumes a non-MPLS IP/Ethernet or TDM access being aggregated in a relatively large scale network.

Figure 3-3. Labeled BGP Core and Aggregation

NOT CISCO CONFIDENTIAL

The network infrastructure is organized by segmenting the core and aggregation networks into independent IGP/LDP domains. The segmentation between the core and aggregation domains could be based on a single AS multi-area design or an inter-AS organization. In the single AS multi-area option, the separation can be enabled by making the aggregation network part of a different IGP area from the core network, or by running a different IGP process on the core ABR nodes corresponding to the aggregation and core networks. The mobile RAN access is based on native IP or Ethernet links in point-to-point or ring topologies over fiber and newer Ethernet microwave-based access, or point-to-point TDM+Ethernet links over hybrid microwave.

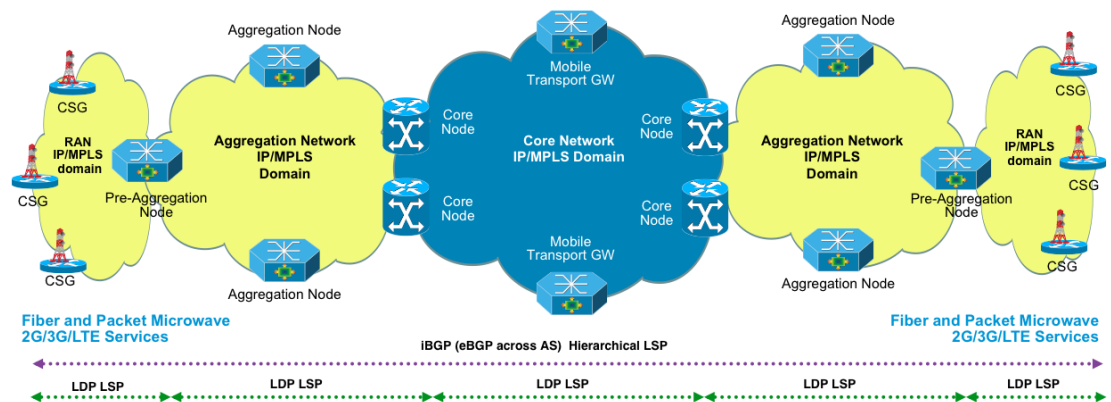
All mobile (and wireline) services are enabled by the aggregation nodes. LDP is used to build intra-area LSP within each segmented domain. The aggregation and core networks are integrated with labeled BGP LSPs. In the single AS multi-area option, the core ABRs perform BGP NHS function to extend the iBGP hierarchical LSP across the aggregation and core domains. When the core and aggregation networks are organized in different autonomous systems, iBGP is used to build the hierarchical LSP from the pre-aggregation node to the ASBRs and eBGP is used to extend the end-to-end LSP across the AS boundary.

BGP community-based egress filtering is performed towards the aggregation networks at the core ABRs so that the pre-aggregation and aggregation nodes only learn required remote destinations and all unwanted prefixes are dropped. This helps reduce the size of BGP tables on these nodes and also prevents unnecessary updates.

3.2.4 Labeled BGP Core, Aggregation, and Access

This architecture model applies to networks deployed in large geographies. It assumes an MPLS-enabled access network with fiber and packet microwave links being aggregated in a large scale network.

Figure 3-4. Labeled BGP Core, Aggregation, and Access



The network infrastructure is organized by segmenting the core, aggregation, and access networks into independent IGP/LDP domains. The segmentation between the core, aggregation, and access domains could be based on a single AS multi-area design or an inter-AS organization. In the single AS multi-area option, the separation between core and aggregation networks can be enabled by making the aggregation network part of a different IGP area from the core network, or by running a different IGP process on the core ABR nodes corresponding to the aggregation and core networks. The separation between aggregation and access networks is enabled by running a different IGP process on the pre-aggregation nodes corresponding to the aggregation and RAN access networks. In the inter-AS option, while the core and aggregation networks are in different autonomous systems, the separation between aggregation and access networks is enabled by making the access network part of a different IGP area

NOT CISCO CONFIDENTIAL

from the aggregation network, or by running a different IGP process on the pre-aggregation nodes corresponding to the aggregation and RAN access networks.

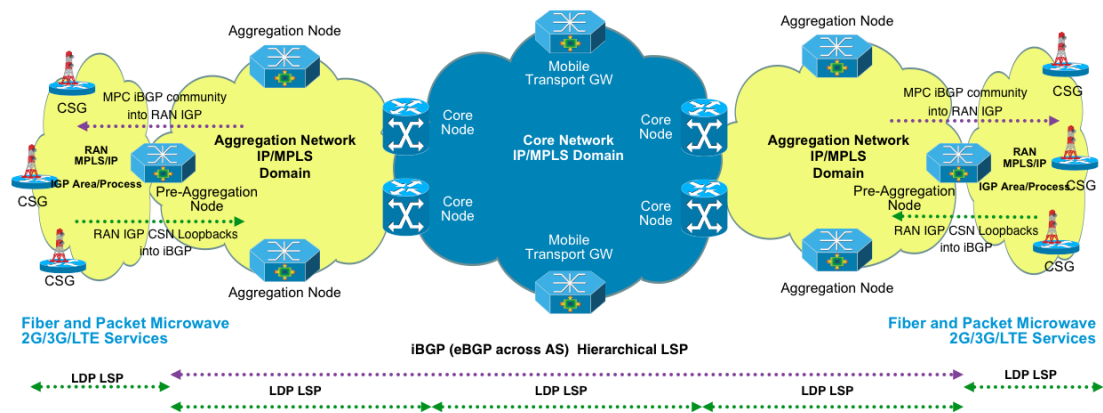
The mobile 2G/3G/LTE (and wireline) services can be enabled by the CSGs in the access as well as the pre-aggregation/aggregation nodes. LDP is used to build intra-area LSP within each segmented domain. The access, aggregation, and core networks are integrated with labeled BGP LSPs. In the single AS multi-area option, the pre-aggregation nodes and core ABRs act as ABRs for their corresponding domains and extend the iBGP hierarchical LSP across the access, aggregation, and core domains. When the core and aggregation networks are organized in different autonomous systems, the pre-aggregation nodes act as ABRs performing BGP NHS function to extend the iBGP hierarchical LSP across the access and aggregation domains. At the ASBRs, eBGP is used to extend the end-to-end LSP across the AS boundary.

BGP community-based egress filtering is performed towards the aggregation networks at the core ABRs, and towards the RAN access at the pre-aggregation node ABRs so that the corresponding nodes in each domain only learn required remote destinations and all unwanted prefixes are dropped. This helps reduce the size of BGP tables on these nodes and also prevents unnecessary updates.

3.2.5 Labeled BGP Core and Aggregation with Redistribution into Access Network IGP

This architecture model applies to networks deployed in large geographies. It assumes an MPLS-enabled access network with fiber and packet microwave links being aggregated in a large scale network.

Figure 3-5. Labeled BGP Core and Aggregation with Redistribution into Access Network IGP



The network infrastructure organization in this architecture model is the same as the one described in [Section 3.2.4 Labeled BGP Core, Aggregation, and Access](#), with options for both Single AS Multi-Area and Inter-AS designs. The service options in this model are also the same with support for mobile 2G/3G/LTE (and wireline) services that can be enabled by the CSGs in the access as well as the pre-aggregation/aggregation nodes. This model differs from the aforementioned one in that the hierarchical-labeled BGP LSP spans only the core and aggregation networks and does not extend to the RAN access. Instead of using BGP for inter-domain label distribution in the RAN, the end-to-end unified MPLS LSP is extended into the RAN access using LDP with redistribution. The IGP scale in the RAN access is kept small by selective redistribution of required remote prefixes from iBGP based on communities.

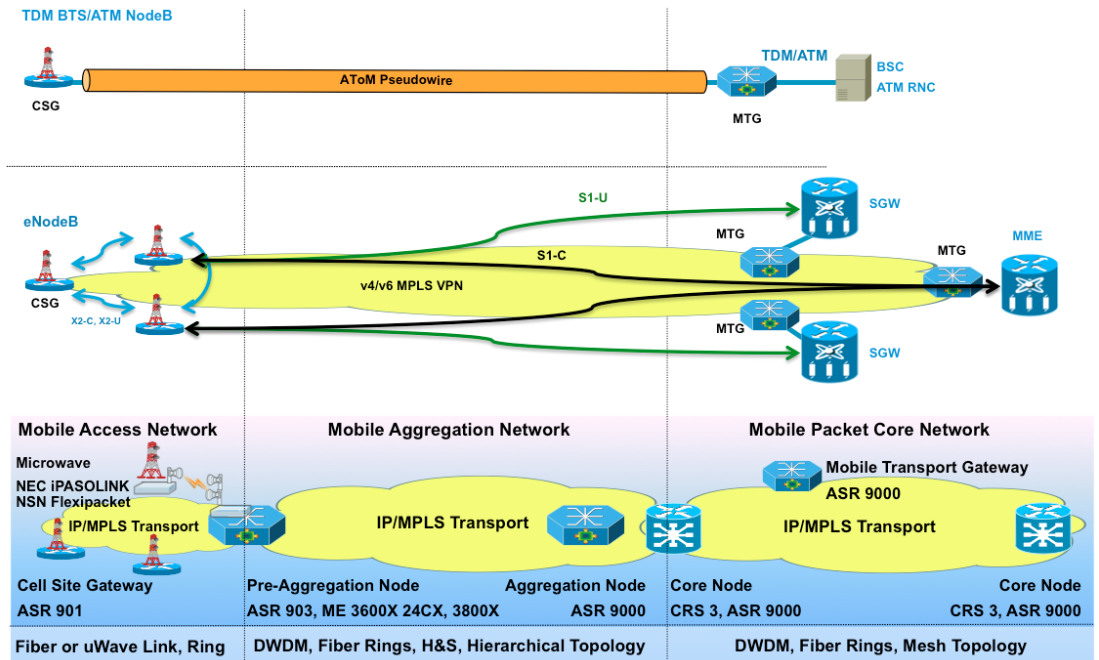
NOT CISCO CONFIDENTIAL

3.3 Service Models

The fundamental goal of the UMMT System is the simplification of the end-to-end mobile transport and service architecture. It achieves this goal by decoupling the transport and service layers of the network, thereby allowing these two distinct entities to be provisioned and managed independently. As described in Section 3.2 Transport Architecture Models, Unified MPLS Transport seamlessly interconnects the access, aggregation, and core MPLS domains of the network infrastructure with hierarchical LSPs at the transport layer. Once this unified MPLS transport is established (a task that only needs to be undertaken once), a multitude of services can be deployed on top of it. These services can span any location in the network without restricting topological boundaries.

The decoupling of the transport and service layers makes it possible for the service architecture or service delivery model for any given service to be provisioned, managed, and changed independently, without having to touch the transport layer. It eliminates the unwanted complexity of having to provision and manage intermediate touchpoints like the pre-aggregation, aggregation, and core ABRs for service delivery, requiring service provisioning only at the service endpoints.

Figure 3-6. Mobile Backhaul Services



The UMMT System is a comprehensive RAN backhaul solution that provides the foundation for LTE, legacy 2G GSM, and existing 3G UMTS transport services.

The system proposes a highly-scaled MPLS L3VPN-based service model to meet the immediate needs of LTE transport and accelerate its deployment. The MPLS VPN model provides the required transport virtualization for the graceful introduction of LTE into an existing 2G/3G network, and also satisfies future requirements of RAN sharing in a wholesale scenario. It is well suited to satisfy the mesh connectivity and stringent latency requirements of the LTE X2 interface. Simple MPLS VPN route-target import/export mechanisms can be used to enable:

- Multipoint connectivity within the local RAN access for intra-RAN-access X2 handoff.
- Multipoint connectivity with adjacent RAN access regions for inter-RAN-access region X2 handoff.

- Multipoint connectivity with EPC gateways (SGWs, MMEs) in the MPC for the S1-u/c interface.
- Multipoint connectivity with more than one MME and SGW for MME and SGW pooling scenarios.

The MPLS VPN-based service model allows for eNodeBs and associated CSGs to be added to the RAN at any location in the network, EPC gateways can be added in the MPC and have instant connectivity to each other without additional configuration overhead. It allows seamless migration of eNodeBs initially mapped to centralized EPC gateways to more distributed ones to accommodate capacity and scale demands, without having to re-provision the transport infrastructure. [Section 4.2.1 L3 MPLS VPN Service Model for LTE](#) covers these aspects in detail.

Service virtualization with MPLS-based L2 and L3 VPNs also allows legacy 2G GSM and existing 3G UMTS services to co-exist with LTE on the same transport infrastructure. The system supports MSPs with GSM and ATM-based UMTS deployments wishing to remove, reduce, or cap investments in SONET/SDH and ATM transport infrastructure by using MPLS-based Circuit Emulation over Packet (CEoP) services.

- For the mobile service providers who want to reduce SONET/SDH infrastructure used for GSM, UMMT enables PWE3-based transport of emulated TDM circuits. Structured circuit emulation is achieved with CESoPSN, and unstructured emulation is achieved with SAToP. E1/T1 circuits from BTS equipment connected to the CSG or to the pre-aggregation node (PAN) are transported to MTG, where they are bundled into channelized STM1/OC-3 interfaces for handoff to the BSC.
- For the mobile service providers who want to reduce their ATM infrastructure used for ATM-based UMTS, UMMT enables ATM VC (AAL0 or AAL5) or VP (AAL0) PWE3-based transport. ATM E1/T1 or IMA interfaces from NodeB equipment connected to the CSG or PAN can be transported to the MTG, where they are bundled into STM1 ATM interfaces for handoff to the RNC. Cell packing may be used to optimize the bandwidth used for this transport.

[Section 4.2.2 L2 MPLS VPN Service Model for 2G and 3G](#) covers these aspects in detail.

For the above service models, the system supports physical layer synchronization of frequency based on SyncE, or packet-based synchronization of frequency and phase based on 1588 PTP, as described in [Section 5.2 Synchronization Distribution](#).



CHAPTER 4

System Architecture

This chapter includes the following major topics:

- [Section 4.1 Transport Architecture](#)
- [Section 4.2 Service Models](#)
- [Section 4.3 Inter-Domain Hierarchical LSPs](#)
- [Section 4.4 Transport and Service Control Plane](#)
- [Section 4.5 Prefix Filtering](#)
- [Section 4.6 Scale Considerations](#)

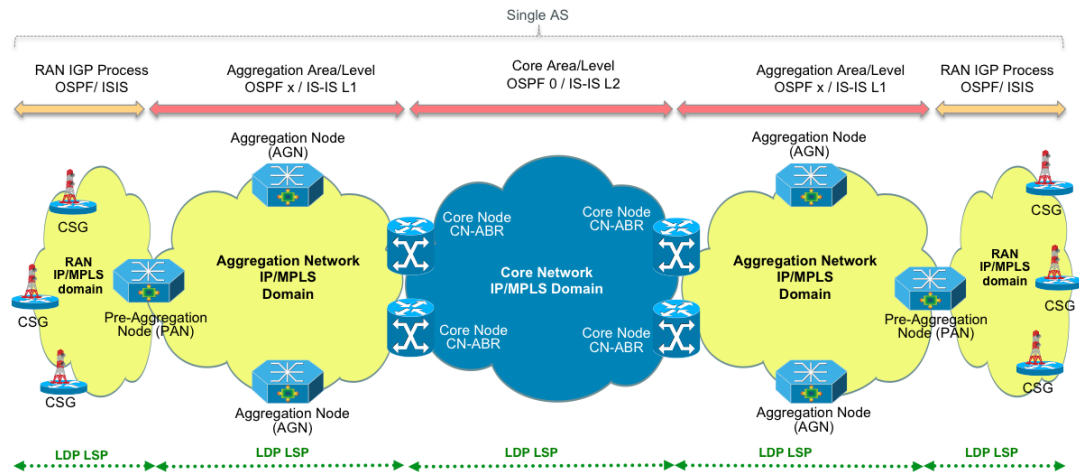
4.1 Transport Architecture

This section includes the following topics:

- [Section 4.1.1 Large Network, Multi-Area IGP Design with IP/MPLS Access](#)
- [Section 4.1.2 Large Network, Inter-AS Design with IP/MPLS Access](#)
- [Section 4.1.3 Large Network, Multi-Area IGP Design with non_IP/MPLS Access](#)
- [Section 4.1.4 Large Network, Inter-AS Design with non_IP/MPLS Access](#)
- [Section 4.1.5 Small Network, Integrated Core and Aggregation with IP/MPLS Access](#)
- [Section 4.1.6 Small Network, Integrated Core and Aggregation with non_IP/MPLS Access](#)

4.1.1 Large Network, Multi-Area IGP Design with IP/MPLS Access

This section details the system architecture for a transport model where the network organization between the core and aggregation domains is based on a single autonomous system, multi-area IGP design. This model follows the approach of enabling a Unified MPLS LSP using hierarchical-labeled BGP LSPs across the core and aggregation network, and presents two approaches for extending the unified MPLS LSP into the mobile RAN access domain.

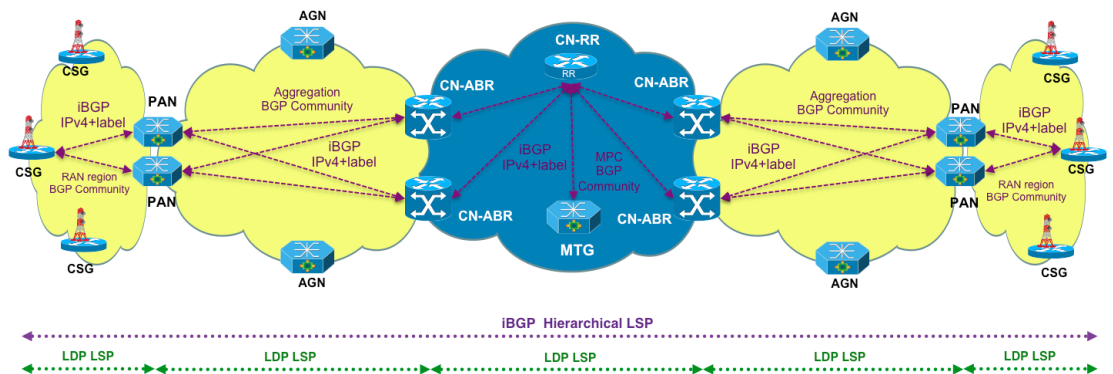
Figure 4-1. Multi-Area IGP/LDP Domain Organization

From a multi-area IGP organization perspective, the core network is either an intermediate system to intermediate system (IS-IS) Level 2 or an open shortest path first (OSPF) backbone area. The aggregation domains, in turn, are IS-IS Level 1 or OSPF non-backbone areas. No redistribution occurs between the core and aggregation IGP levels/areas, thereby containing the route scale within each domain. The MPLS/IP mobile access networks subtending from aggregation or pre-aggregation nodes are based on a different IGP process, restricting their scale to the level of the local RAN. To accomplish this, the pre-aggregation nodes run two distinct IGP processes, with the first process corresponding to core-aggregation network (IS-IS Level 1 or OSPF non-backbone area) and the second IGP process corresponding to the mobile RAN access network. The second IGP process could be an OSPF backbone area or IS-IS Level 2 domain. All CSGs that are part of the mobile RAN access network subtending from a pair of pre-aggregation nodes are part of this second IGP process.

Partitioning these network layers into such independent and isolated IGP domains helps reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence within each of these domains. LDP is used for label distribution to build intra-domain LSPs within each independent access, aggregation, and core IGP domain. Inter-domain reachability is enabled with hierarchical LSPs using BGP-labeled unicast as per RFC 3107 procedures, where iBGP is used to distribute labels in addition to remote prefixes, and LDP is used to reach the labeled BGP next-hop. Two options are presented below to extend the unified MPLS LSP into the mobile RAN access domain to accommodate different operator preferences.

Option-1: Multi-Area IGP Design with Labeled BGP Access

This option is based on the transport model described in [Section 3.2.4 Labeled BGP Core, Aggregation, and Access](#).

Figure 4-2. Inter-Domain Transport for Multi-Area IGP Design with Labeled BGP Access

In this option, the access, aggregation, and core networks are integrated with unified MPLS LSPs by extending labeled BGP from the core all the way to the CSGs in the RAN access. Any node in the network that requires inter-domain LSPs to reach nodes in remote domain acts as a labeled BGP PE and runs iBGP IPv4 unicast+labels with their corresponding local RRs.

- The core PoP nodes (CN-ABR) are labeled BGP ABRs and act as inline RRs for their local aggregation network PAN clients. The CN-ABRs peer with other CN-ABRs using iBGP-labeled unicast in either a full mesh configuration or using a centralized core node route reflector (CN-RR) within the core domain. The centralized RR deployment option is shown in [Figure 4-2](#) above.
- The MTG residing in the core network are labeled BGP PEs. They connect to the EPC gateways (SGW, PGW, MME) in the MPC. The MTGs peer either directly with the closest CN-ABR RRs, in the case of a CN-ABR full-mesh configuration, or with the CN-RR, depending on the deployment setting. The MTGs advertise their loopbacks into iBGP-labeled unicast with a common BGP community (MPC BGP community) representing the MPC.
- The PANs are labeled BGP PEs and act as inline RRs for their local access network CSG clients. All the PANs in the aggregation network that require inter-domain LSPs to reach remote PANs in another aggregation network, or the core network (to reach the MTGs, for example), run BGP-labeled unicast sessions with their local CN-ABR inline-RRs. The PANs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the aggregation community. They learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community.
- The CSGs in the RAN access networks are labeled BGP PEs. They peer with iBGP-labeled unicast sessions with their local PAN inline-RRs. The CSGs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the RAN access community. They learn labeled BGP prefixes marked with the MPC BGP community for reachability to the MPC, and the adjacent RAN access BGP community if inter-access X2 connectivity is desired.

Since routes between the core IS-IS Level 2 (or OSPF backbone) and aggregation IS-IS Level 1 (or OSPF non-backbone area) are not redistributed, the CN-ABRs have to reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP switching and allow the aggregation and core IGP routing domains to remain isolated. This CN-ABR NHS function is symmetrically applied by the CN-ABRs towards its PAN clients in its local aggregation domain, and the CN-RR in the core domain. Similarly, since the RAN access and aggregation networks are in different IGP processes, the PANs have to reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP switching. This PAN NHS function is symmetrically applied by the PANs

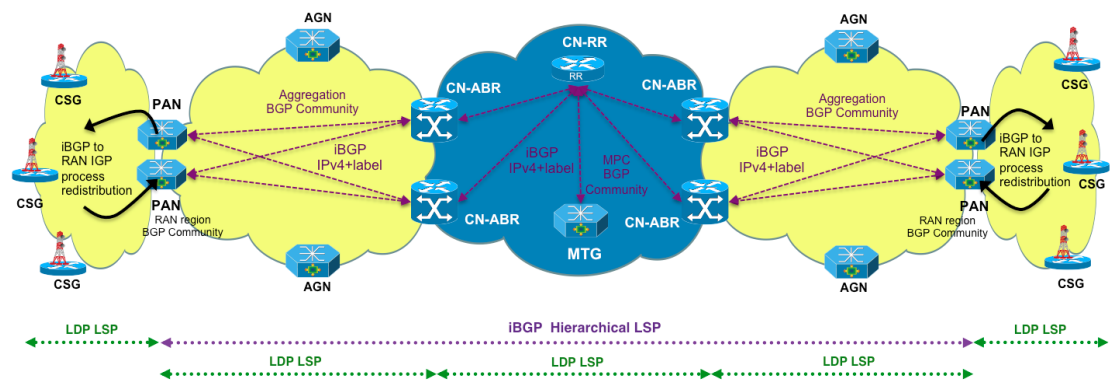
towards its CSG clients in its local RAN access domain, and the higher level CN-ABR inline-RR in the aggregation domain.

The MTGs in the core network are capable of handling large scale and will learn all BGP-labeled unicast prefixes since they need connectivity to all the CGSs in the entire network. Simple prefix filtering based on BGP communities is performed on the CN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into neighboring aggregation domains, where they are not needed. This filtering mechanism is described in detail in [Section 4.5 Prefix Filtering](#). The PANs only learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community. This allows the PANs to enable inter-metro wireline services across the core, and also reflect the MPC prefix to their local access networks. Using a separate IGP process for the RAN access enables the mobile access network to have limited control plane scale, since the CSGs only learn local IGP routes and labeled BGP prefixes marked with the MPC BGP community.

Option-2: Multi-Area IGP Design with IGP/LDP Access

This option is based on the transport model described in [Section 3.2.5 Labeled BGP Core and Aggregation with Redistribution into Access Network IGP](#).

Figure 4-3. Inter-Domain Transport for Multi-Area IGP Design with IGP/LDP Access



This option follows the approach of enabling labeled BGP across the core and aggregation networks and extends the unified MPLS LSP to the access by redistribution between labeled BGP and the access domain IGP. All nodes in the core and aggregation network that require inter-domain LSPs to reach nodes in remote domains act as a labeled BGP PEs and runs iBGP IPv4 unicast+labels with their corresponding local RRs.

- The core PoP nodes (CN-ABR) are labeled BGP ABRs and act as inline RRs for their local aggregation network pre-aggregation node (PAN) clients. The CN-ABRs peer with other CN-ABRs using iBGP-labeled unicast in either a full mesh configuration or using a centralized CN-RR within the core domain. The centralized RR deployment option is shown in [Figure 4-3](#) above.
- The MTG residing in the core network are labeled BGP PEs. They connect to the EPC gateways (SGW, PGW, MME) in the MPC. The MTGs peer either directly with the closest CN-ABR RRs, in the case of a CN-ABR full-mesh configuration, or with the CN-RR, depending on the deployment setting. The MTGs advertise their loopbacks into iBGP-labeled unicast with a common BGP community (MPC BGP community) representing the MPC.
- All the PANs in the aggregation network that require inter-domain LSPs to reach remote PANs in another aggregation network, or the core network (to reach the MTGs, for example), run BGP-labeled unicast sessions with their local CN-ABR inline RRs. The PANs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the

NOT CISCO CONFIDENTIAL

aggregation community. They learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community.

