EPN 4.0 Transport Infrastructure Design and Implementation Guide

September 2014

Cisco Validated Design

Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

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

EPN 4.0 Transport Infrastructure Design and Implementation Guide

CONTENTS

Introduction

The Cisco® Evolved Programmable Networks (EPN) System Release 4.0 continues to enhance the design of the Unified MPLS for Mobile Transport (UMMT) and Fixed Mobile Convergence (FMC) systems. This effort is part of a multi-year ongoing development program that builds towards a flexible, programmable, and cost-optimized network infrastructure that Cisco targets to deliver in-demand fixed and mobile network services.

As described in the Cisco EPN 4.0 System Concept Guide, the EPN System follows a layered design aimed to simplify the end-to-end transport and service architecture. By decoupling the transport and service infrastructure layers of the network it allows these two distinct entities to be provisioned and managed independently.

This guide focuses on the design and implementation aspects of the first layer--the transport layer. This layer provides the framework to achieve connectivity among any two or more nodes in the network and enables all the consumer and enterprise services that the EPN System promotes. Essential features, such as hierarchical Quality of Service (H-QoS) policy, high availability, and multicast further complement the implementation.

This chapter includes the following major topic:

Transport Network Overview

The Cisco EPN System incorporates a network architecture designed to consolidate fixed and mobile services in a single MPLS-based transport network.

Continuous growth in consumer and enterprise services, combined with ubiquitous LTE-driven mobile broadband adoption, has introduced unprecedented levels of scale in terms of access nodes and eNodeBs in the access network. This factor, combined with services requiring ubiquitous connectivity from the access domain into and across the core network, has led to scale challenges in the MPLS network.

In MPLS, the Service Edge (SE) node must be identified by a /32 IP address, thus precluding route summarization from being performed among access, aggregation, and core regions of the network. To address the resulting route scale problem, the EPN System promotes a network design that leverages a Unified MPLS-based hierarchical approach.

Unified MPLS adopts a divide-and-conquer strategy where the core, aggregation, and access networks are partitioned in different MPLS/IP domains that are isolated from both IGP and LDP perspective. Doing so reduces the size of routing and forwarding tables within each domain, which 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, an aggregation, or a core domain to have reachability via intra-domain LDP LSPs to any other device in the same region. Within a domain

both IS-IS and OSPF are suitable choices of IGP protocols. While the selection is largely based on operator's preference, important considerations are discussed later in the "IGP protocol considerations" section of this chapter.

Reachability across domains is achieved using RFC 3107 procedures whereby BGP-labeled unicast is used as an inter-domain LDP 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, leaving all external reachability information to be carried via BGP, which is designed to scale to the order of millions of routes.

The network segmentation between the core and aggregation domains can be based on a single autonomous system (AS) multi-area design, or utilize a multi-AS design with inter-AS organization:

- In Single-AS Multi-Area designs, interior Border Gateway Protocol (iBGP)-labeled unicast is used to build inter-domain LSPs.
- In Inter-AS designs, iBGP-labeled unicast is used to build inter-domain LSPs inside the AS, while 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 to transit across the isolated MPLS domains, and on a LDP-distributed label within the domain to reach the inter-domain area border router (ABR) or autonomous system boundary router (ASBR) corresponding to the labeled BGP next hop.

Transport Models

As described in the EPN 4.0 System Concept Guide, the transport architecture structuring takes into consideration the type of access and the size of the network, leading to six architectural models that fit various customer deployments and operator preferences. This implementation guide covers these six transport models, as shown in Table 1-1.

Table 1-1 EPN Transport Models

Access Type	Small Network	Large Network
Ethernet/TDM access (non-IP/MPLS access)	Flat LDP core and aggregation network	Hierarchical-labeled BGP core and aggregation network
IP/MPLS access	Hierarchical-labeled BGP LSP access network	Hierarchical-labeled BGP LSP access network
IP/MPLS access (mobile only)	Labeled BGP redistribution into access IGP/LDP (optional LDP Downstream-on-Demand [DoD])	Hierarchical-labeled BGP redistribution into access IGP/LDP (optional LDP DoD)

Access Type Considerations

The type of access is divided into the categories described in the following sections.

MPLS 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 ANs.

- Both mobile and wireline services are supported and can be inserted at different levels in the network: directly at the last mile access nodes or backhauled deeper in the network for optimal service edge placement via a pseudowire-based transport.

Ethernet/TDM Access/nV

- Covers point-to-point TDM+Ethernet hybrid links.
- Includes native Ethernet links in point-to-point or ring topologies over fiber and newer Ethernet microwave-based access. Ring topologies can be L3-enabled or L2-only with G.8032 protection.
- Incorporates nV access, with satellite nodes connected to the hosts in ring topologies or over any Layer 2 transport (aka L2 fabric).
- Supports Central Office (CO) located PON OLT access, or WiFi access with centrally managed access points.
- MPLS services are enabled by the aggregation network and includes residential; MEF X-Line, E-LAN, E-Tree transport services and enterprise L3VPN; Mobile transport GSM Abis, ATM IuB, IP IuB, and IP S1/X2 interfaces.

Network Size Considerations

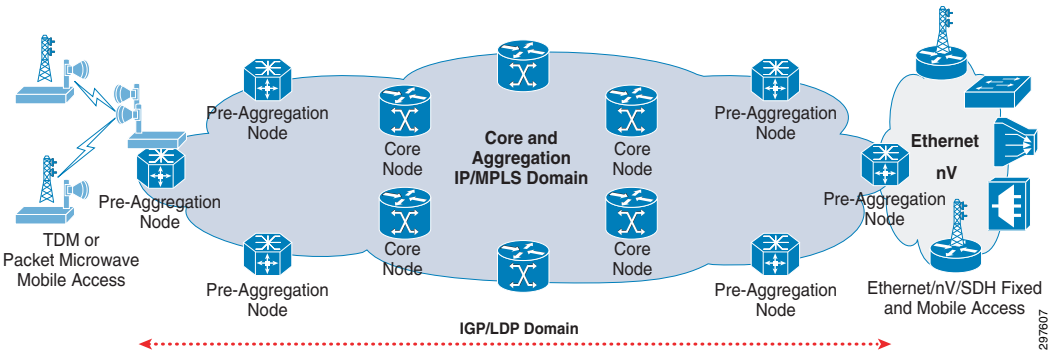
- Small Network:
  - Applies to network infrastructures in small geographies where the core and aggregation network layers are integrated in a single domain.
  - The Single IGP/LDP domain includes less than 1000 core and AGNs nodes.
- Large Network:
  - Applies to network infrastructures built over large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

Transport Models: Small Network - Non-IP/MPLS Access

Flat LDP Core-Aggregation Network

This architecture model applies to small geographies where core and aggregation networks may not have distinct physical topologies and are integrated under common operations, and where network segmentation is not required for availability reasons. It assumes a non-MPLS IP/Ethernet or TDM access being aggregated in a small-scale network. See Figure 1-1.

Figure 1-1 Flat LDP Core-Aggregation



The small-scale aggregation network is assumed to be comprised of core nodes and AGNs 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.

The access network is based on native Layer 1 or Ethernet links in:

- Point-to-point or ring topologies over fiber (FTTH and PON) and newer Ethernet microwave-based access technologies, OR
- Point-to-point TDM+Ethernet links over hybrid microwave, OR
- Simple ring or Layer 2 Fabric network virtualization (nV).

All services are aggregated in AGNs, which provide TDM/ATM/Ethernet VPWS, Ethernet VPLS, PBB-EVPN and MPLS VPN transport.

Transport Models: Small Network - IP/MPLS Access

The following architecture models apply to networks deployed in small geographies. They assume an MPLS-enabled access network with fiber and packet microwave links being aggregated in a small-scale network.

Service end point routes are propagated into the access domain according to one of two models:

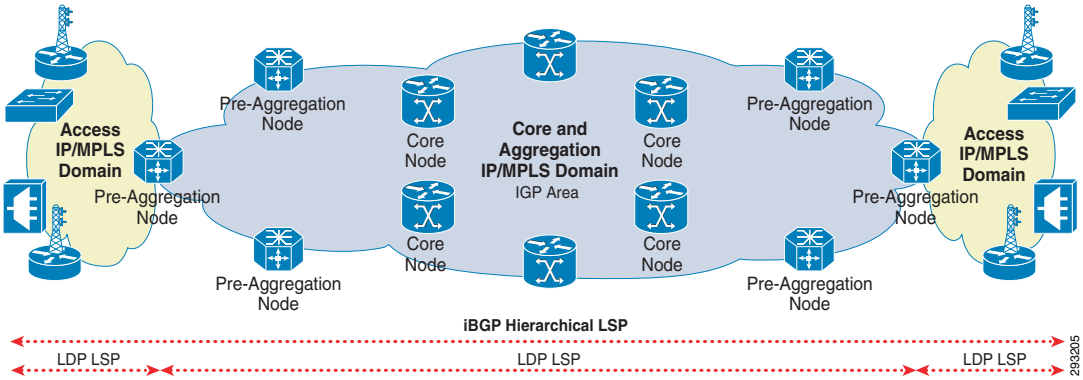
- by extending Labeled BGP into the access domain
- by redistributing relevant inter-domain routes into the access domain

The two models are described in the next sections.

Hierarchical-Labeled BGP LSP Core-Aggregation and Access

Figure 1-2 depicts a small network where access and aggregation-core domains are integrated via Labeled BGP.

Figure 1-2 Hierarchical-Labeled BGP LSP Core-Aggregation and Access



The small-scale aggregation network is comprised of core nodes and AGNs that are integrated in a single IGP/LDP domain consisting of less than 1000 nodes. The 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 PANs 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 access networks are integrated with labeled BGP LSPs, with the PANs acting as ABRs performing a BGP next-hop-self (NHS) function to extend the iBGP hierarchical LSP across the two domains.

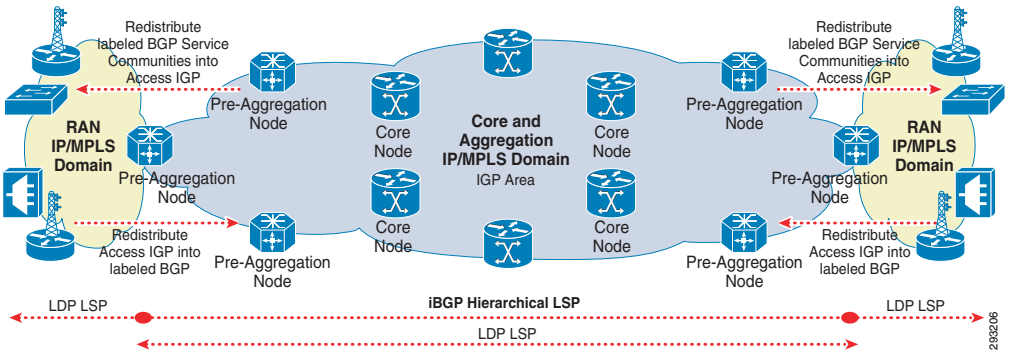
The mobile and wireline services can be enabled by the PANs/AGNs as in the Non-IP MPLS access, as well as by the ANs.

By utilizing a combination of BGP community filtering for mobile services and dynamic IP prefix filtering for wireline services, the ANs perform inbound filtering of BGP updates in order to learn the required remote destinations for the configured services. All other unwanted prefixes are dropped in order to keep the BGP tables small and prevent unnecessary updates.

Labeled BGP Redistribution into Access IGP

Figure 1-3 depicts a small network where access and aggregation-core domains are integrated via redistribution of inter-domain routes.

Figure 1-3 Labeled BGP Redistribution into Access IGP



The network infrastructure organization in this architecture model is the same as the one described in the "Hierarchical-Labeled BGP LSP Core-Aggregation and Access" section on page 1-7.

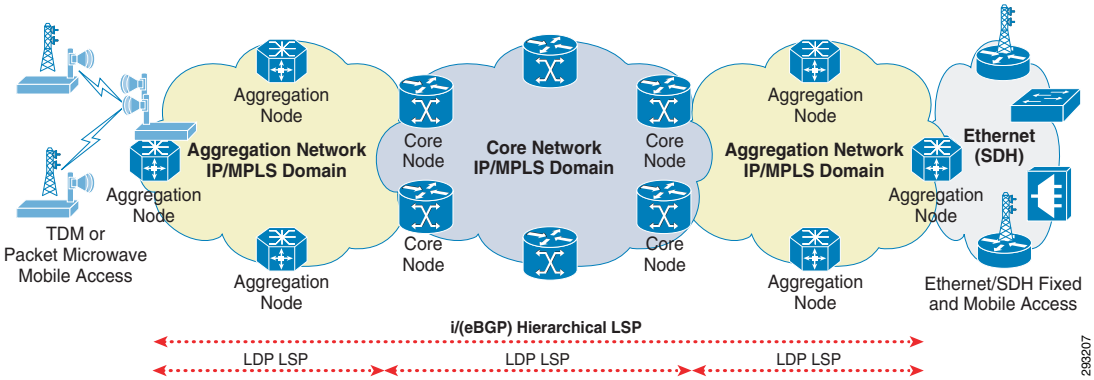
This model differs from the aforementioned one in that the hierarchical-labeled BGP LSP spans only the combined core/aggregation network and does not extend to the access domain. Instead of using BGP for inter-domain label distribution in the access domain, the end-to-end Unified MPLS LSP is extended into the access by using LDP with redistribution. The IGP scale in the access domain is kept small by selective redistribution of required remote prefixes from iBGP based on communities. Because this model has no mechanism for using dynamic IP prefix lists for filtering, the ANs support only mobile services. Both mobile and wireline services can be supported by the PANs or AGNs.

Transport Models: Large Network - Non-IP/MPLS Access

Hierarchical-Labeled BGP LSP Core and Aggregation

Figure 1-4 depicts the architecture model that 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 1-4 Hierarchical-Labeled BGP LSP Core-Aggregation



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 utilize a multi-AS design with 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 access network is based on native L1 or Ethernet links in:

- Point-to-point or ring topologies over fiber (FTTH and PON) and newer Ethernet microwave-based access technologies, or
- Point-to-point TDM+Ethernet links over hybrid microwave, or
- Simple ring or L2 Fabric network virtualization (nV).

All mobile and wireline services are enabled by the AGNs. 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 ASs, iBGP is used to build the hierarchical LSP from the PAN to the ASBRs and eBGP is used to extend the end-to-end LSP across the AS boundary.

The core network route reflector (RR) performs BGP community-based egress filtering towards the core ABRs/ASBRs, so that the aggregation networks learn only the required remote destinations for mobile and wireline service routing, and all unwanted prefixes are dropped. This helps reduce the size of BGP tables on these nodes and prevents unnecessary updates.

Transport Models: Large Network - IP/MPLS Access

The following architecture models apply to networks deployed in large geographies. They assume an MPLS- enabled access network with fiber and packet microwave links being aggregated in a large scale network.

Service endpoint routes are propagated into the access domain according to one of two models:

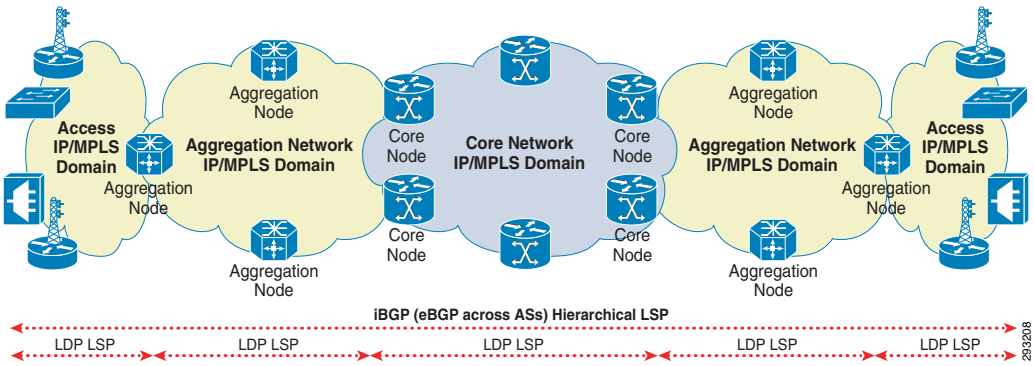
- Extending Labeled BGP into the access domain.
- Redistributing relevant inter-domain routes into the access domain.

The two models are described in the following sections.

Hierarchical-Labeled BGP LSP Core-Aggregation and Access

Figure 1-5 depicts a large network where access and aggregation and core domains are integrated via Labeled BGP.

Figure 1-5 Hierarchical-Labeled BGP LSP 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 utilize a multi-AS design with 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 typically enabled by running a different IGP process on the PANs corresponding to the aggregation and access networks. In the inter-AS option, while the core and aggregation networks are in different ASs, the separation between aggregation and access networks is enabled by making the access network part of a different IGP area from the aggregation network, or by running a different IGP process on the PANs corresponding to the aggregation and RAN access networks.

The mobile and wireline services can be enabled by the ANs in the access as well as the PANs and AGNs. 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 PANs and core

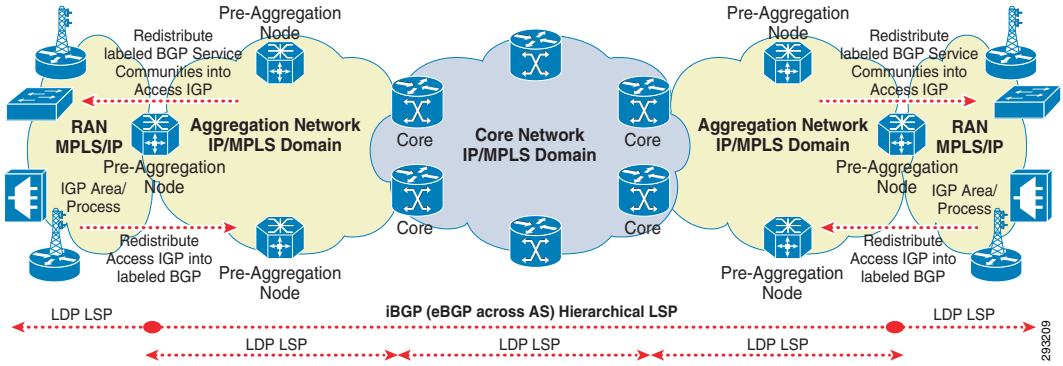
ABRs act as ABRs for their corresponding domains and extend the iBGP hierarchical LSP across the access, aggregation, and core domains. When the core and aggregation networks are organized in different ASs, the PANs act as ABRs performing BGP NHS function in order to extend the iBGP hierarchical LSP across the access and aggregation domains. At the ASBRs, eBGP is used to extend the end-to-end LSP across the AS boundary.

By utilizing a combination of BGP community filtering, in case of mobile services, and dynamic IP prefix filtering, for wireline services, the ANs perform inbound filtering of BGP updates in order to learn the required remote destinations for the configured services. All other unwanted prefixes are dropped in order to keep the BGP tables small and prevent unnecessary updates.

Hierarchical-Labeled BGP Redistribution into Access IGP

Figure 1-6 depicts a large network where the access domain is integrated with the rest of the network via redistribution of inter-domain routes.

Figure 1-6 Hierarchical-Labeled BGP Redistribution into Access IGP



The network infrastructure organization in this architecture model is the same as the one described above, with options for both Single-AS Multi-Area and Inter-AS designs. 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 access domain.

Instead of using BGP for inter-domain label distribution in the access domain, the end-to-end Unified MPLS LSP is extended into the access by using LDP with redistribution. The IGP scale in the access domain is kept small by selective redistribution of required remote prefixes from iBGP based on communities. Because there is no mechanism for using dynamic IP prefix lists for filtering in this model, only mobile services are currently supported by the ANs. Both mobile and wireline services can be supported by the PANs or AGNs.

IGP Protocols Considerations

As discussed earlier, Unified MPLS requires IGP segmentation in the different domains; this can be accomplished using areas or adjacencies levels depending on IGP protocol or IGP processes. The EPN System provides recommendations in segmentation approaches using either IS-IS or OSPF:

- For a Small Network, the EPN System recommends a common IGP process in the integrated core and aggregation domain:
  - In the case of IS-IS, the process establishes Level 2 adjacencies in the core and Level 1 adjacencies in the aggregation domain.
  - In the case of OSPF, the integrated core+aggregation domain behaves as a OSPF backbone area.

  - For both IS-IS and OSPF, a MPLS-enabled access domain uses a dedicated IGP process.
- In the case of a Large Network in a Multi-Area scenario, the EPN System also recommends a common IGP process for the core and aggregation domains:
  - In the case of IS-IS, the protocol establishes Level 2 adjacencies in the core and Level 1 adjacencies in the aggregation domain.
  - In the case of OSPF, the core domain operates as a OSPF backbone area, and the ag-gregation domain as a very stubby area.
  - For both IS-IS and OSPF, a MPLS-enabled access domain uses a dedicated IGP process.
- In the case of a Large Network in a Single-AS scenario, the EPN System recommends dedicated IGP processes for the core and for the aggregation+access domains:
  - In the case of IS-IS, the protocol establishes Level 2 adjacencies in both the core and the aggregation network in their respective process, and Level 1 adjacencies in the access domain. Alternatively, controlled distribution via route-policy-language on a per-area tag is also possible in the access domain.
  - In the case of OSPF, the core and the aggregation domain operate as backbone areas in their respective process, and the access domain as a very stubby area.

Other models are possible, such as individual IGP processes for each domain, however when deciding how to implement IGP segmentation, the following considerations must be kept in mind:

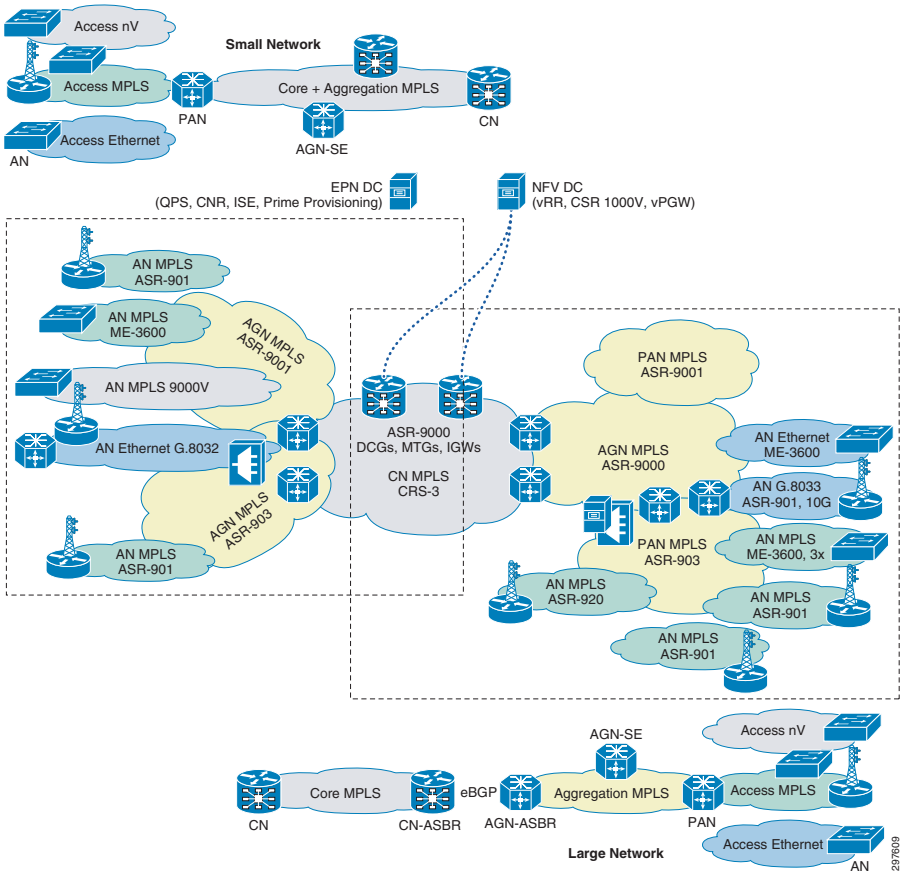
- The number of independent IGP processes supported by a given interdomain node, such as an ABR.
- The feature availability on BVI/SVI interfaces needed for IGP segmentation by process because of the L2 segmentation of the inter ABR links:
  - For instance, remote LFA FRR and BGP PIC are not supportable on SVI interfaces on ASR-903.

System Test Topologies

The development process for the Cisco EPN 4.0 System provides extensive validation of various functional aspects of the system design. This validation is conducted on a test bed designed to emulate the characteristics of a converged operator's production network environment. The details of the system test bed are illustrated in this chapter. The node names, loopback addresses, and other information will correlate to the configuration examples shown in this design and implementation guide.

Figure 2-1 shows a high-level overview of the entire test network topology, illustrating both the small and large network validation areas connected to a common core network domain.

Figure 2-1 Test Topology High-Level Overview



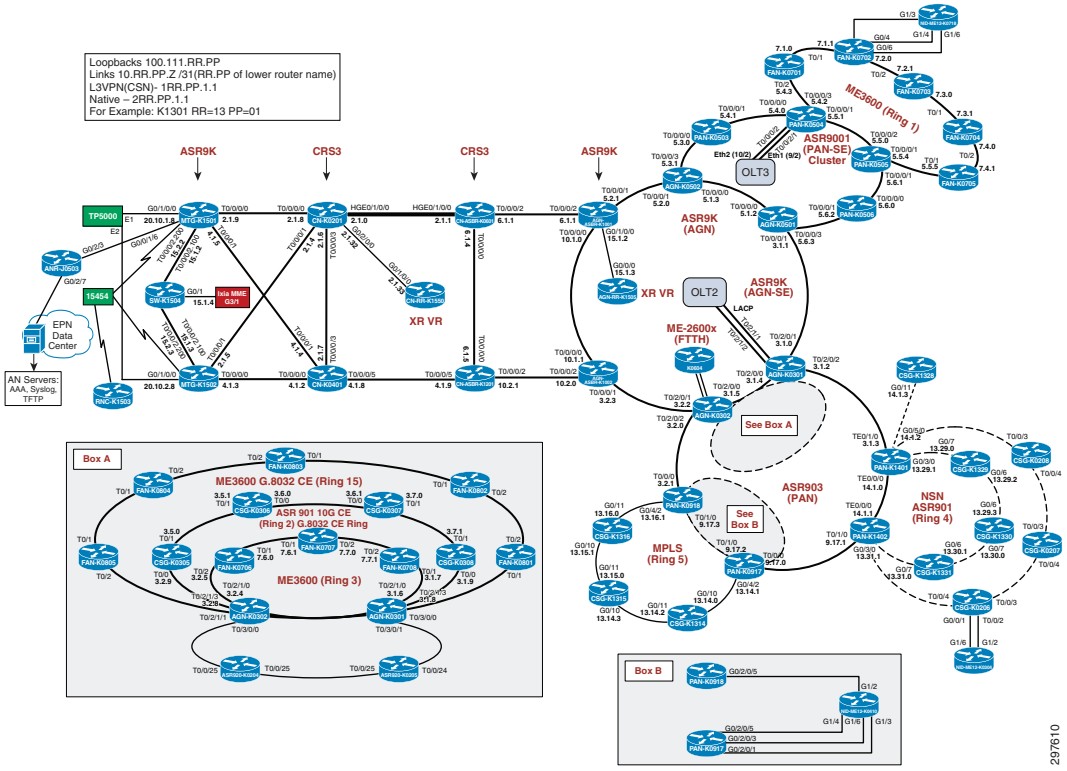
In particular, it shows the various access domains, with the access technologies implemented in each of them, including MPLS, Ethernet (G.8032-enabled rings or hub-and-spoke topologies), network virtualization (nV), and the type of access nodes in place, such as cell site routers for mobile access, and PON OLTs or FTTH fixed access nodes for fixed access.

Figure 2-2 shows a detailed view of the large network test bed, with access and aggregation domains in one BGP autonomous system interfacing via aggregation node-Autonomous System Boundary Routers (AGN-ASBR) and core node ASBRs (CN-ASBR) in a different BGP autonomous systems. The core network is in AS-1000, and the aggregation network (Metro-1) is in AS-101.

In the core network, the Mobile Transport Gateways (MTG) are provider edge (PE) devices terminating Multiprotocol Label Switching (MPLS) VPNs and/or Any Transport over MPLS (AToM) pseudowires in order to provide connectivity to the Evolved Packet Core (EPC) gateways (including Security Gateway [SGW], Packet Data Network Gateway [PGW], and Mobility Management Entities [MME]) in the Mobile Packet Core (MPC).

The nodes marked with aggregation node service edge (AGN-SE)+ or pre-aggregation node service edge (PAN-SE) are SE nodes (SEN) for consumer and enterprise wireline services, providing per-subscriber policy enforcement functions for those services. The nodes marked "OLT#" show the placement of the Gigabit Passive Optical Network (GPON) Optical Link Terminator (OLT) nodes within the network.

Figure 2-2 Test Topology-Large Network, Inter-Autonomous System Design



Within each metro network, multi-area Internet Gateway (IGP) organization between the aggregation and access domains is based on segmenting the aggregation network in Intermediate-System-to-Intermediate-System Protocol (IS-IS) Level 2 and the access networks in IS-IS Level 1. Each routed, or MPLS-enabled, access network subtending from a pair of pre-aggregation nodes (PANs) is part of a unique IS-IS Level 1 domain. All access rings or hub-and-spokes subtending from the same pair of PANs are part of the IS-IS Level 1 domain, where the cell site gateways (CSGs) are

IS-IS L1 nodes and the PAN are L1/L2 nodes. The default IS-IS behavior of Level 1 to Level 2 route distribution is prevented in order to keep the access and aggregation domains isolated and contain the route scale within the respective domains.

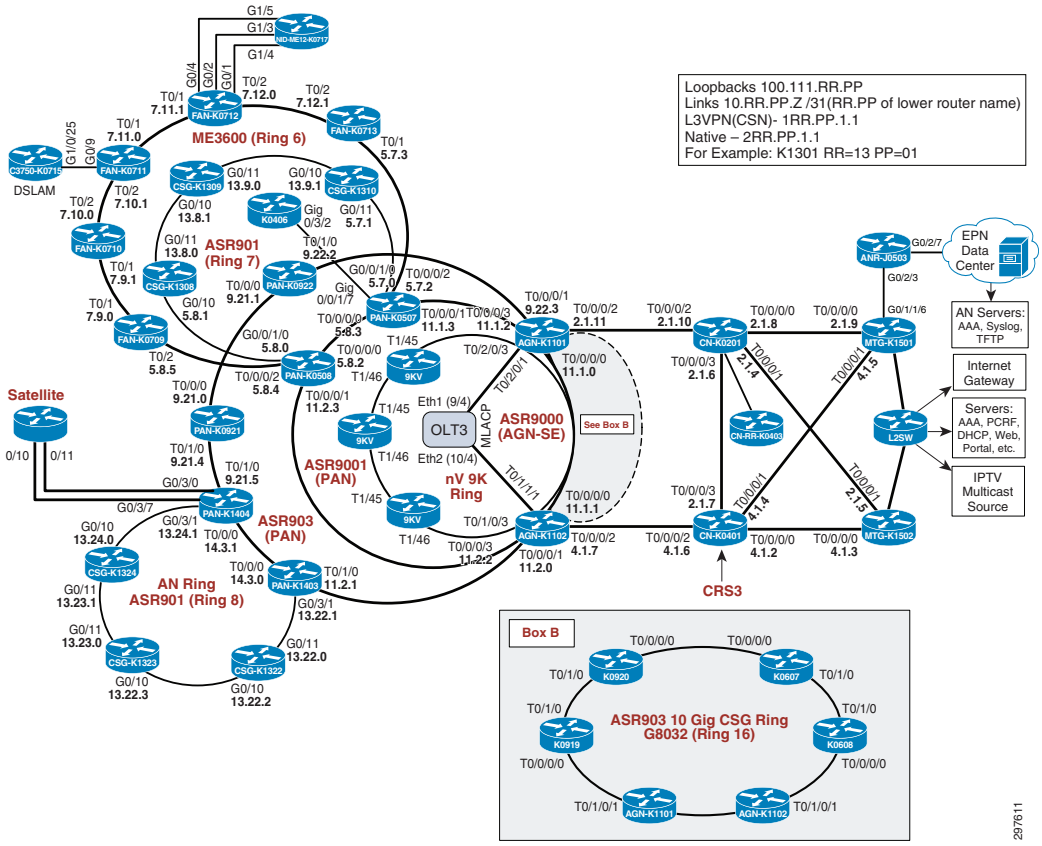
Partitioning these network layers into such independent and isolated IGP domains helps reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence within each of these domains. Intra-domain Label-Switched Paths (LSPs) within the core, aggregation, and access domains are based on Label Distribution Protocol (LDP). Inter-domain LSPs across the core, aggregation, and access domains are based on BGP labeled-unicast, where internal BGP (iBGP) labeled-unicast is used within each autonomous system, and exterior BGP (eBGP) labeled-unicast is used to extend the LSP across autonomous system boundaries, as described in the "Large Network Transport Architecture Design - Inter-AS" section on page 3-17.

Non-MPLS access in the Large Network is implemented as G.8032-enabled access rings, which are capable of sub-50 millisecond reconvergence in case of link or node failures. Each ring is terminated to a pair of PAN nodes for Dual Homing and traffic is load shared among PANs based on VLAN/service.

Figure 2-3 shows a detailed view of the small network test bed, which has the core and aggregation domains integrated into a single IGP/LDP domain. This integrated domain consists of core nodes (CN) that connect to aggregation nodes (AGN), where the combined number is assumed less than 1000 nodes. The MTGs are PE devices terminating MPLS VPNs and/or AToM pseudowires in order to provide connectivity to the EPC gateways (SGW, PGW, and MME) in the MPC.

The AGNs have subtending access networks with CSGs and FANs supporting Cisco EPN service access, both of which are enabled for MPLS and part of the same autonomous system as the integrated core+aggregation network. The AGN-SE nodes provide the service edge functionality for consumer and enterprise wireline services just as in the large network topology. The OLT node shows the placement of the GPON OLT within the network.

Figure 2-3 Test Topology-Small Network, IGP/LDP Design



From a multi-area IGP organization perspective, the network is segmented into different IGP areas where the integrated core+aggregation domain is in IS-IS Level 2, and the subtending routed, or MPLS-enabled, access networks are in IS-IS Level 1. 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 LSPs across the integrated core+aggregation and access domains are based on BGP-labeled unicast, as described in the "Small Network Transport Architecture Design" section on page 3-1.

Non-MPLS access in the Small Network is implemented as either G.8032-enabled access rings, or a collection of nV Satellite Nodes in simple ring or L2 Fabric topologies, terminating directly at the AGN nodes. Both access technologies support Dual Homing to a pair of PAN or AGN nodes with per VLAN and per node load sharing, respectively, for service redundancy, as well as subsecond reconvergence in case of failure.

Transport Architecture Design

This chapter, which details the network design for the transport models introduced previously in Chapter 1, "Introduction," includes the following major topics:

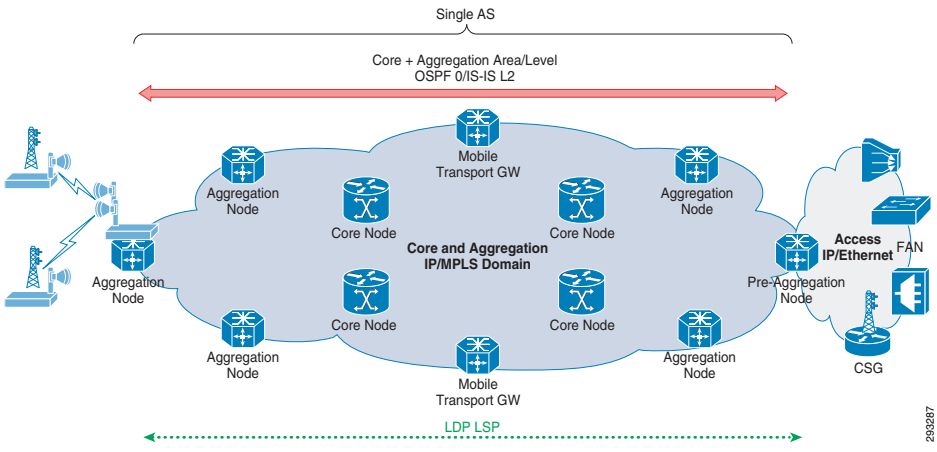
Small Network Transport Architecture Design

This section focuses on the network design for the transport models associated to a small network with either IP/MPLS or Non-IP/MPLS Access.

Non-IP/MPLS Access

This section details the system architecture for the "Flat LDP core-aggregation network" transport model. This model assumes that the core and aggregation networks form a single IGP/LDP domain consisting of less than 1000 nodes. The single IGP domain can be implemented as an OSPF Area 0 or as an IS-IS L2 backbone. Since there is no segmentation between network layers, a flat LDP LSP provides end-to-end reachability across the network. See Figure 3-1.

Figure 3-1 Single-Area IGP with Flat LDP Core and Aggregation



Depending on the service, the access network can be based on:

- TDM and packet microwave links, for mobile transport services.
- FTTH or PON Ethernet links in Hub and Spoke topologies, for consumer, enterprise and MEF services.
- G.8032-protected Ethernet rings, for all service types.
- Simple Ring or L2 Fabric nV, for MEF and enterprise services.

All services are enabled by the AGNs or PANs. These include:

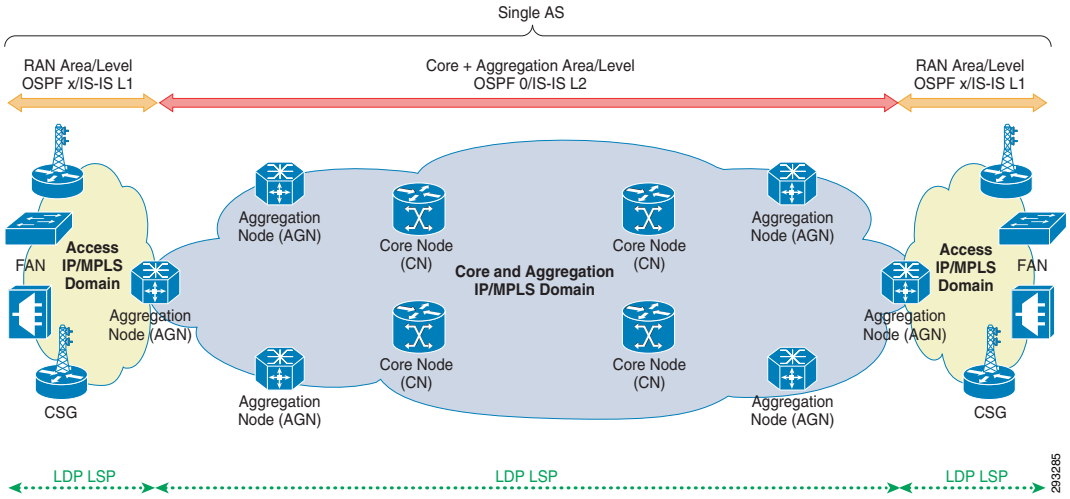
- GSM Abis, ATM IuB, IP IuB, and IP S1/X2 interfaces for 2G/3G/LTE services for RAN access domains with point-to-point connectivity over TDM or hybrid (TDM+Packet) microwave.
- IP IuB, and IP S1/X2 interfaces for 3G/LTE services for RAN access domains with point-to- point or ring topologies over fiber or packet microwave.
- MEF E-Line, E-LAN, and E-Tree L2VPN services and enterprise L3VPN services.
- Consumer triple play services with Ethernet connectivity from the ANs (FANs, PON OLTs, etc.) to the PAN-SE nodes.
- Wireless Access Gateway functions for Community WiFi users connecting from the PON OLTs, or BYOD users connecting from the Access Points and Wireless LAN Controller.

IP/MPLS Access

This section details the system architecture for the transport model described in Hierarchical-Labeled BGP LSP Core-Aggregation and Access, page 1-7.

It assumes that the core and aggregation networks are integrated into a single IGP/LDP domain consisting of less than 1000 nodes. The AGNs have subtending access networks that are MPLS-enabled and part of the same AS as the integrated core+aggregation network. See Figure 3-2.

Figure 3-2 Integrated Core and Aggregation with IP/MPLS Access



From a 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 AGNs are in IS-IS Level 1 or OSPF non-backbone areas. ANs are IS-IS L1 nodes or Area Routers, while

the AGN are L1/L2 nodes or ABRs, for IS-IS and OSPF respectively. 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.

The collapsed core+aggregation and access networks are integrated with labeled BGP LSPs.

Inter-Domain LSPs

The Cisco EPN System uses hierarchical LSPs for inter-domain transport. The hierarchical LSP is built with a BGP-distributed label that transits the isolated MPLS domains and an intra-domain, LDP-distributed label that reaches the labeled BGP next hop.

This section describes inter-domain hierarchical LSPs where core and aggregation networks are integrated into a single IGP/LDP domain. The AGNs have subtending access networks that are MPLS-enabled and part of the same AS.

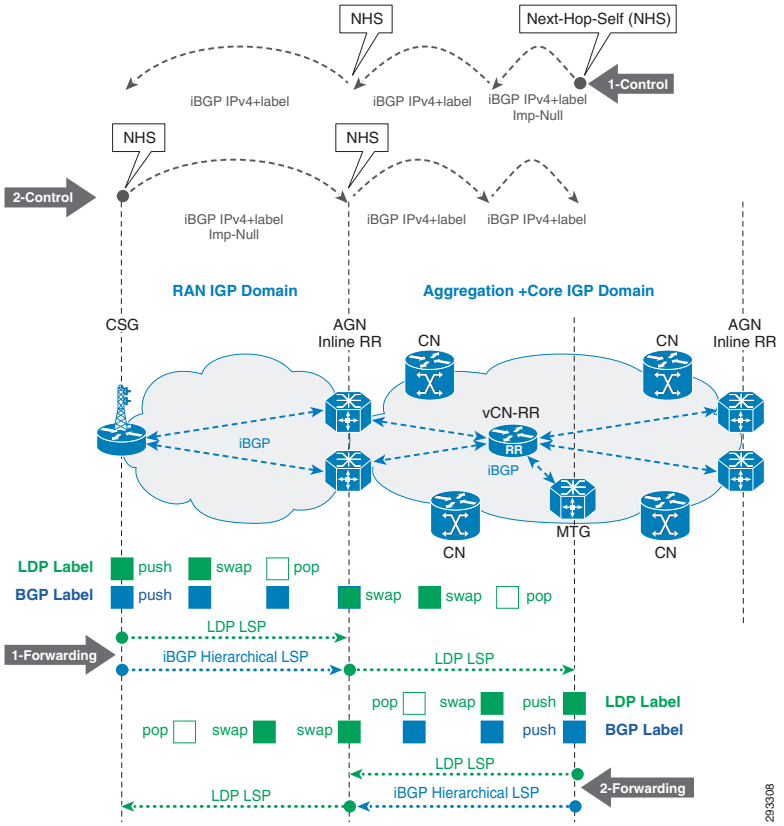
Hierarchical LSPs between Service Edge Nodes

This scenario is applicable to point-to-point X-Line services between CSGs and/or FANs in different labeled BGP access areas. In this instance, the /32 loopback address of the remote AN is added to the inbound prefix filter list at the time of service configuration on the local AN.

The scenario also 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).

As an example, Figure 3-3 shows the hierarchy of LSPs between a CSG and the MTG.

Figure 3-3 Hierarchical LSPs for Integrated Core and Aggregation Design



The CSG in the RAN access learns the loopback 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 3-3, 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 the previous figure, the following sequence occurs:

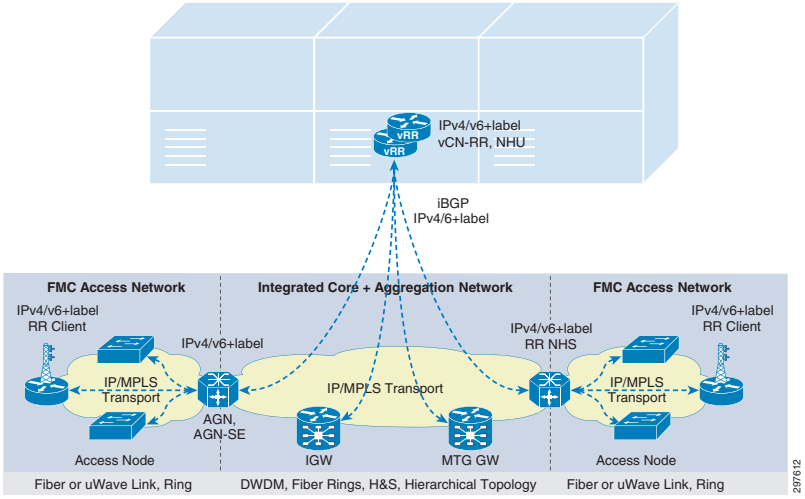
1. The downstream MTG node will first push the BGP label corresponding to the remote prefix and then push the LDP label that is used to reach the AGN that is the labeled BGP next hop.
2. The CNs and AGNs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP 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.

BGP Transport Control Plane

The Cisco EPN System proposes a hierarchical RR design for setting up the Unified MPLS Transport 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 EPN network.

The need for standalone RRs in the lower layer 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 Core Network RR (CN-RR) function that is virtualized in the Data Center (vCN-RR). See Figure 3-4.

Figure 3-4 BGP Control Plane for Integrated Core and Aggregation Design with IP/MPLS 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 RR:

- Gateway routers, such as MTGs providing connectivity to the MPC, or IGWs providing access to the Internet, are labeled BGP PEs in the core. iBGP labeled-unicast sessions are established with the vCN-RR and loopbacks are advertised into iBGP labeled-unicast with a common BGP community representing the respective function: MSE BGP community for MTGs, IGW BGP community for IGWs. MTGs and IGWs learn BGP prefixes marked with the MSE and common RAN community, and with the FSE and IGW community, respectively.
- AGNs are labeled BGP ABRs between the integrated core+aggregation and access domains. iBGP-labeled unicast sessions are established with the virtualized vCN-RRs, and act as inline-RRs for the local access network clients. AGNs also act as labeled BGP PEs and advertise loopbacks into BGP-labeled unicast with a common BGP community that represents the service types in the access network: RAN for mobile, FAN for fixed business wireline. AGNs learn labeled BGP prefixes marked with the MSE and/or IGW BGP communities if services are connected locally. AGNs are inserted into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards the vCN-RRs and the local access clients. Pairs of AGN nodes serving the same access network is configured with the same BGP Cluster-Id to avoid loops. AGNs shared by multiple access networks require different Cluster IDs for each access network.
- FSE gateways, such as AGN-SEs and PAN-SEs, are labeled BGP PEs residing in the aggregation network. iBGP labeled-unicast sessions are established with the vCN-RR, and advertise loopbacks into iBGP-labeled unicast with a common BGP FSE community. FSEs learn labeled BGP prefixes marked with the global FSE and IGW communities. The SE node functionality can reside within the AGN node described previously; there is no technical requirement for separate SE nodes.

- CSGs in the RAN access networks are labeled BGP PEs. iBGP-labeled unicast sessions are established with the local AGN inline-RRs. CSGs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the global RAN access community. To minimize the number of routes a CSG needs to learn to achieve the required Inter-Access X2 communication, CSGs also advertise their loopbacks with a pair of BGP communities designed according to the scaling capacity of the CSGs. Low and high scale CSG nodes export their loopbacks with both the aggregation-wide RAN community and the access-wide local RAN community. The high-scale CSGs import the aggregation-wide RAN community only; the low-scale CSGs still import the access-wide local and neighbor RAN communities.

Note Aggregation-wide RAN community is the common RAN community for an aggregation domain and access-wide RAN community is the community for a specific access domain.

Using an aggregation-wide RAN community simplifies the network planning and filtering operations required for inter-access X2 communication by assigning a single RAN community to all high- scale access nodes within an aggregation domain. In a hybrid network with both low and high-scale CSG nodes, the use of either aggregation-wide or access-wide RAN communities enables inter-access X2 communication between access nodes with same and different scaling capacity and allows for a stepped approach in the upgrade of the access network from low to high capacity devices. Labeled BGP prefixes marked with the MSE BGP community are learned for reachability to the MPC, and the aggregation-wide community or the access-wide adjacent RAN access BGP communities are learned if inter-access X2 connectivity is desired.

Note Use of access-wide RAN community is optional and only required when the local or neighbor access domain has low scale CSG access nodes. If both local and neighbor access domains have only high scale CSG access nodes, then import and export of only aggregation-wide RAN community is sufficient to achieve inter-access X2 communication.

- FANs in the access networks are labeled BGP PEs. iBGP-labeled unicast sessions are established with the local AGN inline-RRs. FANs advertise loopbacks into BGP-labeled unicast with a common BGP community representing the FAN access community. Labeled BGP prefixes marked with the FSE BGP community are learned for reachability to the AGN-SE or PAN-SE, while prefixes marked with the FAN BGP community provide reachability to remote FANs.

The MTGs and IGWs in the integrated core+aggregation network are capable of handling large network scale requirements, and will learn all BGP-labeled unicast prefixes for connectivity to all the CSGs and fixed SE nodes (and possibly ANs) in the entire network.

For mobile services, simple prefix filtering based on BGP communities is performed on the vCN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into other AGNs where they are not needed. The AGNs only learn labeled BGP prefixes marked with the common RAN and the MSE BGP communities, allowing the AGNs to enable inter-metro wireline services across the integrated core+aggregation and also to reflect only these prefixes to their local access networks. Isolating the integrated core+aggregation and access domain by preventing the default IGP redistribution enables the RAN access networks to have limited route scale, since the CSGs only learn local IGP routes and labeled BGP prefixes marked with the MSE BGP community.

For fixed wireline services, nodes providing fixed service edge functionality are also capable of handling a high degree of scalability, and will learn the common FAN community for AN access, the FSE community for service transport to other FSE nodes, and the IGW community for internet access. The use of a separate IGP process for the access domain enables the access network to have limited control plane scale, since ANs only learn local IGP routes and labeled BGP prefixes marked with the FSE BGP community or permitted via a dynamically-updated IP prefix list.

Large Network Transport Architecture Design - Multi-Area IGP

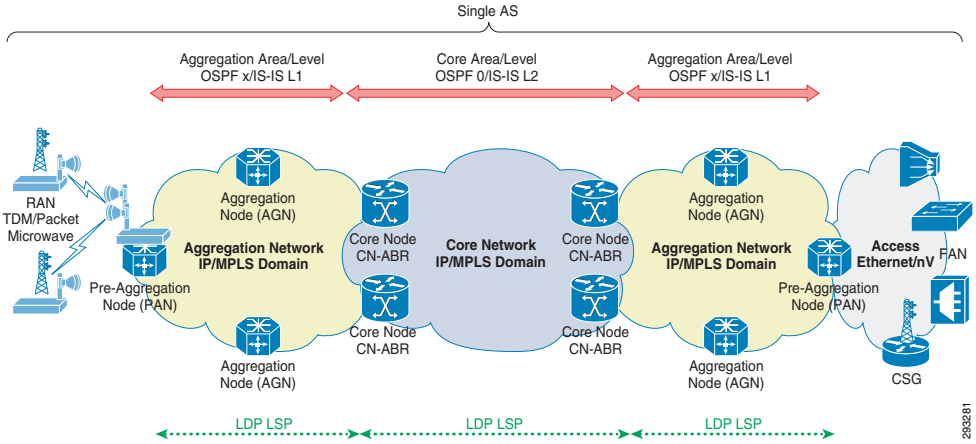
This section focuses on the network design for the transport models associated to Large Networks and it assumes that the network organization between the core and aggregation domains is based on a single AS, multi-area IGP design for both IP/MPLS and Non-IP/MPLS access.

Non-IP/MPLS Access

This section details the system architecture for the transport model described in Hierarchical-Labeled BGP LSP Core and Aggregation, page 1-6.

It assumes a non-MPLS IP/Ethernet or TDM access where all mobile and potentially wireline services are enabled by the AGNs or PANs.

Figure 3-5 Multi-Area IGP/LDP Domain Organization



From a 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.

Depending on the service, the access network can be based on:

- TDM and packet microwave links, for mobile transport services
- FTTH or PON Ethernet links in hub-and-spoke topologies, for consumer, enterprise and MEF services
- G.8032-protected Ethernet rings, for all service types
- Simple Ring or L2 Fabric network virtualization (nV), for MEF and enterprise services

All MPLS services are enabled by the AGNs or 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.
- MEF E-Line, E-LAN and E-Tree L2VPN services and Enterprise L3VPN services.

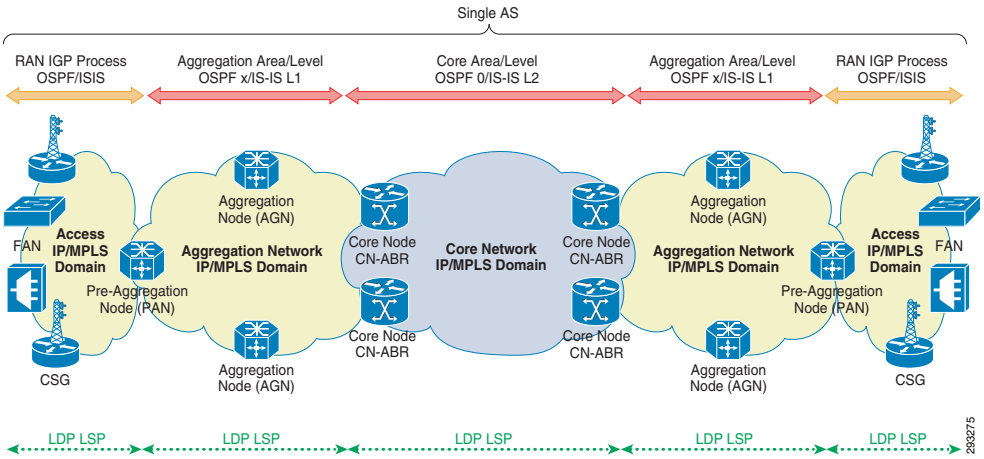
- Consumer triple play services with Ethernet connectivity from the access nodes (FANs, PON OLTs, etc.) to the PAN-SE nodes.

RFC 3107 procedures based on iBGP IPv4 unicast+label are used as an inter-domain LDP to build hierarchical LSPs across domains. The BGP Transport control plane is described in BGP Transport Control Plane, page 3-14.

IP/MPLS Access

This paragraph details the system architectures for the transport models described in Hierarchical-Labeled BGP LSP Core-Aggregation and Access, page 1-4 and Hierarchical-Labeled BGP Redistribution into Access IGP, page 1-8. See Figure 3-6.

Figure 3-6 Multi-Area IGP/LDP Domain Organization



From a 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 Protocol 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 access networks subtending from AGNs or PANs are based on a different IGP process, restricting their scale to the level of the local access network. To accomplish this, the PANs run two distinct IGP processes, with the first process corresponding to the core-aggregation network (IS-IS Level 1 or OSPF non-backbone area) and the second process corresponding to the Mobile RAN access network. The second IGP process could be an OSPF backbone area or an IS-IS L2 domain. All nodes belonging to the access network subtending from a pair of PANs 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 by 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. The BGP Transport control plane is described in the "BGP Transport Control Plane" section.

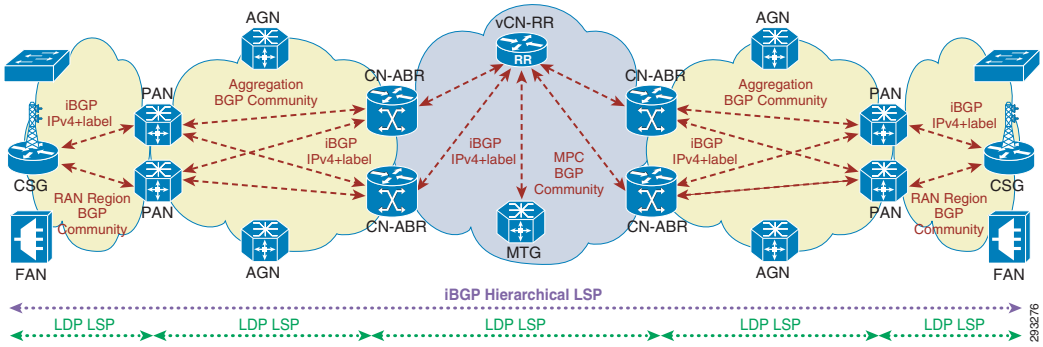
Two options, which are presented below, extend the Unified MPLS LSP into the access domain to accommodate different operator preferences.

Option-1: Labeled BGP Access

This option is based on the transport model described in Hierarchical-Labeled BGP LSP Core-Aggregation and Access, page 1-7.

Note This model supports transport of fixed wireline and mobile services. Figure 3-7 shows the example for RAN transport. The deployment considerations for both RAN transport and fixed wireline transport are covered in this guide.

Figure 3-7 Inter-Domain Transport for Multi-Area IGP Design with Labeled BGP Access



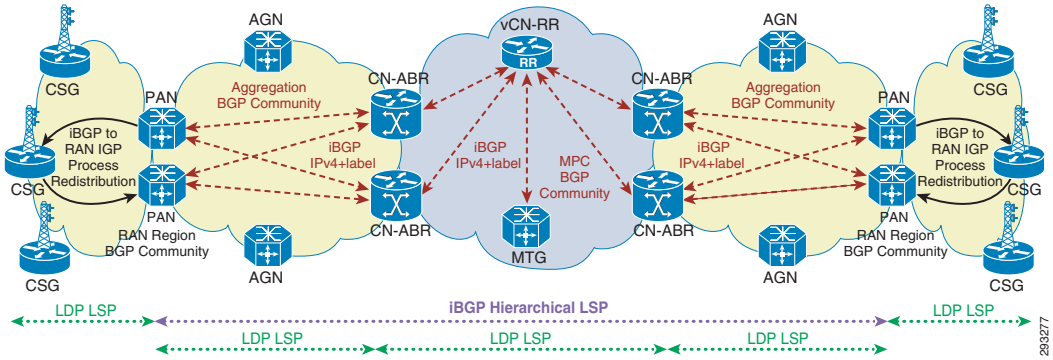
In this option, the access, aggregation, and core networks are integrated with Unified MPLS LSPs by extending labeled BGP from the core all the way to the nodes in the access network. Any node in the network that requires inter-domain LSPs to reach nodes in remote domain acts as a labeled BGP PE and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

Option-2: Labeled BGP Redistribution into Access IGP

This option is based on the transport model described in Hierarchical-Labeled BGP Redistribution into Access IGP, page 1-8.

Note The filtering mechanisms necessary for fixed wireline service deployment are not currently available in this option, so it supports only mobile service transport. Wireline service support will be added for this option in a future release.

