CableLabs®

IPv6 Roadmap Requirements Document

CM-GL-IPv6-REQ-V01-120831

ISSUED

CAUTION

DISCLAIMER

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various agencies; technological advances; or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein. CableLabs makes no representation or warranty, express or implied, with respect to the completeness, accuracy, or utility of the document or any information or opinion contained in the report. Any use or reliance on the information or opinion is at the risk of the user, and CableLabs shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any cable member to purchase any product whether or not it meets the described characteristics. Nothing contained herein shall be construed to confer any license or right to any intellectual property, whether or not the use of any information herein necessarily utilizes such intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	CM-GL-IPv6-REQ-V01-120831			
Document Title:	IPv6 Roadmap Requirements Document			
Revision History:	V01 - 8/31/12			
Date:	August 31, 2012			
Status:	~~Work in Progress~~	~~Draft~~	**Released**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	**CL/Member**	~~CL/ Member/ Vendor~~	~~Public~~

Trademarks

Table of Contents

1 INTRODUCTION 1
1.1 Overview 1
1.2 Scope 1
2 REFERENCES 3
2.1 Reference Acquisition 9
3 TERMS AND DEFINITIONS 10
4 ABBREVIATIONS AND ACRONYMS 11
5 HIGH SPEED DATA (HSD) USE CASES 15
5.1 Provision a DOCSIS 3.0 or DOCSIS 2.0+IPv6 CM using IPv6 15
5.1.1 Provisioning Mode Override 15
5.2 Manage an IPv6 CM Using SNMP 17
5.3 Home Gateway acquires an IPv6 Address and Prefix 17
5.4 Home Gateway enables CPE IPv6 Provisioning using SLAAC 18
5.5 Home Gateway enables CPE IPv6 Provisioning using Stateful DHCPv6 18
5.6 Home Gateway forwards Non-Multicast IPv6 Traffic 19
5.7 Home Gateway Security 19
5.7.1 MSO Protection 19
5.7.2 User Protection 20
5.8 Home Gateway Interaction with UPnP Service 20
5.9 Prefix Stability and Prefix Aggregation 20
5.9.1 IPv6 Prefix Delegation 20
5.9.2 Prefix Stability 21
5.10 Deferred Use Cases 23
5.10.1 Prefix Sub-Delegation 23
5.10.2 Reverse DNS 24
6 VOICE USE CASES 25
6.1 EDVA Provisioning Use Cases 25
6.1.1 EDVA IPv6 Provisioning 25
6.1.2 EDVA Dual-Stack (IPv4 and IPv6) Provisioning 25
6.1.3 eUE SIP Registration 26
6.1.4 Manage an IPv6 E-DVA using SNMP 26
6.2 Basic Dual-Stack Interworking Use Cases 26
6.2.1 Dual-Stack E-DVA attached to IPv4-only Network 26
6.2.2 E-DVA attached to Dual-Stack P-CSCF calls E-DVA attached to IPv4-only P-CSCF 27
6.2.3 Dual-Stack E-DVA calls IPv4-only E-DVA attached to Dual-Stack Network 28
6.2.4 Dual-Stack E-DVA calls IPv4 E-DVA over IPv6 Network 28
6.2.5 E-DVAs in Dual-Stack Regions connect across an IPv4-only Core 29
6.2.6 Dual-Stack E-DVAs place a Call over a Dual-Stack Network 30
6.2.7 E-DVA on an IPv6-only Network Calls another Dual-Stack E-DVA 31
6.2.8 Dual-Stack Interworking Summary 31
6.3 PacketCable 2.0- PacketCable 1.5 Interworking 32
6.3.1 Dual-Stack 2.0 E-DVA Registered using IPv4 calls IPv4 1.5 E-MTA 32
6.3.2 Dual-Stack 2.0 E-DVA Registered using IPv6 calls IPv4 1.5 E-MTA 33
6.3.3 Single-stack IPv4 2.0 E-DVA calls IPv4 1.5 E-MTA 33
6.3.4 Single-Stack IPv6 2.0 E-DVA calls IPv4 1.5 E-MTA 34

6.4 PacketCable 2.0 IPv4/IPv6 Interworking 35
6.4.1 IPv6 E-DVA calls IPv4 E-DVA 35
6.4.2 IPv4 E-DVA calls IPv6 E-DVA 36
6.4.3 IPv6 E-DVA calls Public Switched Telephone Network (PSTN) 36
6.4.4 IPv4 to IPv4 E-DVA over an IPv6 network 37
6.5 PacketCable 2.0 Conferencing 37
6.5.1 IPv4/IPv6 Conferencing with a Conferencing Server that supports IPv4/IPv6 38
6.5.2 IPv4/IPv6 Conferencing with an IPv4-only Conferencing Server 38
6.6 PacketCable Peering 39
6.6.1 IPv4 E-DVA calls IPv6 E-DVA across MSO Domains 39
6.6.2 IPv6 E-DVA calls IPv4 E-DVA across MSO Domains 40
6.6.3 Dual-Stack E-DVA calls Dual-Stack E-DVA over an IPv4 Interconnect 41
6.6.4 IPv6 E-DVA calls IPv6 E-DVA over an IPv4 Interconnect 42
6.7 Softphone Use Cases 42
6.7.1 IPv4 Softphone attached to IPv4 Network 43
6.7.2 IPv6 Softphone attached to IPv6 network 43
6.7.3 IPv4 Softphone attached to IPv4 Network using NAT444 44
6.7.4 IPv4 Softphone attached to IPv6 Network using DS-Lite 45
6.8 PC 1.5 across IPv6 Network 45
6.8.1 IPv4 E-MTA, IPv4 CMS, and an IPv6 Interconnect 45

7 IPV6 WEB CONTENT USE CASES 47

7.1 Internal Web Content/Portal Support 47
7.1.1 Typical Web Services Architecture 47
7.1.2 Enabling IPv6 Web Services 47
7.1.3 Load Balancers with IPv6 Support 48
7.1.4 IPv6-enabled Web Servers 48
7.1.5 IPv6-enabled DNS Servers 49
7.1.6 Secure Web Connection 49
7.1.7 Digital Certificates 49
7.2 Proxy Server 51
7.2.1 Implementation Methods 51
7.2.2 IPv6 Proxy Servers 51
7.3 Geolocation 51
7.3.1 Geolocation in IPv4 51
7.3.2 Geolocation Uses 52
7.3.3 Geolocation Providers 52
7.3.4 IPv6 Implications 52
7.4 Content Distribution Networks (CDNs) 52
7.4.1 CDN and IPv6 52
7.5 Web Content Providers and IPv6 53
7.5.1 Requirements for IPv6 Web Content 53
7.6 IPv6 DNS Support 53
7.6.1 Domain Name System (DNS) Overview 53
7.6.2 DNS IPv6 Behavior 54
7.6.3 Steps to enable IPv6 DNS 54
7.6.4 IPv6 DNS Whitelists 54
7.7 IPv6 High-Value Applications 55
7.7.1 Email 55
7.7.2 FTP 56
7.7.3 Instant Messenger (IM) 56
7.7.4 Gaming and Mobile Platforms 56
7.7.5 P2P File Sharing Apps 56

8 LAWFUL INTERCEPT USE CASES 57

8.1 Cable Broadband Intercept Specification (CBIS) Overview and IPv6 Accommodation 57

8.1.1 CBIS Outline *57*
8.1.2 CBIS Operation *58*
8.1.3 CBIS IPv6 Status *58*
8.1.4 Transition Technology Impact on CBIS *59*
8.2 PacketCable Electronic Surveillance Overview and IPv6 Accommodation 61
8.2.1 PacketCable LAES Overview *61*
8.2.2 IPv6 Support in PC LAES *64*
8.2.3 Transition Technology Impact on Softphone Lawful Intercept *64*
8.2.4 Analysis *66*
8.3 Data/Record Storage 66

9 TECHNICIAN AND OSS ACCESS USE CASES 67

9.1 Assumptions 67
9.2 Network Diagram 67
9.3 Overview of Use Cases 68
9.4 Direct Technician Access Use Cases 68
9.4.1 Technician with Dual-Stack Connectivity *68*
9.4.2 Technician on IPv4-only Network *69*
9.4.3 In-Home Access to eRouter *71*
9.5 Indirect Technician Access 72
9.6 Back Office Access to CM 73
9.6.1 B/OSS Tools with IPv6 Support *73*

10 VIDEO USE CASES 74

10.1 DOCSIS Set-top Gateway (DSG) 74
10.1.1 DSG and MDD Provisioning Mode *74*
10.1.2 DSG Tunnels and IPv6 ..... *75*
10.1.3 Proposed Transition Plan for DSG *75*
10.2 IP Simulcast (IPS) 75
10.2.1 IPv6 Impacts for IPS *77*
10.3 Emergency Alert System (EAS) 78
10.3.1 IPv6 Implications for EAS *78*
10.4 In-Home Video Delivery 79
10.4.1 Universal Plug and Play (UPnP) *79*
10.4.2 Digital Living Network Alliance (DLNA) *80*
10.4.3 OpenCable Home Networking (OCHN) *80*
10.4.4 Service Discovery Use Cases within the Home *81*
10.4.5 In-Home Video Delivery IPv6 Impact *84*
10.5 Close Captioning (CC) and Parental Controls 85
10.5.1 IPv6 Impacts *86*
10.6 Tru2Way ("OpenCable") 86
10.6.1 OpenCable IPv6 Considerations *86*
10.6.2 IPv6 Considerations for Devices in Subscriber Home *86*
10.6.3 IPv6 Considerations for Devices in Operators Network *86*
10.6.4 Dual-Stack Considerations *87*
10.7 Enhanced Television Binary Interchange Format (EBIF) 87
10.7.1 IPv6 Considerations for EBIF *87*
10.8 Content Delivery from Programmer to Multichannel Video Programming Distributor (MVPD) 88
10.8.1 IPv6 Considerations for Acquiring Programming Content *88*
10.9 Online Content Access (OLCA) 88
10.9.1 IPv6 Impacts on OLCA *89*
10.10 Advanced Advertising 89
10.10.1 IPv6 Impacts for Advance Advertising *91*
10.11 Linear Ad Insertion 91
10.11.1 IPv6 Transition Considerations for Ad Insertion *92*

11 CGN USE CASES 93

11.1 Introduction 93
11.2 Overview and scope 93
11.2.1 Overview NAT444 93
11.2.2 Overview DS-Lite 94
11.2.3 Overview 6RD 95
11.3 Deployment Considerations 96
11.3.1 Network Architecture 96
11.3.2 Routing CGN Traffic 98
11.3.3 Redundancy 100
11.3.4 Load Balancing and Scalability 100
11.3.5 Server Location and NAT Bypass 101
11.3.6 IP Addressing 101
11.3.7 Outside Addressing 102
11.3.8 Inside Addressing 102
11.3.9 Geolocation 102
11.3.10 Lawful Intercept (LI) 103
11.3.11 Security 103
11.3.12 Logging 104

12 HOME AND ACCESS SECURITY USE CASES 107

12.1 Introduction, Overview, and Scope 107
12.1.1 Security Threats under Consideration 107
12.1.2 Areas Under Consideration 107
12.2 DOCSIS Security 108
12.2.1 Overview and DOCSIS Security Review 108
12.2.2 Security Threats for DOCSIS 109
12.2.3 Theft of Service 110
12.2.4 Loss of Privacy 111
12.2.5 Spoofing 111
12.2.6 Denial of Service 111
12.2.7 DOCSIS Threats and Controls Summary 113
12.2.8 DOCSIS Security Recommendations 113
12.3 Home Network Security 114
12.3.1 Overview 114
12.3.2 Scope and Out of Scope 114
12.3.3 Theft of Service 115
12.3.4 Spoofing 116
12.3.5 Loss of Privacy and Tampering 116
12.3.6 Denial of Service 117
12.3.7 Home Network Threats and Control Summary 117
12.3.8 Home Network Security Recommendations 118
12.3.9 Firewalls and Filtering 119
12.3.10 Miscellaneous Home Network Security Topics 120
12.4 IPv6 Transition Technologies 123
12.4.1 Introduction and Scope 123
12.4.2 Tunneling Technologies 125
12.4.3 Address Sharing Technologies 128
12.5 Provisioning Server and CMTS Security 129
12.5.1 DHCPv6 Issue (Windows Clients) 129
12.5.2 CMTS ND Table Issue 129
12.6 Deep Packet Inspection 130
12.6.1 DPI Introduction and Background 130
12.6.2 DPI and IPv6 130
12.7 Security Use Case Summary 130

13 ADVANCED HOME NETWORKING USE-CASES 132

13.1 Home Network Architectures 132
13.1.1 Directly Connected Host 132
13.1.2 "Baseline" Architecture 132
13.1.3 "Single Router" Architecture 134
13.1.4 Multi-Router Architectures 135
13.1.5 Other Home-Network Architecture Considerations 146
13.1.6 Timeline 148
13.2 Service Discovery 148
13.2.1 Service Discovery Timeline 149
13.3 IP Video Gateway 149
13.3.1 Combined Data and Video Gateway 150
13.3.2 Independent Gateways 150
13.3.3 Hierarchical Gateways 151
13.3.4 Timeline 155
13.4 Home Routing Protocol 156

14 REQUIREMENTS 158

14.1 General Requirements 158
14.2 Cable Modem Requirements 158
14.2.1 DOCSIS 2.0+IPv6 CM 158
14.2.2 DOCSIS 3.0 CM 158
14.2.3 DSG CM 158
14.3 IP Simulcast Gateway Requirements 158
14.4 eSTB Requirements 159
14.4.1 OCHN Extension Requirements 159
14.5 CMTS Requirements 159
14.5.1 DSG CMTS 159
14.6 eRouter/Home Gateway Requirements 159
14.6.1 Security Requirements 160
14.7 Dual-stack E-DVA Requirements 160
14.8 PC 2.0 Core (e.g., x-CSCF) Requirements 161
14.9 TrGW Requirements 161
14.10 SBC Requirements 161
14.11 Server Requirements 161
14.11.1 Common Requirements for All Servers 161
14.11.2 DHCP Server 162
14.11.3 DNS Server 162
14.11.4 Time Server 163
14.11.5 TFTP Server 163
14.11.6 Network Management Server 163
14.11.7 Syslog Server 164
14.11.8 SMTP Server 164
14.11.9 FTP Server 164
14.11.10 PacketCable Key Distribution Center (KDC) Server 164
14.11.11 Tunnel Server 164
14.11.12 Common Alert Protocol (CAP) Server for EAS 164
14.11.13 DSG Server 164
14.11.14 IP Streaming Server 164
14.11.15 EBIF Application/Aggregation Server 164
14.11.16 OLCA Authentication/Authorization Server 164
14.11.17 Advanced Advertising Servers 165
14.12 CGN Device Requirements 165
14.12.1 Functional Requirements 165
14.12.2 Security Requirements 165

14.12.3 Session Logging and Retrieval Requirements 165
14.12.4 Application Layer Gateway (ALG) Requirements 166
14.12.5 Resiliency Requirements 166
14.12.6 Management Requirements 166
14.13 6to4 Relay, 6RD Relay Security Requirements 167
14.14 MSO Firewall 167
14.14.1 DPI Servers 167
14.15 Other Requirements 168
14.15.1 MSO Recommendations Related to Security 168

15 FEATURES UNDER DEVELOPMENT 169

15.1 IPv6 Home Networking 169

Figures

Figure 1 - Provisioning Mode Override Recommendation 17
Figure 2 - IPv6 Prefix Delegation 21
Figure 3 - IPv6 Aggregation Example 23
Figure 4 - eDVA Provisioning Sequence Diagram 25
Figure 5 - Dual-Stack EDVA, IPv4 Network 26
Figure 6 - E-DVA attached to Dual-Stack P-CSCF calls E-DVA attached to IPv4-only P-CSCF 27
Figure 7 - Dual-Stack E-DVA calls IPv4-only E-DVA attached to Dual-Stack Network 28
Figure 8 - Dual-Stack E-DVA calls IPv4 E-DVA over IPv6 Network 28
Figure 9 - E-DVAs in Dual-Stack Regions Connect across an IPv4-only Core 29
Figure 10 - Dual-Stack E-DVAs Place a Call over a Dual-Stack Network 30
Figure 11 - E-DVA on an IPv6-only Network Calls another Dual-Stack E-DVA 31
Figure 12 - Dual-Stack 2.0 E-DVA Registered using IPv4 calls IPv4 1.5 E-MTA 32
Figure 13 - Dual-Stack 2.0 E-DVA Registered using IPv6 calls IPv4 1.5 E-MTA 33
Figure 14 - Single-Stack IPv4 2.0 E-DVA calls IPv4 1.5 E-MTA 33
Figure 15 - Single-Stack IPv6 2.0 E-DVA calls IPv4 1.5 E-MTA 34
Figure 16 - IPv6 E-DVA calls IPv4 E-DVA 35
Figure 17 - IPv4 E-DVA calls IPv6 E-DVA 36
Figure 18 - IPv6 E-DVA calls PSTN 36
Figure 19 - IPv4 to IPv4 E-DVA over an IPv6 network 37
Figure 20 - IPv4/IPv6 Conferencing with a Conferencing Server that supports IPv4/IPv6 38
Figure 21 - IPv4/IPv6 Conferencing with an IPv4-only Conferencing Server 38
Figure 22 - IPv4 E-DVA calls IPv6 E-DVA across MSO Domains 39
Figure 23 - IPv6 E-DVA calls IPv4 E-DVA across MSO Domains 40
Figure 24 - Dual-Stack E-DVA calls Dual-Stack E-DVA over an IPv4 Interconnect 41
Figure 25 - IPv6 E-DVA calls IPv6 E-DVA over an IPv4 Interconnect 42
Figure 26 - IPv4 Softphone attached to IPv4 Network 43
Figure 27 - IPv6 Softphone attached to IPv6 Network 43
Figure 28 - IPv4 Softphone attached to IPv4 Network using NAT444 44
Figure 29 - IPv4 Softphone attached to IPv6 Network using DS-Lite 45
Figure 30 - PC 1.5 across IPv6 Network 46
Figure 31 - Web Services Architecture 47
Figure 32 - Load Balancers 48
Figure 33 - Web Services Architecture 48
Figure 34 - Certificate Example 50
Figure 35 - DNS Root 54
Figure 36 - CBIS Broadband Intercept Interfaces 57
Figure 37 - CBIS Logical Network 58
Figure 38 - NAT444: LI 59
Figure 39 - DS-Lite: LI 60
Figure 40 - 6RD: LI 60
Figure 41 - PacketCable Lawfully Authorized Electronics Surveillance: Functions and Interfaces 62
Figure 42 - Intercept Points, a Simple Overview 63
Figure 43 - Content IAP Discovery 63