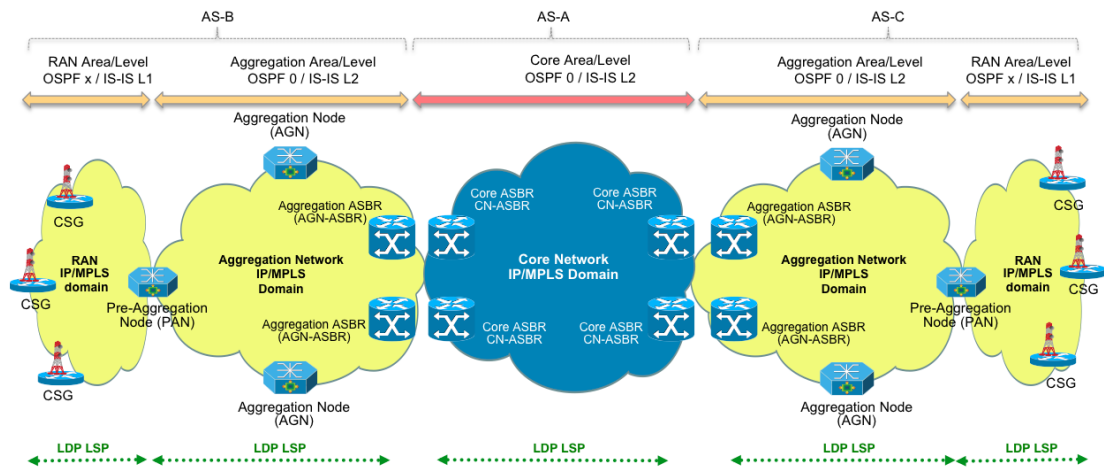
- The inter-domain LSPs are extended to the MPLS/IP RAN access with a controlled redistribution based on IGP tags and BGP communities. Each mobile access network subtending from a pair of PANs is based on a different IGP process. At the PANs, the inter-domain core and aggregation LSPs are extended to the RAN access by redistributing between iBGP and RAN IGP. In one direction, the RAN access node loopbacks (filtered based on IGP tags) are redistributed into iBGP-labeled unicast and tagged with RAN access BGP community that is unique to that RAN access region. In the other direction, the MPC prefixes filtered based on MPC-marked BGP communities, and optionally, adjacent RAN access prefixes filtered based on RAN-region-marked BGP communities (if inter-access X2 connectivity is desired), are redistributed into the RAN access IGP process.

Since routes between the core IS-IS Level 2 (or OSPF backbone) and aggregation IS-IS Level 1 (or OSPF non-backbone area) are not redistributed, the CN-ABRs have to reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP switching and allow the aggregation and core IGP routing domains to remain isolated. This CN-ABR NHS function is symmetrically applied by the CN-ABRs towards its PAN clients in its local aggregation domain, and the CN-RR in the core domain.

The MTGs in the core network are capable of handling large scale and will learn all BGP-labeled unicast prefixes since they need connectivity to all the CGSs in the entire network. Simple prefix filtering based on BGP communities is performed on the CN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into neighboring aggregation domains, where they are not needed. This filtering mechanism is described in detail in [Section 4.5 Prefix Filtering](#). The PANs only learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community. This allows the PANs to enable inter-metro wireline services across the core, and also redistribute the MPC prefix to their local access networks. Using a separate IGP process for the RAN access enables the mobile access network to have limited control plane scale, since the CSGs only learn local IGP routes and labeled BGP prefixes marked with the MPC BGP community.

4.1.2 Large Network, Inter-AS Design with IP/MPLS Access

This section details the system architecture for a transport model where the core and aggregation networks are organized as different autonomous systems. This model follows the approach of enabling a Unified MPLS LSP using hierarchical-labeled BGP LSPs based on iBGP-labeled unicast within each AS, and eBGP-labeled unicast to extend the LSP across AS boundaries. Two approaches are presented for extending the unified MPLS LSP into the mobile RAN access domain.

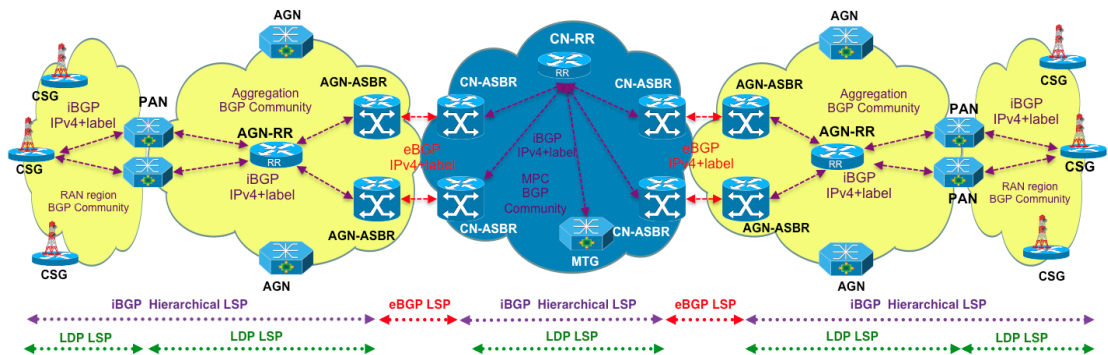
Figure 4-4. Inter-AS IGP/LDP Domain Organization

The core and aggregation networks are segmented into different autonomous systems. Within each aggregation domain, the aggregation and access networks are segmented into different IGP areas or levels, where the aggregation network is either an IS-IS Level 2 or an OSPF backbone area, and subtending access networks are IS-IS Level 1 or OSPF non-backbone areas. No redistribution occurs between the aggregation and access IGP levels/areas, thereby containing the route scale within each domain. Partitioning these network layers into such independent and isolated IGP domains helps reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence within each of these domains. LDP is used for label distribution to build intra-domain LSPs within each independent access, aggregation, and core IGP domain.

Inter-domain reachability is enabled with hierarchical LSPs using BGP-labeled unicast as per RFC 3107 procedures. Within each AS, iBGP is used to distribute labels in addition to remote prefixes, and LDP is used to reach the labeled BGP next-hop. At the ASBRs, the Unified MPLS LSP is extended across the aggregation and core AS boundaries using eBGP-labeled unicast. The Unified MPLS LSP can be extended into the mobile RAN access using two different options as presented below to accommodate different operator preferences.

Option-1: Inter-AS Design with Labeled BGP Access

This option is based on the transport model described in [Section 3.2.4 Labeled BGP Core, Aggregation, and Access](#).

Figure 4-5. Inter-Domain Transport for Inter-AS Design with Labeled BGP Access

In this option the access, aggregation, and core networks are integrated with unified MPLS LSPs by extending labeled BGP from the core all the way to the CSGs in the RAN access. Any node in the network that requires inter-domain LSPs to reach nodes in remote domain acts as a labeled BGP PE and runs iBGP IPv4 unicast+labels with their corresponding local RRs.

- The core PoP nodes are labeled BGP ASBRs (CN-ASBR). They peer with iBGP-labeled-unicast sessions with the centralized CN-RR within the core AS, and peer with eBGP-labeled unicast sessions with the neighboring aggregation ASBRs. The CN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local CN-RRs and eBGP updates towards the neighboring aggregation ASBRs.
- The mobile transport gateways (MTG) residing in the core network are labeled BGP PEs, which connect to the EPC gateways (SGW, PGW, MME) in the MPC. The MTGs peer with iBGP-labeled unicast sessions with the CN-RR, and advertise their loopbacks into iBGP-labeled unicast with a common BGP community (MPC BGP community) representing the MPC.
- The aggregation PoP nodes act as labeled BGP ASBRs (AGN-ASBR) in the aggregation AS. They peer with iBGP-labeled unicast sessions with the centralized aggregation route reflector (AGN-RR) within the aggregation AS, and peer with eBGP-labeled unicast sessions to the CN-ASBR in the core AS. The AGN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local AGN-RRs and eBGP updates towards neighboring CN-ASBRs.
- All the PANs in the aggregation network that require inter-domain LSPs to reach remote PANs in another aggregation network, or the core network (to reach the MTGs, for example), act as labeled BGP PEs and run BGP-labeled unicast sessions with their local AGN-RRs. The PANs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the aggregation community. They learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community. In addition to being labeled BGP PEs, the PANs also act as inline RRs for their local access network Cell Site Gateway (CSG) clients. Each mobile access network subtending from a pair of PANs is part of a unique IS-IS Level 1 domain. All access rings/hub-spokes subtending from the same pair of PANs are part of IS-IS Level 1 domain, where the CSGs are IS-IS L1 nodes and the PAN are L1/L2 nodes. Since routes between the aggregation IS-IS Level 2 (or OSPF backbone) and access IS-IS Level 1 (or OSPF non-backbone area) are not redistributed, the PANs have to reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP switching and allow the aggregation and access IGP routing domains to remain isolated. This PAN NHS function is symmetrically applied by the PANs towards its CSG clients in its local RAN access domain, and the higher level AGN-RR in the aggregation domain.

NOT CISCO CONFIDENTIAL

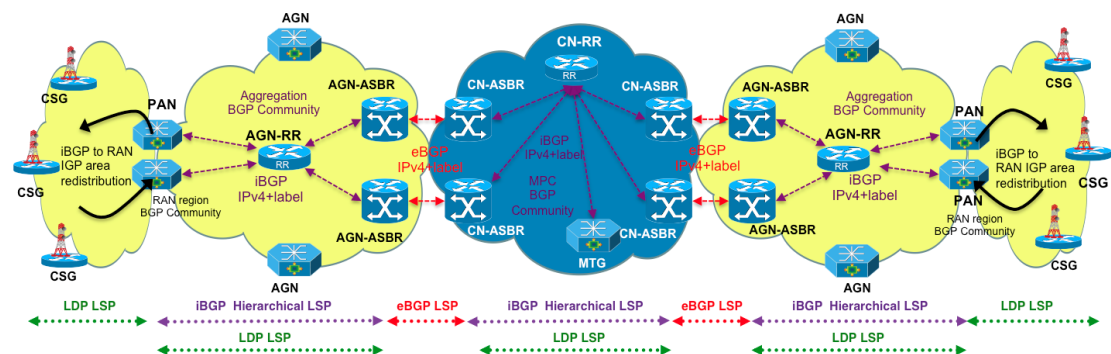
- The CSGs in the RAN access networks are labeled BGP PEs. They peer with iBGP-labeled unicast sessions with their local PAN inline-RRs. The CSGs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the RAN access community. They learn labeled BGP prefixes marked with the MPC BGP community for reachability to the MPC, and the adjacent RAN access BGP community if inter-access X2 connectivity is desired.

The MTGs in the core network are capable of handling large scale and will learn all BGP-labeled unicast prefixes since they need connectivity to all the CGSs in the entire network. Simple prefix filtering based on BGP communities is performed on the CN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into neighboring aggregation domains, where they are not needed. This filtering mechanism is described in detail in [Section 4.5 Prefix Filtering](#). The PANs only learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community. This allows the PANs to enable inter-metro wireline services across the core, and also reflect the MPC prefix to their local access networks. Isolating the aggregation and RAN access domain by preventing the default redistribution enables the mobile access network to have limited route scale, since the CSGs only learn local IGP routes and labeled BGP prefixes marked with the MPC BGP community.

Option-2: Inter-AS Design with IGP/LDP Access

This option is based on the transport model described in [Section 3.2.5 Labeled BGP Core and Aggregation with Redistribution into Access Network IGP](#).

Figure 4-6. Inter-Domain Transport for Inter-AS Design with IGP/LDP Access



This option follows the approach of enabling labeled BGP across the core and aggregation networks and extends the unified MPLS LSP to the access by redistribution between labeled BGP and the access domain IGP. All nodes in the core and aggregation network that require inter-domain LSPs to reach nodes in remote domains act as a labeled BGP PEs and runs iBGP IPv4 unicast+labels with their corresponding local Route Reflectors (RR).

- The core PoP nodes are labeled BGP ASBRs (CN-ASBR). They peer with iBGP-labeled unicast sessions with the centralized CN-RR within the core AS, and peer with eBGP-labeled unicast sessions with the neighboring aggregation ASBRs. The CN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local CN-RRs and eBGP updates towards the neighboring aggregation ASBRs.
- The MTGs residing in the core network are labeled BGP PEs, which connect to the EPC gateways (SGW, PGW, MME) in the MPC. The MTGs peer with iBGP-labeled unicast sessions with the CN-RR, and advertise their loopbacks into iBGP-labeled unicast with a common BGP community (MPC BGP community) representing the MPC.
- The aggregation PoP nodes act as labeled BGP ASBRs (AGN-ASBR) in the aggregation AS. They peer with iBGP-labeled unicast sessions with the centralized AGN-RR within the

NOT CISCO CONFIDENTIAL

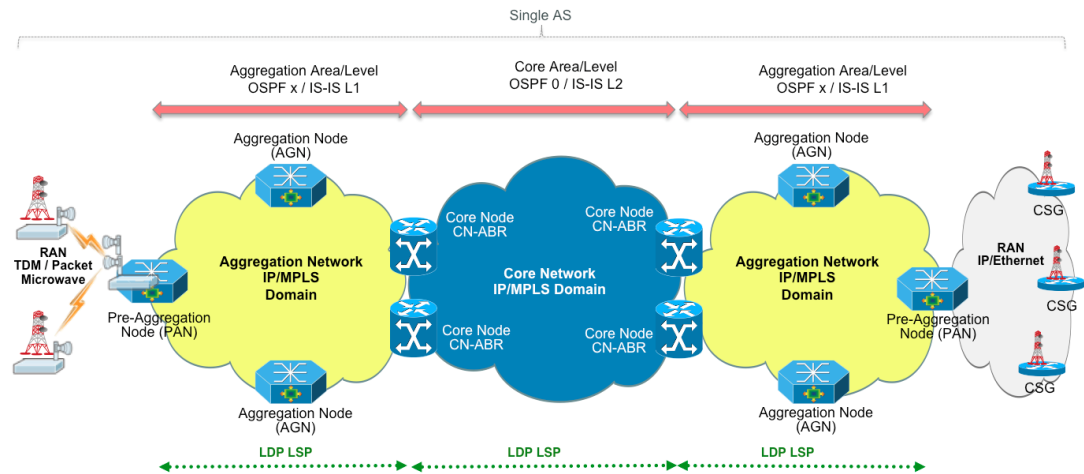
aggregation AS, and peer with eBGP-labeled unicast sessions to the CN-ASBR in the core AS. The AGN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local AGN-RRs and eBGP updates towards neighboring CN-ASBRs.

- All the PANs in the aggregation network that require inter-domain LSPs to reach remote PANs in another aggregation network, or the core network (to reach the MTGs, for example), act as labeled BGP PEs and run BGP-labeled unicast sessions with their local AGN-RRs. The PANs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the aggregation community. They learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community.
- Each mobile access network subtending from a pair of PANs is part of a unique IS-IS Level 1 domain. All access rings/hub-spokes subtending from the same pair of PANs are part of IS-IS Level 1 domain, where the CSGs are IS-IS L1 nodes and the PAN are L1/L2 nodes. The inter-domain LSPs are extended to the MPLS/IP RAN access with a controlled redistribution based on IGP tags and BGP communities. At the PANs, the inter-domain core and aggregation LSPs are extended to the RAN access by redistributing between iBGP and RAN IGP level/area. In one direction, the RAN access node loopbacks (filtered based on IGP tags) are redistributed into iBGP-labeled unicast and tagged with RAN access BGP community that is unique to that RAN access region. In the other direction, the MPC prefixes filtered based on MPC-marked BGP communities, and optionally, adjacent RAN access prefixes filtered based on RAN-region-marked BGP communities (if inter-access X2 connectivity is desired), are redistributed into the RAN access IGP level/area.

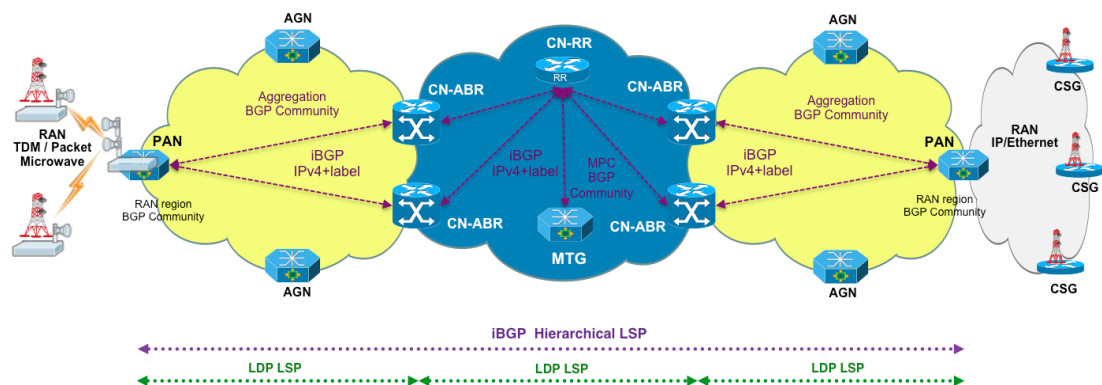
The MTGs in the core network are capable of handling large scale and will learn all BGP-labeled unicast prefixes since they need connectivity to all the CSGs in the entire network. Simple prefix filtering based on BGP communities is performed on the CN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into neighboring aggregation domains, where they are not needed. This filtering mechanism is described in detail in [Section 4.5 Prefix Filtering](#). The PANs only learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community. This allows the PANs to enable inter-metro wireline services across the core, and also reflect the MPC prefix to their local access networks. Using a separate IGP process for the RAN access enables the mobile access network to have limited control plane scale, since the CSGs only learn local IGP routes and labeled BGP prefixes marked with the MPC BGP community.

4.1.3 Large Network, Multi-Area IGP Design with non-IP/MPLS Access

This section details the system architecture for the transport model described in [Section 3.2.3 Labeled BGP Core and Aggregation](#). It assumes that the network organization between the core and aggregation domains is based on a single autonomous system, multi-area IGP design. It assumes a non-MPLS IP/Ethernet or TDM access where all mobile and potentially wireline services are enabled by the aggregation nodes.

NOT CISCO CONFIDENTIAL**Figure 4-7. Multi-Area IGP/LDP Domain Organization**

From an multi-area IGP organization perspective, the core network is either an IS-IS Level 2 or an OSPF backbone area. The aggregation domains, in turn, are IS-IS Level 1 or OSPF non-backbone areas. No redistribution occurs between the core and aggregation IGP levels/areas. This isolation helps reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence. LDP is used for label distribution to build intra-domain LSPs within each independent aggregation and core IGP domain. The access network is based on native IP or Ethernet links over fiber or packet microwave integrated in point-to-point or ring topologies, or based on TDM+Ethernet links over hybrid microwave with point-to-point connectivity.

Figure 4-8. Inter-Domain Transport with Hierarchical LSPs

RFC 3107 procedures based on iBGP IPv4 unicast+label are used as an inter-domain LDP to build hierarchical LSPs across domains. All nodes in the core and aggregation network that require inter-domain LSPs act as labeled BGP PE and run iBGP-labeled unicast peering with designated RRs depending on their location in the network.

- The core PoP nodes are labeled BGP ABRs (CN-ABR) between the aggregation and core areas, and act as inline route reflectors (RR) for their local aggregation area-labeled BGP PE. The CN-ABRs peer with other CN-ABRs using iBGP-labeled unicast in either a full mesh configuration or using centralized RRs over the core network. The centralized RR deployment option is shown in [Figure 4-8](#) above.

NOT CISCO CONFIDENTIAL

- The MTGs residing in the core network are labeled BGP PEs and peer either directly with the closest CN-ABR RRs, in the case of a CN-ABR full-mesh configuration, or with the centralized RRs, depending on the deployment setting. The MTGs advertise their loopbacks into BGP-labeled unicast with a common BGP community representing the MPC. They learn all the labeled BGP prefixes and have reachability across the entire network.
- All aggregation nodes and PANs in aggregation networks that require inter-domain LSPs to either reach nodes in another remote aggregation network, or that need to cross the core network to reach the MTGs, act as labeled BGP PEs, and peer with their local CN-ABR RRs. These aggregation nodes advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the aggregation community. The local CN-ABR RRs may perform BGP egress filtering towards their aggregation clients based on aggregation and MPC-marked BGP communities to drop unwanted remote RAN loopbacks and contain the labeled BGP scale on the aggregation nodes.
- Since redistribution of routes between the core and aggregation IGP levels/areas is prevented in order to keep the routing domains isolated, the CN-ABRs have to insert themselves into the data path to enable inter-domain LSPs. The CN-ABRs acting as inline RRs do this by reflecting the labeled BGP prefixes with NHS symmetrically towards the PANs in their local aggregation network, and MTGs and remote CN-ABRs in the core network.

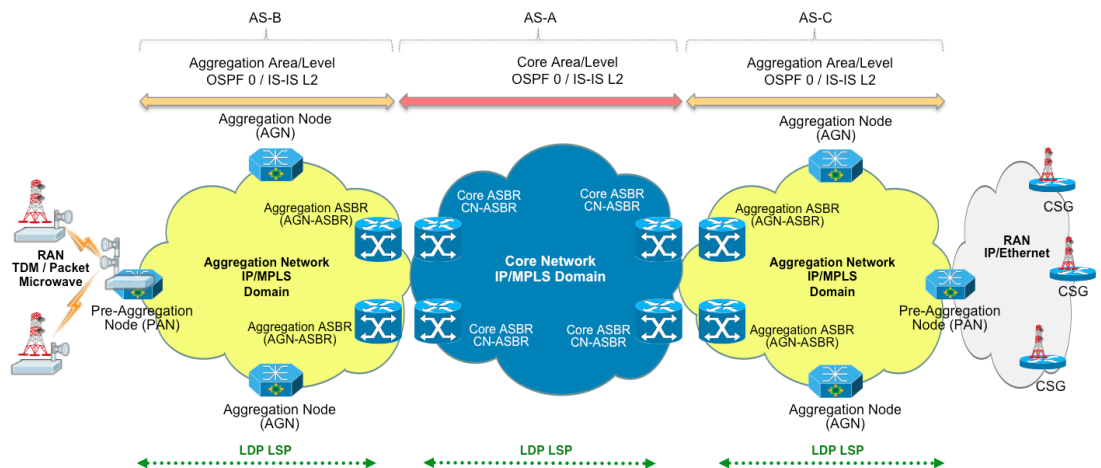
All MPLS services are enabled by the PANs in the aggregation network. These include:

- GSM Abis, ATM IuB, IP IuB, and IP S1/X2 interfaces for 2G/3G/LTE services for RAN access domains with point-to-point connectivity over TDM or hybrid (TDM+Packet) microwave
- IP IuB, and IP S1/X2 interfaces for 3G/LTE services for RAN access domains with point-to-point or ring topologies over fiber or packet microwave.

4.1.4 Large Network, Inter-AS Design with non-IP/MPLS Access

This section details the system architecture for transport model described in [Section 3.2.3 Labeled BGP Core and Aggregation](#). It assumes that the core and aggregation networks are organized as different autonomous systems. It assumes a non-MPLS IP/Ethernet or TDM access where all mobile and potentially wireline services are enabled by the aggregation nodes.

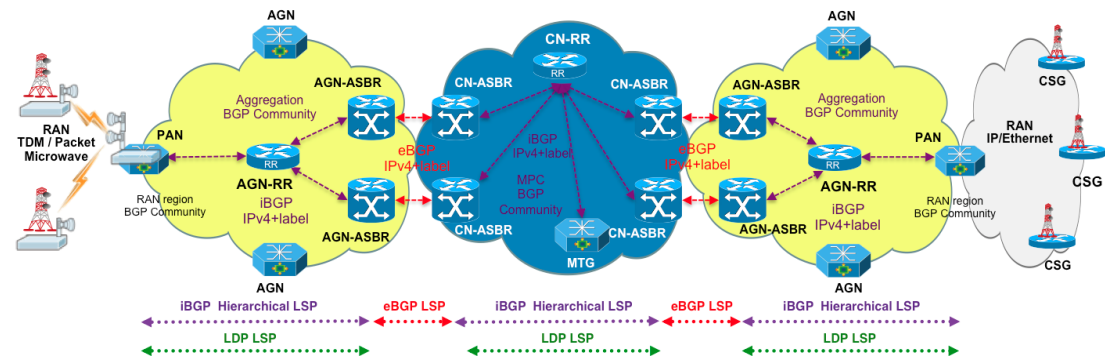
Figure 4-9. Inter-AS IGP/LDP Domain Organization



This model follows the approach of enabling a Unified MPLS LSP using hierarchical-labeled BGP LSPs based on iBGP-labeled unicast within each AS, eBGP-labeled unicast used to extend the LSP

across AS boundaries. The core and aggregation networks are segmented into different autonomous systems. LDP is used for label distribution to build intra-domain LSPs within each independent aggregation and core IGP domain. The access network is based on native IP or Ethernet links over fiber or packet microwave integrated in point-to-point or ring topologies, or based on TDM+Ethernet links over hybrid microwave with point-to-point connectivity.

Figure 4-10. Inter-Domain Transport with Hierarchical LSPs



RFC 3107 procedures based on iBGP IPv4 unicast+label are used as an inter-domain LDP to build hierarchical LSPs across domains. All nodes in the core and aggregation network that require inter-domain LSPs act as labeled BGP PE and run iBGP-labeled unicast peering with designated RRs, depending on their location in the network.

- The MTGs residing in the core network are labeled BGP PEs and peer with iBGP-labeled unicast sessions with the centralized CN-RR. The MTGs advertise their loopbacks into BGP-labeled unicast with a common BGP community representing the MPC. They learn all the labeled BGP prefixes and have reachability across the entire network down to the MPLS/IP RAN access.
- The core PoP nodes act as labeled BGP autonomous system boundary routers (CN-ASBR) in the core AS. They peer with iBGP-labeled unicast sessions with the CN-RR within the core AS, and peer with eBGP-labeled unicast sessions with the neighboring aggregation ASBRs. The CN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all BGP updates towards their local CN-RRs and neighboring aggregation ASBRs.
- The aggregation PoP nodes act as labeled BGP AGN-ASBRs in the aggregation AS. They peer with iBGP-labeled unicast sessions with the centralized AGN-RR within the aggregation AS, and peer with eBGP-labeled unicast sessions to the CN-ASBR in the neighboring AS. The AGN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all BGP updates towards their local AGN-RRs and neighboring core ASBRs.
- All PANs in the aggregation networks that require inter-domain LSPs to either reach nodes in another remote aggregation network, or that need to cross the core network to reach the MTGs, act as labeled BGP PEs, and peer with iBGP-labeled unicast sessions to the local AGN-RR. The PANs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the aggregation community. They learn labeled BGP prefixes marked with the aggregation BGP community and the MPC BGP community.