Figure 3-8 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. Nodes in the access domain only run the IGP protocol.

Inter-Domain LSPs

The Cisco EPN System uses hierarchical LSPs for inter-domain transport. The hierarchical LSP is built with a BGP-distributed label that transits the isolated MPLS domains and an intra-domain, LDP-distributed label that reaches the labeled BGP next hop.

This section describes different hierarchical LSP structures for various service models applicable to a Large Network, single-AS multi-area IGP designs.

Hierarchical LSPs for Non-IP/MPLS Access

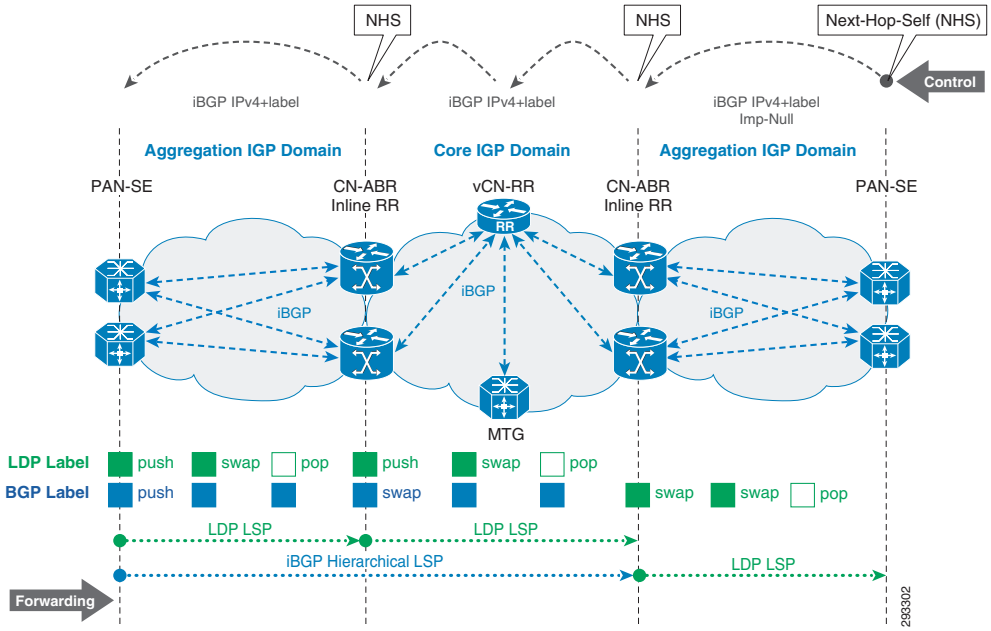
The inter-domain hierarchical LSP described in this paragraph applies to the Large Network Transport Architecture Design with Multi-Area IGP and Non-IP/MPLS Access scenario.

The LSP is set up between the loopback addresses of remote PAN or AGN-SE Nodes, connected across the core network. It is relevant to wireline L2/L3 MPLS VPN enterprise services deployed between remote service edges across the core network that use the /32 loopback address of the remote PEs as the endpoint identifier for the Targeting Label Distribution Protocol (T-LDP) or multiprotocol internal BGP (MP-iBGP) sessions. The enterprise wireline services are delivered to the service edge in one of three ways:

- Directly connected to the PAN.
- Transported from a FAN to the PAN or AGN service edge via native Ethernet network.
- Transported from a FAN to the PAN or AGN service edge via a PW in an MPLS access network scenario, which is terminated via PWHE on the SE.

The service edges are labeled BGP PEs and advertise their loopback using labeled IPv4 unicast address family (AFI/SAFI=1/4).

Figure 3-9 Hierarchical LSPs between Remote PANs for Multi-Area IGP Design



The remote service edges learn each other's loopbacks through BGP-labeled unicast. For traffic flowing between the two service edges as shown in the previous figure, the following sequence occurs:

1. The downstream service edge 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 AGNs 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 service edge via IGP, it will swap the BGP label with an LDP label corresponding to the upstream service edge intra-domain LDP LSP.

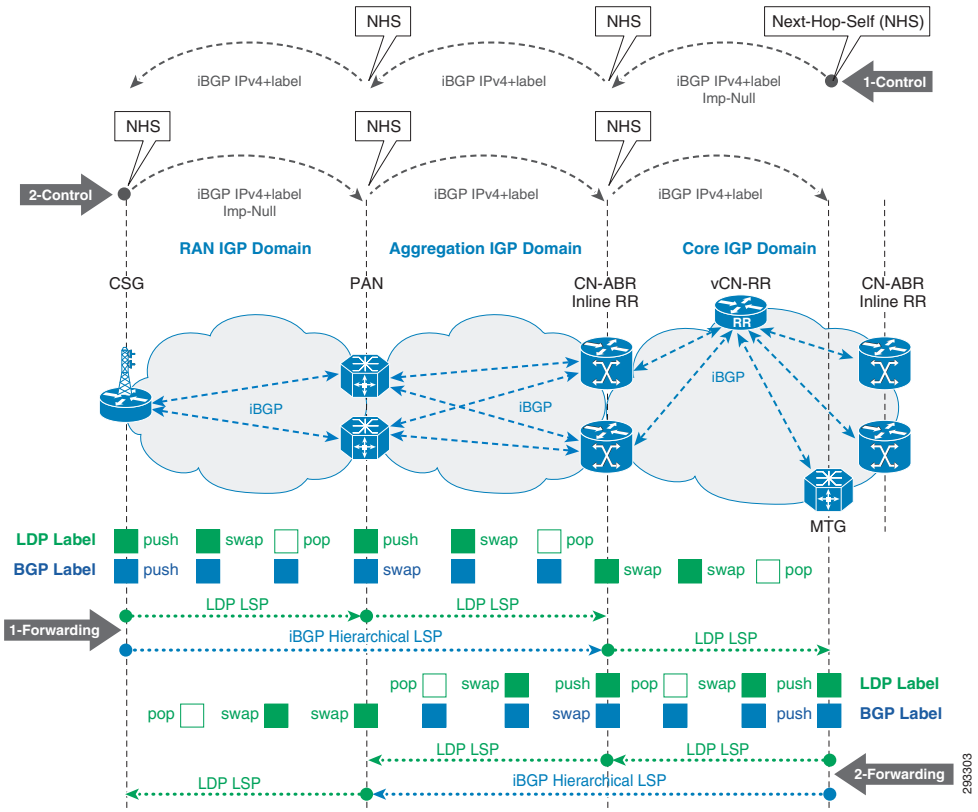
Hierarchical LSPs with Labeled BGP Access

The inter-domain hierarchical LSP described in this paragraph applies to the Large Network Transport Architecture Design with Multi-Area IGP and Labeled BGP IP/MPLS Access scenario.

The LSP is created 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/v6 unicast address family (AFI/SAFI=1/4).

This scenario is also applicable to point-to-point VPWS services between CSGs and/or FANs in different labeled BGP access areas. In this scenario, the /32 loopback address of the remote AN is added to the inbound prefix filter list at the time of service configuration on the local AN.

Figure 3-10 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 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 3-10, 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 AGNs 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 3-10. 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.

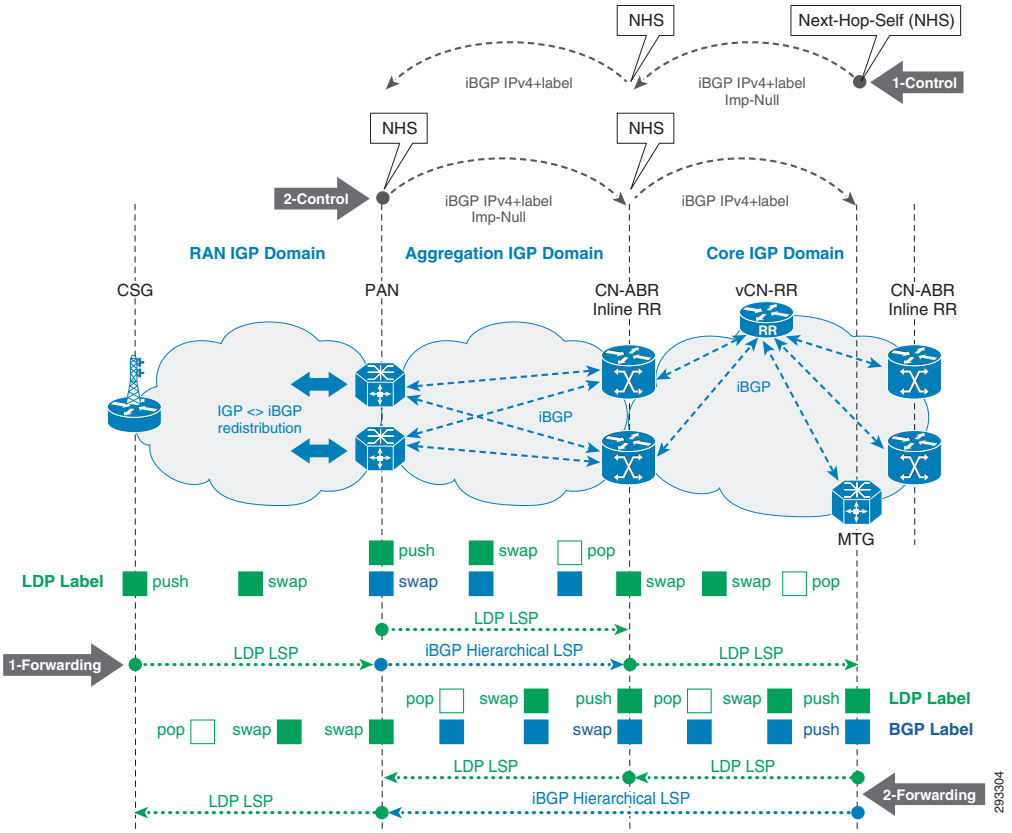
3. The CN-ABR will swap the BGP label corresponding to the remote prefix and then push the LDP label used to reach the PAN that is the labeled BGP next hop.
4. The AGNs that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP before handing off to the PAN.
5. 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 with Label BGP Redistribution in IGP/LDP Access

The inter-domain hierarchical LSP described here applies to the Large Network Transport Architecture Design with Multi-Area IGP and IP/MPLS Access with Labeled BGP Redistribution scenario.

The LSP is set up 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 L2VPNs 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/v6 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 3-11 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 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 3-11, 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.
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 AGNs 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 3-11, the following sequence occurs:

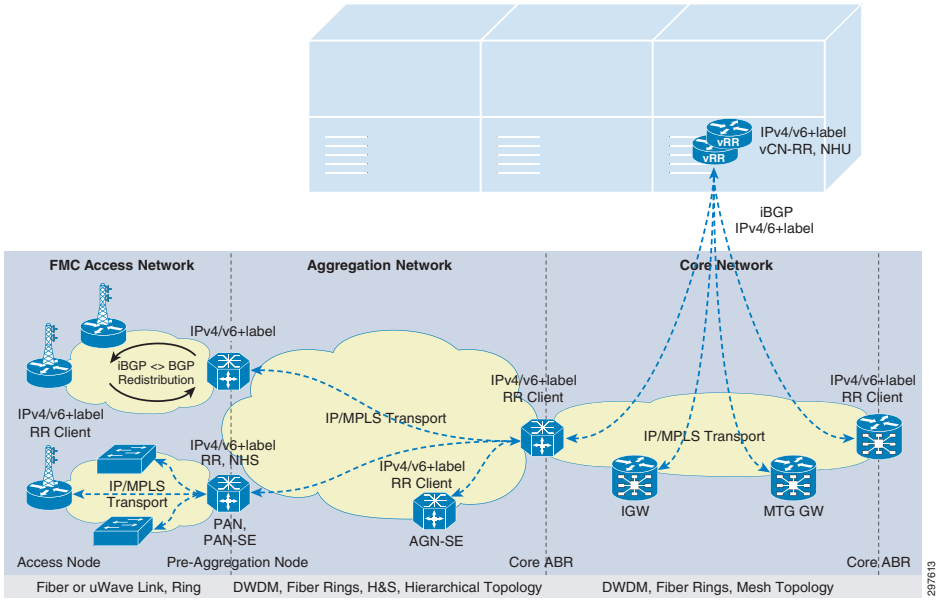
1. The downstream MTG node will first push the BGP label corresponding to the remote prefix and then push the LDP label that is used to reach the CN-ABR that is the labeled BGP next hop.
2. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a PHP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

BGP Transport Control Plane

The Cisco EPN System proposes a hierarchical RR design for setting up the Unified MPLS Transport 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 EPN network. See Figure 3-12.

The need for standalone RRs in the lower layers of the network to support this hierarchy is eliminated by making use of the inline-RR functionality on the CN-ABRs, between the core and aggregation domains, and at the Pre Aggregation Nodes (PANs), between the aggregation and access domains, in the case of labeled BGP access. At the top level of the hierarchy, the CN-ABRs peer as RR clients to a centralized external CN-RR function virtualized in the Data Center (vCN-RR).

Figure 3-12 BGP Control Plane for Large Network Design based on Multi-Area IGP Design and IP/MPLS Access



All nodes in the core and aggregation network that require inter-domain LSPs act as labeled BGP PEs and run iBGP-labeled unicast peering with designated RRs depending on their location in the network.

- Gateway routers, such as MTGs providing connectivity to the MPC or IGWs providing access to the Internet, are labeled BGP PEs in the core. iBGP labeled-unicast sessions are established with the vCN-RR and loopbacks are advertised into iBGP labeled-unicast with a common BGP community representing the respective function: MSE BGP community for MTGs, IGW BGP community for IGWs. MTGs and IGWs learn BGP prefixes marked with the MSE and common RAN community, and with the FSE and IGW community, respectively.
- CN-ABRs are labeled BGP ABRs between the core and aggregation domains. They utilize iBGP labeled-unicast sessions to peer with the virtualized vCN-RR in the core network, and act as inline-RRs for their local aggregation network PAN clients. The CN-ABRs insert themselves into the data path in order to enable inter-domain LSPs by setting NHS on all iBGP updates towards the CN-ABR in the core network and their local aggregation network PAN clients. The vCN-RR applies an egress filter toward the CN-ABR in order to drop prefixes with the common RAN community, which eliminates unnecessary prefixes from being distributed.
- PANs are labeled BGP ABRs between the aggregation and access domains. They utilize iBGP labeled-unicast sessions to peer with the vCN-ABR inline-RRs in the aggregation network, and act as inline-RRs for their local access network CSG/FAN clients. PANs also act as labeled BGP PEs and advertise loopbacks into BGP-labeled unicast with a common BGP community that represents the service communities being serviced by the PAN: RAN for mobile, FAN for fixed business wireline. PANs learn labeled BGP prefixes marked with the MSE and/or IGW BGP communities if services are connected locally. The PANs are inserted into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards the CN-ABRs and the local access clients.
- FSE gateways, such as AGN-SEs and PAN-SEs, are labeled BGP PEs residing in the aggregation network. iBGP labeled-unicast sessions are established with the CN-ABRs, and advertise loopbacks into iBGP-labeled unicast with a common BGP FSE community. FSEs learn labeled BGP prefixes marked with the global FSE and IGW communities. The SE node functionality can reside within the PAN node described previously; there is no technical requirement for separate SE nodes.

In addition, for an IP/MPLS-enabled access domain:

- In the case of Labeled BGP Access, the access nodes, CSGs and FANs, in the access networks are labeled BGP PEs. iBGP-labeled unicast sessions are established with the local PAN inline-RRs.
  - CSGs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the global RAN access community. To minimize the number of routes a CSG needs to learn to achieve the required inter-access X2 communication, CSGs also advertise their loopbacks with a pair of BGP communities designed according to the scaling capacity of the CSGs. Low and high scale CSG nodes export their loopbacks with both the aggregation-wide RAN community and the access-wide local RAN community. The high- scale CSGs import the aggregation-wide RAN community only; the low- scale CSGs still import the access-wide local and neighbor RAN communities. Labeled BGP prefixes marked with the MSE BGP community are learned for reachability to the MPC, and the aggregation-wide community or the access-wide adjacent RAN access BGP communities are learned if inter-access X2 connectivity is desired.

Note Aggregation-wide RAN community is the common RAN community for an aggregation domain and access-wide RAN community is the community for a specific access domain.

  - FANs advertise their loopbacks into BGP-labeled unicast with a common BGP com-munity representing the FAN access community. Labeled BGP prefixes marked with the FSE BGP community are learned for reachability to the AGN-SE or PAN-SE, while prefixes marked with the FAN BGP community provide reachability to remote FANs.
- In the case of Labeled BGP Redistribution into Access IGP, which is only supported for mobile services, 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 AN loopbacks (filtered based on IGP tags) are redistributed into iBGP-labeled unicast and tagged with a RAN access BGP community that is unique to that RAN access region. In the other direction, the MSE prefixes filtered based on MSE-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.

The MTGs and IGWs in the core network are capable of handling large network scale requirements, and will learn all BGP-labeled unicast prefixes because they need connectivity to all the CSGs and fixed SE nodes (and possibly ANs) in the entire network.

For mobile services, simple prefix filtering based on BGP communities is performed on the vCN-RRs for constraining IPv4+label routes from remote RAN access regions from proliferating into neighboring aggregation domains where they are not needed. The PANs learn only labeled BGP prefixes marked with the common RAN and the MSE BGP community allowing the PANs to enable inter-metro wireline services across the core and reflects the MSE prefixes 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 learn only local IGP routes and labeled BGP prefixes marked with the MSE BGP community.

For fixed wireline services, nodes providing fixed service edge functionality are also capable of handling large scale, and will learn the common FAN community for AN access, the FSE community for service transport to other FSE nodes, and the IGW community for internet access. The use of a separate IGP process for the access enables the access network to have limited control plane scale, since ANs only learn local IGP routes and labeled BGP prefixes marked with the FSE BGP community or permitted via a dynamically-updated IP prefix list.

Large Network Transport Architecture Design - Inter-AS

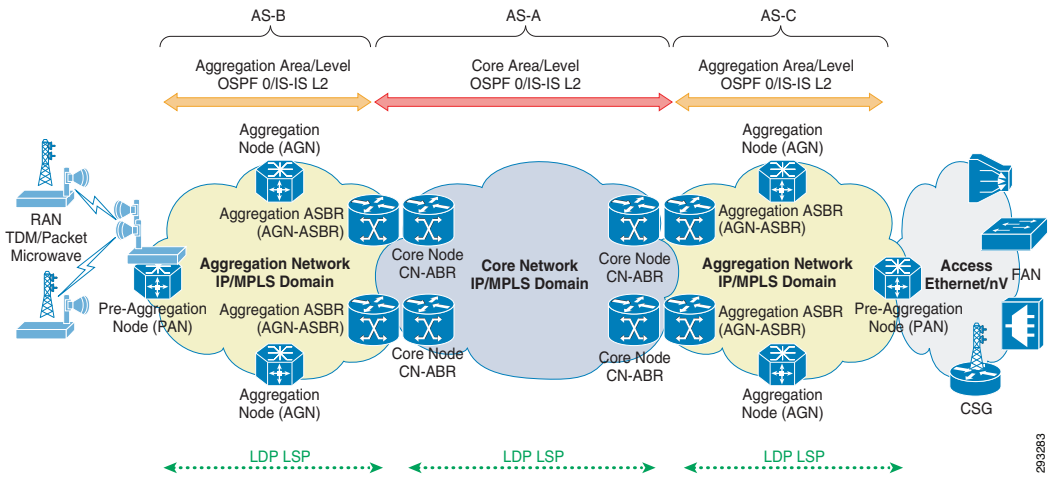
This section focuses on the network design for the transport models associated to Large Networks and it assumes that the core and aggregation networks are organized as different ASs for both IP/MPLS and Non-IP/MPLS access.

Therefore, it describes the creation of hierarchical-labeled BGP LSPs using a combination of iBGP-labeled unicast within each AS, and eBGP-labeled unicast to extend the LSP across AS boundaries.

Non-IP/MPLS Access

This section details the system architecture for the transport model described in Hierarchical-Labeled BGP LSP Core-Aggregation and Access, page 1-4. It assumes a non-MPLS IP/Ethernet or TDM access where all mobile and wireline services are enabled by the AGNs or PANs.

Figure 3-13 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. The core and aggregation networks are segmented into different ASs, and eBGP-labeled unicast is used to extend the LSP across AS boundaries. LDP provides label distribution to build intra-domain LSPs within each independent aggregation and core IGP domain.

Depending on the service, the access network can be based on:

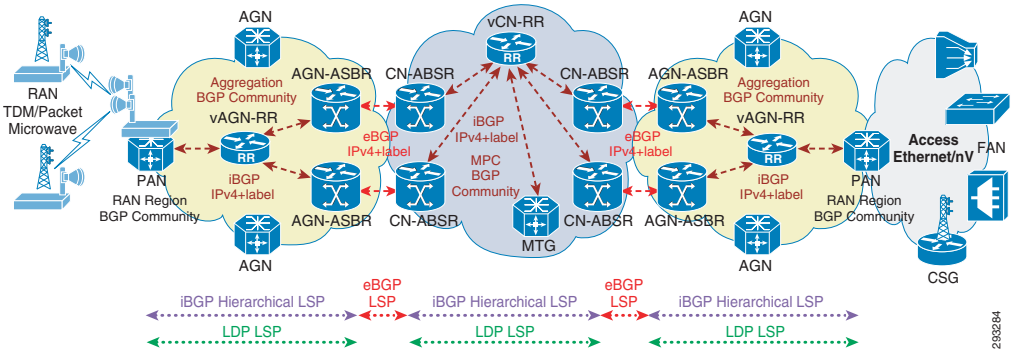
- TDM and packet microwave links, for mobile transport services.
- FTTH or PON Ethernet links in hub-and-spoke topologies, for consumer and enterprise services.
- G.8032-protected Ethernet rings, for all service types.
- Simple ring or L2 Fabric network virtualization (nV), for mobile and enterprise services.

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.
- MEF E-Line, E-LAN and E-Tree L2VPN services and enterprise L3VPN services.

- Consumer triple-play services with Ethernet connectivity from the ASs (FANs, PON OLTs, etc.) to the PAN-SE nodes.

Figure 3-14 Inter-Domain Transport with Hierarchical LSPs



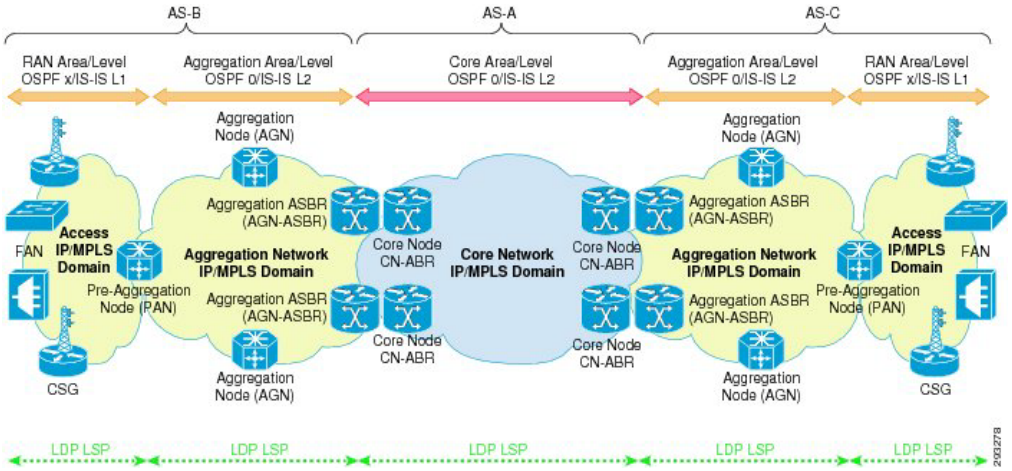
RFC 3107 procedures based on iBGP IPv4 unicast+label are used as an inter-domain LDP to build hierarchical LSPs across domains. All nodes in the core and aggregation network that require inter-domain LSPs act as labeled BGP PEs and run iBGP-labeled unicast peering with designated RRs, depending on their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

The BGP Transport control plane is described in the "BGP Transport control plane" section.

IP/MPLS Access

This section details the system architectures for the transport models described in Hierarchical-Labeled BGP LSP Core-Aggregation and Access, page 1-4 and Hierarchical-Labeled BGP Redistribution into Access IGP, page 1-8. Therefore, it presents two methods for extending the Unified MPLS LSPs from the core and the aggregation domain into the access domain. See Figure 3-15.

Figure 3-15 Inter-AS IGP/LDP Domain Organization



The core and aggregation networks are segmented into different ASs. 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 BGP Transport control plane is described in BGP Transport Control Plane, page 3-25.

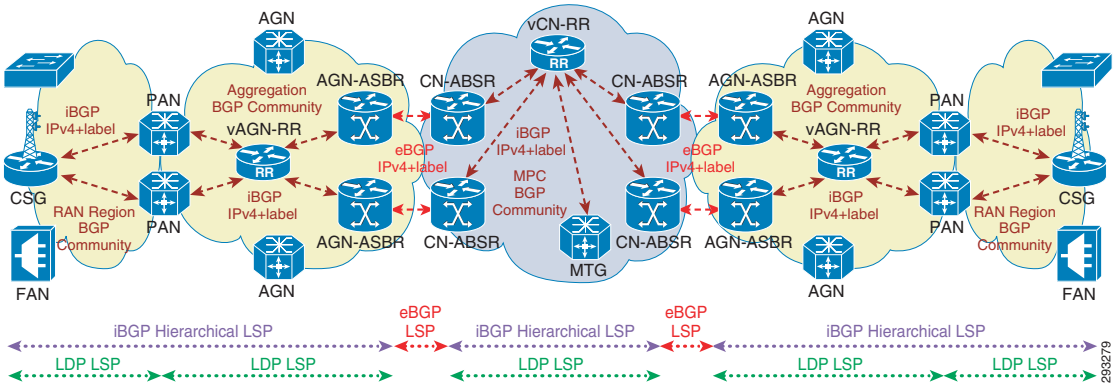
The Unified MPLS LSP can be extended into the access domain using two different options as presented below to accommodate different operator preferences.

Option-1: Labeled BGP Access

This option is based on the transport model described in Hierarchical-Labeled BGP LSP Core-Aggregation and Access, page 1-7.

Note This model supports transport of fixed wireline and mobile services. Figure 3-16 shows the example for RAN transport. The deployment considerations for both RAN transport and fixed wireline transport are covered in this guide.

Figure 3-16 Inter-Domain Transport for Inter-AS Design with Labeled BGP Access



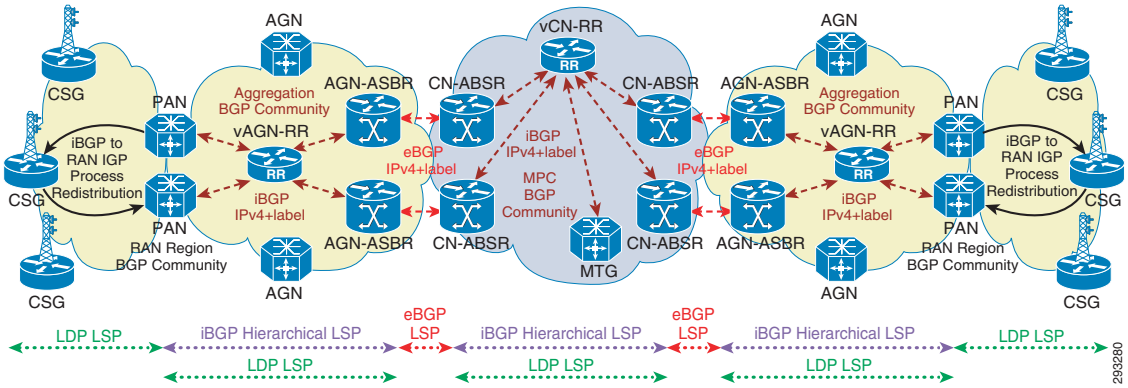
In this option, the access, aggregation, and core networks are integrated with Unified MPLS LSPs by extending labeled BGP from the core all the way to the nodes in the access network. Any node in the network that requires inter-domain LSPs to reach nodes in remote domain acts as a labeled BGP PE and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

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

This option is based on the transport model described in Hierarchical-Labeled BGP Redistribution into Access IGP, page 1-8.

Note This option supports only mobile service transport because the filtering mechanisms necessary for fixed wireline service deployment are not currently available in this option. Wireline service support will be added for this option in a future release.

Figure 3-17 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 RRs. Nodes in the access domain only run the IGP protocol.

Inter-Domain LSPs

The Cisco EPN System uses hierarchical LSPs for inter-domain transport. The hierarchical LSP is built with a BGP-distributed label that transits the isolated MPLS domains and an intra-domain, LDP-distributed label that reaches the labeled BGP next hop.

This section describes different hierarchical LSP structures for various service models applicable to a Large Network Multi-AS designs.

Hierarchical LSPs for Non-IP/MPLS Access

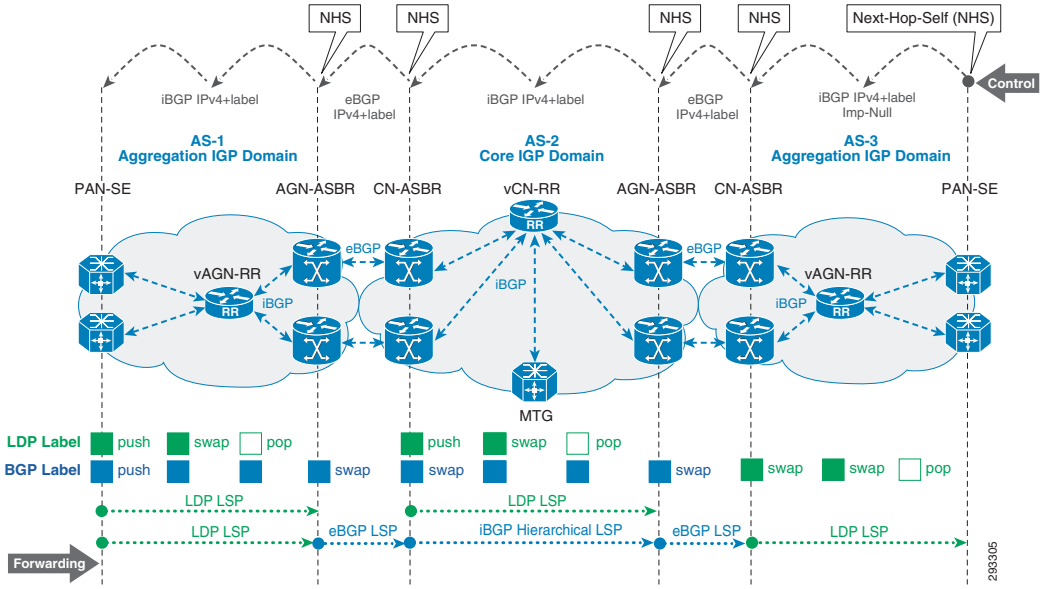
The inter-domain hierarchical LSP described in this paragraph applies to the Large Network Transport Architecture Design with Multi-AS and Non-IP/MPLS Access scenario.

The LSP is set up between the loopback addresses of remote PAN or AGN service edge Nodes, connected across the core network. It is relevant to MEF L2 VPN and enterprise L3VPN services deployed between remote service edges 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 enterprise wireline services are delivered to the service edge in one of three ways:

- Directly connected to the PAN.
- Transported from a FAN to the PAN or AGN service edge via native Ethernet network.
- Transported from a FAN to the PAN or AGN service edge via a PW in an MPLS access network scenario, which is terminated via PW Headend on the SE.

The PANs are labeled BGP PEs and advertise their loopback using labeled IPv4/v6 unicast address family (AFI/SAFI=1/4).

Figure 3-18 Hierarchical LSPs between Remote Service Edges for Inter-AS Design



The remote services edges learn each other's loopbacks through BGP-labeled unicast. iBGP-labeled unicast is used to build the inter-domain hierarchical LSP inside each AS, and eBGP-labeled unicast is used to extend the LSP across the AS boundary. For traffic flowing between the two service edges as shown in Figure 3-18, the following sequence occurs:

1. The downstream service edge 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 AGNs 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 service edge via IGP, it will swap the eBGP label with an LDP label corresponding to the upstream service edge intra-domain LDP LSP.

Hierarchical LSPs with Labeled BGP Access

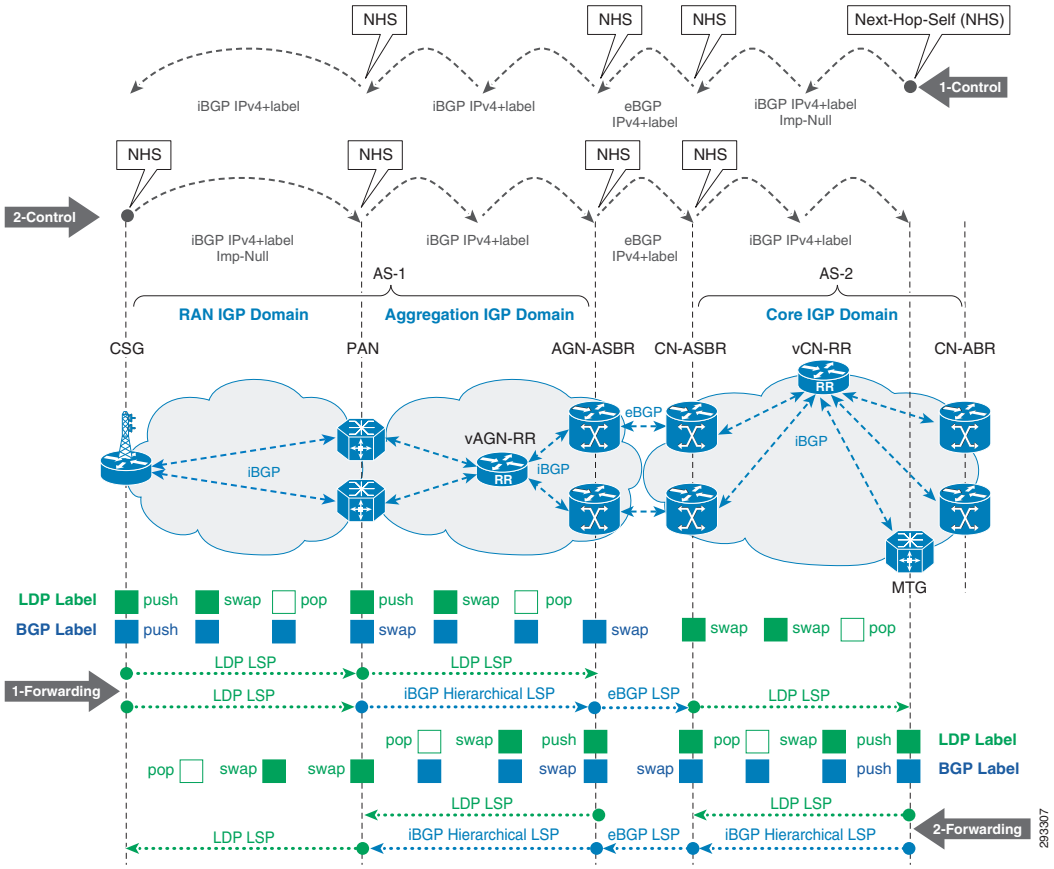
The inter-domain hierarchical LSP described here applies to the Large Network Transport Architecture Design with a Multi-AS Design and Labeled BGP IP/MPLS Access scenario.

The LSP is set up 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).

This scenario is also applicable to point-to-point VPWS services between CSGs and/or FANs in different labeled BGP access areas. In this scenario, the /32 loopback address of the remote AN is added to the inbound prefix filter list at the time of service configuration on the local AN.

Figure 3-19 Hierarchical LSPs between CSGs and MTGs for Inter-AS Design with Labeled BGP Access



The CSG in the RAN access learns the loopback 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 3-19, 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 AGNs 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 3-19, the following sequence occurs:

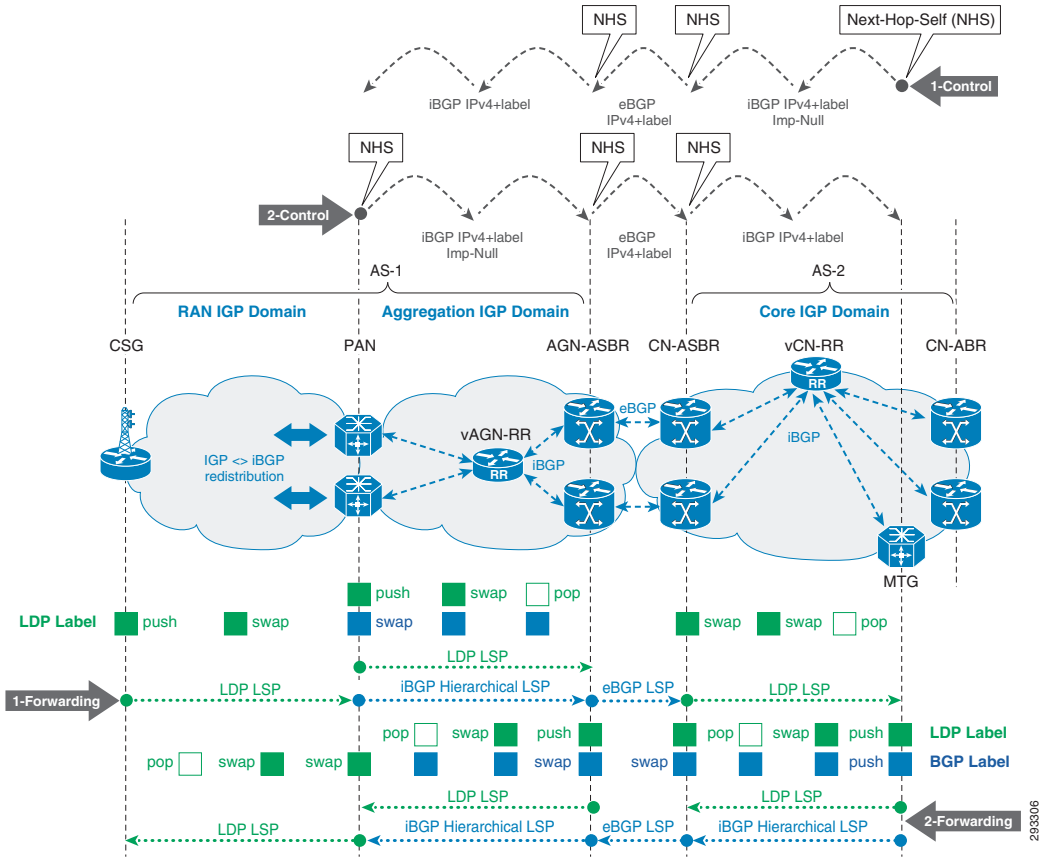
1. The downstream MTG node will first push the iBGP label corresponding to the remote prefix and then push the LDP label that is used to reach the CN-ASBR that is the labeled BGP next hop.
2. The core nodes that transit the inter-domain LSP will swap the intra-domain LDP-based LSP label, performing a 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 AGNs 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 with Label BGP Redistribution in IGP/LDP Access

The inter-domain hierarchical LSP described here applies to the Large Network Transport Architecture Design based on Multi-AS and IP/MPLS Access with Labeled BGP Redistribution scenario.

The LSP is set up 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/v6 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 3-20 Hierarchical LSPs between CSGs and MTGs for Inter-AS Design with IGP/LDP Access



The CSG in the RAN access learns the loopback 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 3-20, 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 AGNs 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 3-20, 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 AGNs 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.

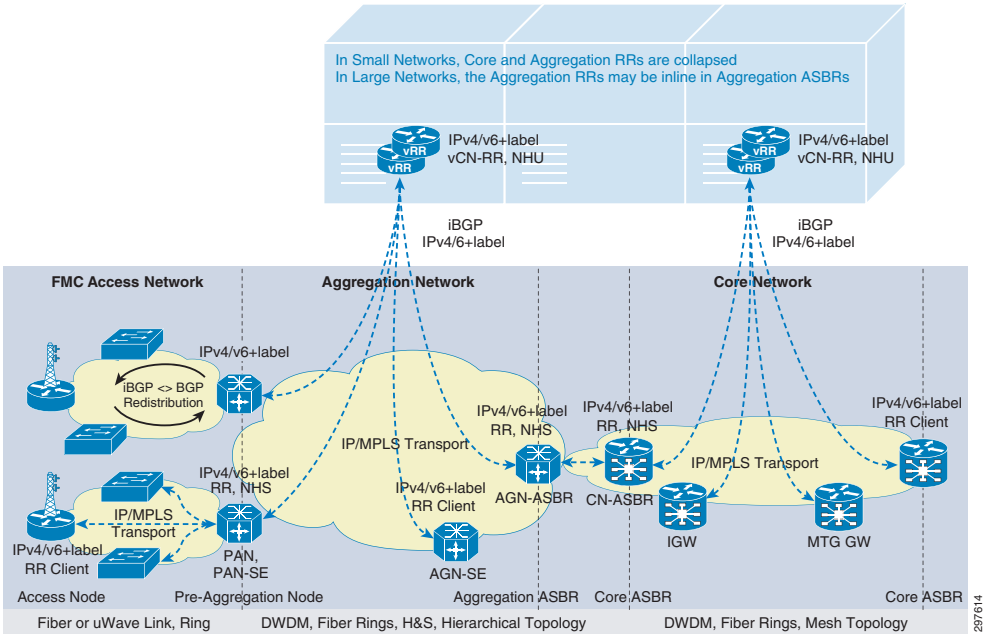
BGP Transport Control Plane

The Cisco EPN System proposes a hierarchical RR design for setting up the Unified MPLS Transport 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 EPN 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.

In each AS, nodes in the aggregation and core domains are RRs clients to their respective local aggregation network and core network RR functions (AGN-RR and CN-RR) that are virtualized in the Data Center (vAGN-RR and vCN-RR). See Figure 3-21.

Figure 3-21 BGP Control Plane for Large Network Design based on Inter-AS Design and IP/MPLS Access



All nodes in the core and aggregation network that require inter-domain LSPs act as labeled BGP PEs and run iBGP-labeled unicast peering with designated RRs depending on their location in the network.

- The core POP nodes are labeled BGP ASBR, and are referred to as CN-ASBRs. They peer with iBGP- labeled unicast sessions with the vCN-RR within the core AS, and peer with eBGP-labeled unicast sessions with the neighboring aggregation AGN-ASBRs. The CN-ASBRs insert themselves into the data path in order to enable inter-domain LSPs by setting NHS on all iBGP updates towards the vCN-RRs and eBGP updates towards the neighboring aggregation ASBRs. The vCN-RR applies an egress filter towards the CN-ASBRs in order to drop prefixes with the common RAN community, which eliminates unnecessary prefixes from being distributed.
- Gateway routers, such as MTGs providing connectivity to the MPC or IGWs providing access to the Internet, are labeled BGP PEs in the core. iBGP labeled-unicast sessions are established with the vCN-RR and loopbacks are advertised into iBGP labeled-unicast with a common BGP community representing the respective function: MSE BGP community for MTGs, IGW BGP community for IGWs. MTGs and IGWs learn BGP prefixes marked with the MSE and common RAN community, and with the FSE and IGW community, respectively.
- The aggregation POP nodes act as labeled BGP ASBRs in the aggregation AS, and are referred to as AGN-ASBRs. They peer with iBGP-labeled unicast sessions with the virtualized vAGN-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 corresponding vAGN-RRs and eBGP updates towards neighboring CN-ASBRs.
- PANs are labeled BGP ABRs between the aggregation and access domains. They utilize iBGP labeled-unicast sessions to peer with the vAN-RR in the local aggregation network, and act as inline-RRs for their local access network CSG/FAN clients. PANs also act as labeled BGP PEs and advertise loopbacks into BGP-labeled unicast with a common BGP community that represents the service communities being serviced by the PAN: RAN for mobile, FAN for fixed business wireline. PANs learn labeled BGP prefixes marked with the MSE and/or IGW BGP communities if services are connected locally. The PANs are inserted into the data path to enable inter-domain LSPs by setting NHS on all iBGP updates towards the AN-RRs and the local access clients.

Note In the case of IP/MPLS Access with Label BGP redistribution in Access IGP, which applies only to mobile transport services, the PANs only import/export mobile related BGP communities (RAN and MSE).

- FSE gateways, such as AGN-SEs and PAN-SEs, are labeled BGP PEs residing in the aggregation network. iBGP labeled-unicast sessions are established with the CN-ABRs, and advertise loopbacks into iBGP-labeled unicast with a common BGP FSE community. FSEs learn labeled BGP prefixes marked with the global FSE and IGW communities. The SE node functionality can reside within the PAN node described previously; there is no technical requirement for separate SE nodes.

In addition, for an IP/MPLS-enabled access domain:

- In the case of Labeled BGP Access, the access nodes, CSGs and FANs, in the access networks are labeled BGP PEs. iBGP-labeled unicast sessions are established with the local PAN inline-RRs.
  - CSGs advertise their loopbacks into BGP-labeled unicast with a common BGP community that represents the global RAN access community. To minimize the number of routes a CSG needs to learn to achieve the required inter-access X2 communication, CSGs also advertise their loopbacks with a pair of BGP communities designed according to the scaling capacity of the CSGs. Low and high- scale CSG nodes export their loopbacks with both the aggregation-wide RAN community and the access-wide local RAN community. The high- scale CSGs import the aggregation-wide RAN community only, the low- scale CSGs still import the access-wide local and neighbor RAN communities. Labeled BGP prefixes marked with the MSE BGP community

are learned for reachability to the MPC, and the aggregation-wide community or the access-wide adjacent RAN access BGP communities are learned if inter-access X2 connectivity is desired.

Note Aggregation-wide RAN community is the common RAN community for an aggregation domain and access-wide RAN community is the community for a specific access domain.

  - FANs advertise their loopbacks into BGP-labeled unicast with a common BGP com-munity representing the FAN access community. Labeled BGP prefixes marked with the FSE BGP community are learned for reachability to the AGN-SE or PAN-SE, while prefixes marked with the FAN BGP community provide reachability to remote FANs.

- In the case of Labeled BGP Redistribution into Access IGP, which is only supported for mobile services, 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 the iBGP and RAN IGP level/ area. In one direction, the RAN AN 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 MSE-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 and IGWs in the core network are capable of handling large network scale requirements, and will learn all BGP-labeled unicast prefixes because they need connectivity to all the CSGs and fixed SE nodes (and possibly ANs) in the entire network.

For mobile services, simple prefix filtering based on BGP communities is performed on the vCN-RRs in order to constrain IPv4+label routes from remote access regions from proliferating into neighboring aggregation domains, where they are not needed. The PANs learn only labeled BGP prefixes marked with the common RAN and the MSE BGP community, allowing the PANs to enable inter- metro wireline services across the core, and reflect the MSE prefixes to their local access networks. Isolating the aggregation and access domain by preventing the default redistribution enables the mobile access network to have limited route scale since the CSGs learn only local IGP routes and labeled BGP prefixes marked with the MSE BGP community.

For fixed wireline services, nodes providing fixed service edge functionality are also capable of handling a high degree of scalability, and will learn the common FAN community for AN access, the FSE community for service transport to other FSE nodes, and the IGW community for internet access. Again, using a separate IGP process for the access enables the access network to have limited control plane scale, since the ANs only learn local IGP routes and labeled BGP prefixes marked with the FSE BGP community or permitted via a dynamically-updated IP prefix list.

Access Network Design

This chapter includes the following major topics:

Microwave ACM

Nearly half of all mobile backhaul access networks worldwide utilize microwave links, which requires including microwave technology in the Cisco EPN System architecture. The Cisco EPN System integrates microwave radios in the access network in order to validate transport of traffic over microwave links, including such aspects as QoS; resiliency; operations, administration, and maintenance (OAM); and performance management (PM). System efforts have validated microwave equipment from multiple vendors, including NEC, SIAE, NSN, DragonWave, and Ceragon.

The typical deployment within the Cisco EPN architecture is to use the microwave gear to provide wireless links between MPLS-enabled or G.8032- enabled access nodes, such as CSGs. The interconnection between the CSG and the microwave equipment is a GigE connection. As most microwave equipment used in this context supports sub-gigabit transmission rates, typically 400 Mbps under normal conditions, certain accommodations are made. Namely, H-QoS policies implemented in the egress direction on either side of the microwave link should be adjusted to limit the flow of traffic to the bandwidth supported across the link, while still assuring the relative priorities across EF and AF classes of traffic. Also, the data path could be recalculated accordingly. For Layer 3 microwave links, the IGP metrics can be adjusted to account for the microwave links in a hybrid fiber-microwave deployment, allowing the IGP to properly understand the weights between true gigabit links, and gigabit ports connected to sub-gigabit microwave links. For Layer 2 microwave links in G.8032- enabled ring topologies, when the bandwidth of a microwave link degrades below threshold value, protection switching can be triggered for the associated G.8032 instance to ensure optimum bandwidth to the network traffic.

Adaptive Code Modulation (ACM)

If the bandwidth provided by a microwave link was constant, then IGP weights and H-QoS shaper rates could be set once and perform correctly. However, the bandwidth supported at a given time by a microwave link depends upon environmental factors. To enable the microwave link to support the optimal amount of bandwidth for the current environmental conditions, the equipment supports Adaptive Code Modulation (ACM) functionality, which automatically changes the modulation being utilized to provide the optimal amount of bandwidth for the given environment.

Regardless of the ACM status of the microwave link, the GigE connection to the access node is constant, so those nodes are unaware of any changes to the bandwidth on the microwave link. To ensure that optimal routing and traffic transport is maintained through the access network, a mechanism is needed to notify the access nodes of any ACM events on the microwave links. Cisco and a number of microwave vendors, such as NSN, SIAE and DragonWave, have implemented a vendor-specific message (VSM) in Y.1731 to allow for the microwave equipment to notify Cisco routers of ACM events, and the bandwidth available with the current modulation on the microwave link. Cisco EPN 4.0 has implemented four actions to be taken on the access nodes, which can be enacted depending upon the bandwidth available on the microwave link and the access technology used, MPLS or G.8032-enabled ring:

- **Adjustment of the H-QoS policy to match the current bandwidth on the microwave link**.
- **MPLS Access**—Adjustment of the IGP metric on the microwave link, triggering an IGP recalculation for MPLS Access.
- **MPLS Access**—Removal of link from the IGP.
- **G.8032 Ring**—Perform protection switching for the associated G.8032 instance.

H-QoS Policy Adjustment

The first action to be taken on an ACM event notification is to adjust the parameters of the egress H-QoS policy on the AN connected to the microwave link. The AN will modify the parent shaper rate to match the current bandwidth rate of the microwave link and adjust child class parameters to ensure that the proper amount of priority and bandwidth-guaranteed traffic is maintained. The goal is that all loss of bandwidth is absorbed by best-effort (BE) class traffic.

If the bandwidth available is less than the total bandwidth required by the total of EF+AF classes, then the operator can choose to have AF class traffic experience loss in addition to BE traffic, or to have the link removed from service.

IGP Metric Adjustment

In addition to H-QoS adjustments, the MPLS AN will adjust the IGP metric on the microwave link to correlate with the current bandwidth available. This will trigger an IGP SPF recalculation, allowing the IGP to take the correct bandwidth into account for routing of traffic in the access network.

Link Removal

At a certain threshold of degradation, determined by the operator, which will impact all service classes across the microwave link, the MPLS AN will remove the microwave link from the IGP. This will instigate the resiliency mechanisms in the access network resiliency to bypass the degraded link, resulting in minimal traffic loss. The link is not brought administratively down so that the microwave equipment can signal to the AN once the microwave link is restored.

Protection Switching

At a certain threshold of degradation, which is determined by the operator and which will affect all service classes across the microwave link, the AN in a G.8032-enabled ring topology will trigger protection switching for the associated G.8032 instance such that the RPL link transitions to the unblocking state and the microwave link are moved to the blocking state. This ensures the optimal usage of bandwidth to network traffic. The link is not brought down administratively so that the microwave equipment can signal to the AN once the microwave link is restored.

Ethernet Access Network

This section described the different designs implemented by the EPN System in the case of an Ethernet-based access network.

Hub-and-Spoke Access Network

Hub-and-spoke topologies are the simplest way of connecting devices, or spokes, to a common aggregation node or spoke.

They can be single or dual homed, with the latter entailing each spoke node to be connected to a pair of hub devices.

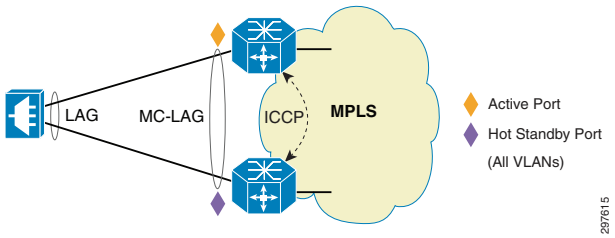
The Cisco EPN System supports the following Dual Homed hub-and-spoke topologies:

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

Per Node Active/Standby Multichassis Link Aggregation Groups

Multichassis Link Aggregation Groups (MC-LAG), or Multichassis LACP (mLACP), provides a flexible redundancy mechanism emulating a single homing environment to a dual-homed access device in hub-and-spoke topologies. The access node is connected to the network via a single Ethernet bundle interface with member links terminating into two different service edge devices. These edge nodes synchronize bundle-related protocol states via Inter-Chassis Control Protocol (ICCP) in order to appear as a single entity to the access node. The ICCP protocol runs over MPLS. MLACP mandates that all the bundle member links toward a specific SE node run in either active or standby mode. See Figure 4-1.

Figure 4-1 Multi Chassis Link Aggregation



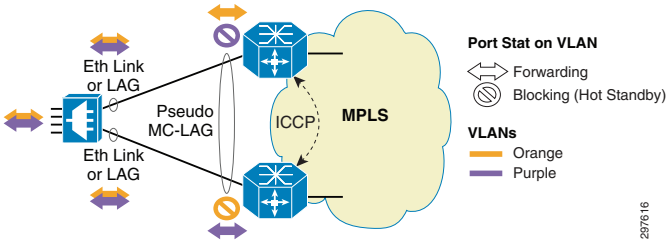
Per VLAN Active/Active Multichassis Link Aggregation Groups (Pseudo MC-LAG)

Pseudo MC-LAG enhances standard MC-LAG by load-balancing traffic across SE nodes maintaining all inter-chassis links active at the same time on a per VLAN basis. See Figure 4-2.

The access node is connected to each service edge device via standalone Ethernet links or Bundle interfaces that are part of the same bridge domain(s). All the links terminate in a common multi-chassis bundle interface at the SE nodes and are placed in active or hot-standby state based on node and VLAN.

ICCP is used again for the correlation required between the SE nodes.

Figure 4-2 Pseudo Multichassis Link Aggregation

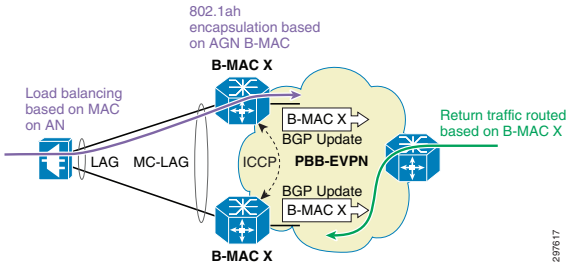


Per Flow Active/Active Multichassis Link Aggregation Groups

Per Flow Active/Active MC-LAG further enhances load-balancing of traffic across SE nodes by maintaining all inter-chassis links active at the same time and forwarding traffic based on MAC addresses. It allows the access node to bundle and operate the NNI ports as if connected to a single aggregation node, and to load balance traffic over all available links. See Figure 4-3.

Working in conjunction with PBB-EVPNs, the aggregation nodes share a common "anycast" Bridge-MAC address (used to further encapsulate traffic forwarded into the PBB-EVPN cloud) to ensure that return traffic is forwarded toward only one AGN. Indeed, return traffic is "routed" at the remote edge of the PBB-EVPN domain based on that B-MAC, which is advertised by both AGNs via BGP.

Figure 4-3 Per Flow Active/Active Multichassis Link Aggregation



G.8032-enabled Ethernet Access Rings

Service providers have connected their equipment in ring topologies for many years. Ring topologies allow for ubiquitous connectivity among networks nodes while achieving the highest degree of sharing of physical resources such as the links that interconnect the various nodes.

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

With the move to next generation networks and the wide adoption of Ethernet as the latest interconnection technology for the delivery of cost effective network infrastructure, service providers are looking into new ring fault detection mechanisms that are once again standardized, predictable and fast. Under those premises, the Cisco EPN System has selected the Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology.

The G.8032 protocol has been developed as a standard alternative to slow converging spanning tree protocol (STP) to achieve faster (~50ms) protection switching in ring topologies without any extensive information exchange, overprovisioning or complex computation. Loop avoidance is achieved by guaranteeing that at any time, traffic within the ring will flow on all but one of the ring links. This link is defined as the Ring Protection Link (RPL). Under normal ring condition, this link is blocked to data traffic. The RPL owner node (a designated node on the Ethernet ring) is responsible to block traffic on the "RPL" link.

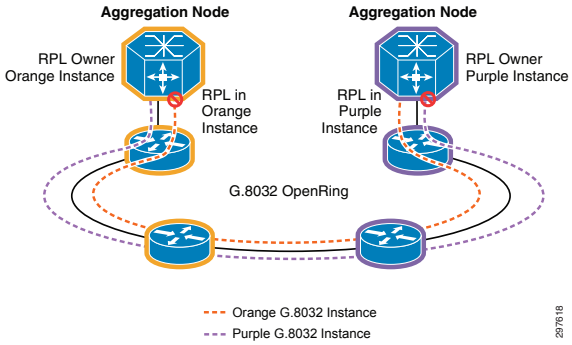
The G.8032 protocol allows to super-impose multiple logical rings over the same physical topology by using different instances. Each instance contains an inclusion list of VLAN IDs and may define different RPL links.

Load sharing between SE nodes is achieved by implementing two G.8032 instances for different S-VLAN ranges. In each instance, RPL link and RPL owner are on different SE nodes.

In each instance, a dedicated VLAN is used to implement the Automatic Protection Switching channel, which carries OAM traffic responsible for the protection of the ring.

As shown in Figure 4-4, the Cisco EPN System implements an Open Ring, with the aggregation nodes, at the ring edges, acting as the RPL owners for two different G.8032 instances, blocking the access ring-facing port in their respective instance.