Figure 44 - Softphone with NAT444 64
Figure 45 - Softphone with DS-Lite 65
Figure 46 - Softphone with 6RD 65
Figure 47 - Technician Access Overview 67
Figure 48 - Direct Technician Dual-Stack Access 68
Figure 49 - Tunneling Using ISATAP 69
Figure 50 - Tunneling Using a Gateway 70
Figure 51 - In Home access to the eRouter 71
Figure 52 - Indirect Technician Access 72
Figure 53 - DSG Components 74
Figure 54 - DSG Tunnels terminating on an eSTB 75
Figure 55 - IPS video Delivery Model 76
Figure 56 - IPS video deliver models 76
Figure 57 - IPS Data Gateway (V-GW) Reference Model 76
Figure 58 - IPS Video Gateway (D-GW) Reference Model 77
Figure 59 - IPv6 Impacts across the IPS Network 77
Figure 60 - Current/Legacy EAS Architecture 78
Figure 61 - Future EAS/CAP/IPAWS Topology 78
Figure 62 - UPnP AV Devices and Services 79
Figure 63 - Basic DLNA Architecture 80
Figure 64 - OCHN Overview 80
Figure 65 - One Flat IPv4 Network 81
Figure 66 - 2 Routed IPv4 Segments 82
Figure 67 - One Flat Dual-Stack Network 83
Figure 68 - Two Routed Segments Dual-Stack Network 84
Figure 69 - In-Home Video Delivery IPv6 Impact 85
Figure 70 - OpenCable Components 86
Figure 71 - EBIF Components 87
Figure 72 - Acquiring Programming Content 88
Figure 73 - OLCA Use Cases 89
Figure 74 - Interactive Advertising 90
Figure 75 - Addressable Advertising 90
Figure 76 - Media Measurement 91
Figure 77 - Linear Ad Insertion Architecture and Components 92
Figure 78 - Timeline of Access Technology Transition 93
Figure 79 - NAT444 Example 94
Figure 80 - DS-Lite Example 95
Figure 81 - 6RD Example 96
Figure 82 - Centralized Architecture 97
Figure 83 - Distributed Architecture 97
Figure 84 - Hybrid CGN Architecture (Phased Approach) 98
Figure 85 - Options for Routing CGN Traffic 99
Figure 86 - Load Balancing and Scalability Example 101
Figure 87 - Overcoming Location-Related Obstacles imposed by CGN 103

Figure 88 - CGN Subscriber Identity Traceback Illustration 104
Figure 89 - Deterministic NAT Illustrated 105
Figure 90 - Scope of Security Focus Areas 107
Figure 91 - DOCSIS Security Snapshot 108
Figure 93 - Teredo Components 126
Figure 95 - Media Intercept Position 128
Figure 96 - Summary of Security Controls at each Device 131
Figure 97 - Example "Baseline" Home Architecture 133
Figure 98 - Example "Single Router" Home Network Architecture 134
Figure 99 - Example Expected Physical Home Network Topology 136
Figure 100 - Example (4x5) Uniform Hierarchical Addressing 137
Figure 101 - High-Level Home Network Addressing Schemes 138
Figure 102 - Addressing Mechanisms 138
Figure 103 - Detailed Home Network Addressing Mechanism Analysis 139
Figure 104 - Hierarchical DHCPv6 PD 140
Figure 105 - Hierarchical DHCPv6 PD + NPT 141
Figure 106 - Hierarchical DHCPv6 PD + Tunnels (Overlay) 142
Figure 107 - Logical GUA Topology for Overlay Network 143
Figure 108 - IR Routing Table for Overlay Network 143
Figure 109 - CER Routing Table for Overlay Network 144
Figure 110 - DHCPv6 Relay 145
Figure 111 - ULA Boundary 147
Figure 112 - Timelines for Future Home-Network Architectures 148
Figure 113 - Service Discovery Timeline 149
Figure 114 - IP Video Gateway Scenario 1: Combined Gateway 150
Figure 115 - IP Video Gateway Scenario 2: Independent Gateways 151
Figure 116 - IP Video Gateway Scenario 3: Hierarchical Gateways 152
Figure 117 - IP Video Gateway Scenario 3.1: Hierarchical Gateway with Dual NPT 153
Figure 118 - IP Video Gateway Scenario 3.2: Hierarchical Gateway with NPT and RIO 153
Figure 119 - IP Video Gateway Scenario 3.3: Hierarchical Gateway with Reverse PD 154
Figure 120 - IP Video Gateway Scenario 3.4: Hierarchical Gateway with Proxy 155
Figure 121 - Proxy and Dual NPT Methods of the Hierarchical Gateway Scenario 155

Tables

Table 1 - Dual-Stack Media Interworking Scenarios 31
Table 2 - PacketCable Internal LAES Interfaces 62
Table 3 - EAS IPv6 Impacts 79
Table 4 - Examples of Routing CGN Traffic 99
Table 5 - DOCSIS Security Mechanisms 109
Table 6 - IPv6 Transition Technologies 124

1 INTRODUCTION

1.1 Overview

This requirements document has been developed by CableLabs and its member companies to enumerate technical and operational requirements for deploying IPv6 for device management and services (e.g., high speed data, voice, and video) over DOCSIS networks.

IPv6, initially defined in the mid-1990s, offers a complete replacement for its predecessor, IPv4. While similar to IPv4 in many ways, IPv6 offers expanded addressing, stateless auto-configuration, enhanced Quality of Service (QoS), and mobility support.

A key feature of IPv6 is the 128-bit addressing scheme that the protocol employs. That is, IPv6 offers 340 undecillion (3.4x1038) addresses, compared to 4.3 billion in IPv4. In effect, IPv6 allows for nearly infinite addresses. There are enough addresses to assign one to every atom on the surface of the earth. This abundance of addresses theoretically enables true end-to-end communications while lessening the need for address sharing technologies such as Network Address Translation (NAT). While IPv6 has many advertised benefits and features, the primary interest for most adopters is its expanded address space compared to IPv4. The rate of IPv6 adoption has seen a noticeable increase in recent years, despite the perceived lack of interest when the protocol was first developed. In fact an active adopter of IPv6, Google reports as of late 2008 that IPv6 makes up about ¼% of Internet traffic. While these figures show growing interest in IPv6, they also clearly indicate how much work remains before IPv6 is widely deployed. One of the variables attributed to the slow adoption of IPv6 was the deferral of fundamental motivators, namely the scarcity of IPv4 addresses. The uses of techniques such as NAT and Classless Inter-Domain Routing (CIDR) delayed IPv4 exhaustion and slowed address consumption, but couldn't stop it.

The Internet Assigned Numbers Authority (IANA) depleted its global free pool of IPv4 addresses in February 2011 and the first Regional Internet Registry, Asia-Pacific Network Information Centre (APNIC), exhausted its supply two months later, in mid-April. The American Registry for Internet Numbers (ARIN) and Réseaux Internet Protocol Européens (RIPE) are expected to hand out their last IPv4 by the middle of 2012 as well, limiting MSOs' (and all ISPs') ability to obtain additional IPv4 addresses needed to continue to grow their subscriber base, offer new services, and support new devices.

Additionally, some operators are starting to experience that in advance of RIR depletion, policy changes have introduced additional scrutiny that is causing delays in obtaining IPv4 address space. Following the RIRs' IPv4 exhaustion, consumers of IPv4 addresses, such as service providers, are likely to experience depletion of their own address pools shortly thereafter. To lessen the impact and ensure that there is ample capacity for growth and service expansion, providers should plan to leverage IPv6 and reclaim unused IPv4 address space in the near future. To that end, they must initiate IPv6 planning and deployment efforts well in advance to make sure that their infrastructure is truly ready and operational from an IPv6 point of view.

1.2 Scope

This document describes IPv6 requirements for cable networks. It is to be used as a resource to guide deployment planning and frame discussions between MSOs and their suppliers. As such, it describes IPv6 use cases for cable and lists high-level requirements used to satisfy them. These requirements will reference CableLabs specifications and Internet Engineering Task Force (IETF) Requests for Comments (RFCs) to delineate the critical IPv6 features to enable data, voice, video, and other services.

Requirements described in this document are applicable to access network devices, such as cable modems (CMs), eRouters, and cable modem termination systems (CMTSs). These requirements are also applicable to back office servers, including DHCP, TFTP, Time of Day, Domain Name System (DNS), syslog, and Carrier Grade NAT (CGN) servers.

This document contains the output of use-case discussions on the following topics:

1. Manage D2.0+IPv6 and 3.0 CM
2. Offer IPv6 HSD Service

3. IPv6 HSD Transition scenarios (including IPv4 address exhaustion)
4. Provide Voice services
5. Enable IPv6 Web content
6. Support Lawful Intercept
7. Provide for Technician Access
8. IP Provisioning Mode Override
9. Prefix Stability
10. Provide Video services
11. World IPv6 Day
12. CGN Requirements
13. Home and Access Security
14. Advanced Home Networking

2 REFERENCES

This document uses the following references.

[AUTH1.0] CableLabs Authentication and Authorization Interface 1.0 Specification, CL-SP-AUTH1.0-I04-120621, June 21, 2012, Cable Television Laboratories, Inc.

[CANN DHCP-Reg] CableLabs DHCP Options Registry Specification, CL-SP-CANN-DHCP-Reg-I09-120809, August 8, 2012, Cable Television Laboratories, Inc.

[CBIS] DOCSIS Cable Broadband Intercept Specification CM-SP-CBI2.0-I04-110224, February 24, 2011, Cable Television Laboratories, Inc.

[DOCSIS2.0-IPv6] CableLabs DOCSIS 2.0+IPv6 Specification, CM-SP-DOCSIS2.0-IPv6-I06-120809, August 8, 2012, Cable Television Laboratories, Inc.

[DSG] DOCSIS Set-top Gateway (DSG) Interface Specification, CM-SP-DSG-I21-120809, August 8, 2012, Cable Television Laboratories, Inc.

[eRouter] CableLabs eRouter Specification, CM-SP-eRouter-I09-120809, August 8, 2012, Cable Television Laboratories, Inc.

[ES DCI] PacketCable Electronic Surveillance Delivery Function to Collection Function Interface Specification PKT-SP-ES-DCI-I02-070925, September 25, 2007, Cable Television Laboratories, Inc.

[ES INF] PacketCable Electronic Surveillance - Intra-Network Functions Specification, PKT-SP-ES-INF-I04-080425, April 25, 2008, Cable Television Laboratories, Inc.

[HOST2.1-CFR] OpenCable Specifications OpenCable Host Device 2.1, Core Functional Requirements, OC-SP-HOST2.1-CFR-I16-120531, May 31, 2012, Cable Television Laboratories, Inc.

[ID-3484bis] IETF Internet Draft, Default Address Selection for Internet Protocol version 6 (IPv6), draft-ietf-6man-rfc3484bis-06, D. Thaler, Ed., R. Draves, A. Matsumoto, T. Chown, June 2012.

[ID-CER-ID] IETF Internet Draft, Customer Edge Router Identification Option, draft-donley-dhc-cer-id-option-00, C. Donley, C. Grundemann, March 2012.

[ID-Prefix-Alloc] IETF Internet Draft, Simple Approach to Prefix Distribution in Basic Home Networks, draft-chakrabarti-homenet-prefix-alloc-01, E. Nordmark, S. Chakrabarti, S. Krishnan, W. Haddad, October 2011.

[ID-DNS46] IETF Internet Draft, DNS46 for the IPv4/IPv6 Stateless Translator, draft-xli-behave-dns46-for-stateless-03, August 2011.

[ID-DNS-SRV] IETF-Internet Draft, DNS-Based Service Discovery, draft-cheshire-dnsext-dns-sd-11, December 2011.

[ID-HNA_IPV6] IETF Internet Draft, Home Networking Architecture for IPv6, draft-arkko-townsley-homenet-arch-04, July 2012.

[ID-Home-Relay] IETF Internet Draft, Home Network Autoconfiguration via DHCPv6 Relay, draft-gmann-homenet-relay-autoconf-01, C. Grundemann, C. Donley, March 2012.

[ID-IPv6SEC] IETF-Internet Draft, Advanced Security for IPv6 CPE, Advanced Security for IPv6 CPE, Eric Vyncke, Andrew Yourtchenko, Mark Townsley, draft-vyncke-advanced-ipv6-security-03, October 2011.

[ID-MAX_SOL_RT] IETF Internet Draft, Modification to Default Value of MAX_SOL_RT, draft-droms-dhc-dhcpv6-maxsolrt-update-00, R. Droms, November 2011.

[ID-MCAST-DNA] IETF Internet Draft, Multicast DNS, draft-cheshire-dnsext-multicastdns-15, December 2011.

[ID-nat444] IETF Internet Draft, NAT444 addressing models, draft-shirasaki-nat444-isp-shared-addr-08.txt, Jiro Yamaguchi, Yasuhiro Shirasaki, Shin Miyakawa, Akira Nakagawa, Hiroyuki Ashida, July 2012.

[ID-Prefix-Alloc] IETF Internet Draft, Simple Approach to Prefix Distribution in Basic Home Networks, draft-chakrabarti-homenet-prefix-alloc-01, E. Nordmark, S. Chakrabarti, S. Krishnan, W. Haddad, October 2011.

[ID-Routing-Req] IETF Internet Draft, Homenet Routing Requirements, draft-howard-homenet-routing-requirements-00, L. Howard, December 2011.

[ID-UP-PIO] IETF Internet Draft, The UP PIO Field: Finding Up in an Unmanaged Network, draft-howard-up-pio-00, L. Howard, November 2011.

[MULPI] DOCSIS MAC and Upper Layer Protocol Interface Specification, CM-SP-MULPIv3.0-I18I19-120809, August 9, 2012, Cable Television Laboratories, Inc.

[OCAP-HNEXT] OpenCable Application Platform Specifications, OCAP Extensions, OCAP Home Networking Extension, OC-SP-OCAP-HNEXT-I09-120531, May 31, 2012, Cable Television Laboratories, Inc.

[OSSI] DOCSIS Operations Support System Interface Specification, CM-SP-OSSIv3.0-I19-120809, August 9, 2012, Cable Television Laboratories, Inc.

[RFC0868] IETF RFC 868/STD0026, Time Protocol, J. Postel and K. Harrenstien, May 1983.

[RFC1157] IETF RFC 1157, A Simple Network Management Protocol, J. Case, M. Fedor, M. Schoffstall, J. Davin, May 1990.

[RFC1350] IETF RFC 1350/STD0033, The TFTP Protocol (Revision 2), K. Sollins, July 1992.

[RFC1901] IETF RFC 1901, Introduction to Community-based SNMPv2 (Informational), J. Case, K. McCloghrie, M. Rose, S. Waldbusser, January 1996.

[RFC1918] IETF RFC 1918, Address Allocation for Private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, February 1996.

[RFC1981] IETF RFC 1981, Path MTU Discovery for IPv6, J. McCann, S. Deering, J. Mogul, August 1996.

[RFC2428] IETF RFC 2428, FTP Extensions for IPv6 and NATs, M. Allman, S. Ostermann, C. Metz, September 1998.

[RFC2460] IETF RFC 2460, Internet Protocol v6 (IPv6) Specification, S. Deering, R. Hinden, December 1998.

[RFC2473] IETF RFC 2473, Generic Packet Tunneling in IPv6, A. Conta, S. Deering, December 1998.

[RFC2578] IETF RFC 2578/STD0058, Structure of Management Information Version 2 (SMIv2), K. McCloghrie, D. Perkins, J. Schoenwaelder, April 1999.

[RFC2579] IETF RFC 2579/STD0058, Textual Conventions for SMIv2, K. McCloghrie, D. Perkins, J. Schoenwaelder, April 1999.

[RFC2580] IETF RFC 2580/STD0058, Conformance Statements for SMIv2, K. McCloghrie, D. Perkins, J. Schoenwaelder, April 1999.

[RFC2784] IETF RFC 2784, Generic Routing Encapsulation (GRE), D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000.

[RFC2786] IETF RFC 2786, Diffie-Helman USM Key Management Information Base and Textual Convention, J. Salsman, H. Alvestrand, May 2000.

[RFC2827] IETF RFC 2827, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, P. Ferguson, D. Senie, May 2000.

[RFC2874] IETF RFC 2874, DNS Extensions to Support IPv6 Address Aggregation and Renumbering, M. Crawford, C. Huitema, July 2000.

[RFC2979] IETF RFC 2979, Behavior of and Requirements for Internet Firewalls. N. Freed., October 2000.

[RFC3056] IETF RFC 3056, Connection of IPv6 Domains via IPv4 Clouds. B. Carpenter, K. Moore. February 2001.

[RFC3226] IETF RFC 3226, DNSSEC and IPv6 A6 aware server/resolver message size requirements, O. Gudmundsson, December 2001.

[RFC3315] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, July 2003.

[RFC3363] IETF RFC 3363, Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS), R. Bush, A. Durand, B. Fink, O. Gudmundsson, T. Hain, August 2002.

[RFC3376] IETF RFC 3376, Internet Group Management Protocol, Version 3, B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, October 2002.

[RFC3410] IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, J. Case, R. Mundy, D. Partain, B. Stewart, December, 2002.

[RFC3411] IETF RFC 3411/STD0062, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, D. Harrington, R. Presuhn, B. Wijnen, December 2002.

[RFC3412] IETF RFC 3412/STD0062, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), J. Case, D. Harrington, R. Preshun, B. Wijnen, December 2002.

[RFC3413] IETF RFC 3413/STD0062, Simple Network Management Protocol (SNMP) Applications, D. Levi, P. Meyer, B. Stewart, December, 2002.

[RFC3414] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), U. Blumenthal, B. Wijnen, December 2002.

[RFC3415] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), B. Wijnen, R. Presuhn, K. McCloghrie, December 2002.

[RFC3416] IETF RFC 3416/STD0062, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), R. Presuhn, December 2002.

[RFC3417] IETF RFC 3417/STD0062, Transport Mappings for the Simple Network Management Protocol (SNMP), R. Presuhn, December 2002.

[RFC3418] IETF RFC 3418/STD0062, Management Information Base for the Simple Network Management Protocol (SNMP), R. Presuhn, December 2002.

[RFC3419] IETF RFC 3419, Textual Conventions for Transport Addresses, M. Daniele, J. Schoenwaelder, December 2002.

[RFC3484] IETF RFC 3484, Default Address Selection for Internet Protocol version 6 (IPv6), R. Draves, February 2003.

[RFC3584] IETF RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, R. Frye, D. Levi, S. Routhier, B. Wijnen, August 2003.

[RFC3596] IETF RFC 3596, DNS Extensions to Support IP Version 6, S. Thomson, C. Huitema, V. Ksinant, M. Souissi, October 2003.

[RFC3633] IETF RFC 3633, IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, O. Troan, R. Droms, December 2003.

[RFC3704] IETF RFC 3704, Ingress Filtering for Multihomed Networks. F. Baker, P. Savola, March 2004.

[RFC3810] IETF RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6, R. Vida, L. Costa, June 2004.

[RFC3826] IETF RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model, U. Blumenthal, F. Maino, K. McCloghrie, June 2004.

[RFC3879] IETF RFC 3879, Deprecating Site Local Addresses C. Huitema, B. Carpenter, September 2004.

[RFC3971] IETF RFC 3971, Secure Neighbor Discovery (SEND). J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander, March 2005.

[RFC3972] IETF RFC 3972, Cryptographically Generated Addresses (CGA). T. Aura, March 2005.

[RFC3974] IETF RFC 3974, SMTP Operational Experience in Mixed IPv4/v6 Environment, M. Nakamura, J. Hagino, January 2005.

[RFC4033] IETF RFC 4033, DNS Security Introduction and Requirements, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, March 2005.

[RFC4034] IETF RFC 4034, Resource Records for the DNS Security Extensions, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, March 2005.