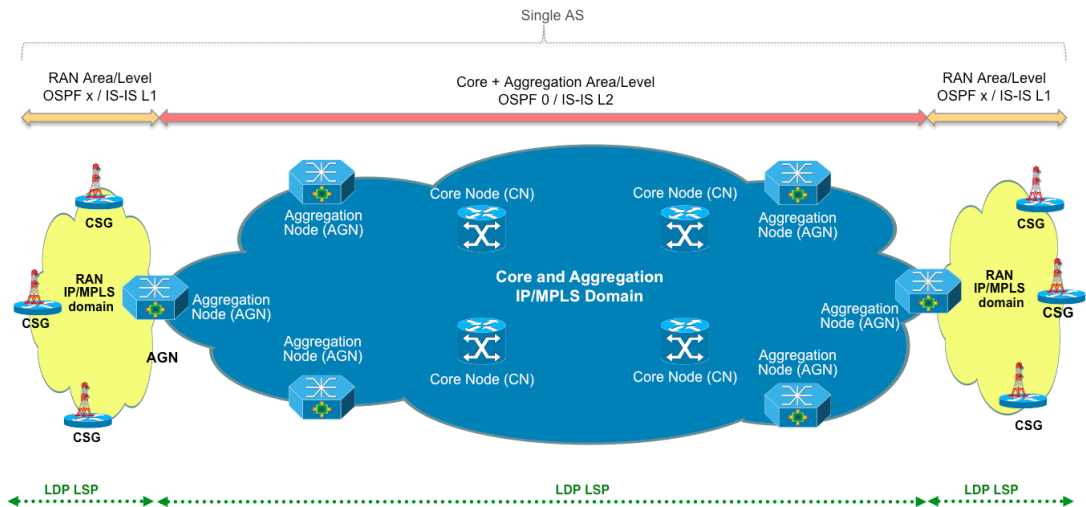
All MPLS services are enabled by the PANs in the aggregation network. These include:

- GSM Abis, ATM IuB, IP IuB, and IP S1/X2 interfaces for 2G/3G/LTE services for RAN access domains with point-to-point connectivity over TDM or hybrid (TDM+Packet) microwave
- IP IuB, and IP S1/X2 interfaces for 3G/LTE services for RAN access domains with point-to-point or ring topologies over fiber or packet microwave.

NOT CISCO CONFIDENTIAL**4.1.5 Small Network, Integrated Core and Aggregation with IP/MPLS Access**

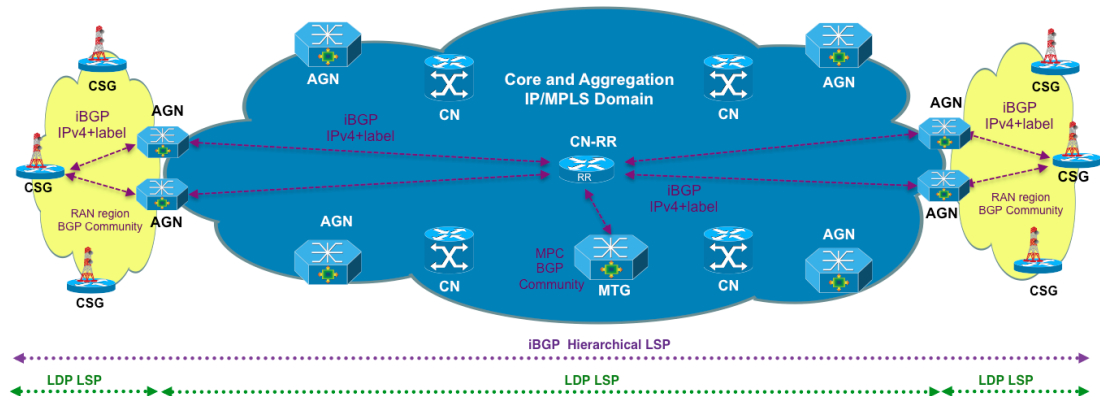
This section details the system architecture for the transport model described in [Section 3.2.2 Labeled BGP Access with Flat LDP Core and Aggregation](#). It assumes that the core and aggregation networks are integrated into a single IGP/LDP domain consisting of less than 1000 nodes. The aggregation nodes have subtending mobile RAN access networks that are MPLS enabled and part of the same AS as the integrated core+aggregation network.

Figure 4-11. Integrated Core and Aggregation with IP/MPLS Access



From an multi-area IGP organization perspective, the integrated core+aggregation networks and the access networks are segmented into different IGP areas or levels, where the integrated core+aggregation network is either an IS-IS Level 2 or an OSPF backbone area, and access networks subtending from the aggregation nodes are in IS-IS Level 1 or OSPF non-backbone areas. No redistribution occurs between the integrated core+aggregation and access IGP levels/areas, thereby containing the route scale within each domain. Partitioning these network layers into such independent and isolated IGP domains helps reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence within each of these domains.

LDP is used for label distribution to build intra-domain LSPs within each independent IGP domain. Inter-domain reachability is enabled with hierarchical LSPs using BGP-labeled unicast as per RFC 3107 procedures, where iBGP is used to distribute labels in addition to remote prefixes, and LDP is used to reach the labeled BGP next-hop.

Figure 4-12. Inter-Domain Transport for Labeled BGP Access with Flat LDP Core and Aggregation

The collapsed core+aggregation and access networks are integrated with labeled BGP LSPs. Any node in the network that requires inter-domain LSPs to reach nodes in remote domain acts as a labeled BGP PE and runs iBGP IPv4 unicast+labels with their corresponding local Route Reflectors (RR).

- The MTGs residing in the core network are labeled BGP PEs. They connect to the EPC gateways (SGW, PGW, MME) in the MPC. The MTGs peer with iBGP-labeled unicast sessions with the CN-RR, and advertise their loopbacks into iBGP labeled unicast with a common BGP community (MPC BGP community) representing the MPC as shown in [Figure 4-12](#) above.
- The Aggregation Nodes (AGN) act as inline-RRs for their local access network CSG clients. Each mobile access network subtending from a pair of AGNs is part of a unique IS-IS Level 1 domain. All access rings/hub-spokes subtending from the same pair of AGNs are part of IS-IS Level 1 domain, where the CSGs are IS-IS L1 nodes and the AGN are L1/L2 nodes. Since routes between the integrated core+aggregation IS-IS Level 2 (or OSPF backbone) and access IS-IS Level 1 (or OSPF non-backbone area) are not redistributed, the AGNs have to reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP switching and allow the two IGP routing domains to remain isolated. This AGN NHS function is symmetrically applied by the AGNs towards its CSG clients in its local RAN access domain, and the higher level CN-RR in the integrated core+aggregation domain.
- The CSGs in the RAN access networks are labeled BGP PEs. They peer with iBGP-labeled unicast sessions with their local AGN inline-RRs. The CSGs advertise their loopbacks into BGP labeled unicast with a common BGP community that represents the RAN access community. They learn labeled BGP prefixes marked with the MPC BGP community for reachability to the MPC, and the adjacent RAN access BGP community if inter-access X2 connectivity is desired.

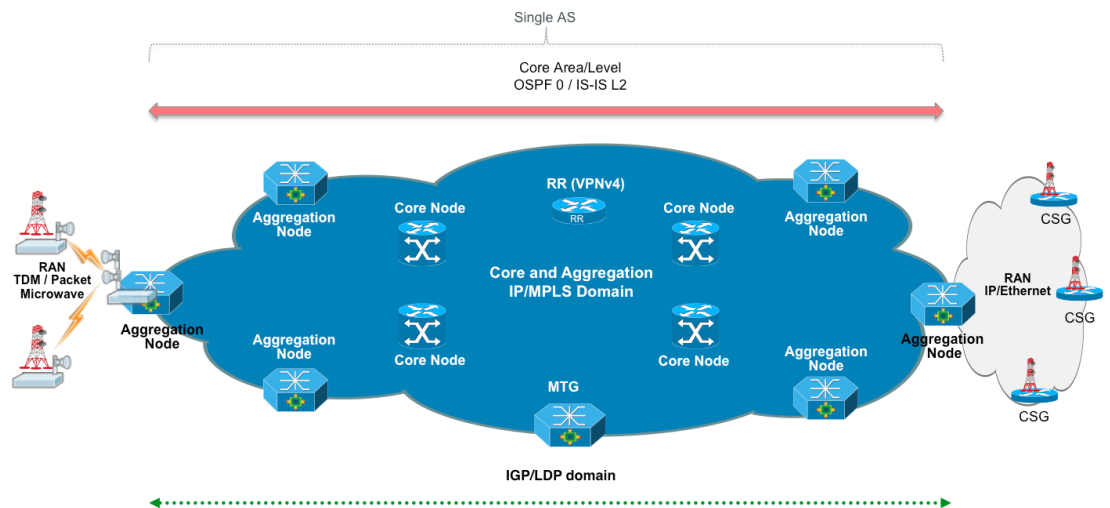
The MTGs in the integrated core+aggregation network are capable of handling large scale and will learn all BGP labeled unicast prefixes since they need connectivity to all the CSGs in the entire network. Simple prefix filtering based on BGP communities is performed on the CN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into other AGNs, where they are not needed. This filtering mechanism is described in detail in [Section 4.5 Prefix Filtering](#). Since all the AGNs are part of the same IGP/LDP domain, they can enable wireline services across each other. The AGNs learn labeled BGP prefixes marked with the MPC BGP community and reflect the MPC prefixes to their local access networks. Isolating the integrated core+aggregation and RAN access domain by preventing the default redistribution enables the mobile access network to have limited route scale, since the CSGs only learn local IGP routes and labeled BGP prefixes marked with the MPC BGP community.

NOT CISCO CONFIDENTIAL

4.1.6 Small Network, Integrated Core and Aggregation with non-IP/MPLS Access

This section details the system architecture for the transport model described in [Section 3.2.1 Flat LDP Core and Aggregation](#).

Figure 4-13. Single-Area IGP with Flat LDP Core and Aggregation



This model assumes that the core and aggregation networks form a single IGP/LDP domain consisting of less than 1000 nodes. Since no segmentation between network layers exists, a flat LDP LSP provides end-to-end reachability across the network. The mobile access is based on TDM and packet microwave links aggregated in aggregation nodes that provide TDM/ATM/Ethernet VPWS and MPLS VPN transport.

All MPLS services are enabled by the aggregation nodes. These include:

- GSM Abis, ATM IuB, IP IuB, and IP S1/X2 interfaces for 2G/3G/LTE services for RAN access domains with point-to-point connectivity over TDM or hybrid (TDM+Packet) microwave
- IP IuB, and IP S1/X2 interfaces for 3G/LTE services for RAN access domains with point-to-point or ring topologies over fiber or packet microwave.

4.2 Service Architecture

The UMMT System design provides transport for both legacy and current mobile services. To accomplish this on a single network, MPLS service virtualization is employed, which provides emulated circuit services via L2VPN for 2G and 3G services and L3VPN services for IP-enabled 3G and 4G/LTE services. Both service models are outlined in this section.

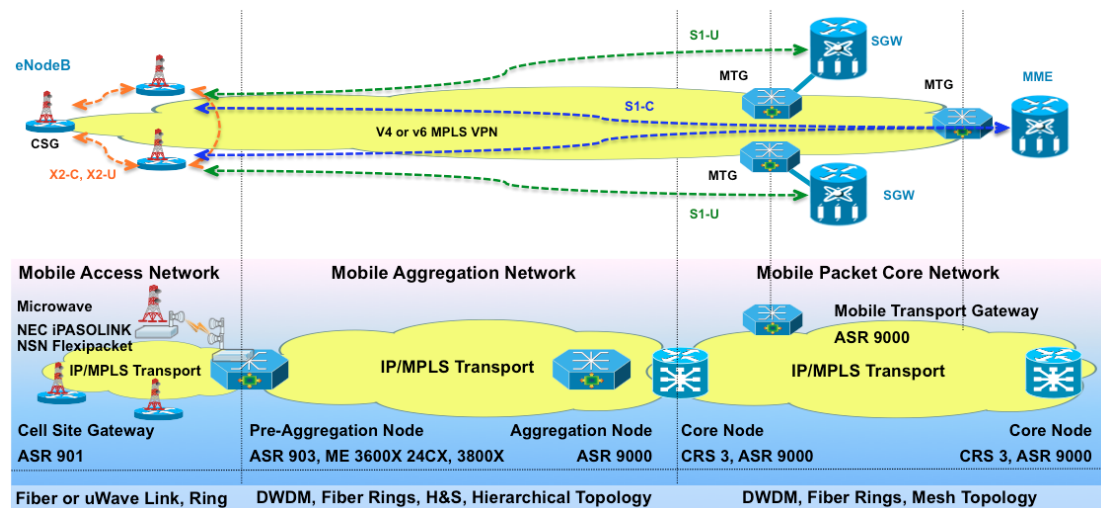
This section includes the following major topics:

- [Section 4.2.1 L3 MPLS VPN Service Model for LTE](#)
- [Section 4.2.2 L2 MPLS VPN Service Model for 2G and 3G](#)
- [Section 4.2.3 Fixed-Mobile Convergence Use Case](#)

NOT CISCO CONFIDENTIAL**4.2.1 L3 MPLS VPN Service Model for LTE**

The UMMT system supports mobile SPs that are introducing 3G UMTS/IP and 4G LTE-based next generation mobile access in order to scale their mobile subscribers and optimize their network infrastructure cost for the mobile broadband growth. To this end, the system proposes a highly-scaled MPLS VPN-based service model to meet the immediate needs of LTE and accelerate its deployment.

Figure 4-14. LTE Backhaul Service



The mobile RAN includes cell sites with eNodeBs that are connected either:

- directly in a point-to-point fashion to the PANs utilizing Ethernet fiber or microwave OR
- through CSGs connected in ring topologies using MPLS/IP packet transport over Ethernet fiber or microwave transmission.

The cell sites in the RAN access are collected in a MPLS/IP pre-aggregation/aggregation network that may be comprised of a physical hub-and-spoke or ring connectivity that interfaces with the MPLS/IP core network that hosts the EPC gateways.

From the E-UTRAN backhaul perspective, the most important LTE/SAE reference points are the X2 and S1 interfaces. The eNodeBs are interconnected with each other via the X2 interface, and towards the EPC via the S1 interface.

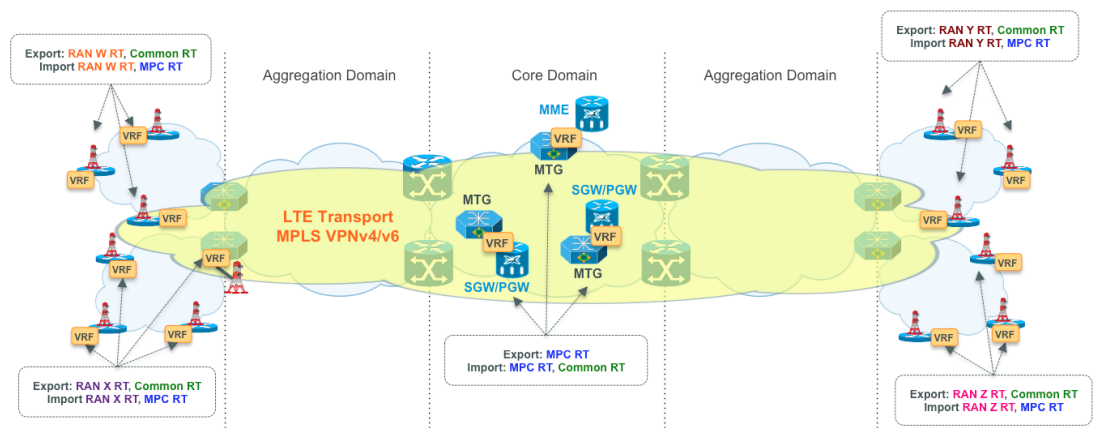
- The **S1-c** or **S1-MME** interface is the reference point for the control plane between E-UTRAN and MME. The S1-MME interface is based on the S1 Application Protocol (S1AP) and is transported over the Stream Control Transmission Protocol (SCTP). The EPC architecture supports MME pooling to enable geographic redundancy, capacity increase, and load sharing. This requires the eNodeB to connect to multiple MMEs. The L3 MPLS VPN service model defined by UMMT allows eNodeBs in the RAN access to be connected to multiple MMEs that may be distributed across regions of the core network for geographic redundancy.
- The **S1-u** interface is the reference point between E-UTRAN and SGW for the per-bearer user plane tunneling and inter-eNodeB path switching during handover. The application protocol used on this interface is GTPv1-U, transported over User Datagram Protocol (UDP). SGW locations affect u-plane latency, and the best practice for LTE is to place S/PGWs in regions closer to the aggregation networks that they serve so that the latency budget of the eNodeBs to which they connect is not compromised. The EPC architecture supports SGW pooling to enable load balancing, resiliency, and signaling optimization by reducing the handovers. This requires the

eNodeB to connect to multiple SGWs. The L3 MPLS VPN service model allows eNodeBs in the RAN access to be connected to multiple SGWs, which include ones in the core close to the local aggregation network and SGWs that are part of the pool serving neighboring core PoPs.

- The **X2** interface comprised of the X1-c and X2-u reference points for control and bearer plane provides direct connectivity between eNodeBs. It is used to hand over a User Equipment (UE) from a source eNodeB to a target eNodeB during the inter-eNodeBs handover process. For the initial phase of LTE, the traffic passed over this interface is mostly control plane related to signaling during handover. This interface is also used to carry bearer traffic for a short period (<100ms) between the eNodeBs during handovers. The stringent latency requirements of the X2 interface requires that the mesh connectivity between CSGs introduces a minimum amount of delay that is in the order of 30ms. The L3 MPLS VPN service model provides shortest path connectivity between eNodeBs so as to not introduce unnecessary latency.
- During initial deployments in regions with low uptake and smaller subscriber scale, MME and SGW/(packet data network gateways (PGW)) pooling can be used to reuse mobile gateways serving neighboring core PoPs. Gradually, as capacity demands and subscriber scale increases, newer gateways can be added closer to the region. L3 MPLS VPN service model for LTE backhaul that is defined by the UMMT System allows migrations to newer gateways to take place without any re-provisioning of the service model or re-architecting of the underlying transport network required.
- With the distribution of the new spectrum made available for 3G and 4G services, many new SPs have entered the mobility space. These new entrants would like to monetize the spectrum they have acquired, but lack the national infrastructure coverage owned by the incumbents. LTE E-UTRAN-sharing architecture allows different core network operators to connect to a shared radio access network. The sharing of cell site infrastructure could be based on:
 - A shared eNodeB: shared backhaul model where different operators are presented on different VLANs by the eNodeB to the CSG, OR
 - A different eNodeB: shared backhaul model where the foreign operator's eNodeB is connected on a different interface to the CSG.

Regardless of the shared model, the UMMT System provides per-mobile SP-based L3 MPLS VPNs that are able to identify, isolate, and provide secure backhaul for different operator traffic over a single converged network.

Figure 4-15. L3 MPLS VPN Service Model



The UMMT System proposes a simple and efficient L3 service model that addresses the LTE backhaul requirements addressed above. The L3 service model is built over a unified MPLS transport with a

NOT CISCO CONFIDENTIAL

common highly-scaled MPLS VPN that covers LTE S1 interfaces from all CSGs across the network and a LTE X2 interface per RAN access region. The single MPLS VPN per operator is built across the network with VRFs on the MTGs connecting the EPC gateways (SGW, MME) in the MPC, down to the RAN access with VRFs on the CSGs connecting the eNodeBs. Prefix filtering across the VPN is done using simple MP-BGP Route Target (RT) import and export statements on the CSGs and MTGs.

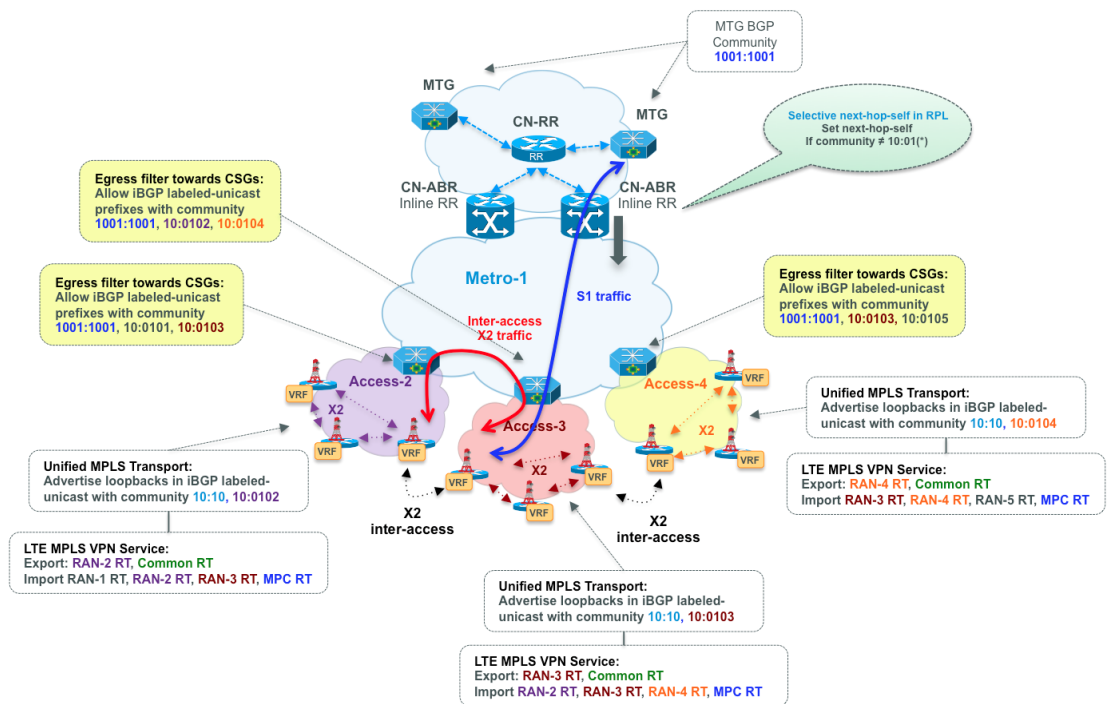
Denoted in [Figure 4-15](#):

- A unique RT denoted as **Common RT** is assigned to the LTE backhaul MPLS VPN. It is either imported or exported at various locations or the VPN, depending on the role of node implementing the VRF.
- A unique RT denoted by **MPC RT** is assigned to the MTGs in the MPC.
- Each RAN access region in the network is assigned a unique RT. These RTs are denoted as **RAN X, RAN Y, and RAN Z RTs**.

In every RAN access region, all CSGs import the *MPC RT* and the *RAN x RT*. The CSGs export the *Common RT* and the *RAN x RT*. Here *x* denotes the unique RT assigned to that RAN access region. With this importing and exporting of RTs, the route scale in the VRF of the CSGs is kept to a minimum since VPNv4 prefixes corresponding to CSGs in other RAN access regions – either in the local aggregation domain, or RAN access regions in remote aggregation domain across the core – are not learnt. The CSGs have reachability to every MTG and the corresponding EPC gateways (SGW, MME) that they connect anywhere in the MPC. They also have shortest path mesh connectivity among themselves for the X2 interface.

In the MPC, the MTGs import the *MPC RT* and the *Common RT*. They export only the *MPC RT*. With this importing and exporting of RTs, the MTGs have connectivity to all other gateways in the MPC, as well as connectivity to the CSGs in the RAN access regions across the entire network. The MTGs are capable of handling large scale and learn all VPNv4 prefixes in the LTE VPN.

The rapid adoption of LTE and the massive increase in subscriber growth is leading to an exponential increase in cell sites that are being deployed in the network. This is introducing a crunch in the number of IP addresses that need to be assigned to the eNodeBs at the cell sites. For mobile SPs that are running out of public IPv4 addresses, or those that cannot obtain additional public IPv4 addresses from the registries for eNodeB assignment, the UMMT system enables carrying IPv6 traffic over a IPv4 Unified MPLS transport infrastructure using 6VPE as defined in RFC 4659. The eNodeBs and EPC gateways can be IPv6 only, or dual-stack enabled to support IPv6 for S1 and X2 interfaces, while using IPv4 for network management functions, if desired. The dual-stack enabled eNodeBs and EPC gateways connect to CSGs and MTGs configured with a dual-stack VRF carrying VPNv4 and VPNv6 routes for the LTE MPLS VPN service. The IPv6 reachability between the eNodeBs in the cell site and the EPC gateways in the MPC is exchanged between the CSGs and MTGs acting as MPLS VPN PE's using the BGP address family [AFI=2, SAFI=128].

Figure 4-16. Inter-Access X2 Connectivity

In some cases, depending on the spread of the macro cell footprint, it might be desirable to provide X2 interfaces between CSGs located in neighboring RAN access regions. This connectivity can easily be accomplished using the BGP community-based coloring of prefixes used in the unified MPLS transport.

- As described in [Section 4.1 Transport Architecture](#), the CSG loopbacks are colored in BGP labeled-unicast with a common BGP community that represents the RAN community and a BGP community that is unique to that RAN access region. This tagging can be done when the CSGs advertise their loopbacks in iBGP labeled-unicast as shown in [Figure 4-16](#) if labeled BGP is extended to the access, or at the PANs when redistributing from the RAN IGP to iBGP when IGP/LDP is used in the the RAN access using the redistribution approach.
- The adjacent RAN access domain CSG loopbacks can be identified at the PAN based on the unique RAN access region BGP community and be selectively propagated into the access based on egress filtering as shown in [Figure 4-16](#), if labeled BGP is extended to the access, or be selectively redistributed into the RAN IGP if IGP/LDP is used in the the RAN access using the redistribution approach.

It is important to note that X2 interfaces are based on eNB proximity, and therefore a given RAN access domain only requires connectivity to the ones immediately adjacent. This filtering approach allows for hierarchical-labeled BGP LSPs to be set up across neighboring access regions while preserving the low route scale in the access. At the service level, any CSG in a RAN access domain that needs to establish inter-access X2 connectivity will import its neighboring CSG access region RT in addition to its own RT in the LTE MPLS VPN as shown in [Figure 4-16](#) above.