Figure 4-4 G.8032-enabled Ethernet Access Ring



Network Virtualization (nV) Satellite Access Network

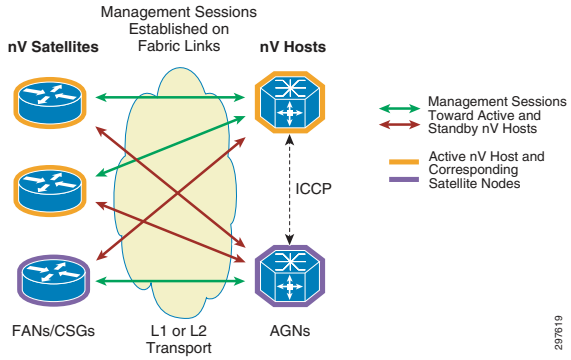
The Cisco EPN System supports network virtualization (nV) satellite solution in the access network. nV Satellite enables a system-wide solution in which one or more remotely located devices or "satellites" complements a pair of host nodes to collectively realize a single virtual switching entity in which the satellites act under management and control of the host nodes. Satellites and Hosts communicate using a Cisco proprietary protocol that offers discovery and remote management functions, thus turning the satellites from standalone nodes into distributed logical line cards of the host.

The technology therefore allows operators to virtualize hundreds of access nodes, converting them into nV Satellite devices, and to manage them through SE nodes that operate as nV hosts. By doing so, the access nodes transform from standalone devices with separate management and control planes, into low profile devices that simply move user traffic from a local UNI port toward a virtual counterpart at the host, where all network control plane protocols and advanced features are applied. The satellite only provides simple functions such as local connectivity and limited (and optional) local intelligence that includes ingress quality of service (QoS), operation, administration, and maintenance (OAM), performance measurements, timing synchronization, and replicating egress multicast traffic. Replication of egress multicast traffic can be offloaded from the nV host to the satellite to optimize bandwidth utilization of the Fabric Links. nV hosts and Satellites communicate multicast information using Cisco proprietary protocol.

Note nV multicast offload is supported on simple ring topology.

Figure 4-5 illustrates a sample satellite switching system formed by a combination of two host nodes and three satellite devices.

Figure 4-5 nV Satellite Technology



The satellites and the hosts exchange data and control traffic over point-to-point virtual connections known as Fabric Links. Customer Ethernet traffic carried over the fabric links is specially encapsulated using 802.1ah. A per-Satellite-Access-Port-derived ISID value is used to map a given satellite node physical port to its virtual counterpart at the host for traffic flowing in the upstream and downstream direction.

The satellite architecture encompasses multiple connectivity models between the host and the satellite nodes. The current release of the Cisco EPN System includes support for:

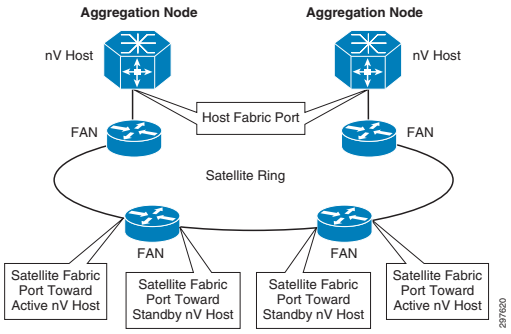
- nV Satellite Simple Rings
- nV Satellite L2 Fabric

In all topologies, host nodes load share traffic on a per-satellite basis. The active/standby role of a host node for a specific satellite is determined by a locally-defined priority and negotiated between the hosts via ICCP.

nV Satellite Simple Rings

In this model, satellite access nodes, such as FANs, are connected in an open ring topology terminating at the AGN-SE host nodes as shown in Figure 4-6.

Figure 4-6 nV Satellite Simple Rings



The aggregation node advertises multicast discovery messages periodically over a dedicated VLAN (VLAN 1).

Each satellite FAN node in the ring listens for discovery messages on all its ports and dynamically detects the Fabric link port toward the host.

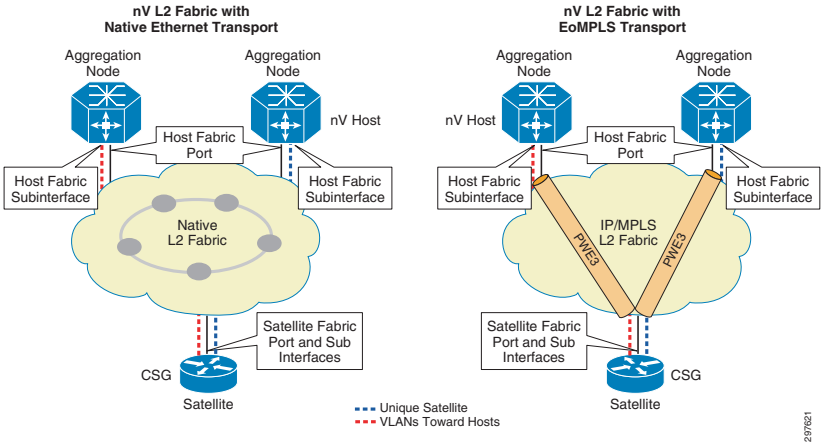
The satellite uses this auto-discovered port for the establishment of a management session and for the exchange of all the upstream and the downstream traffic with each of the hosts (data and control). At the host, incoming and outgoing traffic is associated to the corresponding satellite node using the satellite mac address, which was also dynamically learned during the discovery process.

Discovery messages are propagated from one satellite node to another and from either side of the ring so that all nodes can establish a management session with both hosts.

nV Satellite Layer 2 Fabric

In this model, satellite nodes, such as CSGs, are connected to the host(s) over any L2 Ethernet network. Such network can be implemented as a native or as an overlay Ethernet transport to fit all operator's access network designs. See Figure 4-7.

Figure 4-7 nV Satellite Layer 2 Fabric



In the case of L2 Fabric, a unique VLAN is allocated for the point-to-point emulated connection between the Host and each Satellite CSG device. The host uses such VLAN for the advertisement of multicast discovery messages.

Satellite CSG nodes listen for discovery messages on all the ports and dynamically create a subinterface based on the port and VLAN pair on which the discovery messages were received. VLAN configuration at the satellite is not required.

The satellite uses this auto-discovered sub-interface for the establishment of a management session and for the exchange of all upstream and downstream traffic with each of the hosts (data and control). At the host, incoming and outgoing traffic is associated to the corresponding satellite node based on VLAN assignment.

Autonomic Networking

Autonomic networking makes devices more intelligent and simplifies network operational aspects for the service provider's operational staff by automating various aspects of device initialization, provisioning, and Day 2 operations.

The aim of autonomic networking is to create self-managing networks to overcome the rapidly growing complexity of the Internet and other networks and to enable their further growth. In a self-managing autonomic system, user intervention takes on a new role: instead of controlling the system directly, the user defines policies and rules that guide the self-management process.

The current release of the Cisco EPN System implements four autonomic networking functions:

- Secure registration of access devices
- Autonomic control plane establishment
- Automated access node configuration
- Dynamic interface address assignment via Auto-IP

Secure autonomic network domain registration is accomplished by designating a router as a Registrar. The Registrar contains a database of Universal Device Identifiers (UDI) for devices that are permitted to join the network. The secure registration involves downloading of a digital certificate on every AN node, which is admitted in the AN domain, this certificate is issued by the Certificate Authority (CA) server present in the Registrar. Any device that attempts to join the autonomic networking domain with a UDI that is not listed in this database will be quarantined.

The Registrar must be reachable by all devices within the autonomic networking domain. This is accomplished by either:

- Co-locating the Registrar function on a node within the Autonomic Networking domain, OR
- Introducing a proxy device that offers a tunneling function to a centralized Registrar across a non-autonomic capable network.

While earlier releases of the EPN System focused on distributed Registrar functions, the current release takes the centralized approach. In this model, each Autonomic Networking domain connects to the Registrar via redundant GRE tunnels initiated by the interdomain PAN nodes acting as AN Proxies.

The autonomic control plane provides a virtual out-of-band (OOB) management channel to allow reachability from the network operations center to the new device for initial configuration and provisioning. This eliminates the need for field technicians to have any knowledge of device configuration when bringing up new nodes in the Cisco EPN network. The autonomic control plane is a segment-based system of IPv6 tunnels between autonomic networking devices. Once the first device is successfully registered with the Registrar, this management channel segment is established between the two nodes. This management channel is then extended to subsequent devices by proxying through nodes that have already joined the autonomic domain.

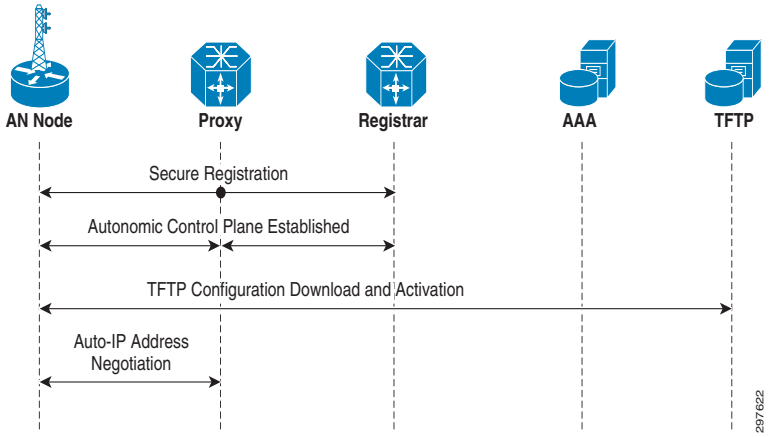
Once the new AN node is registered in the autonomic networking domain and the autonomic control plane is established, the new AN node initiates a TFTP configuration download for full and final node provisioning from a centralized location. The requested configuration file name follows the udi.conf format, where “udi” is AN node's unique device identifier. The AN node autodiscovers the TFTP server through the service-discovery process enabled by the Registrar. This eliminates the need for field technicians to have any knowledge of device configuration when bringing up new nodes in the network.

The Registrar is capable of learning and advertising the capabilities of a directly- connected server farm to the AN domain via multicast DNS. Supported services include AAA, SysLog, and TFTP.

Lastly, once the AN node is fully configured, the Auto-IP feature (if enabled on the node) initiates interface IP auto-provisioning. The Auto-IP function is based on vendor extension of LLDP protocol to provide an automatic method to provision link addresses for nodes inserted in a ring. When used in conjunction with Autonomic Networking, it provides real Zero Touch provisioning for nodes inserted in any position in a ring.

Figure 4-8 shows the high level insertion of a new node into the Autonomic Networking Domain adjacent to the Proxy.

Figure 4-8 Autonomic Networking Zero Touch AN Node Bring Up



CHAPTER 5

Functional Components Design

Up to this point in the design and implementation guide, we have addressed the base transport design, control plane, data plane, and service model aspects of the Cisco EPN System architecture. This chapter, which looks at additional aspects required for delivering and operating a comprehensive EPN System architecture, includes the following major topics:

Quality of Service

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

The Cisco EPN System applies the DiffServ Architecture defined by the IETF in RFC 2475 across all network layers, utilizing classification mechanisms like MPLS Experimental (EXP) bits, IP DSCP, IEEE 802.1p, and ATM CoS for implementing the DiffServ PHBs in use. 0 and 0 depict the QoS models implemented for the upstream and downstream directions.

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

H-QoS policies are required whenever the relative priorities across the different classes of traffic are significant only within the level of service offered to a given subscriber, and/or within a given service category, such as consumer, enterprise or mobile.

In downstream direction, H-QoS for a given subscriber should be performed at the SE node whenever possible to guarantee the most optimal usage of link bandwidth throughout the access network.

For an Ethernet-based access NNI and consumer services, the SE node acting as BNG device is capable of applying QoS at the subscriber level, with per-subscriber queuing and scheduling, as well as at the aggregate level for all consumer subscribers sharing the same N:1 VLAN, or a range of 1:1 VLANs.

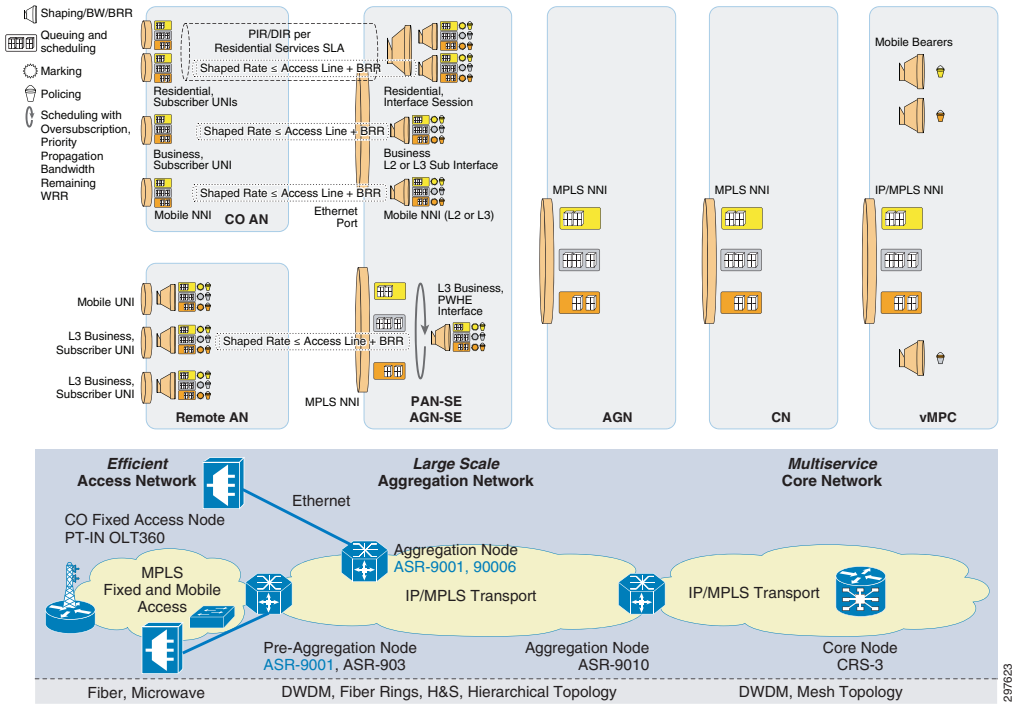
Aggregated QoS at the consumer service level is beneficial to manage oversubscription of the AN from residential traffic, as well as to control sharing of the access-facing NNI bandwidth with mobile and enterprise services. Similarly, enterprise services interfaces at the service edge implement H-QoS for the deployment of subscriber level SLAs as well as access bandwidth sharing.

Mobile services also require the implementation of H-QoS for access bandwidth sharing. Moreover, in the case of microwave links in the access, where the wireless portion of the link is only capable of sub-Gb speeds (typically 400 Mbps sustained) a parent shaper may be used to throttle transmission to the sustained microwave link speed.

Whenever subscriber SLAs are managed at the service edge and the access UNI is not multiplexed, a flat QoS policy can be applied to the AN in order to manage relative priority among the classes of traffic at each UNI port. Multiplexed UNI, typical of Enterprise services, require an H-QoS policy for relative prioritization among services first and then between classes of traffic within each service. In those scenarios, H-QoS on the SE nodes may drive peak information rate (PIR) level traffic, while the access UNI may force the committed information rate (CIR) levels.

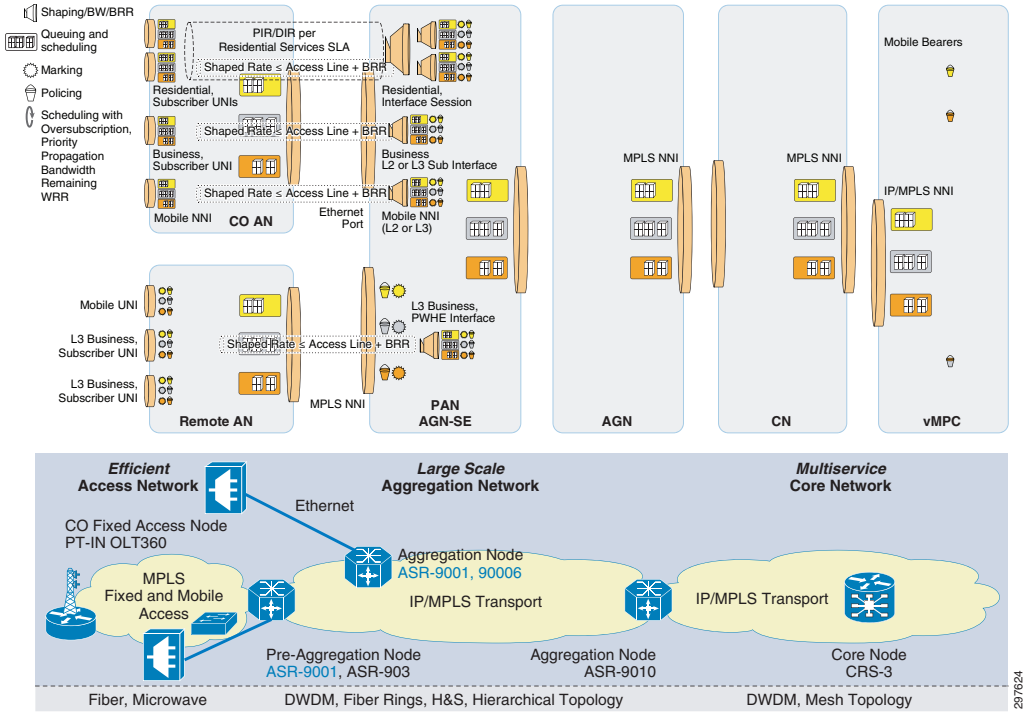
For an MPLS-based NNI, most services do not have a corresponding attachment point at the SE node and therefore the majority of the service level H-QoS logic happens at the AN. The exception are the L3VPN enterprise services for which the customer-edge to provider-edge (CE-PE) LSP is terminated over a PWHE interface at the SE node, which becomes the injection point for H-QoS. See Figure 5-1.

Figure 5-1 Downstream QoS Model



Upstream QoS mainly involves flat egress QoS policies applied to the various network node for relative prioritization among the different classes of traffic. Additionally, ingress QoS is required at the AN UNI and at the SE node access NNI to enforce per subscriber SLAs when an attachment point for the policy is available. At the SE nodes, ingress-coupled policers can be used to throttle the overall subscriber transmission rate to the committed speed, while providing some minimum bandwidth guarantee to the several traffic classes, up to the full subscriber transmission rate. See Figure 5-2.

Figure 5-2 Upstream QoS Model



Administrative boundaries are implemented at the access nodes for traffic received (upstream) from the subscribers and by the core nodes for traffic sent (downstream) to the subscribers in order to control traffic markings within the operator's network. Moreover, administrative boundaries may also exist across domains managed by different operators, thus possibly requiring further traffic remarking in order to correlate the PHBs between different administrative domains.

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 consumer, enterprise, and mobile and MEF transport services. Traffic across all three services is divided into three main categories:

- Expedited forwarding (EF)
- Assured forwarding (AF)
- Best effort (BE)

Figure 5-3 Differentiated Services QoS Domain

Traffic Class	PHB	Unified MPLS Transport		Service Edge			Fixed/Mobile Access Ethernet/TDM/ATM UNI		
		Core, Aggregation, Access		Business PWHE		Res/Bus Ethernet	M	R, B, M	M, B
		DSCP	EXP	DSCP	EXP	802.1P	DSCP	802.1P	ATM
Network Management	AF	56	7	56	7	7	56	(7)	VBR-nrt
Network Control Protocols	AF	48	6	48	6	6	48	(6)	VBR-nrt
Residential Voice Business Realtime Network Sync (1588 PTP) Mobility & Signaling traffic Mobile Conversation/Streaming	EF	46	5	46	5	5	46	5	CBR
Residential TV and Video Distribution	AF	32	4	32	4	4	NA	4	NA
Business Telepresence	AF	24	3	24	3	3	NA	3	NA
Business Critical In Contract Out of Contract	AF	16 8	2 1	16 8	2 1	2 1	16 8	2 1	VBR-nrt
Residential HSI Business Best Effort Mobile Background VQE Fast Channel Change, Repair	BE	0	0	0	0	0	0	0	UBR

293241

Traffic marked as EF is grouped in a single class serviced with priority treatment to satisfy stringent latency and delay variation requirements. The EF PHB defines a scheduling logic able to guarantee an upper limit to the per hop delay variation caused by packets from non-EF services.

This category includes residential voice and business real-time traffic, mobile Network Timing Synchronization (1588 PTP) and mobile signaling and conversation traffic (GSM Abis, UMTS IuB control plane and voice user plane, LTE S1c, X2c, and the LTE guaranteed bit rate (GBR) user plane).

Traffic marked as AF is divided over multiple classes. Each class is guaranteed a predefined amount of bandwidth, thus establishing relative priorities while maintaining fairness among classes and somewhat limiting the amount of latency traffic in each class may experience.

The Cisco EPN System defines five AF classes, two of which are reserved for network traffic, control and management, and the remaining three are dedicated to traffic from residential and business services, such as residential TV and video distribution, and business TelePresence and mission-critical applications.

The third category, best effort (BE), encompasses all traffic that can be transmitted only after all other classes have been served within their fair share. This traffic is neither time nor delay sensitive and includes residential H.323 Signaling Interface (HSI), business best effort, mobile background, and video quality experience control traffic.

For Ethernet UNI interfaces, upstream 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 DSCP and/or MPLS EXP value, depending on the access NNI being Ethernet or MPLS based. In the downstream direction, IP DSCP markings are preserved through the Unified MPLS Transport and may be used for queuing and scheduling at the UNI as well as for restoring 802.1P CoS values.

Specifically to mobile services, TDM UNI interfaces transported via CEoP pseudowires require all traffic to be classified as real-time with EF PHB. The ingress QoS service policy matches all traffic inbound to the interface, and applies an MPLS EXP value of 5. No egress service policy is required for TDM UNI interfaces. For ATM UNI interfaces to be transported via CEoP pseudowires or used for business services, traffic is classified according to the ATM CoS on a particular VC. The ingress QoS service policy is applied to the ATM permanent virtual circuit (PVC) subinterface and imposes an MPLS

EXP value that corresponds to the type of traffic carried on the VC and proper ATM CoS. For further distinction, the ingress QoS service policy may also has the ability to match on the cell loss priority (CLP) 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.

At the SE node, classification performed at the access-facing NNI will use a different set of marking depending on the technology used. For an Ethernet-based access NNI and upstream direction, 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 for transport toward the core. In the downstream direction, IP DSCP markings are preserved through the Unified MPLS Transport and may be used for queuing and scheduling as well as for restoring 802.1P CoS values before forwarding.

For an MPLS-based access NNI and in upstream direction, classification is based on IP DSCP or MPLS EXP markings. The ingress QoS service policy will match on these markings, which are retained when forwarding toward the core. In the downstream direction, IP DSCP or MPLS EXP markings preserved through the Unified MPLS Transport can be used for queuing and scheduling toward the access NNI.

All the remaining core, aggregation, and access network traffic classification is based on MPLS EXP or DSCP. The core network may use different traffic marking and simplified PHB behaviors, therefore requiring traffic remarking in between the aggregation and core networks.

Redundancy and High Availability

As highlighted in the EPN 4.0 System Concept Guide, the Cisco EPN System architecture implements high availability at the transport network level and the service level. By utilizing a combination of several technologies throughout the network, the EPN design is capable of meeting stringent availability service level agreements (SLAs), such as the Next-Generation Mobile Network (NGMN) requirements of 200ms recovery times for long term evolution (LTE) real-time services.

This section covers the implementation of high availability technologies for the transport level, with the exception of HA considerations for Ethernet access and network virtualization that are covered in the "Ethernet Access Network" section on page 4-3 and "Network Virtualization (nV) Satellite Access Network" section on page 4-6 of this guide.

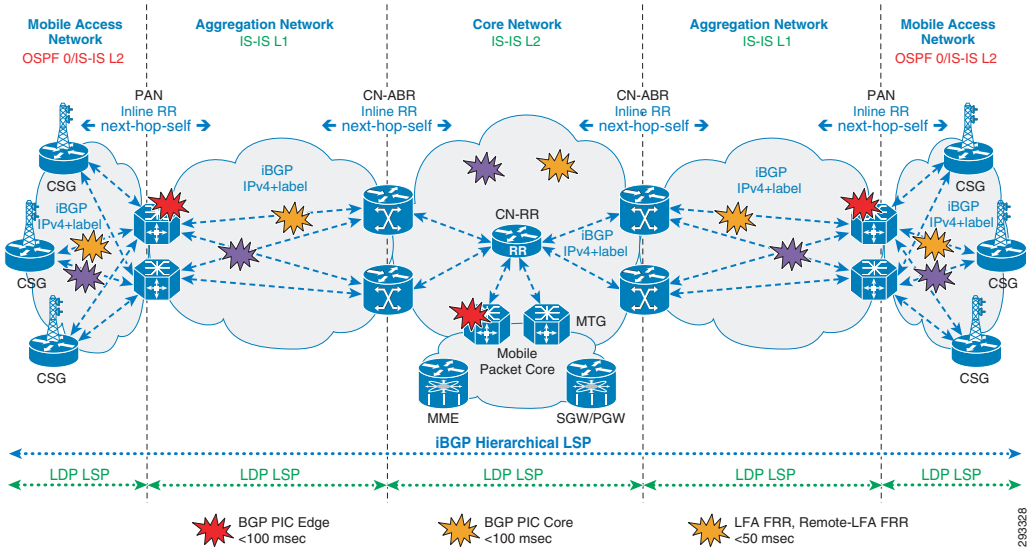
Service level resiliency implementations are covered in the respective service implementation guides. Finally, synchronization resiliency implementations are covered in the EPN 4.0 Mobile Transport Services Design and Implementation Guide.

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

- Loop-Free Alternate Fast Reroute (LFA FRR)
- BGP Core and Edge Fast Reroute and Edge Protection (BGP FRR)
- Bidirectional Forwarding Detection (BFD) at the IGP

Figure 5-4 illustrates the end-to-end Cisco EPN System architecture and where the resiliency mechanisms are utilized for various failures.

Figure 5-4 Cisco EPN High Availability Overview



In addition, the following mechanisms improve resiliency in dual homing scenarios for L2 Ethernet Access

- Multichassis Link Aggregation Groups (MC-LAG) and pseudo MC-LAG for multi-homed Ethernet access nodes in hub-and-spoke topologies. Refer to Hub-and-Spoke Access Network, page 4-3 more details.
- G.8032 Ethernet Ring Protection switching for Ethernet access nodes in ring topologies, with the SE nodes acting as RPL owners for different G.8032 instances. Refer to G.8032-enabled Ethernet Access Rings, page 4-5for more details.
- per nV-Satellite, election of primary and backup nV Host based on host-defined priorities, for nV access in both L1 and L2 Fabric topologies. Refer to nV Satellite Simple Rings, page 4-7for more details.

Loop-Free Alternate Fast Reroute with BFD

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

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

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

Microloop Avoidance in Remote LFA FRR

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

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

BGP Fast Reroute

BGP fast reroute (FRR) provides deterministic network reconvergence, even with the BGP prefix scale encountered in the Cisco EPN System design. BGP FRR 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 Label Forwarding Information Base (LFIB) structure to allow multiple paths to be installed for a single BGP next hop. BGP FRR consists of two different functions: core and edge. Each function handles different failure scenarios within the transport network:

- FRR core protection 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.
- Edge protection and FRR edge protection is used for redundant BGP next-hop nodes, as is the case with redundant ABRs. BGP additional-paths functionality is configured on the PE routers and RRs in order to install both ABR nodes' paths in the RIB and LFIB instead of just the best path. When the primary ABR fails, BGP forwarding simply switches to the path of the backup ABR instead of having to wait for BGP to reconverge at the time of the failure.

Multihop BFD for BGP

BFD Multihop (BFD-MH) is a BFD session between two addresses that are not on the same interface. An example of BFD-MH is a BFD session between routers that are several Time to Live (TTL) hops away. The first application that makes use of BFD-MH is BGP. BFD-MH supports BFD on arbitrary paths, which can span multiple network hops.

The BFD-MH feature provides sub-second forwarding failure detection for a destination more than one hop, and up to 255 hops, away.

BGP Accumulated IGP (AIGP)

The Cisco EPN System uses BGP to provide routing information across different independent IGP domains or ASs. By default, BGP selects best path based on its best path algorithm which only keeps into account the cost to reach the BGP next hop for a path. It does not consider the BGP next-hop's cost to reach the destination prefix. This may lead in selecting a path that has higher overall cost to reach a destination prefix as compared to other available paths, thus causing sub -optimal routing. This problem is addressed by BGP Accumulated IGP (AIGP).

BGP AIGP is an optional non-transitive attribute used to advertise accumulated IGP cost across independent IGP domains or ASs to reach a destination prefix. AIGP impacts BGP best path selection algorithm such that when a device receives multiple BGP paths to the same destination prefix having the AIGP attribute attached, for each path it adds the value of AIGP attribute to the next hop metric and selects the path with the lower value as preferred. The AIGP attribute preference rule applies after the BGP local-preference rule.

AIGP enables BGP to achieve optimal routing by considering overall cost to reach the destination and it is then implemented on all the devices configured with RFC 3107 BGP.

Note You can get more information about BGP AIGP Attribute in internet draft-ietf-idr-aigp-06.

Multicast

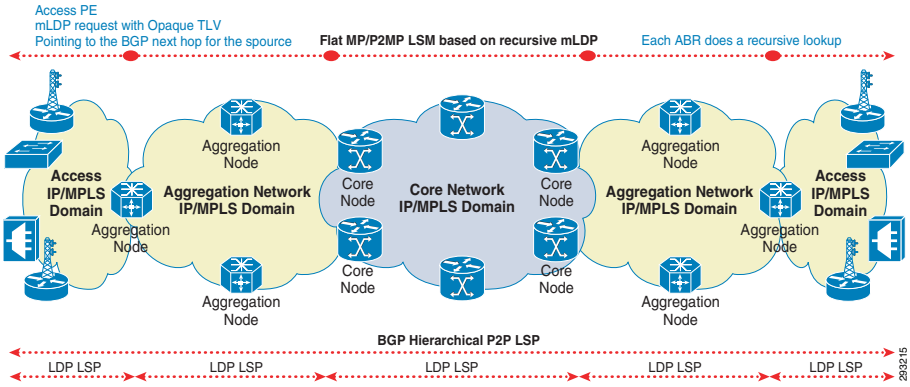
The Cisco EPN System supports services delivered via multicast transport as well as Unicast. Such services include consumer broadcast video, financial trading, and Evolved Multimedia Broadcast Multicast Service (eMBMS) for mobile. It is evident that an operator's network may carry multiple multicast services concurrently on a single infrastructure, which necessitates proper transport of the multicast services in the EPN System in order to provide the required separation between the disparate services.

In order to provide efficient transport of multicast-based services via MPLS, Multicast Label Distribution Protocol (MLDP) provides extensions to LDP, enabling the setup of Multiprotocol Label-Switched Paths (MP LSPs) without requiring multicast routing protocols such as Protocol Independent Multicast (PIM) in the MPLS core. Recursive MLDP, defined in RFC6512, allows end-to-end multicast LSPs to remain flat and to be built within each domain simply based on the local exit node that provides reachability to the source. Such node is advertised in an Opaque TLV added to the MLDP request.

The two types of MP LSPs that can be set up are point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) type LSPs. MLDP constructs the P2MP or MP2MP LSPs without interacting with or relying upon any other multicast tree construction protocol. The benefit of using MLDP is that it utilizes the MPLS infrastructure for transporting IP multicast packets, providing a common data plane (based on label switching) for both unicast and multicast traffic while maintaining service separation.

End-to-end deployment of multicast transport is illustrated in Figure 5-5.

Figure 5-5 Unified MPLS Multicast



Multicast Services in Global Routing

Operators have recently started expanding the use of multicast for the delivery of broadcast video services to the consumer, from the residential users to the mobile subscribers as well.

This section focuses on the mechanisms the Cisco EPN System utilizes to create a common multicast transport infrastructure for consumer video services over the global routing domain.

In the core and aggregation networks down to the SE node, LSM is utilized for transport of global multicast traffic, which in turn utilizes the mLDP-Global in-band signaling profile. In this profile, PIM is required only at the edge of the network domain, eliminating the requirement of deploying PIM in the core network. In the Cisco EPN System design, PIM Source Specific Multicast (PIM-SSM) is used to integrate the multicast transport with the access networks.

In the MPLS and Ethernet access networks and from the PAN to the AGN-SE node, if the service edge functionality is not in the PAN, native IP PIM with SSM is utilized for the transport of IPv4 and IPv6 multicast. This shift permits lower cost and lower power devices to be utilized in the access network by not requiring recursion processing for MPLS encapsulation of the multicast traffic. In this model, multicast IPv4 and IPv6 source addresses must be selectively redistributed at the PAN or AGN-SE for the proper creation of multicast delivery trees within the native IP multicast-enabled access network. For the transport of IPv4 multicast in the nV based access network, IGMP snooping is used on the nV host to learn active multicast receivers and to achieve the multicast offload functionality by propagating the acquired group membership information back to the satellite for local replication.

On the UNI from the AN (CSG or FAN) at the edge of the access network to the eNB/CPE, a dedicated VLANs is utilized for the delivery of multicast traffic.

When a multicast service is requested from a user endpoint device, the CPE/eNB will signal the transport network to start the requested service. The Cisco EPN System design supports both IGMPv2 and IGMPv3 signaling for IPv4 and MLDv2 for IPv6.

- For IGMPv2, the AN will statically map the IGMP requests to the proper PIM-SSM groups.
- For IGMPv3 and MLDv2, the AN supports dynamic IGMP/MLD to PIM-SSM mapping.

The SE node acts as a leaf node for the mLDP-Global domain. It will dynamically map the PIM requests from the CSG into mLDP in-band signaling in order to eliminate the need for PIM within the aggregation and core network domains.

For mobile multicast services, the MTG node uses PIM-SSM for the connection to the MBMS-GW and acts as a root node for the mLDP-Global domain. The MTG node dynamically maps the mLDP in-band signaling into PIM-SSM requests to the MBMS-GW.

For wireline services, similar functions are performed by the border or boundary router that provides gateway functions into the domain where the multicast source resides.

OAM and Performance Monitoring

Operations, administration, and maintenance (OAM) implementation for transport in the Cisco EPN System varies depending on the type of service being monitored. This is covered in the EPN 4.0 Enterprise Services Design and Implementation Guide, the EPN 4.0 MEF Transport Design and Implementation Guide, and the EPN 4.0 Mobile Transport Services Design and Implementation Guide for the EPN System architecture.

Transport Infrastructure Implementation

This chapter, which details the network implementation for the transport models introduced in Chapter 1, "Introduction," includes the following major topics:

In the EPN 4.0 transport infrastructure implementation, the various network components with their architectural role and functions are described in Table 6-1.

Table 6-1 EPN Transport Infrastructure Components

Network Role	Cisco Platform	Software Release	Functional Description
AN	ASR-920	XE 3.13	Access node for MEF, Enterprise, and Mobile Services Access: • Microwave • MPLS: – Unified MPLS IBGP Label Edge Router – IGP/LDP Label Edge Router – BFD, BGP PIC & rLFA FRR
	ASR-901	XE 3.13	Access node for MEF, Enterprise and Mobile Services Access: • Ethernet (Hub & Spoke and G.8032) • Microwave • MPLS: – Unified MPLS IBGP Label Edge Router – IGP/LDP Label Edge Router – BFD, BGP PIC & rLFA FRR Autonomic Network Access Node

Table 6-1 EPN Transport Infrastructure Components (continued)

Network Role	Cisco Platform	Software Release	Functional Description
	ME-3600	XE 3.13	Access node for MEF and Enterprise Services Controller for ME-1200 Access: • Ethernet (Hub & Spoke and G.8032) • MPLS: – Unified MPLS IBGP Label Edge Router – IGP/LDP Label Edge Router – BFD, BGP PIC & rLFA FRR
	ME-4600	OS 3.4	Access node for MEF, Enterprise and Residential Services GPON OLT Access: Ethernet (Hub & Spoke and G.8032)
	ASR-9000v	XR 5.2.2	Access node for MEF and Enterprise Services nV Satellite nV Access Simple Rings & L2 Fabric
	ME-1200	XE 3.13	Network interface Device for MEF, Enterprise and Mobile Services SyncE-based frequency distribution to base station Management - Cisco Prime Provisioning or ME-3600
PAN	ASR-903 (RSP1 and RSP2)	XE 3.13	Unified MPLS IBGP Label Switch Router IGP/LDP Label Edge Router BFD, BGP PIC & rLFA FRR Autonomic Registrar Autonomic Network Proxy Node
	ASR-9001	XR 5.2.2	Unified MPLS IBGP Label Switch/Edge Router IGP/LDP Label Edge Router Service Edge Function BFD, BGP PIC & rLFA FRR
AGN	ASR-900x	XR 5.2.2	Unified MPLS IBGP/EBGP Label Switch/Edge Router IGP/LDP Label Edge Router Service Edge Function BFD, BGP PIC & rLFA FRR nV Host
CN	CRS-3 ASR-900x	XR 5.1.1 XR 5.2.2	IGP/LDP Label Switch Router BFD & rLFA FRR
RR	Virtual RR	XR 5.2.2	Unified MPLS IBGP Route Reflector Service Route Reflector for Enterprise, MEF and Mobile Services BFD & BGP PIC

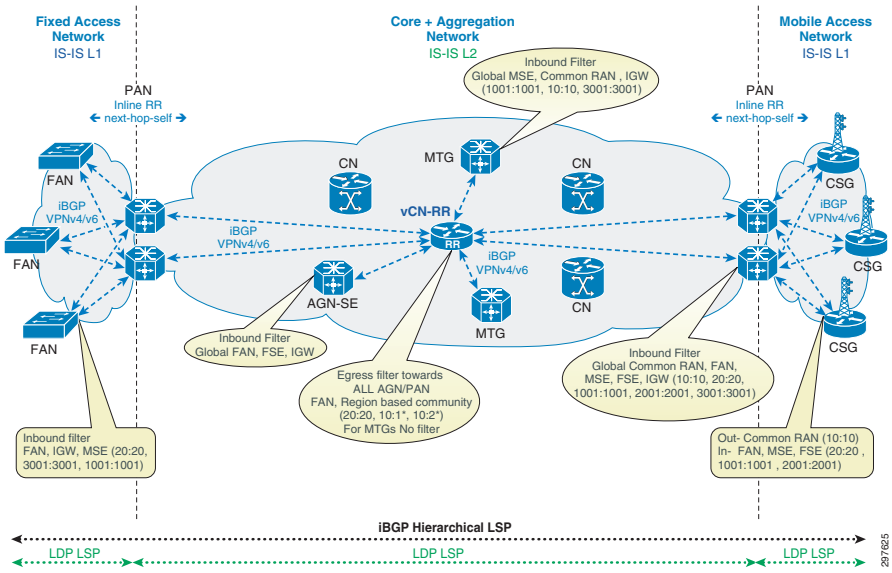
Small Network Transport Architecture Implementation

This section focuses on the network implementation for the transport models associated to a small network with either IP/MPLS or Non-IP/MPLS Access.

MPLS Access

In this model, the collapsed core+aggregation and access networks are integrated with labeled BGP LSPs. 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. See Figure 6-1.

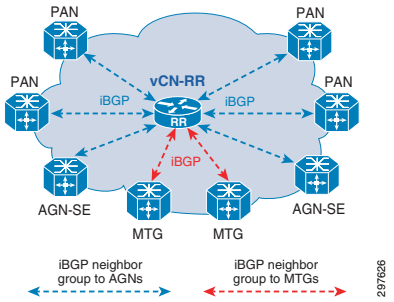
Figure 6-1 Unified MPLS Transport for Small Network, Integrated Core, and Aggregation with Labeled BGP Access



Core Route Reflector Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the centralized core node route reflector (vCN-RR). See Figure 6-2.

Figure 6-2 Centralized Core Node Route Reflector (vCN-RR)



In the Cisco EPN 4.0 System implementation, the Core-RR role is fulfilled by Cisco IOS XRv. IOS XRv enables an emulated classic 32-bit X86 IOS XR router within a virtual machine (VM) on a Cisco Unified Computing System (UCS) platform. Cisco IOS XRv was validated by using a standalone Cisco UCS-C200 series server. A future phase will validate IOS XRv inside a Cisco UCS-B series data center to provide a consolidated virtualized infrastructure.

Interface Configuration

```
interface Loopback0
  description Global Loopback
  ipv4 address 100.111.15.50 255.255.255.255
!
!***Core Interface***
interface GigabitEthernet0/0/0/0
  description To CN-K0201 Gig0/2/0/1
  cdp
  ipv4 address 10.2.1.33 255.255.255.254
  negotiation auto
  load-interval 30
!
```

IGP/LDP Configuration

For reference throughout this document, the following lists the parameters (and the corresponding definitions) used for the IGP configuration:

- **set-overload-bit on-startup**—This new functionality is useful to Internet service providers (ISPs) who run both BGP and IS-IS to avoid certain black hole scenarios in which traffic is temporarily lost. Setting the overload bit for a fixed amount of time right after a reload ensures that the router does not receive transit traffic while the routing protocol is still converging. Time in seconds (sec).
- **lsp-gen-interval**—The lsp-gen-interval command reduces the rate of link-state packet generation during periods of instability in the network. This command can help to reduce CPU load on the router and the number of link-state packet transmissions to its IS-IS neighbors. Time in milliseconds (ms).
- **lsp-refresh-interval**—This command sets the time between regeneration of link-state packets that contain different sequence numbers. Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small). Time in sec.
- **max-lsp-lifetime**—This command sets the maximum time that link-state packets persist without being refreshed. Must be higher than lsp-refresh-interval. Time in sec.
- **ispf**—The iSPF, or incremental SPF, algorithm may be used to reduce the processor load when IS-IS needs to recalculate its topology after minor changes.

- **spf-interval**—This command controls how often the software can perform the SPF calculation. Increasing the SPF interval reduces the processor load of the router, but also potentially slows the rate of convergence. Time in ms.

```
router isis core
 set-overload-bit on-startup 360
  net 49.0100.1001.1100.4003.00
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    address-family ipv4 unicast
    !
  !
  !***Core Interface***
  interface GigabitEthernet0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 100
    !
  !
mpls ldp
  router-id 100.111.15.50
  graceful-restart
  log
    neighbor
    graceful-restart
  !
  mldp
  !
  interface GigabitEthernet0/0/0/0
```

BGP Configuration

For reference throughout this document, the following lists the parameters (and the corresponding definitions) used for the BGP configuration:

- **Nsr**—This command enables the BGP Nonstop Routing (NSR) with Stateful Switchover (SSO). This enables all BGP peerings to maintain the BGP state in order to ensure continuous packet forwarding during events that could interrupt service.
- **bgp default local-preference**—The local preference attribute is a discretionary attribute that is used to apply the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.
- **Bgp graceful-restart**—This command enables graceful-restart for all BGP routers.
- **BGP graceful-restart restart-time**—This commands sets the maximum period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for this argument is 120 seconds. The configurable range of values is from 1 to 3600 seconds.

- **bgp graceful-restart stalepath-time**—This command sets the maximum period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for this argument is 360 seconds. The configurable range of values is from 1 to 3600 seconds.
- **Additional-paths**—This command enables BGP FRR edge functionality to install additional-paths to a destination.
- **Allocate-label all**—Use the allocate-label command with a route policy in order to trigger BGP to allocate labels for all or a filtered set of global routes (as dictated by the route policy). The command enables ASBRs that have labeled unicast sessions to exchange MPLS labels with the routes to the other autonomous system in L3VPN inter-AS deployments.
- **Nexthop trigger-delay critical**—Use the nexthop trigger-delay command to allow for a dynamic way for IGP to converge. This convergence allows BGP to accumulate all notifications and trigger fewer walks, resulting in fewer interprocess communications (IPCs) to the Routing Information Base (RIB) for route addition, deletion, modification, and fewer updates to peers. Time in ms.
- **Maximum-prefix**—Use the maximum-prefix command to configure a maximum number of prefixes that a BGP router is allowed to receive from a neighbor. It adds another mechanism (besides routing policy) to control prefixes received from a peer. The Warning-only command will not terminate peering, but simply generate a log message.
- **soft-reconfiguration inbound**—To filter or modify some of the updates received from a neighbor, you configure an inbound policy by using the route-policy (BGP) command. Configuring soft reconfiguration inbound causes the software to store the original unmodified route beside a route that is modified or filtered. This allows a soft clear to be performed after the inbound policy is changed. To perform a soft clear, use the clear BGP soft command with the in keyword specified. The unmodified routes are then passed through the new policy and installed in the BGP table without completely resetting the BGP session between routers.
- **bgp update-delay**—When BGP is started, it waits a specified period for its neighbors to establish peering sessions and to complete sending their initial updates. After all neighbors complete their initial updates, or after the update delay timer expires, the best path is calculated for each route, and the software starts sending advertisements out to its peers. This behavior improves convergence time. If the software were to advertise a route as soon as it learned it, it would have to re-advertise the route each time it learned a new path that was preferred over all previously learned paths.
- **Bgp redistribute-internal**—To allow the redistribution of iBGP routes into an IGP, such as IS-IS or OSPF, use the BGP redistribute-internal command in an appropriate configuration mode. To disable the redistribution of iBGP routes into IGPs, use the no form of this command.
- **ibgp policy out enforce-modifications**—Use the iBGP policy out enforce-modifications command to set and modify BGP route attributes for updates to iBGP peers.
- **advertise best-external**—To advertise the best-external path to the iBGP and route-reflector peers, when a locally selected best path is from an internal peer, use the advertise best-external command in an appropriate address family configuration mode.

```
router bgp 1000
  nsr
  bgp default local-preference 50
  bgp router-id 100.111.15.50
  bgp cluster-id 1000
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  address-family ipv4 unicast
  !***BGP add-path configuration for BGP Edge FRR***!
    additional-paths receive
    additional-paths send
```

```
  additional-paths selection route-policy add-path-to-ibgp
  nexthop trigger-delay critical 1000
  network 100.111.4.3/32
  allocate-label all
!
address-family vpnv4 unicast
!***session group for iBGP clients (AGNs and MTGs)***
session-group intra-as
  remote-as 1000
  password encrypted 082D4D4C
  update-source Loopback0
!
!***MTG neighbor group***
neighbor-group mtg
  use session-group intra-as
  address-family ipv4 labeled-unicast
    route-reflector-client
    maximum-prefix 150000 85 warning-only
    soft-reconfiguration inbound always
  !
  address-family vpnv4 unicast
  !
  address-family ipv6 labeled-unicast
    route-reflector-client
    maximum-prefix 150000 85 warning-only
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
    route-reflector-client
  !
!
!***AGN neighbor group***
neighbor-group agn
  use session-group intra-as
  address-family ipv4 labeled-unicast
    route-reflector-client
    soft-reconfiguration inbound always
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
    route-reflector-client
  !
  address-family ipv6 mvpn
    route-reflector-client
  !
!
!***PAN neighbor group***
neighbor-group pan
  use session-group intra-as
  address-family ipv4 labeled-unicast
    route-reflector-client
    soft-reconfiguration inbound always
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
!
!***MTG-K1501***
neighbor 100.111.15.1
```

```
    use neighbor-group mtg
  !
  !***MTG-K1502***
  neighbor 100.111.15.2
    use neighbor-group mtg
  !
  !***PANs***
  neighbor 100.111.5.7
    use neighbor-group pan
  !
  neighbor 100.111.5.8
    use neighbor-group pan
  !
  neighbor 100.111.9.21
    use neighbor-group pan
  !
  neighbor 100.111.9.22
    use neighbor-group pan
  !
  neighbor 100.111.14.3
    use neighbor-group pan
  !
  neighbor 100.111.14.4
   use neighbor-group pan
  !
  !***AGNs***
  neighbor 100.111.11.1
    use neighbor-group agn
  !
  neighbor 100.111.11.2
    use neighbor-group agn
  !
!
route-policy add-path-to-ibgp
  set path-selection backup 1 advertise install
end-policy
```

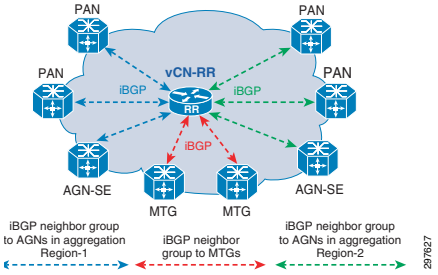
Note The AGNs learn the loopbacks of all CSGs in the network since the above configuration does not perform prefix filtering across RR clients. Since this is a small network scenario, the total number of CSGs is assumed small and easily accommodated by the LFIB of the AGNs. This setup also allows for inter-access region X2 interfaces. If inter-access region X2 handoff is not required, a simple egress filter can be applied on the AGN neighbor group as shown below.

```
!
router bgp 1000
    !***AGN neighbor group***
  neighbor-group agn
    use session-group infra
    address-family ipv4 labeled-unicast
      route-reflector-client
      !***Egress filter to drop unwanted loopbacks towards other AGNs***
      route-policy BGP_Egress_Transport_Filter out
    !
    address-family vpnv4 unicast
    !
route-policy BGP_Egress_Transport_Filter
  !***Passes FAN Loopbacks***
  if community matches-any (20:20) then
    pass
  else
    !***Drops common CSG community***
```

```
      if community matches-any (10:10) then
        drop
      else
        pass
      endif
    endif
  end-policy
```

The following configuration, depicted in Figure 6-3, can be used in cases where the number of CSGs deployed in the network is very large, and it is desirable to constrain the loopbacks from remote RAN access regions from being learned on other AGNs where they are not needed, but still allow inter-access region X2 interfaces within regions.

Figure 6-3 Centralized vCN-RR with Neighbor Groups Segmented per Region




```
!
router bgp 1000
  !***AGN region-1 neighbor group***
  neighbor-group agn-r1
    use session-group infra
    address-family ipv4 labeled-unicast
      route-reflector-client
      !***Egress filter to drop unwanted RAN loopbacks towards neighboring aggregation
regions.***
      route-policy R1-BGP_Egress_Transport_Filter out
    !
    address-family vpnv4 unicast
    !
  !
  !***AGN region-2 neighbor group***
  neighbor-group agn-r2
    use session-group infra
    address-family ipv4 labeled-unicast
      route-reflector-client
      !***Egress filter to drop unwanted RAN loopbacks towards neighboring aggregation
regions.***
      route-policy R2-BGP_Egress_Transport_Filter out
    !
    address-family vpnv4 unicast
    !
  !
  !***MTGs***
  neighbor 100.111.15.1
    use neighbor-group mtg
  !
  neighbor 100.111.15.2
    use neighbor-group mtg
  !
  !***PANs in AGN-R1***
  neighbor 100.111.5.7
    use neighbor-group agn-r1
  !
  neighbor 100.111.5.8
```

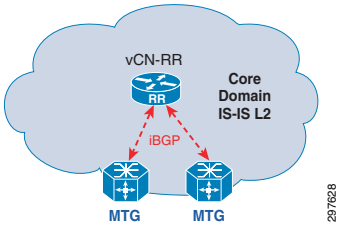
```
    use neighbor-group agn-r1
  !
  !***PANs in AGN-R2*** neighbor 100.111.14.3
    use neighbor-group agn-r2
  !
  neighbor 100.111.14.4
    use neighbor-group agn-r2
  !
!
route-policy R1-BGP_Egress_Transport_Filter
  !***Passes FAN Loopbacks***
  if community matches-any (20:20) then
    pass
  else
    !***Passes Communities in R1: 10:101, 10:102, etc.***
    if community matches-any (10:1*) then
      pass
      !***Drops common CSG community***
      if community matches-any (10:10) then
        drop
      else
        pass
      endif
    endif
  endif
end-policy

route-policy R2-BGP_Egress_Transport_Filter
  !***Passes FAN Loopbacks***
  if community matches-any (20:20) then
    pass
  else
    !***Passes Communities in R2: 10:201, 10:202, etc.***
    if community matches-any (10:2*) then
      pass
      !***Drops common CSG community***
      if community matches-any (10:10) then
        drop
      else
        pass
      endif
    endif
  endif
end-policy
```

Note Please refer to the **BGP Transport Control Plane, page 3-5** for a detailed explanation on how egress filtering is done at the CN-RR for constraining IPv4+label routes from remote RAN access regions.

Mobile Transport Gateway Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs from the MPC to the aggregation and access domains. The MTG node is a Cisco ASR-9006. See Figure 6-4.

Figure 6-4 Mobile Transport Gateway (MTG)



Interface Configuration

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

IGP Configuration

```
router isis core
  set-overload-bit on-startup 250
  net 49.0100.1001.1101.5001.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  interface TenGigE0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
```

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

BGP Configuration

```
router bgp 1000
  nsr
  bgp router-id 100.111.15.1
  bgp update-delay 360
  bgp redistribute-internal
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    !***BGP add-path to receive multiple paths from CN-RR***
    additional-paths receive
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 0
    !***Color loopback prefix in BGP with MSE and IGW Communities***
    network 100.111.15.1/32 route-policy MSE_IGW_Community
    allocate-label all
  !
  address-family vpnv4 unicast
  !
  address-family ipv6 unicast
    redistribute connected
```

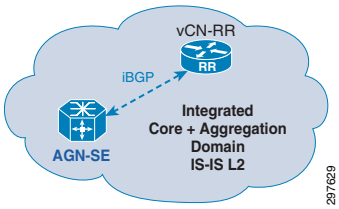
```
    allocate-label all
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  session-group intra-as
    remote-as 1000
    password encrypted 011F0706
    update-source Loopback0
  !
  neighbor-group cn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family ipv6 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
    !
  !
  !***CN-RR***
  neighbor 100.111.15.50
    use neighbor-group cn-rr
  !
community-set IGW_Community
  3001:3001
end-set
!
community-set MSE_Community
  1001:1001
end-set
!
route-policy MSE_IGW_Community
  set community MSE_Community
  set community IGW_Community additive
end-policy

!***Pass Common, MSE, and IGW communities***
community-set PASS_Community
  10:10,
  1001:1001,
  3001:3001
end-set
!
route-policy BGP_Ingress_Transport_Filter
  if community matches-any PASS_Community then
    pass
  else
    drop
  endif
end-policy
!
route-policy add-path-to-ibgp
  set path-selection backup 1 install
```

```
end-policy
```

Aggregation Service Edge Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs in the integrated core+aggregation network. The AGN-SEs are PEs in the aggregation domain, which is in the same IS-IS Level 2 domain as the MTGs and PANs. The AGN-SE node is a Cisco ASR-9006. See Figure 6-5.