[RFC4035] IETF RFC 4035, Protocol Modifications for the DNS Security Extensions, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, March 2005.

[RFC4120] IETF RFC 4120, The Kerberos Network Authentication Service (V5). C. Neuman, T. Yu, S. Hartman, K. Raeburn, July 2005.

[RFC4191] IETF RFC 4191, Default Router Preferences and More-Specific Routes, R. Draves, D. Thaler, November 2005.

[RFC4193] IETF RFC 4193, Unique Local IPv6 Unicast Addresses. R. Hinden, B. Haberman, October 2005.

[RFC4213] IETF RFC4213, Basic Transition Mechanisms for IPv6 Hosts and Routers. E. Nordmark, R. Gilligan, October 2005.

[RFC4291] IETF RFC 4291, IPv6 Addressing Architecture, R. Hinden, S. Deering, February 2006.

[RFC4361] IETF RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), T. Lemon, B. Sommerfeld, February 2006.

[RFC4380] IETF RFC 4380, Teredo: Tunneling IPv6 over UDP through Network Address, Translations (NATs). C. Huitema, February 2006.

[RFC4443] IETF RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, A. Conta, S. Deering, M. Gupta, March 2006.

[RFC4470] IETF RFC 4470, Minimally Covering NSEC Records and DNSSEC On-line Signing, S. Weiler, J. Ihren, April 2006.

[RFC4639] IETF RFC 4639, Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems, R. Woundy, K, Marez, December 2006.

[RFC4861] IETF RFC 4861, Neighbor Discovery for IPv6, T. Narten, E. Nordmark, W. Simpson, H. Soliman, September 2007.

[RFC4862] IETF RFC 4862, IPv6 Stateless Address Auto-configuration, S. Thompson, T. Narten, T. Jinmei, September 2007.

[RFC4864] IETF RFC 4864, Local Network Protection for IPv6. G, Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, May 2007.

[RFC4941] IETF RFC 4941, Privacy Extensions for Stateless Address Autoconfiguration IPv6, T. Narten, R. Draves, S. Krishnan, September 2007.

[RFC4942] IETF RFC 4942, IPv6 Transition/Co-existence Security Considerations. E. Davies, S. Krishnan, P. Savola, September 2007.

[RFC4949] IETF RFC 4949, Internet Security Glossary, Version 2. R. Shirey, August 2007.

[RFC5214] IETF RFC 5214, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), F. Templin, T. Gleeson, D. Thaler, March 2008.

[RFC5308] IETF RFC 5308, Routing IPv6 with IS-IS, C. Hopps, October 2008.

[RFC5340] IETF RFC 5340, OSPF for IPv6. R. Coltun, D. Ferguson, J. Moy, A. Lindem, July 2008.

[RFC5424] IETF RFC 5424, The Syslog Protocol, R. Gerhards, March 2009.

[RFC5569] IETF RFC 5569, IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), R. Despres, January 2010.

[RFC5905] IETF RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, D. Mills, J. Martin, Ed., J. Burbank, W. Kasch, June 2010.

[RFC5969] IETF RFC 5969, IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification, W. Townsley, O. Troan, August 2010.

[RFC6092] IEFT RFC 6092, Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, J. Woodyatt, Ed., January 2011.

[RFC6106] IETF RFC 6106, IPv6 Router Advertisement Options for DNS Configuration, J. Jeong, S. Park, L. Beloeil, S. Madanapalli, November 2010.

[RFC6144] IETF RFC 6144, Framework for IPv4/IPv6 Translation. F. Baker, X. Li, C. Bao, K. Yin, April 2011.

[RFC6145] IETF RFC 6145, IP/ICMP Translation Algorithm. X. Li, C. Bao, F. Baker, April 2011.

[RFC6146] IETF RFC 6146, Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, M. Bagnulo, P. Matthews, I. van Beijnum, April 2011.

[RFC6147] IETF RFC 6147, DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, M. Bagnulo, A. Sullivan, P. Matthews, I. van Beijnum, April 2011.

[RFC6169] IETF RFC 6169, Security Concerns with IP Tunneling. S. Krishnan, D. Thaler, J. Hoagland, April 2011.

[RFC6204] IETF RFC 6024, Basic Requirements for IPv6 Customer Edge Routers, H. Singh, W. Beebee, C. Donley, B. Stark, O. Troan, Ed., April 2011.

[RFC6219] IETF RFC 6219, The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition, X. Li, C. Bao, M. Chen, H. Zhang, J. Wu, May 2011.

[RFC6264] IETF RFC 6264, An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition, S. Jiang, D. Guo, B. Carpenter, June 2011.

[RFC6296] IETF RFC 6296, IPv6-to-IPv6 Network Prefix Translation, M. Wasserman, F. Baker, June 2011.

[RFC6333] IETF RFC 6333, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, A. Durand, R. Droms, J. Woodyatt, Y. Lee, August 2011.

[RFC6346] IETF RFC 6346, The Address plus Port (A+P) Approach to the IPv4 Address Shortage, R. Bush, Ed., August 2011.

[RFC6384] IETF RFC6384, An FTP Application Layer Gateway (ALG) for IPv6-to-IPv4 Translation, I. van Beijnum, October 2011.

[RFC6555] IETF RFC 6555, Happy Eyeballs: Success with Dual-Stack Hosts, Dan Wing, Andrew Yourtchenko, December 2011.

[RFC6598] IANA-Reserved IPv4 Prefix for Shared Address Space, Jason Weil, Victor, Kuarsingh, Chris Donley, Christopher Liljenstolpe, Marla Azinger, April 2012

[SCTE104] ANSI/SCTE 104 2011, Automation System to Compression System Communications Applications Program Interface (API).

[SCTE18] ANSI/SCTE 18 2007, Emergency Alert Messaging for Cable.

[SCTE30] ANSI/SCTE 30 2009, Digital Program Insertion Splicing API.

[SCTE65] ANSI/SCTE 65 2008, Service Information Delivered Out-of-Band for Digital Cable Television.

[SECv3.0] DOCSIS Security Specification, CM-SP-SECv3.0-I13-110611, June 11, 2011, Cable Television Laboratories, Inc.

[UPnP] UPnP Device Architecture v1.1 Annex A – IP Version 6 Support, UPnP Forum, 2011. http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1-AnnexA.pdf

2.1 Reference Acquisition

CableLabs Specifications:

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; Internet: http://www.cablelabs.com.

IETF Specifications:

- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001.
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org/
  Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.
  The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
  Internet-Drafts may also be accessed at http://tools.ietf.org/html/

Society of Cable Telecommunications Engineers:

- http://www.scte.org/standards/Standards_Home.aspx

UPnP Forum

- http://upnp.org/sdcps-and-certification/standards/device-architecture-documents/

3 TERMS AND DEFINITIONS

This document uses the following terms:

Cable Modem (CM)	A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.
Cable Modem Termination System (CMTS)	Cable Modem termination system, located at the cable television system headend or distribution hub, which provides complementary functionality to the Cable Modems to enable data connectivity to a wide-area network.
DOCSIS 2.0+IPv6 CM	A DOCSIS 2.0 Cable Modem that supports IPv6 Provisioning and Management and supports connected IPv6 eSAFEs and external CPE devices.
eRouter	An eSAFE device that is implemented in conjunction with the DOCSIS Embedded Cable Modem.

4 ABBREVIATIONS AND ACRONYMS

This document uses the following abbreviations:

6RD	IPv6 Rapid Deployment
A+P	Address+Port Routing
AAA	Authentication, Authorization, and Accounting
ACA	Accounting Answer
ACL	Access Control List
ACR	Accounting Request
AEIT	Aggregate Event Information Table
AFTR	Address Family Transition Router
ALG	Application Layer Gateway
AM	Application Manager
APM	Alternate Provisioning Mode
ARIN	American Registry for Internet Numbers
BIF	Broadband Intercept Function
BR	Border Relay
CALEA®	Commission on Accreditation for Law Enforcement Agencies, Inc.
CAP	Common Alert Protocol
CAS	Conditional Access System
CC	Call Content, Close Captioning.
CCF	common container format
CDC	Call Data Collection
CDNs	Content Distribution Networks
CER	CPE Edge Router
CER ID	CPE Edge Router Identification
CF	Collection Function
CGN	Carrier Grade NAT
CII	Call-Identifying Information
CM	Cable Modem
CMTS	Cable Modem Termination System
CPD	Control Point Discovery
CPE	Customer Premise Equipment
CSCF	Call session control function
CVT	Code Version Table
DAD	Duplicate Address Detection
DDNS	Dynamic DNS
DF	Delivery Function
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMCA	Digital Millennium Copyright Act

DNS	Domain Name System
DNS-SD	DNS Service Discovery
DNSSEC	Domain Name System Security Extensions
DOCSIS	Data-Over-Cable Service Interface Specifications
DoS	Denial of Service
DPI	Deep Packet Inspection
DPM	Dual-Stack Provisioning Mode
DSG	DOCSIS Set-top Gateway
DS-Lite	Dual-Stack Lite
DTMF	Dual Tone Multi-Frequency
DUID	Device Unique Identifier
EAE	Early Authentication Encryption
EAS	Emergency Alert System
EBIF	Enhanced Television Binary Interchange Format
EVDA	Embedded Digital Voice Adaptor
FQDN	Fully-Qualified Domain Name
GUA	Globally Unique Address
HLR	Home Location Register
IA_PD	Identity Association for Prefix Delegation
IAF	Intercept Access Function
IANA	Internet Assigned Numbers Agency
IAP	Intercept Access Point
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGD	Internet Gateway Device
IPS	Intrusion Prevention System, IP Simulcast
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Internal Router
LAES	Lawfully Authorized Electronics Surveillance
LAN	Local Area Network
LEA	Law Enforcement Agency
LEAF	Law Enforcement Administrative Function
LI	Lawful Interception
LLMNR	Local Multicast Name Resolution
LSN	Large-Scale NAT
MAC	Media Access Control
MDD	MAC Domain Descriptor
mDNS	Multicast DNS
MG	Mmedia Gateway
MGC	Media Gateway Controller

MITM	Man in the Middle
MPD	media presentation description
MSO	Multiple Systems Operator
MVPD	Multichannel Video Programming Distributor
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NAT-PMP	NAT Port Mapping Protocol
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NUD	Neighbor Unreachability Detection
NMS	Network Management System
NPT	Normal Play Time
NS	Neighbor Solicitation
NTP	Network Time Protocol
NTSC	National Television System Committee
NUD	Neighbor Un-reachability Detection
OCHN	OpenCable Home Networking
OLCA	OnLine Content Access
OOB	Out Of Band
PC 2.0	PacketCable 2.0
PCP	Port Control Protocol
PE	Provider Edge
P-CSCF	Proxy Call Session Control Function
PKI	Public Key Infrastructure
PMT	Program Map Table
PS	Policy Server
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RA	Router Advertisement
RAAN	Relay Agent Assignment Notification
RD	Router Discovery
RF	Radio Frequency
RFC	Request For Comment
RIO	Route Information Object
RIPng	Routing Information Protocol next generation
RIR	Regional Internet Registry
RKAP	Reconfigure Key Authentication Protocol
RD	Router Discovery
RRT	rating region table
RS	Router Solicitation
SAML	Secure Association Markup Language

SAV	Source Address Verification
SBC	Session Border Controller
SBE	Signaling Path Border Element
SDP	Session Description Protocol
SEND	Secure Neighbor Discovery
SLAAC	Stateless Address Autoconfiguration
SLP	Service Location Protocol
SMPTE	Society of Motion Picture and Television Engineers
SNMP	Simple Network Management Protocol
SPAF	Service Provider Administration Function
SSDP	Simple Service Discovery Protocol
SSL	Secure Socket Layer
SSM	Site-Specific Multicast
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TLV	Type-Length-Value
ToD	Time of Day
ToS	Type of Service
TrGW	Translation Gateway
TTML	Timed Text in XML
UDC	Upstream Drop Classifier
UDP	User Datagram Protocol
ULA	Unique Local Address
UPMP	Universal Port Mapping Protocol
UPnP	Universal Plug and Play
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
XACML	Extensible Access Control Markup Language
XAIT	Extended Application Information Table

5 HIGH SPEED DATA (HSD) USE CASES

5.1 Provision a DOCSIS 3.0 or DOCSIS 2.0+IPv6 CM using IPv6

This use case discusses provisioning of a DOCSIS 3.0 or DOCSIS 2.0+IPv6 CM and includes IPv6 address assignment, Time-of-Day (ToD) acquisition, and configuration file acquisition through Trivial File Transfer Protocol (TFTP).

During IP initialization, a DOCSIS 3.0 CM acquires an IP address, the current time-of-day, and a binary configuration file from the cable operator. DOCSIS 3.0 defines use of IP version 4 and IP version 6 and four provisioning modes: IPv4 Only, IPv6 Only, Alternate, and dual-stack. For IPv4 Only provisioning, the CM uses DHCPv4 to acquire an IPv4 address and operational related parameters. For IPv6 Only provisioning, the CM uses DHCPv6 to acquire an IPv6 address and operational parameters. The CM uses the IPv6 address to obtain the current time-of-day and a configuration file. For Alternate Provisioning Mode (APM) the CM combines the first two provisioning modes, IPv6 Only and IPv4 Only, in sequential order, attempting IPv6 provisioning first. If IPv6 provisioning fails, the CM attempts IPv4 provisioning next. In the first three provisioning modes, IPv6 Only, IPv4 Only, and APM, the CM operates with only one IP address type (v4 or v6) at any given time; and thus these modes are called single-stack modes. For Dual-stack Provisioning Mode (DPM), the CM acquires both IPv6 and IPv4 addresses and parameters through DHCPv6 and DHCPv4 almost simultaneously, prioritizing the use of the IPv6 address for time-of-day and configuration file acquisition. In this mode, the CM makes both the IPv4 and the IPv6 addresses available for management.

There are only slight differences in the provisioning processes of a DOCSIS 2.0+IPv6 CM and a DOCSIS 3.0 CM. First, the CM supports the ToD process defined in [DOCSIS2.0-IPv6] rather than [MULPI]. Second, support for Dual-stack and Alternate Provisioning Modes is optional for DOCSIS2.0+IPv6 CM. The CM establishes IPv6 connectivity, which includes assignment of a Link-local address, the default router, the IPv6 management address, and other IPv6 configuration parameters.

5.1.1 Provisioning Mode Override

5.1.1.1 Problem Statement and Solution

In the current DOCSIS Provisioning model, the CM Provisioning mode is set by CMTS in the MAC Domain Descriptor (MDD) message. The Provisioning modes allowed are IPv4, IPv6, APM, and DPM. Only IPv4 and IPv6 are used in practice today. The problem is that some CMs do not fully support IPv6 with the current firmware.

The solution is to allow MDD Override to be set in the CM using Simple Network Management Protocol (SNMP) or CM config files. Three values are allowed for this configuration parameter: IPv4only, IPv6only, and HonorMDD. Not all CMs support MDD override currently.

In order to support Multiple Systems Operator (MSO) requirements for more granular control over provisioning modes and to enable smooth IPv6 rollouts, the following MIB objects have been recently added to CableLabs specifications.

- Provisioning Mode Storage type determines whether the CM retains the value of the MDD override across a single reset or all resets. The default is non-volatile - to persist Override mode across all resets. This gives MSOs granular control when introducing IPv6. When setting Override to IPv6 on a CM for the first time, the persistence can be set to volatile - single reset. If the CM does not provision correctly in IPv6 mode, the override will be removed on next reboot, thus going back to IPv4 mode. If the CM comes up in IPv6 mode and is fully operational, the persistence can be changed to non-volatile - all resets. This reduces the chance of permanently disabling CM by accident.
- The Reset on Change object determines whether the CM resets upon a change to the MDD override value or waits for MSO action (docsDevResetNow). The default is False (No Reset). The Reset on Change Hold Off Timer object determines how long the CM waits (in seconds) before the automatic reset (0=immediate, max 300 seconds). The default is 0 (immediate reset). These settings give MSOs granular control when changing value of MDD override as part of IPv6 rollout. They allow reboot to be manually initiated during the maintenance cycle.

The sub-sections below describe how these controls are to be used, what the current recommendation is and how the recommendation may change over time.

5.1.1.2 Evaluation of Deployment Modes

The deployment modes and outcomes can vary a lot depending on the following variables:

- Does CM support IPv6 per DOCSIS specs? (Yes/No)
- Does CM support Prov mode override? (Yes/No)
- MDD mode? (IPv4, IPv6)
- Override mode? (IPv4, IPv6, HonorMDD)

The following sub-sections consider the outcomes when setting Provisioning Mode Override using different settings on CMs that may or may not entirely support IPv6 and/or Provisioning Mode Override. These sections are followed by a summary of viable combinations.

5.1.1.2.1 Deploying with MDD Mode=IPv4

Does CM support IPv6 per DOCSIS specs?	Does CM support Prov mode override?	MDD mode	Override mode	Result
Yes	Yes	IPv4	IPv6	CM comes up in IPv6 mode, works
No	No	IPv4	IPv6	CM comes up in IPv4 mode, works
Yes	No	IPv4	IPv6	CM comes up in IPv4 mode, works
No	Yes	IPv4	IPv6	CM tries to come up in IPv6 mode, permanently broken

5.1.1.2.2 Deploying with MDD Mode=IPv6

Does CM support IPv6 per DOCSIS specs?	Does CM support Prov mode override?	MDD mode	Override mode	Result
Yes	Yes	IPv6	Honor MDD	CM comes up in IPv6 mode, works
No	Yes	IPv6	IPv4	CM comes up in IPv4 mode, works
Yes	No	IPv6	Honor MDD	CM comes up in IPv6 mode, works
No	No	IPv6	IPv4	CM tries IPv6 mode, broken until moved to IPv4 network

5.1.1.3 Summary of Viable Combinations

Operation for CMs with full IPv6 support is described below:

- CM comes up in IPv6 mode when MDD or Override is set to IPv6.
- CM that does not support Override will come up in IPv4 mode if MDD is set to IPv4.

Operation for CMs without full IPv6 support is described below:

- CM comes up in IPv4 mode when MDD or Override set to IPv4.
- CM that does not support Override will not come up at all if MDD is set to IPv6.
- CM becomes permanently unresponsive ("brick") if it supports Override and Override is set to IPv6.

5.1.1.4 Recommendations

The near-term recommendation is as follows:

- CMTS always sets MDD to IPv4 for all CMs. CMs prior to passing QA get IPv4 (no Override).

For CMs that have passed QA, set Override to IPv6 using volatile override mode. If CM provisions are OK, then change to non-volatile mode. If CM fails IPv6 provisioning, then remove override, upgrade firmware, and try again.

Over time, the IPv6 implementations are expected to mature, so the longer term recommendation timeline that takes advantage of this trend is shown below. Note that this timeframe may be different for each MSO depending on the vendor they work with.