The CN-ABR inline-RR applies selective NHS function using Route Policy in the egress direction towards its local PAN neighbor group in order to provide shortest-path connectivity for the X2 interface between CSGs across neighboring RAN access regions. The Routing Policy Language (RPL) logic involves changing the next-hop towards the PANs for only those prefixes that do not match the local RAN access regions based on a simple regular expression matching BGP communities. This

NOT CISCO CONFIDENTIAL

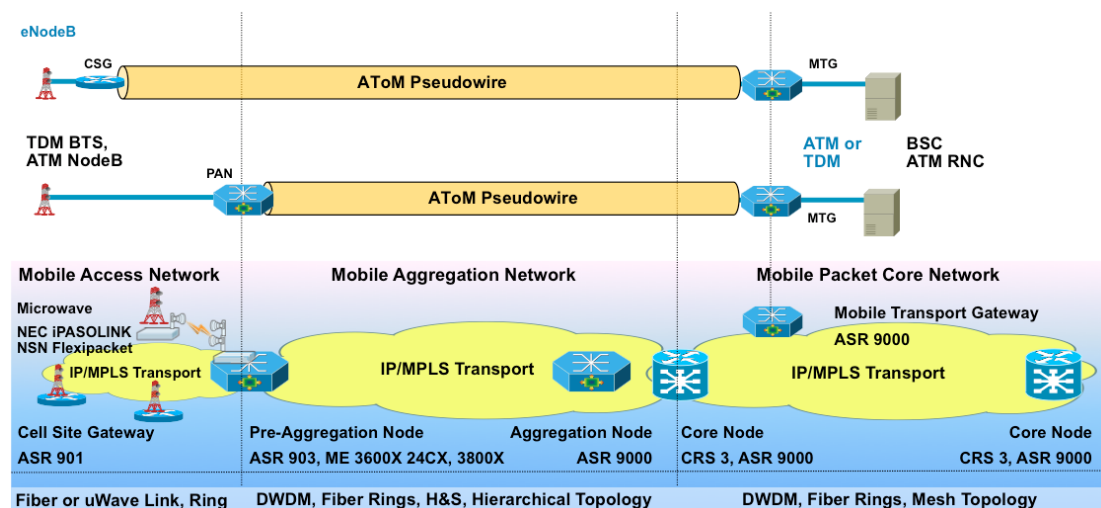
allows for the CN-ABR to change the BGP next-hop and insert itself in the data path for all prefixes that originate in the core corresponding to the S1 interface, while keeping the next-hop set by the PANs unchanged for all prefixes from local RAN regions. With this, the inter-access X2 traffic flows across adjacent access regions along the shortest path interconnecting the two PANs without having to loop through the inline-RR CN-ABR node.

4.2.2 L2 MPLS VPN Service Model for 2G and 3G

The UMMT system architecture allows MSPs with TDM-based 2G GSM and ATM-based 3G UMTS infrastructures to remove, reduce, or cap investments in SONET/SDH and ATM transport infrastructure through the use of MPLS-based CEoP services.

- For the MSPs that want to reduce SONET/SDH infrastructure used for GSM, UMMT enables PWE3-based transport of emulated TDM circuits. Structured circuit emulation is achieved with CESoPSN, and unstructured emulation is achieved with SAToP. E1/T1 circuits from BTS equipment connected to the CSG or to the PAN are transported to MTG, where they are bundled into channelized STM1/OC-3 interfaces for handoff to the BSC. Synchronization is derived from the BSC via TDM links, or from a Primary Reference Clock (PRC), and transported across the core, aggregation, and access domains via SyncE, or via 1588 across domains where SyncE is not supported.
- For the MSPs that want to reduce their ATM infrastructure used for ATM-based UMTS, UMMT enables PWE3-based transport of ATM VC (AAL0 or AAL5) or VP (AAL0) circuits. ATM E1/T1 or IMA interfaces from NodeB equipment connected to the CSG or PAN are transported to the MTG, where they are bundled into STM1 ATM interfaces for handoff to the RNC. Cell packing may be used to optimize the bandwidth used for this transport. Synchronization is derived from the RNC via ATM links, or from a PRC, and transported across the core, aggregation, and access domains via SyncE, or via 1588 across domains where SyncE is not supported.

Figure 4-17. ATM/TDM Transport Services



Typical GSM (2G) deployments will consist of cell sites that don't require a full E1/T1 for support. In such cell sites, a fractional E1/T1 is used. The operator can deploy these cell sites in a daisy chain fashion (i.e., down a highway) or aggregate them at the BSC location. To save in the CAPEX investment on the number of channelized STM-1/OC-3 ports required on the BSC, the operator will utilize a digital XConnect to merge multiple fractional E1/T1 links into a full E1/T1. This reduces the number of T1/E1s needed on the BSC, which results in fewer channelized STM-1/OC-3 ports

NOT CISCO CONFIDENTIAL

being needed. Deploying CESoPSN PWs from the CSG to the RAN distribution node supports these fractional T1/E1s and the aggregation of them at the BSC site. In this type of deployment, the default behavior of CESoPSN for alarm sync needs to be changed. Typically, if a T1/E1 on the access nodes goes down, the PWs will forward the AIS alarm through the PW to the distribution node and then propagate the alarm indication signal (AIS) alarm to the BSC by taking the T1/E1 down. In this multiplexed scenario, TS alarming must be enabled on a CESoPSN PW to only propagate the AIS alarm on the affected time slots, thus not affecting the other time slots (e.g., cell sites) on the same T1/E1.

The same BGP-based control plane and label distribution implemented for the L3VPN services is also used for circuit emulation services. For hub-and-spoke access topologies, BFD-protected static routes can be used to eliminate the need for an IGP at the cell site. The CSGs utilize MPLS/IP routing in this system release when deployed in a physical ring topology. TDM and ATM PWE3 can be overlaid in either deployment model.

The CSGs, PAN, aggregation nodes, and MTGs enforce the contracted ATM CoS SLA, and mark the ATM and TDM PWE3 traffic with the corresponding PHB inside the access, aggregation, and core DiffServ domains. The MTG enables multi-router automatic protection switching (MR-APS) (or single-router automatic protection switching (SR-APS)) redundancy for the BSC or RNC interface, as well as pseudowire redundancy and two-way pseudowire redundancy for transport protection.

4.2.3 Fixed-Mobile Convergence Use Case

This section describes how a wireline L2VPN service can be enabled in the access network to facilitate fixed-mobile converged deployments. This scenario assumes that the cell site is located in a urban area with fiber access from the business to the CSG. A CSG is used as a T-PE in this example, but the model is applicable to any MPLS-enabled access node subtending from the pre-aggregation.

Figure 4-18. Wireline VPWS Service between CSGs across the Core Network

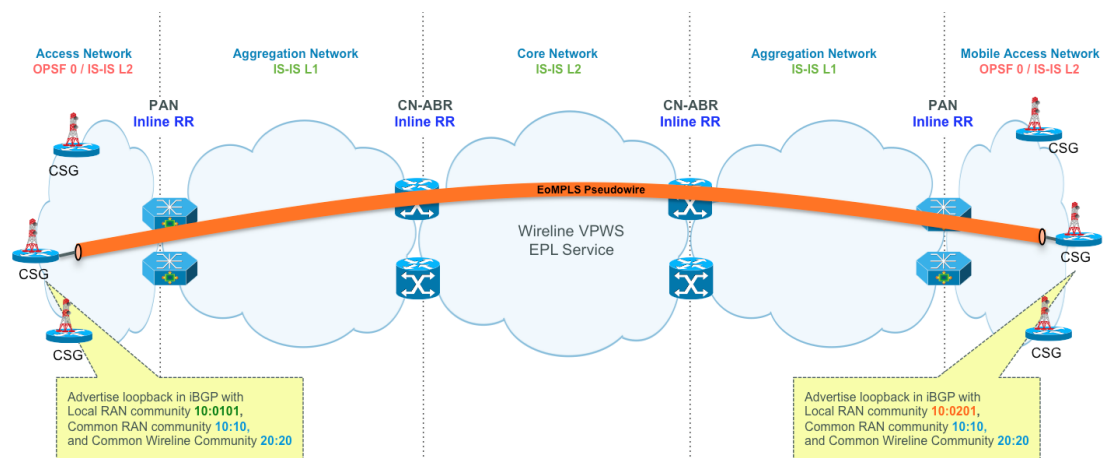
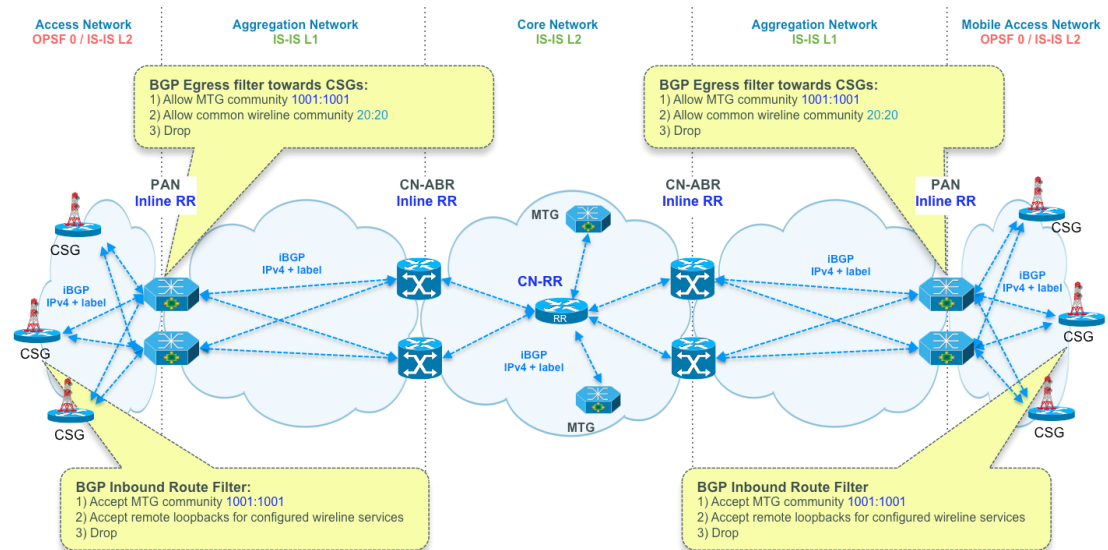


Figure 4-18 shows a wireline VPWS like an Ethernet Private Line (EPL) or Ethernet Virtual Private Line (EVPL) business service enabled using an EoMPLS pseudowire between two CSGs in the RAN access across the core network. The CSGs enabling the VPWS learn each others loopbacks via BGP labeled-unicast that is extended to the access network using the PANs as inline RR, as described in [Section 3.2.4 Labeled BGP Core, Aggregation, and Access](#). As detailed in the [Section 4.1 Transport Architecture](#), the route scale in the RAN access is kept to a minimum by egress filtering on the PAN inline-RRs. The CSGs that enable mobile services advertise their loopbacks in iBGP labeled-unicast with a unique local RAN community and a common RAN community. The PANs acting as inline-RRs only reflect prefixes marked with the local RAN community (corresponding to local CSG loopbacks) and MTG community (corresponding to MTG loopbacks) towards the RAN access.

NOT CISCO CONFIDENTIAL

In this case, since we are enabling a new service, we need to use an additional BGP community. The CSGs that also enable wireline services, tag their loopbacks in iBGP labeled-unicast with a common wireline community in addition to the local RAN and common RAN community. Note that this common wireline community is only used on CSGs where wireline services are enabled. The filtering mechanism used to maintain the low route scale in the RAN while enabling this fixed-mobile deployment is explained below.

Figure 4-19. Scalability Control for Fixed-Mobile Converged Deployments



When reflecting labeled BGP routes towards their CSG clients, the PAN inline-RRs follow the logic of:

1. Allowing the MTG community.
2. Allowing the common wireline community.
3. Dropping all other prefixes.

The first rule enables the LTE S1 between the CSGs and the MPC. Reachability for VPN next-hops for LTE X2 interface between CSGs is available through LDP LSPs since the CSGs are in same RAN IGP/LDP domain. The second rule enables wireline services to the access. All other prefixes are dropped to ensure only required prefix updates are sent to the RAN access. This filtering logic is a one time configuration that is performed on the PANs.

The CSGs on the other hand perform inbound filtering on a per PAN RR neighbor basis using a route-map that:

1. Accepts the MTG community.
2. Accepts loopbacks of remote destination to which wireline service(s) are configured on the device.
3. Drops all other prefixes.

When a wireline service is activated to new destination, the route-map used for inbound filtering has to be updated. Since adding a new wireline service on the device results in a change in the routing policy of a BGP neighbor, dynamic inbound soft reset function is used to initiate nondisruptive dynamic

NOT CISCO CONFIDENTIAL

exchange of route refresh requests between the CSG and the PAN. Note that both BGP peers must support the route refresh capability to use dynamic inbound soft reset capability.

```

route-map Inbound_Filter permit 10
  match community Allowed_Communities
!
route-map Inbound_Filter permit 20
  match ip address prefix-list WL-Service-Destinations
!
ip community-list standard Allowed_Communities permit 10:101
ip community-list standard Allowed_Communities permit 1001:1001
!
ip prefix-list WL-Service-Destinations seq 5 permit 100.111.13.23/32
ip prefix-list WL-Service-Destinations seq 6 permit 100.111.13.24/32

router bgp 100
  address-family ipv4
    neighbor 100.111.9.17 route-map Inbound_Filter in <<< PAN inline-RR K0917
    neighbor 100.111.9.18 route-map Inbound_Filter in <<< PAN inline-RR K0918

```

4.3 Inter-Domain Hierarchical LSPs

The UMMT System uses hierarchical LSPs for inter-domain transport. The hierarchical LSP is based on a BGP-distributed label that is used to transit the isolated MPLS domains, and a LDP-distributed label that is used intra-domain to reach the labeled BGP next hop. This section describes the different hierarchical LSPs that apply to various transport architecture options and their corresponding service models.

This section includes the following topics:

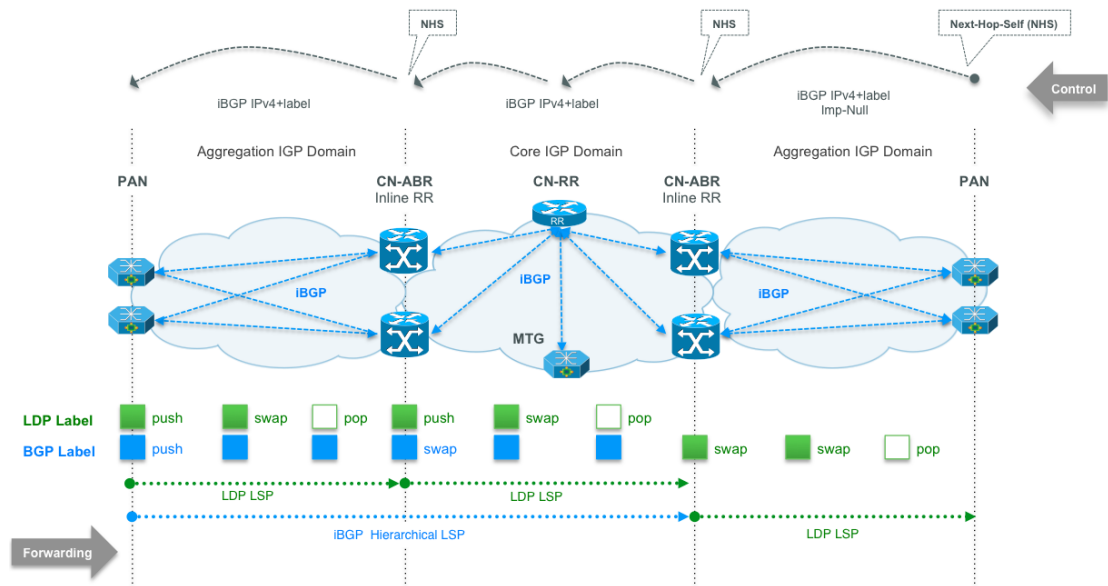
- [Section 4.3.1 Inter-Domain LSPs for Multi-Area IGP Design](#)
- [Section 4.3.2 Inter-Domain LSPs for Inter-AS Design](#)
- [Section 4.3.3 Inter-Domain LSPs for Integrated Core and Aggregation Design](#)

4.3.1 Inter-Domain LSPs for Multi-Area IGP Design

This section describes inter-domain hierarchical LSPs that apply to Large Network, Single-AS Multi-Area IGP designs where the core and aggregation networks are part of the same autonomous system, but segmented into isolated IGP areas.

Hierarchical LSPs between Remote PANs for Multi-Area IGP Design

This scenario applies to inter-domain LSPs between the loopback addresses of remote PANs connected across the core network. It is relevant to wireline L2/L3 MPLS VPN business services deployed between remote PANs across the core network, that use the /32 loopback address of the remote PEs as the endpoint identifier for the t-LDP or MP-iBGP sessions. The PANs are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4).

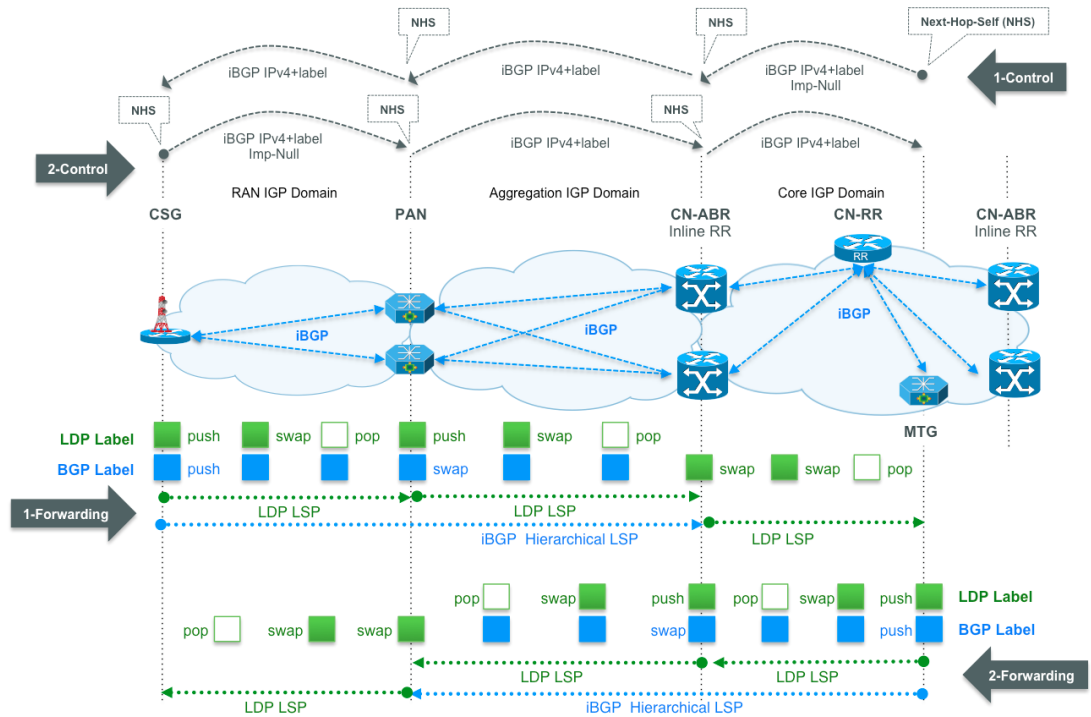
Figure 4-20. Hierarchical LSPs between Remote PANs for Multi-Area IGP Design

The remote PANs learn each other's loopbacks through BGP-labeled unicast. For traffic flowing between the two PANs as shown in [Figure 4-20](#), the following sequence occurs:

1. The downstream PAN pushes the BGP label corresponding to the remote prefix, and then pushes the LDP label that is used to reach the local core ABR (CN-ABR) that is the labeled BGP next hop.
2. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a penultimate hop popping (PHP) before handing to the local CN-ABR.
3. The local CN-ABR will swap the BGP-based inter-domain LSP label, and push the LDP label used to reach the remote CN-ABR that is the labeled BGP next hop.
4. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the remote CN-ABR.
5. Since the remote CN-ABR has reachability to the destination PAN via IGP, it will swap the BGP label with an LDP label corresponding to the upstream PAN intra-domain LDP LSP.

Hierarchical LSPs between CSG and MTG for Multi-Area IGP Design with Labeled BGP Access

The inter-domain hierarchical LSP described here applies to the *Option-1: Multi-Area IGP Design with Labeled BGP Access* transport model described in [Section 4.1.1 Large Network, Multi-Area IGP Design with IP/MPLS Access](#). This scenario applies to inter-domain LSPs between the loopback addresses of CSGs in the RAN and the MTGs in the core network. It is relevant to 4G LTE and 3G UMTS/IP services deployed using MPLS L3 VPNs or 2G GSM and 3G UMTS/ATM services deployed using MPLS L2 VPNs that use the /32 loopback address of the remote PEs as the endpoint identifier for the t-LDP or MP-iBGP sessions. The MTGs and CSGs are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4).

Figure 4-21. Hierarchical LSPs between CSGs and MTGs for Multi-Area IGP Design with Labeled BGP Access

The CSG in the RAN access learns the loopback address address of the MTG through BGP-labeled unicast. For traffic flowing between the CSG in the RAN and the MTG in the MPC, as shown in Figure 4-21, the following sequence occurs:

1. The downstream CSG node will first push the BGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the PAN that is the labeled BGP next hop.
2. The CSGs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the PAN.
3. The PAN will swap the BGP label corresponding to the remote prefix, and then push the LDP label used to reach the CN-ABR that is the labeled BGP next hop.
4. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the local CN-ABR.
5. Since the local CN-ABR has reachability to the MTG via the core IGP, it will swap the BGP label with an LDP label corresponding to the upstream MTG intra-domain core LDP LSP.

The MTG in the MPC learns the loopback address of the remote RAN CSG through BGP-labeled unicast. For traffic flowing between the MTG and the CSG in the RAN as shown in Figure 4-21, the following sequence occurs:

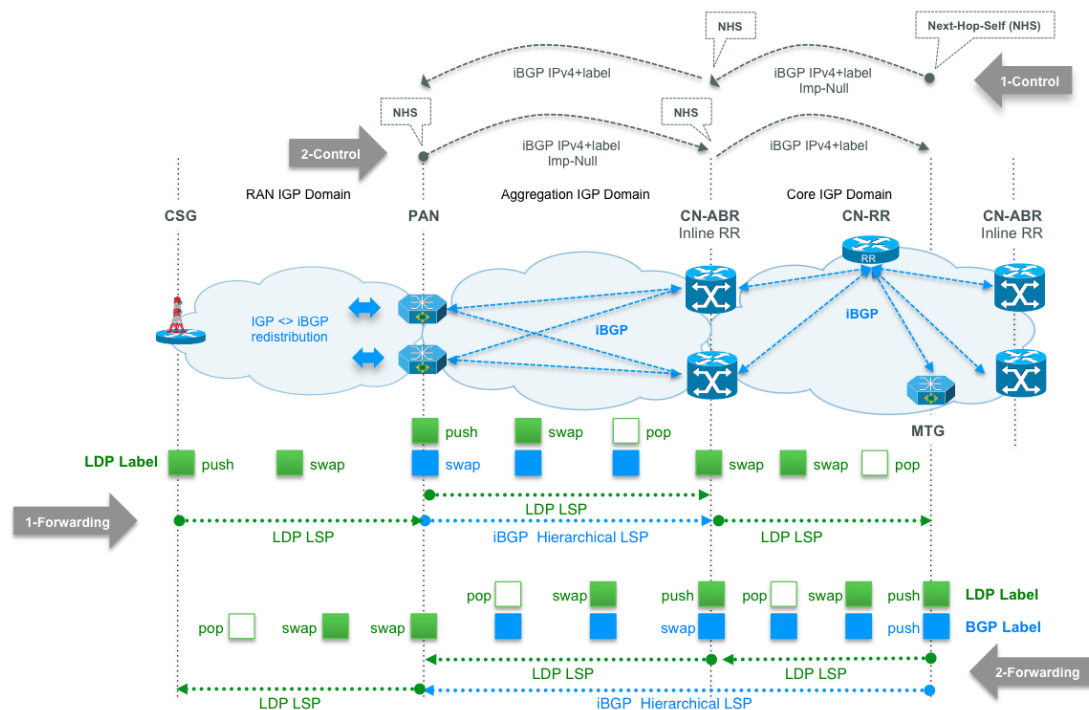
1. The downstream MTG node will first push the BGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the CN-ABR that is the labeled BGP next hop.
2. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the CN-ABR.
3. The CN-ABR will swap the BGP label corresponding to the remote prefix, and then push the LDP label used to reach the PAN that is the labeled BGP next hop.

4. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the PAN.
5. Since the PAN has reachability to the CSG via the RAN IGP process, it will swap the BGP label with an LDP label corresponding to the upstream CSG intra-domain RAN LDP LSP.

Hierarchical LSPs between CSG and MTG for Multi-Area IGP Design with IGP/LDP Access

The inter-domain hierarchical LSP described here applies to the *Option-2: Multi-Area IGP Design with IGP/LDP Access* transport model described in [Section 4.1.1 Large Network, Multi-Area IGP Design with IP/MPLS Access](#). This scenario applies to inter-domain LSPs between the loopback addresses of CSGs in the RAN and the MTGs in the core network. It is relevant to 4G LTE and 3G UMTS/IP services deployed using MPLS L3 VPNs or 2G GSM and 3G UMTS/ATM services deployed using MPLS L2 VPNs that use the /32 loopback address of the remote PE as the endpoint identifier for the t-LDP or MP-iBGP sessions. The MTGs are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4). The CSGs do not run labeled BGP, but have connectivity to the MPC via the redistribution between RAN IGP and BGP-labeled unicast done at the local PANs, which are the labeled BGP PEs.

Figure 4-22. Hierarchical LSPs between CSGs and MTGs for Multi-Area IGP Design with IGP/LDP Access



The CSG in the RAN access learns the loopback address address of the MTG through the BGP-labeled unicast to RAN IGP redistribution done at the PAN. For traffic flowing between the CSG in the RAN and the MTG in the MPC, as shown in [Figure 4-22](#), the following sequence occurs:

1. The downstream CSG will push the LDP label used to reach the PAN that redistributed the labeled BGP prefix into the RAN IGP.
2. The CSGs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label towards the PAN.