Figure 6-5 Aggregation Service Edge Node (AGN-SE)



Interface Configuration

```
interface Loopback0
  ipv4 address 100.111.11.1 255.255.255.255
  ipv6 address 2001:100:111:11::1/128
!
!***Redundant AGN-SE Node***
interface TenGigE0/0/0/0
  description To AGN-9006-K1102 TenGigE0/0/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.11.1.0 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  transceiver permit pid all
!
!***Downstream PAN Node***
interface TenGigE0/0/0/1
  description To PAN-903-K0922 Ten0/1/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.9.22.3 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  transceiver permit pid all
!
!***Upstream Core Node***
interface TenGigE0/0/0/2
  description To CN-CRS8-K0401 T0/0/0/2
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.2.1.11 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  transceiver permit pid all
!
!***Downstream PAN Node***
interface TenGigE0/0/0/3
  description to K0508 on Ten0/0/0/1
  cdp
  ipv4 address 10.11.1.2 255.255.255.254
  carrier-delay up 2000 down 0
```

```
  load-interval 30
  transceiver permit pid all
  !
!
```

IGP/LDP Configuration

```
router isis core
  !***AGN-SE is Level-2 only IS-IS node***
  is-type level-2-only
  net 49.0100.1001.1101.1001.00
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  !***Redundant AGN-SE Node***
  interface TenGigE0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
    !
  !
  !***Downstream PAN Node***
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
  !***Upstream Core Node***
  interface TenGigE0/0/0/2
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
```

```
    !
  !
  !***Downstream PAN Node***
  interface TenGigE0/0/0/3
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
!
```

LDP Configuration

```
mpls ldp
  router-id 100.111.11.1
  discovery targeted-hello accept
  graceful-restart
  igp sync delay 5
  log
    graceful-restart
  !
  mldp
    make-before-break delay 0 0
    logging notifications
    recursive-fec
  !
  interface TenGigE0/0/00
  !
  interface TenGigE0/0/0/1
    mldp disable
  !
  interface TenGigE0/0/0/2
  !
  interface TenGigE0/0/0/3
    mldp disable
  !
!
```

BGP Configuration

```
router bgp 1000
  bfd minimum-interval 50
  bfd multiplier 3
  bgp router-id 100.111.11.1
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  bgp log neighbor changes detail
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    additional-paths receive
    bgp attribute-download
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 0
    !***Color Loopback with FSE Community***
    network 100.111.11.1/32 route-policy FSE_Community
    allocate-label all
  !
  address-family vpnv4 unicast
```

```
  !
  address-family ipv6 unicast
    allocate-label all
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  address-family ipv6 mvpn
  !
  session-group intra-as
    remote-as 1000
    password encrypted 13091610
    update-source Loopback0
  !
  !***Neighbor group for CN-RR***
  neighbor-group cn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
    !
    address-family ipv6 mvpn
    !
  !
  !***CN-RR***
  neighbor 100.111.15.50
    use neighbor-group cn-rr
  !
!
route-policy FSE_Community
  set community FSE
end-policy
!
community-set FSE
  2001:2001
end-set

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

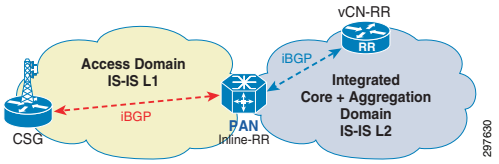
Note Please refer to BGP Transport Control Plane, page 3-14 for a detailed explanation of how BGP communities are used to color prefixes for selective redistribution and filtering.

Pre-Aggregation Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs in the integrated core+aggregation network. The PANs are ABRs between the core/aggregation and access domains. The segmentation between the two domains is achieved by making the integrated core+aggregation network as IS-IS Level 2 and each fixed or mobile access network subtending from a pair of PANs as part of a unique IS-IS Level 1 domain. All

access ring networks and hub-and-spoke connected nodes subtending from the same pair of PANs are part of this IS-IS Level 1 domain, where the FANs or CSGs are IS-IS L1 nodes and the PAN are L1/L2 nodes. The PAN nodes are Cisco ASR-9001 and ASR-903. See Figure 6-6.

Figure 6-6 Pre-Aggregation Node (PAN)



Interface Configuration

```
interface Loopback0
  ipv4 address 100.111.5.8 255.255.255.255
!
!***Redundant PAN Node***
interface TenGigE0/0/0/0
  description to K0507 on Ten0/0/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.5.8.2 255.255.255.254
  transceiver permit pid all
!
!***Upstream AGN-SE Node***
interface TenGigE0/0/0/1
  description to K1102 on Ten0/0/0/3
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.11.2.3 255.255.255.254
  load-interval 30
  transceiver permit pid all
!
!***Downstream FAN Node***
interface TenGigE0/0/0/2
  description to K0709 on Ten0/0/0/2
  cdp
  ipv4 address 10.5.8.4 255.255.255.254
  transceiver permit pid all
!
!***Downstream CSG Node***
interface GigabitEthernet0/0/1/0
  description to K1308 on Gig0/10
  cdp
  ipv4 address 10.5.8.0 255.255.255.254
  negotiation auto
  load-interval 30
  transceiver permit pid all
!
```

IGP/LDP Configuration

```
router isis core
  set-overload-bit on-startup 360
  net 49.0100.1001.1100.5008.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
```

```
    metric-style wide
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 20
    !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  !***Downstream CSG Node***
  interface GigabitEthernet0/0/1/0
    circuit-type level-1
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 100
      mpls ldp sync
    !
  !
  !***Redundant PAN Node***
  interface TenGigE0/0/0/0
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
  !***Upstream AGN-SE Node***
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
  !***Downstream FAN Node***
  interface TenGigE0/0/0/2
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
!
!***Only propagate prefixes with tag 1300***
!***Limits prefix redistribution between access rings***
route-policy RIB-to-ISIS
  if tag eq 1300 then
    pass
  else
    drop
  endif
```

```
end-policy
!
mpls ldp
  router-id 100.111.5.8
  discovery targeted-hello accept
  graceful-restart
  log
    neighbor
    graceful-restart
  !
  interface GigabitEthernet0/0/1/0
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
  interface TenGigE0/0/0/2
  !
!
```

BGP Configuration

```
router bgp 1000
  bgp router-id 100.111.5.8
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  bgp log neighbor changes detail
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    !***Color Loopback of PAN with proper communities***
    network 100.111.5.8/32 route-policy PAN_RAN_FAN_Community
    allocate-label all
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  !***Session group for all CSGs***
  session-group csg
    remote-as 1000
    password encrypted 151E0A0E
    update-source Loopback0
  !
  !***Session group for all AGNs and MTGs***
  session-group intra-as
    remote-as 1000
    password encrypted 13091610
    update-source Loopback0
  !
  !***CSG Neighbor group***
  neighbor-group csg
    use session-group csg
    address-family ipv4 labeled-unicast
      route-reflector-client
      !***Insert PAN as next-hop self for all CSGs***
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family vpnv6 unicast
    !
  !
  !***CN-RR Neighbor group***
```

```
  neighbor-group cn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family vpnv6 unicast
    !
  !
  !***CN-RR***
  neighbor 100.111.15.50
    use neighbor-group cn-rr
  !
  !***FANs***
  neighbor 100.111.7.9
    use neighbor-group csg
  !
  neighbor 100.111.7.10
    use neighbor-group csg
  !
  neighbor 100.111.7.11
    use neighbor-group csg
  !
  neighbor 100.111.7.12
    use neighbor-group csg
  !
  neighbor 100.111.7.13
    use neighbor-group csg
  !
  !***CSGs***
  neighbor 100.111.13.8
    use neighbor-group csg
  !
  neighbor 100.111.13.9
    use neighbor-group csg
  !
  neighbor 100.111.13.10
    use neighbor-group csg
  !
!

route-policy PAN_RAN_FAN_Community
  set community PAN_RAN_FAN_Community
end-policy
!
!***10:10 = Common CSG Community***
!***20:20 = FAN Community***
community-set PAN_RAN_FAN_Community
  10:10,
  20:20
end-set

route-policy BGP_Ingress_Transport_Filter
  if community matches-any PASS_Community then
    pass
  else
    drop
  endif
end-policy
!
community-set PASS_Community
  10:10,
```

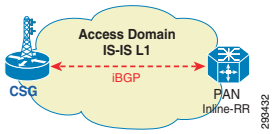
```
  20:20,
  1001:1001,
  2001:2001,
  3001:3001
end-set
```

Note The above described configuration belongs to ASR-9001 as a PAN node.

Cell Site Gateway Configuration

This section shows the IGP/LDP configuration required on the CSGs. All access ring networks and hub-and-spoke connected subtending from the same pair of AGNs are part of the same IS-IS Level 1 domain where the CSGs are IS-IS L1 nodes and the PANs are L1/L2 nodes. The inter-domain LSPs are enabled by extending labeled BGP to the CSGs in the RAN access. The CSG nodes are Cisco ASR-920 and ASR-901. See Figure 6-7.

Figure 6-7 Cell Site Gateway (CSG)



Interface Configuration

```
!
interface Loopback0
  ip address 100.111.13.8 255.255.255.255
!
!***Uplink to PAN***
interface GigabitEthernet0/10
  description To PAN-K0508 G0/0/1/0
  no ip address
  negotiation auto
  cdp enable
  service instance 40 ethernet
    encapsulation untagged
    bridge-domain 40
  !
!
interface Vlan40
  ip address 10.5.8.1 255.255.255.254
  ip router isis core
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 5
  bfd interval 50 min_rx 50 multiplier 3
  isis circuit-type level-1
  isis network point-to-point
  isis metric 100
  isis csnp-interval 10
  hold-queue 512 in
  hold-queue 512 out
!
!***Interface to next CSG***
interface GigabitEthernet0/11
  description To CSG-K1309 G0/10
  no ip address
  load-interval 30
```

```
  negotiation auto
  bfd interval 50 min_rx 50 multiplier 3
  cdp enable
  service instance 20 ethernet
    encapsulation untagged
    bridge-domain 20
  !
!
interface Vlan20
  ip address 10.13.8.0 255.255.255.254
  ip router isis core
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 5
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
  isis network point-to-point
  isis metric 100
  isis csnp-interval 10
  hold-queue 512 in
  hold-queue 512 out
!
```

IGP/LDP Configuration

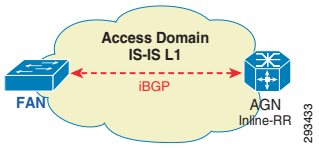
```
router isis core
  net 49.0100.1001.1101.3008.00
  is-type level-1
  advertise passive-only
  ispf level-1
  metric-style wide
  fast-flood
  set-overload-bit on-startup 120
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 5 200
  no hello padding
  log-adjacency-changes
  !***Remote LFA FRR with microloop avoidance***
  fast-reroute per-prefix level-1 all
  fast-reroute remote-lfa level-1 mpls-ldp
  microloop avoidance protected
  redistribute connected
  passive-interface Loopback0
  bfd all-interfaces
  mpls ldp sync
!

mpls label protocol ldp
mpls ldp discovery targeted-hello accept
!
mpls ldp router-id Loopback0 force
BGP Configuration
router bgp 1000
  bgp router-id 100.111.13.8
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor pan peer-group
  neighbor pan remote-as 1000
```

```
  neighbor pan password lab
  neighbor pan update-source Loopback0
  neighbor 100.111.5.7 peer-group pan
  neighbor 100.111.5.8 peer-group pan
  !
  address-family ipv4
    bgp additional-paths install
    bgp nexthop trigger delay 1
    !***Color loopback with CSG communities***
    network 100.111.13.8 mask 255.255.255.255 route-map ACC_RAN_FAN_Community
    neighbor pan send-community
    neighbor pan next-hop-self
    neighbor pan route-map BGP_Ingress_Transport_Filter in
    neighbor pan send-label
    neighbor 100.111.5.7 activate
    neighbor 100.111.5.8 activate
  exit-address-family
  !
  address-family vpnv4
    <SNIP>
  exit-address-family
  !
  address-family vpnv6
    <SNIP>
  exit-address-family

!***10:10 = Common RAN Community***
!***10:202 = CSG is in Metro-2, Access-2***
route-map ACC_RAN_FAN_Community permit 10
  set community 10:10 10:202

ip bgp-community new-format
ip community-list expanded PASS_Community permit 10:202|20:20|1001:1001|2001:2001
!
route-map BGP_Ingress_Transport_Filter permit 10
 match community PASS_Community
!
```

Fixed Access Node Configuration

This section shows the IGP/LDP configuration required on the FANs, which are nearly identical to the CSG configurations. All access ring networks and hub-and-spoke connected nodes subtending from the same pair of PANs are part of the same IS-IS Level 1 domain, where the FANs are IS-IS L1 nodes and the PANs are L1/L2 nodes. The inter-domain LSPs are enabled by extending labeled BGP to the FANs in the access. The FAN nodes are ME-3600 and ASR-920. See Figure 6-8.

Figure 6-8 Fixed Access Node (FAN)



Interface Configuration

```
!
interface Loopback0
  ip address 100.111.7.9 255.255.255.255
!
```

```
!***Interface to next FAN in ring***
interface TenGigabitEthernet0/1
  description To FAN-ME36-K0710
  no switchport
  ip address 10.7.9.0 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
  isis network point-to-point
!
!***Uplink to PAN***
interface TenGigabitEthernet0/2
  description To PAN-K0508
  no switchport
  ip address 10.5.8.5 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
  isis network point-to-point
!
```

IGP/LDP Configuration

```
router isis agg-acc
  net 49.0100.1001.1100.7009.00
  is-type level-1
  ispf level-1
  metric-style wide
  fast-flood
  set-attached-bit route-map DO_NOT_SET_ATT_BIT
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 5 200
  no hello padding
  log-adjacency-changes
  fast-reroute per-prefix level-1 all
  fast-reroute remote-lfa level-1 mpls-ldp
  passive-interface Loopback0
  bfd all-interfaces
  mpls ldp sync
!

clns filter-set DO_NOT_SET_ATT_BIT deny 00.0000
!
route-map DO_NOT_SET_ATT_BIT permit 10
  match clns address DO_NOT_SET_ATT_BIT

mpls label protocol ldp
mpls ldp discovery targeted-hello accept
!
mpls ldp router-id Loopback0 force
BGP Configuration
!
router bgp 1000
```

```
  bgp router-id 100.111.7.9
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor pan peer-group
  neighbor pan remote-as 1000
  neighbor pan password lab
  neighbor pan update-source Loopback0
  neighbor 100.111.5.7 peer-group pan
  neighbor 100.111.5.8 peer-group pan
  !
  address-family ipv4
    bgp additional-paths install
    bgp nexthop trigger delay 1
    !***Color loopback with CSG communities***
    network 100.111.7.9 mask 255.255.255.255 route-map ACC_RAN_FAN_Community
    neighbor pan send-community
    neighbor pan next-hop-self
    !***Permit only needed BGP prefixes from PANs***
    neighbor pan route-map BGP_Ingress_Transport_Filter in
    neighbor pan send-label
    neighbor 100.111.5.7 activate
    neighbor 100.111.5.8 activate
  exit-address-family
  !
  address-family vpnv4
  exit-address-family
  !
  address-family vpnv6
    exit-address-family
!***20:20 is the common FAN community***
route-map FAN_Community permit 10
  set community 20:20
!***Permitted FAN prefixes for configured E-Line services***
ip prefix-list WL-Service-Destinations permit 100.111.7.10/32
!
route-map BGP_Ingress_Transport_Filter permit 10
  match ip address prefix-list WL-Service-Destinations
```

Note The above described configuration belongs to a ME-3600 device acting as a FAN. ASR-920 can also be implemented as a FAN and its configuration will be identical to CSG node with the FAN community being used instead of the CSG community for loopback advertisement and BGP inbound permit filter.

Dynamic Prefix List Script

Each time a new wireline service is enabled on the FAN, the ip prefix-list for the inbound route-map needs to be updated to allow the remote destination loopback of wireline service to be accepted. This process can be easily automated by using a simple Embedded Event Manager (EEM) script, which is shown later in this section.

With this EEM script in place on the FAN, when the operator configures a new Virtual Private Wire Service (VPWS) service on the device, the remote loopback corresponding to the destination argument will automatically be added to the "WL-Service-Destinations" prefix-list of allowed wireline destinations. The script will also trigger a dynamic inbound soft reset using the clear ip bgp destination soft in command in order to initiate a nondisruptive dynamic route refresh.

Note The IP addresses shown in these scripts for the dynamic inbound soft reset must be updated in order to reflect the actual PAN addresses for the particular FAN.

```
#-------------------------------------------------------------------
# EEM scripts to automatically fetch IP /32 endpoints
# of configured PWs. IP addresses are advertised via a BGP session.
# To get prefixes the inbound WL-Service-Destinations filter list
# is changed accordingly. Removing a configuration of PW removes
# also the /32 prefix from the filter list.
#
# October 2012, Cisco Systems
#-------------------------------------------------------------------

==========================================
To add PW primary and backup
Supporting EoMPLS, ATMoMPLS, CESoPSN, SAToP
==========================================

!***Handles PWE3 xconnect***
event manager applet UpdateInboundFilter11
  event cli pattern ".*xconnect.*encapsulation.*mpls" sync no skip no
  action 10 regexp " [0-9.]+" "$_cli_msg" result
  action 20 cli command "enable" action 30 cli command "conf t"
  action 40 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 50 puts "Inbound Filter updated for $result/32"
  action 60 cli command "end"
  action 70 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 80 cli command "clear ip bgp 100.111.5.4 soft in"
  action 81 cli command "clear ip bgp 100.111.5.5 soft in"
  action 90 puts "Triggered Dynamic Inbound Soft Reset towards PANs"

!***Handles PWE3 xconnect with only PW-class***
event manager applet UpdateInboundFilter12
  event cli pattern ".*xconnect.*pw-class.*" sync no skip no
  action 10 regexp " [0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 50 puts "Inbound Filter updated for $result/32"
  action 60 cli command "end"
  action 70 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 80 cli command "clear ip bgp 100.111.5.4 soft in"
  action 81 cli command "clear ip bgp 100.111.5.5 soft in"
  action 90 puts "Triggered Dynamic Inbound Soft Reset towards PANs"

!***Handles backup PWE3 under xconnect***
event manager applet UpdateInboundFilter13
  event cli pattern ".*backup.*peer.*" sync no skip no
  action 10 regexp " [0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 50 puts "Inbound Filter updated for $result/32"
  action 60 cli command "end"
  action 70 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 80 cli command "clear ip bgp 100.111.5.4 soft in"
  action 81 cli command "clear ip bgp 100.111.5.5 soft in"
  action 90 puts "Triggered Dynamic Inbound Soft Reset towards PANs"
```

Similarly, when a wireline service is removed from the FAN, the ip prefix-list needs to be updated in order to remove the remote destination loopback of the deleted wireline service. The following two EEM scripts will automate this process through the following logic:

1. The operator removes the XConnect by using the no xconnect command. No IP address is required to remove a correct line from a prefix-list.
2. To obtain the IP address, the "tovariable_int_num<X>" applet is used with an environmental variable $_int. This applet is triggered by the interface, service instance, cem, or pvc command, which informs the variable that there can be a potential change in the configuration.
3. The applet "UpdateInboundFilter21" and is triggered by the no xconnect command and uses the interface derived from the "tovariable" applets in order to obtain the IP address and remove it from the prefix-list. The applet "UpdateInboundFilter23" does the same function for the no backup peer command in order to handle removal of backup PW3s.

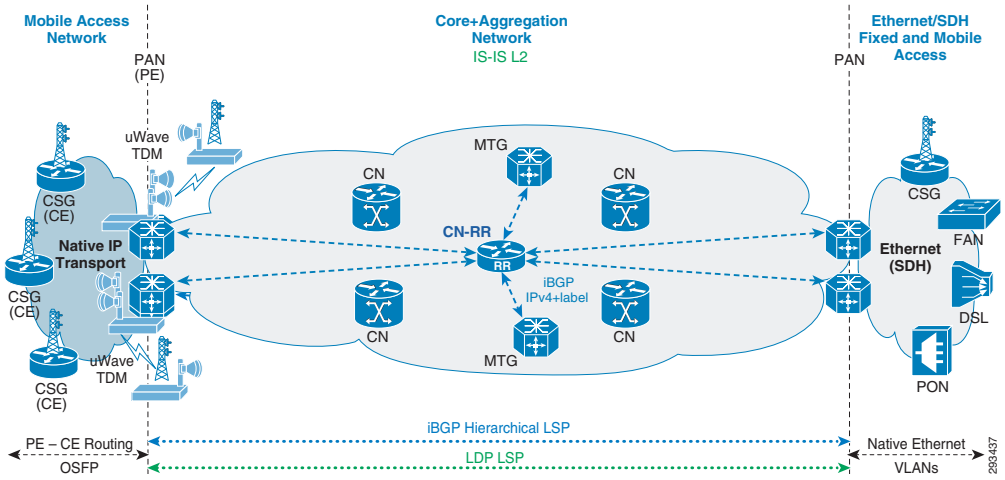
```
==========================================
To remove PW
Supporting Ethernet, CES, ATM interfaces
==========================================
!***Handles interface configurations***
event manager applet tovariable_int
  event cli pattern "^interface" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int $_cli_msg"
  action 40 cli command "event manager environment _int_sec 0"

!***Handles service instance configurations***
event manager applet tovariable_int_num1
  event cli pattern "^service instance" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int_num $_cli_msg"
  action 40 cli command "event manager environment _int_sec 1"

!***Handles cem interface configurations***
event manager applet tovariable_int_num2
  event cli pattern "^cem" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int_num $_cli_msg"
  action 40 cli command "event manager environment _int_sec 2"

!***Handles ATM pvc configurations***
event manager applet tovariable_int_num3
  event cli pattern "^pvc" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int_num $_cli_msg"
  action 40 cli command "event manager environment _int_sec 3"

!***Triggers on "no xconnect" and parses IP prefix to be removed***
no event manager applet UpdateInboundFilter21
event manager applet UpdateInboundFilter21
  event cli pattern "no xconnect" sync no skip yes
  action 10 cli command "enable"
  action 12 string trimright "$_int_num"
  action 13 set _int_num "$_string_result"
  action 19 if $_int_sec eq 0 goto 35
  action 20 cli command "show run $_int | s $_int_num"
  action 30 regexp "xconnect.*" "$_cli_result" line
  action 32 if $_int_sec ne 0 goto 40
```

```
  action 35 cli command "show run $_int | i xconnect"
  action 36 set line $_cli_result
  action 40 regexp "[0-9.]+" "$line" result
  action 50 cli command "enable"
  action 60 cli command "conf t"
  action 70 cli command "no ip prefix-list WL-Service-Destinations permit $result/32"
  action 80 cli command "$_int"
  action 81 cli command "$_int_num"
  action 82 cli command "no xc"
  action 92 cli command "do show run | i xconnect $result"
  action 93 string first "xconnect $result" "$_cli_result"
  action 94 if $_string_result eq "-1" goto 96
  action 95 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 96 cli command "end"
  action 97 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 100 cli command "clear ip bgp 100.111.5.4 soft in"
  action 110 cli command "clear ip bgp 100.111.5.5 soft in"
  action 120 puts "Triggered Dynamic Inbound Soft Reset towards PANs"

==========================================
To remove a backup PW
Supporting Ethernet, CES, ATM interfaces
==========================================

!***Triggers on "no backup peer" and parses IP prefix to be removed***
event manager applet UpdateInboundFilter23
  event cli pattern "no backup peer" sync no skip no
  action 10 regexp "[0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "no ip prefix-list WL-Service-Destinations permit $result/32"
  action 96 cli command "end"
  action 97 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 100 cli command "clear ip bgp 100.111.5.4 soft in"
  action 110 cli command "clear ip bgp 100.111.5.5 soft in"
  action 120 puts "Triggered Dynamic Inbound Soft Reset towards PANs"
==========================================
```

Non-IP/MPLS Access

In this model, the core and aggregation networks are integrated with a flat IGP and LDP control plane from the core to the PANs in the aggregation domain. Labeled BGP is not utilized in this model, as the scale of the network does not warrant the additional transport layer. See Figure 6-9.

Figure 6-9 Small Network with non-MPLS Access



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

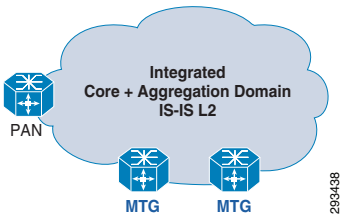
In this model, the access network could be one of the following options:

- CSGs in point-to-point or ring topologies over fiber or packet microwave running native IP transport, supporting 3G/LTE services. In this case, the CSGs act as CEs and PANs are the L3 MPLS VPN PEs enabling the backhaul. The BTS or ATM NodeBs can connect to the PANs with TDM microwave for 2G and 3G ATM-based services. Here the PANs enable the L2 MPLS VPN service with pseudowire-based circuit emulation for backhaul to the BSC/RNC.
- FANs in point-to-point and G.8032-enabled ring topologies over fiber access running native Ethernet, supporting enterprise, MEF, and even mobile transport services. The FAN may be a fiber access node or a GPON OLT. In this case, the PANs provide service edge functionality for the services from the FANs and connect the services to the proper L2VPN or L3VPN service backhaul mechanism. In either scenario, the MPLS services are always enabled by the PANs in the aggregation network.
- FANs or CSGs operating in nV mode, over Simple Ring and L2 Fabric topologies, supporting enterprise and MEF transport services. In this case, the AGNs provide subscriber and service UNI functionality for all services physically initiating at the FANs/CSGs.

Mobile Transport Gateway Configuration

This section shows the IGP/LDP configuration required to build the LSPs to the PANs. See Figure 6-10.

Figure 6-10 Mobile Transport Gateway (MTG)



Interface Configuration

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

IGP Configuration

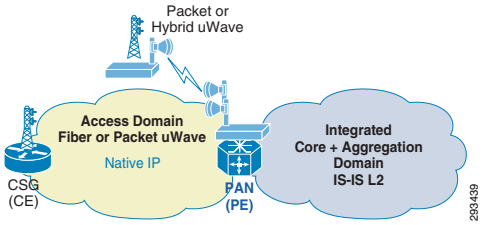
```
router isis core-agg
  set-overload-bit on-startup 250
  net 49.0100.1001.1101.5001.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  interface TenGigE0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      metric 10
      mpls ldp sync
    !
  !
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
```

```
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      metric 10
      mpls ldp sync
    !
  !
!
mpls ldp
  router-id 100.111.15.1
  discovery targeted-hello accept
  nsr
  graceful-restart
  session protection
  igp sync delay 10
  log
    neighbor
    graceful-restart
    session-protection
    nsr
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
!
```

Pre-Aggregation Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs. Minimal BGP configuration is shown as the basis for building the transport MPLS VPN. The actual service configuration is in the EPN 4.0 Mobile Transport Design and Implementation Guide. See Figure 6-11.

Figure 6-11 Pre-Aggregation Node (PAN)



Interface Configuration

```
interface Loopback0
  ip address 100.111.14.3 255.255.255.255
!
!***Redundant PAN interface***
interface TenGigabitEthernet0/0/0
  description To PAN-K1404 Ten0/0/0
  ip address 10.14.3.0 255.255.255.254
  ip router isis core
  load-interval 30
  carrier-delay msec 0
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
```

```
  cdp enable
  isis network point-to-point
  isis metric 10
  isis csnp-interval 10
  service-policy output PMAP-NNI-E
  hold-queue 1500 in
  hold-queue 2000 out
!
!***Uplink interface***
interface TenGigabitEthernet0/1/0
  description To AGN-K1102 Ten0/0/0/1
  ip address 10.11.2.1 255.255.255.254
  ip router isis core
  load-interval 30
  carrier-delay msec 0
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis circuit-type level-2-only
  isis network point-to-point
  isis metric 10
  service-policy output PMAP-NNI-E
  hold-queue 1500 in
  hold-queue 2000 out
!
!***Interface toward native IP CE ring in MPLS VPN RFS***
!***Shown here for reference. Not part of Unified MPLS config.***
interface GigabitEthernet0/4/2
  description To CSG-901-K1314
  vrf forwarding RFS
  ip address 10.13.14.1 255.255.255.254
  ip ospf network point-to-point
  load-interval 30
  negotiation auto
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  hold-queue 350 in
  hold-queue 2000 out
!
```

IGP/LDP Configuration

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

```
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
Small Network Non-IP/MPLS Access Network Implementation
```

Dual Homed Hub-and-Spoke Ethernet Access

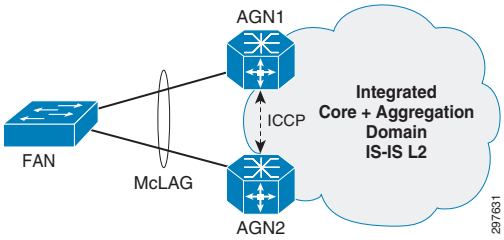
In the Large Network, Dual Homed topologies for hub-and-spoke access have been implemented in the following mode:

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

Per Node Active/Standby MC-LAG

Figure 6-12 illustrates the implementation of hub-and-spoke Ethernet access with MC-LAG operating in Per Node Active and Standby Mode.

Figure 6-12 Per Node Active/Standby MC-LAG



The FAN access node, either a ASR 901 or a PON OLT, is Dual Homed to the AGN nodes using a bundle interface. The AGN node establish a interchassis bundle and correlate the states of the bundle member ports using ICCP.

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

The following configuration shows the implementation of the AGN nodes, AGN-K1101 and AGN-K1102, and the FANs, CSG-K0306 and OLT-3.

Aggregation Node Configuration

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

NNI Interfaces

For reference throughout this document, the following is a list of settings used for MC-LAG configuration.

The access-facing virtual bundle interface is configured as follows:

- Suppress-flaps timer set to 300 ms. This prevents the bundle interface from flapping during a LACP failover.
- Associated with ICCP redundancy group 300.
- Lowest possible port-priority (to ensure node serves as active point of attachment (PoA) initially).

- MAC address for bundle interface. This needs to match the MAC address configured on the other PoA's bundle interface.
- Wait-while timer set to 100 ms to minimize LACP failover time.
- Maximum links allowed in the bundle limited to 1. This configuration ensures that the access node will never enable both links to the PoAs simultaneously if ICCP signaling between the PoAs fails.

Note The following configuration is collected for AGN1 connectivity toward the PON OLT. A similar configuration is applied for connectivity toward the ME3400 node

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

ICCP and Multichassis LACP

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

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

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

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

NNI Interfaces

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

ICCP and Multichassis LACP

The ICCP redundancy group is configured as follows:

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

```
!*** ICCP Configuration ***
redundancy
 iccp
  group 102
   mlacp node 2
   mlacp system mac 0000.1101.1111
   mlacp system priority 20
   member
    neighbor 100.111.11.1
   !
   backbone
    interface TenGigE0/0/0/0
    interface TenGigE0/0/0/2
   !
  !
 !
!
```

Fixed Access Node Configuration: ASR-901

NNI Interfaces

```
!*** Interface configuraton towards the AGN nodes ***
interface GigabitEthernet0/8
 description por to 1101 gi 0/0/1/16
 no ip address
 load-interval 30
 negotiation auto
 channel-protocol lacp
 channel-group 6 mode active
!
interface GigabitEthernet0/6
 description por to 1102 gi 0/0/1/17
 no ip address
 load-interval 30
 negotiation auto
```

```
 channel-protocol lacp
 channel-group 6 mode active
!
!*** Port-Channel configuration towards the AGN nodes ***
interface Port-channel6
 no ip address
 load-interval 30
 no negotiation auto
 ethernet dot1ad nni
 !
!
```

Fixed Access Node Configuration: PON OLT

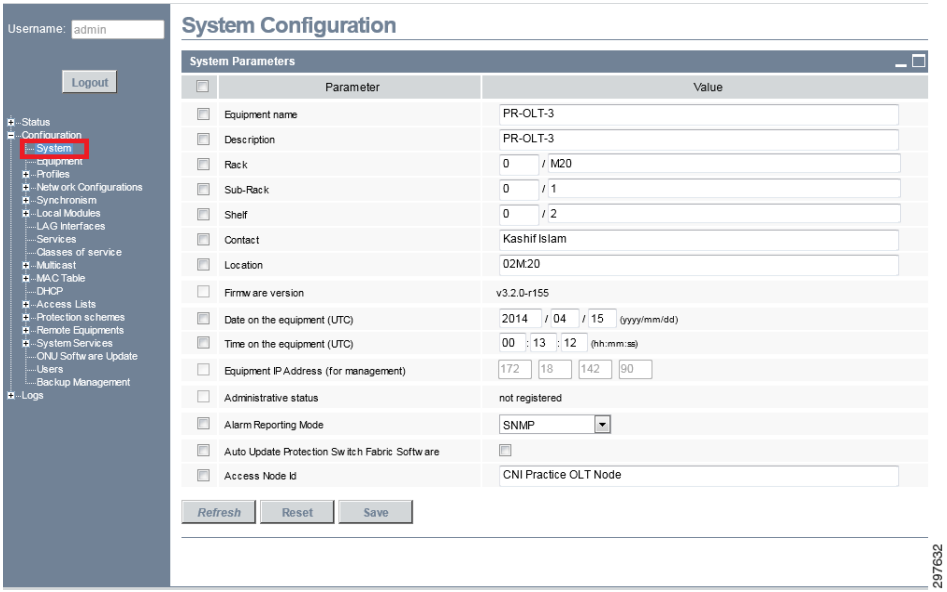
This section shows the basic setup for the ME 4600 PON OLT. Configuration includes the provisioning of the following:

- System
- Network
- Equipment
- Ethernet uplink ports
- LAG interface
- ONU profiles
- PON downlink ports
- ONU discovery
- ONU configuration

System Configuration

You configure the system by setting logistics-related information such as the system name, location, contact owner, date, and time. See Figure 6-13.

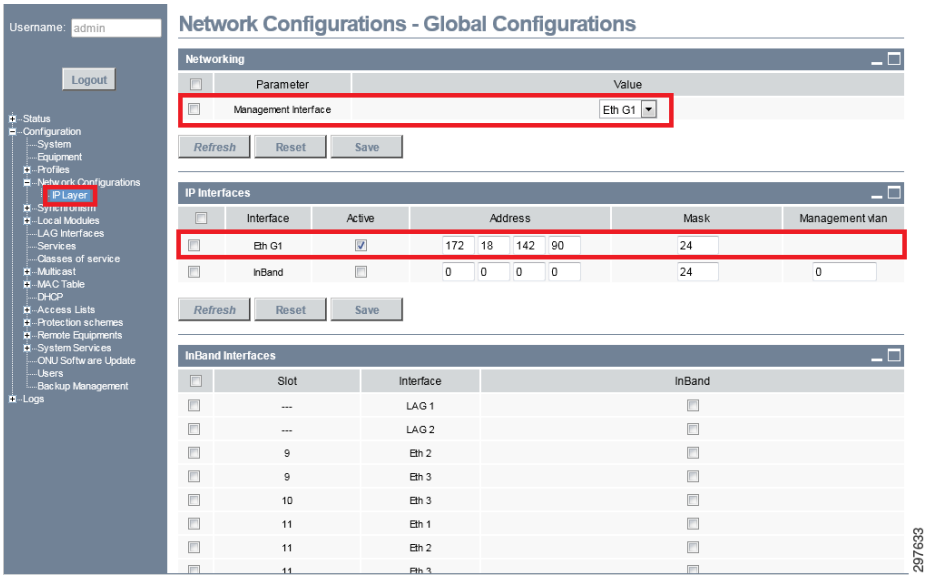
Figure 6-13 System Configuration



Network Configuration

You configure the network by choosing the Management Interface and setting its address. See Figure 6-14.

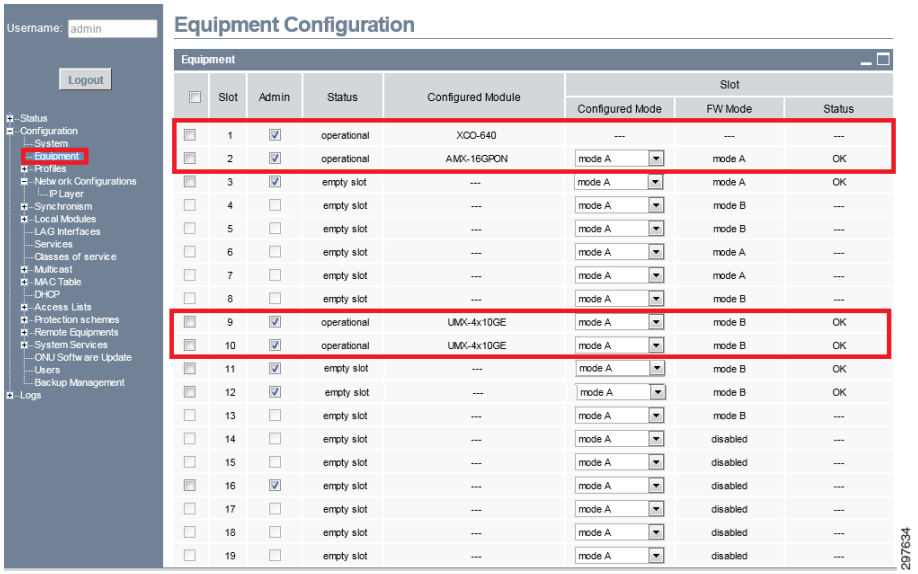
Figure 6-14 Network Configuration



Equipment Configuration

Using administrative credentials, you configure the equipment by bringing up of the various system components such as I/O line cards and fabric cards. See Figure 6-15.

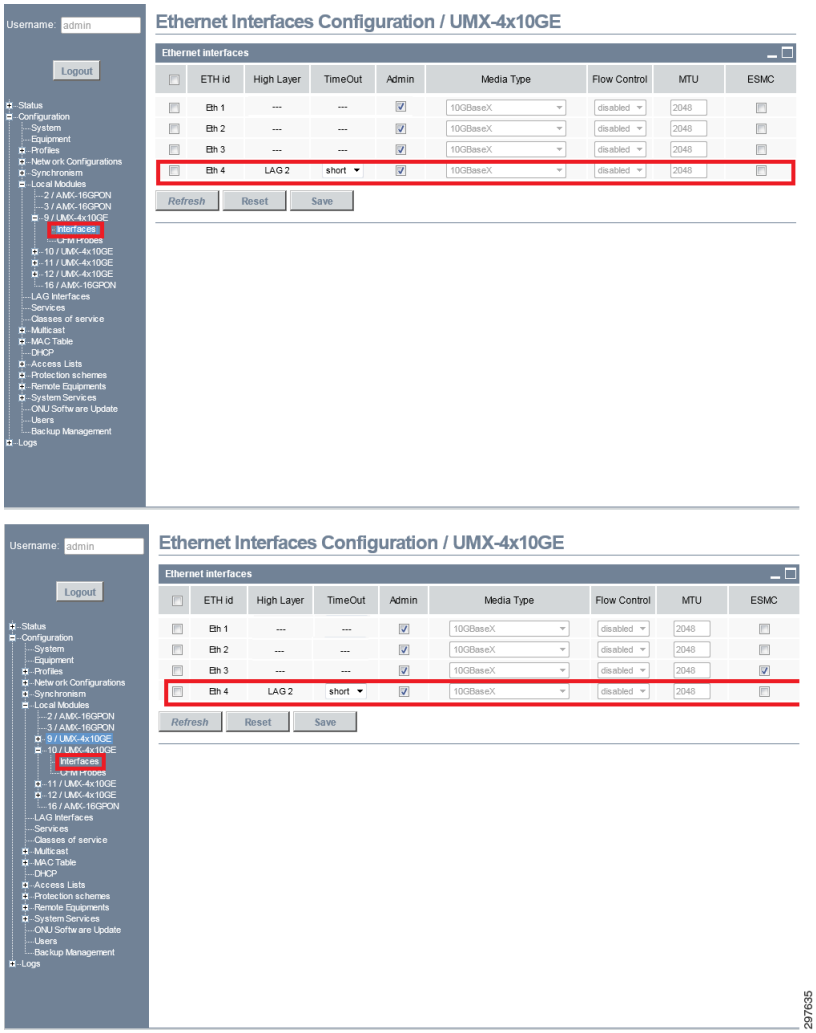
Figure 6-15 Equipment Configuration



Ethernet Uplink Ports Configuration

Using administrative credentials, you configure Ethernet uplink ports by enabling the port, selecting the media type, enabling or disabling flow control, and setting the MTU. See Figure 6-16.

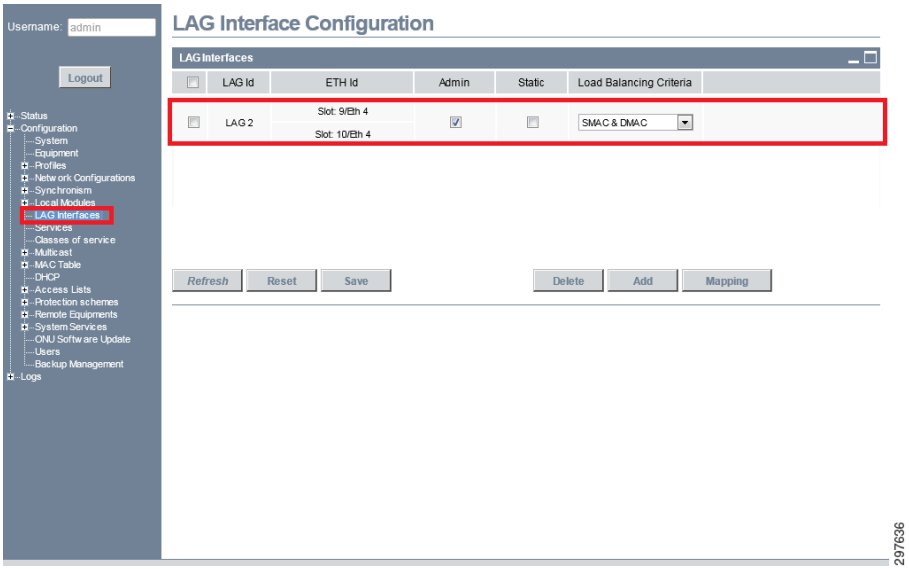
Figure 6-16 Ethernet Uplink Ports Configuration



LAG Interface Configuration

You configure a LAG interface by selecting the uplink Ethernet ports to be bundled and setting the load balancing algorithm. See Figure 6-17.

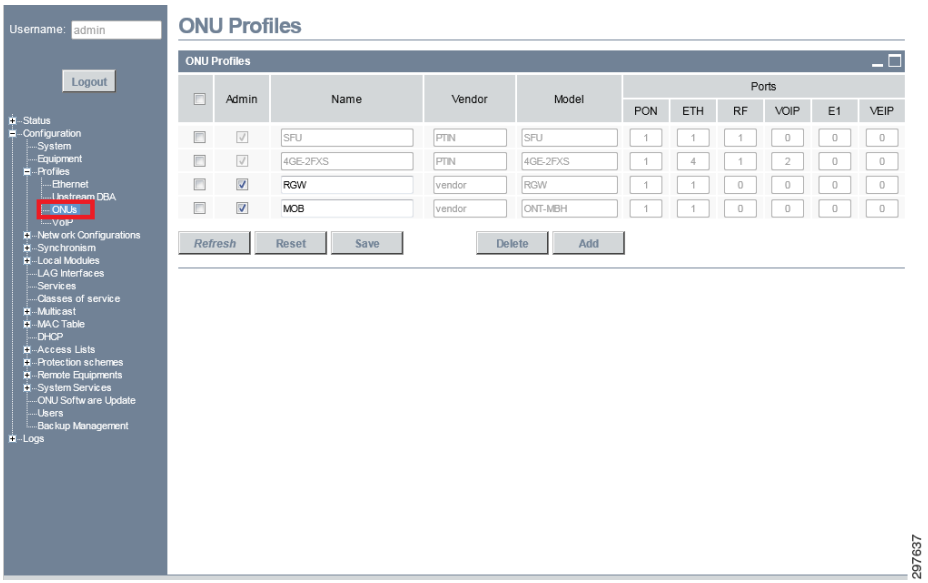
Figure 6-17 LAG Interface Configuration



ONU Profiles Configuration

ONU profiles describe the hardware layout of the ONU devices connected to the OLT node. See Figure 6-18.

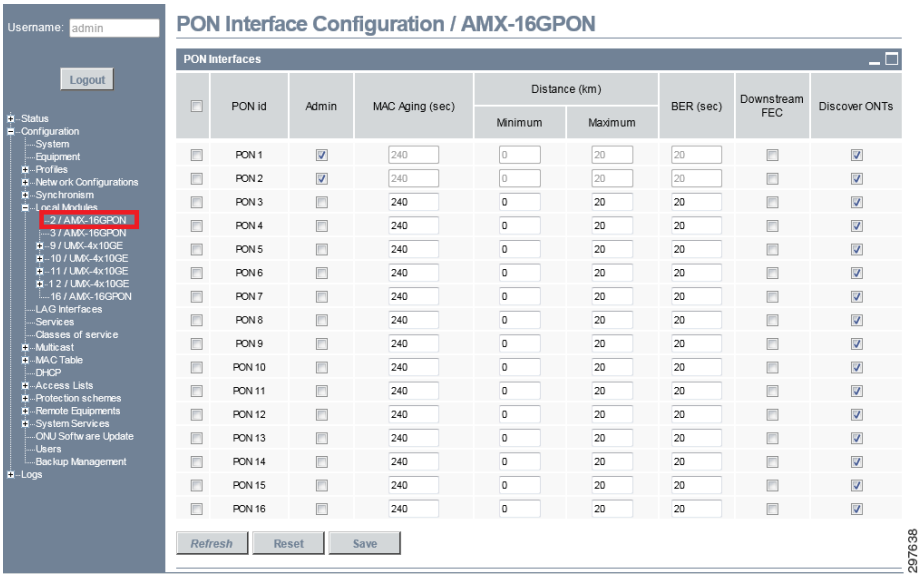
Figure 6-18 ONU Profiles Configuration



PON Downlink Ports Configuration

Using administrative credentials, you configure Ethernet uplink ports by enabling the port and setting the minimum and maximum distance between ONUs and OLT. See Figure 6-19.

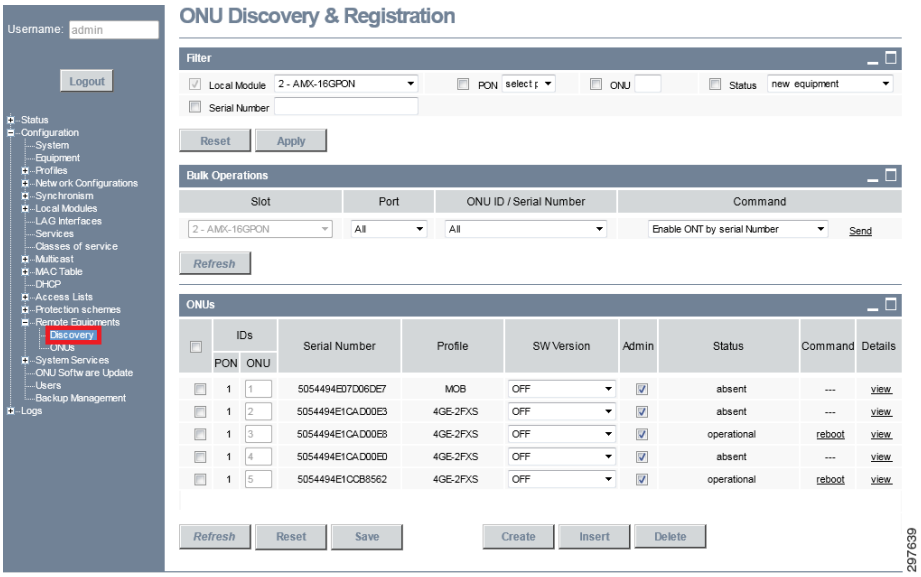
Figure 6-19 PON Downlink Ports Configuration



ONU Discovery Configuration

ONU devices are pre-provisioned on the ONU and their presence and operational state is dynamically discovered. To pre-provision a ONU, choose a unique ID number, specify its serial number, and then map it to a previously created profile. See Figure 6-20.

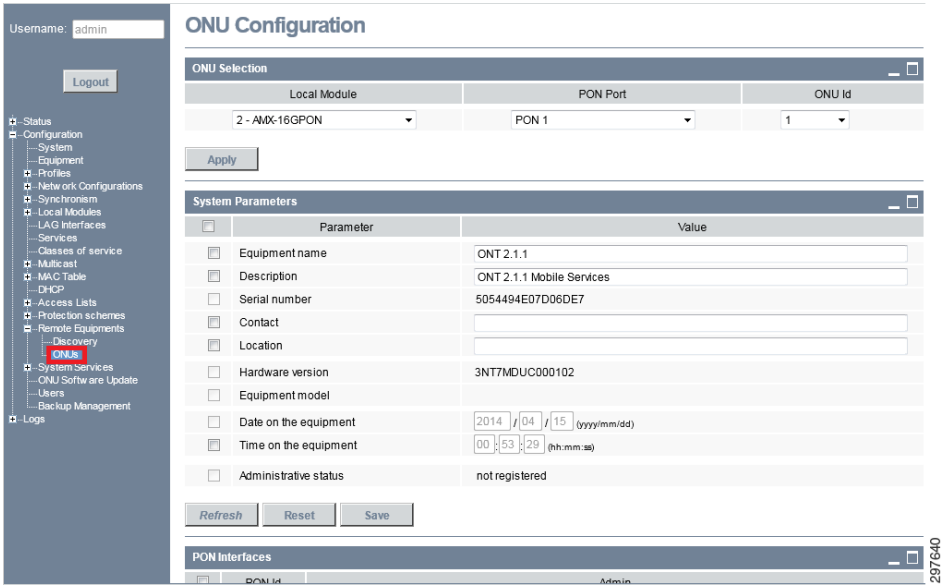
Figure 6-20 ONU Discovery Configuration



ONU Configuration

Once pre-provisioned, you can apply name, location, date and time settings to the ONU device. See Figure 6-21,

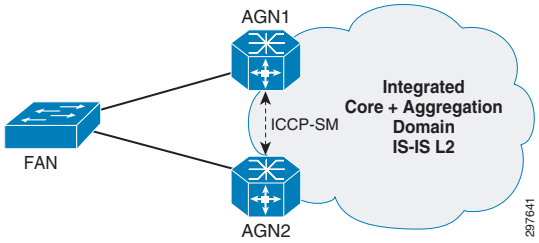
Figure 6-21 ONU Configuration



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

Figure 6-22 illustrates the implementation of hub-and-spoke Ethernet access with MC-LAG operating in per VLAN active/active load balancing.

Figure 6-22 Per VLAN Active/Active MC-LAG



The FAN access node, a ME 3400, connects to each AGN via standalone Ethernet links or Bundle interfaces that are part of a common bridge domain(s). All the links terminate in a common multi-chassis bundle interface at the AGN and are placed in active or hot-standby state based on node and VLAN via ICCP-SM negotiation.

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

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

Aggregation Nodes Configuration

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

NNI Interfaces

```
interface Bundle-Ether1
    !
```

```
interface Bundle-Ether1.100 l2transport
 encapsulation dot1q 100
!
interface Bundle-Ether1.101 l2transport
 encapsulation dot1q 101
!
interface GigabitEthernet0/0/1/1
  bundle id 1 mode on
```

ICCP and ICCP-SM and Multichassis LACP

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

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

```
redundancy
  iccp
    group 1
      member
        neighbor 100.111.11.2
      !
      backbone
        interface TenGigE0/0/0/0
        interface TenGigE0/0/0/2
      !
    !
  !
!

l2vpn
  redundancy
    iccp group 1
      multi-homing node-id 1
      interface Bundle-Ether1
        primary vlan 100
        secondary vlan 101
        recovery delay 60
      !
    !
  !
```

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

NNI Interfaces

```
interface GigabitEthernet0/3/1/12
 bundle id 1 mode on
!
interface Bundle-Ether1
!
interface Bundle-Ether1.100 l2transport
 encapsulation dot1q 100
!
interface Bundle-Ether1.101 l2transport
 encapsulation dot1q 101
!
```

ICCP and Multichassis LACP

The ICCP redundancy group is configured as follows:

```
redundancy
 iccp
  group 1
   member
    neighbor 100.111.11.1
   !
   backbone
    interface TenGigE0/0/0/0
    interface TenGigE0/0/0/2
   !
  !
 !
!*** ICCP-SM configuration ***
l2vpn
 redundancy
  iccp group 1
   multi-homing node-id 2
   interface Bundle-Ether1
    primary vlan 101
    secondary vlan 100
    !
  !
!
```

Fixed Access Node: ME3400

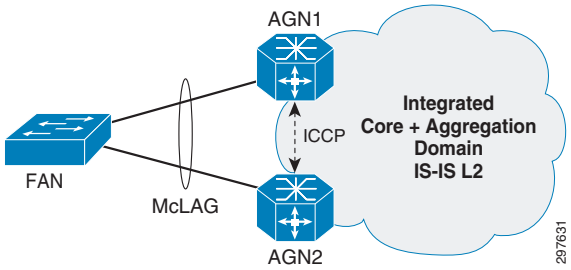
NNI Interfaces

```
interface GigabitEthernet0/13
 port-type nni
 switchport trunk allowed vlan 100-101
 switchport mode trunk
 load-interval 30
!
interface GigabitEthernet0/14
 port-type nni
 switchport trunk allowed vlan 100-101
 switchport mode trunk
 load-interval 30
 !
```

Per Flow Active/Active MC-LAG

Figure 6-23 illustrates the implementation of hub-and-spoke Ethernet access with MC-LAG operating in per flow active/active load balancing.

Figure 6-23 Per Flow Active/Active MC-LAG



The FAN access node, a ME 3400, is dual homed to the AGN nodes using a bundle interface. The AGN node establish an interchassis bundle and correlate the states of the bundle member ports using ICCP.

In the steady state, traffic from the FAN is load balanced between the AGN nodes based on the MAC addresses. In case of link or AGN node failure, the remaining AGN node takes over the traffic forwarding responsibility.

The following configuration example shows the implementation of active/active Per Flow MC-LAG for VLANs 602 and 605 and on the AGN nodes, AGN-K1101 and AGN-K1102, and the FAN, ME-K0904.

Note Per flow active/active MC-LAG is only supported for L2VPN services implemented using a PBB-EVPN core.

Aggregation Node Configuration

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

NNI Interfaces

```
interface GigabitEthernet0/0/1/18
 bundle id 601 mode active
 transceiver permit pid all
!
interface Bundle-Ether601
 mlacp iccp-group 601
!
interface Bundle-Ether601.602 l2transport
 encapsulation dot1q 602
!
interface Bundle-Ether601.605 l2transport
 encapsulation dot1q 605
!
```

ICCP and Multichassis LACP

```
!*** ICCP configuration for active active per flow load sharing ***
redundancy
 iccp
  group 601
   mlacp node 1
   mlacp system mac 1111.2222.3333
   mlacp system priority 10
   mode singleton
   backbone
    interface TenGigE0/0/0/0
    interface TenGigE0/0/0/2
    !
   !
  !
```

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

NNI Interfaces

```
interface GigabitEthernet0/0/1/18
 bundle id 601 mode active
 transceiver permit pid all
!
interface Bundle-Ether601
 mlacp iccp-group 601
!
interface Bundle-Ether601.602 l2transport
 encapsulation dot1q 602
!
interface Bundle-Ether601.605 l2transport
 encapsulation dot1q 605
!
```

ICCP and Multichassis LACP

```
!*** ICCP configuration fir Active Active per Flow load sharing***
redundancy
 iccp
  group 601
   mlacp node 2
   mlacp system mac 1111.2222.3333
   mlacp system priority 10
   mode singleton
   backbone
    interface TenGigE0/0/0/0
    interface TenGigE0/0/0/2
   !
  !
 !
```

Fixed Access Node Configuration: ME3400

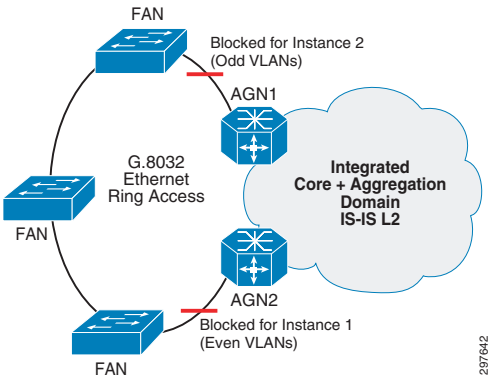
NNI Interfaces

```
!*** Interface configuration towards the AGN nodes ***
interface GigabitEthernet0/3
 port-type nni
 switchport mode trunk
 load-interval 30
 channel-protocol lacp
 channel-group 6 mode active
!
interface GigabitEthernet0/4
 port-type nni
 switchport trunk allowed vlan 602-605
 switchport mode trunk
 load-interval 30
 channel-protocol lacp
 channel-group 6 mode active
 !
!*** Port-Chnnel towards the AGN nodes ***
interface Port-channel6
 port-type nni
 switchport trunk allowed vlan 602-605
 switchport mode trunk
 load-interval 30
!
```

G.8032-enabled Ethernet Access Ring

This section discusses about the implementation and configuration details for G.8032-enabled Ethernet access ring. See Figure 6-24.

Figure 6-24 G.8032-enabled Ethernet Access Ring Implementation



The G.8032-enabled Ethernet ring implements two instances for odd and even VLAN numbers, respectively.

In steady-state conditions, the AGN nodes are configured as RPL owners for:

- AGN1: RPL owner on Instance 2 and for odd VLANs. RPL is the ring-facing link.
- AGN2: RPL owner on Instance 1 and even VLANs. RPL is the ring-facing link.

In addition, VLAN 99 is used to carry APS channel traffic for instance 1 and VLAN 199 is used to carry APS channel traffic for instance 2.

Ring PAN Nodes Configuration

The following configuration applies to FANs: CE-903-K0920 / 919 / 0606 / 0607 in the system test topology for a Small Network.

Ring Interfaces Configuration

```
interface TenGigabitEthernet0/0/0
 no ip address
 load-interval 30
 cdp enable
 !
 service instance 99 ethernet
  encapsulation dot1q 99
  rewrite ingress tag pop 1 symmetric
  bridge-domain 99
 !
 service instance 199 ethernet
  encapsulation dot1q 199
  rewrite ingress tag pop 1 symmetric
  bridge-domain 199
 !
interface TenGigabitEthernet0/1/0
 no ip address
 load-interval 30
 cdp enable
 !*** APS channel configuration ***
 service instance 99 ethernet
  encapsulation dot1q 99
```

```
 rewrite ingress tag pop 1 symmetric
 bridge-domain 99
!
service instance 199 ethernet
 encapsulation dot1q 199
 rewrite ingress tag pop 1 symmetric
 bridge-domain 199
!
!
```

Note The full configuration of ring interfaces includes additional service instances for the service VLANs/bridge-domains associated to the G.8032 instances. Such instances are service-specific and only included in the respective Design and Implementation Guides.

G.8032 Instances Configuration

```
ethernet ring g8032 profile ring_profile
 timer wtr 10
 timer guard 100
!
ethernet ring g8032 ring_test
 open-ring
 exclusion-list vlan-ids 1000
 port0 interface TenGigabitEthernet0/0/0
 port1 interface TenGigabitEthernet0/1/0
 !*** Define the Instance 1 and included Vlans ***
 instance 1
  profile ring_profile
  !*** VLANs enabled with G.8032 ***
  inclusion-list vlan-ids 99,106,108,118,301-302,310-311,1001-2000
  aps-channel
   !*** APS Channel Vlans ***
   port0 service instance 99
   port1 service instance 99
  !
 !
 !*** Define Instance 2 and Allowed Vlans ***
 instance 2
  profile ring_profile
  rpl port1 next-neighbor
  inclusion-list vlan-ids 107,109,119,199,351,2001-3000
  aps-channel
   !*** APS Channel Vlans ***
   port0 service instance 199
   port1 service instance 199
  !
 !
!
```

Aggregation Nodes Configuration

The following configuration applies to AGN1 and AGN2, respectively AGN-K1101 and AGN-K1102, in the system test topology for a Small Network.

AGN1

Ring-facing Interfaces Configuration

```
interface TenGigE0/1/0/1
 description To Access Ring
 cdp
 load-interval 30
```

```
 transceiver permit pid all
!
interface TenGigE0/1/0/1.99 l2transport
 encapsulation dot1q 99
!
interface TenGigE0/1/0/1.199 l2transport
 encapsulation dot1q 199
 !
!
```

Note The full configuration of ring interfaces includes additional subinterface for the service VLANs/bridge-domains associated to the G.8032 instances. Such instances are service-specific and only included in the respective Design and Implementation Guides.

G.8032 Instances Configuration

```
ethernet ring g8032 ring_test
  port0 interface TenGigE0/1/0/1
  !
  port1 none
  open-ring
  instance 1
   profile ring_profile
   inclusion-list vlan-ids 99,106,108,118,341,1001-2000
   aps-channel
    port0 interface TenGigE0/1/0/1.99
    port1 none
   !
  !
  instance 2
   profile ring_profile
   !*** RPL For instance 2 VLANs ***
   rpl port0 owner
   inclusion-list vlan-ids 199,107,109,119,351,2001-3000
   aps-channel
    port0 interface TenGigE0/1/0/1.199
    port1 none
   !
  !
 !
```

AGN2

Ring-facing Interfaces Configuration

```
interface TenGigE0/1/0/1
 description To Access Ring
 cdp
 load-interval 30
 transceiver permit pid all
!
interface TenGigE0/1/0/1.99 l2transport
 encapsulation dot1q 99
!
interface TenGigE0/1/0/1.199 l2transport
 encapsulation dot1q 199
 !
!
```

G.8032 Instances Configuration

```
ethernet ring g8032 ring_test
  port0 interface TenGigE0/1/0/1
```

```
!
port1 none
open-ring
instance 1
 profile ring_profile
 !*** RPL for instance 1 Vlans ***
 rpl port0 owner
 inclusion-list vlan-ids 99,106,108,118,210,341,1001-2000
 aps-channel
  port0 interface TenGigE0/1/0/1.99
  port1 none
 !
!
instance 2
 profile ring_profile
 inclusion-list vlan-ids 199,107,109,119,351,2001-3000
 aps-channel
  port0 interface TenGigE0/1/0/1.199
  port1 none
 !
```

nV Access Implementation

The Cisco EPN 4.0 System incorporates nV as an access technology, which allows to manage the entire access network as one virtual system. The nV Satellites devices act as virtual line cards of a centralized nV host, thus appearing as part of a single logical network element. All management and configuration tasks are performed on the nV Host Device only.

Note ASR9000v and ASR901 are implemented as a Satellite Devices. ASR9000v has 4 10gig ports that can be used as ICL and ASR901 has two GigE ports that can be used as ICL.

The nV Hosts are connected to the Satellites over virtual point-to-point connections over any L2 access known as Inter Chassis Links (ICLs) or Fabric links. A Cisco Proprietary Satellite discovery and control protocol is used for discovery and monitoring of satellites from the nV Hosts over the ICLs. Once connectivity is established, Satellite access ports are mapped as local ports at the Host using the naming convention:

```
<port type><Satellite-ID>/<satellite-slot>/<satellite-bay>/<satellite-port>
```

where:

- <port type> is GigabitEthernet for all existing Satellite models
- <Satellite-ID> is the satellite number as defined at the Host
- <satellite-slot>/<satellite-bay>/<satellite-port> are the access port information as known at the Satellite node.

Connectivity between the satellite and the nV Host can be modeled in one of two topologies: as simple ring or L2 Fabric.

In simple ring topologies, the satellites are cascaded using their 10GigabitEthernet ports to form a ring that terminates directly at a pair of nV Hosts.

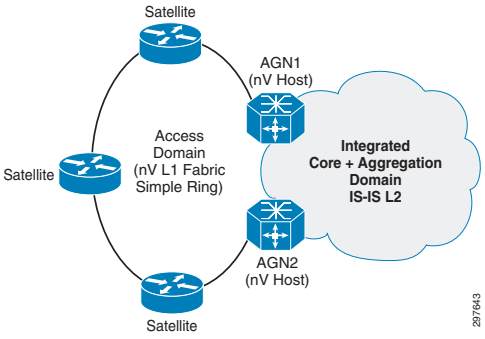
In L2 fabric, connectivity between the Hosts and their Satellite nodes can be achieved over a Layer 2 cloud, implemented as a native Ethernet network or as a EoMPLS transport.

At steady state, the nV hosts load share traffic from different satellites depending on a locally defined host priority. The host active/standby role for a given satellite is negotiated and maintained using ICCP.

Simple Ring nV Access Implementation

Figure 6-25 illustrates how nV satellites are connected to the nV Hosts in simple ring topologies.

Figure 6-25 Simple Ring nV Access Implementation



Configurations apply to nV hosts AGN-K1101 and AGN-K1102 in the system test topology for a Small Network. No configuration is required on the nV satellites.

Note The ASR901 requires a special software image to operate in Satellite mode.

Aggregation Nodes Configuration

AGN1

Fabric Link Interfaces Configuration

```
!*** ICL / Fabric link configuration on nV host ***
interface TenGigE0/2/0/3
 description "NV SAT Simple ring"
 ipv4 point-to-point
 ipv4 unnumbered Loopback10
 nv
  satellite-fabric-link network
   redundancy
    iccp-group 210
   !
   satellite 100
    !*** Define the Access ports of satellite ID 100 ***
    remote-ports GigabitEthernet 0/0/0-30,31-43
   !
   satellite 101
    remote-ports GigabitEthernet 0/0/0-43
   !
   satellite 102
    remote-ports GigabitEthernet 0/0/0-43
   !
  !
 !
!
```

nV Satellite Interfaces Configuration

```
!*** Access port configuration ***
interface GigabitEthernet100/0/0/40
 negotiation auto
 load-interval 30
```

```
!
!*** Sample configurarion of a Satellite UNI for a L2VPN EP-* service ***!
interface GigabitEthernet100/0/0/40.502 l2transport
 encapsulation default
!