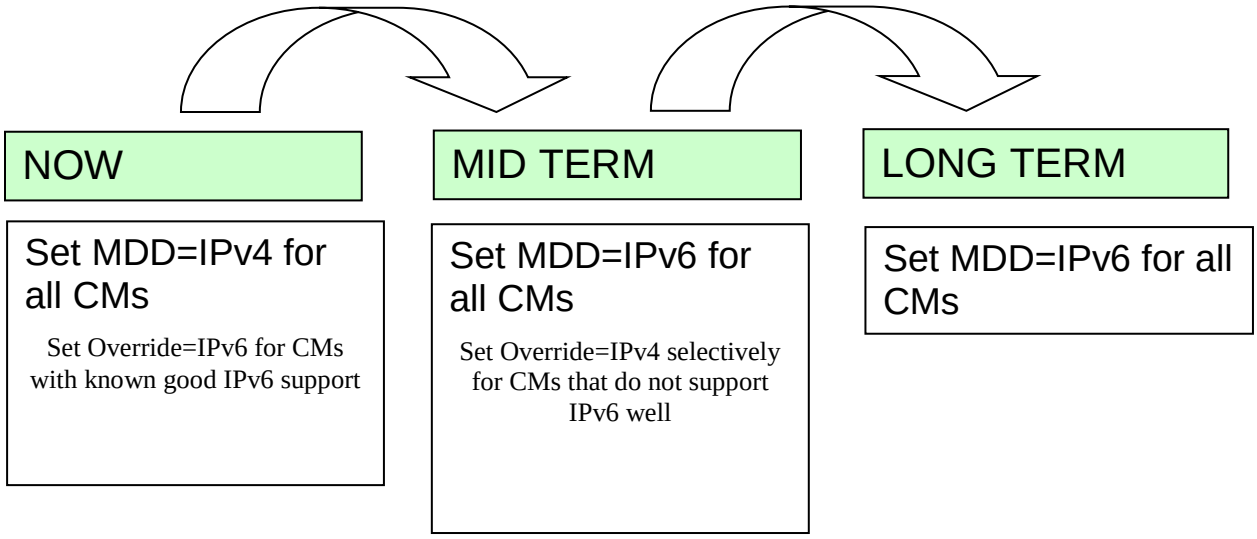

Figure 1 - Provisioning Mode Override Recommendation

5.2 Manage an IPv6 CM Using SNMP

This use case discusses managing a CM (provisioned in IPv6 mode) using SNMP. A Network Management Server can accomplish this through one of two methods: either directly by contacting the CM, or indirectly by contacting the CMTS.

There are three methods for managing an IPv6-enabled CM from an NMS using SNMP.

- Exchanging SNMP messages directly with the CM

NOTE: DOCSIS 3.0 and DOCSIS 2.0+IPv6 CMs are managed in SNMPv1v2c Coexistence mode or NmAccess Mode. The CM will only allow access to the SNMP agent in accordance with OSSIv3.0.

- Exchanging SNMP messages with the CMTS using IPv6
- Exchanging SNMP messages with the CMTS using IPv4

In addition, the CM may also send syslog messages to an IPv6-enabled syslog server. When certain events occur or thresholds are crossed, the CM and/or CMTS sends an SNMP trap message and/or syslog message to the appropriate server. The CM acquires the address of the appropriate syslog server(s) during provisioning through the DHCP advertise/reply messages. The CM acquires its trap receiver address through TLV 38 in the CM configuration file. The CMTS can also send syslog and trap messages to the syslog server and SNMP trap receiver, respectively.

5.3 Home Gateway acquires an IPv6 Address and Prefix

This use case describes how an IPv6 Home Gateway connected to a DOCSIS 2.0+IPv6 or 3.0 Cable Modem acquires its IPv6 address and prefix from the service provider network.

The Home Gateway connects to the MSO network through the Cable Modem. On its Operator Facing Interface, the Home Gateway assigns itself a Link-Local IPv6 address and performs Duplicate Address Detection on the Link-Local address. The 2.0+IPv6 or 3.0 Cable Modem enables propagation of Link-Local Multicast traffic for Neighbor Solicitation (NS) Duplicate Address Detection (DAD) message from the CMTS to the Home Gateway. The Home Gateway looks for a Router Advertisement (RA); if it does not see one within the stipulated timeout period, it sends out a Router Solicit. The CM propagates the RA received on its Radio Frequency (RF) to the Home Gateway.

The Home Gateway examines the contents of RAs it receives and obeys the following rules: If the M bit in the RA is set to 1, the Home Gateway uses DHCPv6 to obtain its IPv6 address for its Operator-Facing Interface and other configuration information (and ignore the O bit). If there are no prefix information options in the RA, the Home Gateway should not perform Stateless Address Autoconfiguration (SLAAC). If the RA contains a prefix advertisement with the A bit set to 0, the Home Gateway should not perform SLAAC on that prefix. The Home Gateway follows the M, O, and A flag bits from the RA and initiates stateful DHCPv6 with the MSO network.

The Operator's DHCPv6 provisioning server is able to distinguish the Home Gateway from an Operator-provided device (e.g., a CM) by using the device capabilities reported in the DHCP requests. The Home Gateway completes the four-message DHCPv6 exchange with the Operator's DHCPv6 server or with just two messages if using the Rapid Commit Option, and then performs Duplicate Address Detection on the Operator-assigned DHCPv6 address. The CM enables propagation of Link-Local Multicast traffic for NS (DAD) message from the CMTS to the Home Gateway. Now the Home Gateway gains IPv6 connectivity and is capable of passing IPv6 traffic to and from the Operator network and sends a DHCPv6 solicit to the Operator's DHCPv6 server requesting a Prefix Delegation to use for provisioning the subscriber IPv6 Hosts.

5.4 Home Gateway enables CPE IPv6 Provisioning using SLAAC

This scenario describes how an IPv6 Home Gateway provisions a subscriber IPv6 host using SLAAC.

The Subscriber IPv6 host device connects to the Home Gateway and assigns itself a Link-Local IPv6 address. The IPv6 host performs DADfor the Link-Local address. It then looks for an RA; if it does not see one within the stipulated timeout period, it sends out a Router Solicit.

The Home Gateway generates RAs on its Customer-Facing Interfaces as per [RFC4862]. Unless the Home Gateway is otherwise configured by an administrator, the RA sets: the M bit to 0, the O bit to 1, and a prefix advertisement with the A bit set to 1 derived from the prefix acquired via DHCPv6.

The Home Gateway generates the RA towards its Customer Facing Interface and includes at least one /64 that it acquired for subscriber host provisioning from the Operator during its DHCPv6 exchange. The IPv6 host follows the M, O, and A flag bits from the RA and initiates stateless auto-configuration of its IPv6 Address using the /64 from the RA. Now the IPv6 host assigns itself an IPv6 Address using the /64 provided in the RA and then performs DAD on the auto-configured IPv6 address. The host uses DHCPv6 to obtain the IPv6 address of the Domain Name Server (DNS) from the Home Gateway. The IPv6 host thus gains IPv6 connectivity and is capable of passing IPv6 traffic to and from the Home Gateway.

5.5 Home Gateway enables CPE IPv6 Provisioning using Stateful DHCPv6

This scenario describes how an IPv6 Home Gateway provisions a subscriber IPv6 host using stateful DHCPv6.

The Subscriber IPv6 host device connects to the Home Gateway. The host assigns itself a Link-Local IPv6 address and performs DAD for the Link-Local address. The IPv6 host looks for an RA; if it does not see one within the stipulated timeout period, it sends out a Router Solicit.

The default CPE provisioning mode is to use SLAAC; however, the Home Gateway also supports DHCPv6. When configured to enable DHCPv6, the Home Gateway generates RAs on its Customer-Facing Interfaces, as per [RFC4862] as follows: (the M bit set to 1, O bit set to 0, A bit set to 0).

The Home Gateway generates an RA towards its Customer Facing Interface. It includes at least one /64 that it acquired from the Operator. The IPv6 host follows the M, O, and A flag bits from the RA and initiates stateful DHCPv6 with the Home Gateway. The IPv6 host performs a DHCPv6 exchange with the Home Gateway and performs DAD on the DHCPv6-assigned IPv6 address. The IPv6 host gains IPv6 connectivity and is capable of passing IPv6 traffic to and from the Home Gateway.

5.6 Home Gateway forwards Non-Multicast IPv6 Traffic

This scenario describes how an IPv6 Home Gateway routes IPv6 traffic to and from a subscriber IPv6 host after successful provisioning. The Subscriber IPv6 host device connects to the Home Gateway, gains IPv6 connectivity, and is capable of passing IPv6 traffic to and from the Home Gateway.

The IPv6 Home Gateway is responsible for implementing IPv6 routing. The Neighbor Discovery (ND) protocol is required on the Home Gateway. This provides a mechanism for converting IPv6 network addresses to Ethernet MAC addresses on both Customer-Facing and Operator-Facing IPv6 Interfaces Network Address Translation and also provides a mechanism for the Home Gateway to advertise its presence, host configuration parameters, routes, and on-link preferences.

The IPv6 Home Gateway uses a local IPv6 routing table to forward packets. The Home Gateway creates the IPv6 routing table upon initialization of the IPv6 portion of the Home Gateway and adds entries according to the receipt of RA messages containing on-link prefixes and routes.

The Home Gateway receives a packet and checks the destination address of the packet. If the destination IPv6 address matches the address assigned to the Home Gateway's IP interface, the Home Gateway forwards the packet to its local IP stack for processing. If the destination IPv6 address does not match the Home Gateway's address, the Home Gateway determines the next-hop address of the destination in order to forward the packet. The next-hop can be a router or the destination itself. The next-hop is determined by comparing the destination IPv6 address to the subnets assigned to the IP interface on which the Home Gateway is transmitting. If the destination IPv6 address matches a sub-net prefix, the destination is considered directly connected or "on-link," and the next-hop to use for ND purposes is the destination IPv6 address. If it does not match, the destination is considered remote or "off-link", and the next-hop to use for ND purposes is the address of the intermediate router.

The typical scenario for packets routed to the Operator-Facing IP Interface is that the next-hop router will be the Home Gateway's default, learned via RA, from the CMTS. Discovering other routers, aside from the CMTS (or routing delegate chosen if the CMTS is a bridge), on the Operator-Facing IP Interface is left to vendor implementation. Discovery of other directly connected devices on the Operator-Facing IP Interface is also vendor-specific.

The typical scenario for packets routed back out the Customer-Facing IP interface is that the next-hop is a local host on a different subnet than that of the source, but directly connected to the Home Gateway. If the Home Gateway cannot determine the next-hop of the IPv6 destination address, then it drops the packet.

Once a next-hop is determined, the Home Gateway's Neighbor Cache is consulted for the link-layer address of the next-hop address. If necessary, address resolution is performed. Address resolution is accomplished by multicasting an NS that prompts the addressed neighbor to return its link-layer address in a Neighbor Advertisement. The neighbor cache entry is then updated with this link-layer address and the Home Gateway then forwards the packet to the link-layer address contained in this cache entry. If an error occurs at any point in the process, the Home Gateway discards the packet.

5.7 Home Gateway Security

This use case involves protecting the MSO from malicious user traffic and protecting the user from malicious Internet traffic. It describes how an MSO can filter obviously malicious user traffic without blocking legitimate customer traffic. The MSO role is not to provide exhaustive security to the customer; however the MSO can take basic precautions to protect the user from obviously malicious traffic.

5.7.1 MSO Protection

It is considered a best practice to filter traffic as close to the source as possible. For an MSO network, that suggests that filtering of obviously malicious customer traffic should occur at the edge – in the cable modem or CMTS.

The DOCSIS 3.0 specification defines Upstream Drop Classifiers (UDCs), which direct CMs to filter traffic, including IPv6 traffic. MSOs include UDCs in CM config files, and CMs activate them during the provisioning and registration process. MSOs could configure UDCs to drop traffic likely to be malicious, such as traffic sourced from an IPv6 address outside of the MSO's IPv6 range or destined for restricted IPv6 addresses, such as MSO corporate billing or database servers.

DOCSIS 2.0+IPv6 modems do not support UDCs. In order to filter malicious customer traffic in a DOCSIS 2.0+IPv6 mixed 2.0+IPv6/3.0 environment, the MSO will need to install ingress traffic filters at the CMTS RF interface.

5.7.2 User Protection

In keeping with security best practices, there are three places to filter malicious traffic: at the MSO's Internet edge, at the CMTS, or in a Home Gateway.

At the MSO Internet edge, firewalls should inspect incoming traffic for invalid parameters, such as an IPv6 source address from the MSO IPv6 address range, invalid IP protocol numbers, or invalid TCP/UDP port numbers. MSO firewalls could also inspect traffic for viruses.

The MSO could perform similar packet inspections at the CMTS to filter for malicious subscriber-to-subscriber traffic.

The customer is advised to have a firewall installed at the edge of the DOCSIS network, such as in a Home Gateway. A Home Gateway firewall has been excluded from the eRouter specification [eRouter], but it is expected that vendors would choose to implement eRouter with a firewall. Firewall configuration is the responsibility of the customer.

5.8 Home Gateway Interaction with UPnP Service

This use case describes the scenario when the customer has enabled UPnP services within the home network.

UPnP specs are currently being updated to include support for IPv6. Once IPv6 is standardized to be used with UPnP, the IPv6 Home Gateway will need to implement a UPnP service agent to announce its capabilities for various services that are available to connect home devices. Home Gateway may be employed for traffic prioritization to home devices with UPnP applications. Further details on UPnP interaction with devices in the home is covered in Section 10.4.1.

5.9 Prefix Stability and Prefix Aggregation

Service Providers assign addresses differently in IPv4 and IPv6. In IPv4, the Service Provider offers one or more public IP addresses via DHCP or static configuration, and the customer applies it to the router Wide Area Network (WAN) port. The customer configures the router LAN port with [RFC1918] private address space and provides [RFC1918] space to PCs via DHCP. The customer uses NAT translation to convert from the LAN side private IP to the WAN side public IP.

For IPv6, [RFC1918] NAT is not supported. To assign IPv6 addresses, the Service Provider offers the customer an address prefix (subnet) for the LAN port and a single public address for the WAN port via DHCPv6. The customer uses this prefix to provide addresses for LAN side PCs using SLAAC or DHCP.

MSO topology changes need to accommodate events like node splits or load balancing events without requiring customer LAN renumbering. Some devices (e.g., older Linux machines) will not renumber via SLAAC/DHCPv6; such devices will keep old addresses until the valid/preferred lifetimes expire. This is generally an issue for commercial customers, and is less of a concern for most residential customers. MSOs are interested in a common approach to Prefix Stability and delegation to minimize impact to commercial customers.

There are two aspects to the problem

- Propagation - CMTS needs to learn the delegated prefix/route.
- Aggregation - MSOs need to determine the optimal aggregation point to maximize stability and minimize routing table sizes.

5.9.1 IPv6 Prefix Delegation

DHCPv6 offers Prefix Delegation (IA_PD), which allocates a range of addresses to a customer site. This is intended for network elements that behave as a router. The client requesting an IPv6 prefix is the "requesting router," and the

server that leases the IPv6 prefix is the "delegating router". The Requesting router sends a DHCPv6 Solicit message to obtain an IPv6 prefix and the Delegating router assigns an IPv6 prefix (for e.g., a /56). The CPE Router uses this prefix to assign subnets to its interfaces. RAs contain /64s from delegated prefix. CPE devices acquire addresses in the same range from DHCPv6 or SLAAC.

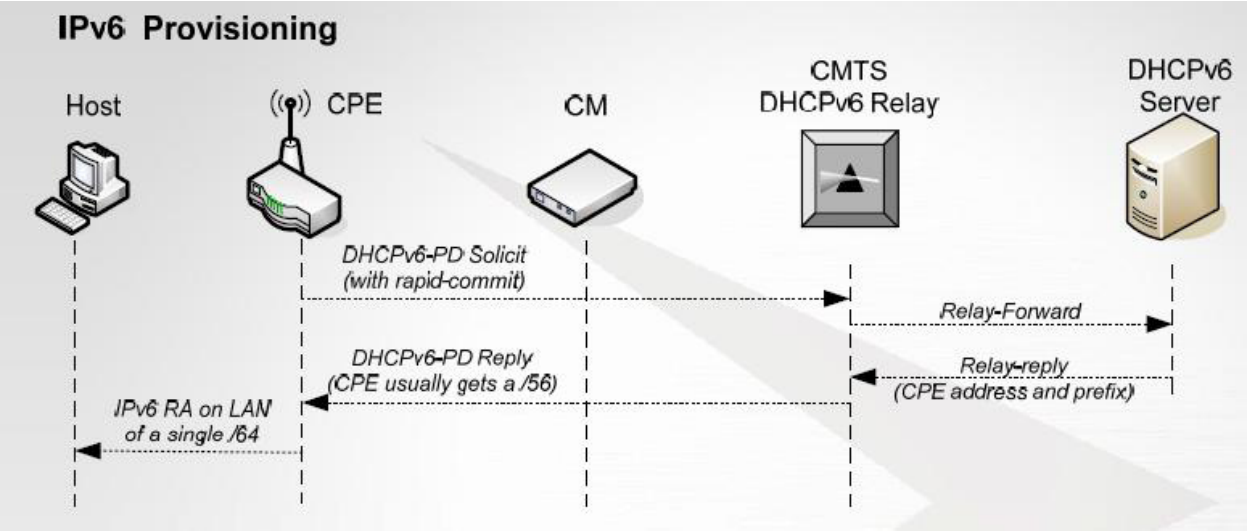

Figure 2 - IPv6 Prefix Delegation

5.9.2 Prefix Stability

Following a node split, a Home Gateway may be assigned a different IPv6 address. This use case describes how an operator can continue to delegate and route the same IPv6 prefix to the same customer, despite moving the customer to a different CMTS or CMTS downstream service group.

5.9.2.1 Prefix Assignment

The Home Gateway sends a DHCPv6 Solicit message. The Solicit message includes an IA_PD option to obtain its delegated IPv6 prefix and a client identifier option containing a DHCP Unique ID (DUID). The Home Gateway may optionally include its previously allocated prefix in the IA_PD option as a hint to the DHCP server. Based on the Home Gateway DUID and IA_PD, the DHCP server may assign the Home Gateway the same prefix, even if the gateway is connected to a different CMTS and obtains a different IPv6 address.

If, as part of routine maintenance, a Home Gateway is removed from one customer home and installed in another, the MSO must be able to clear the previously assigned prefix from the gateway.

5.9.2.2 Route Propagation

This section describes how the route to a prefix delegated to a Home Gateway can be injected into a provider network.

There are several different methods by which a prefix assigned to a Home Gateway can be installed in an MSO's headend routing table. These include the use of a routing protocol (e.g., RIPng) on the Home Gateway, through DHCPv6 snooping, through a Relay-Agent option exchanged between the DHCP server and CMTS, using BGP to exchange routing information, or through static provisioning.

If the Home Gateway is moved to a different CMTS during the node split, the original CMTS may not learn of the Home Gateway move for some time, and may continue advertising the prefix in its IGP updates, causing routing problems within the headend. This could leave the customer out of service until the prefix is cleared from the original CMTS. Possible solutions to the routing issue depend on the selected route injection method.

- If the Home Gateway injects its prefix via RIPng, it will advertise its prefix to the new CMTS as soon as it comes on-line following the node split. When it does not receive periodic updates, the original CMTS times out the prefix in a matter of minutes, depending on configured timers.
- If the CMTS learns of the prefix through DHCP snooping, it may not learn when the prefix moves to another CMTS during the node split. The operator would need to manually clear the entry from the original CMTS or wait for the original DHCP lease to expire.
- If the CMTS learns of the prefix through a relay agent option (DHCP Relay Agent Assignment Notification (RAAN) option) in a message from the DHCP server, it removes the prefix from its routing table in response to a message from the DHCP server notifying it of the change.
- If the CMTS learns of the prefix via a BGP advertisement from the DHCP server, it would receive an update when the lease expires or is updated. As mixing routing information with address assignment creates a layer violation, this is not a preferred solution.
- If the prefix assignment was configured statically, a technician would remove the prefix from the original CMTS and install it on the new one.