NOT CISCO CONFIDENTIAL

3. The PAN will first swap the LDP label with the BGP label corresponding to the remote prefix, and then push the LDP label used to reach the local CN-ABR that is the labeled BGP next hop.
4. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the local CN-ABR.
5. Since the local CN-ABR has reachability to the MTG via the core IGP, it will swap the BGP label with an LDP label corresponding to the upstream MTG intra-domain core LDP LSP.

The MTG in the MPC learns the loopback address of the remote RAN CSG through BGP-labeled unicast. For traffic flowing between the MTG and the CSG in the RAN as shown in [Figure 4-22](#), the following sequence occurs:

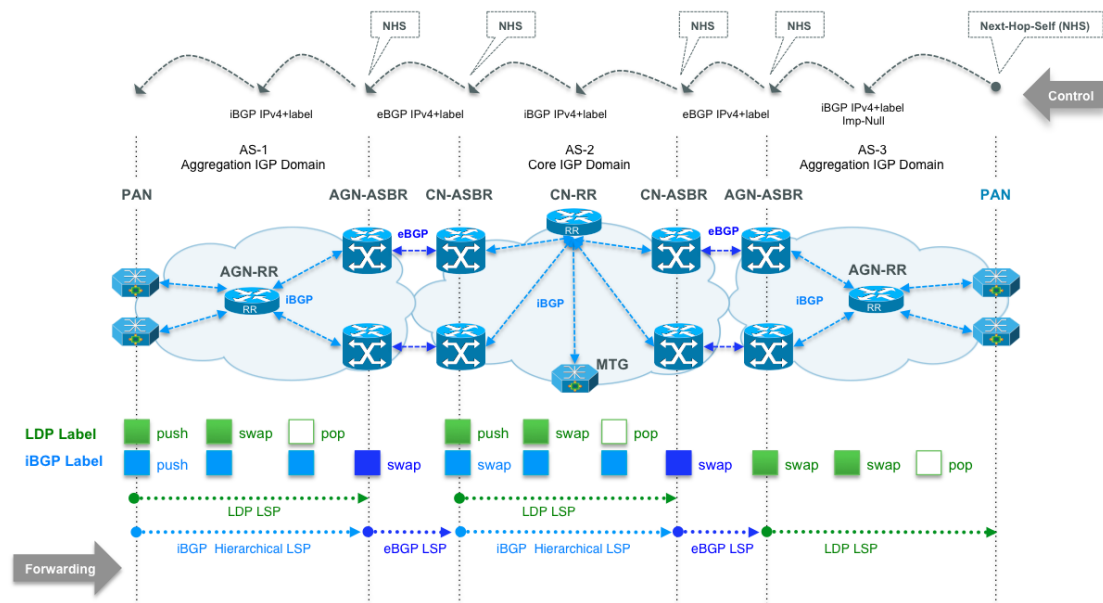
1. The downstream MTG node will first push the BGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the CN-ABR that is the labeled BGP next hop.
2. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the CN-ABR.
3. The CN-ABR will swap the BGP label corresponding to the remote prefix, and then push the LDP label used to reach the PAN that is the labeled BGP next hop.
4. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the PAN connecting the RAN.
5. The PAN will swap the locally-assigned BGP label and forward to the upstream CSG using the local RAN intra-domain LDP-based LSP label.

4.3.2 Inter-Domain LSPs for Inter-AS Design

This section describes inter-domain hierarchical LSPs that apply to inter-AS designs where the core and aggregation networks are segmented into different autonomous systems.

Hierarchical LSPs between Remote PANs for Inter-AS Design

This scenario applies to inter-domain LSPs between the loopback addresses of remote PANs connected across the core network. It is relevant to wireline L2/L3 MPLS VPN business services deployed between remote PANs across the core network that use the /32 loopback address of the remote PEs as the endpoint identifier for the t-LDP or MP-iBGP sessions. The PANs are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4).

Figure 4-23. Hierarchical LSPs between Remote PANs for Inter-AS Design

The remote PANs learn each other's loopbacks through BGP-labeled unicast. iBGP-labeled unicast is used to build the inter-domain hierarchical LSP inside each autonomous systems, and eBGP-labeled unicast is used to extend the LSP across the AS boundary. For traffic flowing between the two PANs as shown in [Figure 4-23](#), the following sequence occurs:

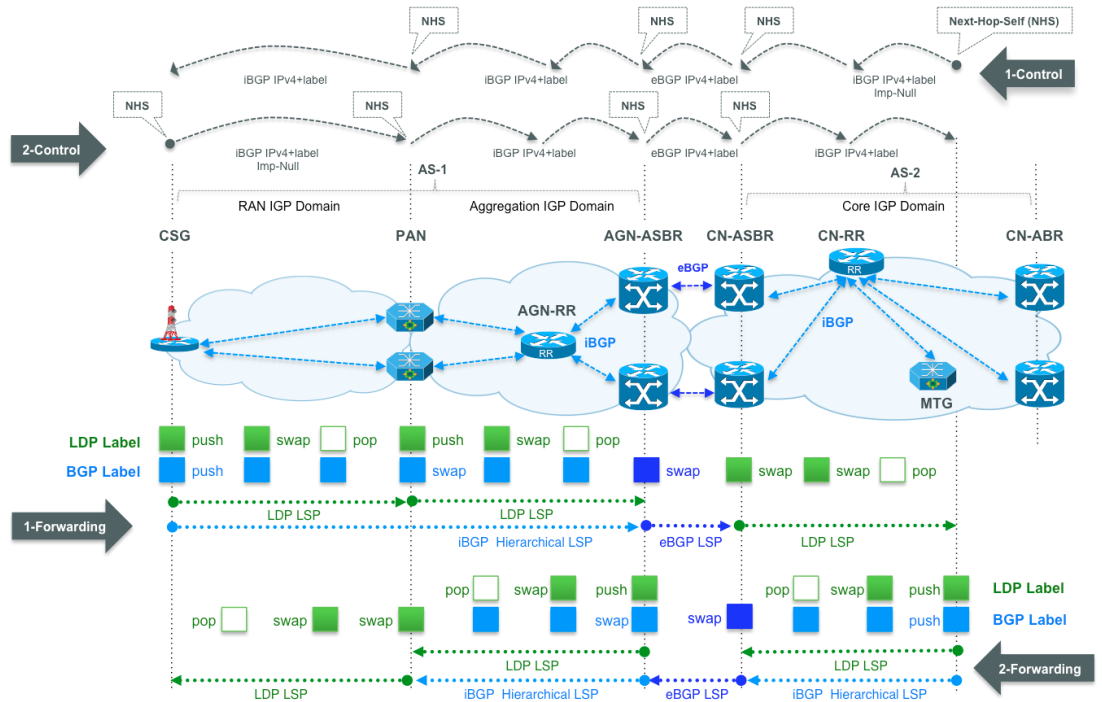
1. The downstream PAN pushes the iBGP label corresponding to the remote prefix, and then pushes the LDP label that is used to reach the local AGN-ASBR that is the labeled BGP next hop.
2. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the local AGN-ASBR.
3. The local AGN-ASBR will swap the iBGP-based inter-domain LSP label with the eBGP label assigned by the neighboring CN-ASBR.
4. The CN-ASBR will swap the eBGP label with the iBGP inter-domain LSP label, and then push the LDP label that is used to reach the remote CN-ASBR that is the labeled BGP next hop.
5. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the remote CN-ASBR.
6. The remote CN-ASBR will swap the iBGP-based inter-domain LSP label with the eBGP label assigned by the neighboring aggregation domain AGN-ASBR.
7. Since the remote AGN-ASBR has reachability to the destination PAN via IGP, it will swap the eBGP label with an LDP label corresponding to the upstream PAN intra-domain LDP LSP.

Hierarchical LSPs between CSG and MTG for Inter-AS Design with Labeled BGP Access

The inter-domain hierarchical LSP described here applies to the *Option-1: Inter-AS Design with Labeled BGP Access* transport model described in [Section 4.1.2 Large Network, Inter-AS Design with IP/MPLS Access](#). This scenario applies to inter-domain LSPs between the loopback addresses of CSGs in the RAN and the MTGs in the core network. It is relevant to 4G LTE and 3G UMTS/IP services deployed using MPLS L3 VPNs or 2G GSM and 3G UMTS/ATM services deployed using MPLS L2 VPNs that use the /32 loopback address of the remote PEs as the endpoint identifier for the t-LDP or

MP-iBGP sessions. The MTGs and CSGs are labeled BGP PE and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4).

Figure 4-24. Hierarchical LSPs between CSGs and MTGs for Inter-AS Design with Labeled BGP Access



The CSG in the RAN access learns the loopback address address of the MTG through BGP-labeled unicast. For traffic flowing between the CSG in the RAN and the MTG in the MPC, as shown in Figure 4-24, the following sequence occurs:

1. The downstream CSG node will first push the BGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the PAN that is the labeled BGP next hop.
2. The CSGs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the PAN.
3. The PAN will swap the BGP label corresponding to the remote prefix, and then push the LDP label used to reach the AGN-ASBR that is the labeled BGP next hop.
4. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the local AGN-ASBR.
5. The local AGN-ASBR will swap the iBGP-based inter-domain LSP label with the eBGP label assigned by the neighboring CN-ASBR.
6. Since the CN-ASBR has reachability to the MTG via the core IGP, it will swap the eBGP label with an LDP label corresponding to the upstream MTG intra-domain core LDP LSP.

The MTG in the MPC learns the loopback address of the remote RAN CSG through BGP-labeled unicast. For traffic flowing between the MTG and the CSG in the RAN as shown in Figure 4-24, the following sequence occurs:

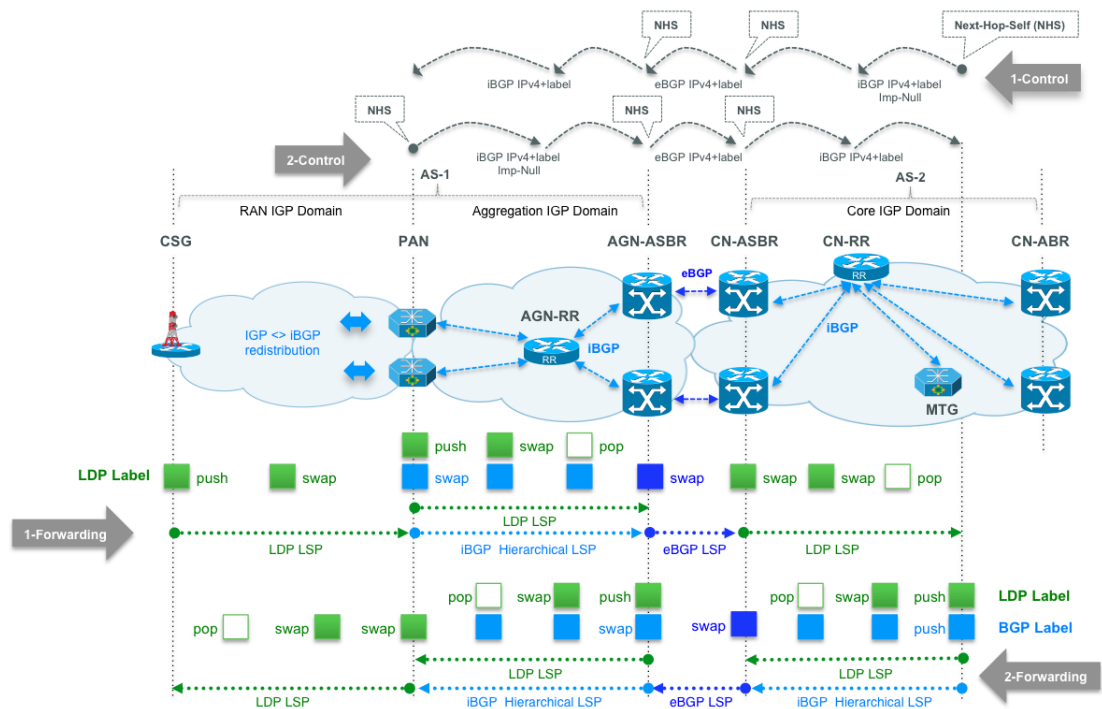
1. The downstream MTG node will first push the iBGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the CN-ASBR that is the labeled BGP next hop.

2. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the CN-ASBR.
3. The CN-ASBR will swap the iBGP-based inter-domain LSP label with the eBGP label assigned by the neighboring aggregation domain AGN-ASBR.
4. The AGN-ASBR will swap the eBGP label with the iBGP inter-domain LSP label corresponding to the remote prefix, and then push the LDP label that is used to reach the PAN that is the labeled BGP next hop.
5. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the PAN.
6. Since the PAN has reachability to the CSG via the RAN IGP area/level, it will swap the BGP label with an LDP label corresponding to the upstream CSG intra-domain RAN LDP LSP.

Hierarchical LSPs between CSG and MTG for Inter-AS Design with IGP/LDP Access

The inter-domain hierarchical LSP described here applies to the *Option-2: Inter-AS Design with IGP/LDP Access* transport model described in [Section 4.1.2 Large Network, Inter-AS Design with IP/MPLS Access](#). This scenario applies to inter-domain LSPs between the loopback addresses of CSGs in the RAN and the MTGs in the core network. It is relevant to 4G LTE and 3G UMTS/IP services deployed using MPLS L3 VPNs or 2G GSM and 3G UMTS/ATM services deployed using MPLS L2 VPNs that use the /32 loopback address of the remote PEs as the endpoint identifier for the t-LDP or MP-iBGP sessions. The MTGs are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4). The CSGs do not run labeled BGP, but have connectivity to the MPC via the redistribution between RAN IGP and BGP-labeled unicast done at the local PANs, which are the labeled BGP PEs.

Figure 4-25. Hierarchical LSPs between CSGs and MTGs for Inter-AS Design with IGP/LDP Access



NOT CISCO CONFIDENTIAL

The CSG in the RAN access learns the loopback address address of the MTG through the BGP-labeled unicast to RAN IGP redistribution done at the local PAN. For traffic flowing between the CSG in the RAN and the MTG in the MPC, as shown in [Figure 4-25](#), the following sequence occurs:

1. The downstream CSG will push the LDP label used to reach the PAN that redistributed the labeled iBGP prefix into the RAN IGP.
2. The CSGs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label towards the PAN.
3. The PAN will first swap the LDP label with the iBGP label corresponding to the remote prefix, and then push the LDP label used to reach the AGN-ASBR that is the labeled BGP next hop.
4. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the local AGN-ASBR.
5. The local AGN-ASBR will swap the iBGP-based inter-domain LSP label with the eBGP label assigned by the neighboring CN-ASBR.
6. Since the CN-ASBR has reachability to the MTG via the core IGP, it will swap the eBGP label with an LDP label corresponding to the upstream MTG intra-domain core LDP LSP.

The MTG in the MPC learns the loopback address of the remote RAN CSG through BGP-labeled unicast. For traffic flowing between the MTG and the CSG in the RAN as shown in [Figure 4-25](#), the following sequence occurs:

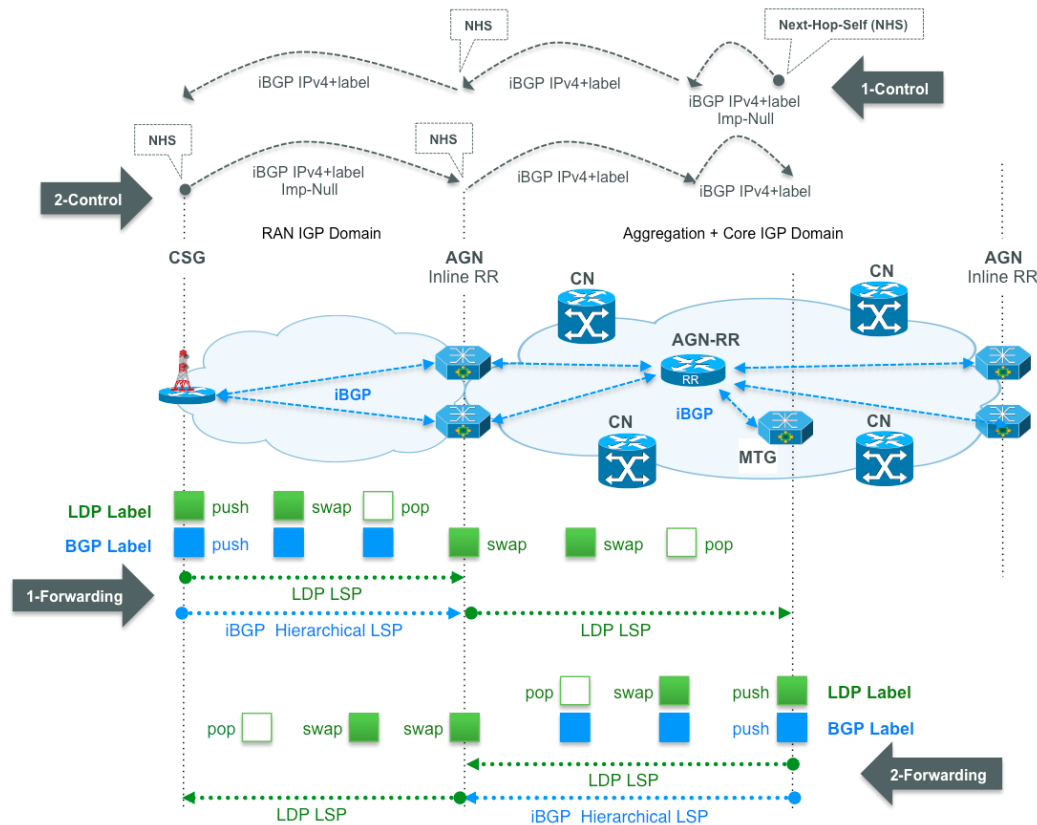
1. The downstream MTG node will first push the iBGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the CN-ASBR that is the labeled BGP next hop.
2. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the CN-ASBR.
3. The CN-ASBR will swap the iBGP-based inter-domain LSP label with the eBGP label assigned by the neighboring aggregation domain AGN-ASBR.
4. The AGN-ASBR will swap the eBGP label with the iBGP inter-domain LSP label corresponding to the remote prefix, and then push the LDP label that is used to reach the PAN that is the labeled BGP next hop.
5. The aggregation nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the PAN connecting the RAN.
6. The PAN will swap the locally-assigned BGP label and forward to the upstream CSG using the local RAN intra-domain LDP-based LSP label.

4.3.3 Inter-Domain LSPs for Integrated Core and Aggregation Design

This section describes inter-domain hierarchical LSPs that apply to Small Network, Integrated Core and Aggregation designs where core and aggregation networks are integrated into a single IGP/LDP domain. The aggregation nodes have subtending mobile RAN access networks that are MPLS enabled and part of the same AS.

Hierarchical LSPs between CSG and MTG for Integrated Core and Aggregation Design

This scenario applies to inter-domain LSPs between the loopback addresses of CSGs in the RAN and the MTGs in the integrated core and aggregation network. It is relevant to 4G LTE and 3G UMTS/IP services deployed using MPLS L3 VPNs or 2G GSM and 3G UMTS/ATM services deployed using MPLS L2 VPNs that use the /32 loopback address of the remote PEs as the endpoint identifier for the t-LDP or MP-iBGP sessions. The MTGs and CSGs are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4).

NOT CISCO CONFIDENTIAL**Figure 4-26. Hierarchical LSPs between CSGs and MTGs for Integrated Core and Aggregation Design**

The CSG in the RAN access learns the loopback address address of the MTG through BGP-labeled unicast. For traffic flowing between the CSG in the RAN and the MTG in the MPC, as shown in Figure 4-26, the following sequence occurs:

1. The downstream CSG node will first push the BGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the AGN that is the labeled BGP next hop.
2. The CSGs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the AGN.
3. Since the AGN has reachability to the MTG via the aggregation IGP, it will swap the BGP label with an LDP label corresponding to the upstream MTG intra-domain aggregation LDP LSP.

The MTG in the MPC learns the loopback address of the remote RAN CSG through BGP labeled unicast. For traffic flowing between the MTG and the CSG in the RAN as shown in Figure 4-26, the following sequence occurs:

1. The downstream MTG node will first push the BGP label corresponding to the remote prefix, and then push the LDP label that is used to reach the AGN that is the labeled BGP next hop.
2. The CN and AGN nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing to the AGN connecting the RAN Access.
3. Since the AGN has reachability to the CSG via the RAN IGP area-x/level-1, it will swap the BGP label with an LDP label corresponding to the upstream CSG intra-domain RAN LDP LSP.

NOT CISCO CONFIDENTIAL

4.4 Transport and Service Control Plane

The UMMT System proposes a hierarchical RR design for setting up the Unified MPLS transport and LTE MPLS VPN service BGP control plane. The hierarchical RR approach is used to reduce the number of iBGP peering sessions on the RRs across different domains of the backhaul network. The following sections describe the BGP control plane aspects for network designs based on Multi-Area IGP and Inter-AS organizations.

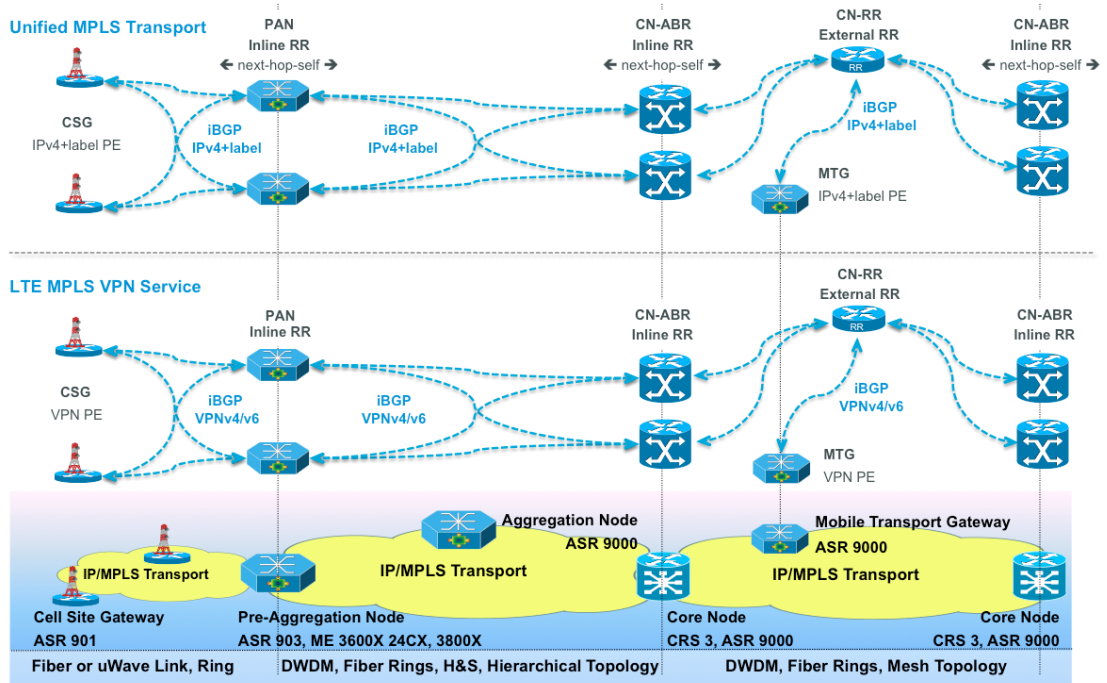
This section includes the following topics:

- [Section 4.4.1 BGP Control Plane for Multi-Area IGP Design](#)
- [Section 4.4.2 BGP Control Plane for Inter-AS Design](#)
- [Section 4.4.3 BGP Control Plane for Integrated Core and Aggregation Design](#)

4.4.1 BGP Control Plane for Multi-Area IGP Design

This section details the hierarchical RR design to enable the BGP control plane for the Unified MPLS transport and LTE MPLS VPN service in a Single AS, Multi-Area IGP-based network. The need for standalone RRs in the lower layers of the network to support this hierarchy are eliminated by making use of the inline-RR functionality on the PANs and CN-ABRs. At the top level of the hierarchy, the CN-ABRs can either peer in a full mesh configuration across the core, or peer as RR clients to a centralized external CN-RR. In deployments with only a few PoPs, a full-mesh configuration between the CN-ABRs would suffice. In larger deployments, a external CN-RR to support the top level of the hierarchy helps simplify provisioning as well as prefix filtering across various PoPs. A external CN-RR based deployment is shown in the figures below.

Figure 4-27. BGP Control Plane for Multi-Area IGP Design with Labeled BGP Access



BGP Control Plane for Unified MPLS Transport

For the Unified MPLS Transport layer, the PANs are inline-RRs to the CSG clients for the MP-iBGP IPv4 labeled unicast address-family:

- They form iBGP session neighbor groups with the CSG RR-clients that are the labeled BGP PEs implementing the inter-domain iBGP hierarchical LSPs in the local RAN access network
- They also form iBGP session neighbor groups towards the local CN-ABR inline RRs.
- The PANs reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP across the access and aggregation domains.

The CN-ABRs are inline-RRs to the PAN clients for the MP-iBGP IPv4 labeled unicast address-family and form the next level of the RR hierarchy:

- They form iBGP session neighbor groups with the PAN RR-clients that are the labeled BGP PEs implementing the inter-domain iBGP hierarchical LSPs in the local aggregation network
- They either form neighbor groups towards other non-client ABRs in the core if a full-mesh configuration is used, or form neighbor groups towards higher level CN-RRs in the core network at the top level of the hierarchy as shown in [Figure 4-27](#).
- If the full mesh option is used, the CN-ABRs also act as RRs serving the closest MTG RR clients in the core network that are labeled BGP PEs implementing the inter-domain iBGP hierarchical LSPs.
- The CN-ABRs reflect the labeled BGP prefixes with the next-hop changed to self in order to insert themselves into the data path to enable the inter-domain LSP across the aggregation and core domains.