ICCP Configuration for Inter-nV Host Synchronization
!***ICCP configuration ***
redundancy
 iccp
  group 210
   member
    neighbor 100.111.11.2
   !
   !*** Ensure same system MAC address is configured on both hosts ***!
   !*** Required for proper discovery of Dual Homed topology ***!
   nv satellite
    system-mac cccc.cccc.cccc
   !
  !
 !
!
```

nV configuration

```
nv
 !*** Define the Satellite ID ***
 satellite 100
  !*** Type of Satellite platform ***
  type asr9000v
   ipv4 address 100.100.1.10
  redundancy
   !*** Define the priority for the Hosts ***
   Host-priority 20
  !
  !*** Satellite chassis serial number ***
  serial-number CAT1729U3BF
  !
 !
 satellite 101
  type asr9000v
  ipv4 address 100.100.1.3
  redundancy
   host-priority 20
  !
  serial-number CAT1729U3BB
 !
 satellite 102
  type asr9000v
  ipv4 address 100.100.1.20
  redundancy
   Host-priority 20
  !
  serial-number CAT1729U3AU
 !
```

AGN2

Fabric Link Interfaces Configuration

```
interface TenGigE0/1/1/3
 description "NV SAT Simple ring"
 ipv4 point-to-point
 ipv4 unnumbered Loopback10
```

```
 nv
  satellite-fabric-link network
   redundancy
    iccp-group 210
   !
   satellite 100
    remote-ports GigabitEthernet 0/0/0-43
   !
   satellite 101
    remote-ports GigabitEthernet 0/0/0-43
   !
   satellite 102
    remote-ports GigabitEthernet 0/0/0-43
   !
  !
 !
!
```

nV Satellite Interfaces Configuration

```
interface GigabitEthernet100/0/0/40
 negotiation auto
 load-interval 30
!
!*** Sample configurarion of a Satellite UNI for a L2VPN EP-* service ***!
interface GigabitEthernet100/0/0/40.502 l2transport
 encapsulation default
!
```

ICCP Configuration for Inter-nV Host Synchronization

```
redundancy
 iccp
  group 210
   member
    neighbor 100.111.11.1
   !
   !*** Ensure same system MAC address is configured on both hosts ***!
   !*** Required for proper discovery of Dual Homed topology ***!
   nv satellite
    system-mac cccc.cccc.cccc
   !
  !
 !
!
```

nV Configuration

```
nv
 satellite 100
  type asr9000v
  ipv4 address 100.100.1.10
  redundancy
   Host-priority 20
  !
  serial-number CAT1729U3BF
 !
 satellite 101
  type asr9000v
  ipv4 address 100.100.1.3
  redundancy
   host-priority 20
  !
  serial-number CAT1729U3BB
 !
```

```
satellite 102
 type asr9000v
 ipv4 address 100.100.1.20
 redundancy
  Host-priority 20
 !
 serial-number CAT1729U3AU
!
```

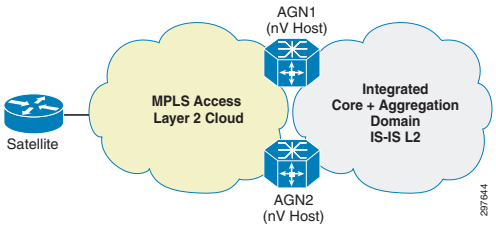
L2 Fabric nV Access Implementation

This section describes the implementation of nV access in L2 Fabric topologies. It focuses on the nV-specific aspects of the solution. For details on the implementation of the L2 Fabric transport, please refer to the nV Access L2 Fabric Transport Implementation, page 6-56.

Figure 6-26 illustrates how nV satellites are connected to the nV Hosts in L2 Fabric topologies.

Note In the case of L2 Fabric, Fabric Links are created as subinterfaces of the Host physical ports, with a dedicated VLAN for each Satellite and host port. Carving of L2 Fabric Links out of bundle interfaces is not supported.

Figure 6-26 L2 Fabric nV Access Implementation



Configurations apply to nV hosts AGN-K1101 and AGN-K1102 in the system test topology for a Small Network. No configuration is required on the nV satellites.

Note The ASR901 requires a special software image to operate in Satellite mode.

Aggregation Nodes Configuration

AGN1

Fabric Link Interfaces Configuration

```
interface TenGigE0/1/1/3
 description "SAT NV host"
 load-interval 30
 transceiver permit pid all
!
interface TenGigE0/1/1/3.210
 ipv4 point-to-point
 ipv4 unnumbered Loopback200
 encapsulation dot1q 210
 nv
  satellite-fabric-link satellite 210
   ethernet cfm
    continuity-check interval 10ms
    !
```

```
   redundancy
    iccp-group 210
   !
   remote-ports GigabitEthernet 0/0/0-9
  !
 !
!
```

nV Satellite Interfaces Configuration

```
interface GigabitEthernet210/0/0/0
 negotiation auto
 load-interval 30
!
!*** Sample L3vpn Config on Host for Satellite 210 access port ***
interface GigabitEthernet210/0/0/0.49
 vrf RES-VPN
 ipv4 address 51.1.1.1 255.255.255.252
 encapsulation dot1q 49
!
```

ICCP Configuration for Inter-nV Host Synchronization

```
!*** ICCP configuration ***
redundancy
 iccp
  group 210
   member
    neighbor 100.111.11.2
   !
   nv satellite
    system-mac cccc.cccc.cccc
   !
  !
 !
!
```

nV Configuration

```
!*** Define the Satellite ID 210 and type of platform ASR 901 ***
nv
 satellite 210
  type asr901
  ipv4 address 30.30.30.10
  redundancy
   host-priority 17
  !
  serial-number CAT1650U00D
 !
!
```

AGN2

Fabric Link Interfaces Configuration

```
interface TenGigE0/1/0/3
 description "SAT NV host"
 load-interval 30
 transceiver permit pid all
!
interface TenGigE0/1/0/3.211
 ipv4 point-to-point
 ipv4 unnumbered Loopback200
 encapsulation dot1q 211
 nv
```

```
  satellite-fabric-link satellite 210
   ethernet cfm
    continuity-check interval 10ms
   !
   redundancy
    iccp-group 210
   !
   remote-ports GigabitEthernet 0/0/0-9
  !
 !
!
```

nV Satellite Interfaces Configuration

```
interface GigabitEthernet210/0/0/0
 negotiation auto
 load-interval 30
!
!*** Sample L3vpn Config on Host for Satellite 210 access port ***
interface GigabitEthernet210/0/0/0.49
 vrf RES-VPN
 ipv4 address 51.1.1.1 255.255.255.252
 encapsulation dot1q 49
!
```

ICCP Configuration for Inter-nV Host Synchronization

```
redundancy
 iccp
  group 210
   member
    neighbor 100.111.11.1
   !
   nv satellite
    system-mac cccc.cccc.cccc
   !
  !
```

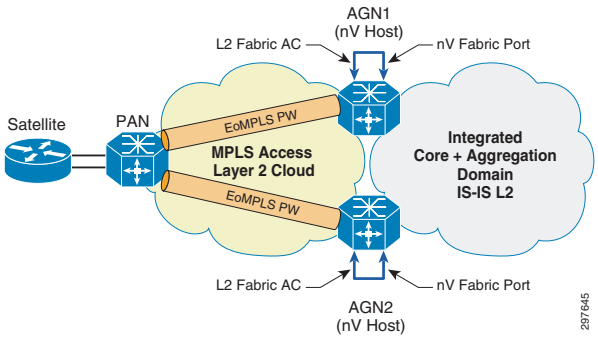
nV configuration

```
nv
 satellite 210
  type asr901
  ipv4 address 30.30.30.10
  redundancy
   host-priority 16
  !
  serial-number CAT1650U00D
 !
!
```

nV Access L2 Fabric Transport Implementation

This section describes the implementation of the L2 transport network that provides connectivity between the Satellites and the Hosts for L2 Fabric-based nV access. See Figure 6-27.

Figure 6-27 nV Access L2 Fabric transport implementation



The nV L2 Fabric transport is implemented as a MPLS-enabled access network terminating directly at the nV host nodes. The Ethernet connectivity between the satellite and the hosts is achieved using Ethernet over MPLS PWs originated from a PAN node and terminating on attachment circuits at the hosts. Such attachment circuits connect the nV fabric ports at the host to the L2 Fabric cloud over an external loopback cable.

Alternatively, the L2 Fabric could have been terminated on a downstream device to the nV host and the nV host fabric ports could be directly connected to it.

Configurations apply to nV hosts, AGN-K1101 and AGN-K1102, and PAN, PAN-K1404, in the system test topology for a Small Network.

Pre-Aggregation Node Configuration

```
!*** Interface towards the nV Sattellite ***
interface GigabitEthernet0/3/0
description "to 901 SAT gig0/11"
mtu 1536
no ip address
negotiation auto
no keepalive
!*** PW to AGN1 nV Host ***
service instance 210 ethernet
  encapsulation dot1q 210
  xconnect 100.111.11.1 210 encapsulation mpls
!
!*** Interface towards the nV Sattellite ***
interface GigabitEthernet0/3/7
description "to 901 SAT gig0/10"
no ip address
negotiation auto
no keepalive
!*** PW to AGN2 nV Host ***
service instance 211 ethernet
  encapsulation default
  xconnect 100.111.11.2 211 encapsulation mpls
!
```

Aggregation Node Configuration - nV host: AGN1

```
!*** Interface connecting to AGN1 nV Fabric Link ports***
interface TenGigE0/1/1/2
description "to AGN Fabric Link interface"
mtu 1546
transceiver permit pid all
!
interface TenGigE0/1/1/2.210 l2transport
encapsulation dot1q 210
```

```
!
!*** PW to the Access node connected to nV sttellite ***
l2vpn
xconnect group NV
  p2p test_nv
   interface TenGigE0/1/1/2.210
   neighbor ipv4 100.111.14.4 pw-id 210
   !
  !
 !
!
```

Aggregation Node Configuration - nV host: AGN2

```
!*** Interface connecting to AGN2 nV Fabric Link ports ***
interface TenGigE0/1/0/2
description "SAT NV XCONNECT"
load-interval 30
transceiver permit pid all
!
interface TenGigE0/1/0/2.211 l2transport
encapsulation default
!
!*** PW to the Access node connected to nV sttellite ***
l2vpn
xconnect group NV
  p2p test_nv
   interface TenGigE0/1/0/2.211
   neighbor ipv4 100.111.14.4 pw-id 211
   !
  !
```

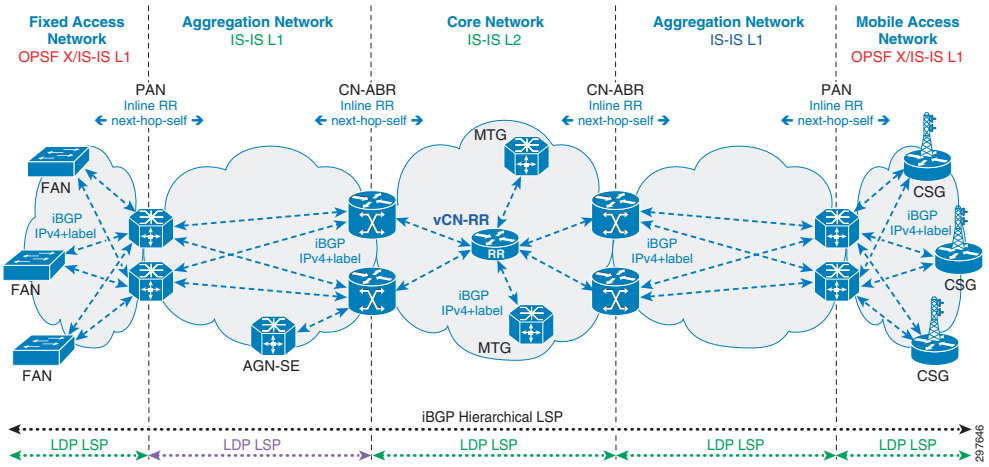
Large Network Transport Multiple Area IGP Implementation

This section focuses on the network implementation for the transport models associated to a large network multiple area IGP with either IP/MPLS or Non-IP/MPLS Access.

MPLS Access

This option assumes an end-to-end labeled BGP transport where the access, aggregation, and core domains 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 a remote domain acts as a labeled BGP PE and runs iBGP IPv4 unicast+label with its corresponding local RRs.

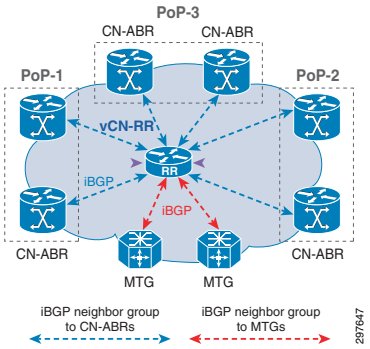
Figure 6-28 Unified MPLS Transport for Large Network Multiple Area IGP Design with Labeled BGP Access



Core Route Reflector Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the centralized CN-RR.

Figure 6-29 Centralized Virtual Core Route Reflector (vCN-RR)



Interface Configuration

```
interface Loopback0
  description Global Loopback
  ipv4 address 100.111.15.50 255.255.255.255
!
!***Core Interface***
interface GigabitEthernet0/0/0/0
  description To CN-K0201 Gig0/2/0/1
  cdp
  ipv4 address 10.2.1.33 255.255.255.254
  negotiation auto
  load-interval 30
!
```

IGP/LDP Configuration

```
router isis core
```

```
  set-overload-bit on-startup 360
  net 49.0100.1001.1100.4003.00
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    address-family ipv4 unicast
    !
  !
  !***Core Interface***
  interface GigabitEthernet0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 100
    !
  !

mpls ldp
  router-id 100.111.15.50
  graceful-restart
  log
    neighbor
    graceful-restart
  !
  mldp
  !
  interface GigabitEthernet0/0/0/0
```

BGP Configuration

```
router bgp 1000
  nsr
  bgp default local-preference 50
  bgp router-id 100.111.15.50
  bgp cluster-id 1000
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  address-family ipv4 unicast
  !***BGP add-path configuration for BGP Edge FRR***!
    additional-paths receive
    additional-paths send
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 1000
    network 100.111.4.3/32
    allocate-label all
  !
  address-family vpnv4 unicast
  !***session group for iBGP clients (AGNs and MTGs)***
  session-group intra-as
    remote-as 1000
    password encrypted 082D4D4C
    update-source Loopback0
```

```
!
!***MTG neighbor group***
neighbor-group mtg
  use session-group intra-as
  address-family ipv4 labeled-unicast
    route-reflector-client
    maximum-prefix 150000 85 warning-only
    soft-reconfiguration inbound always
  !
  address-family vpnv4 unicast
  !
  address-family ipv6 labeled-unicast
    route-reflector-client
    maximum-prefix 150000 85 warning-only
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
    route-reflector-client
  !
!
!***AGN neighbor group***
neighbor-group agn
  use session-group intra-as
  address-family ipv4 labeled-unicast
    route-reflector-client
    soft-reconfiguration inbound always
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
    route-reflector-client
  !
  address-family ipv6 mvpn
    route-reflector-client
  !
!
!***PAN neighbor group***
neighbor-group pan
  use session-group intra-as
  address-family ipv4 labeled-unicast
    route-reflector-client
    soft-reconfiguration inbound always
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
!
!***MTG-K1501***
neighbor 100.111.15.1
  use neighbor-group mtg
!
!***MTG-K1502***
neighbor 100.111.15.2
  use neighbor-group mtg
!
!***PANs***
neighbor 100.111.5.7
  use neighbor-group pan
!
neighbor 100.111.5.8
```

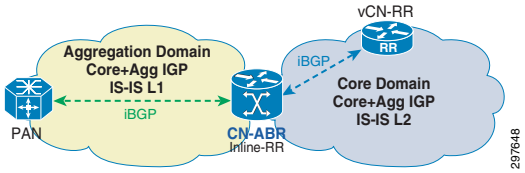
```
    use neighbor-group pan
  !
  neighbor 100.111.9.21
    use neighbor-group pan
  !
  neighbor 100.111.9.22
    use neighbor-group pan
  !
  neighbor 100.111.14.3
    use neighbor-group pan
  !
  neighbor 100.111.14.4
   use neighbor-group pan
  !
  !***AGNs***
  neighbor 100.111.11.1
    use neighbor-group agn
  !
  neighbor 100.111.11.2
    use neighbor-group agn
  !
!
route-policy add-path-to-ibgp
  set path-selection backup 1 advertise install
end-policy

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

route-policy BGP_Egress_Transport_Filter
  !***20:20 = FAN_Community for Fixed Access Nodes***
  if community matches-any (20:20) then
    pass
  else
    !***10:10 = RAN_Community for CSGs***
    if community matches-any (10:10) then
      drop
    else
      pass
    endif
  endif
end-policy
```

Note Please refer to BGP Transport Control Plane, page 3-14 for a detailed explanation of how egress filtering is done at the CN-RR for constraining IPv4+label routes from remote RAN access regions.

Mobile Transport Gateway Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs from the MPC to the aggregation and access domains. See Figure 6-31.

Figure 6-30 Mobile Transport Gateway (MTG)



Interface Configuration

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

IGP Configuration

```
router isis core
  set-overload-bit on-startup 250
  net 49.0100.1001.1101.5001.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  !***Core-facing Interface***
  interface TenGigE0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
```

```
    address-family ipv4 unicast
      fast-reroute per-prefix
      mpls ldp sync
    !
  !
  !***Core-facing Interface***
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      mpls ldp sync
    !
!
mpls ldp
  router-id 100.111.15.1
  discovery targeted-hello accept
  nsr
  graceful-restart
  session protection
  igp sync delay 10
  log
    neighbor
    graceful-restart
    session-protection
    nsr
  !
  mldp
    logging notifications
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
!
```

BGP Configuration

```
router bgp 1000
  nsr
  bgp router-id 100.111.15.1
  bgp update-delay 360
  bgp redistribute-internal
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    !***BGP add-path to receive multiple paths from CN-RR***
    additional-paths receive
    additional-paths selection route-policy add-path-to-ibgp
    !***Color loopback prefix in BGP with MSE and IGW Communities***
    network 100.111.15.1/32 route-policy MSE_IGW_Community
    allocate-label all
  !
  address-family vpnv4 unicast
    <SNIP>
  !
  address-family ipv6 unicast
    redistribute connected
    allocate-label all
  !
  address-family vpnv6 unicast
  !
```

```
  address-family ipv4 mvpn
  !
  session-group intra-as
    remote-as 1000
    password encrypted 011F0706
    update-source Loopback0
  !
  neighbor-group cn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family ipv6 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
    !
  !
  !***CN-RR***
  neighbor 100.111.15.50
    use neighbor-group cn-rr
  !

community-set IGW_Community
  3001:3001
end-set
!
community-set MSE_Community
  1001:1001
end-set
!
route-policy MSE_IGW_Community
  set community MSE_Community
  set community IGW_Community additive
end-policy

community-set PASS_Community
  !***Common RAN community***
  10:10,
  !***MSE & MPC community***
  1001:1001,
  !***FSE community***
  2001:2001,
  !***IGW community***
  3001:3001
end-set
!
!***Set communities to pass***
route-policy BGP_Ingress_Transport_Filter
  if community matches-any PASS_Community then
    pass
  else
    drop
  endif
end-policy
!
```

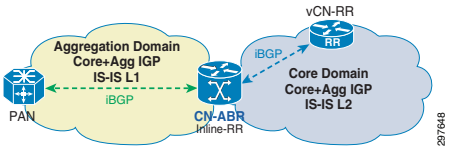
```
route-policy add-path-to-ibgp
  set path-selection backup 1 install
  end-policy
```

Core Area Border Router Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the core ABRs. The multi-level IGP organization between the core and aggregation is based on segmenting the core network in IS-IS Level 2 and the aggregation networks in IS-IS Level 1. The CN-ABR is an IS-IS L1-L2 node, where core-facing interfaces are IS-IS L2 links, local aggregation network-facing interfaces are IS-IS L1 links, and the interface connecting the redundant ABR is an IS-IS L1/L2 link.

The CN-ABR provides inline-RR functionality between the core and aggregation domains. For routes reflected to the core domain, all updates are sent with next hop self (NHS) in order to set the CN-ABR as the next-hop (NH) router for any transport from the core domain to the local aggregation domain. For routes reflected to the local aggregation domain, setting NHS is not so absolute. All prefixes received from the core domain reflected towards the local aggregation domain must have NHS set. However, all prefixes received from the local aggregation domain must be reflected with next hop unchanged (NHU) in order to allow for optimum transport of services between PANs in the local aggregation domain. If NHS is set on all reflected prefixes, then a service transported between two local PANs would have to route through the CN-ABR, since it's the NH router. By leaving NHU, then services may be transported directly between the local PANs. This selective NHS is accomplished through a route-policy that applies NHS only to updates received from the CN-RR. See Figure 6-31.

Figure 6-31 Core Node Area Border Router (CN-ABR)



Interface Configuration

```
!
!***Router ID Loopback***
interface Loopback0
  ipv4 address 100.111.11.1 255.255.255.255
!
!***Redundant-ABR Interface***
interface TenGigE0/0/0/0
  description To AGN-9006-K1102 TenGigE0/0/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.11.1.0 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  transceiver permit pid all
!
!***Aggregation-facing Interface***
interface TenGigE0/0/0/1
  description To PAN-903-K0922 Ten0/1/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.9.22.3 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
```

```
  transceiver permit pid all
!
!***Core-facing Interface***
interface TenGigE0/0/0/2
  description To CN-ASBR-CRS8-K0401 T0/0/0/2
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.2.1.11 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  transceiver permit pid all
!
```

IGP/LDP Configuration

```
router isis core
  set-overload-bit on-startup 360
  net 49.0100.1001.1101.1001.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
    !***Disable default IS-IS L1 to L2 redistribution***
    propagate level 1 into level 2 route-policy drop-all
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
      tag 1000
    !
  !
  !***L1/L2 Link to Redundant ABR***
  interface TenGigE0/0/0/0
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      mpls ldp sync
    !
  !
  !***L1 Link to Aggregation***
  interface TenGigE0/0/0/1
    circuit-type level-1-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      mpls ldp sync
    !
  !
  !***L2 Link to Core***
  interface TenGigE0/0/0/2
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
```

```
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      mpls ldp sync
    !
    !
!
!***Route policy to disable IS-IS L1 to L2 redistribution***
route-policy drop-all
  drop
end-policy
!
mpls ldp
  router-id 100.111.11.1
  discovery targeted-hello accept
  graceful-restart
  igp sync delay 10
  log
    neighbor
    graceful-restart
  !
  mldp
    logging notifications
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
  interface TenGigE0/0/0/2
```

BGP Configuration

```
router bgp 1000
  nsr
  bgp router-id 100.111.11.1
  !***Redundant ABRs K1101 and K1102 have a cluster ID 1001 to prevent loops***
  bgp cluster-id 1001
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    !***BGP add-path to receive multiple paths from CN-RR***
    additional-paths receive
    additional-paths selection route-policy add-path-to-ibgp
    !***Color Service loopback prefix in BGP with CN_ABR_Community***
    network 100.111.11.1/32 route-policy CN_ABR_Community
    allocate-label all
  !
  address-family vpnv4 unicast
  !
  address-family ipv6 unicast
    allocate-label all
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  address-family ipv6 mvpn
  !
  !***session group for iBGP clients***
  session-group intra-as
    remote-as 1000
    password encrypted 03085A09
    cluster-id 1001
```

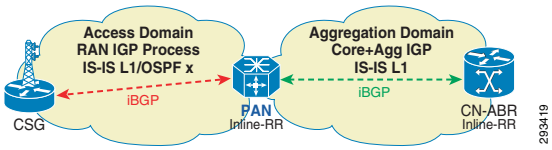
```
    update-source Loopback0
    graceful-restart
  !
  !***iBGP neighbor group for CN-RR***
  neighbor-group cn-rr
    use session-group intra-as
    !***Address family for RFC 3107 based transport***
    address-family ipv4 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      !***next-hop-self to insert into data path***
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family ipv6 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
    !
  !***iBGP neighbor group for local PANs***
  neighbor-group agg
    use session-group intra-as
    !***set next-hop to self for only reflected prefixes from CN-RR***
    address-family ipv4 labeled-unicast
      route-reflector-client
      route-policy SET_NEXT_HOP_SELF out
    !
    address-family ipv6 labeled-unicast
      route-reflector-client
      route-policy SET_NEXT_HOP_SELF out
    !
  !
  !
  !***CN-RR***
  neighbor 100.111.15.50
    use neighbor-group cn-rr
  !
  !***PAN K1403***
  neighbor 100.111.15.5
    use neighbor-group agg
  !
  !***PAN K1404***
  neighbor 100.111.14.4
    use neighbor-group agg
  !
!

!***Only set NHS on updates from CN-RR***
route-policy SET_NEXT_HOP_SELF
  if source in (100.111.15.50) then
      set next-hop self
    else
      pass
    endif
end-policy

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

```
end-policy
!

!
route-policy CN_ABR_Community
  set community CN_ABR_Community
  end-policy
!
community-set CN_ABR_Community
  1000:1000
  end-set
!
```

Pre-Aggregation Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs in the aggregation network. The PANs are ABRs between the aggregation and RAN access domains. The segmentation between the two domains is achieved by enabling two different IGP processes on the PANs. The first process is the core/aggregation IGP process and the second process is another independent RAN IGP process. All CSGs subtending from the same pair of PANs are part of this RAN IGP process. See Figure 6-32.

Figure 6-32 Pre-Aggregation Node (PAN)



Interface Configuration

```
!***Loopback for core IGP process***
interface Loopback0
  ip address 100.111.14.3 255.255.255.255
!
!***Loopback for RAN IGP process***
interface Loopback100
  ip address 100.111.144.3 255.255.255.255

mpls ldp router-id Loopback0 force

!***Interface to Redundant PAN***
!***VLANs to close Core and RAN IGP processes***
interface TenGigabitEthernet0/0/0
  description To PAN-K1404 Ten0/0/0
  no ip address
  load-interval 30
  service instance 100 ethernet
    encapsulation dot1q 100
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100
  !
    service instance 200 ethernet
    encapsulation dot1q 200
    rewrite ingress tag pop 1 symmetric
    bridge-domain 200
!
!***Core IGP VLAN***
interface BDI100
```

```
  ip address 10.14.3.0 255.255.255.254
  ip router isis core
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  isis network point-to-point
  isis metric 10
  isis csnp-interval 10
!
!***RAN IGP VLAN***
!***Ignore ISIS statements if OSPF used for RAN IGP***
interface BDI200
  ip address 10.14.3.4 255.255.255.254
  ip router isis ran
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  isis network point-to-point
  isis metric 10
  isis csnp-interval 10
!
!***RAN Access Ring-facing interface***
interface GigabitEthernet0/3/1
  description To CSG-K1322 G0/11
  no ip address
  load-interval 30
  carrier-delay msec 0
  negotiation auto
  synchronous mode
  service instance 10 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    bridge-domain 10
  !
!
!***Ignore ISIS statements if OSPF used for RAN IGP***
interface BDI10
  description To CSG-K1322 G0/11
  ip address 10.13.22.1 255.255.255.254
  ip router isis ran
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
  isis network point-to-point
  isis metric 100
  hold-queue 1500 in
  hold-queue 2000 out
!
```

Interface TenGigabitEthernet0/0/0 is the link that connects to the redundant PAN. Since this configuration is running two independent IGP processes on the PANs, you need to make sure you provide a closed path for both processes. This is enabled by configuring VLANs on the common link between the two PANs. Here VLAN 100 is used to close the core IGP process and VLAN 200 to close the RAN IGP process.

Note PAN K1403's LDP ID Loopback0 is in the core IS-IS process and not in the RAN IS-IS IGP process. The command mpls ldp discovery transport-address 100.111.144.7 changes the transport address to Loopback100 for LDP discovery out of the RAN access ring-facing interface G0/11.

Core-Aggregation LDP/IGP Process Configuration

```
router isis core
  net 49.0100.1001.1101.4003.00
  !***IS-IS Level-1***
  is-type level-1
  ispf level-1
  metric-style wide
  fast-flood
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 50 200
  no hello padding
  log-adjacency-changes
  passive-interface Loopback0
  bfd all-interfaces
!
```

Depending on the operator, the RAN IGP process could either be a IS-IS process at Level 2 with the access domains at Level 1, or a OSPF process with the PAN in area 0 with the access domains in totally-stubby areas. The following sections describe configurations for both options.

Option 1: OSPF as RAN IGP Process

This shows the configuration if OSPF is used as the choice of RAN IGP process.

```
router ospf 1
  router-id 100.111.144.3
  ispf
  timers throttle spf 50 50 5000
  timers throttle lsa 10 20 5000
  timers lsa arrival 10
  timers pacing flood 5
  !***Loopback100 interface for RAN IGP***
  network 100.111.144.3 0.0.0.0 area 0
  !***VLAN 200 trunked on redundant PAN interface***
  network 10.14.3.4 0.0.0.1 area 0
  !***RAN Access facing interface***
  network 10.13.22.1 0.0.0.1 area 0
  !***Make area 10 totally stub area***
  area 10 stub no-summary
  bfd all-interfaces
!
```

Option 2: IS-IS as RAN IGP Process

This shows the configuration if IS-IS is used as the choice of RAN IGP process.

```
router isis ran
  net 49.0100.1001.1101.4403.00
  !***IS-IS Level-1-2***
  is-type level-1-2
```

```
  ispf level-1-2
  metric-style wide
  fast-flood
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 50 200
  no hello padding
  log-adjacency-changes
  !***Loopback100 interface for RAN IGP***
  passive-interface Loopback100
  bfd all-interfaces
!
```

BGP Configuration

```
!
router bgp 1000
  bgp router-id 100.111.14.3
  bgp cluster-id 1403
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  !***Peer group for CSGs in local RAN network***
  neighbor csg peer-group
  neighbor csg remote-as 1000
  neighbor csg password lab
  !***RAN IGP Loopback100 used as source***
  neighbor csg update-source Loopback100
  !***Peer group for CN-ABRs***
  neighbor abr peer-group
  neighbor abr remote-as 1000
  neighbor abr password lab
  !***Core IGP Loopback0 used as source***
  neighbor abr update-source Loopback0
  neighbor 100.111.11.1 peer-group abr
  neighbor 100.111.11.2 peer-group abr
  neighbor 100.111.13.22 peer-group csg
  neighbor 100.111.13.23 peer-group csg
  neighbor 100.111.13.24 peer-group csg
  !
  !***Address family for RFC 3107 based transport***
  address-family ipv4
    bgp redistribute-internal
    !***Color Loopback 0 with Aggregation Community***
    network 100.111.14.3 mask 255.255.255.255 route-map AGG_Community
    neighbor abr send-community
    !***Set NHS to insert into data path***
    neighbor abr next-hop-self all
    !***send labels with BGP routes***
    neighbor abr send-label
    neighbor csg send-community
    !***Filter PAN Community towards CSGs***
    neighbor csg route-map BGP_Egress_Transport_Filter out
    neighbor csg route-reflector-client
    neighbor csg next-hop-self all
    neighbor csg send-label
    neighbor 100.111.11.1 activate
    neighbor 100.111.11.2 activate
    neighbor 100.111.13.22 activate
    neighbor 100.111.13.23 activate
```

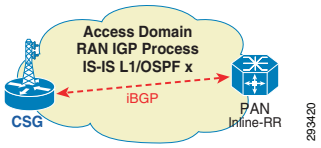
```
    neighbor 100.111.13.24 activate
  exit-address-family
  !
  address-family vpnv4
  !
  address-family rtfilter unicast
  !

!***100:100 is the common aggregation community.***
!***100:101 is the community identifying this PAN as being in metro-1, location-1.***
route-map AGG_Community permit 10
  set community 100:100 100:101

route-map BGP_Egress_Transport_Filter permit 10
!***Allows loopbacks for MTG endpoints***
  match community MTG_Community
  set mpls-label
!
route-map BGP_Egress_Transport_Filter permit 20
!***Allows loopbacks needed for wireline services***
  match community WL_Community
  set mpls-label
!
ip bgp-community new-format
ip community-list standard MTG_Community permit 1001:1001
ip community-list standard WL_Community permit 20:20
```

Cell Site Gateway Configuration

The IGP organization between the aggregation and RAN access networks is based on running two different IGP processes on the PANs as discussed in the previous section. The first process is the core-aggregation IGP process and the second process is an independent RAN IGP process for the mobile RAN network. The CSGs in all access ring networks and hub-and-spoke connected nodes subtending from the same pair of PANs are part of this RAN IGP process.

Depending on the operator, the RAN IGP process could either be an IS-IS process at Level 1 or an OSPF process in Area 0. Configurations for both options are shown below. See Figure 6-33.

Figure 6-33 Cell Site Gateway (CSG)



Interface Configuration

```
!
interface Loopback0
 ip address 100.111.2.8 255.255.255.255
 ipv6 address 2001:100:111:2::8/128
 ipv6 enable
 isis tag 1500!
!***NNI facing PAN***
interface TenGigabitEthernet0/0/3
 description "to gig0/2/1 K1401"
 no ip address
 load-interval 30
 carrier-delay msec 0
 synchronous mode
```

```
 cdp enable
 service instance 30 ethernet
  encapsulation dot1q 30
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
 !
!
!***Ignore ISIS configurations if OSPF used for RAN IGP***

interface BDI30
 ip address 10.2.6.0 255.255.255.254
 ip router isis agg-acc
 ip pim sparse-mode
 load-interval 30
 ipv6 address 2001:10:2:6::/127
 ipv6 enable
 ipv6 router isis agg-acc
 mpls ip
 mpls ldp igp sync delay 30
 bfd interval 50 min_rx 50 multiplier 3
 isis circuit-type level-1
 isis network point-to-point

!***NNI facing next CSG***
interface TenGigabitEthernet0/0/4
 no ip address
 load-interval 30
 carrier-delay msec 0
 synchronous mode
 cdp enable
 service instance 20 ethernet V20
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  service-policy input PMAP-UNI-I
  service-policy output PMAP-uW-NNI-P-E
  bridge-domain 20

!***Ignore ISIS configurations if OSPF used for RAN IGP***

interface BDI20
 ip address 10.2.6.2 255.255.255.254
 ip router isis agg-acc
 ip pim sparse-mode
 ipv6 address 2001:10:2:6::2/127
 ipv6 enable
 ipv6 router isis agg-acc
 mpls ip
 mpls ldp igp sync delay 30
 bfd interval 50 min_rx 50 multiplier 3
 isis circuit-type level-1
 isis network point-to-point
 isis metric 100
 !
```

Option 1: OSPF as RAN IGP Process

This section shows the CSG configuration if OSPF is used as the RAN IGP.

```
router ospf 1
  router-id 100.111.2.8
  ispf
  timers throttle spf 50 50 5000
  timers throttle lsa 510 50 200
```

```
 timers lsa arrival 10
 timers pacing flood 5
 passive-interface Loopback0
 network 10.13.0.0 0.0.255.255 area 10
 network 100.111.23.0 0.0.0.255 area 10
 area 10 stub no-summary
 bfd all-interfaces
```

Option2: IS-IS as RAN IGP Process

This section shows the CSG configuration if IS-IS is used as the RAN IGP.

```
router isis agg-acc
 net 49.0100.1001.1102.0008.00
 is-type level-1
 ispf level-1
 metric-style wide
 fast-flood 10
 ip route priority high tag 1500
 set-overload-bit on-startup 120
 max-lsp-lifetime 3600
 lsp-refresh-interval 1800
 spf-interval 5 50 200
 prc-interval 5 50 200
 lsp-gen-interval 5 50 200
 no hello padding
 log-adjacency-changes
 fast-reroute per-prefix level-1 all
 fast-reroute remote-lfa level-1 mpls-ldp
 passive-interface Loopback0
 bfd all-interfaces
 !
 address-family ipv6
  multi-topology
 exit-address-family
 mpls ldp sync
!
!
```

BGP Configuration

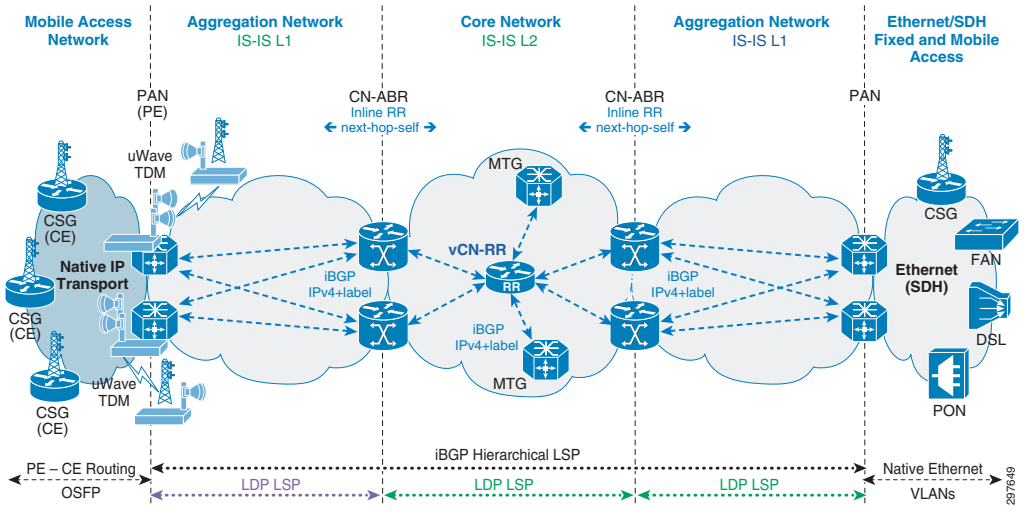
```
!
router bgp 101
 bgp router-id 100.111.2.8
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor pan peer-group
 neighbor pan remote-as 101
 neighbor pan password lab
 neighbor pan update-source Loopback0
 neighbor 100.111.14.1 peer-group pan
 neighbor 100.111.14.2 peer-group pan
 !
  address-family ipv4
  bgp additional-paths install
  bgp recursion host
  bgp nexthop trigger delay 6
    !***Advertise Loopback-0 with CSG Community***
network 100.111.2.8 mask 255.255.255.255 route-map ACC_RAN_FAN_Community
    redistribute connected
```

```
    neighbor pan send-community
    neighbor pan aigp
    neighbor pan next-hop-self
    neighbor pan send-label
    !***Import routes based on the defined communities***
neighbor 100.111.14.1 route-map BGP_Ingress_Transport_Filter in
    neighbor 100.111.14.3 activate
    neighbor 100.111.14.4 activate
  exit-address-family
  !
  address-family vpnv4
  !
  address-family rtfilter unicast
  exit-address-family
  !

!***10:10 is the common CSG community.***
!***10:111 is the common CSG community for ASR920***
!***10:1051 is the community identifying this CSG as being in metro-1, location-51.***
route-map ACC_RAN_FAN_Community permit 10
set community 10:10 10:105 10:111
```

Non-MPLS Access

In this model, the core and aggregation networks are integrated with unified MPLS LSPs by extending labeled BGP from the core to the PANs in the aggregation domain. Any node in the network that requires inter-domain LSPs to reach nodes in a remote domain acts as a labeled BGP PE and runs BGP labeled-unicast with the core RR. See Figure 6-34.

Figure 6-34 Unified MPLS Transport for Multiple Area IGP Design with non-MPLS Access



Note The network infrastructure organization of this model at the top layers of network, namely the core and aggregation domains, is exactly the same as that defined in MPLS Access, page 6-3. The difference here is that the labeled BGP transport spans only the core and aggregation networks and does not extend to the RAN access. Instead, the end-to-end unified MPLS LSP is extended into the RAN access with selective redistribution between labeled BGP and the RAN access domain IGP at the PAN. Please refer to MPLS Access, page 6-58 for configuration details on the Core Route Reflector, Mobile Transport Gateway, and Core ABR, because the same configuration also applies to this model.

In this model, the access network could be one of the following options:

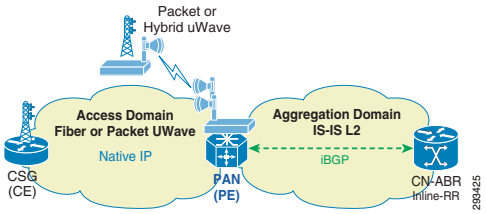
- CSGs in point-to-point or ring topologies over fiber or packet microwave running native IP transport and supporting 3G/LTE services. In this case, the CSGs act as CEs and PANs are the L3 MPLS VPN PEs enabling the backhaul. The BTS or ATM NodeBs can connect to the PANs with TDM microwave for 2G and 3G ATM-based services. Here the PANs enable the L2 MPLS VPN service with pseudowire-based circuit emulation for backhaul to the BSC/RNC.
- Point-to-point topologies over GPON fiber access, supporting mobile services over Ethernet connections transported via GPON. In this case, the PANs provide service edge functionality for the services from the CSGs connected via PON, and also connect the services to the proper L2VPN or L3VPN service backhaul mechanism.

In either scenario, the MPLS services are always enabled by the PANs in the aggregation network.

Pre-Aggregation Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs in the aggregation network.

Figure 6-35 Pre-Aggregation Node (PAN)



Interface Configuration

```
interface Loopback0
  ip address 100.111.14.3 255.255.255.255
!
!***Redundant PAN interface***
interface TenGigabitEthernet0/0/0
  description To PAN-K1404::TenGigabitEthernet0/0/0
  ip address 10.14.3.0 255.255.255.254
  ip router isis core
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis network point-to-point
  isis metric 10
  isis csnp-interval 10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
!***Core-facing interface***
interface TenGigabitEthernet0/1/0
  description To AGN-K1102::T0/0/0/1
  ip address 10.11.2.1 255.255.255.254
  ip router isis core
  load-interval 30
  mpls ip
```

```
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis circuit-type level-2-only
  isis network point-to-point
  isis metric 10
  isis csnp-interval 10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
!***Interface toward native IP CE ring in MPLS VPN RFS***
!***Shown here for reference. Not part of Unified MPLS config.***
interface GigabitEthernet0/3/0
  description To CSG-901-K1319
  vrf forwarding RFS
  ip address 10.13.19.1 255.255.255.254
  ip ospf network point-to-point
  load-interval 30
  negotiation auto
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  hold-queue 350 in
  hold-queue 2000 out
!
```

IGP/LDP Configuration

```
router isis agg-acc
  net 49.0100.1001.1101.4004.00
  !***PAN is a IS-IS Level-1-2 node***
  ispf level-1-2
  metric-style wide
  fast-flood
  set-overload-bit on-startup 180
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 5 200
  no hello padding
  log-adjacency-changes
  nsf cisco
  passive-interface Loopback0
  bfd all-interfaces
  mpls ldp sync

mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
```

BGP Configuration

```
router bgp 1000
  bgp router-id 100.111.14.3
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  !***Peer group for CN-ABRs***
  neighbor abr peer-group
```

```
  neighbor abr remote-as 1000
  neighbor abr password lab
  !***Core IGP Loopback0 used as source***
  neighbor abr update-source Loopback0
  neighbor 100.111.11.1 peer-group abr
  neighbor 100.111.11.2 peer-group abr
  !
  !***Address family for RFC 3107 based transport***
  address-family ipv4
    bgp redistribute-internal
    !***Color Loopback 0 with Aggregation Community***
    network 100.111.14.3 mask 255.255.255.255 route-map AGG_Community
    neighbor abr send-community
    !***Set NHS to insert into data path***
    neighbor abr next-hop-self all
    !***send labels with BGP routes***
    neighbor abr send-label
    !***CN-ABRs***
    neighbor 100.111.11.1 activate
    neighbor 100.111.11.2 activate
  exit-address-family
  !
  address-family ipv4 vrf RFS
    !
  exit-address-family
  !
!

route-map AGG_Community permit 10
  !***100:100 is the common aggregation community***
  !***100:101 identifies this PAN as being in metro-1, location-1***
  set community 100:100 100:101
```

Access Network Implementation Configuration

Implementation of the access network is common for Large Network architectures across Single-AS or Multi-Area aggregation and core routing design models. Please refer to Large Network Non-IP/MPLS Access Network Implementation, page 6-124 for details on the implementation of Non-IP/MPLS access networks with the Large Networks.

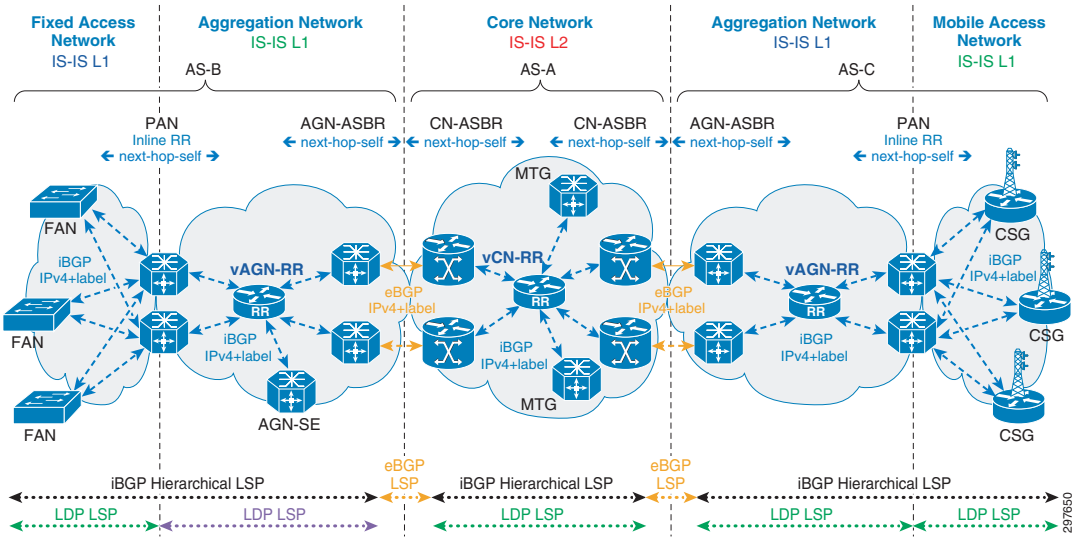
Large Network Transport Inter-AS Implementation

This section describes the implementation of a large network deployment of the Cisco EPN System architecture, which uses a separate BGP autonomous system for the core domain and for each aggregation and access domain. This section details the base deployment aspects of the Inter-AS model with labeled BGP access and then describes the variations for deployment with non-MPLS access networks.

MPLS Access

This option assumes an end-to-end labeled BGP transport where 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 or FANs in the access domain, or SENs in the aggregation domain. Any node in the network that requires inter-domain LSPs to reach nodes in a remote domain acts as a labeled BGP PE, and runs BGP labeled-unicast with its corresponding local RRs. See Figure 6-36.

Figure 6-36 Unified MPLS Transport for Inter-AS Design with Labeled BGP Access



The CN-ASBRs are labeled BGP ASBR in the core autonomous system. The CN-ASBR uses iBGP-labeled unicast sessions to peer with the centralized CN-RR within the core autonomous system, and eBGP-labeled unicast sessions to peer with the AGN-ASBRs in the neighboring aggregation autonomous systems. The CN-ASBRs are inserted into the data path by setting NHS on all iBGP updates toward the local CN-RRs, and eBGP updates toward the neighboring aggregation ASBRs, thus enabling inter-domain LSPs.

Gateway routers, such as MTGs providing connectivity to MPC or IGWs providing access to the Internet, are labeled BGP PEs in the core. iBGP labeled-unicast sessions are established with the CN-RR and loopbacks are advertised into iBGP labeled-unicast with a common BGP community representing the respective function: MSE BGP community for MTGs, IGW BGP community for IGWs.

The AGN-ASBRs are labeled BGP ASBR in the aggregation autonomous system. iBGP labeled-unicast sessions are established with the centralized AGN-RR within the aggregation autonomous system, and eBGP-labeled unicast sessions are established with the neighboring core AS CN-ASBRs. The AGN-ASBRs are inserted into the data path in order to enable inter-domain LSPs by setting NHS on all iBGP updates toward the local AGN-RRs and eBGP updates toward neighboring CN-ASBRs. If a centralized RR is not employed in the aggregation domain, and the AGN-ASBR provides the RR functionality for the domain instead, then NHS is applied only to the eBGP prefixes from the CN-ASBR that are reflected toward the local iBGP RR clients. Local iBGP updates from the PANs in the aggregation network are reflected with NHU in order to avoid inter-PAN service forwarding from having to pass through the AGN-ASBR.

The PANs are labeled BGP ABRs between the aggregation and access domains. iBGP labeled-unicast sessions are established with the higher level AGN-RRs in the aggregation network, and the PANs act as inline-RRs for local access network CSG and FAN 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) also act as labeled BGP PEs and advertise loopbacks into BGP-labeled unicast with a common BGP community (PAN_RAN_FAN_Community) that represents the service communities being serviced by the PAN. The PANs learn labeled BGP prefixes marked with the aggregation BGP community and the MSE BGP community. The PANs are inserted into the data path in order to enable inter-domain LSPs by setting NHS on all iBGP updates towards the higher-level AGN-RRs and the local access CSG and FAN clients.

FSE gateways, such as AGN-SEs and PAN-SEs, are labeled BGP PEs residing in the aggregation network, optimally located with the access networks for residential and business fixed wireline services. iBGP labeled-unicast sessions are established with the AGN-RR, and loopbacks are advertised into

iBGP-labeled unicast with a common BGP community (FSE_Community). The SE node functionality can reside within the AGN node described previously; there is no technical requirement for separate SE nodes.

The CSGs in the RAN are labeled BGP PEs. iBGP-labeled unicast sessions are established with the local PAN inline-RRs. The CSGs advertise loopbacks into BGP-labeled unicast with a common BGP community that represents the RAN access community. BGP prefixes marked with the MSE BGP community are learned for reachability to the MTGs, and the adjacent RAN access BGP communities are learned if inter-access X2 connectivity is desired.

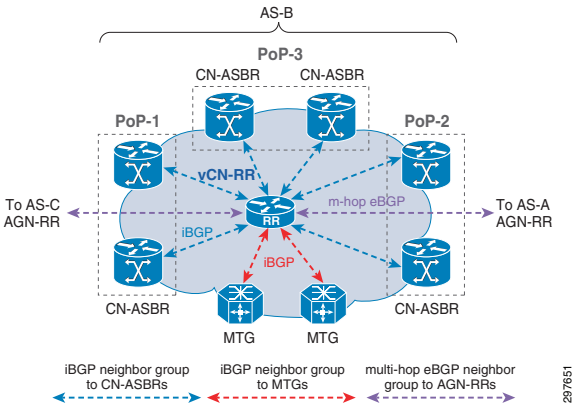
The FANs in the access networks are labeled BGP PEs. iBGP-labeled unicast sessions are established with the local PAN inline-RRs. The FANs advertise loopbacks into BGP-labeled unicast with a common BGP community that represents the FAN access community. Labeled BGP prefixes marked with the FSE BGP community are learned for reachability to the AGN-SE or PAN-SE.

The MTGs and IGWs in the core network are capable of handling large scale and will learn all BGP-labeled unicast prefixes for connectivity to all the CSGs and SE nodes in the entire network. For mobile services, simple prefix filtering based on BGP communities is performed on the CN-RRs for the purpose of constraining IPv4+label routes that are from remote RAN access regions from proliferating between aggregation domains where they are not needed. The PANs and SE nodes only learn labeled BGP prefixes marked with the FAN, FSE, IGW, and MSE BGP communities. This allows the AGNs to reflect these prefixes to local access networks. Isolating the aggregation and access domains by preventing the default IGP redistribution enables the access networks to have limited route scale. CSGs only learn local IGP routes and labeled BGP prefixes marked with the MSE BGP community. The FAN nodes implement dynamic ip prefix-lists in order to permit only the prefixes for SE nodes and remote FAN nodes with currently configured services on the FAN.

Core Route Reflector Configuration

This section describes the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the centralized CN-RR. Figure 6-37 shows multiple aggregation BGP autonomous systems with multiple pairs of CN-ASBRs, but for simplicity only one set of CN-ASBRs are shown in the configuration below.

Figure 6-37 Centralized Virtual Core Route Reflector (vCN-RR)



Interface Configuration

```
interface Loopback0
  description Global Loopback
  ipv4 address 100.111.4.3 255.255.255.255
!
```

```
!***Core Interface***
interface GigabitEthernet0/1/0/0
  description To CN-K0201 Gig0/2/0/0
  cdp
  ipv4 address 10.2.1.3 255.255.255.254
  negotiation auto
  load-interval 30
!
!***Core Interface***
interface GigabitEthernet0/1/0/1
  description To CN-K0401 Gig0/1/0/1
  cdp
  ipv4 address 10.4.1.1 255.255.255.254
  negotiation auto
  load-interval 30
!
```

IGP/LDP Configuration

```
router isis core
  set-overload-bit on-startup 360
  net 49.0100.1001.1100.4003.00
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    address-family ipv4 unicast
    !
  !
  !***Core Interface***
  interface GigabitEthernet0/1/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 100
    !
  !
  !***Core Interface***
  interface GigabitEthernet0/1/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 100
    !
  !
!

mpls ldp
  router-id 100.111.4.3
  graceful-restart
  log
```

```
    neighbor
    graceful-restart
  !
  mldp
  !
  interface GigabitEthernet0/1/0/0
  !
  interface GigabitEthernet0/1/0/1
  !
```

BGP Configuration

```
router bgp 1000
  nsr
  bgp default local-preference 50
  bgp router-id 100.111.4.3
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  address-family ipv4 unicast
    !***BGP add-path configuration for BGP Edge FRR***!
    additional-paths receive
    additional-paths send
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 0
    network 100.111.4.3/32
    allocate-label all
  !
  address-family vpnv4 unicast
  !
  address-family ipv6 unicast
    allocate-label all
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  address-family ipv6 mvpn
  !
  !***session group for iBGP clients (CN-ASBRs and MTGs)***
  session-group intra-as
    remote-as 1000
    password encrypted 082D4D4C
    update-source Loopback0
  !
  !***session group for multi-hop eBGP neighbors (AGN-RRs)***
  session-group inter-as-rr
    remote-as 101
    update-source Loopback0
  !
  !***MTG neighbor group***
  neighbor-group mtg
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-reflector-client
      maximum-prefix 150000 85 warning-only
      soft-reconfiguration inbound always
    !
    address-family vpnv4 unicast
    !
    address-family ipv6 labeled-unicast
      route-reflector-client
      maximum-prefix 150000 85 warning-only
    !
```

```
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
      route-reflector-client
    !
  !
  !***neighbor group for CN-ASBRs***
  neighbor-group cn-asbr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-reflector-client
      !***Egress filter to drop unwanted RAN loopbacks towards neighboring aggregation
regions***
      route-policy BGP_Egress_Transport_Filter out
    !
    address-family ipv6 labeled-unicast
      route-reflector-client
      !***Egress filter to drop unwanted RAN loopbacks towards neighboring aggregation
regions***
      route-policy BGP_Egress_Transport_Filter out
    !
  !
  !***AGN-RR multi-hop eBGP neighbor group***
  neighbor-group inter-as-rr
    use session-group inter-as-rr
    ebgp-multihop 20
    address-family vpnv4 unicast
      <SNIP>
    !
    address-family vpnv6 unicast
    <SNIP>
    !
    address-family ipv4 mvpn
    <SNIP>
    !
    address-family ipv6 mvpn
    !
  !
  !***CN-ASBR-K0601***
  neighbor 100.111.6.1
    use neighbor-group cn-asbr
  !
  !***AGN-RR-K1103***
  neighbor 100.111.11.3
    use neighbor-group inter-as-rr
  !
  !***CN-ASBR-K1201***
  neighbor 100.111.12.1
    use neighbor-group cn-asbr
  !
  !***MTG-K1501***
  neighbor 100.111.15.1
    use neighbor-group mtg
  !
  !***MTG-K1502***
  neighbor 100.111.15.2
    use neighbor-group mtg
  !
!
route-policy add-path-to-ibgp
  set path-selection backup 1 advertise install
end-policy

route-policy BGP_Egress_Transport_Filter
```

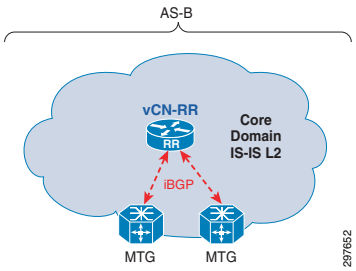
```
  !***20:20 = FAN_Community for Fixed Access Nodes***
  if community matches-any (20:20) then
    pass
  else
    !***10:10 = RAN_Community for CSGs***
    if community matches-any (10:10) then
      drop
    else
      pass
    endif
  endif
end-policy
```

Note Please refer to the BGP Transport Control Plane, page 3-25 for a detailed explanation of how egress filtering is done at the CN-RR for constraining IPv4+label routes from remote RAN access regions.