The best available solution is DHCPv6 snooping with enhancements to check for device reachability. This solution is further defined below.

5.9.2.3 DHCPv6 Snooping Solution

The CMTS acts as a DHCPv6 Relay Agent, observing all messages between CPEs and the DHCPv6 server. As such, the CMTS observes IA_PD assignments in DHCPv6 Relay messages and installs an entry for each IA_PD observed in its routing and forwarding tables ('DHCP snooping'). When installing an entry in the routing and forwarding tables for the observed IA_PD assignments, the CMTS maps the IA_PD to the CM transmitting the request. The CMTS purges the IA_PD entry and the route to the prefix upon IA_PD lease expiration.

Whenever the CMTS receives an IGP or BGP route addition for a route it has previously learned via DHCP snooping, it checks whether the CM associated with the route is online and appropriately retains or purges its existing route and mapping between IA_PD and CM. Effectively, the CMTS prefers 'snooped' routes for PD prefixes to those learned via dynamic routing protocols including BGP or any IGP.

From the packet forwarding perspective, the CMTS considers the CPE reachable as long as the lease time (valid lifetime) of the corresponding PD prefix has not expired at the CMTS, the corresponding CM is online, and the next-hop CPE address is resolved.

Some network configurations will allow CMTSs to advertise aggregate routes (e.g., multiple PDs). In such cases, the CMTS identifies the individual PDs associated with each CM before making any purge or add decisions as described above.

The CMTS implementation may also provide a mechanism to manually clear CPE delegated routes. This deletion could be based on a CM MAC address, IPv6 Prefix, or downstream interface. Such a command is useful in the case where a CMTS cannot always see the new route coming from another CMTS, for example if BGP route reflection is used.

5.9.2.4 Prefix Aggregation

Route aggregation offers routing table efficiency.

A hierarchical network design allows only summary routes to be exchanged. The Provider Edge (PE) Router delegates sub-prefixes to CMTSs and the CPE routers receive sub-prefixes based on the CMTS. This design poses challenges for prefix stability. In this case moving a customer to a new CMTS would require assigning a different prefix or injecting more specific routes.

Prefix stability is aided by aggregating at PE Router. This offers clients greater flexibility to move within a headend. This requires additional routes in the routing table and is not scalable to all customers. This is a viable option if limited to a smaller group of customers (e.g., commercial or residential-plus). This requires a provisioning system update to allow a prefix to be bound to multiple CMTSs.

The recommendation is to aggregate the IPv6 prefixes at the edge router to allow for Prefix stability.

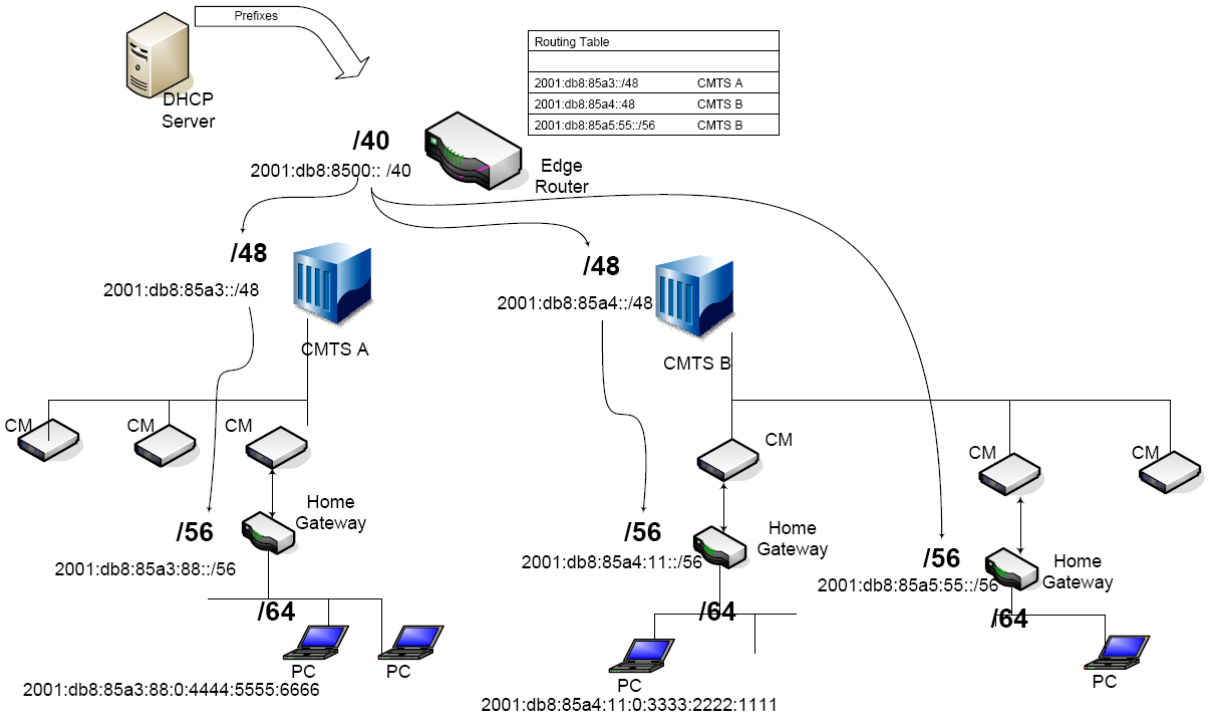

Figure 3 - IPv6 Aggregation Example

5.10 Deferred Use Cases

This section includes use cases that were discussed by the MSO IPv6 Working Group, but deferred until such time as the IETF completes work on some items and MSOs gain additional IPv6 experience.

5.10.1 Prefix Sub-Delegation

This use case describes how a Home Gateway can sub-delegate an assigned prefix to a customer-owned router connected behind the Home Gateway device. There are two methods for sub-delegating the prefix: manually and automatically. This use case addresses automatic sub-delegation.

An eRouter is not currently required to support sub-delegation of prefixes to connected routers. Thus, this use case describes a potential enhancement for a Home Gateway. One potential mechanism for sub-delegating the prefix is described below.

1. The Home Gateway divides the subnetting bits in its delegated prefix by two when determining prefixes for delegation. For example, if a Home Gateway is delegated a /56, it would sub-delegate /60s.
2. The Home Gateway assigns a unique /64 from its delegated prefix to each of its customer facing interfaces. To allow for efficient subnetting, the Home Gateway should begin assigning /64s from the lowest-available sub-prefix. If it runs out of addresses in its first sub-prefix, the Home Gateway may use additional sub-prefixes, as necessary.
3. Attached customer routers request prefix delegation using [RFC3315] and [RFC3633].
4. The Home Gateway delegates a sub-prefix in response to the customer router request from the remaining block of sub-prefixes.

The Home Gateway installs a route in its routing table for the delegated sub-prefix.

Prefix sub-delegation was re-visited in the Advanced Home Networking use case, documented in Section 13.

5.10.2 Reverse DNS

This use case describes how an IPv6 CPE device behind a Home Gateway registers its address with a DNS server, and how the DNS server offers AAAA and PTR resolution on behalf of the CPE.

The CPE device can be provisioned using SLAAC or DHCP. Depending on the provisioning method, operators have four different options for reverse DNS resolution. The four options include:

1. Provide no support for customer reverse address resolution
2. Dynamically generate PTR records on demand
3. Generate 'wildcard' PTR records on the DNS server
4. Use dynamic DNS on the Home Gateway to update the DNS server

CPE devices provisioned using SLAAC can use options 1-3. In addition to the options available to support SLAAC-provisioned CPE devices, MSOs can also use Dynamic DNS to resolve customer addresses for DHCP-provided hosts.

While it is acceptable to not provide support for reverse address resolution (option 1), the IETF is discussing options for Reverse DNS service, and this issue should be revisited once the IETF completes work.

6 VOICE USE CASES

6.1 EDVA Provisioning Use Cases

This scenario describes two different provisioning scenarios: the basic IPv6-only provisioning and the dual-stack provisioning of an Embedded Digital Voice Adaptor (E-DVA) device in a PacketCable Network.

6.1.1 EDVA IPv6 Provisioning

E-DVA Provisioning involves the provisioning of both the eCM and the eUE ('eDVA' here). The PacketCable framework requires that an eUE be provisioned either in IPv4 or IPv6 modes, a choice obtained by the eCM component as part of its IP configuration. The eUE attempts provisioning with the provided parameters and once successfully provisioned, it is provided with the configuration necessary to participate in a PacketCable network.

The eCM provisioning is accomplished using the procedures specified by DOCSIS and eDOCSIS, with additional enhancements. An eCM uses the DOCSIS DHCP process to get the eCM configuration information with certain modifications, such as obtaining PacketCable eUE DHCP Server information.

PacketCable defines three provisioning flows for the eUE: Secure, Basic and Hybrid, which essentially follow the same process as far as IP provisioning is concerned. Once the eCM has completed provisioning, the eUE is initialized using the eUE DHCP Server Address obtained during eCM provisioning. An eCM contained within an E-DVA passes on information obtained in its DHCP process to the eUE component to determine the IP addressing Mode Preference for the E-DVA, i.e., depending on the addressing mode, the eUE proceeds to provision in IPv4 or IPv6 modes. The eUE acquires the ToD from the eCM. In the eUE IPv6 Secure Provisioning Flow, the eUE constructs a link-local address for its management interface according to [RFC4862]. After successful link-local address assignment is accomplished, the eUE performs discovery of the default and neighboring routers by sending Router Solicitation (RS) messages per [RFC4861]. Once the eUE has completed router discovery, it follows the steps shown in the sequence diagram in Figure 4 which explains the remaining steps in the secure IPv6 provisioning flow. All of these flows use IPv6 and work with back-end servers that support IPv6.

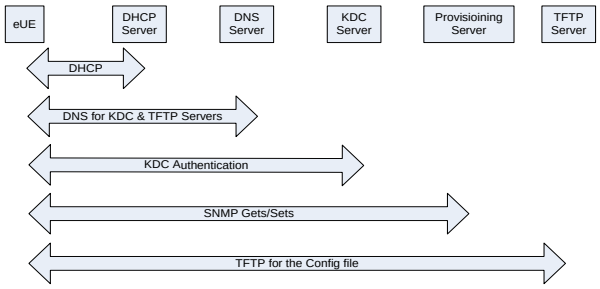

Figure 4 - eDVA Provisioning Sequence Diagram

6.1.2 EDVA Dual-Stack (IPv4 and IPv6) Provisioning

This use case describes the IPv4 and IPv6 dual-stack provisioning for an E-DVA device.

E-DVA Provisioning follows the process described in Section 6.1.1. In addition, for dual-stack operation, it performs DHCP for the second address family, thus acquiring both an IPv4 and IPv6 address. The eUE initializes after the eCM has completed provisioning.

The E-DVA performs both DHCPv4 and DHCPv6 to acquire addresses from each family. A dual-stack E-DVA must be capable of identifying one address family to be "preferred". The E-DVA will use its "preferred" address for steps in the provisioning process that should not be replicated, i.e., all signaling and configuration steps after address acquisition (i.e., DHCP). The preferred address flow will follow the normal flows defined currently in the PC specs while the secondary address flow will include only acquisition of the IP address.

6.1.3 eUE SIP Registration

The E-DVA Residential SIP Telephony (RST) client needs to perform SIP registration with the IMS core to enable the voice functionality of the device.

In order for the E-DVA to register with the IMS Core, it learns the IP address or Fully-Qualified Domain Name (FQDN) of the Proxy Call Session Control Function (P-CSCF) server from its configuration file or SNMP. A dual-stack E-DVA will only register using one address family. It will use the P-CSCF address to determine which address family to use. If the E-DVA learns a P-CSCF address in each address family, it will use its "preferred" address to determine whether to use IPv4 or IPv6 for registration.

Once the E-DVA completes this registration process, it is capable of placing a call. In Dual-Stack Operation Mode, the media can be carried over either IPv6 or IPv4. The signaling only uses the chosen IP protocol with which it registered.

6.1.4 Manage an IPv6 E-DVA using SNMP

This use case involves managing an E-DVA that was provisioned in IPv6 mode using SNMP.

An IPv6-enabled E-DVA can be managed from an NMS using SNMP by exchanging SNMP messages directly with the E-DVA. In addition, the E-DVA may also send syslog messages to an IPv6-enabled syslog server. When certain events occur or thresholds are crossed, the E-DVA sends an SNMP trap message and/or syslog message to the appropriate server using IPv6. The E-DVA acquires the address of the appropriate syslog server(s) during provisioning through the DHCP advertise/reply messages. Traps need to be specifically provisioned via the config file; otherwise the E-DVA will only send syslog messages. The trap receiver address is provided via TLV 38 in the config file.

6.2 Basic Dual-Stack Interworking Use Cases

This use case defines the IPv4/IPv6 Interworking for a hypothetical dual-stack E-DVA. Dual-stack operational E-DVAs are not currently supported in PacketCable specifications.

As a note for all the use cases below, the IMS Core includes all the x-CSCF functionality.

6.2.1 Dual-Stack E-DVA attached to IPv4-only Network

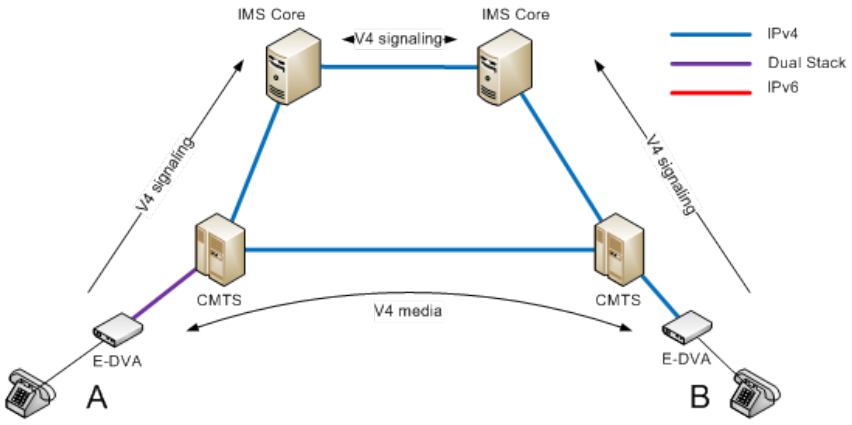

Figure 5 - Dual-Stack EDVA, IPv4 Network

Setup: The MSO attaches the dual-stack E-DVA 'A' to an IPv4-only network. The far end E-DVA 'B' is attached to the network using only IPv4. Both the IMS Cores are attached to the network using only IPv4.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in Dual-stack mode and completes SIP registration using IPv4. E-DVA 'B' is provisioned in IPv4 mode, and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv4. The P-CSCF forwards the INVITE over IPv4 as well. E-DVA 'B' replies with the 200-OK message over IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and alternate address is IPv6. E-DVA 'B' replies that it can support media on IPv4. So since both E-DVAs indicated a preference for IPv4, E-DVAs 'A' and 'B' establish an IPv4 media path.

6.2.2 E-DVA attached to Dual-Stack P-CSCF calls E-DVA attached to IPv4-only P-CSCF

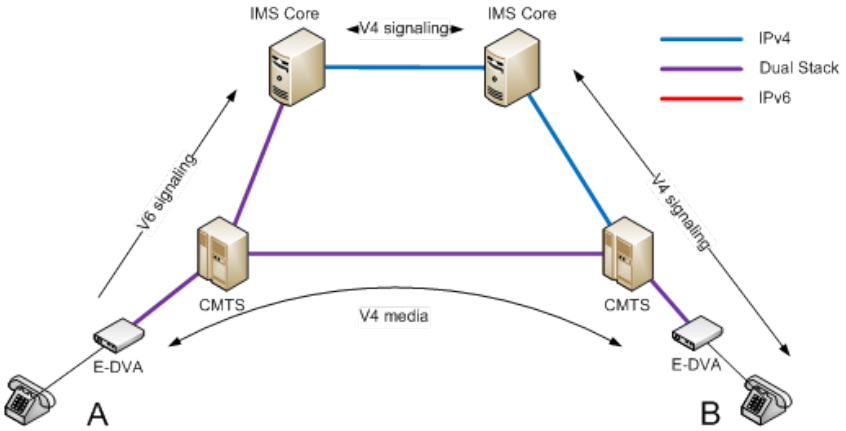

Figure 6 - E-DVA attached to Dual-Stack P-CSCF calls E-DVA attached to IPv4-only P-CSCF

Setup: The MSO attaches the dual-stack E-DVA 'A' to a dual-stack network. The far end E-DVA 'B' is also attached to a dual-stack network. The near end IMS Core also supports dual-stack. The far end IMS Core only supports IPv4.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in Dual-stack mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in IPv4 mode, and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The first P-CSCF performs interworking between the protocols and forwards the INVITE over IPv4. E-DVA 'B' replies with the 200-OK message over IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and alternate address is IPv6. B replies that it can support media on IPv4 and IPv6. Since both E-DVAs indicated a preference for IPv4, E-DVAs 'A' and 'B' establish an IPv4 media path.

6.2.3 Dual-Stack E-DVA calls IPv4-only E-DVA attached to Dual-Stack Network

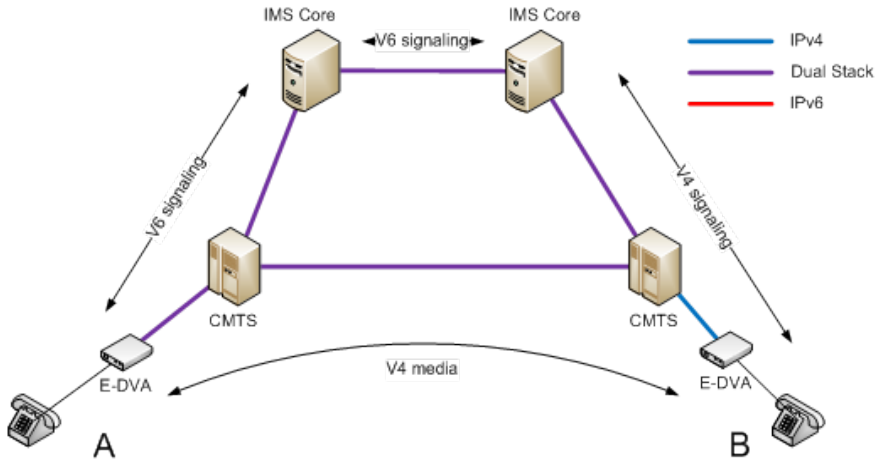

Figure 7 - Dual-Stack E-DVA calls IPv4-only E-DVA attached to Dual-Stack Network

Setup: The MSO attaches the dual-stack E-DVA 'A' to a dual-stack network. The far end 'B' E-DVA supports only IPv4 and is attached to the network as an IPv4 E-DVA. The far and near end IMS Cores both support dual-stack.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in Dual-stack mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in IPv4 mode, and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The second P-CSCF performs interworking between the protocols and forwards the INVITE over IPv4. E-DVA 'B' replies with the 200-OK message over IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and the alternate address is IPv6. 'B' replies that it can support media on IPv4. Since both E-DVAs indicated a preference for IPv4, E-DVAs 'A' and 'B' set up an IPv4 media path.