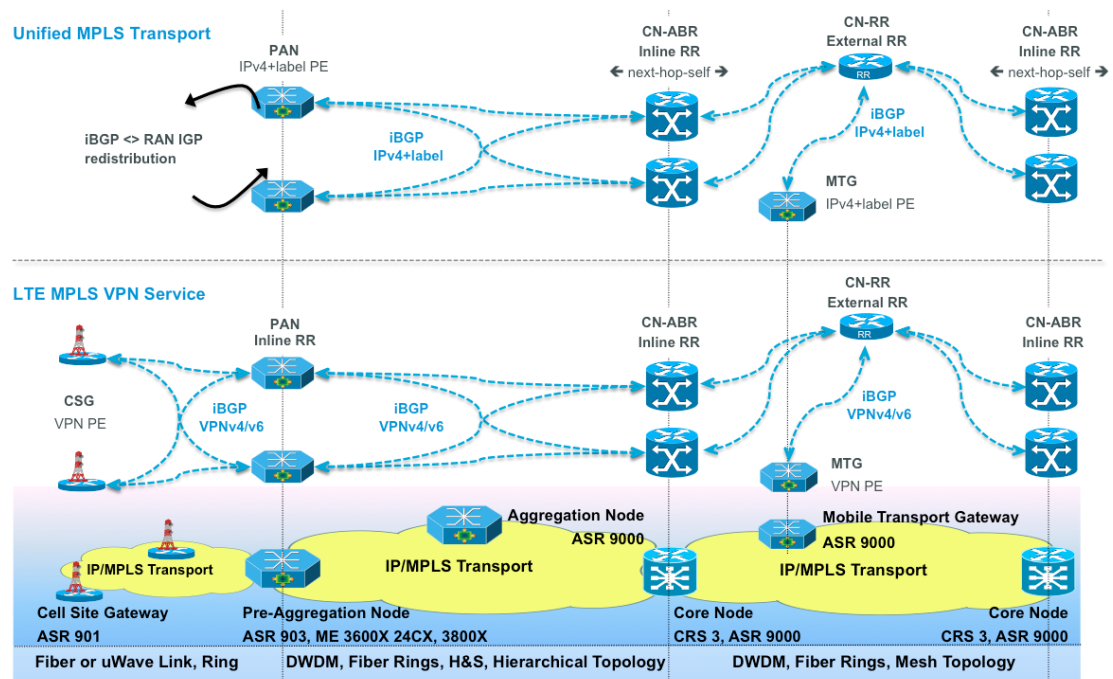
BGP Control Plane for LTE MPLS VPN Service

For the LTE MPLS VPN service, the PANs are inline-RRs to the CSG clients for the MP-iBGP VPNv4 and VPNv6 address-family:

- They form iBGP session neighbor groups towards the local RAN access network to serve the CSG RR-clients that are the PEs implementing the LTE MPLS VPN.
- They also form iBGP session neighbor groups towards the local CN-ABR inline RRs.

The CN-ABRs are inline RRs for the MP-iBGP VPNv4 and VPNv6 address-family and form the next level of the RR hierarchy:

- They form iBGP session neighbor groups towards the local aggregation network to serve the PAN RR clients.
- They either form neighbor groups towards other non-client CN-ABRs in the core if a full-mesh configuration is used, or form neighbor groups towards higher level CN-RRs in the core network at the top level of the hierarchy as shown in [Figure 4-27](#) above.
- If the full-mesh option is used, the core ABR RRs also form neighbor groups for the closest MTG RR clients in the core network that are the PEs implementing the LTE MPLS VPN.

NOT CISCO CONFIDENTIAL**Figure 4-28. BGP Control Plane for Multi-Area IGP Design with IGP/LDP Access****BGP Control Plane for Unified MPLS Transport**

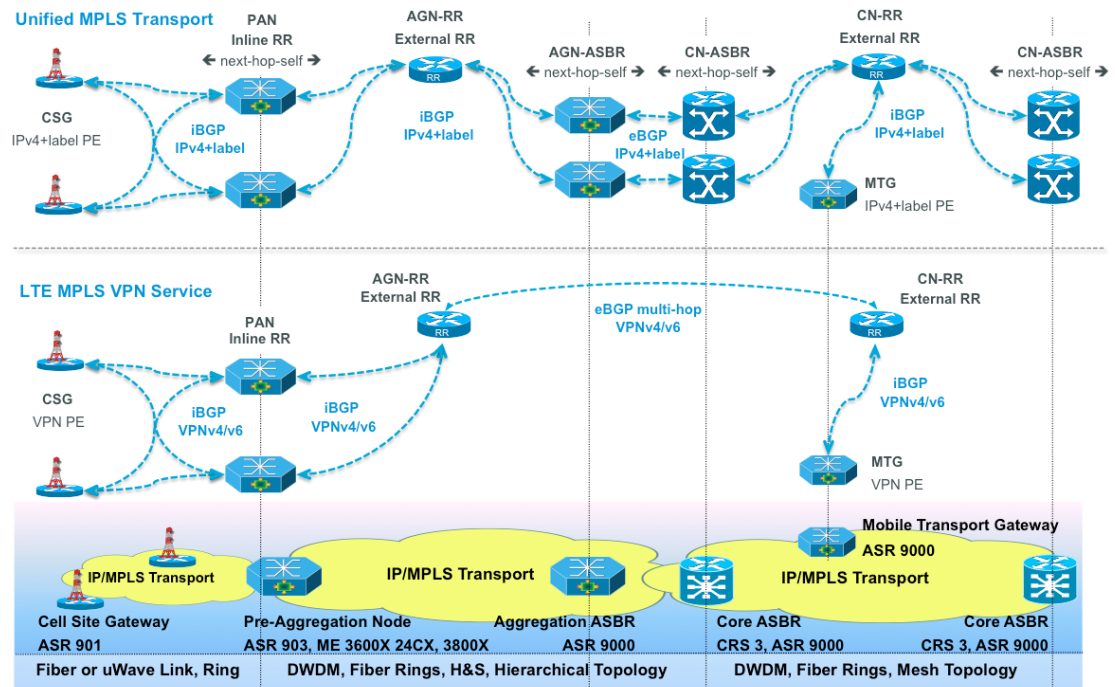
At the top layers of the network, namely the core and aggregation domains, the BGP control plane for Unified MPLS transport is exactly the same as that in the multi-area design with end-to-end labeled BGP case described above. The only difference here is in the access domain of the network. In this case, since we are terminating labeled BGP at the PANs in the aggregation domain, the PANs are labeled BGP PEs and do not have to perform the inline-RR function to the CSGs in the RAN access. The end-to-end unified MPLS LSP is extended into the RAN access using LDP with redistribution.

BGP Control Plane for LTE MPLS VPN Service

For the LTE MPLS VPN service, the BGP control plane is exactly the same as that in the multi-area design with end-to-end Labeled BGP case described above.

4.4.2 BGP Control Plane for Inter-AS Design

This section details the hierarchical RR design to enable the BGP control plane for the Unified MPLS transport and LTE MPLS VPN service in a network where the core and aggregation networks are organized as different autonomous systems. The hierarchical RR approach is used to reduce the number of iBGP peering sessions on the RRs across different domains of the backhaul network. The need for standalone RRs in the access network to support this hierarchy is eliminated by making use of the inline-RR functionality on the PANs.

Figure 4-29. BGP Control Plane for Inter-AS Design with Labeled BGP Access

BGP Control Plane for Unified MPLS Transport

In the aggregation AS, the PANs are inline-RRs to the CSG clients for the MP-iBGP IPv4 labeled unicast address-family:

- They form iBGP session neighbor groups with the CSG RR-clients that are the labeled BGP PEs implementing the inter-domain iBGP hierarchical LSPs in the local RAN access network
- They also form iBGP session neighbor groups towards the local AGN-RRs.
- The PANs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local AGN-RRs and CSG RR-clients.

The AGN-RRs are external RRs for the MP-iBGP IPv4 labeled unicast address-family and form the next level of the RR hierarchy:

- They form iBGP session neighbor groups towards the AGN-ASBR and PAN RR-clients in the aggregation network.
- The AGN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local AGN-RRs and eBGP updates towards neighboring CN-ASBRs.

In the core AS, the CN-RRs are external RRs for the MP-iBGP IPv4-labeled unicast address-family:

- They form iBGP session neighbor groups towards the MTG and CN-ASBR RR-clients in the core network.
- The CN-ASBRs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local CN-RRs and eBGP updates towards the neighboring aggregation ASBRs.

BGP Control Plane for LTE MPLS VPN Service

For the LTE MPLS VPN service, the PANs are inline RRs for the MP-iBGP VPNv4 and VPNv6 address-family:

- They form iBGP session neighbor groups towards the local RAN access network to serve the CSG RR-clients that are the PEs implementing the LTE MPLS VPN.
- They also form iBGP session neighbor groups towards the local aggregation network AGN-RR external RRs.

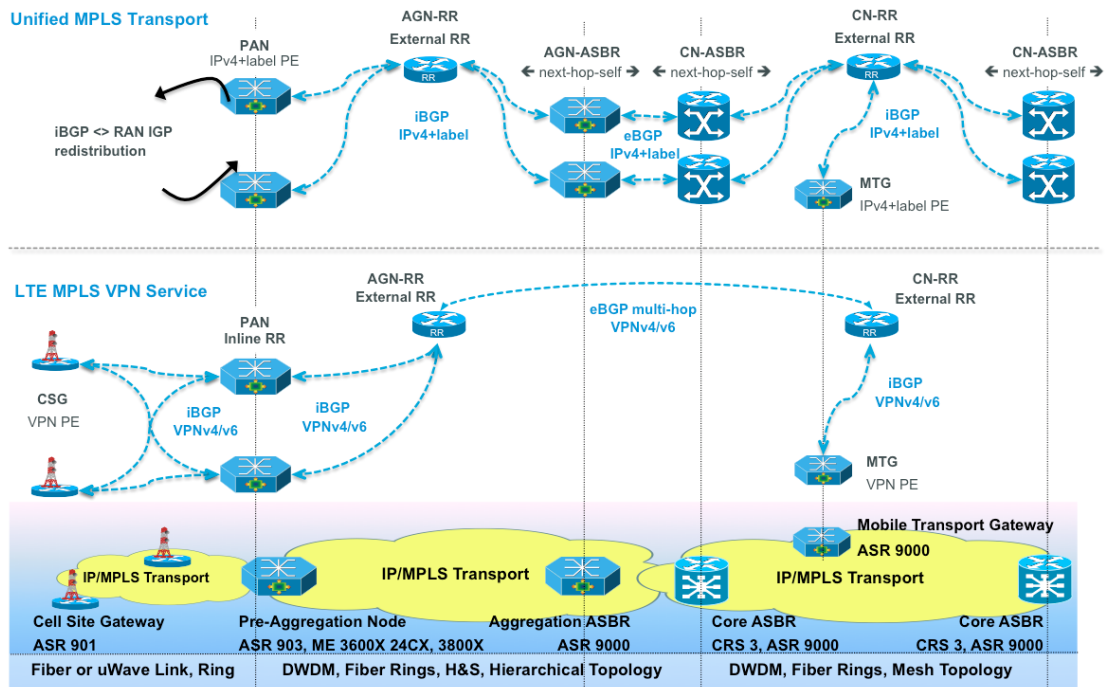
The AGN-RRs are external RRs for the MP-iBGP VPNv4 and VPNv6 address-family in the aggregation network and form the next level of the RR hierarchy:

- They form iBGP session neighbor groups towards the local aggregation network to serve the PAN RR clients.
- They enable the LTE VPN service with a eBGP multi-hop session towards the CN-RR in the core network to exchange VPNv4/v6 prefixes over the inter-domain transport LSP.

The CN-RRs are external RRs for the MP-iBGP VPNv4 and VPNv6 address-family in the core network:

- They form iBGP session neighbor groups in the core network to serve the MTG RR clients that are the PEs implementing the LTE MPLS VPN.
- They enable the LTE VPN service with a eBGP multi-hop session towards the AGN-RRs in the neighboring aggregation network autonomous systems to exchange VPNv4/v6 prefixes over the inter-domain transport LSP.

Figure 4-30. BGP Control Plane for Inter-AS Design with IGP/LDP Access



BGP Control Plane for Unified MPLS Transport

At the top layers of the network, namely the core and aggregation domains, the BGP control plane for Unified MPLS transport is exactly the same as that in the inter-AS design with end-to-end labeled BGP case described above. The only difference here is in the access domain of the network. In this

NOT CISCO CONFIDENTIAL

case, since we are terminating labeled BGP at the PANs in the aggregation domain, the PANs are labeled BGP PEs and do not have to perform the inline-RR function to the CSGs in the RAN access. The end-to-end unified MPLS LSP is extended into the RAN access using LDP with redistribution.

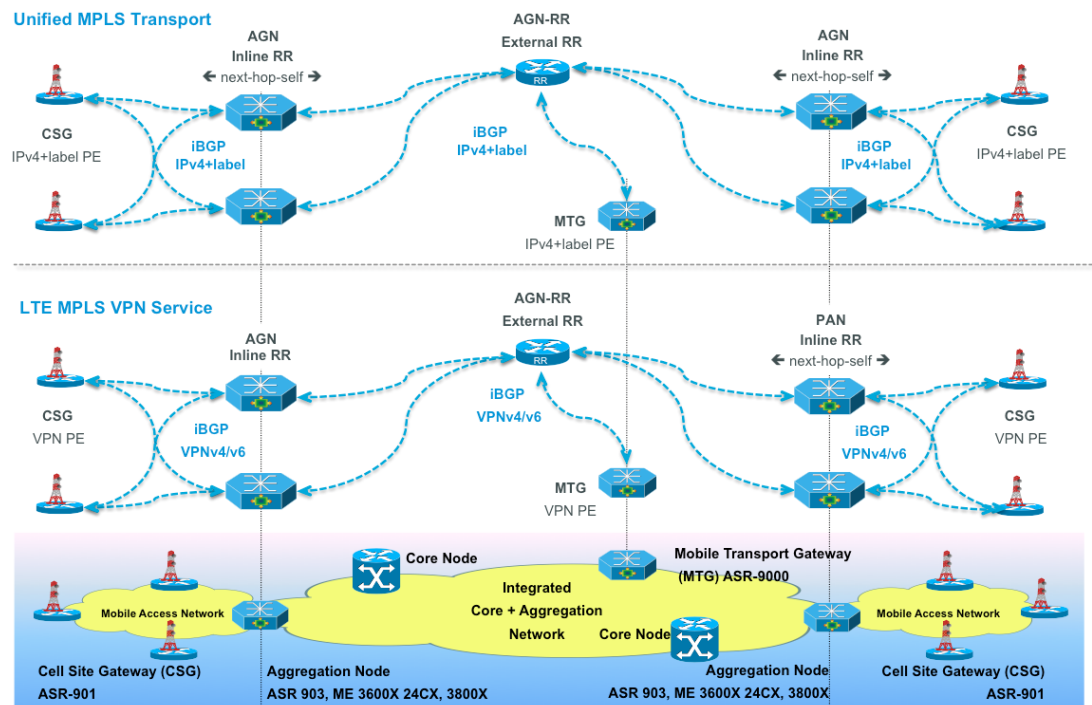
BGP Control Plane for LTE MPLS VPN Service

For the LTE MPLS VPN service the BGP Control Plane is exactly the same as that in the Inter-AS Design with end-to-end Labeled BGP case described above.

4.4.3 BGP Control Plane for Integrated Core and Aggregation Design

This section details the hierarchical RR design to enable the BGP control plane for the Unified MPLS transport and LTE MPLS VPN service in a network where the core and aggregation networks are integrated into a single IGP/LDP domain. The need for standalone RRs in the lower layers of the network to support this hierarchy are eliminated by making use of the inline-RR functionality on the AGNs. At the top level of the hierarchy, the AGNs peer as RR clients to a centralized external AGN-RR.

Figure 4-31. BGP Control Plane for Integrated Core and Aggregation Design with Labeled BGP Access

**BGP Control Plane for Unified MPLS Transport**

For the Unified MPLS Transport layer, the AGNs are inline-RRs to the CSG clients for the MP-iBGP IPv4 labeled unicast address-family:

- They form iBGP session neighbor groups with the CSG RR-clients that are the labeled BGP PEs implementing the inter-domain iBGP hierarchical LSPs in the local RAN access network
- They also form iBGP session neighbor groups towards the local AGN-RRs.
- The AGNs insert themselves into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards their local CSG RR-clients and higher level AGN-RR.

NOT CISCO CONFIDENTIAL

BGP Control Plane for LTE MPLS VPN Service

For the LTE MPLS VPN service, the AGNs are inline RRs for the MP-iBGP VPNv4 and VPNv6 address-family:

- They form iBGP session neighbor groups towards the local RAN access network to serve the CSG RR-clients that are the PEs implementing the LTE MPLS VPN.
- They also form iBGP session neighbor groups towards the higher level external AGN-RR in the aggregation network.

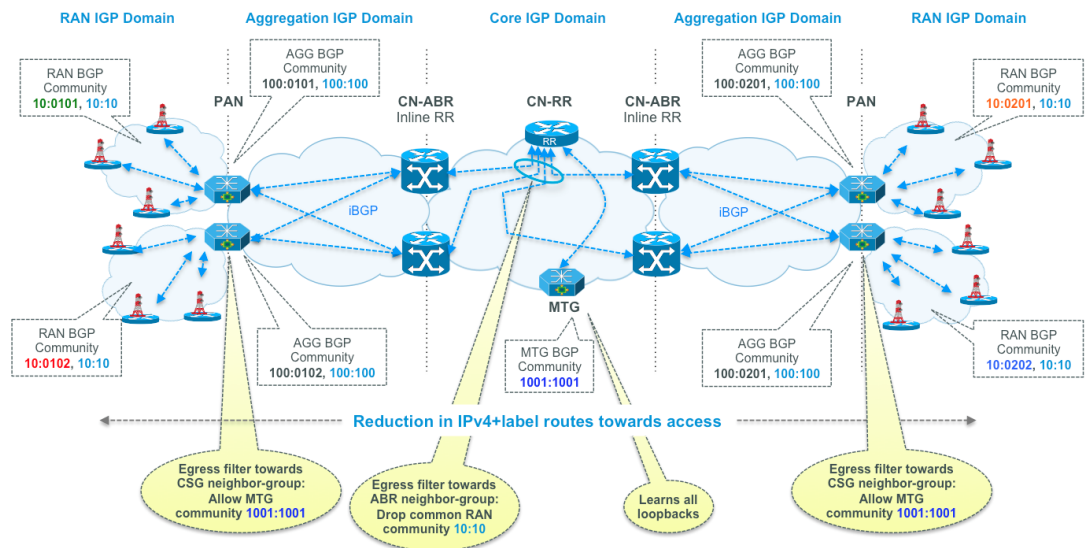
4.5 Prefix Filtering

While the hierarchical RR approach described in [Section 4.4 Transport and Service Control Plane](#) helps reduce the number of BGP sessions multi-fold when compared to using a centralized RR, the number of routes held in the RRs remains the same. In large LTE deployments involving several tens of thousands of eNodeBs and associate CSGs, a few steps can be taken to ensure that the CSGs and PANs in the network are not overloaded with huge numbers of IPv4+label and VPNv4 routes from remote RAN access regions.

Constraining IPv4 Routes from Remote RAN Access Regions

In terms of inter-domain reachability, the CSGs in RAN access need to reach the MTGs in the core network, whereas the PANs may need to reach remote aggregation domains across the core for wireline services. The number of CSGs is several magnitudes larger than the number of PANs in the network, and so it may be desirable to filter the RAN access prefixes in remote aggregation networks where they are not needed.

Figure 4-32. BGP-Community based Coloring of Transport Prefixes



As described in [Section 4.1 Transport Architecture](#), all PANs in the network advertise their loopbacks into BGP labeled-unicast with a common BGP community that represents the aggregation community and a unique BGP community that represents the aggregation location. Depending on the transport model being deployed, the CSG loopbacks are colored as follows:

- If labeled BGP is deployed to the access as shown in [Figure 4-32](#) above, the CSGs advertise their loopbacks into BGP labeled-unicast with a common BGP community that represents the RAN community and a BGP community that is unique to that RAN access region.
- If IGP/LDP is used in the access with redistribution approach, the CSG loopbacks that are redistributed from the RAN access IGP into BGP labeled-unicast at the PANs are marked with a common BGP community that represents the RAN community and a BGP community that is unique to that RAN access region.

Based on this BGP community-based coloring scheme, simple BGP community-based egress filtering can be performed at the top level RRs to constrain the IPv4 labeled-unicast route scale towards the aggregation domains:

- If an external RR is used in the core network as show in [Figure 4-32](#), then an egress filter is applied towards the neighbor group corresponding to the CN-ABR or CN-ASBR clients that drops the common RAN community so that RAN prefixes from one aggregation domain are not propagated into other domains.
- If a full-mesh configuration is used between CN-ABRs, then this egress filter based on common RAN community is applied at each CN-ABR towards the neighbor group corresponding to its local aggregation domain PANs to drop remote aggregation domain RAN prefixes.

Within an aggregation domain, the PANs perform the next level of filtering to further constrain the IPv4 labeled-unicast route scale towards the access domains such CSG loopbacks from disparate RAN access domains within the same aggregation domain are not propagated into each other.

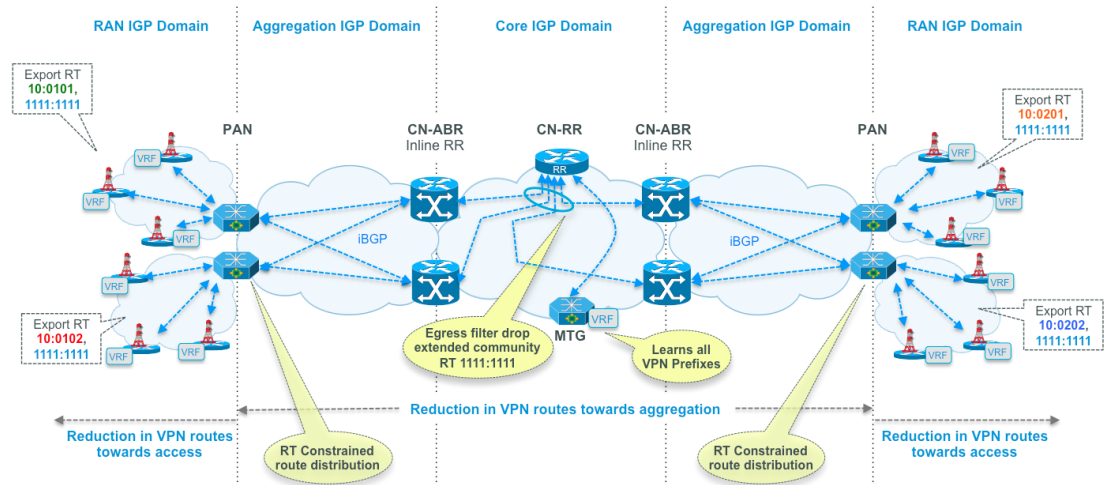
- If labeled BGP is deployed to the access as shown in [Figure 4-32](#) above, the PANs inline-RR enable an egress filter towards their local CSG clients that only allows the MTG BGP community for the LTE S1 interface. Reachability for VPN next-hops for LTE X2 interface between CSG is available through the RAN IGP/LDP LSPs.
- If IGP/LDP is used in the access with redistribution approach, the PANs only redistribute prefixes marked with the MTG community into the RAN IGP process for the LTE S1 interface. Reachability for VPN next-hops for LTE X2 interface between CSG is available through the RAN IGP/LDP LSPs.

**Note**

If inter-access X2 communication is required, selective filtering of adjacent RAN domain BGP communities can be performed as described in [Section 4.2.1 L3 MPLS VPN Service Model for LTE](#).

Constraining VPNv4 Routes from Remote RAN Access Regions

BGP extended-community-based egress filtering based on the RTs used for the LTE MPLS VPN can be performed at the top level RRs to constrain the VPN route scale towards the aggregation domains. As per the RT import/export schema defined in [Section 4.2.1 L3 MPLS VPN Service Model for LTE](#), the filtering logic would involve dropping the common RT-extended BGP communities in the egress direction towards neighboring aggregation domains where they are not needed.

NOT CISCO CONFIDENTIAL**Figure 4-33. BGP Extended Community-based Coloring of Service Prefixes**

- For Single AS Multi-Area IGP designs, if an external CN-RR is used in the core network as shown in Figure 4-33, then an egress filter is applied towards the neighbor group corresponding to the CN-ABRs so that VPN prefixes with common RT assigned the LTE VPN service are dropped.
- For Single AS Multi-Area IGP designs involving full-mesh peering between CN-ABRs, an egress filter is applied at the CN-ABRs towards the neighbor group corresponding to the PANs such that VPN prefixes with common RT assigned the LTE VPN service that do not match the local aggregation domain RTs are dropped.
- For Inter-AS designs, an egress filter is applied at the CN-RR towards the neighboring aggregation domain AGN-RRs so that VPN prefixes with common RT assigned the LTE VPN service are dropped.

Within each aggregation domain, the PANs can implement RT Constrained Route Distribution (RFC 4684) towards the CSG VPNv4 clients. With this feature, the CSGs will send RT constraint Network Layer Reachability Information (NLRI) to the local PAN inline RRs corresponding to the *MPC RT* and *RAN x RT* import statements (as denoted in Figure 4-33) configured for the LTE VPN. The PAN inline-RR function RR will translate the NLRI into a dynamic outbound route filter that only permits MP-iBGP updates matching these RTs towards the local CSG RR-clients. This would result in the CSG receiving only a limited number of VPNv4 prefixes corresponding to the MTG for the S1 interface and the neighboring local eNodeB prefixes for the X2 interface.

4.6 Scale Considerations

This section describes the route scale and the control plane scaling aspects involved in setting up the unified MPLS transport across the network domains.

As an example, we consider a large scale LTE deployment following the Single AS Multi Area design described in Section 4.1.1 *Large Network, Multi-Area IGP Design with MPLS Access* involving 60,000 CSGs across 25 PoPs in a SP network. In the core network, we consider around fifteen EPC S/PGW locations and five EPC MME locations, with each location connected to a pair of redundant MTGs. This leads a total of forty MTGs for transport connectivity from the core to the CSGs in the RAN access domain. If we consider that each RAN access domain is comprised of twenty CSGs connected in physical ring topologies of five nodes each to the pre-aggregation network, and (for the

purpose of illustration) we assume an even distribution of RAN backhaul nodes across the twenty-five PoPs, we end up with the network sizing shown in [Table 4-1](#).