Mobile Transport Gateway Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the MTG. See Figure 6-38.

Figure 6-38 Mobile Transport Gateway (MTG)



Interface Configuration

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

IGP Configuration

```
router isis core
  set-overload-bit on-startup 250
  net 49.0100.1001.1101.5001.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
    !***Determines which prefixes are updated first during SPF calculation***
    spf prefix-priority critical isis-critical-acl
    spf prefix-priority medium isis-medium-acl
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  interface TenGigE0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      metric 10
      mpls ldp sync
    !
  !
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      metric 10
      mpls ldp sync
    !
  !
!

!***Prioritize CN-ASBR Loopback during SPF recalculation***
ipv4 prefix-list isis-critical-acl
  10 permit 100.111.6.1/32 le 32
  20 permit 100.111.12.1/32 le 32
!
ipv4 prefix-list isis-medium-acl
  10 permit 0.0.0.0/0 le 32
!

mpls ldp
  router-id 100.111.15.1
  discovery targeted-hello accept
  nsr
  graceful-restart
```

```
  session protection
  igp sync delay 10 log
    neighbor
    graceful-restart
    session-protection
    nsr
  !
  mldp
    logging notifications
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
!
```

BGP Configuration

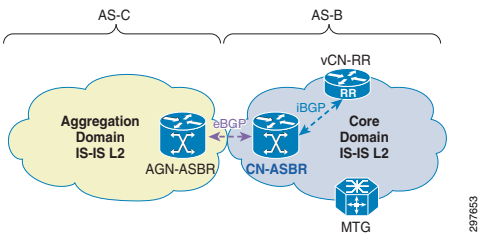
```
router bgp 1000
  nsr
  bgp router-id 100.111.15.1
  bgp update-delay 360
  bgp redistribute-internal
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    !***BGP add-path to receive multiple paths from CN-RR***
    additional-paths receive
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 0
    !***Color loopback prefix in BGP with MSE and IGW Communities***
    network 100.111.15.1/32 route-policy MSE_IGW_Community
    allocate-label all
  !
  address-family vpnv4 unicast
    <SNIP>
  !
  address-family ipv6 unicast
    redistribute connected
    allocate-label all
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  session-group intra-as
    remote-as 1000
    password encrypted 011F0706
    update-source Loopback0
  !
  neighbor-group cn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family ipv6 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
```

```
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
    !
  !
  !***CN-RR***
  neighbor 100.111.4.3
    use neighbor-group cn-rr
  !

community-set IGW_Community
  3001:3001
end-set
!
community-set MSE_Community
  1001:1001
end-set
!
route-policy MSE_IGW_Community
  set community MSE_Community
  set community IGW_Community additive
end-policy

!***Pass Common, MSE, and IGW communities***
community-set PASS_Community
  10:10,
  1001:1001,
  3001:3001
end-set
!
route-policy BGP_Ingress_Transport_Filter
  if community matches-any PASS_Community then
    pass
  else
    drop
  endif
end-policy
!

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

Core ASBR Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the CN-ASBRs. See Figure 6-39.

Figure 6-39 Core Node-Autonomous System Border Router (CN-ASBR)



Interface Configuration

```
!
interface Loopback0
  ipv4 address 100.111.12.1 255.255.255.255
!
!***Interface to redundant CN-ASBR-K0601***
interface TenGigE0/0/0/0
  description To CN-ASBR-K0601::Ten0/0/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.6.1.5 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
!
!***Interface to AGN-ASBR-K1002***
interface TenGigE0/0/0/0
  description To AGN-ASBR-K1002::T0/0/0/2
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.10.2.1 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
!
!***Interface to Core Node CN-K0401***
interface TenGigE0/0/0/5
  description To CN-K0401::Ten0/0/0/5
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.4.1.9 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
!
```

Static Route Configuration

```
!***Static route to AGN-ASBR-K1002 Loopback***
router static
  address-family ipv4 unicast
    100.111.10.2/32 10.10.2.0 bfd fast-detect minimum-interval 10 multiplier 3
!
```

IGP/LDP Configuration

```
router isis core
  net 49.0100.1001.1101.2001.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
    !***Prioritization of prefixes during SFP recalculation***
    spf prefix-priority critical isis-critical-acl
    spf prefix-priority medium isis-medium-acl
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
```

```
  !*** Interface to redundant CN-ASBR***
  interface TenGigE0/0/0/0
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      metric10
      mpls ldp sync
    !
  !
  !*** Interface to AGN-ASBR***
  interface TenGigE0/0/0/2
    circuit-type level-2-only
    point-to-point
    address-family ipv4 unicast
      metric 10
    !
  !
  !*** Interface to core network***
  interface TenGigE0/0/0/5
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
!

!***Prioritize CN-ASBR prefixes over all others***
ipv4 prefix-list isis-critical-acl
  10 permit 100.111.6.1/32 le 32
  20 permit 100.111.12.1/32 le 32
!
ipv4 prefix-list isis-medium-acl
  10 permit 0.0.0.0/0 le 32
!

mpls ldp
  router-id 100.111.12.1
  discovery targeted-hello accept
  graceful-restart
  session protection
  log
    neighbor
    graceful-restart
  !
  mldp
    make-before-break delay 0 0
    logging notifications
    recursive-fec  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/5
  !
```

BGP Configuration

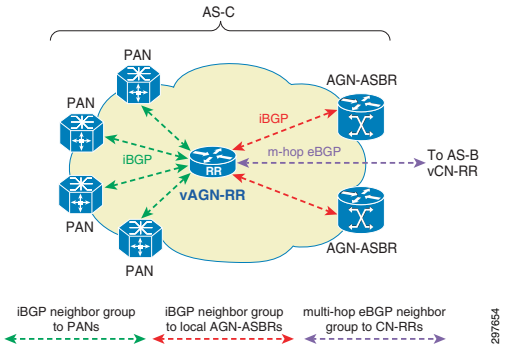
```
router bgp 1000
  nsr
  bgp router-id 100.111.12.1
  !***MPLS forwarding on interface with eBGP neighbor AGN-ASBR***
  mpls activate
    interface TenGigE0/0/0/0
  !
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    !***BGP add-path to receive multiple paths from CN-RR***
    additional-paths receive
    additional-paths send
    advertise best-external
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 0
    allocate-label all
  !
  !***session group for AGN-ASBR***
  session-group inter-as
    remote-as 101
    update-source Loopback0
  !
  !***session group for local CN-RR***
  session-group intra-as
    remote-as 1000
    password encrypted 011F0706
    update-source Loopback0
  !
  !***iBGP neighbor group for CN-RR***
  neighbor-group cn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
       maximum-prefix 150000 85 warning-only
       next-hop-self
  !
    address-family ipv6 labeled-unicast
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
  !
  !***eBGP neighbor group for AGN-ASBR.***
  !***Implicit next-hop-self set towards eBGP neighbor.***
  neighbor-group agn-asbr
    use session-group inter-as
    address-family ipv4 labeled-unicast
      send-community-ebgp
      route-policy pass-all in
      route-policy pass-all out
    !
    address-family ipv6 labeled-unicast
      send-community-ebgp
      route-policy pass-all in
      route-policy pass-all out
    !
  !
  !***CN-RR***
  neighbor 100.111.4.3
    use neighbor-group cn-rr
  !
  !***Redundant CN-ASBR***
  neighbor 100.111.6.1
```

```
    use neighbor-group cn-rr
  !
  !***AGN ASBR***
  neighbor 100.111.10.2
    use neighbor-group agn-asbr
    ebgp-multihop 10
  !
!

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

!
route-policy pass-all
  pass
end-policy
!
```

Aggregation Route Reflector Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the AGN-RR. See Figure 6-40.

Figure 6-40 Virtual Aggregation Route Reflector (vAGN-RR)



In the Cisco EPN 4.0 System design:

- The AGN-RR role is fulfilled by Cisco IOS XRv. IOS XRv enables an emulated classic 32-bit X86 IOS XR router within a VM on a Cisco Unified Computing System (UCS) platform.
- Cisco IOS XRv was validated by using a standalone Cisco UCS-C200 series server. A future phase will validate IOS XRv inside a Cisco UCS-B series data center to provide a consolidated virtualized infrastructure.

Interface Configuration

```
interface Loopback0
  ip address 100.111.15.5 255.255.255.255
!
```

IGP Configuration

```
router isis agg-acc
 is-type level-2-only
 net 49.0100.1001.1101.5004.00
```

```
 log adjacency changes
 lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
 lsp-refresh-interval 65000
 max-lsp-lifetime 65535
 address-family ipv4 unicast
  metric-style wide
  spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
 !
 interface Loopback0
  passive
  point-to-point
  address-family ipv4 unicast
   !
 !
 interface GigabitEthernet0/0/0/0
  circuit-type level-2-only
  bfd minimum-interval 50
  bfd multiplier 3
  bfd fast-detect ipv4
  point-to-point
  address-family ipv4 unicast
   metric 500
   !
 !
!
```

BGP Configuration

```
router bgp 101
 bgp router-id 100.111.15.5
 !***Cluster-ID for RR***
 bgp cluster-id
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 bgp log neighbor changes detail
 address-family ipv4 unicast
!***BGP add-path configuration for BGP Edge FRR***
  additional-paths receive
  additional-paths send
  additional-paths selection route-policy add-path-to-ibgp
  nexthop trigger-delay critical 0
  network 100.111.15.5/32
  allocate-label all
 !
 address-family vpnv4 unicast
 !
 address-family ipv6 unicast
 !***BGP add-path configuration for BGP Edge FRR***
  additional-paths receive
  additional-paths send
  additional-paths selection route-policy add-path-to-ibgp
  allocate-label all
 !
 address-family vpnv6 unicast
 !
 address-family ipv4 mvpn
 !
 address-family ipv6 mvpn
 !
 address-family l2vpn evpn
 !
 !***session group for multi-hop eBGP neighbors (CN-RR)***
 session-group inter-as
```

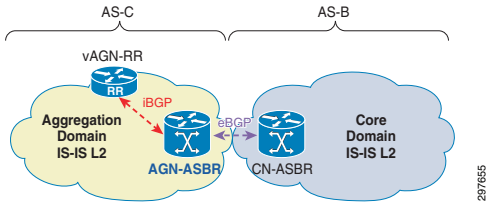
```
 remote-as 1000
 ebgp-multihop 20
 update-source Loopback0
!

!***session group for iBGP clients (AGN-ASBRs, SE Nodes, PANs)***
session-group intra-as
 remote-as 101
 password encrypted 082D4D4C
 update-source Loopback0
!
!***CN-RR multi-hop eBGP neighbor group***
neighbor-group inter-as
 use session-group inter-as
 address-family vpnv4 unicast
 !
 address-family vpnv6 unicast
 !
 address-family ipv4 mvpn
 !
 address-family ipv6 mvpn
 !
!
!***Neighbor group for iBGP clients with mVPN***
neighbor-group intra-as-mvpn
 use session-group intra-as
 address-family ipv4 labeled-unicast
  route-policy pass-all in
  route-policy pass-all out
  route-reflector-client
  maximum-prefix 150000 85 warning-only
  soft-reconfiguration inbound always
 !
 address-family vpnv4 unicast
 !
 address-family ipv6 labeled-unicast
  route-policy pass-all in
  route-policy pass-all out
  route-reflector-client
  maximum-prefix 150000 85 warning-only
 !
 address-family vpnv6 unicast
 !
 address-family ipv4 mvpn
 !
 address-family ipv6 mvpn
 !
!
!***Neighbor group for iBGP clients***
neighbor-group intra-as
 use session-group intra-as
 address-family ipv4 labeled-unicast
  route-policy pass-all in
  route-policy pass-all out
  route-reflector-client
  maximum-prefix 150000 85 warning-only
  soft-reconfiguration inbound always
 !
 address-family vpnv4 unicast
 !
 address-family ipv6 labeled-unicast
  route-policy pass-all in
  route-policy pass-all out
  route-reflector-client
```

```
   maximum-prefix 150000 85 warning-only
  !
  address-family vpnv6 unicast
  !
 !
 !***AGN-SE nodes***
 neighbor 100.111.3.1
  use neighbor-group intra-as-mvpn
 !
 neighbor 100.111.3.2
  use neighbor-group intra-as-mvpn
 !
 !***CN-RR***
 neighbor 100.111.4.3
  use neighbor-group inter-as
 !
 !***PAN-SE Nodes***
 neighbor 100.111.5.4
  use neighbor-group intra-as-mvpn
 !
 neighbor 100.111.5.5
  use neighbor-group intra-as-mvpn
 !
 !***AGN-ASBR Nodes***
 neighbor 100.111.10.1
  use neighbor-group intra-as-mvpn
 !
 neighbor 100.111.10.2
  use neighbor-group intra-as-mvpn
 !
 !***PAN Nodes***
 neighbor 100.111.14.1
  use neighbor-group intra-as
 !
 neighbor 100.111.14.2
  use neighbor-group intra-as
 !
neighbor 100.111.9.17
  use neighbor-group intra-as
 !
 neighbor 100.111.9.18
  use neighbor-group intra-as
 !
!
route-policy pass-all
  pass
end-policy
!
!***For BGP FRR Edge functionality***
route-policy add-path-to-ibgp
  set path-selection backup 1 advertise install
end-policy
!
```

Aggregation ASBR Configuration

This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the AGN-ASBRs. See Figure 6-41.

Figure 6-41 Aggregation Node Autonomous System Border Router (AGN-ASBR)



Interface Configuration

```
interface Loopback0
  description Global Loopback
  ipv4 address 100.111.10.2 255.255.255.255
!
!***Redundant AGN-ASBR interface***
interface TenGigE0/0/0/0
  description To AGN-ASBR-K1001 T0/0/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.10.1.1 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  !
!
!***Aggregation Network facing interface***
interface TenGigE0/0/0/1
  description To AGN-K0302::T0/0/0/1
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.3.2.3 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  !
!
!***Neighbor CN-ASBR facing interface***
interface TenGigE0/0/0/2
  description To CN-ASBR-K1201::Te0/0/0/2
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.10.2.0 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
!
```

Static Route Configuration

```
!***Static route to CN-ASBR-K1201 Loopback***
router static
  address-family ipv4 unicast
    100.111.12.1/32 10.10.2.1 bfd fast-detect minimum-interval 10 multiplier 3
!
```

IGP/LDP Configuration

```
router isis agg-acc
  set-overload-bit on-startup 360
  is-type level-2-only
  net 49.0100.1001.1101.0002.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
```

```
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
  !
  !***redundant AGN-ASBR facing interface***
  interface TenGigE0/0/0/0
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
    !
  !
  !***Aggregation network facing interface***
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
    !
  !
!

mpls ldp
  router-id 100.111.10.2
  graceful-restart
  explicit-null
  log
    neighbor
    graceful-restart
  !
  mldp
    logging notifications
    recursive-fec
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
  interface TenGigE0/0/0/2
  !
!
```

BGP Configuration

```
router bgp 101
  nsr
  bfd minimum-interval 15
  bfd multiplier 3
  bgp router-id 100.111.10.2
  !***MPLS forwarding on interface to eBGP neighbor CN-ASBR***
  mpls activate
    interface TenGigE0/0/0/2
  !
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    additional-paths receive
    additional-paths send
    advertise best-external
    additional-paths selection route-policy add-path-to-ibgp
    !***Color loopback prefix in BGP with AGN_ASBR_Community***
    network 100.111.10.2/32 route-policy AGN_ASBR_Community
    allocate-label all
  !
  !***session group for neighbor AS CN-ASBR***
  session-group inter-as
    remote-as 1000
  !
  !***session group for local AGN-RR***
  session-group intra-as
    remote-as 101
    password encrypted 0703204E
    update-source Loopback0
  !
  !***iBGP neighbor group for AGN-RR***
    neighbor-group agn-rr
    use session-group intra-as
    !***set next-hop to self for all labels***
    address-family ipv4 labeled-unicast
      next-hop-self
    !
    address-family ipv6 labeled-unicast
      next-hop-self
    !
  !
  !***eBGP neighbor group for AGN-ASBR.***
  !***Implicit next-hop-self set towards eBGP neighbor.***
  neighbor-group cn-asbr
    use session-group inter-as
    address-family ipv4 labeled-unicast
      send-community-ebgp
      route-policy pass-all in
      route-policy pass-all out
    !
    address-family ipv6 labeled-unicast
      send-community-ebgp
      route-policy pass-all in
      route-policy pass-all out
    !
  !
  !***Neighbor CN-ASBR***
  neighbor 100.111.12.1
    use neighbor-group cn-asbr
    ebgp-multihop 10
  !
  !***Local AGN-RR***
```

```
  neighbor 100.111.15.5
    use neighbor-group agn-rr
  !
!
route-policy AGN_ASBR_Community
  set community AGN_ASBR_Community
end-policy
!
community-set AGN_ASBR_Community
  1111:1111,
  1001:1001
end-set
!
route-policy pass-all
  pass
end-policy
!
route-policy add-path-to-ibgp
  set path-selection backup 1 advertise install
end-policy
```

Aggregation ASBR with Inline-RR Configuration

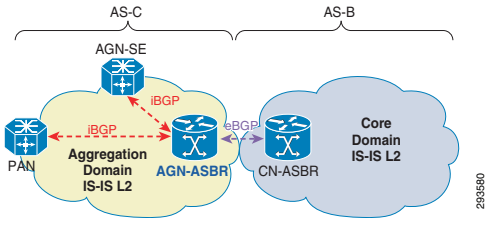
This section shows the IGP/LDP configuration required to build intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs on the AGN-ASBRs. In this option, no AGN-RR node exists so the AGN-ASBR functions as the RR for the aggregation network.

Because the RR functionality is in the data path in this case, NHS cannot be set on every update reflected towards the PANs, PAN-SEs, and AGN-SEs in the network. If this were the case, then all intra-AS transported services, such as E-Line services within this autonomous system or inter-area X2 interface transport, would have to be routed through the AGN-ASBR instead of directly between PANs. This leads to non-optimal routing of services. This can be addressed by only setting NHS on reflected prefixes from other BGP autonomous systems. Because all updates from other autonomous systems are received via eBGP updates from the CN-ASBRs, then this can be used as the distinguishing criteria for applying NHS.

In this case, the PAN nodes would have iBGP exchanges directly with the AGN-ASBR instead of an AGN-RR. This is the only change required in the PAN configurations shown in this section. See Figure 6-42.

Note This configuration example was not validated as part of the Cisco EPN 4.0 System effort. It is adapted from configurations validated in a previous system.

Figure 6-42 Aggregation Autonomous System Border Router (AGN-ASBR) with Inline-RR



Interface Configuration

```
!
interface Loopback0
  description Global Loopback
  ipv4 address 100.111.10.2 255.255.255.255
!
!***Redundant AGN-ASBR interface***
interface TenGigE0/0/0/0
  description To AGN-ASBR-K1001 T0/0/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.10.1.1 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  !
!
!***Aggregation Network facing interface***
interface TenGigE0/0/0/1
  description To AGN-K0302::T0/0/0/1
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.3.2.3 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
  !
!
!***Neighbor CN-ASBR facing interface***
interface TenGigE0/0/0/2
  description To CN-ASBR-K1201::Te0/0/0/2
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.10.2.0 255.255.255.254
  carrier-delay up 2000 down 0
  load-interval 30
!
```

Static Route Configuration

```
!***Static route to CN-ASBR-K1201 Loopback***
router static
  address-family ipv4 unicast
    100.111.12.1/32 10.10.2.1 bfd fast-detect minimum-interval 10 multiplier 3
!
```

IGP/LDP Configuration

```
router isis agg-acc
  set-overload-bit on-startup 360
  is-type level-2-only
  net 49.0100.1001.1101.0002.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
```

```
  !
  !***redundant AGN-ASBR facing interface***
  interface TenGigE0/0/0/0
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
  !***Aggregation network facing interface***
  interface TenGigE0/0/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    link-down fast-detect
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
!

mpls ldp
  router-id 100.111.10.2
  graceful-restart
  explicit-null
  log
    neighbor
    graceful-restart
  !
  mldp
    logging notifications
  !
  interface TenGigE0/0/0/0
  !
  interface TenGigE0/0/0/1
  !
  interface TenGigE0/0/0/2
  !
!
```

BGP Configuration

```
router bgp 101
  nsr
  bfd minimum-interval 15
  bfd multiplier 3
  bgp router-id 100.111.10.2
  !***MPLS forwarding on interface to eBGP neighbor CN-ASBR***
  mpls activate
    interface TenGigE0/0/0/2
  !
  bgp graceful-restart
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    additional-paths receive
    additional-paths send
    advertise best-external
```

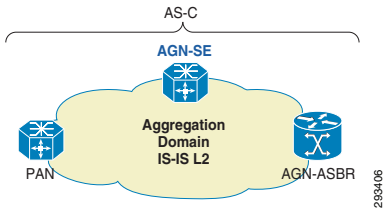
```
  additional-paths selection route-policy add-path-to-ibgp
  !***Color loopback prefix in BGP with AGN_ASBR_Community***
  network 100.111.10.2/32 route-policy AGN_ASBR_Community
  allocate-label all
!
!***session group for neighbor AS CN-ASBR***
session-group inter-as
  remote-as 1000
!
!***iBGP neighbor group for local PANs***
  neighbor-group pan
  use session-group intra-as
  !***set next-hop to self for only reflected eBGP prefixes***
  address-family ipv4 labeled-unicast
    route-reflector-client
    route-policy SET_NEXT_HOP_SELF out
  !
  address-family ipv6 labeled-unicast
    route-reflector-client
    route-policy SET_NEXT_HOP_SELF out
  !
!
!***eBGP neighbor group for AGN-ASBR.***
!***Implicit next-hop-self set towards eBGP neighbor.***
neighbor-group cn-asbr
  use session-group inter-as
  address-family ipv4 labeled-unicast
    send-community-ebgp
    route-policy pass-all in
    route-policy pass-all out
  !
  address-family ipv6 labeled-unicast
    send-community-ebgp
    route-policy pass-all in
    route-policy pass-all out
  !
!
!***Neighbor CN-ASBR***
neighbor 100.111.12.1
  use neighbor-group cn-asbr
  ebgp-multihop 10
!
!***Local PANs, PAN-SEs, AGN-SEs***
neighbor 100.111.3.1 activate
  use neighbor-group pan
!
neighbor 100.111.3.2 activate
  use neighbor-group pan
!
neighbor 100.111.5.3 activate
  use neighbor-group pan
!
neighbor 100.111.5.4 activate
  use neighbor-group pan
!
neighbor 100.111.9.17 activate
  use neighbor-group pan
!
neighbor 100.111.9.18 activate
  use neighbor-group pan
!
neighbor 100.111.14.1 activate
  use neighbor-group pan
!
```

```
  neighbor 100.111.14.2 activate
    use neighbor-group pan
  !
!

!***Only match on eBGP received updates***
route-policy SET_NEXT_HOP_SELF
  if origin is egp then
      set next-hop self
    else
     pass
    endif
end-policy

route-policy AGN_ASBR_Community
  set community AGN_ASBR_Community
end-policy
!
community-set AGN_ASBR_Community
  1111:1111
end-set
!

route-policy pass-all
  pass
end-policy

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

Aggregation Service Edge Node Configuration

This section shows the IGP/LDP and BGP configuration for aggregation nodes providing SE functionality. See Figure 6-43.

Figure 6-43 Aggregation Service Edge Node (AGN-SE)



Interface Configuration

```
interface Loopback0
  ipv4 address 100.111.3.2 255.255.255.255
  ipv6 address 2001:100:111:3::2/128
!
!***Redundant AGN-SE interface***
interface TenGigE0/2/0/0
  description To AGN-9006-K0301 T0/2/0/0
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.3.1.5 255.255.255.254
  carrier-delay up 2000 down 0
  transceiver permit pid all
!
```

```
!***AGN-ASBR interface***
interface TenGigE0/2/0/1
  description To AGN-ASBR-9006-K1002 T0/0/0/1
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.3.2.2 255.255.255.254
  load-interval 30
!
!***PAN interface for subtended CSG ring***
interface TenGigE0/2/0/2
  description To PAN-ME38-K0913 TE0/1
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.3.2.0 255.255.255.254
  load-interval 30
  transceiver permit pid all
!
!***CSG interface for RAN access ring***
interface TenGigE0/2/0/3
  description To CSG-K0912 Ten0/1
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.9.12.1 255.255.255.254
  load-interval 30
  transceiver permit pid all
!
!***FAN interface for FAN access ring***
interface TenGigE0/2/1/0
  description To FAN-K0706 Ten 0/2
  cdp
  service-policy output PMAP-NNI-E
  ipv4 address 10.3.2.4 255.255.255.254
  transceiver permit pid all
!
```

IGP/LDP Configuration

```
router isis agg-acc
  set-overload-bit on-startup 360
  net 49.0100.1001.1100.3002.00
  nsf cisco
  log adjacency changes
  lsp-gen-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
  lsp-refresh-interval 65000
  max-lsp-lifetime 65535
  address-family ipv4 unicast
    metric-style wide
    metric 10
    !***Provides better performance for Remote LFA-FRR***
    microloop avoidance rib-update-delay 60000
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
    propagate level 1 into level 2 route-policy L1intoL2
  !
  interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
      metric 100
    !
  !
  interface TenGigE0/2/0/0
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
```

```
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
    !
  !
  interface TenGigE0/2/0/1
    circuit-type level-2-only
    bfd minimum-interval 15
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
    !
  !
  interface TenGigE0/2/0/2
    circuit-type level-2-only
    bfd minimum-interval 50
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      fast-reroute per-prefix level 2
      fast-reroute per-prefix remote-lfa tunnel mpls-ldp
      metric 10
      mpls ldp sync
    !
  !
  interface TenGigE0/2/0/3
    circuit-type level-1
    bfd minimum-interval 50
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
  interface TenGigE0/2/1/0
    circuit-type level-1
    bfd minimum-interval 50
    bfd multiplier 3
    bfd fast-detect ipv4
    point-to-point
    address-family ipv4 unicast
      metric 10
      mpls ldp sync
    !
  !
!***Permits redundant AGN-ASBR info for Remote LFA FRR***
prefix-set L1intoL2
  100.111.3.1/32,
  10.3.1.4/32,
  10.3.1.5/32
end-set
!
route-policy L1intoL2
```

```
  if destination in L1intoL2 then
    pass
  else
    drop
  endif
end-policy
!
mpls ldp
  router-id 100.111.3.2
  discovery targeted-hello accept
  graceful-restart
  igp sync delay 5
  log
    neighbor
    graceful-restart
  !
  mldp
    make-before-break delay 0 0
    logging notifications
    recursive-fec
  !
  interface TenGigE0/2/0/0
  !
  interface TenGigE0/2/0/1
  !
  interface TenGigE0/2/0/2
    mldp disable
  !
  interface TenGigE0/2/0/3
    mldp disable
  !
  interface TenGigE0/2/1/0
    mldp disable
  !
!
```

BGP Configuration

```
router bgp 101
  bgp router-id 100.111.3.2
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp redistribute-internal
  bgp graceful-restart
  bgp log neighbor changes detail
  ibgp policy out enforce-modifications
  address-family ipv4 unicast
    additional-paths receive
    additional-paths selection route-policy add-path-to-ibgp
    nexthop trigger-delay critical 0
    !***Color Loopback with FSE Community***
    network 100.111.3.2/32 route-policy FSE_Community
    allocate-label all
  !
  address-family vpnv4 unicast
  !
  address-family ipv6 unicast
    network 2001:100:111:3::2/128 route-policy FSE_Community
    allocate-label all
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
```

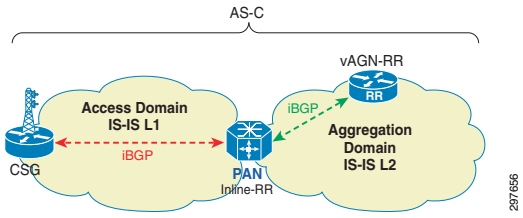
```
  address-family ipv6 mvpn
  !
  session-group intra-as
    remote-as 101
    password encrypted 11051807
    update-source Loopback0
  !
  neighbor-group csg
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-reflector-client
      maximum-prefix 150000 85 warning-only
      next-hop-self
    !
    address-family vpnv4 unicast
    !
    address-family vpnv6 unicast
    !
  !
  neighbor-group agn-rr
    use session-group intra-as
    address-family ipv4 labeled-unicast
      route-policy BGP_Ingress_Transport_Filter in
      next-hop-self
      soft-reconfiguration inbound always
    !
    address-family vpnv4 unicast
    !
    address-family ipv6 labeled-unicast
      next-hop-self
    !
    address-family vpnv6 unicast
    !
    address-family ipv4 mvpn
    !
    address-family ipv6 mvpn
    !
  !
  !***AGN-RR***
  neighbor 100.111.15.5
    use neighbor-group agn-rr
  !
  !***FAN nodes in FAN access ring***
  neighbor 100.111.7.6
    use neighbor-group csg
  !
  neighbor 100.111.7.7
    use neighbor-group csg
  !
  neighbor 100.111.7.8 use
    neighbor-group csg
  !
  !***CSG nodes in RAN access ring***
  neighbor 100.111.9.11
    use neighbor-group csg
  !
  neighbor 100.111.9.12
    use neighbor-group csg
  !
  neighbor 100.111.9.14
    use neighbor-group csg
 !
!
community-set PASS_Community
```

```
  !***Common RAN community***
  10:10,
  !***Common FAN community***
  20:20,
  !***MSE & MPC community***
  1001:1001,
  !***FSE community***
  2001:2001,
  !***IGW community***
  3001:3001
end-set
!
!***Set communities to pass***
route-policy BGP_Ingress_Transport_Filter
  if community matches-any PASS_Community then
    pass
  else
    drop
  endif
end-policy

community-set FSE_RAN_FAN_Community
  20:20,
  2001:2001
end-set
!
route-policy FSE_Community
  set community FSE_RAN_FAN_Community
end-policy
!

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

Pre-Aggregation Node Configuration for Labeled BGP Access

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs in the aggregation network. The PANs are ABRs between the aggregation and RAN access domains. The segmentation between the two domains is achieved by making the aggregation network as IS-IS Level 2 and each mobile access network subtending from a pair of PANs as part of a unique IS-IS Level 1 domain. All access ring networks and nodes with hub-and-spoke connections subtending from the same pair of PANs are part of this IS-IS Level 1 domain, where the CSGs are IS-IS L1 nodes and the PAN are L1/L2 nodes. See Figure 6-43.

Figure 6-44 Pre-Aggregation Node (PAN)



Interface Configuration

```
interface Loopback0
  ip address 100.111.14.1 255.255.255.255
!
!***Redundant PAN interface***
interface TenGigabitEthernet0/0/0
  description To PAN-903-K1402::TenGigabitEthernet0/0/0
  ip address 10.14.1.0 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis network point-to-point
  isis metric 10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
!***Upstream AGN interface***
interface TenGigabitEthernet0/1/0
  description To AGN-K0301::T0/0/0/2
  ip address 10.3.1.3 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis circuit-type level-2-only
  isis network point-to-point
  isis metric 10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
!***CSG interface via NSN microwave ODU***
interface GigabitEthernet0/3/0
  no ip address
  load-interval 30
  negotiation auto
  cdp enable
  service-policy input PMAP-UNI-I
  service-policy output PMAP-uW-NNI-P-E
  service instance 61 ethernet
    encapsulation dot1q 61
    rewrite ingress tag pop 1 symmetric
    bridge-domain 61
  !
!
interface BDI61
  description To CSG-901-K1329::Gi0/10
  ip address 10.13.29.1 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
```

```
  isis network point-to-point
  isis metric 100
  isis csnp-interval 10
  hold-queue 350 in
  hold-queue 2000 out
!
```

IGP/LDP Configuration

```
router isis agg-acc
  net 49.0100.1001.1101.4001.00
  !***PAN is an ISIS Level 1-2 node***
  ispf level-1-2
  metric-style wide
  fast-flood
  set-overload-bit on-startup 180
  !***Do not set attached bit (default router)***
  set-attached-bit route-map DO_NOT_SET_ATT_BIT
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 5 200
  no hello padding
  log-adjacency-changes
  nsf cisco
  !***Remote LFA FRR***
  fast-reroute per-prefix level-2 all
  fast-reroute remote-lfa level-2 mpls-ldp
  !***Selective redistribution of L1 into L2***
  redistribute isis ip level-1 into level-2 route-map L1intoL2
  passive-interface Loopback0
  distance 201 100.111.14.2 0.0.0.0 BGP_redistributed_prefixes
  bfd all-interfaces
  mpls ldp sync

!
route-map DO_NOT_SET_ATT_BIT permit 10
  match clns address DO_NOT_SET_ATT_BIT
!
clns filter-set DO_NOT_SET_ATT_BIT deny 00.0000
!
route-map L1intoL2 permit 10
  match ip address Pre-Agg
  set level level-2
!
ip access-list standard Pre-Agg
  !***Loopback 0***
  permit 100.111.14.1
  !***Redundant PAN interface***
  permit 10.14.1.0 0.0.0.1
!

ip access-list standard BGP_redistributed_prefixes
  permit 100.111.10.1
  permit 100.111.10.2
  permit 100.111.15.1
  permit 100.111.15.2

mpls label protocol ldp
mpls ldp explicit-null
mpls ldp graceful-restart
mpls ldp session protection
mpls ldp discovery targeted-hello accept
```

```
!
mpls ldp router-id Loopback0 force
```

BGP Configuration

```
router bgp 101
  bgp router-id 100.111.14.1
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  !***Peer group for CSGs in local RAN network***
  neighbor csg peer-group
  neighbor csg remote-as 101
  neighbor csg password lab
  neighbor csg update-source Loopback0
  !*** Peer group for local AGN-RR***
  neighbor agn-rr peer-group
  neighbor agn-rr remote-as 101
  neighbor agn-rr password lab
  neighbor agn-rr update-source Loopback0
  !***AGN-RR***
  neighbor 100.111.11.3 peer-group agn-rr
  !***CSGs in RAN access ring***
  neighbor 100.111.13.28 peer-group csg
  neighbor 100.111.13.29 peer-group csg
  neighbor 100.111.13.30 peer-group csg
  neighbor 100.111.13.31 peer-group csg
  !
  address-family ipv4
    bgp redistribute-internal
    bgp additional-paths receive
    bgp additional-paths install
    bgp nexthop trigger delay 0
    !***Advertise Loopback with common community***
    network 100.111.14.1 mask 255.255.255.255 route-map PAN_RAN_FAN_Community
    neighbor agn-rr send-community
    !***Set next-hop-self to assign local labels for RAN redistributed prefixes***
    neighbor agn-rr next-hop-self all
    !***Filter inbound prefixes***
    neighbor agn-rr route-map BGP_Ingress_Transport_Filter in
    !***Send labels with BGP routes***
    neighbor agn-rr send-label
    neighbor csg send-community
    neighbor csg route-reflector-client
    neighbor csg next-hop-self all
    neighbor csg send-label
    neighbor 100.111.11.3 activate
    neighbor 100.111.13.28 activate
    neighbor 100.111.13.29 activate
    neighbor 100.111.13.30 activate
    neighbor 100.111.13.31 activate
  exit-address-family
  !
  address-family vpnv4
    <SNIP>
  exit-address-family
  !
  address-family rtfilter unicast
    <SNIP>
  exit-address-family
  !
!
```

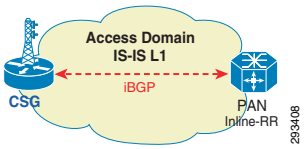
```
route-map PAN_RAN_FAN_Community permit 10
  set community 10:10

route-map BGP_Ingress_Transport_Filter permit 10
  match community PASS_Community
!
ip community-list expanded PASS_Community permit 20:20|1001:1001|2001:2001|3001:3001
```

Note Please refer to the BGP Transport Control Plane, page 3-25 for a detailed explanation of how BGP communities are used to color prefixes for selective redistribution and filtering.

Cell Site Gateway Configuration for Labeled BGP Access

This section shows the IGP/LDP configuration required on the CSGs. All access ring networks and nodes with hub-and-spoke connections subtending from the same pair of PANs are part of the same 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 enabled by extending labeled BGP to the CSGs in the RAN access. See Figure 6-45.

Figure 6-45 Cell Site Gateway (CSG)



Interface Configuration

```
!
interface Loopback0
 ip address 100.111.2.7 255.255.255.255
 ipv6 address 2001:100:111:2::7/128
 ipv6 enable
 isis tag 1500
end!
!***Link to next CSGUplink to PAN***
interface TenGigabitEthernet0/0/3
 description "To CSG-920-K0208::TenGigabitEthernet0/0/4"
 no ip address
 load-interval 30
 carrier-delay msec 0
 synchronous mode
 cdp enable
 service-policy input PMAP-NNI-I
 service-policy output PMAP-NNI-E
 service instance 20 ethernet V20
  encapsulation dot1q 20
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
 !
!!***Link to next CSG in ring***
interface TenGigabitEthernet0/0/4
 description "To CSG-920-K0206::TenGigabitEthernet0/0/4"
 no ip address
 load-interval 30
 carrier-delay msec 0
synchronous mode
 cdp enable
```

```
 service-policy input PMAP-NNI-I
 service-policy output PMAP-NNI-E
 service instance 30 ethernet
  encapsulation dot1q 30
  rewrite ingress tag pop 1 symmetric
  bridge-domain 30
 !!
interface BDI20
 ip address 10.2.6.3 255.255.255.254
 ip router isis agg-acc
 ip pim sparse-mode
 ipv6 address 2001:10:2:6::3/127
 ipv6 enable
 ipv6 router isis agg-acc
 mpls ip
 mpls ldp igp sync delay 30
 bfd interval 50 min_rx 50 multiplier 3
 isis circuit-type level-1
 isis network point-to-point!
interface BDI30
 ip address 10.2.6.4 255.255.255.254
 ip router isis agg-acc
 ip pim sparse-mode
 load-interval 30
 ipv6 address 2001:10:2:6::4/127
 ipv6 enable
 ipv6 router isis agg-acc
 mpls ip
 mpls ldp igp sync delay 30
 bfd interval 50 min_rx 50 multiplier 3
 isis circuit-type level-1
 isis network point-to-point!
```

IGP/LDP Configuration

```
router isis agg-acc
 net 49.0100.1001.1102.0007.00
 is-type level-1
 advertise passive-only
 ispf level-1
 metric-style wide
 fast-flood 10
 ip route priority high tag 1500
 set-overload-bit on-startup 120
 max-lsp-lifetime 3600
 lsp-refresh-interval 1800
 spf-interval 5 50 200
 prc-interval 5 50 200
 lsp-gen-interval 5 50 200
 no hello padding
 log-adjacency-changes
 fast-reroute per-prefix level-1 all
 fast-reroute remote-lfa level-1 mpls-ldp
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback207
 bfd all-interfaces
 !
 address-family ipv6
  multi-topology
 exit-address-family
 mpls ldp sync

mpls label protocol ldp
```

```
mpls ldp explicit-null
mpls ldp graceful-restart
mpls ldp session protection
mpls ldp igp sync holddown 2000
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
```

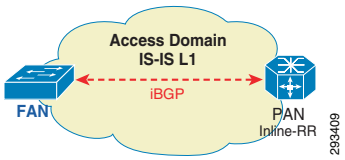
BGP Configuration

```
router bgp 101
 bgp router-id 100.111.2.7
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor pan peer-group
 neighbor pan remote-as 101
 neighbor pan password lab
 neighbor pan update-source Loopback0
 neighbor 100.111.14.1 peer-group pan
 neighbor 100.111.14.2 peer-group pan
 !
 address-family ipv4
  bgp additional-paths install
  bgp recursion host
  bgp nexthop trigger delay 1
  network 100.111.2.7 mask 255.255.255.255 route-map ACC_RAN_FAN_Community
  neighbor pan send-community
  neighbor pan aigp
  neighbor pan next-hop-self
  neighbor pan route-map BGP_Ingress_Transport_Filter in
  neighbor pan send-label
  neighbor 100.111.14.1 activate
  neighbor 100.111.14.2 activate
 exit-address-family
 !  !
  address-family vpnv4
    <SNIP>
  exit-address-family

!!!***10:10 is the common CSG community***
!***10:111 is the common CSG community for ASR920***
!***10:105 is the community identifying this CSG as being in metro-1, location-5***


route-map ACC_RAN_FAN_Community permit 10
 set community 10:10 10:105 10:11 1
```

Inter-AS Design Fixed Access Node Configuration for Labeled BGP Access

This section shows the IGP/LDP configuration required on the FANs. All access ring networks and nodes with hub-and-spoke connections subtending from the same pair of PANs are part of the same IS-IS Level 1 domain where the FANs are IS-IS L1 nodes and the PAN are L1/L2 nodes. The inter-domain LSPs are enabled by extending labeled BGP to the FANs. See Figure 6-46.

Figure 6-46 Fixed Access Node (FAN)



Interface Configuration

```
!
interface Loopback0
  ip address 100.111.7.1 255.255.255.255
!
!***Adjacent FAN interface***
interface TenGigabitEthernet0/1
  description To FAN-ME36-K0702
  no switchport
  ip address 10.7.1.0 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
  isis network point-to-point
!
!***Uplink to PAN***
interface TenGigabitEthernet0/2
  description To PAN-K0504
  no switchport
  ip address 10.5.4.3 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  isis circuit-type level-1
  isis network point-to-point
!
```

IGP/LDP Configuration

```
router isis agg-acc
  net 49.0100.1001.1100.7001.00
  is-type level-1
  ispf level-1
  metric-style wide
  fast-flood
  set-attached-bit route-map DO_NOT_SET_ATT_BIT
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 5 200
  no hello padding
  log-adjacency-changes
  !***Remote LFA FRR configuration***
  fast-reroute per-prefix level-1 all
  fast-reroute remote-lfa level-1 mpls-ldp
  passive-interface Loopback0
```

```
  bfd all-interfaces
  mpls ldp sync
!

clns filter-set DO_NOT_SET_ATT_BIT deny 00.0000
!
route-map DO_NOT_SET_ATT_BIT permit 10
  match clns address DO_NOT_SET_ATT_BIT

mpls label protocol ldp
mpls ldp explicit-null
mpls ldp session protection
mpls ldp igp sync holddown 2000
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
```

BGP Configuration

```
router bgp 101
  bgp router-id 100.111.7.1
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor pan peer-group
  neighbor pan remote-as 101
  neighbor pan password lab
  neighbor pan update-source Loopback0
  neighbor 100.111.5.4 peer-group pan
  neighbor 100.111.5.5 peer-group pan
  !
  address-family ipv4
    bgp additional-paths install
    bgp recursion host
    bgp nexthop trigger delay 6
    !***Color loopback with FAN communities***
    network 100.111.7.1 mask 255.255.255.255 route-map FAN_Community
    redistribute connected
    neighbor pan send-community
    neighbor pan aigp
    neighbor pan next-hop-self
    !***Permit only needed BGP prefixes from PANs***
    neighbor pan route-map BGP_Ingress_Transport_Filter in
    neighbor pan send-label
    neighbor 100.111.5.4 activate
    neighbor 100.111.5.5 activate
  exit-address-family
  !
  address-family vpnv4
    <SNIP>
  exit-address-family

!!!***20:20 is the common FAN community***
route-map FAN_Community permit 10
  set community 20:20

!***Permitted FAN prefixes for configured E-Line services***
ip prefix-list WL-Service-Destinations permit 100.111.7.10/32
!
route-map BGP_Ingress_Transport_Filter permit 10
  match ip address prefix-list WL-Service-Destinations
```

Dynamic Prefix List Script

Each time a new wireline service is enabled on the FAN, the IP prefix-list for the inbound route-map needs to be updated in order to allow the remote destination loopback of wireline service to be accepted. This process can be easily automated by using a simple EEM script, which is shown in this section.

With this EEM script in place on the FAN, when the operator configures a new VPWS service on the device, the remote loopback corresponding to the destination argument will automatically be added to the "WL-Service-Destinations" prefix-list of allowed wireline destinations. The script will also trigger a dynamic inbound soft reset using the clear ip bgp destination soft in command to initiate a nondisruptive dynamic route refresh.

Note The IP addresses shown in these scripts for the dynamic inbound soft reset must be updated to reflect the actual PAN addresses for the particular FAN

```
#-------------------------------------------------------------------
# EEM scripts to automatically fetch IP /32 endpoints
# of configured PWs. IP addresses are advertised via a BGP session.
# To get prefixes the inbound WL-Service-Destinations filter list
# is changed accordingly. Removing a configuration of PW removes
# also the /32 prefix from the filter list.
#
# October 2012, Cisco Systems
#-------------------------------------------------------------------

==========================================
To add PW primary and backup
Supporting EoMPLS, ATMoMPLS, CESoPSN, SAToP
==========================================

!***Handles PWE3 xconnect***
event manager applet UpdateInboundFilter11
  event cli pattern ".*xconnect.*encapsulation.*mpls" sync no skip no
  action 10 regexp " [0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 50 puts "Inbound Filter updated for $result/32"
  action 60 cli command "end"
  action 70 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 80 cli command "clear ip bgp 100.111.5.4 soft in"
  action 81 cli command "clear ip bgp 100.111.5.5 soft in"
  action 90 puts "Triggered Dynamic Inbound Soft Reset towards PANs"

!***Handles PWE3 xconnect with only PW-class***
event manager applet UpdateInboundFilter12
  event cli pattern ".*xconnect.*pw-class.*" sync no skip no
  action 10 regexp " [0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 50 puts "Inbound Filter updated for $result/32"
  action 60 cli command "end"
  action 70 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 80 cli command "clear ip bgp 100.111.5.4 soft in"
  action 81 cli command "clear ip bgp 100.111.5.5 soft in"
  action 90 puts "Triggered Dynamic Inbound Soft Reset towards PANs"
```

```
!***Handles backup PWE3 under xconnect***
event manager applet UpdateInboundFilter13
  event cli pattern ".*backup.*peer.*" sync no skip no
  action 10 regexp " [0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 50 puts "Inbound Filter updated for $result/32"
  action 60 cli command "end"
  action 70 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 80 cli command "clear ip bgp 100.111.5.4 soft in"
  action 81 cli command "clear ip bgp 100.111.5.5 soft in"
  action 90 puts "Triggered Dynamic Inbound Soft Reset towards PANs"
```

Similarly, when a wireline service is removed from the FAN, the ip prefix-list needs to be updated in order to remove the remote destination loopback of the deleted wireline service. The following two EEM scripts will automate this process through the following logic:

1. The operator removes the XConnect by using the no xconnect command. No IP address is required to remove a correct line from a prefix-list.
2. To obtain the IP address, the "tovariable_int_num<X>" applet is used with an environmental variable $_int. This applet is triggered by the interface, service instance, cem, or pvc command, which informs the variable that there can be a potential change in the configuration.
3. The applet "UpdateInboundFilter21" is triggered by the no xconnect command and uses the interface derived from the "tovariable" applets in order to obtain the IP address and remove it from the prefix-list. The applet "UpdateInboundFilter23" does the same function for the no backup peer command to handle removal of backup PW3s.

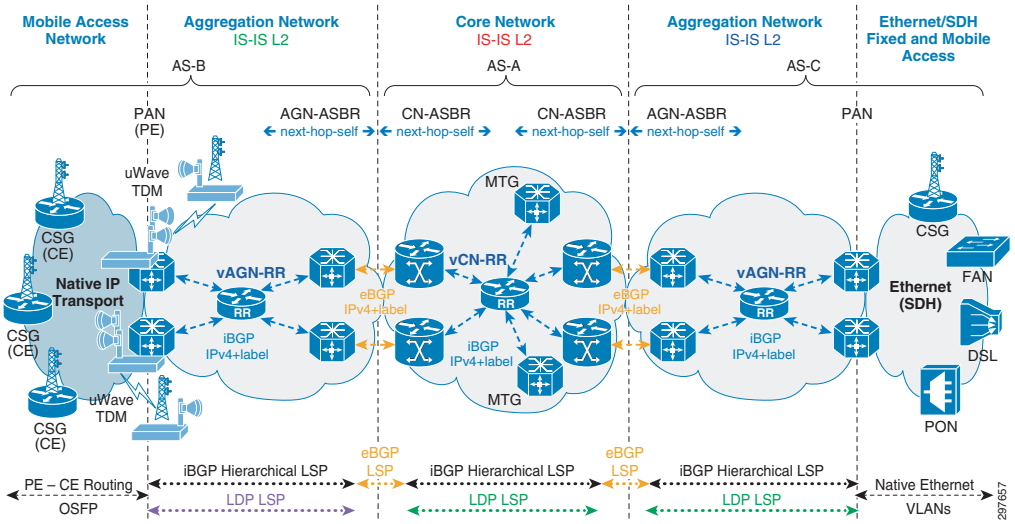
```
==========================================
To remove PW
Supporting Ethernet, CES, ATM interfaces
==========================================
!***Handles interface configurations***
event manager applet tovariable_int
  event cli pattern "^interface" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int $_cli_msg"
  action 40 cli command "event manager environment _int_sec 0"

!***Handles service instance configurations***
event manager applet tovariable_int_num1
  event cli pattern "^service instance" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int_num $_cli_msg"
  action 40 cli command "event manager environment _int_sec 1"

!***Handles cem interface configurations***
event manager applet tovariable_int_num2
  event cli pattern "^cem" sync no skip no
  action 10 cli command "enable"
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int_num $_cli_msg"
  action 40 cli command "event manager environment _int_sec 2"

!***Handles ATM pvc configurations***
event manager applet tovariable_int_num3
  event cli pattern "^pvc" sync no skip no
  action 10 cli command "enable"
```

```
  action 20 cli command "conf t"
  action 30 cli command "event manager environment _int_num $_cli_msg"
  action 40 cli command "event manager environment _int_sec 3"

!***Triggers on "no xconnect" and parses IP prefix to be removed***
no event manager applet UpdateInboundFilter21
event manager applet UpdateInboundFilter21
  event cli pattern "no xconnect" sync no skip yes
  action 10 cli command "enable"
  action 12 string trimright "$_int_num"
  action 13 set _int_num "$_string_result"
  action 19 if $_int_sec eq 0 goto 35
  action 20 cli command "show run $_int | s $_int_num"
  action 30 regexp "xconnect.*" "$_cli_result" line
  action 32 if $_int_sec ne 0 goto 40
  action 35 cli command "show run $_int | i xconnect"
  action 36 set line $_cli_result
  action 40 regexp "[0-9.]+" "$line" result
  action 50 cli command "enable"
  action 60 cli command "conf t"
  action 70 cli command "no ip prefix-list WL-Service-Destinations permit $result/32"
  action 80 cli command "$_int"
  action 81 cli command "$_int_num" action 82 cli command "no xc"
  action 92 cli command "do show run | i xconnect $result"
  action 93 string first "xconnect $result" "$_cli_result"
  action 94 if $_string_result eq "-1" goto 96
  action 95 cli command "ip prefix-list WL-Service-Destinations permit $result/32"
  action 96 cli command "end"
  action 97 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 100 cli command "clear ip bgp 100.111.5.4 soft in"
  action 110 cli command "clear ip bgp 100.111.5.5 soft in"
  action 120 puts "Triggered Dynamic Inbound Soft Reset towards PANs"

===========================================
To remove a backup PW
Supporting Ethernet, CES, ATM interfaces
===========================================

!***Triggers on "no backup peer" and parses IP prefix to be removed***
event manager applet UpdateInboundFilter23
  event cli pattern "no backup peer" sync no skip no
  action 10 regexp "[0-9.]+" "$_cli_msg" result
  action 20 cli command "enable"
  action 30 cli command "conf t"
  action 40 cli command "no ip prefix-list WL-Service-Destinations permit $result/32"
  action 96 cli command "end"
  action 97 cli command "enable"
  !***These IP addresses must match the actual PAN IP addresses***
  action 100 cli command "clear ip bgp 100.111.5.4 soft in"
  action 110 cli command "clear ip bgp 100.111.5.5 soft in"
  action 120 puts "Triggered Dynamic Inbound Soft Reset towards PANs"

===========================================
```

Non-MPLS Access

In this model, the core and aggregation networks are integrated with unified MPLS LSPs by extending labeled BGP from the core to the PANs in the aggregation domain. Any node in the network that requires inter-domain LSPs to reach nodes in a remote domain acts as a labeled BGP PE and runs BGP labeled-unicast with its corresponding local RRs. See Figure 6-47.

Figure 6-47 Unified MPLS Transport for Inter-AS Design with non-MPLS Access



Note The network infrastructure organization of this model at the top layers of network, namely the core and aggregation domains, is exactly the same as that defined in "MPLS Access." The difference here is that labeled BGP spans only the core and aggregation networks and does not extend to the RAN access. Instead, the end-to-end unified MPLS LSP is extended into the RAN access with selective redistribution between labeled BGP and the RAN access domain IGP at the PAN. For configuration details on the Core Route Reflector, MTG, Core ASBR, AGN-RR, Aggregation ASBR, and Aggregation SE node, please see Large Network Transport Architecture Design - Inter-AS, page 3-17, because the same configuration also applies to this model.

In this model, the access network could be one of the following options:

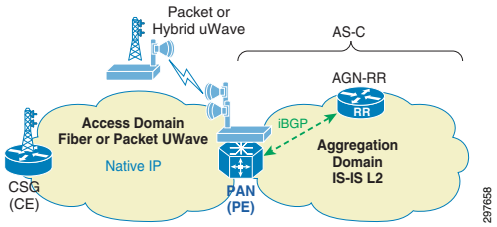
- CSGs in point-to-point or ring topologies over fiber or packet microwave running native IP transport, supporting 3G/LTE services. In this case, the CSGs act as CEs and PANs are the L3 MPLS VPN PEs enabling the backhaul. The base transceiver station (BTS) or ATM NodeBs can connect to the PANs with time-division multiplexing (TDM) microwave for 2G and 3G ATM-based services. Here the PANs enable the L2 MPLS VPN service with pseudowire-based circuit emulation for backhaul to the base station controller/radio network controller (BSC/RNC).
- FANs in point-to-point topologies over fiber access running native Ethernet, supporting residential, business, and even mobile services. The FAN may be a fiber access node or a GPON OLT. In this case, the PANs provide service edge functionality for the services from the FANs and connect the services to the proper L2VPN or L3VPN service backhaul mechanism.

In either scenario, the MPLS services are always enabled by the PANs in the aggregation network.

Pre-Aggregation Node Configuration

This section shows the IGP/LDP configuration required to build the intra-domain LSPs and the BGP configuration required to build the inter-domain LSPs in the aggregation network. See Figure 6-48.

Figure 6-48 Pre-Aggregation Node (PAN)



Interface Configuration

```
interface Loopback0
  ip address 100.111.14.1 255.255.255.255
!
!***Redundant PAN interface***
interface TenGigabitEthernet0/0/0
  description To PAN-903-K1402::TenGigabitEthernet0/0/0
  ip address 10.14.1.0 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis network point-to-point
  isis metric 10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
!***AGN uplink interface***
interface TenGigabitEthernet0/1/0
  description To AGN-K0301::T0/0/0/2
  ip address 10.3.1.3 255.255.255.254
  ip router isis agg-acc
  load-interval 30
  mpls ip
  mpls ldp igp sync delay 10
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  cdp enable
  isis circuit-type level-2-only
  isis network point-to-point
  isis metric 10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
!***Interface toward native IP CE ring in MPLS VPN RFS***
!***Shown here for reference. Not part of Unified MPLS config.***
interface GigabitEthernet0/4/2
  description To CSG-901-K1314
  vrf forwarding RFS
  ip address 10.13.14.1 255.255.255.254
  ip ospf network point-to-point
  load-interval 30
  negotiation auto
  bfd interval 50 min_rx 50 multiplier 3
  no bfd echo
  hold-queue 350 in
```

```
  hold-queue 2000 out
!
!***Interface toward native Ethernet Fixed Access Node***
!***Shown here for reference. Not part of Unified MPLS config.***
!***Services will be configured under service instances***
interface GigabitEthernet0/3/3
  no ip address
  load-interval 30
  negotiation auto
  no keepalive
```

IGP/LDP Configuration

```
router isis agg-acc
  net 49.0100.1001.1101.4001.00
  !***PAN is a IS-IS Level-1-2 node***
  ispf level-1-2
  metric-style wide
  fast-flood
  set-overload-bit on-startup 180
  max-lsp-lifetime 65535
  lsp-refresh-interval 65000
  spf-interval 5 50 200
  prc-interval 5 50 200
  lsp-gen-interval 5 5 200
  no hello padding
  log-adjacency-changes
  nsf cisco
  !***Remote LFA FRR***
  fast-reroute per-prefix level-2 all
  fast-reroute remote-lfa level-2 mpls-ldp
  passive-interface Loopback0
  bfd all-interfaces
  mpls ldp sync

mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
```

BGP Configuration

```
router bgp 101
  bgp router-id 100.111.14.1
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no bgp default ipv4-unicast
  !***Peer group for local AGN-RR***
  neighbor agn-rr peer-group
  neighbor agn-rr remote-as 101
  neighbor agn-rr password lab
  neighbor agn-rr update-source Loopback0
  neighbor 100.111.11.3 peer-group agn-rr
  !
  !***Address family for RFC 3107 based transport***
  address-family ipv4
    bgp redistribute-internal
    bgp nexthop trigger delay 2
    !***Advertise Loopback-0 with PAN Community***
    network 100.111.14.1 mask 255.255.255.255 route-map RAN_FAN_Community
    neighbor agn-rr send-community
    neighbor agn-rr aigp
```