6.2.4 Dual-Stack E-DVA calls IPv4 E-DVA over IPv6 Network

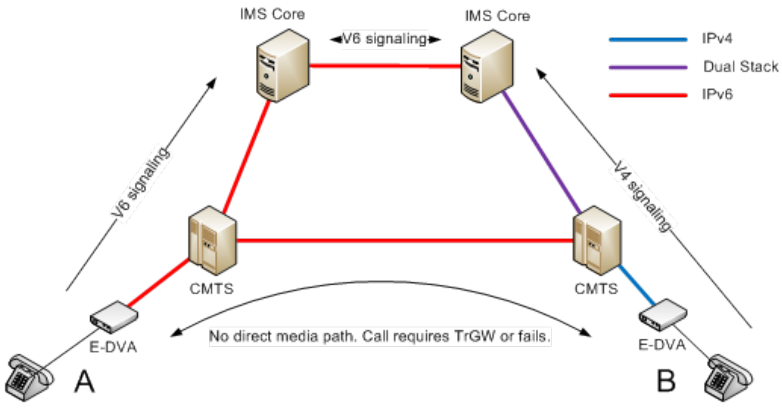

Figure 8 - Dual-Stack E-DVA calls IPv4 E-DVA over IPv6 Network

Setup: The MSO attaches the dual-stack E-DVA 'A' to an IPv6-only network. The far end 'B' E-DVA supports only IPv4 and is attached to the network as an IPv4 E-DVA. The far and near end IMS Cores both support dual-stack.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The second P-CSCF performs interworking between the protocols and forwards the INVITE over IPv4. E-DVA 'B' replies with the 200-OK message over IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. E-DVA 'B' rejects this proposal because it does not have an IPv6 address. Therefore, since both E-DVAs indicate support for different protocol families, E-DVAs 'A' and 'B' are unable to set up a media path. The call could be completed if the MSO installs a Translation Gateway (TrGW) to perform media address family translation.

Conclusion: The call fails unless a TrGW is available for media path interworking.

6.2.5 E-DVAs in Dual-Stack Regions connect across an IPv4-only Core

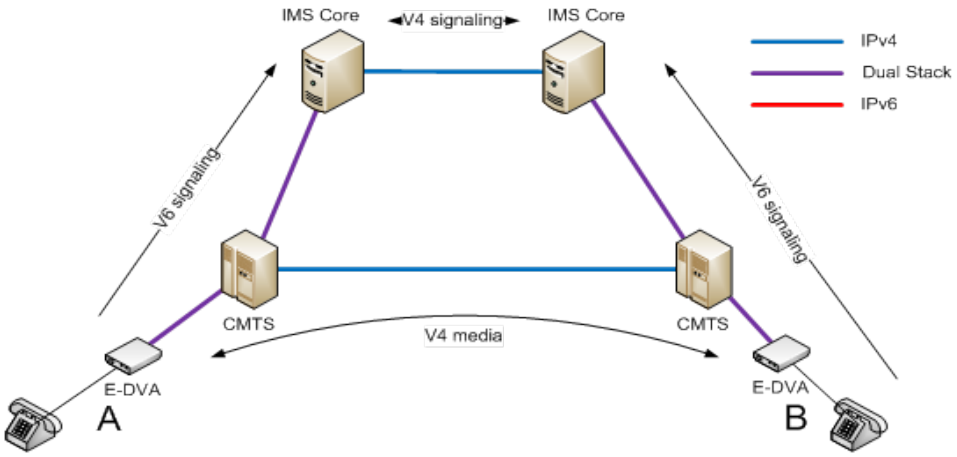

Figure 9 - E-DVAs in Dual-Stack Regions Connect across an IPv4-only Core

Setup: The MSO attaches the dual-stack E-DVA 'A' to a dual-stack regional network. The far end E-DVA 'B' also supports dual-stack and is attached to the network as a dual-stack E-DVA. The network core only supports IPv4. The far and near end IMS Cores both support dual-stack.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in Dual-stack mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in Dual-stack mode and completes SIP registration using IPv6.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The first P-CSCF performs protocol interworking and forwards the INVITE over IPv4. The second P-CSCF performs interworking between the protocols again and forwards the INVITE over IPv6. E-DVA 'B' replies with the 200-OK message using IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and the alternate address is IPv6. 'B' replies that it can support media on IPv4 and IPv6. Since both E-DVAs indicated a preference for IPv4, E-DVAs 'A' and 'B' set up an IPv4 media path.

6.2.6 Dual-Stack E-DVAs place a Call over a Dual-Stack Network

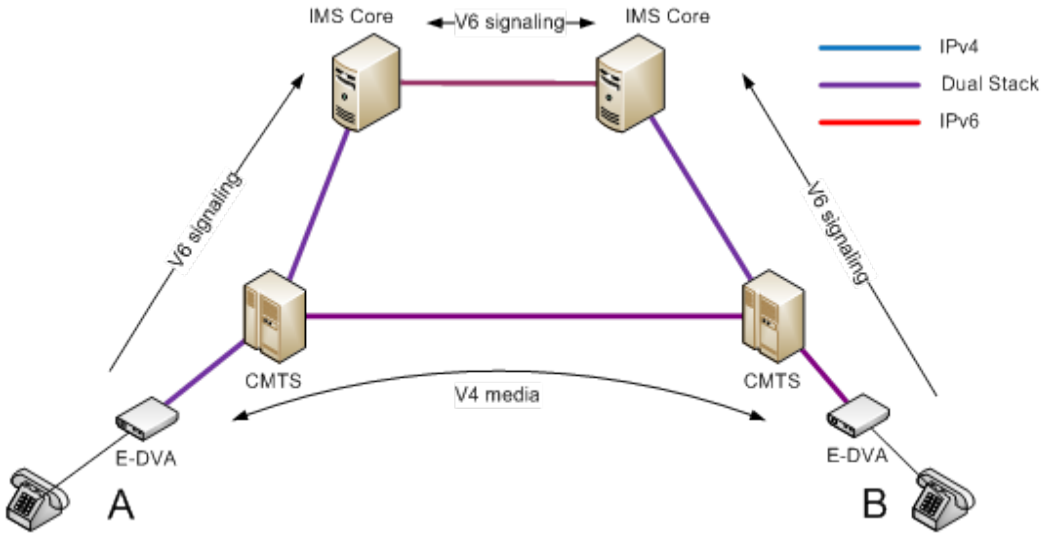

Figure 10 - Dual-Stack E-DVAs Place a Call over a Dual-Stack Network

Setup: The MSO attaches the dual-stack E-DVA 'A' to a dual-stack regional network. The far end E-DVA 'B' also supports dual-stack and is attached to the network as a dual-stack E-DVA. The network core supports dual-stack. The far and near end IMS Cores both support dual-stack.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in Dual-stack mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in Dual-stack mode and completes SIP registration using IPv6.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The P-CSCF forwards the INVITE over IPv6. E-DVA 'B' replies with the 200-OK message using IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and the alternate address is IPv6. 'B' replies that it can support media on IPv4 and IPv6. Since both E-DVAs indicated a preference for IPv4 E-DVAs, 'A' and 'B' establish an IPv4 media path.

6.2.7 E-DVA on an IPv6-only Network Calls another Dual-Stack E-DVA

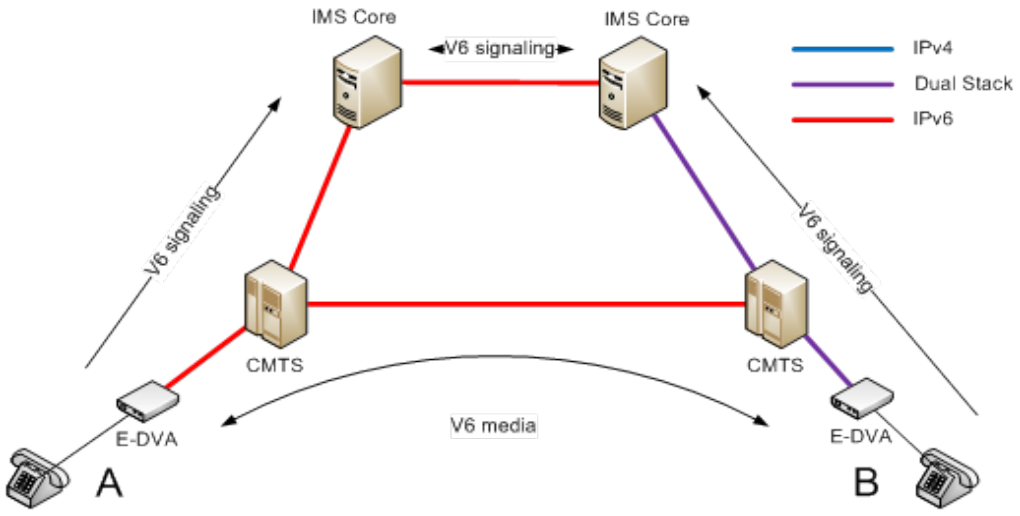

Figure 11 - E-DVA on an IPv6-only Network Calls another Dual-Stack E-DVA

Setup: The MSO attaches the dual-stack E-DVA 'A' to an IPv6-only network. The far end E-DVA 'B' supports dual-stack and is attached to the network as a dual-stack E-DVA. The network core supports dual-stack. The far and near end IMS Cores both support dual-stack.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in Dual-stack mode and completes SIP registration using IPv6.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The second P-CSCF performs interworking between the protocols and forwards the INVITE over IPv4. E-DVA 'B' replies with the 200-OK message using IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. 'B' replies that it can do media forwarding using both IPv4 and IPv6. Since both E-DVAs indicated a preference for IPv6, E-DVAs 'A' and 'B' establish an IPv6 media path.

6.2.8 Dual-Stack Interworking Summary

Although signaling is done over a single version of IP with the IMS core, a dual-stack UE must be able to navigate all of the media interworking scenarios listed in Table 1. All versions of PacketCable UE-2 are supported in the following scenarios.

Table 1 - Dual-Stack Media Interworking Scenarios

UE-1	Network-1	Network-2	UE-2
Dual-Stack	Dual-Stack	Dual-Stack	Dual-Stack
Dual-Stack	Dual-Stack	Dual-Stack	IPv6-Only
Dual-Stack	Dual-Stack	Dual-Stack	IPv4-Only
Dual-Stack	Dual-Stack	IPv6-Only	Dual-Stack
Dual-Stack	Dual-Stack	IPv6-Only	IPv6-Only
Dual-Stack	Dual-Stack	IPv4-Only	Dual-Stack
Dual-Stack	Dual-Stack	IPv4-Only	IPv4-Only

UE-1	Network-1	Network-2	UE-2
Dual-Stack	IPv6-Only	Dual-Stack	Dual-Stack
Dual-Stack	IPv6-Only	Dual-Stack	IPv6-Only
Dual-Stack	IPv6-Only	IPv6-Only	Dual-Stack
Dual-Stack	IPv6-Only	IPv6-Only	IPv6-Only
Dual-Stack	IPv4-Only	Dual-Stack	Dual-Stack
Dual-Stack	IPv4-Only	Dual-Stack	IPv4-Only
Dual-Stack	IPv4-Only	IPv4-Only	Dual-Stack
Dual-Stack	IPv4-Only	IPv4-Only	IPv4-Only
NOTE: Scenarios not listed here may require a Translation Gateway to perform IPv4/IPv6 media interworking in order to function.			

6.3 PacketCable 2.0- PacketCable 1.5 Interworking

These use cases define IPv4/IPv6 Interworking for a hypothetical PacketCable 2.0 dual-stack E-DVA. Dual-stack operational E-DVAs are not currently supported in PacketCable specifications.

6.3.1 Dual-Stack 2.0 E-DVA Registered using IPv4 calls IPv4 1.5 E-MTA

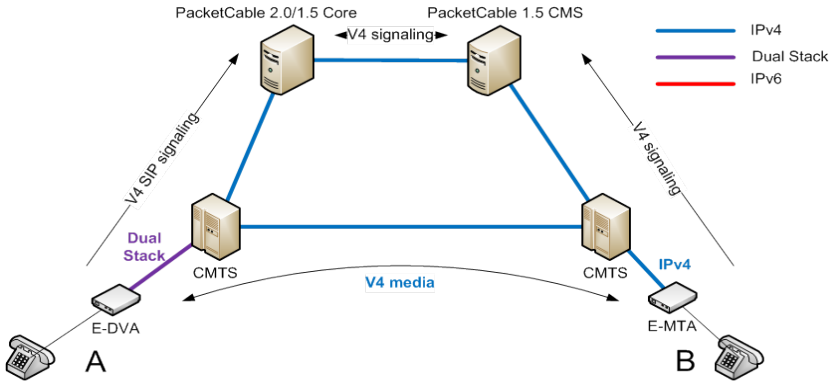

Figure 12 - Dual-Stack 2.0 E-DVA Registered using IPv4 calls IPv4 1.5 E-MTA

Setup: The MSO attaches the dual-stack E-DVA 'A' to an IPv4-only PacketCable 2.0 Core. The far end E-MTA 'B' supports IPv4 only and signals to the PacketCable 1.5 CMS using only IPv4. The network core supports IPv4 only.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in dual-stack mode and completes SIP registration using IPv4.

E-MTA Provisioning/SIP Registration: 'B' is provisioned in IPv4 mode and completes registration with the CMS using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-MTA 'B' over IPv4. The IMS Core performs PacketCable 2.0/1.5 Interworking, and sends the call setup message to E-MTA 'B' via the PacketCable 1.5 CMS over IPv4. E-MTA 'B' replies with the 200-OK message using IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and the alternate is IPv6. 'B' replies that it can do media forwarding using IPv4. Since both endpoints can support IPv4, E-DVA 'A' and E-MTA 'B' establish an IPv4 media path.

6.3.2 Dual-Stack 2.0 E-DVA Registered using IPv6 calls IPv4 1.5 E-MTA

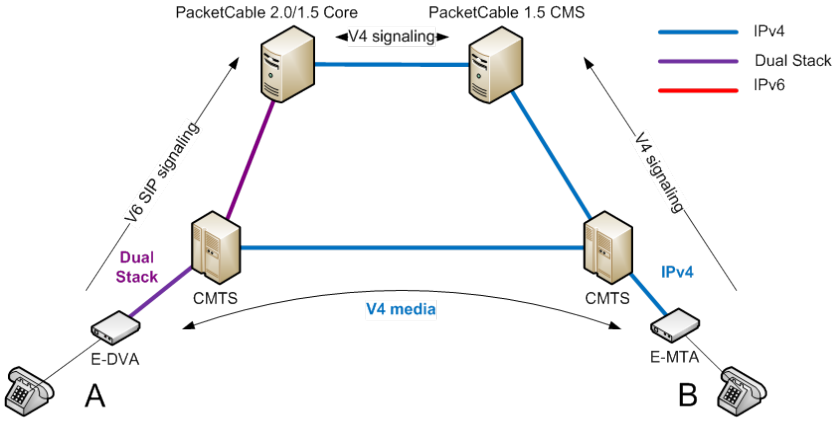

Figure 13 - Dual-Stack 2.0 E-DVA Registered using IPv6 calls IPv4 1.5 E-MTA

Setup: The MSO attaches the dual-stack E-DVA 'A' to a dual-stack network and a dual-stack capable PacketCable 2.0 Core. The far end E-MTA 'B' supports IPv4 only and signals to the PacketCable 1.5 CMS using IPv4 only. The network core supports IPv4 only.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in dual-stack mode and completes SIP registration using IPv6.

E-MTA Provisioning/SIP Registration: 'B' is provisioned in IPv4 mode and completes registration with the CMS using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-MTA 'B' over IPv6. The IMS Core performs PacketCable 2.0/1.5 Interworking, and sends the call setup message to E-MTA 'B' via the PacketCable 1.5 CMS over IPv4. E-MTA 'B' replies with the 200-OK message using IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv4 and the alternate is IPv6. 'B' replies that it can do media forwarding using IPv4. Since both endpoints can support IPv4, 'A' and 'B' set up an IPv4 media path.

6.3.3 Single-stack IPv4 2.0 E-DVA calls IPv4 1.5 E-MTA

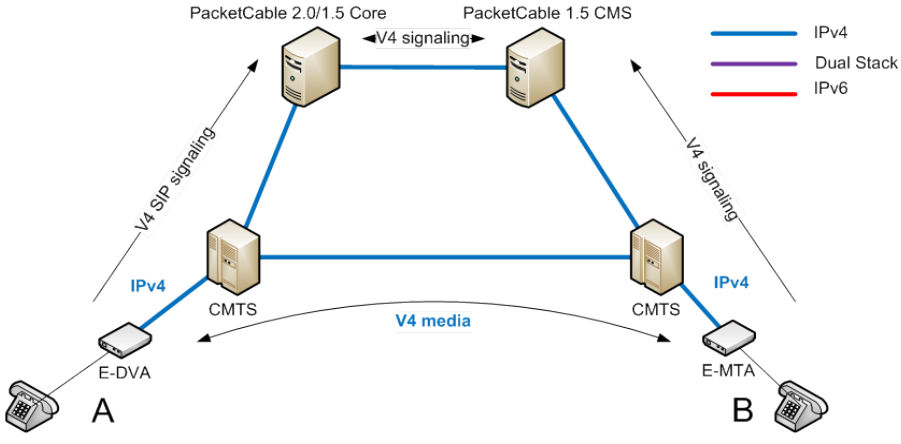

Figure 14 - Single-Stack IPv4 2.0 E-DVA calls IPv4 1.5 E-MTA

Setup: The MSO attaches the IPv4 E-DVA 'A' to an IPv4 network and an IPv4 only PacketCable 2.0 Core. The far end E-MTA 'B' supports IPv4 only and so signals to the PacketCable 1.5 CMS using only IPv4. The network core supports IPv4 only.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4.

E-MTA Provisioning/SIP Registration: 'B' is provisioned in IPv4 mode and completes registration with the CMS using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-MTA 'B' over IPv4. The IMS Core performs PacketCable 2.0/1.5 Interworking, and sends the call setup message to E-MTA 'B' via the PacketCable 1.5 CMS over IPv4. E-MTA 'B' replies with the 200-OK message using IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv4. E-MTA 'B' replies that it can do media forwarding using IPv4. Since both endpoints can support IPv4 E-DVA 'A' and E-MTA 'B' set up an IPv4 media path.