Table 4-1. Network Sizing

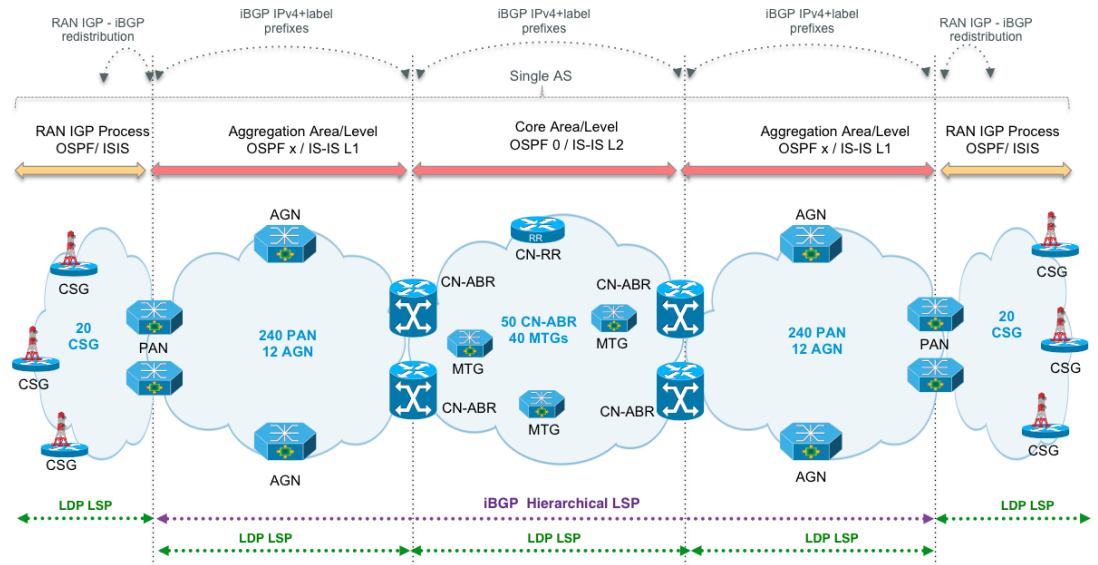
Node	Access Domain	Aggregation Domain	Network Wide
CSGs	20	2,400	60,000
PANs	2	240	6,000
AGNs	NA	12	300
CN-ABRs	NA	2	50
MTGs	NA	NA	40

Route Scale

RAN backhaul for LTE requires connectivity between the CSGs in the RAN access and the MTGs in the core network. In an MPLS environment, since route summarization of PE's /32 loopback IP address cannot be performed, a flat IGP/LDP network design would imply that the core network would have to learn all the 60,000 loopback addresses corresponding to the CSGs deployed across the entire network. While this level route of scale in a IGP domain may be technically feasible, it is an order of magnitude higher than typical deployments and would present huge challenges in IGP convergence when a topology change event is encountered.

The UMMT System architecture provides a scalable solution to this problem by adopting a divide-and-conquer approach of isolating the access, aggregation, and core network layers into independent and isolated IGP/LDP domains. While LDP is used to set up intra-domain LSPs, the isolated IGP domains are connected to form a unified MPLS network in a hierarchical fashion by using RFC 3107 procedures based on iBGP to exchange loopback addresses and MPLS label bindings for transport LSPs across the entire MPLS network. This approach prevents the flooding of unnecessary routing and label binding information into domains or parts of the network that do not need them. This allows scaling the network to hundreds of thousands of LTE cell sites without overwhelming any of the smaller nodes like CGS in the network. Since the route scale in each independent IGP domain is kept to a minimum, and all remote prefixes are learnt via BGP, each domain can easily achieve sub-second IGP fast convergence.

Figure 4-34. UMMT Hierarchical Network



If we consider a hierarchical network design as shown in Figure 4-34, we end up with a route scale across various domains of the unified MPLS transport network, as depicted in Table 4-2.

Table 4-2. Route Scale

Node	Routes in Core-Agg IGP Process	Routes in RAN IGP Process	iBGP IPv4-Labeled Routes
CSGs	NA	87	NA
PAN	~ 504	47	5,821
AGN	~ 504	NA	NA
CN-ABR	~ 742	NA	66,040
MTG	~ 240	NA	66,000

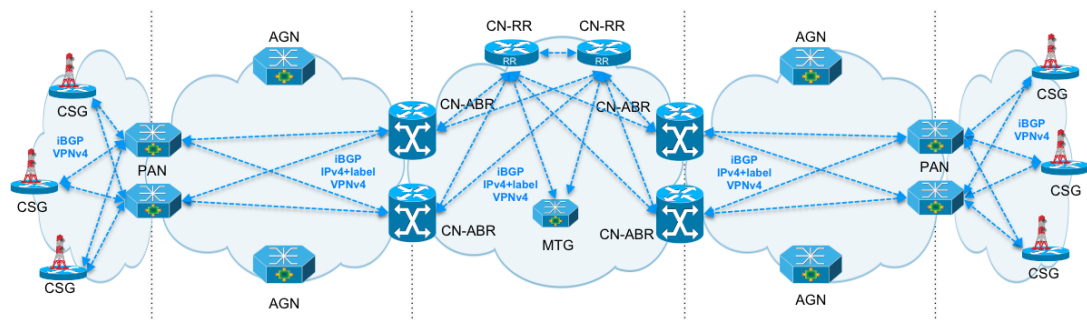
**Note**

- On CSGs, the 87 IGP routes correspond to 20 local RAN access CSG loopbacks + 25 links in RAN access network + 2 local PANs + 40 MTG loopbacks from the MPC.
- On PANs:
 - The 504 IGP routes in Core-AGG IGP process correspond to 240 local PANs + 12 local AGNs + 2 local CN-ABRs + around 250 links in the aggregation network, depending on physical topology.
 - The 47 IGP routes in the RAN IGP process correspond to 20 local RAN access CSG loopbacks + 25 links in the RAN access network + 2 local loopback addresses in RAN IGP.
 - The 5,821 iBGP IPv4-labeled routes correspond to 20 locally-redistributed RAN access CSG loopbacks + 1 own loopback + 5760 remote PAN loopbacks + 40 MTG loopbacks from the core network.
- On AGNs, the 504 IGP routes correspond to 240 local PANs + 12 local AGNs + 2 local CN-ABRs + around 250 links in aggregation network, depending on physical topology.
- On CN-ABRs:
 - The 742 IGP routes correspond to 240 local PANs + 12 local AGNs + around 250 links in the aggregation network, depending on physical topology, + 50 CN-ABRs + 40 MTG nodes + around 150 links in core network, depending on physical topology.
 - The 66,040 iBGP IPv4-labeled routes correspond to 60,000 CSG loopbacks + 6000 PAN loopbacks + 40 MTG loopbacks.
- On MTGs:
 - The 240 IGP routes correspond to 50 core ABRs + 40 MTG nodes + around 150 links in the core network, depending on physical topology.
 - The 66,000 iBGP IPv4-labeled routes correspond to 60,000 CSG loopbacks + 6000 PAN.

Control Plane Scale

As described in [Section 4.4 Transport and Service Control Plane](#), the UMMT System uses a hierarchical RR design with inline RR functionality on the CN-ABRs and PANs to greatly reduce the number of iBGP peering sessions across different domains of the backhaul network.

Figure 4-35. UMMT Hierarchical RR Topology



For the example network sizing shown in [Table 4-1](#), if we consider the peering organization illustrated in [Figure 4-35](#), we have the following BGP session scale on different elements in the network (see [Table 4-3](#)).

Table 4-3. BGP Session Scale

Node	Address-Family	Client iBGP Sessions	RR iBGP Sessions	Non-Client iBGP Sessions	Total iBGP Sessions
CSG	VPNv4	NA	2	NA	2
PAN	IPv4+label, VPNv4	20	2	NA	22
CN-ABR	IPv4+label, VPNv4	240	2	NA	242
MTG	IPv4+label, VPNv4	NA	2	NA	2
CN-RR	IPv4+label, VPNv4	90	NA	1	91

**Note**

- CSRs in each RAN access domain peer with their two redundant local PAN inline-RRs.
- PANs in each aggregation domain peer with their CSG clients and with their two redundant local CN-ABR inline-RRs.
- MTGs in the core domain connecting regional EPC GWs peer with the redundant external CN-RRs.
- CN-ABRs peer with their PAN clients and with the redundant external CN-RRs in the core domain.

NOT CISCO CONFIDENTIAL

**CHAPTER 5**

Functional Components

Up to this point in the design guide, we have addressed the base transport design, control plane, data plane, and service model aspects of the Unified MPLS for Mobile Transport system architecture. This chapter looks at additional aspects required for delivering and operating a comprehensive mobile backhaul system architecture.

This chapter includes the following major topics:

- [Section 5.1 Quality of Service](#)
- [Section 5.2 Synchronization Distribution](#)
- [Section 5.3 Redundancy and High Availability](#)
- [Section 5.4 OAM and Performance Monitoring](#)
- [Section 5.5 Network Management with Cisco Prime](#)

5.1 Quality of Service

The UMMT System applies the IETF DiffServ Architecture (RFC 2475) across all network layers, utilizing classification mechanisms like MPLS EXP, IP DSCP, IEEE 802.1p, and ATM CoS for implementing the DiffServ PHBs in use.

In a transport network, congestion can occur anywhere. However, congestion is more likely where statistical estimates of peak demand are conservative (i.e., under-provisioned), which happens more often on the design of access and aggregation bandwidth links. Congestion due to instantaneous ingress bandwidth to a node exceeding egress bandwidth (assuming the node can process all ingress bandwidth) therefore requires all nodes to be able to implement DiffServ scheduling functions. The result is that the under-provisioning is unfairly distributed among the services transported. This redistribution with DiffServ can result in over-provisioning for higher quality services (like VoIP and video) and differing levels of under-provisioning for other services. This is inline with the functional requirements defined by standards bodies, such as the NGMN and Broadband Forum TR-221 specification for mobile backhaul.

Each network layer defines an administrative boundary, where traffic remarking may be required in order to correlate the PHBs between different administrative domains. A critical administrative and trust boundary is required for enforcing subscriber SLAs. Subscriber SLAs are enforced with sound capacity management techniques and functions, such as policing/shaping, marking, and hierarchical scheduling mechanisms. This administrative boundary is implemented by the CSG, NodeB equipment, or radio controllers, depending on the service model, for traffic received (upstream) from the subscribers and by the core nodes for traffic sent (downstream) to the subscribers.

NOT CISCO CONFIDENTIAL

Figure 5-1 and Figure 5-2 present visual representations of the QoS model for the upstream and downstream directions. In most administrative domains in the UMMT System, a flat QoS policy with a single-level scheduler and shaper is sufficient for the required DiffServ functionality, as all links are capable of line rate transmission. The exception is in the case of microwave links in the access, where the connection to the equipment on either end of the link is GbE, but the wireless portion of the link is only capable of sub-gigabit speeds (typically 400Mbps sustained). In this case, the PAN interface facing the microwave access implements a H-QoS policy with a parent shaper equal to the sustained microwave link speed required for proper DiffServ functionality. If the microwave systems support DiffServ QoS and are able to synchronize the QoS classes used by the CSGs in the access to provide EF and AF guarantees, then flat QoS policies on the transit CSG NNIs are sufficient. On the other hand, if the microwave systems do not support DiffServ QoS, or are unable to synchronize the QoS classes used by the CSGs, the CSGs have to implement H-QoS policy with a parent shaper equal to the sustained microwave link speed on their network-to-network interface (NNI), as shown in Figure 5-1 and Figure 5-2.

Figure 5-1. UMMT System Upstream QoS Model

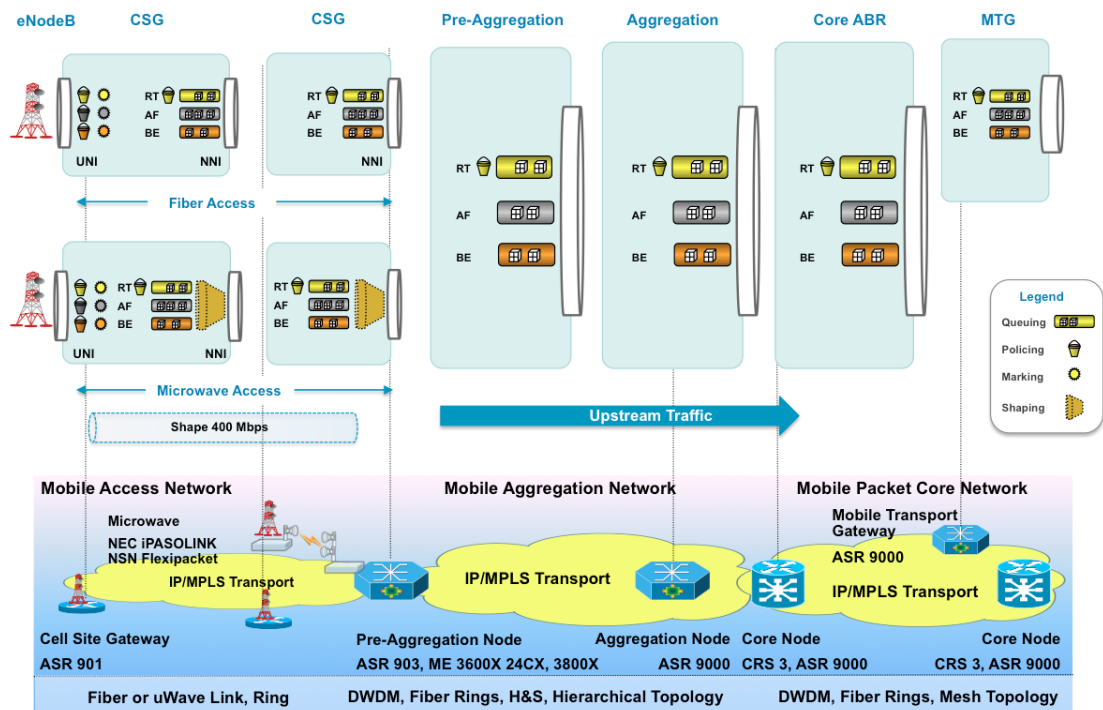
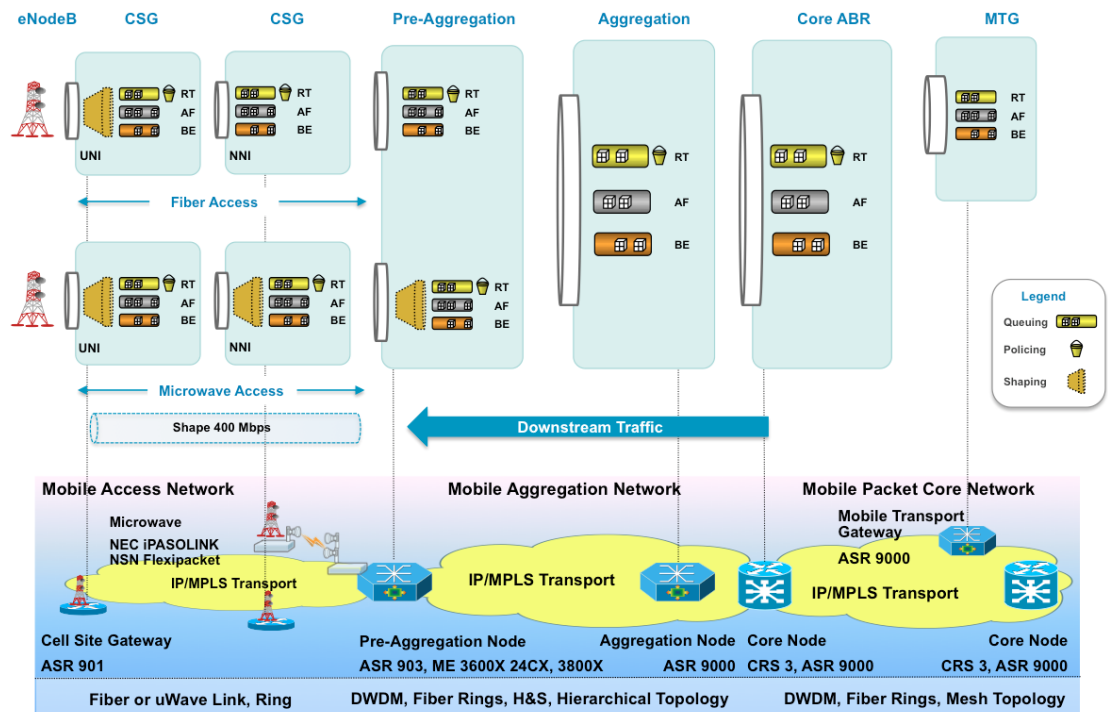


Figure 5-2. UMMT System Downstream QoS Model

DiffServ QoS Domain

The traffic classification, marking, and DiffServ PHB behaviors considered in the system architecture, which are depicted in Figure 5-3, are targeted to fit the deployment of mobile services.

PTP synchronization, GSM Abis, UMTS Iub control plane and voice user plane, LTE S1c, X2c, and the LTE GBR user plane are classified in a traffic class that requires an expedited forwarding (EF) PHB, as described in RFC 3246. This class will be serviced with a priority queue due to the stringent latency and delay variation requirements these services have. The EF PHB defines a scheduling behavior that guarantees an upper limit on per hop delay variation that can be caused by packets from non-EF services.

UMTS IuB user plane that needs guaranteed bandwidth and the LTE MBR user plane are classified in traffic classes that use the advanced forwarding (AF) PHB behavior, as described in RFC 2597. The AF PHB guarantees a certain amount of bandwidth to an AF class while guaranteeing a certain limit of latency.

IuB and LTE S1 and X2 best effort (BE) traffic will use the BE PHB behavior.

The system includes additional AF traffic classes, used for network control protocols and network management traffic that will be serviced in the aggregation network by a weighted queue.

NOT CISCO CONFIDENTIAL**Figure 5-3. UMMT System DiffServ QoS Domain**

Traffic Class	QCI	Resource	DiffServ PHB	Core, Aggregation, Access Network	Mobile Access UNI	
				MPLS/IP	IP NodeB, eNodeB	ATM NodeB
				MPLS EXP	DSCP	ATM
Network Management	7	Non-GBR	AF	7	56	VBR-nrt
Network Control Protocols	6	Non-GBR	AF	6	48	VBR-nrt
Network Sync (1588 PTP, ACR)	1	GBR	EF	5	46	CBR
Mobile Conversation (Voice & Video)	2					
Signaling (GSM Abis, UMTS Iub control, LTE S1c, X2c)	3					
Reserved	4	-	AF	4	32	VBR-nrt
Hosted Video	5	Non-GBR	AF	3	24	VBR-nrt
Reserved	8	-	AF	2 1	16 8	VBR-nrt
Internet Best Effort	9	Non-GBR	BE	0	0	UBR

QoS Policy Enforcement

The QoS model described above is implemented via QoS service policies applied to the UNI interfaces at the edges of the network for classification and remarking, and QoS service policies applied throughout the intermediate nodes within the network to provide proper queuing and scheduling of those traffic classes.

For Ethernet UNI interfaces, traffic classification is based on IP DSCP or 802.1P CoS markings. The ingress QoS service policy will match on these markings and map them to the corresponding MPLS EXP value based on the DiffServ QoS Domain table shown in [Figure 5-3](#). IP DSCP markings are preserved within the MPLS transport, and thus the egress QoS service policy may use DSCP markings for queuing and scheduling. In the case of 802.1P, an ingress service policy on the CSG or MTG will map the MPLS EXP values back to 802.1P, and the egress service policy can thus use the 802.1P CoS for queuing and scheduling.

For TDM UNI interfaces to be transported via CEdPs pseudowires, both for SAToP and CESoPSN, all traffic is classified as real-time and requires EF PHB. The ingress QoS service policy matches all traffic inbound to the interface, and applies an MPLS EXP value of 5. There is no egress service policy required for TDM UNI interfaces.

For ATM UNI interfaces to be transported via CEdPs pseudowires, traffic is classified according to the ATM CoS on a particular VC. The ingress QoS service policy is applied to the ATM PVC subinterface and imposes an MPLS EXP value that corresponds to the type of traffic carried on the VC and proper ATM CoS according to the table in [Figure 5-3](#). For further distinction, the ingress QoS service policy also has the ability to match on the Cell Loss Priority bit of the incoming ATM traffic, and can map to two different MPLS EXP values based on this. For egress treatment, the PVC interface is configured with the proper ATM CoS. If the CLP to EXP mapping is being used, then an egress QoS service policy applied to the ATM PVC subinterface can map an EXP value back to a CLP value for proper egress treatment of the ATM cells.

The core, aggregation, and access network traffic marking is based on MPLS EXP. The core network may use different traffic marking and simplified PHB behaviors, or may be transporting services in addition to mobile backhaul, therefore requiring traffic remarking in between the aggregation and core networks.

NOT CISCO CONFIDENTIAL

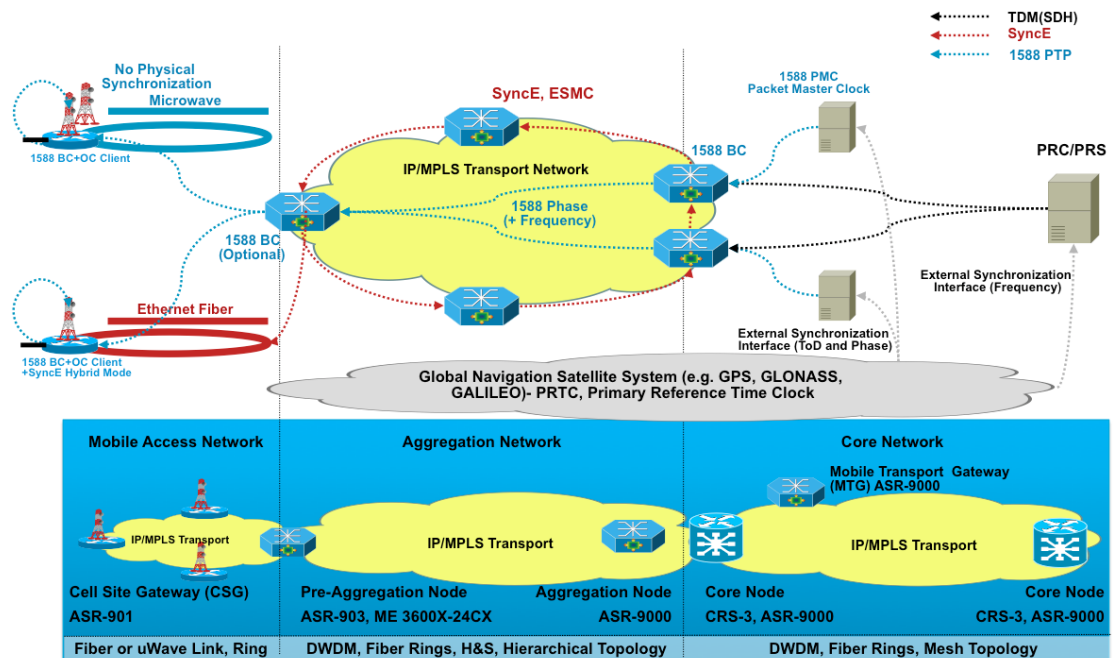
5.2 Synchronization Distribution

Synchronization distribution for both frequency and phase is a fundamental functional component of the access and aggregation areas of the UMMT System. The primary target for the current system release is to provide frequency synchronization using the Ethernet physical layer (SyncE) and phase synchronization using IEEE 1588-2008 PTP. SyncE operates on a link-by-link basis and will provide a high quality frequency reference in a way equivalent to SONET and SDH networks. SyncE is complemented by ESMC (Ethernet Synchronization Messaging Channel), which allows transmitting over SyncE-enabled links a Quality Level value as done with Synchronization Status Message (SSM) in SONET and SDH. This allows the SyncE node to select a timing signal from the best available source and help detecting timing loops, which is essential for deployment of SyncE in ring topologies.

Because not all links on the network may be SyncE-capable or have synchronization distribution at the physical layer, IEEE 1588-2008 Precise Time Protocol (PTPv2) may also be used for frequency distribution. IEEE 1588 packet-based synchronization distribution is overlaid across the entire system infrastructure; third-party master and third-party IP-NodeB client equipment are considered outside the scope of the system. The mechanism is standards based and can provide frequency and/or phase distribution, relying on unicast or multicast packet-based transport. As with any packet-based mechanism, IEEE 1588 PTP traffic is subject to loss, delay, and delay variation. However the packet delay variation (PDV) is the main factor to control. To minimize the effects of these factors and meet the requirements for synchronization delivery utilizing PTP, EF PHB treatment across the network is required.

The UMMT system also supports a combination of both SyncE and PTPv2 in a hybrid synchronization architecture, aiming to improve the stability and accuracy of the phase and frequency synchronization delivered to the client for deployments such as TDD-LTE eNodeBs. In such architecture, the packet network infrastructure is frequency synchronized by SyncE. The phase signal is delivered by 1588-2008 PTPv2. The Cell Site Gateway (CSG), acting as a PTP ordinary clock or as a boundary clock (BC), may combine the two synchronization methods, using the SyncE frequency as frequency reference clock for the 1588-2008 PTP engine. The combined recovered frequency and phase can be delivered to clients via 1PPS (Pulse Per Second), 10MHz and "BITS" timing interfaces, SyncE and PTP. For access networks that don't support SyncE, the hybrid 1588 BC function may be move to the Pre-Aggregation Nodes (PAN).

[Figure 5-4](#) illustrates how synchronization distribution is achieved for mobile RAN services over both fiber and microwave access networks in the UMMT architecture.

Figure 5-4. Synchronization Distribution

The frequency source for the mobile backhaul network is the Primary Reference Clock (PRC), which can be based on free-running atomic clock (typically Cesium), a GNSS receiver which derived frequency from signals received from one or more satellite system, or a combination of both.