```
    neighbor agn-rr next-hop-self all
    !***Send labels with BGP routes***
    neighbor agn-rr send-label
    !***AGN-RR***
    neighbor 100.111.15.5 activate
  exit-address-family
  !
  address-family ipv4 vrf RFS
    <SNIP>
  exit-address-family
  !
!

route-map RAN_FAN_Community permit 10
  !***10:10 is the common RAN community***
  !***20:20 is the common Wireline community***
  set community 10:10 20:20
```

Access Network Implementation

Implementation of the acces nework is common for Large Network architectures across Single AS or Multi-Area aggregation and core routing design models. Please refer to Large Network Non-IP/MPLS Access Network Implementation, page 6-124 for details on the implementation of Non-IP/MPLS Access networks with the Large Networks.

Large Network Non-IP/MPLS Access Network Implementation

Single Homed Hub and Spoke Ethernet Access

In the Large Network, Single Homed topologies for hub-and-spoke access have been implemented for PON access.

The following configuration example shows the implementation of Single Homed hub-and-spoke Ethernet access on PAN nodes, PAN-K0504, and the OLT, OLT-3. A similar configuration applies to AGN, AGN-K0301, and OLT, OLT-2.

Aggregation Nodes Configuration

NNI Interfaces

```
interface TenGigE0/0/0/2
 description Connection to OLT360_3 Port10/2
 bundle id 102 mode active
 load-interval 30
 transceiver permit pid all
!

interface TenGigE0/0/2/1
 description Connection to OLT360_3 Port10/2
 bundle id 102 mode active
 load-interval 30
 transceiver permit pid all
!
interface Bundle-Ether102
!
```

Fixed Access Node Configuration: PON OLT

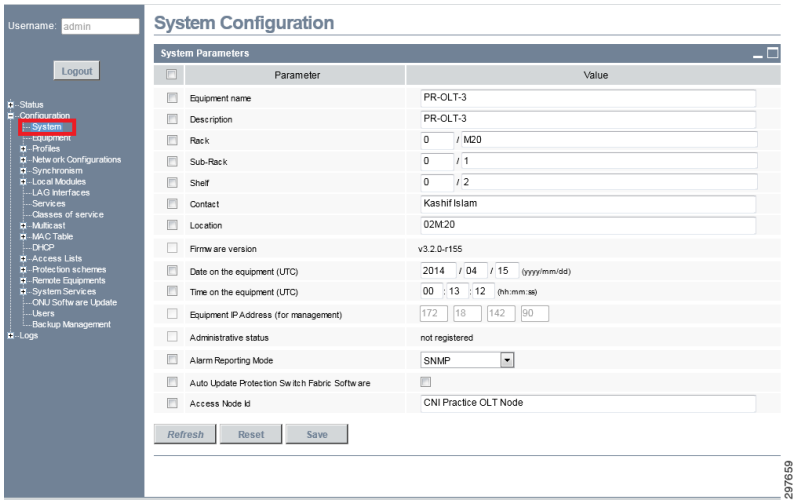
This section shows the basic setup for the Cisco ME 4600 PON OLT. Configuration includes the provisioning of the following:

- System
- Network
- Equipment
- Ethernet uplink ports
- LAG interface
- ONU profiles
- PON downlink ports
- ONU discovery
- ONU configuration

System Configuration

You configure the system by setting logistics-related information such as the system name, location, contact owner, date, and time.

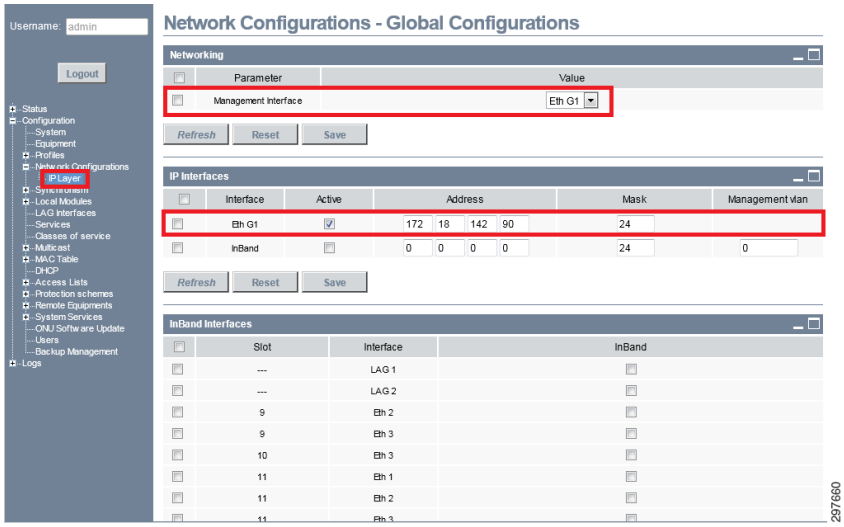
Figure 6-49 System Configuration



Network Configuration

You configure the network configuration by choosing the Management Interface and setting its address.

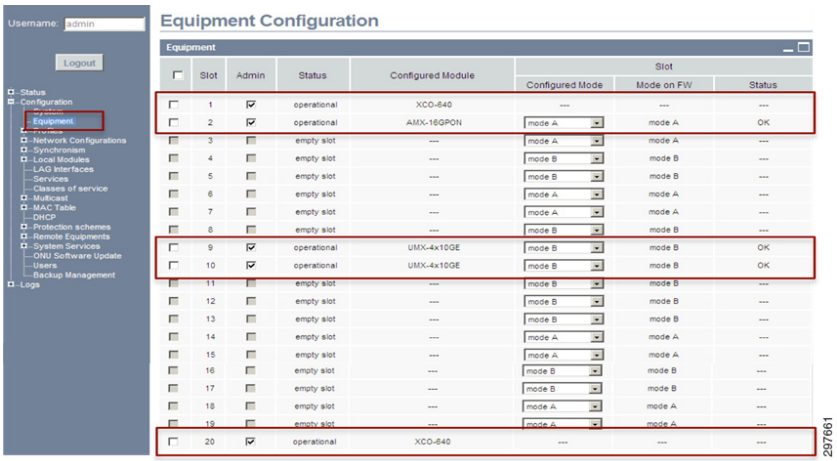
Figure 6-50 Network Configuration



Equipment Configuration

Using administrative credentials, you configure by bringing up of the various system components such as I/O line cards and fabric cards.

Figure 6-51 Equipment Configuration



Ethernet Uplink Ports Configuration

Using administrative credentials, you configure Ethernet uplink ports by enabling the port, selecting the media type, enabling or disabling flow control, and setting the MTU.

Figure 6-52 Ethernet Uplink Ports Configuration 1

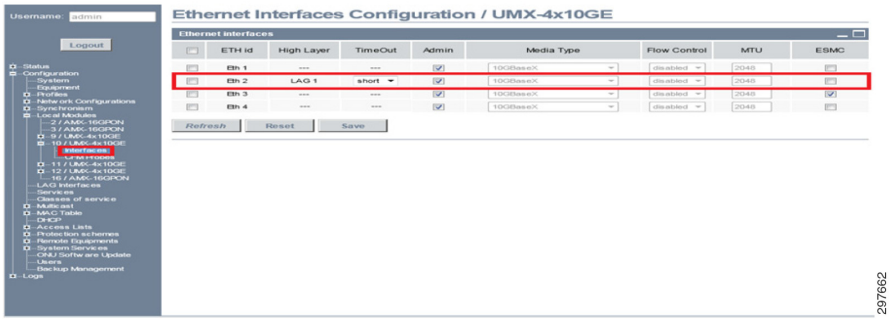
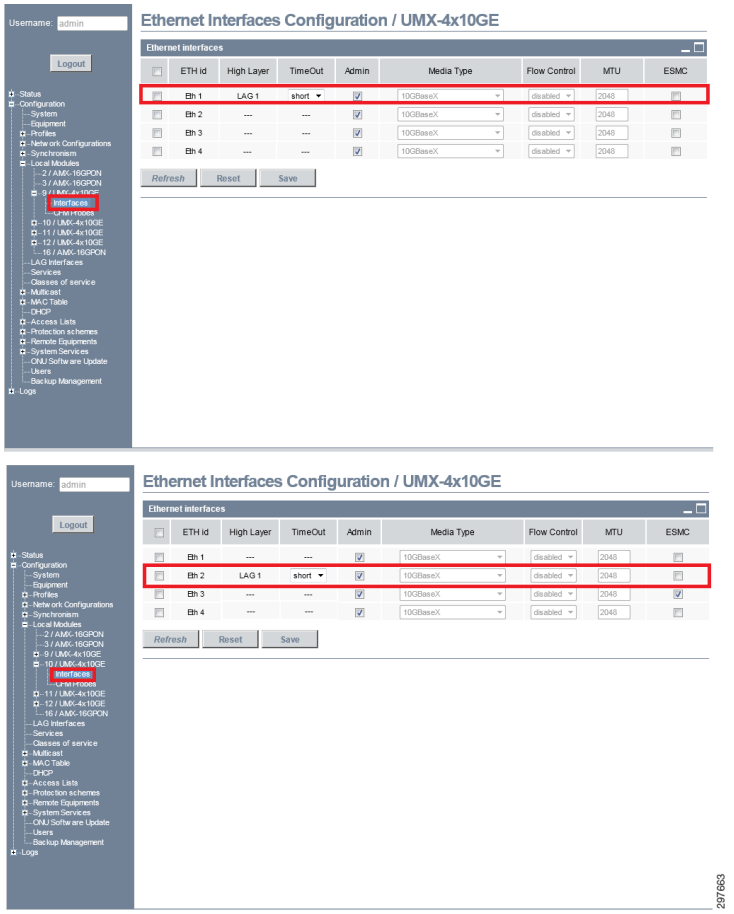


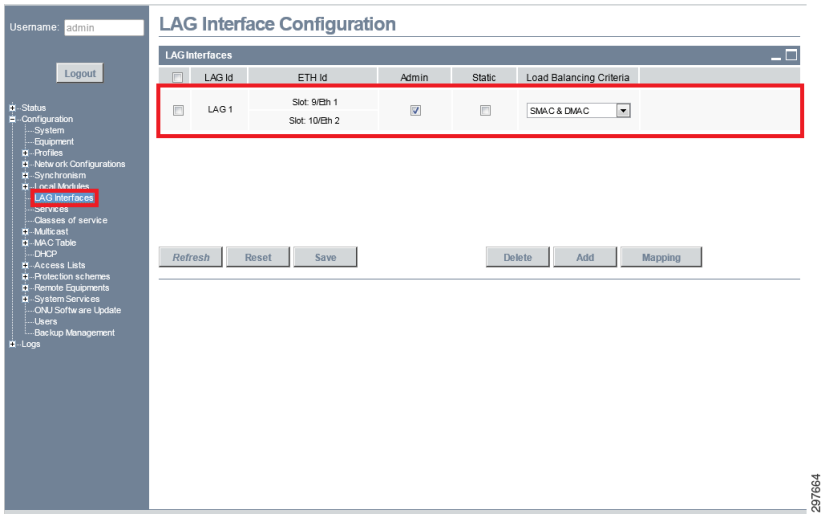
Figure 6-53 Ethernet Uplink Ports Configuration 2



LAG Interface Configuration

You configure a LAG interface by selecting the uplink Ethernet ports to be bundled and setting the load balancing algorithm.

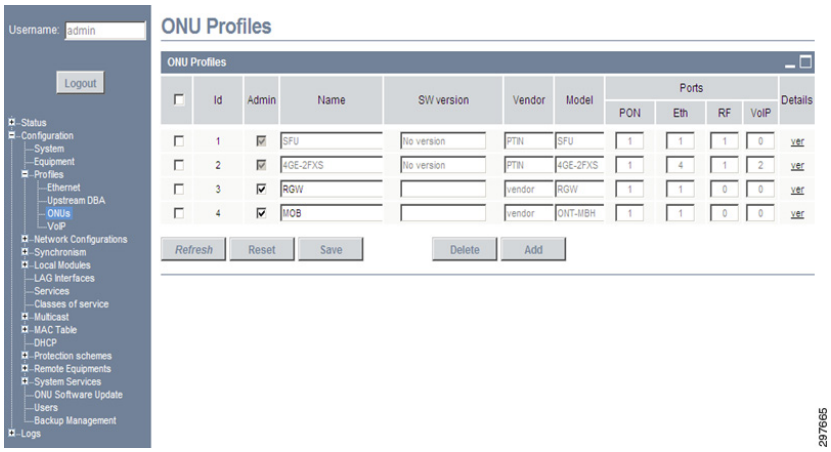
Figure 6-54 LAG Interface Configuration



ONU Profiles Configuration

ONU profiles describe the hardware layout of the ONU devices connected to the OLT node.

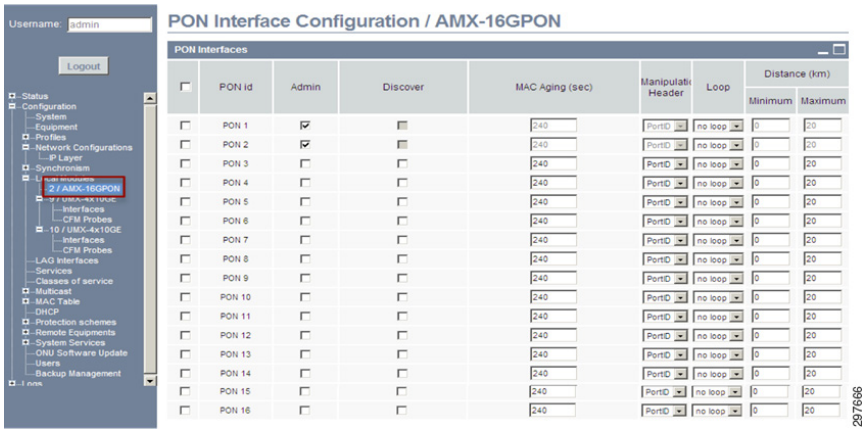
Figure 6-55 ONU Profiles Configuration



PON Downlink Ports Configuration

Using administrative credentials, you configure Ethernet uplink ports by enabling the port and setting the minimum and maximum distance between ONUs and OLT.

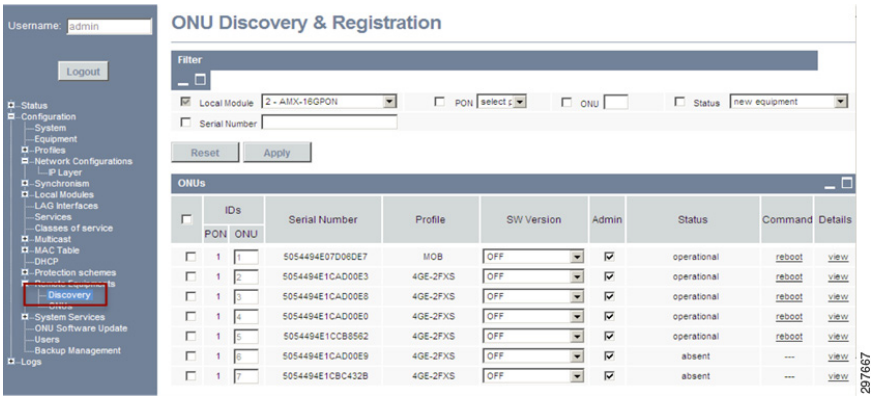
Figure 6-56 PON Downlink Ports Configuration



ONU Discovery Configuration

ONU devices are pre-provisioned on the ONU and their presence and operational state is dynamically discovered. To pre-provision a ONU choose a unique ID number, specify its serial number, and map it to a previously created profile.

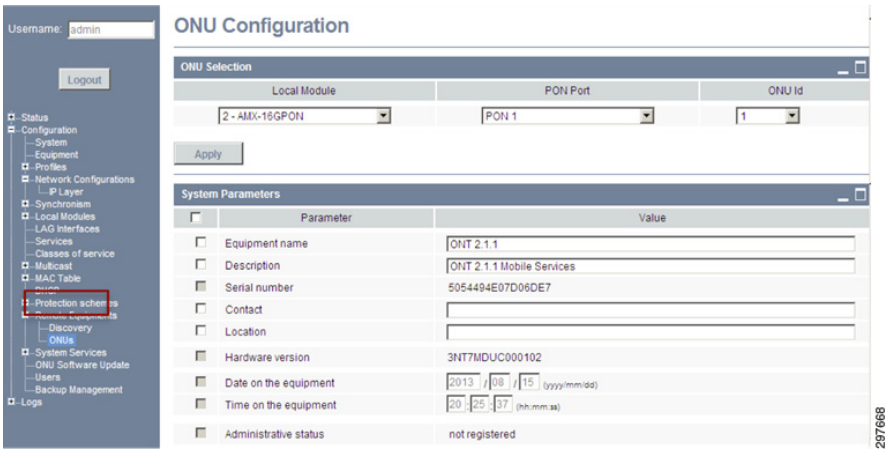
Figure 6-57 ONU Discovery Configuration



ONU Configuration

Once pre-provisioned, you can apply name, location, date and time settings to the ONU device.

Figure 6-58 ONU Configuration



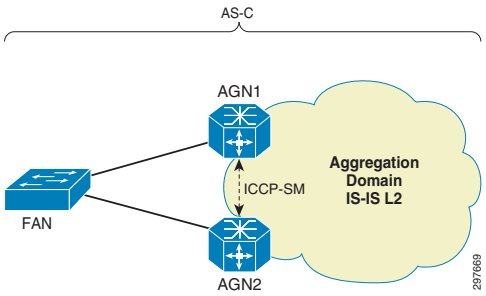
Dual-Homed Hub-and-Spoke Ethernet Access

In the Large Network, Dual Homed topologies for hub-and-spoke access have been implemented for FTTH access and in the Per VLAN Active/Active MC-LAG (pseudo mLACP) mode.

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

Figure 6-59 illustrates the implementation of hub-and-spoke Ethernet access with MC-LAG operating in per VLAN active/active load balancing.

Figure 6-59 Per VLAN Active/Active MC-LAG



The FAN access node, a ME 3400, connects to each AGN via standalone Ethernet links or Bundle interfaces that are part of a common bridge domain(s). All the links terminate in a common multi-chassis bundle interface at the AGN and are placed in active or hot-standby state based on node and VLAN via ICCP-SM negotiation.

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

The following configuration example shows the implementation of active/active per VLAN MC-LAG for VLANs 100 and 101, on the AGN nodes, AGN-K0301 and AGN-K0302, and the FAN, ME-K0903.

Aggregation Node Configuration

AGN1: Active Point-of-Attachment (PoA) AGN-A9K-K0301: ASR9000

NNI Interfaces

```
interface GigabitEthernet0/3/1/12
 bundle id 1 mode on
!
interface bundle-ether1
!
interface bundle-ether1.100 l2transport
 encapsulation dot1q 100
!
interface bundle-ether1.101 l2transport
 encapsulation dot1q 101
!
```

ICCP and ICCP-SM and Multichassis LACP

```
!*** ICCP configuration ***
redundancy
 iccp
  group 1
   member
    neighbor 100.111.3.2
   !
   backbone
    interface Ten0/2/0/0
    interface Ten0/2/0/1
   !
l2vpn
 !*** ICCP-SM configuration ***
 redundancy
  iccp group 1
   multi-homing node-id 1
   interface Bundle-Ether1
    primary vlan 100
    secondary vlan 101
    recovery delay 60
   !
```

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

NNI Interfaces

```
interface GigabitEthernet0/0/1/1
 bundle id 1 mode on
!
interface Bundle-Ether1
!
interface Bundle-Ether1.100 l2transport
 encapsulation dot1q 100
!
interface Bundle-Ether1.101 l2transport
 encapsulation dot1q 101
!
```

ICCP and Multichassis LACP

The ICCP redundancy group is configured as follows:

```
!*** ICCP Configuration ***
```

```
redundancy
 iccp
  group 1
   member
    neighbor 100.111.3.1
   !
   backbone
    interface TenGigE0/2/0/0
    interface TenGigE0/2/0/1
   !
  !
 !
!
!*** ICCP-SM Configuration ***
l2vpn
 redundancy
  iccp group 1
   multi-homing node-id 2
   interface Bundle-Ether1
    primary vlan 101
    secondary vlan 100
    recovery delay 60
   !
  !
 !
!
```

Fixed Access Node: ME3400

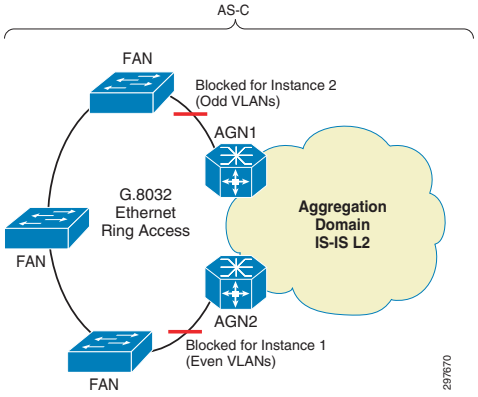
NNI Interfaces

```
!*** Interfaces towards the AGN nodes ***
interface GigabitEthernet0/13
 description Connects to AGN-9006-K0301 Gig 0/3/1/12
 port-type nni
 switchport mode trunk
interface GigabitEthernet0/14
 description Connects to AGN-9006-K0302 Gig 0/3/1/12
 port-type nni
 switchport mode trunk
```

G.8032-enabled Ethernet Access Ring Implementation

This section discusses the implementation and configuration details for G.8032-enabled Ethernet access ring. See Figure 6-60.

Figure 6-60 G.8032-enabled Ethernet Access Ring Implementation



The G.8032-enabled Ethernet ring implements two instances for odd and even VLAN numbers, respectively.

In steady-state conditions, the AGN nodes are configured as RPL owners for:

- AGN1: RPL owner on Instance 2 and for odd VLANs. RPL is the ring-facing link.
- AGN2: RPL owner on Instance 1 and even VLANs. RPL is the ring-facing link.

In addition, VLAN 99 is used to carry APS channel traffic for instance 1 and VLAN 199 is used to carry APS channel traffic for instance 2.

Aggregation Node Configuration

The following configuration applies to AGN1 and AGN2, respectively AGN-K0301 and AGN-K1102 in the system test topology for a Large Network.

AGN1

Ring-facing Interfaces Configuration

```
interface TenGigE0/3/0/0
!
 interface TenGigE0/3/0/0.99 l2transport
 encapsulation dot1q 99
!
interface TenGigE0/3/0/0.199 l2transport
 encapsulation dot1q 199

G.8032 Instances configuration
l2vpn
 ethernet ring g8032 ring_test
  port0 interface TenGigE0/3/0/0
  !
  port1 none
  open-ring
  instance 1
   inclusion-list vlan-ids 99,106,108,118,500,64,604,1001-2000
   aps-channel
    port0 interface TenGigE0/3/0/0.99
    port1 none
   !
  !
  instance 2
   profile ring_profile
```

```
  !*** RPL Owner for Instance 2 vlans ***
  rpl port0 owner
  inclusion-list vlan-ids 199,107,109,109,119,501,2001-3000
  aps-channel
   port0 interface TenGigE0/3/0/0.199
   port1 none
  !
 !
!
```

AGN2

Ring-facing Interfaces Configuration

```
interface TenGigE0/2/1/1
!
interface TenGigE0/2/1/1.99 l2transport
 encapsulation dot1q 99
!
interface TenGigE0/2/1/1.199 l2transport
 encapsulation dot1q 199
```

G.8032 Instances Configuration

```
ethernet ring g8032 ring_test
  port0 interface TenGigE0/2/1/1
  !
  port1 none
  open-ring
  instance 1
   !*** RPL Owner for instance 1 ***
   rpl port0 owner
   inclusion-list vlan-ids 99,106,108,118,500,502,64,604,1001-2000
   aps-channel
    port0 interface TenGigE0/2/1/1.99
    port1 none
   !
  !
  instance 2
   profile ring_profile
   inclusion-list vlan-ids 199,107,109,119,501
   aps-channel
    port0 interface TenGigE0/2/1/1.199
    port1 none
   !
  !
```

Ring FAN Node Configuration

The following configuration applies to FANs: CE-ME36-K0801 / 802 / 803 / 804 / 805 in the system test topology for a Large Network.

Ring Interfaces Configuration

```
interface TenGigabitEthernet0/1
 description to 802 ten 0/1
 switchport trunk allowed vlan none
 switchport mode trunk
 load-interval 30
 service instance 99 ethernet
  encapsulation dot1q 99
```

```
  rewrite ingress tag pop 1 symmetric
  bridge-domain 99
 !
 service instance 199 ethernet
  encapsulation dot1q 199
  rewrite ingress tag pop 1 symmetric
  bridge-domain 199
 !
!
interface TenGigabitEthernet0/2
 description to 804 int ten 0/2
 switchport trunk allowed vlan none
 switchport mode trunk
 load-interval 30
 service instance 99 ethernet
  encapsulation dot1q 99
  rewrite ingress tag pop 1 symmetric
  bridge-domain 99
 !
 service instance 199 ethernet
  encapsulation dot1q 199
  rewrite ingress tag pop 1 symmetric
  bridge-domain 199
 !
!
```

G.8032 Instances Configuration

```
ethernet ring g8032 ring_test
 open-ring
 exclusion-list vlan-ids 1000
 port0 interface TenGigabitEthernet0/1
 port1 interface TenGigabitEthernet0/2
 instance 1
  profile ring_profile
  !*** Instance VLANs ***
  inclusion-list vlan-ids 64,99,106,108,118,500,502,604,1001-2000
  aps-channel
   port0 service instance 99
   port1 service instance 99
  !
 !
 instance 2
  profile ring_profile
  inclusion-list vlan-ids 107,109,119,199,501,2001-3000
  aps-channel
   port0 service instance 199
   port1 service instance 199
  !
 !
!
```

Functional Components Implementation

This chapter includes the following major topics:

Quality of Service

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

This section covers the aggregate QoS policies implemented on the NNI interfaces in the transport network, illustrating the treatment of all services traversing the transport network. QoS policies for UNI interfaces and other service-specific QoS aspects are covered in the QoS section of the service-specific Cisco EPN design and implementation guides.

The classification criteria used to implement the DiffServ PHBs is covered in Figure 7-1.

Figure 7-1 Differentiated Service QoS Domain

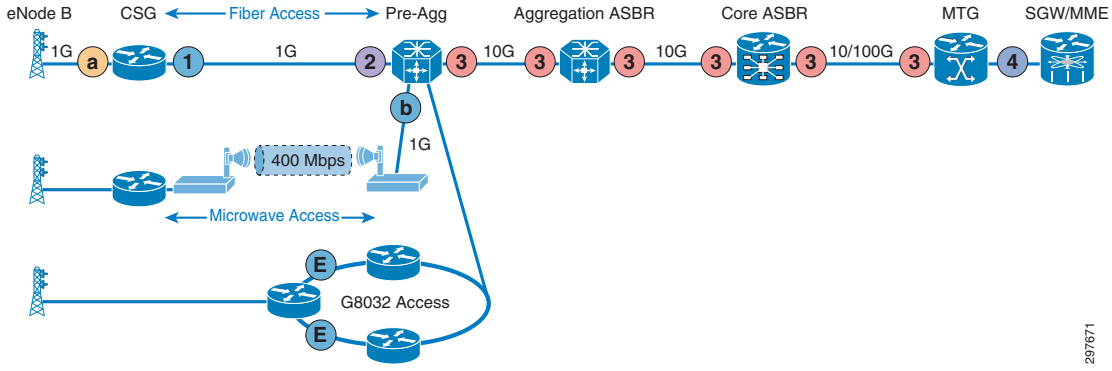
Traffic Class	PHB	Unified MPLS Transport		Service Edge			Fixed/Mobile Access Ethernet/TDM/ATM UNI		
		Core, Aggregation, Access		Business PWHE		Res/Bus Ethernet	M	R, B, M	M, B
		DSCP	EXP	DSCP	EXP	802.1P	DSCP	802.1P	ATM
Network Management	AF	56	7	56	7	7	56	(7)	VBR-nrt
Network Control Protocols	AF	48	6	48	6	6	48	(6)	VBR-nrt
Residential Voice Business Realtime Network Sync (1588 PTP) Mobility & Signaling traffic Mobile Conversation/Streaming	EF	46	5	46	5	5	46	5	CBR
Residential TV and Video Distribution	AF	32	4	32	4	4	NA	4	NA
Business Telepresence	AF	24	3	24	3	3	NA	3	NA
Business Critical In Contract Out of Contract	AF	16 8	2 1	16 8	2 1	2 1	16 8	2 1	VBR-nrt
Residential HSI Business Best Effort Mobile Background VQE Fast Channel Change, Repair	BE	0	0	0	0	0	0	0	UBR

293241

In Figure 7-2, the following elements are called out:

- (a) H-QoS policy map on CSG UNIs
- (b) H-QoS policy map on pre-aggregation NNI connecting microwave access network
- (1) (2) Flat QoS policy map on CSG and pre-aggregation NNIs in fiber access network
- (3) Flat QoS policy map on aggregation and core network NNIs
- (4) Flat QoS policy map on ingress for ATM and TDM UNIs

Figure 7-2 QoS Enforcement Points



CSG QoS Configuration

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

Class Maps

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

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

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

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

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

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

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

NNI Classification for MPLS Access

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

NNI Classification for G.8032 Access

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

Fiber Ring NNI QoS Policy Maps

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

```
!***QoS enforcement point (1).***
```

```
!***Interface connecting Fiber Access Ring.***
interface GigabitEthernet0/10
  service-policy input PMAP-NNI-I
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
policy-map PMAP-NNI-I
  class CMAP-RT-EXP
    set qos-group 5
  class CMAP-NMgmt-EXP
    set qos-group 7
  class CMAP-CTRL-EXP
    set qos-group 6
  class CMAP-Video-EXP
    set qos-group 4
  class class-default
!
policy-map PMAP-NNI-E
  class CMAP-RT-GRP
    priority percent 20
  class CMAP-NMgmt-GRP
    bandwidth percent 5
  class CMAP-CTRL-GRP
    bandwidth percent 2
  class CMAP-Video-GRP
    bandwidth percent 50
  class class-default
```

Note The real time traffic mapped to the priority or low-latency queue (LLQ) is implicitly policed at rate configured.

Microwave Ring NNI QoS Policy Maps

- The model assumes a microwave system that has the ability to do DiffServ QoS that matches with the access node NNI expedited forwarding (EF) and assured forwarding (AF) DiffServ classes.
- For downstream and transit traffic, an H-QoS policy map with parent shaper and child queuing is applied in the NNI egress direction. Parent shaping rate can be adapted by Microwave Adaptive Code Modulation (ACM) Integration. For more information, see the "Transport Integration with Microwave ACM" section on page 7-14 in this guide.
  - MPLS Experimental bit (EXP) classification for CSG ring local traffic needs MPLS explicit-null (mpls ldp explicit-null) over all CSG routers. MPLS EXP must be marked indirectly by marking qos- group on ingress.
- For upstream and transit traffic, a QoS policy map with DiffServ queuing based on QoS groups is used, with:
  - QoS group mapping for traffic transiting the access ring being done at the ingress NNI.

```
policy-map PMAP-uWave-NNI-E-C
  class CMAP-RT-GRP
    priority percent 20
  class CMAP-NMgmt-GRP
    bandwidth percent 5
  class CMAP-CTRL-GRP
    bandwidth percent 2
  class CMAP-Video-GRP
    bandwidth percent 50
  class class-default
```

```
policy-map PMAP-uWave-NNI-E-P
  class class-default
  !***Nominal transmission rate of 400Mbps***
  shape average 400000000
    service-policy PMAP-uWave-NNI-E-C
!
policy-map PMAP-uWave-NNI-I
  class CMAP-RT
    set qos-group 5
  class CMAP-NMgmt
    set qos-group 7
  class CMAP-CTRL
    set qos-group 6
  class CMAP-Video
    set qos-group 4
  class class-default
```

G.8032 Fiber Ring NNI QoS Policy Maps

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

```
!*** QoS enforcement point (E)***
!***Interface connecting to G.8032 Fiber Access Ring.***
interface TenGigabitEthernet0/0
 service-policy input PMAP-NNI-I
 service-policy output PMAP-NNI-E
!
policy-map PMAP-NNI-E
!*** Egress policy on NNI PORT ***
 class CMAP-RT-GRP
  priority percent 20
 class CMAP-BC-GRP
  bandwidth percent 5
 class CMAP-BC-Tele-GRP
  bandwidth percent 10
 class class-default
!
policy-map PMAP-NNI-I
!*** Ingress Policy on NNI Port ***
 class CMAP-BC-COS
  set qos-group 2
 class CMAP-RT-COS
  set qos-group 5
  police rate 1000000
 class CMAP-BC-Tele-COS
  set qos-group 3
!
```

FAN QoS Configuration

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

Class Maps

- QoS classification at the UNI in the ingress direction for upstream traffic is based on IP DSCP with the marking done by the connected device for residential and mobile services.

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

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

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

- QoS classification at the UNI in the egress direction for downstream traffic is based on either DSCP or CoS classification, depending upon the particular service.
- QoS classification at the NNI in the ingress and egress direction is based on MPLS EXP.

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

Fiber Ring UNI QoS Policy Maps

The ingress and egress QoS service policies on the UNI are service-specific, and thus are covered in the respective service-specific Cisco EPN design and implementation guide.

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

```
!
!***QoS enforcement point (1).***
!***Interface connecting Fiber Access Ring.***
interface GigabitEthernet0/10
  service-policy output PMAP-NNI-E
  hold-queue 350 in
  hold-queue 2000 out
!
policy-map PMAP-NNI-E
  class CMAP-RT-EXP
    police 1000000000
    priority
  class CMAP-BC-EXP
    bandwidth percent 10
  class CMAP-BC-Tele-EXP
    bandwidth percent 20
  class CMAP-Video-EXP
    bandwidth percent 20
  class CMAP-NMgmt-EXP
    bandwidth percent 5
  class CMAP-CTRL-EXP
    bandwidth percent 2
  class class-default
```

Pre-Aggregation Node QoS Configuration (Cisco ASR 903)

Class Maps

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

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

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

```
!***Voice/Real-Time traffic***
```

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

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

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

Microwave Access NNI QoS Policy Map

- For downstream traffic, an H-QoS policy map with parent shaper and child queuing is applied in the egress direction to 1-G interface connecting microwave access. The 1-G interface is shaped to 400 Mbps microwave link capacity.

```
!***QoS enforcement point (b).***
!***Interface connecting uWave Access Network.***
interface GigabitEthernet0/1
  service-policy output PMAP-uW-NNI-P-E

policy-map PMAP-uW-NNI-C-E
  class CMAP-RT-EXP
    priority
  class CMAP-CTRL-EXP
    bandwidth remaining ratio 1
  class CMAP-NMgmt-EXP
    bandwidth remaining ratio 3
  class CMAP-HVideo-EXP
    bandwidth remaining ratio 2
!
policy-map PMAP-NNI-uw-P-E
  class class-default
  shape average 400000000
    service-policy PMAP-NNI-uw-C-E
```

Fiber Ring UNI QoS Policy Maps

The ingress and egress QoS service policies on the UNI are service-specific and thus are covered in the respective service-specific Cisco EPN design and implementation guide.

Fiber Access NNI QoS Policy Maps

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

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

Aggregation NNI QoS Policy Map

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

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

Aggregation and Core Network QoS Configuration

Class Maps

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

```
class-map match-any CMAP-BC-EXP
  match mpls experimental topmost 1 2
  end-class-map
!
class-map match-any CMAP-BUS-Tele-EXP
  match mpls experimental topmost 3
  end-class-map
!
class-map match-any CMAP-Video-EXP
  match mpls experimental topmost 4
  end-class-map
!
class-map match-any CMAP-RT-EXP
  match mpls experimental topmost 5
  end-class-map
!
class-map match-any CMAP-CTRL-EXP
  match mpls experimental topmost 6
  end-class-map
!
class-map match-any CMAP-NMgmt-EXP
  match mpls experimental topmost 7
  end-class-map
```

NNI QoS Policy Maps

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

```
!***10Gbps NNI***
policy-map PMAP-NNI-E
  class CMAP-RT-EXP
    priority level 1
    police rate 1 gbps
    !
  !
  class CMAP-CTRL-EXP
    bandwidth 200 mbps
  !
  class CMAP-NMgmt-EXP
    bandwidth 500 mbps
  !
  class CMAP-Video-EXP
    bandwidth 2 gbps
  !
  class CMAP-BC-EXP
    bandwidth 1 gbps
    !***Random Detect preserves CIR over PIR traffic***
    random-detect exp 2 80 ms 100 ms
    random-detect exp 1 40 ms 50 ms
  !
  class CMAP-BUS-Tele-EXP
    bandwidth 2 gbps
  !
  class class-default
  !
```

```
  end-policy-map

!***100Gbps NNI***
policy-map PMAP-NNI-100GE-E
  class CMAP-RT-EXP
    priority level 1
    police rate 10 gbps
    !
  !
  class CMAP-CTRL-EXP
    bandwidth 2 gbps
  !
  class CMAP-NMgmt-EXP
    bandwidth 5 gbps
  !
  class CMAP-Video-EXP
    bandwidth 20 gbps
  !
  class CMAP-BC-EXP
    bandwidth 10 gbps
    !***Random Detect preserves CIR over PIR traffic***
    random-detect exp 2 80 ms 100 ms
    random-detect exp 1 40 ms 50 ms
  !
  class CMAP-BUS-Tele-EXP
    bandwidth 20 gbps
  !
  class class-default
  !
  end-policy-map
!
```

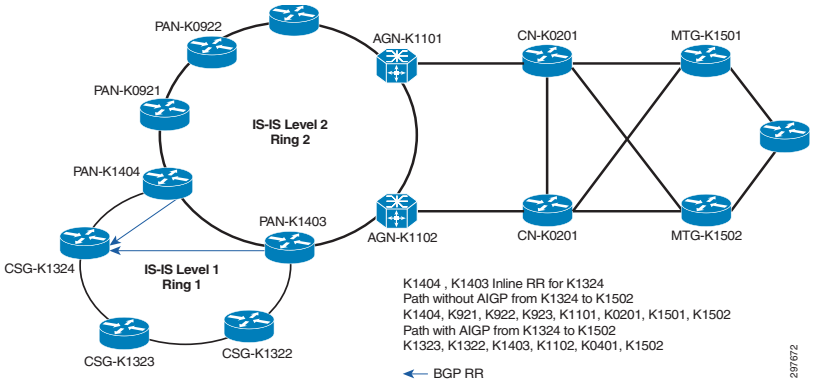
BGP AIGP

For deployments in which a single administration runs several contiguous BGP networks, it can be desirable for BGP to select paths based on a metric, just as an IGP would do.

The following example describes how AIGP can be useful in choosing the shortest path that spans across two different IGP domains. As per Figure 7-3:

- In the absence of AIGP, for an X2 communication that happens between CSGK1324 and MTG 1501, the path taken is the longer path through PANK1404 due to the BGP computation of CSGK1324 where it chooses the closest IGP path to the next hop.
- When AIGP is enabled, the routes reflected by PAN K1403 and PAN K1404 contain additional information about the IGP cost to the destination. This helps the CSG prefix choose the overall shortest path, which is through PANK1403, rather than the shortest path in its own IGP domain.

Figure 7-3 AIGP Example



The configurations of the feature are shown below.

Note In IOS XR, AIGP is by default enabled for IBGP neighbors. It is not enabled by default for EBGP neighbors and must be manually enabled for eBGP peers. In IOS, manual configuration of AIGP is required for both IBGP and EBGP peering.

IOS Configuration (PAN K1403)

```
router bgp 1000
  !
 address-family ipv4
  bgp additional-paths receive
  bgp additional-paths install
  bgp nexthop trigger delay 0
  network 100.111.14.3 mask 255.255.255.255 route-map PAN_RAN_FAN_Community
  neighbor cn-rr send-community
  !***enabling AIGP for the neighbor***!
  neighbor cn-rr aigp
  neighbor csg aigp
!
route-map PAN_RAN_FAN_Community permit 10
 set aigp-metric igp-metric
```

IOS-XR Configuration (MTG K1502)

```
router bgp 1000
address-family ipv4 unicast
  network 100.111.15.2/32 route-policy MSE_IGW_Community
neighbor-group cn-rr
  use session-group intra-as
  address-family ipv4 labeled-unicast
   route-policy BGP_Ingress_Transport_Filter in
   maximum-prefix 150000 85 warning-only
   next-hop-self
  !
!***Setting the metric of locally originated prefixes **!
route-policy MSE_IGW_Community
  set community MSE_Community
  set community IGW_Community additive
  set aigp-metric igp-cost
end-policy
```

Transport Integration with Microwave ACM

Nearly half of all mobile backhaul access networks worldwide utilize microwave links, necessitating the inclusion of microwave technology in the Cisco EPN System architecture. The Cisco EPN System integrates microwave radios in the access network in order to validate transport of traffic over microwave links, including such aspects as QoS; resiliency; operations, administration, and maintenance (OAM); and performance management. System efforts have validated microwave equipment from multiple vendors, including NEC, SIAE, NSN, Dragonwave, and Ceragon.

The typical deployment within the Cisco EPN architecture is to use the microwave gear to provide wireless links between MPLS-enabled access nodes, such as CSGs. The interconnection between the CSG and the microwave equipment is a GbE connection. As most microwave equipment used in this context supports sub-Gb transmission rates, typically 400 Mbps under normal conditions, certain accommodations are made. Namely, H-QoS policies are implemented in the egress direction on either side of the microwave link, providing the ability to limit the flow of traffic to the bandwidth supported across the link, while providing per-hop behavior (PHB) enforcement for EF and AF classes of traffic. Also, IGP metrics can be adjusted to account for the microwave links in a hybrid fiber-microwave deployment, allowing the IGP to properly understand the weights between true Gb links, and Gb ports connected to sub-Gb microwave links.

Adaptive Code Modulation (ACM) for MPLS Access

If the bandwidth provided by a microwave link was constant, then IGP weights and H-QoS shaper rates could be set once and perform correctly. However, the bandwidth supported at a given time by a microwave link depends upon environmental factors. To enable the microwave link to support the optimal amount of bandwidth for the current environmental conditions, the equipment supports Adaptive Code Modulation (ACM) functionality, which automatically changes the modulation being utilized to provide the optimal amount of bandwidth for the given environment.

Regardless of the ACM status of the microwave link, the GbE connection to the MPLS-enabled node is constant, so those nodes are unaware of any changes to the bandwidth on the microwave link. To ensure that optimal routing and traffic transport is maintained through the access network, a mechanism is needed to notify the MPLS nodes of any ACM events on the microwave links. Cisco and microwave vendors NSN and SIAE have implemented a vendor-specific message (VSM) in Y.1731 to allow for the microwave equipment to notify Cisco routers of ACM events, and the bandwidth available with the current modulation on the microwave link. Cisco EPN has implemented three actions to be taken on the MPLS nodes, which can be enacted depending upon the bandwidth available on the microwave link:

- Adjustment of the H-QoS policy to match the current bandwidth on the microwave link.
- Adjustment of the IGP metric on the microwave link, triggering an IGP recalculation.
- Removal of link from the IGP.

Figure 7-4 Test Bed Topology for Microwave ACM Integration Validation

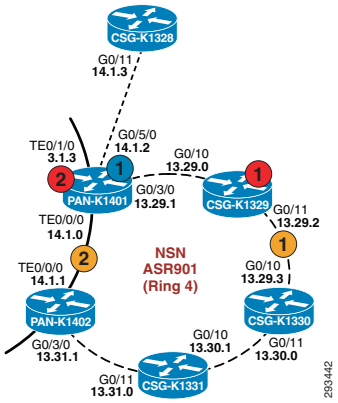
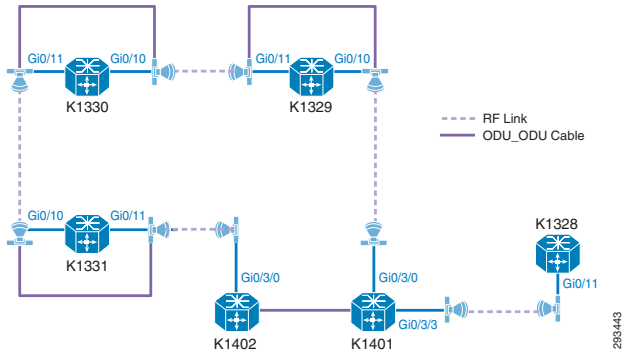


Figure 7-5 Physical Connections for Microwave ACM Integration Validation



Y.1731 Configuration for Microwave ACM Integration on CSG-K1330 (Cisco ASR 901)

The Microwave ODU will use Y.1731 Connectivity Fault Management (CFM) Vendor-Specific Message (VSM) to communicate an ACM change with CSG. This "ETHERNET_EVENT-4-MW_BW_CHANGE" VSM contains three parameters: Interface, Current Bandwidth, and Nominal Bandwidth.

The configuration for enabling Y.1731 CFM communication on the Cisco ASR 901 with the microwave ODU is shown here:

```
ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
!
ethernet cfm domain ACM level 4
  sender-id chassis
  service microwave1 evc V60 vlan 60 direction down
    continuity-check
  service microwave61 evc V61 vlan 61 direction down
    continuity-check
!
ethernet cfm domain ODU level 3
  sender-id chassis
  service microwave61 evc V61 vlan 61 direction down
    continuity-check
  service microwave62 evc V62 vlan 62 direction down
    continuity-check
```

```
interface GigabitEthernet0/10
  description To CSG-901-K1329::GigabitEthernet0/11
  !***QoS policy-map name must match script***
  service-policy input PMAP-uWave-NNI-I
  service-policy output PMAP-uWave-NNI-E-P
  service instance 60 ethernet V60
    encapsulation dot1q 60
    rewrite ingress tag pop 1 symmetric
    bridge-domain 60
    cfm mep domain ACM mpid 1330
  !
interface GigabitEthernet0/11
  description To CSG-901-K1331::GigabitEthernet0/10
  service-policy input PMAP-uWave-NNI-I
  service-policy output PMAP-uWave-NNI-E-P
  service instance 61 ethernet V61
    encapsulation dot1q 61
    rewrite ingress tag pop 1 symmetric
    bridge-domain 61
    cfm mep domain ODU mpid 1330
!
interface Vlan60
  ip router isis agg-acc
  isis network point-to-point
  isis metric 100
!
interface Vlan61
  ip router isis agg-acc
  isis network point-to-point
  isis metric 100
!
```

QoS Policy Modified by the EEM Script

```
policy-map PMAP-uWave-NNI-E-C
  class CMAP-RT-GRP
    priority percent 20
  class CMAP-NMgmt-GRP
    bandwidth percent 5
  class CMAP-CTRL-GRP
    bandwidth percent 2
  class CMAP-HVideo-GRP
    bandwidth percent 50
  class class-default
!
policy-map PMAP-uWave-NNI-E-P
  class class-default
    shape average 400000000
      service-policy PMAP-uWave-NNI-E-C
```

EEM Script for Microwave ACM Integration

The EEM script for microwave ACM integration was validated in the Cisco EPN 4.0 System effort. It implements the three actions taken based on Microwave ACM notifications from the ODU. Based on the information received regarding Interface, Current Bandwidth, and Nominal Bandwidth in the "ETHERNET_EVENT-4- MW_BW_CHANGE" VSM from the ODU, this script will determine which of the following actions to take:

- H-QoS policy adjustment-Adjusts bandwidth percentages in Child AF classes.
- IGP metric adjustment and SPF recalculation-Adjusts either "isis metric X" or "ip ospf cost X."
- Removal of link from the IGP.

```
#-------------------------------------------------------------------
```

```
# EEM script to configure metric on a microwave link
# and adjust a QoS policy
# according to the ethernet event parameters sent through OAM.
#
# Metric Algorithm:
# Degraded Link Cost = [n +1- n*CB/NB] * Original Link Cost
# where:
# CB = Current (degraded) BW
# NB = Nominal BW
# n = nodes in the ring
# OLC for ISIS = 100
# OLC for OSPF = 100
#
# QoS Algorithm (BW):
# if (EF+AF) < CB then change just EF classes
# if EF < CB < (EF+AF) then change both EF and AF classes
# if EF > CB then change the IGP metric
#
# Parameters to be configured:
#
# 1. Ring nodes number as a global variable.
# 2. VLAN interface of the ring as a global variable.
# 3. Physical interface where VSM message is received. Configured inside the eem
script.
#
# QoS:
# 0 - QoS only
# 1 - QoS and IGP
# 2 - IGP only
#
# conf t
# event manager environment _ring_nodes 4
# event manager environment _svi61 61
# event manager environment _eem_mode 1
# !
# January 2013, Cisco Systems
#------------------------------------------------------------------

event manager environment _svi61 61
event manager environment _int_num service instance 601 ethernet EVC-601
event manager environment _int interface GigabitEthernet0/10
event manager environment _ethernet_intf_name GigabitEthernet0/10
event manager environment _int_sec 0
event manager environment _eem_mode 1
event manager environment _ring_nodes 5

################################################################
# Start of the ACM62 script tested on CSG-901-K1331 (ASR901) #
################################################################
no event manager applet ACM62
event manager applet ACM62
event tag event_cd ethernet microwave clear-sd interface GigabitEthernet0/10
event tag event_sd ethernet microwave sd interface GigabitEthernet0/10 threshold
1000
trigger
correlate event event_cd or event event_sd

# Variable settings
action 100 set olc "100"
action 102 set dlc "1"
action 104 set n "$_ring_nodes"
action 106 set cb "$_ethernet_current_bw"
action 108 set nb "$_ethernet_nominal_bw"
action 110 set ifname "vlan $_svi61"
```

```
action 112 set cpmap_bw 0
action 114 set pri_bw 0
action 116 set ppmap 0
action 118 set s1 "EEM-"
action 120 set zeros "000000"
action 122 set cb_bps "$cb$zeros"
action 124 set nb_bps "$nb$zeros"
action 126 set ifcfg 1

action 130 cli command "enable"
action 132 cli command "conf t"

# Restore the original QoS policy
action 160 if $cb eq $nb
action 162 cli command "interface $_ethernet_intf_name"
action 163 cli command "no service-policy output $s1$ppmap"
action 164 cli command "service-policy output $ppmap"

# QoS block
# Find an original parent policy-map name and create a new name
action 180 elseif $_eem_mode le "1"
action 181 if $ppmap eq "0"
action 182 cli command "do show run int $_ethernet_intf_name | i service-policy
output"
# action 184 syslog msg "cli_result 184: $_cli_result, into: $_ethernet_intf_name"
action 186 regexp "service-policy output (.*)\n" "$_cli_result" line pmap
# action 188 syslog msg "line 196: $line"
# action 190 string replace "$line" 0 21 ""
action 192 string trimright "$pmap"
# action 194 syslog msg "QoS done. string 194: $_string_result, line: $line"
action 196 set pmap $_string_result
action 197 else
action 198 set pmap $ppmap
action 199 end
action 200 syslog msg "s1pmap 200: $s1$pmap"

# Find an original child policy-map name and create a new name
action 214 cli command "do show run policy-map $pmap | i service-policy"
# action 215 syslog msg "cli_result 215: $_cli_result"
action 216 regexp "service-policy (.*)\n" "$_cli_result" line cpmap
action 217 string trimright "$cpmap"
action 218 set cpmap "$_string_result"
# action 219 syslog msg "cpmap 219: $s1$cpmap"
action 220 cli command "do show run policy-map $cpmap"
action 221 regexp "class .*!" $_cli_result string

# Configuration of a new child policy-map
action 223 cli command "policy-map $s1$cpmap"
action 226 foreach var "$string" "\n"
action 228 regexp "class (.*)" $var match cname
action 230 if $_regexp_result eq 1
# action 233 syslog msg "233: cname: $cname"
action 234 end

# Calculate BW for each of the classes
action 236 regexp "(priority|bandwidth) percent (.*)" $var line cmd ef_bw_perc
action 238 if $_regexp_result eq 1
action 256 string trimright "$ef_bw_perc"
# action 258 syslog msg "258: cb_bps: $nb_bps, ef_bw_perc:$_string_result"
action 260 divide $nb_bps 100
action 262 multiply $_result $_string_result
action 263 set bw_demand $_result
action 264 add $cpmap_bw $_result
action 266 syslog msg "266: cpmap_bw: $_result, bw_demand: $bw_demand"
```

```
action 268 set cpmap_bw $_result
action 269 syslog msg "269: cpmap_bw sub-sum: $cpmap_bw"
action 270 regexp "priority percent (.*)" $line match
action 272 if $_regexp_result eq 1
action 274 add $pri_bw $bw_demand
action 276 multiply $bw_demand 100
action 278 divide $_result $cb_bps
action 279 if $_remainder gt 0
action 280 increment _result
action 281 end
action 282 set match1 "priority percent $_result"
action 283 set match2 "priority percent $_result"
action 284 end
action 286 regexp "bandwidth percent (.*)" $line match
action 288 if $_regexp_result eq 1
action 290 set match1 "$match"
action 292 set match2 "bandwidth percent 1"
action 294 end
action 296 else
action 298 set match1 "$var"
action 300 set match2 "$var"
action 302 end
action 304 append cfg_out1 "$match1 \n"
action 306 append cfg_out2 "$match2 \n"
action 308 end

# Check if there is enough BW on a uwave link
action 310 syslog msg "310: cpmap_bw sum: $cpmap_bw"
action 312 if $cpmap_bw lt $cb_bps
action 314 set cfg_out "$cfg_out1"
action 316 elseif $pri_bw lt $cb_bps
action 318 set cfg_out "$cfg_out2"
action 320 else
action 322 set metric 1000000
action 323 set ifcfg 0
action 324 end

# Configuration of a child QoS policy
action 325 if $ifcfg eq 1
action 326 foreach var "$cfg_out" "\n"
action 328 cli command "$var"
action 330 end
action 331 end

# Configuration of a parent QoS policy
action 332 cli command "policy-map $s1$pmap"
action 334 syslog msg "config 334: policy-map $s1$pmap"
action 336 cli command "class class-default"
action 338 cli command "shape average $cb_bps"
action 340 cli command "service-policy $s1$cpmap"

# Apply the QoS policy on a PHY interface
action 344 cli command "int $_ethernet_intf_name"
action 346 cli command "no service-policy output $pmap"
action 348 cli command "service-policy output $s1$pmap"

# End of the QoS part
action 390 end

# IGP metric block
action 400 if $_eem_mode ge 1
action 402 multiply $n $cb
action 404 divide $_result $nb
action 406 syslog msg "406: cb: $cb nb: $nb result: $_result"
```

```
action 408 set m $_result
action 410 syslog msg "m: $m"
action 412 increment n
action 414 subtract $n $m
action 416 multiply $_result $olc
action 418 if $ifcfg eq 0
action 420 set dlc $metric
action 422 else
action 424 set dlc $_result
action 426 end
action 428 syslog msg "428: n:$n m:$m olc:$olc dlc:$dlc result:$_result intf:
  $ifname"
# action 430 cli command "enable"
# action 432 cli command "conf t"
action 434 cli command "int $ifname"
action 436 cli command "do show run int $ifname"
action 438 string first "ip router isis" "$_cli_result"
action 440 if $_string_result ne "-1"
action 442 cli command "isis metric $dlc"
action 444 cli command "do show ip ospf int | i $ifname"
action 446 string first "$ifname" "$_cli_result"
action 448 elseif $_string_result ne "-1"
action 450 cli command "ip ospf cost $dlc"
action 452 end
action 454 end

# Adjust the current applet
action 456 syslog msg "The EEM script executed"
action 458 cli command "event manager applet ACM62"
action 460 cli command "event tag event_sd ethernet microwave sd interface
GigabitEthernet0/10 threshold $nb"
action 462 if $ppmap eq 0
action 464 if $_eem_mode le 1
action 466 cli command "action 116 set ppmap $pmap"
action 468 end
action 470 end

################################################
# The end of the script
################################################
```

Adaptive Code Modulation for Ethernet Access

In case of Ethernet access, the traffic is loadbalanced on the ring according to the instances configured under the G.8032 configuration. The routers participating in the ring are unaware of the bandwidth changes due to signal fading. Using microwave ACM, the routers become aware of the bandwidth change, and are able to take appropriate action among the below

- Adjustment of the H-QoS policy to match the current bandwidth on the microwave link
- Manual switch of the ring which results in not using the particular interface which is degraded

Y.1731 Configuration for Microwave ACM Integration on CSG-K0306 (Cisco ASR 901)

The Microwave ODU will use Y.1731 Connectivity Fault Management (CFM) Vendor-Specific Message (VSM) to communicate an ACM change with CSG. This "ETHERNET_EVENT-4-MW_BW_CHANGE" VSM contains three parameters: Interface, Current Bandwidth, and Nominal Bandwidth.

The configuration for enabling Y.1731 CFM communication on the Cisco ASR 901 with the microwave ODU is shown here:

```
CSG-ASR901-K0306

ethernet cfm ieee
ethernet cfm global
ethernet cfm traceroute cache
ethernet cfm traceroute cache size 200
ethernet cfm traceroute cache hold-time 200
ethernet cfm domain 8032 level 1
 service 99 evc EVC-99 vlan 99 direction down
  continuity-check
 service 199 evc EVC-199 vlan 199 direction down
  continuity-check
!
!
ethernet ring g8032 profile ring_profile
 timer wtr 10
 timer guard 100
!
ethernet ring g8032 CERING
 open-ring
 port0 interface TenGigabitEthernet0/0
 port1 interface TenGigabitEthernet0/1
 instance 1
  inclusion-list vlan-ids 99,300-350
  aps-channel
   port0 service instance 99
   port1 service instance 99
  !
 !
 instance 2
  inclusion-list vlan-ids 199,351-400
  aps-channel
   port0 service instance 199
   port1 service instance 199
  !
 !
 interface TenGigabitEthernet0/1
 description to Ten 0/1 on K0305
 no ip address
 load-interval 30
 l2proto-forward tagged
 synchronous mode
 cdp enable
 service-policy input PMAP-NNI-I
 service-policy output PMAP-NNI-E-P
!
service instance 99 ethernet EVC-99
  encapsulation dot1q 99
  rewrite ingress tag pop 1 symmetric
  bridge-domain 99
  cfm mep domain 8032 mpid 3061

interface TenGigabitEthernet0/0
 description to Ten 0/0 on K0307
 no ip address
 load-interval 30
 l2proto-forward tagged
 synchronous mode
 cdp enable
 service-policy input PMAP-NNI-I
service-policy output PMAP-NNI-E-P
!
service instance 99 ethernet EVC-99
```