6.3.4 Single-Stack IPv6 2.0 E-DVA calls IPv4 1.5 E-MTA

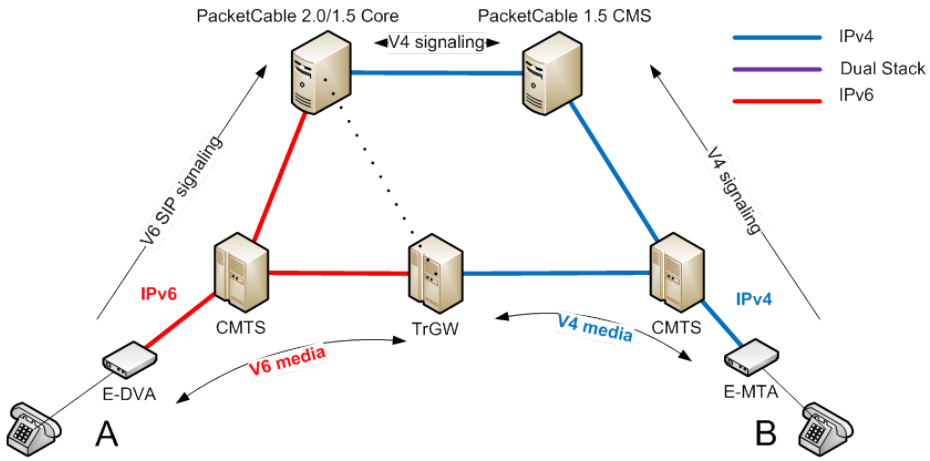

Figure 15 - Single-Stack IPv6 2.0 E-DVA calls IPv4 1.5 E-MTA

Setup: The MSO attaches the dual-stack E-DVA 'A' to an IPv6 network and a dual-stack capable PacketCable 2.0 Core. The far end E-MTA 'B' supports IPv4 only and signals to the PacketCable 1.5 CMS using only IPv4. The network core supports IPv4 only. A TrGW performs media path interworking.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6.

E-MTA Provisioning/SIP Registration: 'B' is provisioned in IPv4 mode and completes registration with the CMS using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-MTA 'B' over IPv6. The IMS Core performs PacketCable 2.0/1.5 Interworking, and sends the call setup message to E-MTA 'B' via the PacketCable 1.5 CMS over IPv4. E-MTA 'B' replies with the 200-OK message using IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. 'B' replies with an error since it does not support IPv6. Since there is not a common media path, PC 2.0 Core directs E-DVA 'A' to set up IPv6 media path to the TrGW and E-MTA 'B' to set up IPv4 media path to the TrGW. So the TrGW translates the media between IPv4 and IPv6 and enables the call to go through.

6.4 PacketCable 2.0 IPv4/IPv6 Interworking

These Single-Stack Interworking use cases describe the PacketCable 2.0 IPv4/IPv6 interworking available today.

6.4.1 IPv6 E-DVA calls IPv4 E-DVA

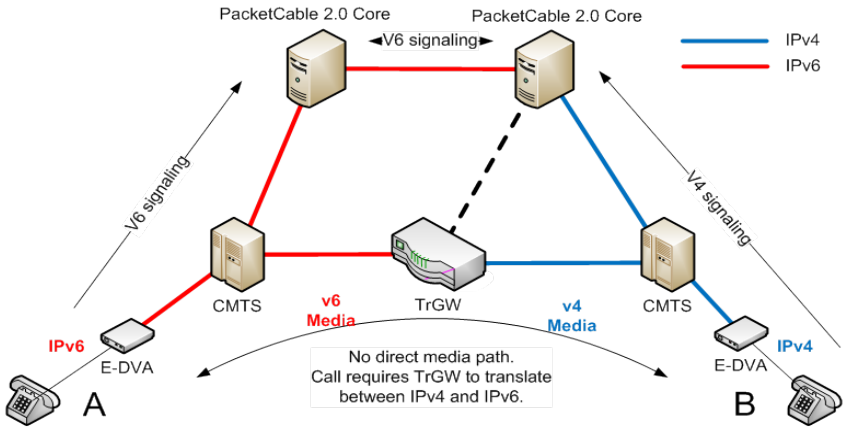

Figure 16 - IPv6 E-DVA calls IPv4 E-DVA

Setup: The MSO attaches the IPv6 E-DVA 'A' to an IPv6 only network. The far end E-DVA 'B' supports IPv4 and is attached to the network as an IPv4 E-DVA. The network core supports single stack but includes a TrGW to translate protocols. The far-end IMS Core supports translation between IPv4 and IPv6.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv6. The receiving PC 2.0 core (P-CSCF) performs interworking between the protocols and forwards the INVITE over IPv4. E-DVA 'B' replies with the 200-OK message using IPv4.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. The receiving Core realizes that E-DVA 'B' does not support IPv6, so directs E-DVA 'A' to send media to the TrGW over IPv6 and 'B' to send media to the TrGW over IPv4. The TrGW translates the media between IPv4 and IPv6 and enables the call to go through.

6.4.2 IPv4 E-DVA calls IPv6 E-DVA

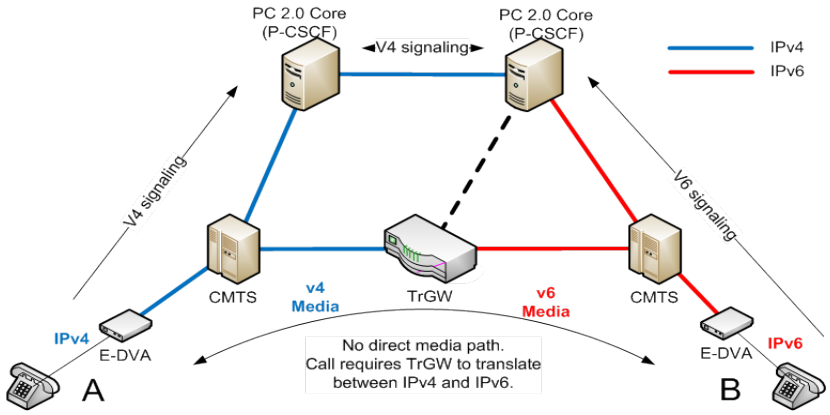

Figure 17 - IPv4 E-DVA calls IPv6 E-DVA

Setup: The MSO attaches the IPv4 E-DVA 'A' to an IPv4 only network/PC 2.0 core. The far end E-DVA 'B' supports IPv6 and so is attached to the network as an IPv6 E-DVA. The network core supports single stack but includes a TrGW to translate protocols. The far-end IMS Core supports translation between IPv4 and IPv6.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4. E-DVA 'B' is provisioned in IPv6 mode and completes SIP registration using IPv6.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv4. The receiving PC 2.0 core (P-CSCF) performs interworking between the protocols and forwards the INVITE over IPv6. E-DVA 'B' replies with the 200-OK message using IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv4. The receiving Core realizes that E-DVA 'B' does not support IPv4, so directs E-DVA 'A' to send media to the TrGW over IPv4 and 'B' to send media to the TrGW over IPv6. The TrGW translates the media between IPv4 and IPv6 and enables the call to go through.

6.4.3 IPv6 E-DVA calls Public Switched Telephone Network (PSTN)

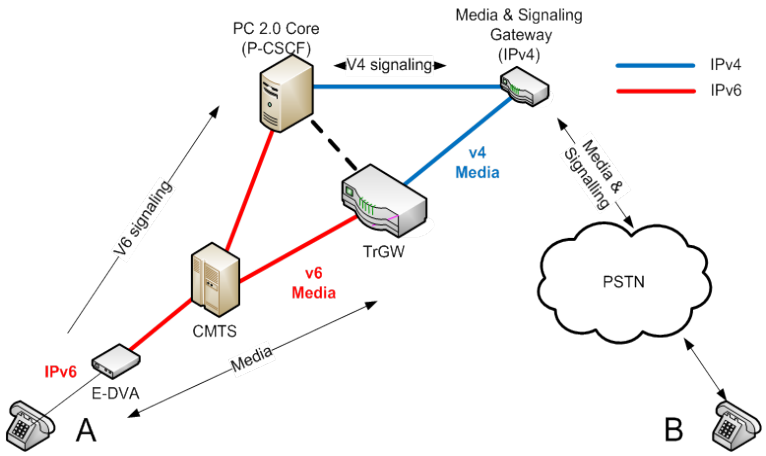

Figure 18 - IPv6 E-DVA calls PSTN

Setup: The MSO attaches the IPv6 E-DVA 'A' to an IPv6-only network. The far end phone 'B' is attached to the network over the PSTN. The network core supports single stack but includes a TrGW to translate protocols.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6. 'B' is registered with the PSTN.

Signaling: E-DVA 'A' sends the SIP INVITE message towards 'B' over IPv6. The PC 2.0 core (P-CSCF) performs interworking between the protocols and forwards the INVITE over IPv4 to the PSTN Media and Signaling Gateway.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. The PC 2.0 Core realizes that the PSTN gateway does not support IPv6, so directs 'A' to send media to the TrGW over IPv6, and the Gateway to send media to the TrGW over IPv4. So the TrGW translates the media between IPv4 and IPv6 and enables the call to go through. 'A' and 'B' talk across networks using the PSTN Media and Signaling Gateway.

6.4.4 IPv4 to IPv4 E-DVA over an IPv6 network

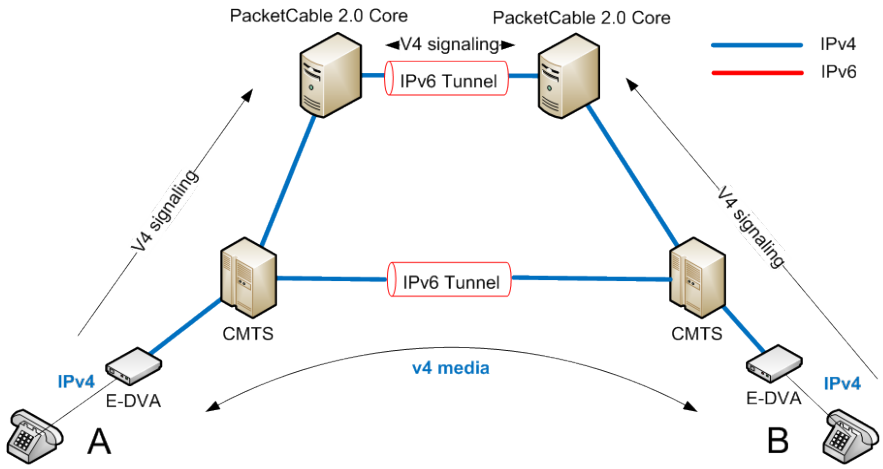

Figure 19 - IPv4 to IPv4 E-DVA over an IPv6 network

Setup: The MSO attaches the IPv4 E-DVA 'A' to an IPv4-only network/PC 2.0 core. The far end E-DVA 'B' supports IPv4 and is attached to the network as an IPv4 E-DVA. The network core supports IPv6 only and includes a tunneling capability between the two PC 2.0 Cores.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4. E-DVA 'B' is provisioned in IPv6/4 mode and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message towards E-DVA 'B' over IPv4. The PC 2.0 core (P-CSCF) realizes that the receiving PC 2.0 Core can be reached only through an IPv6 Tunnel that can carry the IPv4 payload within the tunnel. The INVITE traverses an IPv6 tunnel to reach E-DVA 'B'. E-DVA 'B' replies with the 200-OK message using IPv4, which also traverses the tunnel.

Media: E-DVA 'A' indicates that the primary address for media is IPv4. E-DVA 'B' responds that it can support media on IPv4. The path gets setup with the use of another IPv6 tunnel in between the endpoints. Here the Media uses IPv4, but traverses an IPv6 tunnel.

6.5 PacketCable 2.0 Conferencing

Two use cases describe PacketCable 2.0 conferencing between IPv4-IPv6 endpoints.

6.5.1 IPv4/IPv6 Conferencing with a Conferencing Server that supports IPv4/IPv6

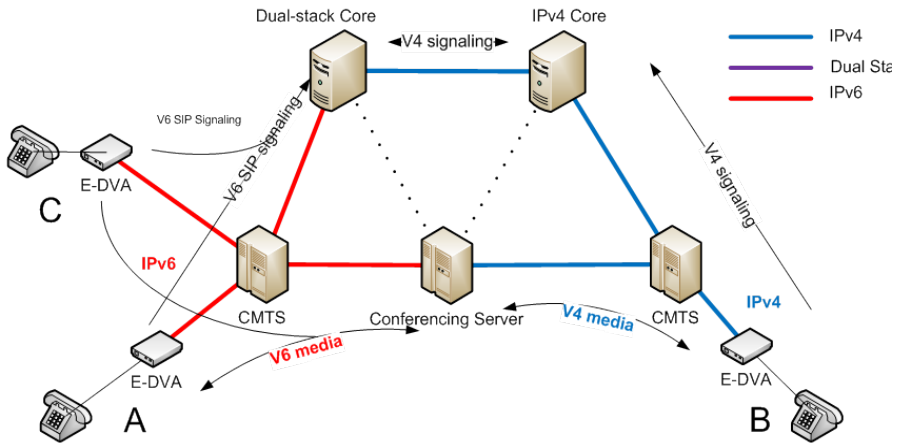

Figure 20 - IPv4/IPv6 Conferencing with a Conferencing Server that supports IPv4/IPv6

Setup: The MSO attaches an IPv6 E-DVA 'A' to an IPv6-only network. The far end E-DVA 'B' supports IPv4 and is attached to the network as an IPv4 E-DVA. The near end IMS Core supports dual-stack, the far end IMS core is IPv4 only. 'C' is an IPv6 EDVA that is attached to the IPv6 network also.

E-DVA: 'A' (IPv6 E-DVA) sets up a three-way conference with 'C' (IPv6 E-DVA) and 'B' (IPv4 E-DVA). The conferencing server supports both IPv4 and IPv6.

E-DVA Provisioning/SIP Registration: E-DVA 'A' and 'C' are provisioned in IPv6 mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message to the IMS core. The IMS core in turn sends the INVITE towards endpoints E-DVAs 'B' and 'C' over IPv4 and IPv6, respectively. E-DVA 'B' replies with the 200-OK message using IPv4, and 'C' replies over IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. The IMS Core directs 'A' and 'C' to send traffic to the conferencing server over IPv6, and 'B' over IPv4. The conferencing server ties together the media streams from 'A', 'B', and 'C', and forwards the traffic using the appropriate protocol to all the endpoints.

6.5.2 IPv4/IPv6 Conferencing with an IPv4-only Conferencing Server

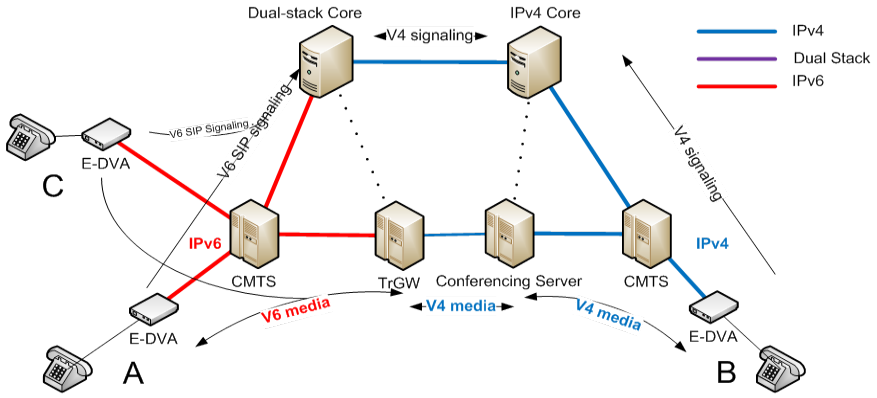

Figure 21 - IPv4/IPv6 Conferencing with an IPv4-only Conferencing Server

Setup: The MSO attaches an IPv6 E-DVA 'A' to an IPv6-only network. The far end E-DVA 'B' supports IPv4 and is attached to the network as an IPv4 E-DVA. The near end IMS Core supports dual-stack, the far end IMS core is IPv4 only. 'C' is an IPv6 EDVA and also attached to the IPv6 network.

E-DVA 'A' (IPv6 E-DVA) sets up a three-way conference with 'C' (IPv6 E-DVA) and 'B' (IPv4 E-DVA). The conferencing server supports only IPv4, and a TrGW is required to translate between IPv4 and IPv6.

E-DVA Provisioning/SIP Registration: E-DVA 'A' and 'C' are provisioned in IPv6 mode and completes SIP registration using IPv6. E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration using IPv4.

Signaling: E-DVA 'A' sends the SIP INVITE message to the IMS core over IPv6. The IMS core in turn sends the INVITE towards endpoints E-DVAs 'B' and 'C' over IPv4 and IPv6, respectively. E-DVA 'B' replies with the 200-OK message using IPv4 and 'C' replies over IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv6. The IMS Core realizes that the conferencing server only supports IPv4, therefore it directs 'A' and 'C' to send traffic to the TrGW over IPv6. The TrGW translates the incoming media from 'A' and 'C' to IPv4 media addresses, and sends the traffic to the conferencing server. The IMS Core directs 'B' to send media to the conferencing server over IPv4. The conferencing server ties together the media streams from 'A', 'B', and 'C', and forwards the traffic using the appropriate protocol to all the endpoints.

6.6 PacketCable Peering

This section describes PacketCable 2.0 IPv4/IPv6 peering across different MSO networks.

6.6.1 IPv4 E-DVA calls IPv6 E-DVA across MSO Domains

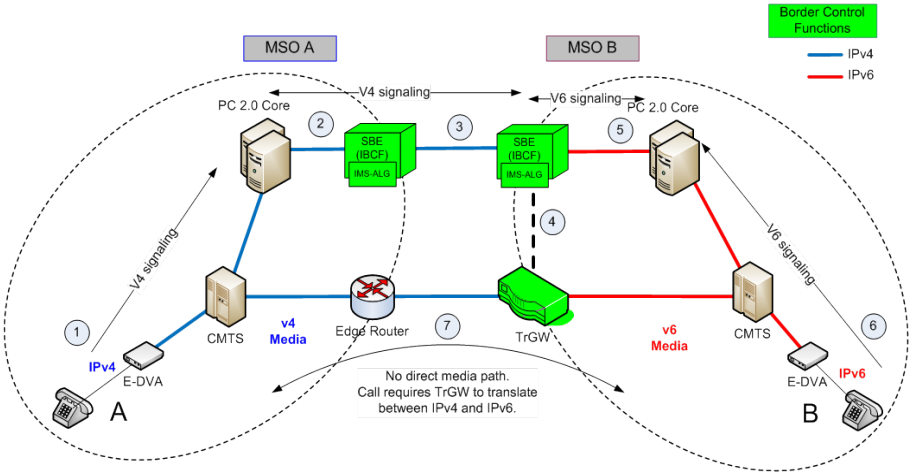

Figure 22 - IPv4 E-DVA calls IPv6 E-DVA across MSO Domains

Setup: The 'MSO A' has an IPv4 E-DVA 'A' attached to the PC 2.0 Core in that MSO's IPv4 network. The far end E-DVA 'B' in the 'MSO B's IPv6 network supports IPv6 and is attached to the network as an IPv6 E-DVA. Both MSO networks have Session Border Controllers (SBCs) at the edge of their networks. The IPv6 Network also has a TrGW at its edge.

IPv4 E-DVA on 'MSO A's network calls IPv6 E-DVA on 'MSO B's network.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4 with 'MSO A's Core. E-DVA 'B' is provisioned in IPv6 mode and completes SIP registration using IPv6 with 'MSO B's Core.

Signaling: E-DVA 'A' sends the SIP INVITE to 'MSO A's PacketCable 2.0 Core and SBE using IPv4. The SBE routes it to 'MSO B's SBE using IPv4. 'MSO B's SBE performs IPv4/IPv6 interworking and forwards the INVITE through 'MSO B's network using IPv6. E-DVA 'B' replies with the 200-OK message using IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv4. 'B' replies that it can only do IPv6. Since both sides support incompatible protocols, 'MSO B's SBE routes the call through the TrGW to interwork between IPv4 and IPv6.