The time (phase and Time of Day -ToD) source for the mobile backhaul network is the Primary Time Reference Clock (PRTC), which is usually based on GNSS receiver that derived time synchronization from one or more satellite systems with traceability to the Coordinated Universal Time (UTC). A PRC provides a frequency signal of G.811/Stratum-1 quality signal (traceable to UTC frequency if coming from GNSS) to the Aggregation Nodes via G.703-compliant dedicated external interfaces (aka BITS input) or 10Mhz interface. A PRTC provides time via a 1PPS signal for phase, and a serial ToD interface. DOCSIS Timing Interface (DTI) is an alternative to the frequency, 1PPS and ToD interface. A PRTC can also provide frequency as a PRC. If required by the architecture, the IEEE 1588 Primary Master Clock (PMC) will also derive synchronization from the PRC or PRTC. From this point, three models of synchronization distribution are supported:

1. For mobile services that only require frequency synchronization, where all network nodes support SyncE, then frequency is carried to the NodeB via SyncE. The ESMC provides source traceability between nodes through the QL value which helps selecting best signal and preventing timing loops in Synchronous Ethernet topologies.
2. For mobile services that require synchronization over an infrastructure which does not support SyncE, 1588v2 PTP is then utilized for frequency synchronization distribution. The PMC generates PTP streams for each PTP slave that is routed globally by the regional MTG to the CSG, which then provides sync to the eNodeB. The PMC can be a network node which receives the frequency source signal via physical layer (e.g., SyncE). Proper network engineering shall prevent excessive PDV to allow timing network to provide packet-based quality signal to the slaves.
3. For mobile services that require frequency and phase and/or time of day (ToD) synchronization, IEEE 1588-2008 PTP can be used in conjunction with SyncE to provide a hybrid synchronization solution, where SyncE provides accurate and stable frequency distribution, and PTPv2 is used for allowing phase and/or ToD synchronization. In this UMMT release, the PTPv2 streams are

NOT CISCO CONFIDENTIAL

routed globally from the regional MTG to the CSG, which, combined with SyncE frequency, then provides synchronization to the eNodeBs.

In general, a packet-based timing mechanism such as IEEE 1588 PTP has strict packet delay variation requirements, which restricts the number and type of hops over which the recovered timing from the source is still valid. With globally routed model, strict priority queuing of the PTP streams is necessary. With (good) implementation of 1588 BC on intermediate transit nodes, it is possible to provide better guarantee over more hops from the PMC to the NodeB.

Scalability and reliability of PTPv2 in the UMMT System is enhanced by enabling BC in some or all of the following: the aggregation node, the PAN, and CSG. Implementing BC functionality in these nodes serves two purposes:

1. Increases scaling of PTPv2 phase/frequency distribution, by replicating a single stream from the PMC to multiple destinations, thus reducing the number of PTP streams needed from the PMC.
2. Improves the phase stability of PTPv2, by stabilizing the frequency of the PTP servo with SyncE or another physical frequency source as described in the hybrid synchronization architecture.

5.3 Redundancy and High Availability

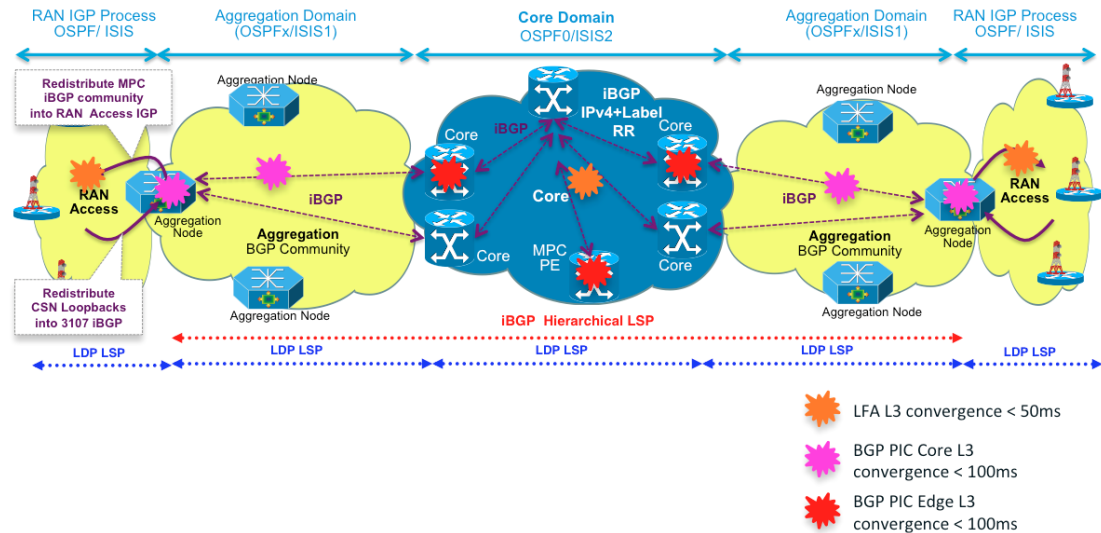
The UMMT System seeks to provide a highly resilient and robust network architecture to provide rapid recovery from any link or node failure within the transport network, with a target of well below sub-second convergence for any failure within the network in order to meet the NGMN requirements for LTE real-time services of 50-200 msec. A hierarchical implementation of mechanisms at the network and service levels achieves this resilient design. The mechanisms described in this section are applicable to both single AS and multiple AS models.

The UMMT System implements the following baseline transport mechanisms for improving network availability:

- For intra-domain LSPs, remote LFA FRR is utilized for unicast MPLS/IP traffic in both hub-and-spoke and ring topologies. Remote 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. More information regarding LFA FRR can be found in IETF RFC 5286, 5714, and 6571. Also integrated are BFD rapid failure detection and ISIS/OSPF extensions for incremental SPF and LSA/SPF throttling (XR defaults should be applied to IOS devices).
- For inter-domain LSPs, network reconvergence is accomplished via BGP PIC core and edge throughout the system, allow for deterministic network reconvergence on the order of 100 msec, regardless of the number of BGP prefixes. BGP PIC is similar to remote LFA FRR in that it pre-calculates a backup path for every prefix in the BGP forwarding table, relying on a hierarchical Labeled-FIB (LFIB) structure to allow for multiple paths to be installed for a single BGP next hop. BGP PIC core and edge each handle different failure scenarios within the transport network:
 - PIC core is used when the BGP next-hop is still active, but there is a failure in the path to that next hop. As soon as the IGP has reconverged, the pointer in BGP is updated to use the new IGP next hop and forwarding resumes. Thus, the reconvergence time for BGP is the same as the IGP reconvergence, regardless of the number of BGP prefixes in the RIB.
 - PIC edge is used for redundant BGP next hops, like the case where there are redundant ABRs. Additional paths functionality is configured on the PE routers and RRs to install both ABR paths in the RIB and LFIB instead of just the best path. When there is a failure of the primary ABR, BGP forwarding simply switches to the path of the backup ABR instead of having to wait for BGP to reconverge.

Figure 5-5 illustrates the end-to-end UMMT System architecture, and where each of the resiliency mechanisms is utilized for various failures.

Figure 5-5. UMMT High Availability Overview



The MPLS VPN services providing the backhaul of LTE services between the CSG and MTG implement the following mechanisms for improving network availability:

- For UNI connections at the CSG to the eNodeB, static routes to the MTG are utilized in the eNodeB.
- For UNI connections to the MPC from the MTG, fast IGP convergence with BFD keep-alive checks or multichassis Link Aggregation Control Protocol (mLACP) port-bundles are utilized.
- For the MPLS VPN transport between the CSG and MTG, network convergence is handled by BGP PIC, similar to the base transport infrastructure.

For PWE3-based circuit emulation services providing transport of TDM-based 2G and ATM-based 3G services, the following mechanisms are implemented:

- For TDM and ATM connections from the MTG to the BSC or RNC, MR-APS allow for redundant connections.
- For the Circuit Emulation PWE3 between the CSG and MTG, backup pseudowires and two-way backup pseudowires provide failover protection in the transport network.

In order to protect critical synchronization functions, the following mechanisms are implemented within the UMMT System for synchronization distribution:

- For SyncE frequency synchronization, the ESMC is used to pass frequency quality between nodes. In ring topologies, SSMs allow nodes within the ring to avoid timing loops, and to switch from one side of the ring to another if a network failure is encountered within the ring.
- For frequency, phase, and ToD synchronization via 1588 PTP, active and standby streams from two different PRCs are received at each 1588 client. If the active stream becomes unavailable, then the backup stream can be utilized. As 1588 is a packet-based protocol, L2 or IGP resiliency mechanisms will prevent loops within a ring topology. 1588 BC implementation at the various network levels enhances scalability and resiliency as well.

NOT CISCO CONFIDENTIAL

5.4 OAM and Performance Monitoring

The UMMT System defines an operations, administration, and maintenance (OAM) subsystem that is broadly classified into two categories: Service OAM and Transport OAM. Service OAM and Transport OAM rely on the same set of protocols to provide end-to-end OAM capabilities, including fault and performance management, but focus on different functional areas.

Service OAM is a service-oriented mechanism that operates and manages the end-to-end services carried across the network. It is provisioned only at the touch points associated with the end-to-end service, and is primarily used for monitoring the health and performance of the service. Service OAM ensures services are up and functional, and that the SLA is being met. When services are affected due to network events, it provides the mechanisms to detect, verify, and isolate the network faults. The following protocols are the building blocks of Service OAM:

- ATM Service OAM:
 - F4/F5 VC/VP ATM OAM
- Ethernet Service OAM and PM:
 - 802.1ag Connectivity Fault Management (CFM)
 - MEF Ethernet Local Management Interface (E-LMI)
 - ITU-T Y.1731: OAM/PM for Ethernet-based networks
 - Cisco IP SLA PM based on CFM
- MPLS VPWS Service OAM and PM:
 - Virtual Circuit Connectivity Verification (VCCV) PW OAM: PW Ping, BFD failure detection
 - Cisco IP SLA PM based on CFM. A future release of the UMMT architecture will support PW OAM-based PM
- MPLS VPLS Service OAM and PM:
 - VCCV PW OAM: PW Ping, BFD failure detection
 - Cisco IP SLA PM based on CFM
- IP/MPLS VPN Services OAM and PM:
 - IP and VRF ping and trace route
 - BFD single and multi-hop failure detection
 - Cisco IP SLA PM based on CFM

Transport OAM is a network-oriented mechanism that operates and manages the network infrastructure. It is ubiquitous in the network elements that make up the network infrastructure, and it is primarily used for monitoring health and performance of the underlying transport mechanism on which the services are carried. The primary purpose of Transport OAM is to keep track of the state of the transport entities (MPLS LSP, Ethernet VLAN, etc). It monitors the transport entities to ensure that they are up and functional and performing as expected, and provides the mechanisms to detect, verify, and isolate the faults during negative network events. The following protocols are the building blocks of Transport OAM:

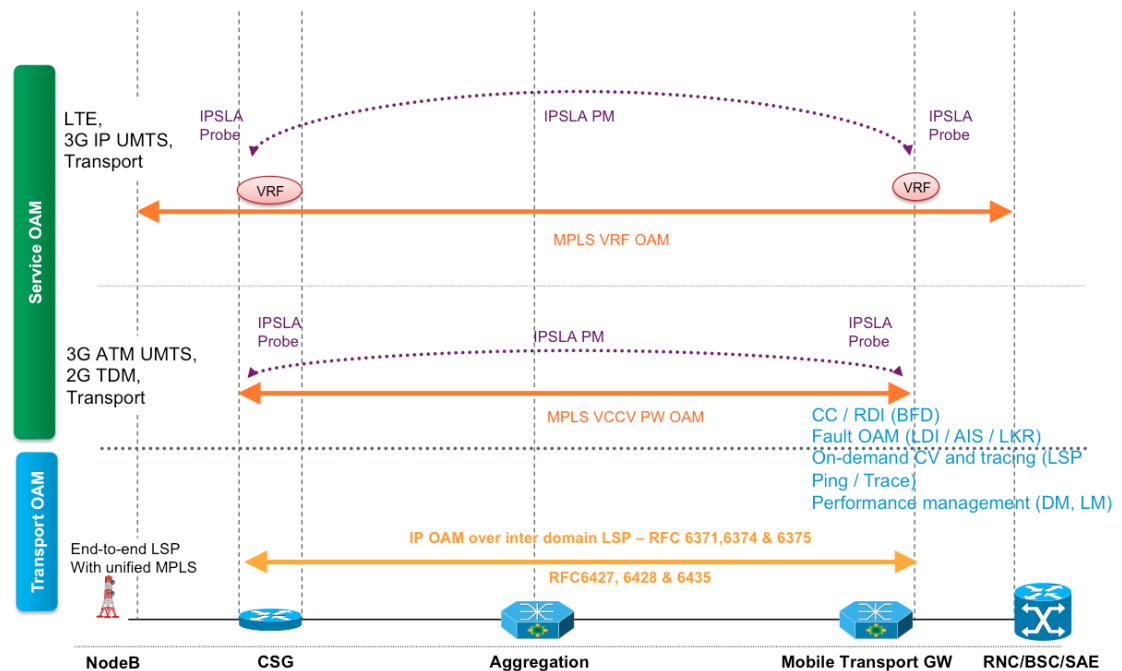
- Ethernet Transport OAM and PM:
 - IEEE 802.3ah: Ethernet Link OAM (EFM OAM)
 - 802.1ag CFM

NOT CISCO CONFIDENTIAL

- ITU-T Y.1731: OAM/PM for Ethernet-based networks
- Cisco IP SLA PM based on CFM
- IP/MPLS Transport OAM and PM:
 - BFD single and multi-hop failure detection
 - IP and MPLS LSP ping and traceroute
 - Cisco IP SLA PM
 - Future releases of the UMMT architecture will support G-ACh-based OAM and PM for MPLS LSPs

OAM Implementation in the UMMT System

The UMMT System, due to the nature of the mobile backhaul services supported, only utilizes a subset of these protocols to provide the required Service and Transport OAM and PM functionality. The details of the required mechanism are highlighted in [Figure 5-6](#).

Figure 5-6. OAM Protocol Positioning

5.5 Network Management with Cisco Prime

Cisco Prime™ provides integrated service lifecycle management capabilities for UMMT. By helping enable mobile service providers to design, fulfill, assure, and analyze the performance of services over mobile backhaul networks, Cisco Prime lowers operating expenses (OpEx), increases backhaul link utilization, and delivers faster time-to-service value across any combinations of radios, media, and content.

The Cisco Prime for IP NGN suite of products offers advanced integration with key Cisco hardware and third-party devices and is extensible over any transport media. The solution also increases efficiency with seamless transition between each of its software components. Designed as a modular suite of applications, Cisco Prime for IP NGN allows customers to adopt the capabilities they need

to solve business problems today while having the flexibility to adopt new solutions as their business requirements evolve:

- **Cisco Prime Network** provides comprehensive assurance and device management for heterogeneous mobile backhaul networks from cell sites to core networks.
- **Cisco Prime Performance Manager** provides actionable performance metrics for Cisco and multivendor backhaul networks and components to facilitate assurance and capacity planning.
- **Cisco Prime Provisioning** accelerates service deployments by providing automated resource management and rapid, profile-based provisioning capabilities.
- **Cisco Prime Central** tightly integrates all components of the Cisco Prime for IP NGN suite through a centralized management interface providing a single view of integrated operator workflows.

The Cisco Prime suite provides the following key benefits when managing the UMMT system architecture:

- Accelerates service design and activation of "IP over Anything" with best-in-class multivendor discovery and plug-and-play capabilities.
- Brings new equipment and services online faster and more cost effectively with day-one device support and zero-touch deployment for fastest time to value.
- Reduces OpEx by up to 90 percent by automating routine operational tasks across the service lifecycle to eliminate truck rolls and other manual processes.
- Helps ensure efficient and profitable capacity utilization using powerful visualization and performance measurement capabilities to minimize backhaul congestion, facilitate service differentiation, and help ensure SLAs through robust prioritization and optimization of service traffic.
- Reduces operating costs through a centralized user portal with integrated framework and intuitive GUI for rapid visualization and diagnosis, single-point entry into the network, and point-and-click operation.
- Lowers outage costs by 40 percent through advanced monitoring tools that help enable rapid diagnosis of faults, 50:1 event reduction, and the ability to assure SLAs across multiple domains and thousands of cell sites.

More information on the Cisco Prime suite of products can be found at <http://www.cisco.com/go/prime>.

NOT CISCO CONFIDENTIAL

**CHAPTER 6**

Conclusion

As illustrated and explained in depth in this design guide, the third release of Cisco UMMT System gives operators a proven architecture, platforms, and solutions to stay ahead of the curve for bandwidth demand and provide operational simplification, all at optimized cost points. The UMMT System is a comprehensive RAN backhaul solution that supports LTE, 3G, and 2G service deployment. It provides flexible cell site connectivity options, including integration of third-party microwave vendors. It supports both retail and wholesale backhaul options, and concurrent transport for residential and business services traffic over the same infrastructure.

UMMT 3.0 builds upon the foundation delivered by the first two UMMT releases, which introduced key technologies from Cisco's Unified MPLS suite of technologies to deliver highly scalable and simple-to-operate MPLS-based IP RAN backhaul networks. Unified MPLS resolves legacy challenges such as scaling MPLS to support tens of thousands of end nodes, which provides the required MPLS functionality on cost-effective platforms and without the complexity of technologies like TE-FRR to meet transport SLAs. By addressing the scale, operational simplification, and cost of the MPLS platform, UMMT 3.0 provides a comprehensive solution to the mobile operator seeking an immediately deployable architecture suitable for LTE deployment.

UMMT 3.0 Highlights

To recap, here are the highlights of the third release of the UMMT System:

- Full validation and deployment recommendations new deployment models, including labeled BGP control plane to the access domain and IPv6 VPN support for LTE.
- Addition of ATM transport over packet for the UMTS Iub interface, including pseudowire redundancy and MR-APS to provide comprehensive resiliency.
- Addition of the ME 3600X-24CX platform to provide a 2RU, cost-effective pre-aggregation solution supporting legacy interfaces.
- Inclusion of IEEE 1588v2 BC functionality in all domains, plus a hybrid model incorporating Synchronous Ethernet and 1588v2 to provide the highest level of accuracy in delivering frequency, phase, and ToD synchronization for TDD-LTE deployments.
- Improvements in high availability functionality with Remote LFA FRR and expanded BGP PIC core and edge support.
- Comprehensive network management system provided by the Cisco PRIME network suite.
- QoS: UMMT leverages DiffServ QoS for core and aggregation, H-QoS for microwave access and customer-facing SLAs, and support for LTE QCIs and wireline services, to deliver a comprehensive QoS design.

NOT CISCO CONFIDENTIAL

- OAM and Performance Monitoring: OAM and performance management for LSP transport, MPLS VPN, and VPWS services are based on IP SLA, PW OAM, MPLS and MPLS OAM, and future IETF MPLS PM enhancements.

Until now, mobile network infrastructures have been composed of a mixture of many legacy technologies that have reached the end of their useful life. UMMT 3.0 continues to advance the UMMT baseline that has provided the first integrated, tested, and validated mobile network architecture, to meet all the demands of legacy service transport and highly scaled any-to-any connectivity for LTE networks.

UMMT 3.0 Benefits Summary

- Flexible deployment options for multiple platforms to optimally meet size and throughput requirements of differing networks.
- High-performance solution, utilizing the highest capacity Ethernet aggregation routers in the industry. The components of this system can be in service for decades to come.
- Tested and validated reference architecture that allows operators to leverage a pre-packaged framework for different traffic profiles and subscriber services.
- Promotes significant capital savings from various unique features such as pre-tested solutions, benchmarked performance levels, and robust interoperability, all of which are validated and pre-packaged for immediate deployment.
- Enables accelerated time-to-market based on a pre-validated, turnkey LTE RAN backhaul system.
- Complementary system support, with mobile video transport optimization integration; I-WLAN untrusted offload support on the same architecture; mobile packet core (MPC); and cost-optimized performance for VoLTE, plus additional services such as Rich Communication Suite (RCS).
- Cisco's IP expertise is available to operators deploying UMMT 3.0 through Cisco Services. These solutions include physical tools, applications, and resources plus training and annual assessments designed to suggest improvements to the operator's network.



CHAPTER 7

Related Documents

The *UMMT 3.0 Design Guide* is part of a set of resources that comprise the UMMT System documentation suite. The resources include:

- **UMMT 3.0 System Brochure:** At a Glance brochure of the Unified MPLS for Mobile Transport System
- **UMMT 3.0 Design Guide:** This document. Provides detailed information about Cisco's UMMT 3.0 system architecture, components, service models, and implementation details.
- **UMMT Implementation Guide - Large Network, Multi-Area IGP Design with IP/MPLS Access:** Implementation guide with configurations for a transport model where the network organization between the core and aggregation domains is based on a single autonomous system, multi-area IGP design. The model follows the approach of enabling Unified MPLS LSPs using hierarchical-labeled BGP LSPs across the core and aggregation network, and presents two approaches for extending the unified MPLS LSPs into the mobile RAN access domain.
- **UMMT Implementation Guide - Large Network, Inter-AS Design with IP/MPLS Access:** Implementation guide with configurations for a transport model where the core and aggregation networks are organized as different autonomous systems. The model follows the approach of enabling Unified MPLS LSPs using hierarchical labeled BGP LSPs based on iBGP labeled unicast within each AS, and eBGP labeled unicast to extend the LSP across AS boundaries. Two approaches are presented for extending the unified MPLS LSPs into the mobile RAN access domain.
- **UMMT Implementation Guide - Large Network, Inter-AS Design with non-IP/MPLS Access:** Implementation guide with configurations for a transport model where the core and aggregation networks are organized as different autonomous systems. The model follows the approach of enabling Unified MPLS LSPs using hierarchical labeled BGP LSPs based on iBGP labeled unicast within each AS, and eBGP labeled unicast to extend the LSP across AS boundaries. The model assumes a non-MPLS IP/Ethernet or TDM access where all mobile and potentially wireline services are enabled by the aggregation nodes.
- **UMMT Implementation Guide - Small Network, Integrated Core and Aggregation with IP/MPLS Access:** Implementation guide with configurations for a transport model in a small network where the core and aggregation networks are integrated into a single IGP/LDP domain. The aggregation nodes have subtending mobile RAN access networks that are MPLS enabled, and the unified MPLS LSPs are extended into the access network using hierarchical-labeled BGP LSPs.

Note that all of the documents listed above, with the exception of this Design Guide, are considered Cisco Confidential documents. Copies of these documents may be obtained under a current Non-

NOT CISCO CONFIDENTIAL

Disclosure Agreement with Cisco. Please contact a Cisco Sales account team representative for more information about acquiring copies of these documents.



GLOSSARY

A

ABR	area border router
AF	assured forwarding
AIS	alarm indication signal
AS	autonomic system
ASBR	autonomous system border router
ATM	asynchronous transfer mode
AToM	Any Transport over MPLS

B

BC	boundary clock
BE	Best Effort
BGP	Border Gateway Protocol (RFC 4271)
BITS	Building Integrated Timing Supply
BNG	Broadband Network Gateway
BSC	base station controller (GSM)
BTS	base transceiver station

C

CEoP	Circuit Emulation over Packet (Cisco)
CESoPSN	Circuit Emulation over Packet Switching Network
CFM	Connectivity Fault Management (IEEE 802.1ag)

CN-ABR	core node Area Border Router
CN-ASBR	core node Autonomous System Border Router
CN-RR	core node Route Reflector
CSG	cell site gateway

D

DiffServ	Differentiated Services
-----------------	-------------------------

E

eBGP	External Border Gateway Protocol
EEM	Embedded Event Manager
EF	expedited forwarding
E-LMI	Ethernet Local Management Interface
EPC	Evolved Packet Core
EPL	Ethernet Private Line
ESMC	Ethernet Synchronization Monitoring Channel
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EV-DO	Evolution Data Only Optimized
EVPL	Ethernet Virtual Private Line

F

FEC	Forwarding Equivalency Class
------------	------------------------------

G

GSM	Global System for Mobile Communications
------------	---

H

H-QoS	Hierarchical QoS
HSPA	High-Speed Packet Access

I

iBGP	Internal Border Gateway Protocol
IGP	Interior Gateway Protocol
I-HSPA	Internet-High Speed Packet Access
IS-IS	intermediate system to intermediate system
I-WLAN	Internet-Wireless LAN

L

LDP	Label Distribution Protocol (MPLS)
LFA-FRR	Loop-Free Alternate Free Reroute
LFIB	Labeled-FIB
LSP	Label-Switched Protocol
LTE	Long Term Evolution (3G)

M

MEF	Metro Ethernet Forum
MIMO	multiple input multiple output
mLACP	multichassis Link Aggregation Control Protocol
MME	Mobility Management Entity
MPC	Mobile Packet Core
MPLS	Multiprotocol Label Switching

MR-APS	Multi-Router Automatic Protection Switching
MSP	mobile service provider
MSPW	multi-segment pseudowire
MTG	mobile transport gateway

N

NHS	next-hop-self
NLRI	Network Layer Reachability Information
NNI	network-to-network interface

O

OAM	Operation, Administration, and Maintenance
OSPF	Open Shortest Path First

P

PAN	pre-aggregation node
PE	provider edge
PGW	packet data network gateway
PHB	per hop behavior
PHP	Penultimate Hop Popping
PIC	Prefix Independent Convergence
PMC	Packet Master Clock
PRC	Primary Reference Clock
PRTC	Primary Reference Time Clock
PTP	Precision Time Protocol
PW	pseudowire

PWE Pseudowire Emulation

Q

QCI QoS class identifier

QoS quality of service

R

RCS Rich Communication Suite

RNC radio network controller (UMTS)

RPL Routing Policy Language

RR Route Reflector

RT Route Target

S

S1AP S1 Application Protocol

SAE System Architecture Evolution

SAToP Structure-Agnostic Transport over Packet

SCTP Stream Control Transmission Protocol (RFC 2960)

SDH Synchronous Digital Hierarchy

SGW Serving Gateway (LTE)

SONET Synchronous Optical Networking

SR-APS Single-Router Automatic Protection Switching

SSM synchronization status message

T

TCO total cost of ownership

TDM	time division multiplexing
TE-FRR	Traffic Engineering Fast ReRoute
ToD	Time of Day

U

UDP	User Datagram Protocol
UE	User Equipment
UMMT	Unified MPLS Mobile Transport
UMTS	Universal Mobile Telecommunications System

V

VCCV	Virtual Circuit Connectivity Verification
VNI	Cisco Visual Networking Index
VoLTE	Voice over LTE
VPWS	virtual private wireline service
VRF	virtual routing and forwarding