```
  encapsulation dot1q 99
  rewrite ingress tag pop 1 symmetric
  bridge-domain 99
  cfm mep domain 8032 mpid 306
!
###policy-maps used
policy-map PMAP-NNI-E-P
 class class-default
  shape average 400000000
   service-policy PMAP-NNI-E
!
end
 policy-map PMAP-NNI-E
 class CMAP-RT-GRP
  priority percent 20
 class CMAP-BC-GRP
  bandwidth percent 5
 class CMAP-BC-Tele-GRP
  bandwidth percent 10
 class CMAP-NMgmt-GRP
  bandwidth percent 5
 class CMAP-CTRL-GRP
  bandwidth percent 2
 class CMAP-Video-GRP
  bandwidth percent 20
 class class-default
!
```

EEM Script for Microwave ACM Integration

The EEM script for microwave ACM integration was validated in the Cisco EPN 4.0 System effort. It implements the three actions taken based on Microwave ACM notifications from the ODU. Based on the information received regarding Interface, Current Bandwidth, and Nominal Bandwidth in the "ETHERNET_EVENT-4- MW_BW_CHANGE" VSM from the ODU, this script will determine which of the following actions to take:

- H-QoS policy adjustment-Adjusts bandwidth percentages in Child AF classes.
- Manual switchover of the ring if the current bandwidth cannot accommodate the bandwidth demand

```
# Variable settings
event manager environment _ring_nodes 5
event manager environment _int interface tengigabitethernet0/1
event manager environment _ethernet_intf_name tengigabitethernet0/1
event manager environment _int_sec 0
event manager environment _eem_mode 1 >>>>> Mode value can be 1 (for QOS and
switchover) OR 2 (for Switchover only)
event manager applet ACM62
 event tag event_cd ethernet microwave clear-sd interface TenGigabitEthernet0/1
 event tag event_sd ethernet microwave sd interface TenGigabitEthernet0/1 threshold
400
 trigger
  correlate event event_cd or event event_sd
 action 100   set olc "100"
 action 102   set dlc "1"
 action 104   set n "$_ring_nodes"
 action 106   set cb "$_ethernet_current_bw"
 action 108   set nb "$_ethernet_nominal_bw"
 action 110   set ifname "tengigabitethernet0/1"
 action 112   set cpmap_bw "0"
 action 114   set pri_bw "0"
 action 116   set ppmap "PMAP-NNI-E-P"
 action 118   set s1 "EEM-"
 action 120   set zeros "000000"
```

```
 action 122   set cb_bps "$cb$zeros"
 action 124   set nb_bps "$nb$zeros"
 action 126   set ifcfg "1"
 action 127   set th_bps "200000000"   >>>> This is the threshold bandwidth for Mode 2
and can be defined by the operator as preferred.
 action 130   cli command "enable"
 action 132   cli command "conf t"

# Restore the original QoS policy and G8032 Ring
 action 160   if $cb eq "$nb"
 action 162    cli command "interface $_ethernet_intf_name"
 action 163    cli command "no service-policy output $s1$ppmap"
 action 164    cli command "service-policy output $ppmap"
 action 165    switch ring g8032 clear CERING instance all

# QoS block
# Find an original parent policy-map name and create a new name
 action 180   elseif $_eem_mode le 1
 action 181    if $ppmap eq "0"
 action 182     cli command "do show run int $_ethernet_intf_name | i service-policy
output"
 action 184     syslog msg "cli_result 184: $_cli_result, into: $_ethernet_intf_name"
 action 186     regexp "service-policy output (.*)\n" "$_cli_result" line pmap
 action 188     syslog msg "line 196: $line"
 action 190     string replace "$line" 0 21
 action 192     string trimright "$pmap"
 action 194     syslog msg "QoS done. string 194: $_string_result, line: $line"
 action 196     set pmap "$_string_result"
 action 197    else
 action 198     set pmap "$ppmap"
 action 199    end
 action 200    syslog msg "s1pmap 200: $s1$pmap"

# Find an original child policy-map name and create a new name
 action 214    cli command "do show run policy-map $pmap | i service-policy"
 action 215    syslog msg "cli_result 215: $_cli_result"
 action 216    regexp "service-policy (.*)\n" "$_cli_result" line cpmap
 action 217    string trimright "$cpmap"
 action 218    set cpmap "$_string_result"
 action 219    syslog msg "cpmap 219: $s1$cpmap"
 action 220    cli command "do show run policy-map $cpmap"
 action 221    regexp "class .*!" "$_cli_result" string

# Configuration of a new child policy-map
 action 223    cli command "policy-map $s1$cpmap"
 action 226    foreach var "$string" "\n"
 action 228     regexp "class (.*)" "$var" match cname
 action 230     if $_regexp_result eq "1"
 action 233      syslog msg "233: cname: $cname"
 action 234     end

# Calculate BW for each of the classes
 action 236     regexp "(priority|bandwidth) percent (.*)" "$var" line cmd ef_bw_perc
 action 238     if $_regexp_result eq "1"
 action 256      string trimright "$ef_bw_perc"
 action 258      syslog msg "258: cb_bps: $nb_bps, ef_bw_perc:$_string_result"
 action 260      divide $nb_bps 100
 action 262      multiply $_result $_string_result
 action 263      set bw_demand "$_result"
 action 264      add $cpmap_bw $_result
 action 266      syslog msg "266: cpmap_bw: $_result, bw_demand: $bw_demand"
 action 268      set cpmap_bw "$_result"
 action 269      syslog msg "269: cpmap_bw sub-sum: $cpmap_bw"
 action 270      regexp "priority percent (.*)" "$line" match
```

```
 action 272      if $_regexp_result eq "1"
 action 274     set pri_bw "$bw_demand"
 action 276       divide $cb_bps 100
 action 278       divide $bw_demand $_result
 action 282       set match1 "priority percent $_result"
 action 283       set match2 "priority percent $_result"
 action 284      end
 action 286      regexp "bandwidth percent (.*)" "$line" match
 action 288      if $_regexp_result eq "1"
 action 290       set match1 "$match"
 action 292       set match2 "bandwidth percent 1"
 action 294      end
 action 296     else
 action 298      set match1 "$var"
 action 300      set match2 "$var"
 action 302     end
 action 304     append cfg_out1 "$match1 \n"
 action 306     append cfg_out2 "$match2 \n"
 action 308    end

# Check if there is enough BW on a uwave link
 action 310    syslog msg "310: cpmap_bw sum: $cpmap_bw"
 action 312    if $cpmap_bw lt "$cb_bps"
 action 314     set cfg_out "$cfg_out1"
 action 316    elseif $pri_bw lt $cb_bps
 action 318     set cfg_out "$cfg_out2"
 action 320    else
 action 322     switch ring g8032 CERING instance 1
 action 323     set ifcfg "0"
 action 324    end

# Configuration of a child QoS policy
 action 325    if $ifcfg eq "1"
 action 326     foreach var "$cfg_out" "\n"
 action 328      cli command "$var"
 action 330     end
 action 331    end

# Configuration of a parent QoS policy
 action 332    cli command "policy-map $s1$pmap"
 action 334    syslog msg "config 334: policy-map $s1$pmap"
 action 336    cli command "class class-default"
 action 338    cli command "shape average $cb_bps"
 action 340    cli command "service-policy $s1$cpmap"

# Apply the QoS policy on a PHY interface
 action 344    cli command "int $_ethernet_intf_name"
 action 346    cli command "no service-policy output $pmap"
 action 348    cli command "service-policy output $s1$pmap"

# End of Mode 1 for QOS Change and G8032 Switchover
 action 390   end

#  Mode 2 Block for G8032 switchover only if Current Bandwidth is below Configured
Threshold
 action 400   if $_eem_mode gt "1"
 action 402    if $cb_bps le "$th_bps"
 action 404     switch ring g8032 CERING instance 1
 action 406    end
 action 408   end
```

Operations, Administration, and Maintenance

Operations, administration, and maintenance (OAM) implementation for transport in the Cisco EPN System varies depending on the type of service being monitored. This is covered in the EPN 4.0 MEF Transport Services Design and Implementation Guide, EPN 4.0 Mobile Transport Services Design and Implementation Guide, and the EPN 4.0 Enterprise Transport Services Design and Implementation Guide for the EPN System architecture.

Multicast Services in Global Routing Implementation

This section describes the implementation of multicast in global routing in order to support services such as eMBMS v4/v6 and IPTV v4 for mobile and residential users over a common transport infrastructure. The system architecture is mainly composed of two parts:

1. Label-Switched Multicast (LSM) with Multicast Label Distribution Protocol (MLDP) Global in-band signaling profile used in the MPLS aggregation and core networks.
2. Native Ipv4/IPv6 Multicast in the access and pre-aggregation networks.

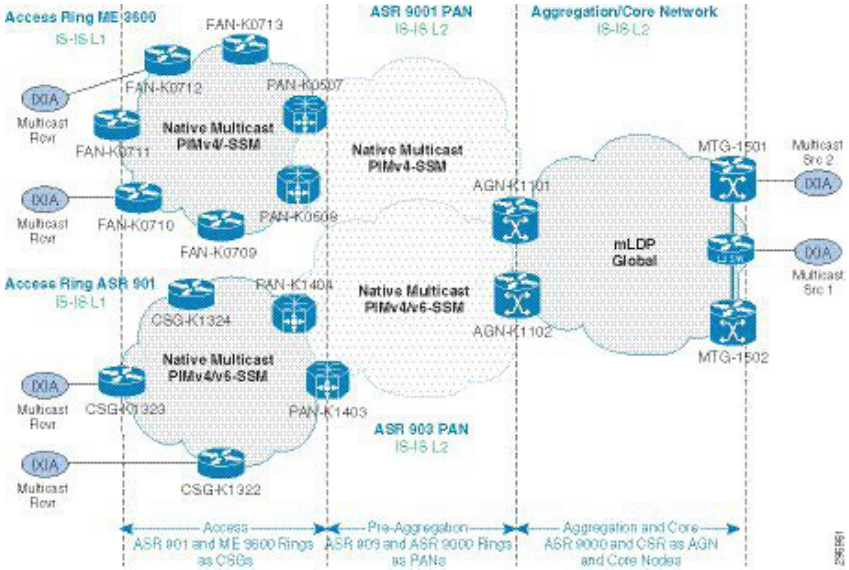
As shown in Figure 7-6 on page 7-26, this implementation covers two types of access domains depending on the platforms involved:

- ASR 901 ring to ASR 903 PAN nodes -wherein Cisco ASR 901 Series routers are used as the CSGs in the access ring, while Cisco ASR 903 Series routers are used as the PAN in the pre-aggregation ring. In this model, native multicast is implemented for both IPv6 & IPv4.
- ME 3600 ring to ASR 9000 PAN nodes -wherein Cisco ME 3600X Series switches are used as the fixed access nodes (FANs) or CSGs in the access ring, while a Cisco ASR 9001 router is used as the PAN in the pre-aggregation ring. in this access model, native multicast is implemented only for IPv4.

In both access domains, multicast traffic is delivered natively over the IPv4/v6 multicast-enabled infrastructure. The implementation of multicast delivery in these domains is discussed later in this section.

The SE node acts as the boundary between the native IP Multicast domains in the access and pre-aggregation networks, and the MPLS multicast domain in the core and aggregation networks. The MPLS Multicast domain is based on LSM, which is a solution that enables forwarding of IP multicast traffic over MPLS, thus allowing the MPLS infrastructure to provide a common data plane (based on label switching) for both unicast and multicast traffic.

Figure 7-6 Multicast Transport Implementation for eMBMS Services



As shown in Figure 7-6, the eMBMS service is implemented attaching a multicast sources to each of the Mobile Transport Gateways, MTG-1501 and MTG-1502, respectively. Multicast receivers are located to both access rings,

AGN K1101 and AGN K1102 mark the end of aggregation/core to where the mLDP domain extends. Both PAN rings, ASR 9001 PAN and ASR 903 PAN, and the access rings, ME 3600 and ASR 901, run native IP multicast; multicast forwarding in the access domain is based on PIM SSM v4/v6.

Native IPv4 multicast forwarding is implemented in both the ME 3600 and in the ASR901 access rings, while native IPv6 multicast is implemented in the ASR901 access ring only.

Within the LSM domain, which terminates at the SE nodes, AGN-K1101 and AGN-K1102, MLDP relies on RFC 3107-learnt IPv6 multicast source addresses to build the multicast tree in core. The AGNs then redistribute the IPv4/v6 multicast source addresses learnt via RFC 3107 into the level 2 ISISv4/6 process running in the native multicast domain.

At the PAN nodes, the multicast source prefixes now available in ISISv4/6 Level 2 are leaked into ISISv4/6 Level1 such that the nodes in the access ring are aware of the multicast source prefixes and PIM can build end-to-end multicast distribution trees.

Note Please refer to the "Multicast Service Model for LTE eMBMS" section in the EPN 4.0 Mobile Transport Design and Implementation Guide for implementation of eMBMS v4 & v6 service.

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

```
!***Advertise the network prefix where the Multicast source of the Internet Protocol
Television (IPTV) & eMBMS service is located***
router bgp 1000
 bgp router-id 100.111.15.1
!***Advertising the IPv4 multicast source prefixes***
 address-family ipv4 unicast
  network 200.15.12.0/24 route-policy MSE_IGW_Community
  network 200.15.1.0/24 route-policy MSE_IGW_Community
!***Advertising the IPv6 multicast source prefixes***
  address-family ipv6 unicast
```

```
  network 2001:100:111:15::1/128
  network 2001:100:192:10::/64
  allocate-label all
!***Enable MLDP***
mpls ldp
 mldp
  logging notifications
!
 interface TenGigE0/0/0/0
 interface TenGigE0/0/0/1
 interface TenGigE0/0/0/2
 !***Disable mLDP on interfaces that don't need mLDP***
  mldp disable
!***Configure route-policy to set the type of MLDP core tree***
route-policy MLDP-Inband
  !***Set mLDP-Inband signaling***
  set core-tree mldp-inband
end-policy
!***Assign the configured MLDP route-policy under router PIM***
router pim
 address-family ipv4
  rpf topology route-policy MLDP-Inband
 !
 address-family ipv6
  rpf topology route-policy MLDP-Inband
 !
!
!***Configure Multicast-routing to enable Multicast interfaces, MDT source, and MLDP
in-band signaling ***
multicast-routing
 address-family ipv4
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  rate-per-route
  !***Enable multicast on all interfaces***
  interface all enable
  accounting per-prefix
 !
 address-family ipv6
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  rate-per-route
  !***Enable multicast on all interfaces***
  interface all enable
  accounting per-prefix
 !
!
```

CN-CRS8-K0401 (BRANCH node)

```
!*** In the BRANCH-node/P-routers, the only configuration needed is MLDP***
!***Enable MLDP***
mpls ldp
!***Enables mLDP***
 mldp
  logging notifications
  !***Needed for faster LSM convergence***
  make-before-break delay 0 0
 !
 interface TenGigE0/0/0/0
 interface TenGigE0/0/0/1
 interface TenGigE0/0/0/2
```

```
 interface TenGigE0/0/0/3
 interface GigabitEthernet0/2/0/0
 !***Disable mLDP on CN-RR interface***
  mldp disable
```

AGN-9006-K1102(LEAF-node/Egress-PE)

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

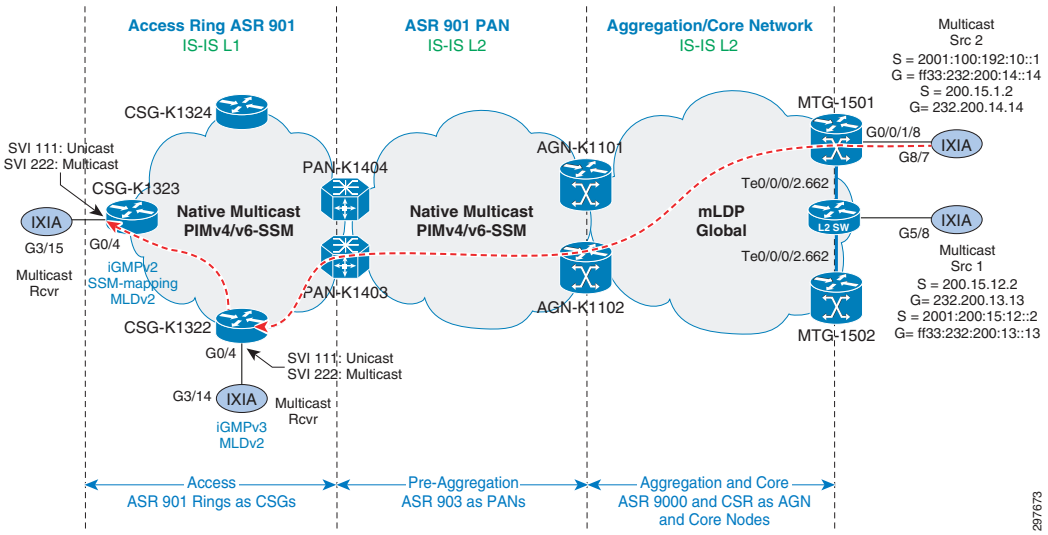
```
 mpls ldp
 !***Enables mLDP***
 mldp
  logging notifications
 !
 interface TenGigE0/0/0/0
 interface TenGigE0/0/0/2
 interface TenGigE0/0/0/1
   mldp disable
 interface TenGigE0/0/0/3
 !***mLDP uses the LDP interfaces by default.***
 !***Disable mLDP on interfaces facing the Access and Pre-Agg***
   mldp disable
!***Configure route-policy to set the type of MLDP core tree***!
route-policy MLDP-Inband
!***Set mLDP-Inband signaling***
  set core-tree mldp-inband
!***Assign the configured MLDP route-policy under router PIM***
router pim
 address-family ipv4
  rpf topology route-policy MLDP-Inband
 !
 address-family ipv6
  rpf topology route-policy MLDP-Inband
 !
!***Configure Multicast-routing to enable Multicast interfaces, MDT source, and MLDP
in-band signaling***
multicast-routing
 address-family ipv4
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  rate-per-route
  accounting per-prefix
  !***Enable multicast on all IPv4 interfaces***
  interface all enable
  accounting per-prefix
 !
 address-family ipv6
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  rate-per-route
  accounting per-prefix
  !***Enable multicast on all IPv6 interfaces***
  interface all enable
  accounting per-prefix
 !
!***Enable IPv6 for ISIS at the SE node on the interface connecting to ASR 903 PAN
ring and the  ASR 903 PAN ring also***
router isis core
```

```
!***Enables ISIS for IPv6 ***
    address-family ipv6 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
    !
    interface Loopback0
    passive
    point-to-point
    address-family ipv4 unicast
    !
     address-family ipv6 unicast
    !
    interface TenGigE0/0/0/1
    address-family ipv4 unicast
    metric 10
    mpls ldp sync
    !
!***Enables IPv6 for ISIS on the interface going towards 903 PAN ring & 901 Access
ring***
     address-family ipv6 unicast
        metric 10
!***Redistribute BGP IPv6 multicast source prefixes into ISISv6 Level 2***
 router isis core
    address-family ipv6 unicast
    metric-style wide
    ispf
    spf-interval maximum-wait 5000 initial-wait 50 secondary-wait 200
    !***redistributing BGP IPv6 multicast source address into ISIS level 2***
   redistribute bgp 1000 level-2
```

Native IP Multicast Implementation in ASR 901-to-ASR 903 Access Domain

As depicted in Figure 7-7, the Cisco ASR 903 Series Router (PAN-ASR903) forms the PAN ring which connect to ASR 901 access ring. Native multicast for both IPv4 & IPv6 is supported in this ASR 903 PAN ring. IPv6 multicast source prefixes present in as level 2 ISISv6 routes are injected into level 1 in this ring.

Figure 7-7 Multicast Transport Implementation for eMBMS services in ASR901 to ASR 903 Access Domain



Note The configuration shown below is applicable to all Cisco ASR 903 Series PANs in the pre-aggregation ring.

PAN-903-K1403

```
   router isis core
!***Enables ISIS for IPv6 in the 903 PAN ring ***
    address-family ipv6
      multi-topology
!
interface TenGigabitEthernet0/0/0
 description To PAN-K1404 Ten0/0/0
 !***Enables ISIS for IPv6  on the 903 PAN ring interfaces***
 ipv6 address 2001:10:14:3::/127
 ipv6 enable
 ipv6 router isis core


interface TenGigabitEthernet0/1/0
 description To AGN-K1102 Ten0/0/0/1
 !***Enables ISIS for IPv6  on the 903 PAN ring interfaces***
 ipv6 address 2001:10:11:2::1/127
 ipv6 enable
 ipv6 router isis core
!
interface BDI10
 description To CSG-K1322 G0/11
 !***Enables ISIS for IPv6  on the interface connecting 901 Access ring ***
 ipv6 address 2001:10:13:22::1/127
 ipv6 enable
 ipv6 router isis core
!***Redistribute ISIS IPv6 level 2 routes into Level 1***
router isis core
    address-family ipv6
       multi-tpology
!***Redistributes isisv6 level 2 into level-1 in the 903 PAN ring ***
     redistribute isis level-2 into level-1
```

```
     exit-address-family
!***Enable Multicast routing for IPv4 & IPv6 and PIM-SSM with ssm default range
232.0.0.0/8 for IPv4***
ip multicast-routing distributed
ipv6 multicast-routing
ip pim ssm default
```

Note Enabling PIMv6 requires, global "ipv6 multicast-routing" and enable IPv6 on the interfaces

```
!***Enable PIMv4/v6 in the relevant L3 interfaces that should be involved in the
Multicast distribution tree path***
interface TenGigabitEthernet0/0/0
  description To PAN-K1404 Ten0/0/0
  ip address 10.14.3.0 255.255.255.254
  ipv6 address 2001:10:14:3::/127
  ipv6 enable
  ip pim sparse-mode
!
interface TenGigabitEthernet0/1/0
  description To AGN-K1102 Ten0/0/0/1
  ip address 10.11.2.1 255.255.255.254
  ipv6 address 2001:10:11:2::1/127
  ipv6 enable
  ip pim sparse-mode
!***Connects CSG ASR 901 ring***
interface BDI10
  description To CSG-K1322 G0/11
  ip address 10.13.22.1 255.255.255.254
  ipv6 address 2001:10:13:22::1/127
  ipv6 enable
  ip pim sparse-mode
```

CSG-901-K1322

```
!***Enable IPv6 for ISIS in the 901 access ring***
   router isis core
!***Enables ISIS for IPv6 in the 901 Access ring ***
    address-family ipv6
       multi-topology
     exit-address-family
!
interface GigabitEthernet0/11
 description To PAN-K1403 G0/3/1
 service instance 10 ethernet
 encapsulation dot1q 10
 rewrite ingress tag pop 1 symmetric
 bridge-domain 10
!
interface Vlan10
!***Enables ISIS for IPv6  on the 901 Access ring interfaces***
 ipv6 address 2001:10:13:22::/127
 ipv6 enable
 ipv6 router isis core
!
interface GigabitEthernet0/10
 description To CSG-K1323 G0/10
 service instance 10 ethernet
 encapsulation dot1q 10
 rewrite ingress tag pop 1 symmetric
    bridge-domain 20
    !
```

```
interface Vlan20
!***Enables ISIS for IPv6  on the 901 Access ring interfaces***
 ipv6 address 2001:10:13:22::2/127
 ipv6 enable
 ipv6 router isis core
!***Enable Multicast routing for IPv4 & IPv6 and platform support for Multicast***
ip multicast-routing
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
asr901-platf-multicast enable
!***Enable PIM-SSM and use the default SSM range 232.0.0.0/8 for IPv4. If you are
using a non-232.0.0.0/8 Multicast group address, use the ssm range command***
ip pim ssm default
!***Enable PIMv4/v6 in the L3 interfaces connecting other nodes in the ring and the L3
interface facing the eNodeB***
interface Vlan10
  ip address 10.13.22.0 255.255.255.254
  ipv6 address 2001:10:13:22::/127
  ipv6 enable
  ip pim sparse-mode
!
interface Vlan20
  ip address 10.13.22.2 255.255.255.254
  ipv6 address 2001:10:13:22::2/127
  ipv6 enable
    ip pim sparse-mode
!
```

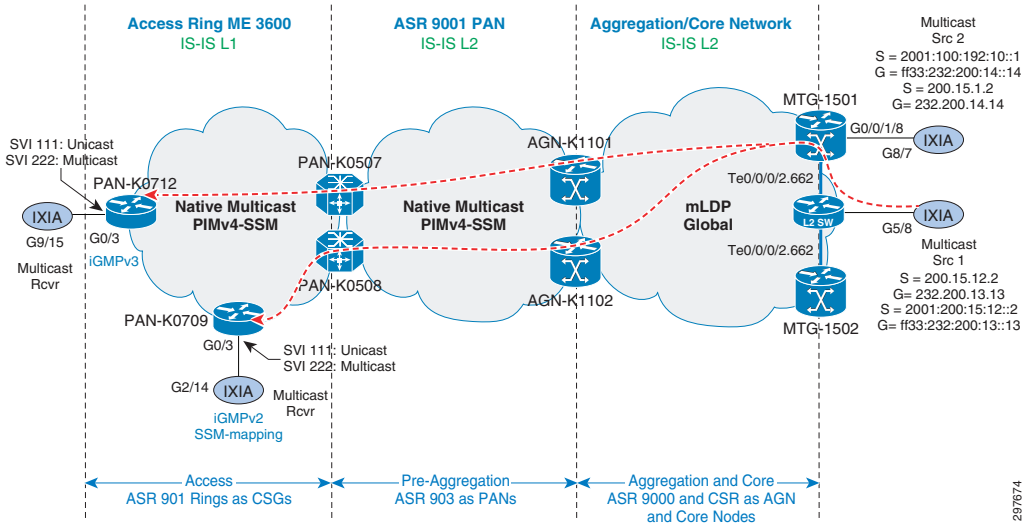
CSG-901-K1323

Note IGMPv2 configuration requires static SSM mapping at the CSG access node.

```
!***Enable Multicast routing and platform support for Multicast***
ip multicast-routing
asr901-platf-multicast enable
!***Enable PIM-SSM and use the default SSM range 232.0.0.0/8 for IPv4. If you are
using a non-232.0.0.0/8 Multicast group address, use the ssm range command***
ip pim ssm default
!***Enable SSM mapping and define a static SSM map to support IGMPv2 in the PIM-SSM
network***
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static SSM-map2 200.15.1.2
ip igmp ssm-map static SSM-map1 200.15.12.2
!
ip access-list standard SSM-map1
  permit 232.200.13.0 0.0.0.255
ip access-list standard SSM-map2
  permit 232.200.14.0 0.0.0.255
!***Enable PIM in the L3 interfaces connecting other nodes in the ring and the L3
interface facing the simulated eNodeB***
interface Vlan10
  ip address 10.13.23.0 255.255.255.254
  ip pim sparse-mode
!
interface Vlan20
  ip address 10.13.22.3 255.255.255.254
  ip pim sparse-mode
!
```

Native IP Multicast Implementation in ME 3600 to ASR 9000 Access Domain

Figure 7-8 Multicast Transport Implementation for eMBMS Services in ME 3600 to ASR 9000 Access Domain



PAN-9001-K0508

The following configuration is applicable to all Cisco ASR 9000 Series PANs in the pre-aggregation ring.

```
!***Enable Multicast routing on the relevant interfaces.
multicast-routing
 address-family ipv4
  interface TenGigE0/0/0/0
   enable
  interface TenGigE0/0/0/1
   enable
  interface TenGigE0/0/0/2
   enable
```

FAN-ME36-K0712

```
!***Enable Multicast routing and platform support for Multicast***
ip multicast-routing
ip pim ssm default
!***Enable PIM in the L3 interfaces connecting other nodes in the ring and the L3
interface facing the eNodeB***
interface TenGigabitEthernet0/1
  no switchport
  ip address 10.7.11.1 255.255.255.254
  ip pim sparse-mode
!
interface TenGigabitEthernet0/2
  no switchport
  ip address 10.7.12.0 255.255.255.254
  ip pim sparse-mode
!
```

FAN-ME36-K0712

Note IGMPv2 configuration requires static SSM mapping at the CSG access node.

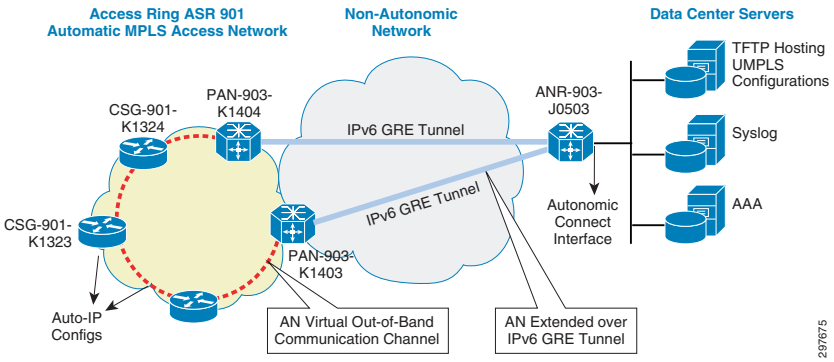
```
!***Enable Multicast routing and platform support for Multicast***
ip multicast-routing
!***Enable PIM-SSM and use the default SSM range 232.0.0.0/8 for IPv4. If you are
using a non-232.0.0.0/8 Multicast group address, use the ssm range command***
ip pim ssm default
!***Enable SSM mapping and define a static SSM map. This supports IGMPv2 in the
PIM-SSM network***
ip igmp ssm-map enable
no ip igmp ssm-map query dns
ip igmp ssm-map static SSM-map2 200.15.1.2
ip igmp ssm-map static SSM-map1 200.15.12.2
!
ip access-list standard SSM-map1
  permit 232.200.13.0 0.0.0.255
ip access-list standard SSM-map2
  permit 232.200.14.0 0.0.0.255
!***Enable PIM in the L3 interfaces connecting other nodes in the ring and the L3
interface facing the simulated eNodeB***
interface TenGigabitEthernet0/1
  no switchport
  ip address 10.7.11.1 255.255.255.254
  ip pim sparse-mode
!
interface TenGigabitEthernet0/2
  no switchport
  ip address 10.7.12.0 255.255.255.254
  ip pim sparse-mode
!
```

Autonomic Networking

This section describes the implementation of Autonomic Networking in the EPN 4.0 Transport Infrastructure System.

Figure 7-9 illustrates the implementation of Autonomic Networking in a access domain made of a ring of CSG nodes implemented using ASR 901 and terminating on a pair of PAN nodes, implemented using ASR 903 with RSP1.

Figure 7-9 Autonomic Networking Implementation



The Registrar node responsible for the secure registration of access devices is implemented using a Cisco ASR903 node with RSP1, ANR-903-K0104 and it is located near the data center hosting AN management servers, which currently host AAA, Syslog, and TFTP servers.

The Registrar connects to the Autonomic Network domain over a pair of IPv6 GRE tunnels that terminate on the PAN nodes acting as AN proxies and that allow for remote discovery of autonomic adjacencies. As a result, the VOBC network space virtually extends from the Autonomic Networking enabled access network to the remote Registrar.

The detailed bootstrap sequence for an Autonomic Network is described here:

- Registrar first discovers the PAN nodes, acting as AN proxies, over the pair of manual IPv6 GRE tunnels
- The VOBC is set up between the Registrar and the AN proxies over the IPv6 GRE tunnels
- New AN nodes that connects to the AN proxies or to other nodes that have already joined the AN domain are then bootstrapped and accepted into the autonomic networking domain by the Registrar
- The VOBC is then extended to these devices by mean of proxying through the AN-enabled devices.

The Registrar discovers the different services available to the AN domain, like AAA, TFTP, and Syslog, through a service discovery functionality that is based on multicast DNS.

When a service is provisioned on the external server, it is advertised over the VOBC channel to all existing AN nodes, which will store its availability in their local cache. New nodes joining the AN or refreshing their cache learn about service availability from their neighbors.

Once the new AN node is registered in the Autonomic Networking domain and the VOBC control plane is established, it initiates a TFTP configuration download for full and final node provisioning from the TFTP server present in the server farm connected to the Registrar and auto-discovered by the Registrar. The requested configuration file name follows the udi.conf format, where “udi” is the AN node's unique device identifier.

- The name of the configuration file used for this implementation for the device CSG-901-K1323 is PID_A901-12C-FT-D_SN_CAT1546U03B.conf.
- The udi for this node configured by the autonomic process is PID:A901-12C-FT-D SN:CAT1546U03B,

This is automatically derived from the device's processor board serial number and Product ID (PID) of the device. In this case, PID for CSG-901-K1323 is A901-12C-FT-D and processor board serial number is CAT1546U03B.

Note The Syslog message seen when the config download is successfully completed on a newly provisioned node is as follows:

- Jun 30 06:41:47.216: %SYS-5-CONFIG_I: Configured from tftp://2001:10:114:9::10/autonomic-networking/PID_A901-12C-FT-D_SN_CAT1546U03B.conf by console
- Jun 30 06:41:47.220: %AN-6-CONFIG_DOWNLOAD_SUCCESS: Auto Config Download for the device with UDI- PID:A901-12C-FT-D SN:CAT1546U03B, is Success
- Jun 30 06:41:47.668: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 2001:10:114:9::10 port 514 (cisco_autonomic) started - CLI initiated

The autonomic networking feature is enabled by default on all AN-capable nodes inserted in the domain with factory configuration.

Note Any change made to the node factory configuration will automatically disable all AN functions.

AN proxies and registrar require manual boot-up and autonomic networking configuration to accommodate the need for defining the IPv6 GRE tunnels between them and enable autonomic adjacency discovery over them. Also, the Registrar requires special configuration to enable service discovery on its server farm-facing interface.

Note Autonomic functions should not be used on any device without a functioning Registrar node within the network. A device configured with "autonomic" will actively seek to join a domain. If the new device cannot join a legitimate domain, either because a valid Registrar is not configured, or if there is no L3 connectivity to a valid Registrar, any other Layer 3-adjacent device can make the device join its domain, which may lead to full control of the device by an unauthorized third party.

The following configurations apply to Registrar: ANR-903-K0104 and PANs, PAN-K1403 and PAN-K1404, in the system test topology for a Small Network.

Autonomic Registrar Router Configuration: ANR-903-K0104

This section shows all the configuration aspects involved in configuring an Autonomic Registrar router.

ANR-903-K0104

Autonomic Networking Domain Configuration

```
autonomic registrar
     domain-id epn-an
    !***Certificate authority is configured as local to Regsitrar ***
    CA local
    !***need to un shut, by default it is shut ***
      no shut
    !***Whitelist file listing the UDIs for nodes allowed in the AN domain***
      whitelist flash:whitelist.txt
    !
    !
```

Autonomic Networking Domain "facing" Interface Configuration

```
!***IPv6 GRE tunnel configs on ANR-J0503 ***
interface Tunnel11403
 no ip address
 ipv6 address 2001:111:111:333::2/112
 ipv6 enable
 !***Enable autonomic adjacency discovery over IPv6 GRE tunnel***
 autonomic adjacency-discovery
 tunnel source BDI20
 tunnel mode ipv6ip
 tunnel destination 10.11.2.1
!
interface GigabitEthernet0/2/3
 no ip address
 negotiation auto
 !***autonomic must be disabled on interfaces carrying the IPv6 GRE tunnel***
 no autonomic
 service instance 20 ethernet
 encapsulation untagged
 bridge-domain 20
!
interface BDI20
 ip address 10.5.13.0 255.255.255.254
 ip router isis core
 load-interval 30
 mpls ip
 mpls ldp igp sync delay 5
 !*** autonomic must be disabled on interfaces carrying the IPv6 GRE tunnel ***
 no autonomic
 isis circuit-type level-2-only
 isis network point-to-point
 isis metric 100
 isis csnp-interval 10
!
Server farm "facing" interface Configuration
!***interface configuration on Registrar connecting to the data center servers ***
!
interface GigabitEthernet0/2/7
 no ip address
 negotiation auto
 service instance 70 ethernet
  encapsulation untagged
  bridge-domain 70
 !
interface BDI70
 no ip address
 ipv6 address 2001:10:114:9::1/64
 ipv6 enable
 !*** Connects external servers to AN domain***
 autonomic connect
```

Whitelist File for Device Acceptance in AN Domain

A sample whitelist file, listing the Unique Device Identifiers (UDIs) for nodes allowing to join the Autonomic Networking domain, is shown here.

```
!*** more flash: whitelist.txt ***
!*** List each device Unique Device Identifier (UDI) entry on a separate line in
whitelist file ***
PID:ASR-903 SN:FOX1718P28T
PID:ASR-903 SN:FOX1610P15T
PID:ASR-903 SN:FOX1610P00Y
```

```
PID:A901-12C-FT-D SN:CAT1546U03B
PID:A901-12C-FT-D SN:CAT1546U05J
PID:A901-12C-FT-D SN:CAT1546U00Z
```

Acceptance of a Quarantined Device

The following command on the Registrar allows a quarantined device that was not listed in the whitelist file to join the autonomic networking domain.

```
ANR-903-K0104(config-registrar)# device-accept  <UDI>
EX: device-accept " PID:A901-12C-FT-D SN:CAT1546U05J"
```

External AAA, TFTP, and Syslog Servers Configuration

This section shows the implementation of AAA, TFTP, and Syslog servers offering service discovery services to the Autonomic Networking domain.

Avahi Service

The Avahi daemon enables support for multicast DNS and service discovery and must be enabled on all external servers providing services for the Autonomic Networking domain.

```
root@AN:/# service avahi-daemon status
avahi-daemon start/running, process 493
root@AN:/#
```

Shared key, authentication, and accounting port numbers to be used by AAA are defined in aaa.service file, syslog-specific details used by Syslog server are defined in syslog.service file and the directory where the router configuration files are stored in TFTP are defined in conf.service file. All these files are copied into the location /etc/avahi/services on the external server to facilitate the automatic service discovery functions.

```
root@AN:/etc/avahi/services#
aaa.service  conf.service  syslog.service
```

The content of the Avahi configuration files for AAA and Syslog services is shown here for reference.

Avahi AAA Service Configuration File: aaa.service

```
<?xml version="1.0" standalone='no'?><!--*-nxml-*-->
<!DOCTYPE service-group SYSTEM "avahi-service.dtd">

<!-- $Id$ -->

<!--
  This file is part of avahi.

  avahi is free software; you can redistribute it and/or modify it
  under the terms of the GNU Lesser General Public License as
  published by the Free Software Foundation; either version 2 of the
  License, or (at your option) any later version.

  avahi is distributed in the hope that it will be useful, but
  WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
  General Public License for more details.

  You should have received a copy of the GNU Lesser General Public
```

```
  License along with avahi; if not, write to the Free Software
  Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA
  02111-1307 USA.
-->

<!-- See avahi.service(5) for more information about this configuration file -->

<service-group>

  <name replace-wildcards="no">AAA</name>

  <service>
    <type>_aaa._udp</type>
    <txt-record>auth_port=1645;</txt-record>
    <txt-record>acct_port=1646;</txt-record>
    <txt-record>secret_key=rad123;</txt-record>
  </service>

</service-group>
```

Avahi Syslog Service Configuration File: syslog.service

```
<?xml version="1.0" standalone='no'?><!--*-nxml-*-->
<!DOCTYPE service-group SYSTEM "avahi-service.dtd">

<!-- $Id$ -->

<!--
  This file is part of avahi.

  avahi is free software; you can redistribute it and/or modify it
  under the terms of the GNU Lesser General Public License as
  published by the Free Software Foundation; either version 2 of the
  License, or (at your option) any later version.

  avahi is distributed in the hope that it will be useful, but
  WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
  General Public License for more details.

  You should have received a copy of the GNU Lesser General Public
  License along with avahi; if not, write to the Free Software
  Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA
  02111-1307 USA.
-->

<!-- See avahi.service(5) for more information about this configuration file -->

<service-group>

  <name replace-wildcards="no">Syslog on 2005::100</name>

  <service>
    <type>_syslog._udp</type>
  </service>

</service-group>
```

Avahi TFTP Service Configuration File: conf.service

```
<?xml version="1.0" standalone ='no'?><!--*-nxml-*-->
<!DOCTYPE service-group SYSTEM "avahi-service.dtd">

<!-- $Id$ -->
```

```
<!--
  This file is part of avahi.

  avahi is free software; you can redistribute it and/or modify it
  under the terms of the GNU Lesser General Public License as
  published by the Free Software Foundation; either version 2 of the
  License, or (at your option) any later version.

  avahi is distributed in the hope that it will be useful, but
  WITHOUT ANY WARRANTY; without even the implied warranty of
  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
  General Public License for more details.

  You should have received a copy of the GNU Lesser General Public
  License along with avahi; if not, write to the Free Software
  Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA
  02111-1307 USA.
-->

<!-- See avahi.service(5) for more information about this configuration file -->

<service-group>

  <name replace-wildcards="yes">CONFIG on %h</name>

  <service>
    <type>_config._udp</type>
    <txt-record>path=autonomic-networking/;</txt-record>
  </service>

</service-group>
```

AAA Server

Servers providing AAA services to the autonomic network must have a list of all AN devices in their clients file, and the user credentials used by the EEM script for the SSH login in their user profile database.

For AAA functions in an Autonomic Networking environment, the EPN System leverages the FreeRADIUS implementation.

The following changes are required:

- "clients.conf" file in /etc/freeradius/ need to be updated with the information of new AN devices like the ULA IPv6 address allocated by the ANR, secret and nastype as shown below, this has to be done for every AN device which is added in the AN domain.

```
client FD9F:56DB:93E5:0:1C1D:868C:200:1{
        secret   = rad123
        shortname= FD9F:56DB:93E5:0:1C1D:868C:200:1
        nastype=cisco
```

- "users" file in /etc/freeradius/ need to be added with user credentials as shown below:

```
nsite Cleartext-Password := "lab"
     Service-Type = NAS-Prompt-User,
     Cisco-AVPair = "shell:priv-lvl=15"
```

- "radius.conf" file in /etc/freeradius/ need to be modified to enable listening to IPv6 addresses as shown below:

```
listen {
```

```
#       ipaddr = *
        ipv6addr = ::
        port = 1646
        type = acct
}
listen {
#       ipaddr = *
        ipv6addr = ::
        port = 1645
        type = auth
}
```

TFTP Server

The requirement on the TFTP server is that all the configuration files for the respective new devices be maintained in the path /tftpboot/autonomic-networking/. These files are required for the auto-configuration file download after the Zero Touch bootstrap by autonomic process.

```
root@AN:/tftpboot/autonomic-networking# pwd
/tftpboot/autonomic-networking
root@AN:/tftpboot/autonomic-networking# ls
PID_A901-12C-FT-D_SN_CAT1546U00Z.conf  PID_A901-12C-FT-D_SN_CAT1709U0YF.conf
PID_A901-12C-FT-D_SN_CAT1546U03B.conf
                          root@AN:/tftpboot/autonomic-networking#
```

AN Proxy Nodes Configuration: PAN-K1403: ASR 903

This section shows the configuration of the PAN nodes acting as AN proxy devices toward the remote registrar.

```
!*** enables autonomic feature on the node***
autonomic
interface TenGigabitEthernet0/1/0
 description To AGN-K1102 Ten0/0/0/1
!***Need to disable "autonomic feature" on the interface through which IPv6 GRE tunnel
passes on AN Proxy ***
 no autonomic adjacency-discovery
 no autonomic
end
interface Tunnel11403
 no ip address
 ipv6 address 2001:111:111:333::1/112
 ipv6 enable
!***Enabling autonomic adjacency discovery over the IPv6 GRE tunnel in AN Proxy ***
 autonomic adjacency-discovery
 tunnel source TenGigabitEthernet0/1/0
 tunnel mode ipv6ip
 tunnel destination 10.5.13.0
```

Note The configuration is also applicable to PAN-903-K1404, Cisco ASR 903 in the system test topology for a Small Network.

AN Nodes Configuration: CSG-901-K1322, CSG-901-K1323 and CSG-901-K1324

This section shows the Auto-IP portion of the configuration downloaded from the TFTP Server onto the AN nodes after they are successfully bootstrapped into the autonomic network domain and VOBC channel is setup.

Note The following configuration only reflects the Auto-IP enablement portion of a full CSG configuration. The full configuration depends on the connectivity, functional components, and services enabled on the node and it is covered on the respective sections of this guide and its companion service-specific design and implementation guides.

CSG-901-K1322

```
interface GigabitEthernet0/10
 description To CSG-K1323 G0/10
 no ip address
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
!
interface Vlan20
!***Auto-IP configuration on the ring-facing interfaces ***
auto-ip-ring 8 ipv4-address 10.13.22.7
 no ip address
```

CSG-901-K1323

```
interface GigabitEthernet0/10
 description To CSG-K1322 G0/10
 no ip address
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
 !
interface Vlan10
!***Auto-IP configuration on the ring-facing interfaces ***
 auto-ip-ring 8 ipv4-address 10.13.22.3
 ip address 10.13.22.3 255.255.255.254
!
interface GigabitEthernet0/11
 description To CSG-K1324 g0/11
 no ip address
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 20
 !
interface Vlan20
!***Auto-IP configuration on the ring-facing interfaces ***
 auto-ip-ring 8 ipv4-address 10.13.22.3
 ip address 10.13.23.0 255.255.255.254
 ip router isis core
 ip pim sparse-mode
```

CSG-901-K1324

```
interface GigabitEthernet0/11
 description To CSG-K1323 g0/11
 no ip address
service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
 !
interface Vlan10
```

```
!***Auto-IP configuration on the ring-facing interfaces ***
auto-ip-ring 8 ipv4-address 10.13.23.1
 ip address 10.13.23.1 255.255.255.254
 ip router isis core
 ip pim sparse-mode
```

Transport Scale Considerations

This chapter, which describes the route scale and the control plane scaling aspects involved in setting up the Unified MPLS Transport across the network domains, includes the following major topics:

- Route and Control Plane Scale, page 8-3
- BGP Control Plane Scale, page 8-5

As an example, we'll consider a large scale deployment following the Inter-AS design described in Large Network Transport Architecture Design - Inter-AS, page 3-17, including support for Consumer, Enterprise, and MEF and Mobile Transport Services.

- For Mobile Transport Services, the network includes 60,000 CSGs across 20 POPs in a SP network. In the core network, consider around 10 EPC locations, with each location connected to a pair of redundant MTGs. This leads a total of 20 MTGs for transport connectivity from the core to the CSGs in the RAN access domain. If you consider that each RAN access domain is comprised of 30 CSGs connected in physical ring topologies of five nodes each to the pre-aggregation network, and (for the purpose of illustration) you assume an even distribution of RAN backhaul nodes across the 20 POPs, you end up with the network sizing shown in Table 8-1.
- For Consumer and Enterprise wireline services, the network includes 3000 FANs across the same 20 POPs in the SP network. In addition, there are 20 OLTs per POP providing PON access for wireline services. These rings are divided among 100 pairs of PANs per POP, which are configured in rings to 5 pairs of AGNs and 5 pairs of AGN-SE nodes.

The entire POP is aggregated by a pair of AGN-ASBR nodes, which connect to a pair of CN-ASBR nodes for handling all service traffic transport between the core and aggregation domains.

Table 8-1 Large Network Sizing

Large Network	Access	Aggregation	Network (20 POPs)	Comments
CSGs	30	3000 (1-5% FAN)	60000	Assuming 100 access rings in each POP with 30 CSGs in each ring (100*30=3000) (20*3000=60000)
FANs	30	150 (30% RAN)	3000	Assuming 5 access rings in each POP with 30 FANs in each ring (5*30=150) (20*150=3000)
OLTs	20	200	4000	Assuming 10 access rings in each POP with 20 OLTs in each ring (10*20=200) (20*200=4000)

Table 8-1 Large Network Sizing (continued)

Large Network	Access	Aggregation	Network (20 POPs)	Comments
PANs	2	200	4000	Assuming 10 aggregation rings in each POP with 20 PANs in each ring (10*20=200) (20*200=4000)
AGNs		10	200	Assuming 10 AGNs in each POP (20*10=200)
AGN/PAN-SE		10	200	Assuming 10 AGN/PAN-SEs in each POP (20*10=200)
AGN-ASBR		2	40	(20*2=40)
CN-ASBR		2	40	(20*2=40)
Core Node			10	
MTG			20	Assuming 20 MTGs network wide

As another example, consider a smaller scale deployment following the single-AS, multi-area design described in Small Network Transport Architecture Design, page 3-1, including support for Consumer, Enterprise, and MEF and Mobile Transport Services.

- For Mobile Transport Services, the network includes 7,000 CSGs across 20 POPs in a SP network. In the core network, consider around 5 EPC locations, with each location connected to a pair of redundant MTGs. This leads a total of 10 MTGs for transport connectivity from the core to the CSGs in the RAN access domain. If you consider that each RAN access domain is comprised of 30 CSGs connected in physical ring topologies of five nodes each to the pre-aggregation network, and (for the purpose of illustration) you assume an even distribution of RAN backhaul nodes across the 10 POPs, you end up with the network sizing shown in Table 8-2.
- For Consumer and Enterprise wireline services, the network includes 300 FANs across the same 10 POPs in the SP network. In addition, there are 20 OLTs per POP providing PON access for wireline services. These rings are divided among 25 pairs of PANs per POP, which are configured in rings to a pair of AGNs and a pair of AGN-SE nodes.

The entire POP is aggregated by a pair of Core nodes for handling all service traffic transport between the core and aggregation domains.

Table 8-2 Small Network Sizing

Small Network	Access	Aggregation	Network (10 POPs)	Comments
CSGs	30	700	7000	Assuming 23 access rings in each POP with 30 CSGs in each ring (23*30=690) Rounding to 700 (10*700=7000)
FANs	30	30	300	Assuming 1 access ring in each POP with 30 FANs in each ring (10*30=300)
OLTs	20	20	200	Assuming 1 ring with 20 OLTs in each POP. (20*10=200)

Table 8-2 Small Network Sizing (continued)

Small Network	Access	Aggregation	Network (10 POPs)	Comments
PANs	2	50	500	Assuming 2 PANs per Access Ring and 25 Rings Per POP.
AGNs		2	20	2 AGNs per POP
AGN-SE		2	20	2 AGN-SEs per POP
Core Node			20	2 Core Nodes per POP
MTG			10	

Route and Control Plane 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. See Table 8-3.

The Cisco EPN 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 CSG 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 subsecond IGP fast convergence.

Table 8-3 Route Scaling for Transport and Mobile Services

Large Network Devices	Unified MPLS Transport			Mobile Services	
	Core IGP	Access IGP	BGP IP+label	L3 VPN VRFxRoutes	VPWS PW
CSGs		30	20 MSE 10 FXX	3 x (20+30)	3xSAToP
FANs		30	20 MSE 20 FXX	3 x (20+10)	3xSAToP
OLTs					
PANs		212	4000 FAN 200 FSE 20 MSE 30 RAN		

Table 8-3 Route Scaling for Transport and Mobile Services (continued)

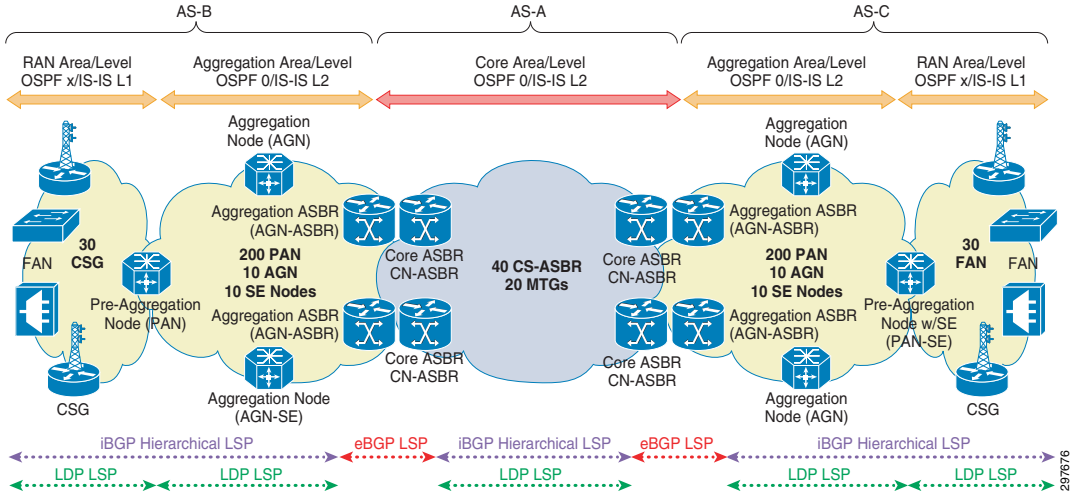
Large Network Devices	Unified MPLS Transport			Mobile Services	
AGNs +Service edge		212 212	4000 FAN 200 FSE		
AGN-ASBR		212	4000 FAN 200 FSE 20 MSE 3000 RAN		
CN-ASBR	70		4000 FAN 200 FSE 20 MSE 3000 RAN		
Core Node	70				
MTG	70		61,000		20

For Consumer and Enterprise Services, the Cisco EPN System design employs a similar hierarchical mechanism as for the Mobile Service transport. All access nodes providing wireline service require connectivity to the SE nodes and any remote access nodes for which E-Line services are configured. This allows for scaling to handle the required service scale without overwhelming the smaller access nodes. See Table 8-4.

Table 8-4 Route Scaling for Consumer and Enterprise Services

Large Network Devices	Consumer Services		Enterprise Services				
	Sessions from Cisco Optical Network Terminators (ONTs)	Multicast Groups	VPWS	VPLS		L3VPN	
				UNI	VFIs	UNI	VRFx Routes
CSGs			5	2	N/A	3	N/A
FANs			10	5		5	
OLTs	3000	300	300	200		500	
PANs							
AGNs +Service edge	60,000 3 services 1 account	500	300 ONTs 30 Ethernet	200 ONTs 5 x30+ 2x60 PWs 20 Ethernet	20	500 ONTs 3x60+ 5x50 PWs 50 Ethernet	50 x 500-1000
AGN-ASBR							
CN-ASBR							
Core Node							
MTG							

Figure 8-1 Cisco EPN System Hierarchical Network



If you consider a hierarchical network design as shown in Figure 8-1, you end up with a route scale across various domains of the Unified MPLS transport network, as shown in Table 8-3 and Table 8-4.

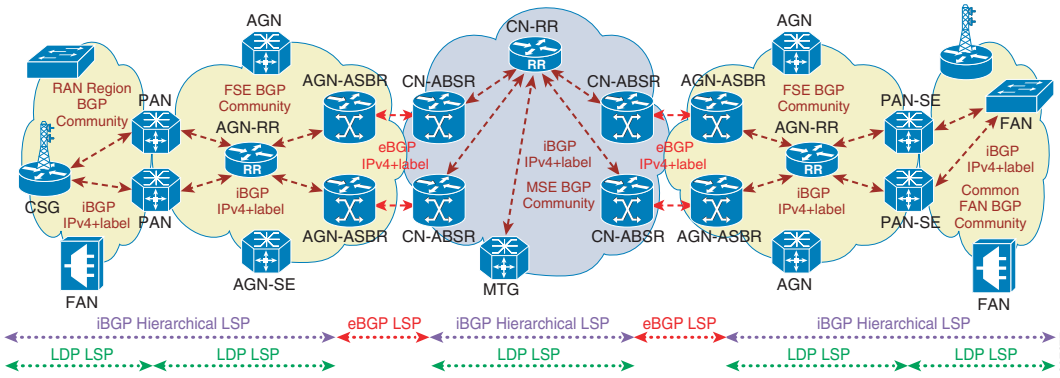
Note

- On CSGs, there are 30 IGP routes that correspond to the local RAN access CSG loopbacks + 2 local PANs, and 30 iBGP routes that correspond to the 20 MTG nodes + a total of 10 nodes between remote FANs and FSEs.
- On PANs, AGNs/-SEs, and AGN-ASBRs, the 212 IGP routes in Core-AGG IGP process correspond to 200 local PANs + 10 local AGN-SEs + 2 local AGN-ASBRs. The iBGP routes are explained in the table.
- On MTGs, the 70 IGP routes correspond to 40 core ABRs + 20 MTG nodes + 10 other core nodes. The 61,000 iBGP IPv4-labeled routes correspond to 60,000 CSG loopbacks + 1000 PANs with locally-attached eNBs.

BGP Control Plane Scale

As described in the "BGP Transport Control Plane" sections of Small Network Transport Architecture Design, page 3-1, the Cisco EPN System uses a hierarchical RR design, utilizing a top-level virtualized RR in each AS, with inline RR functionality on the CN-ASBRs, AGN-ASBRs, and PANs to greatly reduce the number of iBGP peering sessions across different domains of the backhaul network.

Figure 8-2 Cisco EPN System Hierarchical RR Topology



For the example network sizing shown in Figure 8-2, if you consider the peering organization illustrated in Figure 8-1, you have the following BGP session scale on different elements in the network.

Table 8-5 BGP Control Plane Scale

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

Note

- CSGs 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 the vAGN-RR for that domain.
- AGN-SEs in each aggregation domain peer with the vAGN-RR for that domain.
- AGN-ASBRs in each aggregation domain peer with the vAGN-RR for that domain.
- CN-ASBRs peer with the redundant external vCN-RRs in the core domain.
- MTGs in the core domain that connect with regional EPC GWs peer with the redundant external vCN-RRs.

Related Documents

The Cisco EPN 4.0 Transport Infrastructure Design and Implementation Guide is part of a set of resources that comprise the Cisco EPN System documentation suite. The resources include:

- EPN 4.0 System Concept Guide: Provides general information about Cisco's EPN 4.0 System architecture, its components, service models, and the functional considerations, with specific focus on the benefits it provides to operators.
- EPN 4.0 System Brochure: At-a-glance brochure of the Cisco Evolved Programmable Network (EPN).
- EPN 4.0 MEF Transport Services Design and Implementation Guide: Design and Implementation guide with configurations for deploying the Metro Ethernet Forum service transport models and use cases supported by the Cisco EPN System concept.
- EPN 4.0 Mobile Transport Services Design and Implementation Guide: Design and Implementation guide with configurations for deploying the mobile backhaul service transport models and use cases supported by the Cisco EPN System concept.
- EPN 4.0 Residential Services Design and Implementation Guide: Design and Implementation guide with configurations for deploying the consumer service models and the unified experience use cases supported by the Cisco EPN System concept.
- EPN 4.0 Enterprise Services Design and Implementation Guide: Design and Implementation guide with configurations for deploying the enterprise L3VPN service models over any access and the personalized use cases supported by the Cisco EPN System concept.

Note All of the documents listed above, with the exception of the System Concept Guide and System Brochure, are considered Cisco Confidential documents. Copies of these documents may be obtained under a current Non-Disclosure Agreement (NDA) with Cisco. Please contact a Cisco Sales account team representative for more information about acquiring copies of these documents.