6.6.2 IPv6 E-DVA calls IPv4 E-DVA across MSO Domains

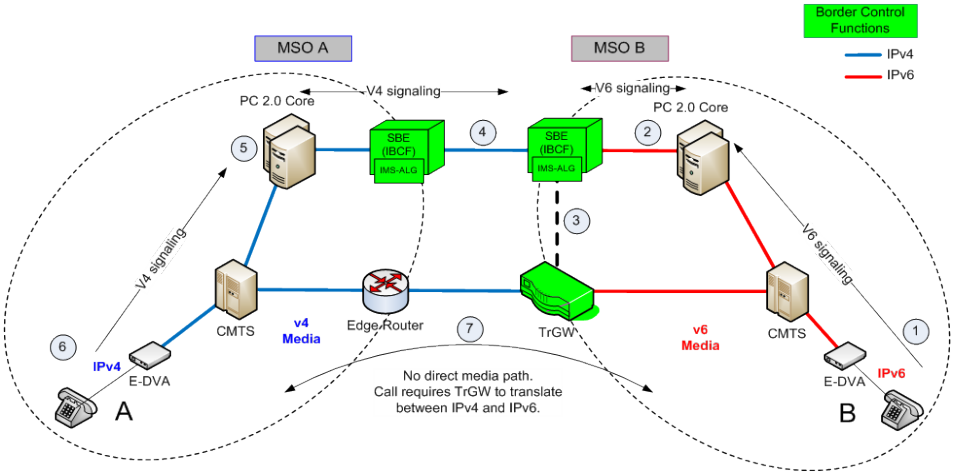

Figure 23 - IPv6 E-DVA calls IPv4 E-DVA across MSO Domains

Setup: The 'MSO A' has an IPv4 E-DVA 'A' attached to the PC 2.0 Core in that MSO's IPv4 network. The far end E-DVA 'B' in 'MSO B's IPv6 network supports IPv6 and is attached to the network as an IPv6 E-DVA. Both MSO networks have SBCs at the edge of their networks. The IPv6 Network also has a TrGW at its edge)

IPv6 E-DVA on 'MSO B's network calls IPv4 E-DVA on 'MSO A's network.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4 with 'MSO A's Core. E-DVA 'B' is provisioned in IPv6 mode and completes SIP registration using IPv6 with 'MSO B's Core.

Signaling: 'D' sends the SIP INVITE to 'MSO B's PacketCable 2.0 Core and SBE using IPv6. 'MSO B's SBE performs interworking and routes it to 'MSO A's SBE using IPv4. 'MSO A's SBE forwards the INVITE through 'MSO A's network using IPv4. E-DVA 'A' replies with the 200-OK message using IPv4.

Media: E-DVA 'B' indicates that the primary address for media is IPv6. E-DVA 'A' replies that it can only support IPv4. E-DVA 'B's SBE routes the call through the TrGW to interwork between IPv4 and IPv6.

6.6.3 Dual-Stack E-DVA calls Dual-Stack E-DVA over an IPv4 Interconnect

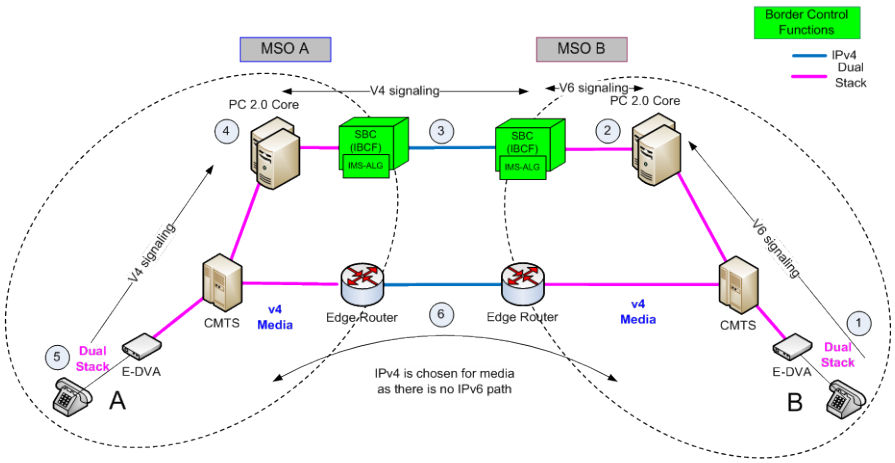

Figure 24 - Dual-Stack E-DVA calls Dual-Stack E-DVA over an IPv4 Interconnect

Setup: The 'MSO A' has a dual-stack E-DVA 'A' attached to the PC 2.0 Core in that MSO's dual-stack network. The far end E-DVA 'B' in 'MSO B's IPv6 network supports dual-stack and is also attached to the network as a dual-stack E-DVA. Both MSO networks have SBCs at their edge of the networks.

The Dual-stack E-DVA 'A' on 'MSO A's network calls the dual-stack E-DVA 'B' on 'MSO B's network.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in dual-stack mode and completes SIP registration using IPv4 with 'MSO A's Core. E-DVA 'B' is provisioned in dual-stack mode and completes SIP registration using IPv6 with 'MSO B's Core.

Signaling: E-DVA 'A' sends the SIP INVITE to 'MSO A's PacketCable 2.0 Core and SBE using IPv4. The SBE routes it to 'MSO B's SBE using IPv4. 'MSO B's SBE performs IPv4/IPv6 interworking and forwards the INVITE through 'MSO B's network using IPv6. E-DVA 'B' replies with the 200-OK message using IPv6.

Media: E-DVA 'A' indicates that the primary address for media is IPv4. 'B' replies with IPv4 as a primary and IPv6 as secondary. Since both E-DVAs indicated a preference for IPv4, both sides negotiate an IPv4 media path without requiring a TrGW.

6.6.4 IPv6 E-DVA calls IPv6 E-DVA over an IPv4 Interconnect

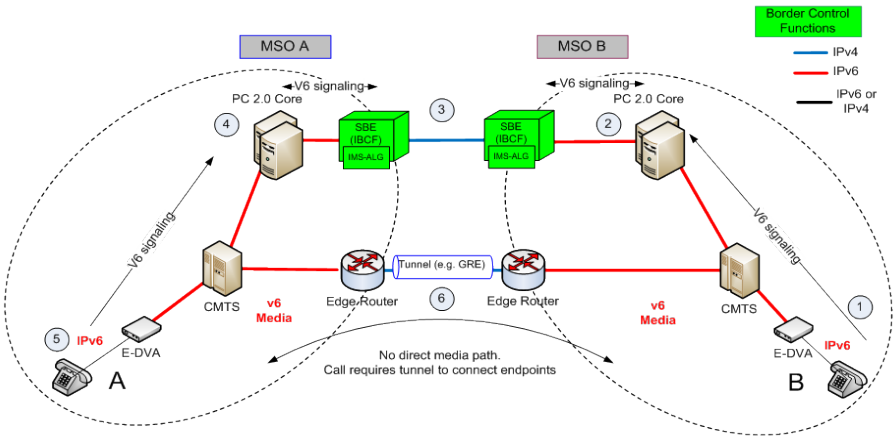

Figure 25 - IPv6 E-DVA calls IPv6 E-DVA over an IPv4 Interconnect

Setup: The 'MSO A' has an IP E-DVA 'A' attached to the PC 2.0 Core in that MSO's IPv6 network. The far end E-DVA 'B' in 'MSO B's IPv6 network supports IPv6 and is also attached to the network as an IPv6 E-DVA. Both MSO networks have SBCs at the edge of their networks. The two networks also have an IPv4 tunnel, which can carry IPv6 traffic between the two peering networks.

The IPv6 E-DVA 'B' on 'MSO B's network calls IPv6 E-DVA 'A' on 'MSO A's network.

E-DVA Provisioning/SIP Registration: E-DVA 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6 with 'MSO A's Core. E-DVA 'B' is provisioned in IPv6 mode and completes SIP registration using IPv6 with 'MSO B's Core.

Signaling: E-DVA 'B' sends the SIP INVITE to 'MSO B's PacketCable 2.0 Core and SBE using IPv6. 'MSO B's SBE performs IPv4/IPv6 interworking and routes it to 'MSO A's SBE using IPv4. 'MSO A's SBE performs IPv4/IPv6 interworking and forwards the INVITE through 'MSO A's network using IPv6. E-DVA 'A' replies with the 200-OK message using IPv6.

Media: E-DVA 'B' indicates that the primary address for media is IPv6. E-DVA 'A' replies with IPv6 as a primary address. Each side negotiates an IPv6 media path. The media traverses the IPv4 network in a tunnel (e.g., GRE, etc.). It is encapsulated at 'B's router, and decapsulated at 'A's router. Since both E-DVAs indicated a preference for IPv6, both sides negotiate an IPv6 media path with a tunnel in between.

6.7 Softphone Use Cases

This use case describes the use of IPv6 Softphones (MSO-provided).

6.7.1 IPv4 Softphone attached to IPv4 Network

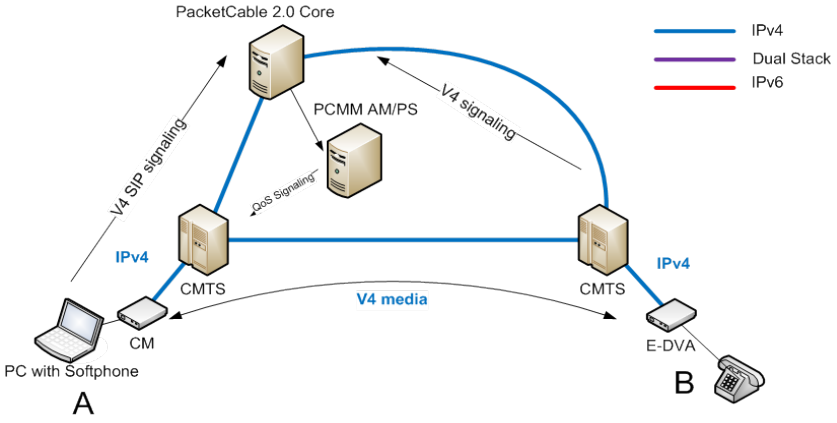

Figure 26 - IPv4 Softphone attached to IPv4 Network

Setup: The MSO attaches an IPv4 PC-based Softphone 'A' to an IPv4-only PacketCable 2.0 Core. The MSO uses PCMM for QoS. The far end E-DVA 'B' is also in MSO network as an IPv4 E-DVA.

Softphone Provisioning/SIP Registration: Softphone 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4 with PC 2.0 Core. E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration as well.

Signaling: Softphone 'A' sends the SIP INVITE to the PC 2.0 Core using IPv4. The PacketCable 2.0 Core sends the call setup message to 'B' over IPv4. E-DVA 'B' replies with the 200-OK message using IPv4.

Media: Softphone 'A' indicates that the primary address for media is IPv4. 'B' replies with IPv4 as a primary. So both sides negotiate an IPv4 media path.

QoS: During media establishment, the PacketCable 2.0 Core notifies the PCMM Application Manager (AM)/Policy Server (PS) about the QoS needs. The PCMM AM/PS signals the CMTS to set up a UGS service flow for the media with the CM to which the Softphone is attached.

6.7.2 IPv6 Softphone attached to IPv6 network

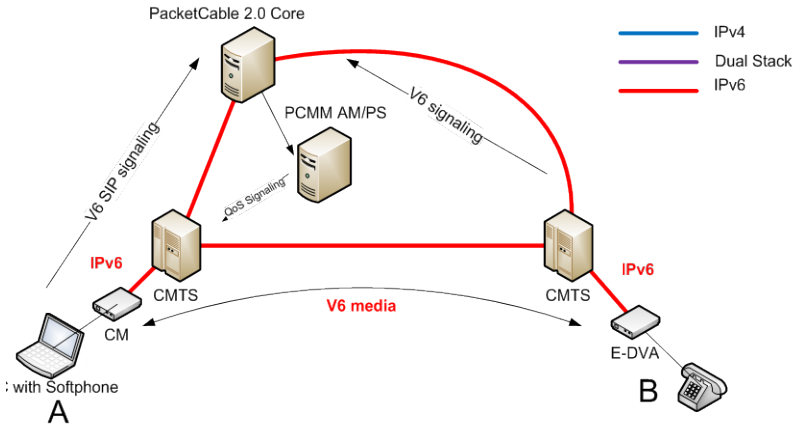

Figure 27 - IPv6 Softphone attached to IPv6 Network

Setup: The MSO attaches an IPv6 PC-based Softphone 'A' to an IPv6-only PacketCable 2.0 Core. The MSO uses PCMM for QoS. The far end E-DVA 'B' is also in the MSO network as an IPv6 E-DVA.

Softphone Provisioning/SIP Registration: Softphone 'A' is provisioned in IPv6 mode and completes SIP registration using IPv6 with the PC 2.0 Core. E-DVA 'B' is provisioned in IPv6 mode and completes SIP registration as well.

Signaling: Softphone 'A' sends the SIP INVITE to the PC 2.0 Core using IPv6. The PacketCable 2.0 Core sends the call setup message to 'B' over IPv6. E-DVA 'B' replies with the 200-OK message using IPv6.

Media: Softphone 'A' indicates that the primary address for media is IPv6. 'B' replies with IPv6 as a primary. So both sides negotiate an IPv4 media path.

QoS: During media establishment, the PacketCable 2.0 Core notifies the PCMM AM/PS about the QoS needs. The PCMM AM/PS signals the CMTS to set up a UGS service flow for the media with the CM to which the Softphone is attached.

6.7.3 IPv4 Softphone attached to IPv4 Network using NAT444

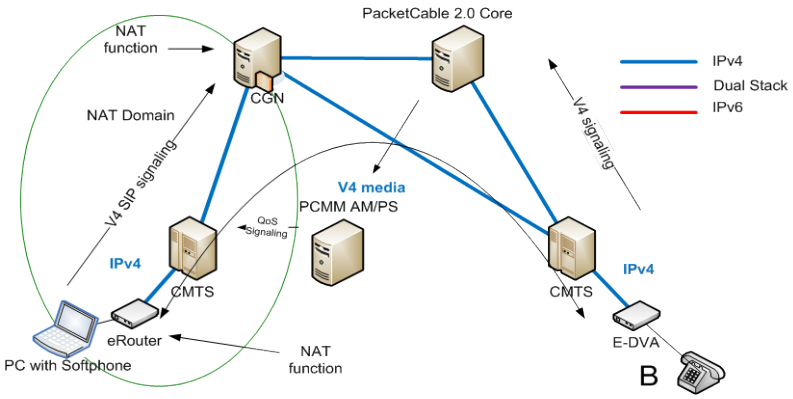

Figure 28 - IPv4 Softphone attached to IPv4 Network using NAT444

Setup: The MSO attaches an IPv4 PC-based Softphone 'A' to an IPv4-only PacketCable 2.0 Core. The far end E-DVA 'B' is also in the MSO's network as an IPv4 E-DVA.

The MSO uses NAT444, and has deployed PCMM for QoS.

Softphone Provisioning/SIP Registration: Softphone 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4 with the PC 2.0 Core. (Note: PacketCable Core receives packets with translated address, due to the NAT444). E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration as well.

Signaling: Softphone 'A' sends the SIP INVITE to the PC 2.0 Core using IPv4. The PacketCable 2.0 Core sends the call setup message to 'B' over IPv4. E-DVA 'B' replies with the 200-OK message using IPv4.

Media: Softphone 'A' uses ICE to set up the media path through two layers of NAT (eRouter and CGN). E-DVA 'B' replies with IPv4 address. Softphone 'A' sets up IPv4 media path and indicates that the primary address for media is IPv4. E-DVA 'B' replies with IPv4 as a primary. So both sides negotiate an IPv4 media path.

QoS: During media establishment, the PacketCable 2.0 Core notifies the PCMM AM/PS. Whether QoS establishment is successful depends on the nature and location of the NAT, whether it can manipulate SIP headers, and whether the IP address of the eRouter is exposed as a candidate media address. If possible, the PCMM AM/PS signals the CMTS to set up a UGS service flow for the media with the CM to which the Softphone is attached.

6.7.4 IPv4 Softphone attached to IPv6 Network using DS-Lite

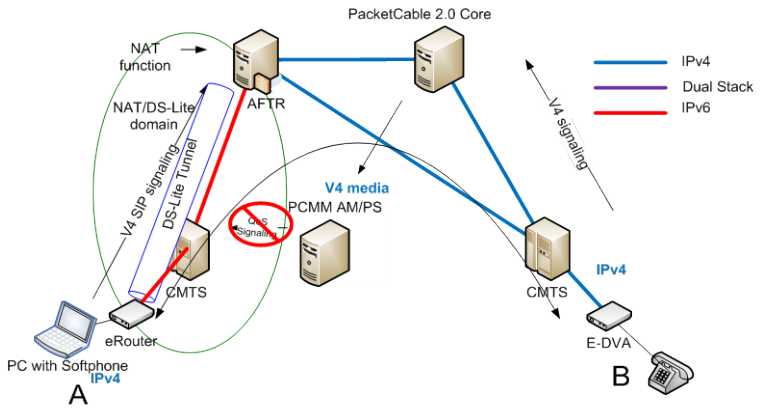

Figure 29 - IPv4 Softphone attached to IPv6 Network using DS-Lite

Setup: The MSO attaches an IPv4 PC-based Softphone 'A' to an IPv4-only PacketCable 2.0 Core. The far end E-DVA 'B' is also in the MSO's network as an IPv4 E-DVA.

The MSO uses DS-Lite, and has deployed PCMM for QoS.

Softphone Provisioning/SIP Registration: Softphone 'A' is provisioned in IPv4 mode and completes SIP registration using IPv4 with the PC 2.0 Core. (Note: PacketCable Core receives packets with translated address, due to the DS-Lite). E-DVA 'B' is provisioned in IPv4 mode and completes SIP registration as well.

Signaling: Softphone 'A' sends the SIP INVITE to the PC 2.0 Core using IPv4. The PacketCable 2.0 Core sends the call setup message to 'B' over IPv4. E-DVA 'B' replies with the 200-OK message using IPv4.

Media: Softphone 'A' uses NAT Traversal Functionality to set up the media path through the DS-Lite NAT function at the CGN. E-DVA 'B' replies with IPv4 address. Both sides negotiate an IPv4 media path. 'A' sets up IPv4 media path.

QoS: During media establishment, the PacketCable 2.0 Core notifies the PCMM AM/PS about the QoS needs. The PCMM AM/PS notifies the CMTS to set up a UGS service flow for the media. However, since the media is encapsulated in IPv6, the CMTS cannot set up classifiers to establish a service flow for media with the CM to which the Softphone is attached, so voice traffic receives no QoS.

6.8 PC 1.5 across IPv6 Network

6.8.1 IPv4 E-MTA, IPv4 CMS, and an IPv6 Interconnect

PacketCable 1.5 E-MTAs and CMSs only support IPv4. MSOs can connect islands of IPv4 across an IPv6 core using tunnels. The Signaling and Media can then successfully traverse across the network.

Equipment: The Routers must support tunnels (e.g., IP-in-IP, GRE). No other new components are needed. Specifically, no TrGWs are required.

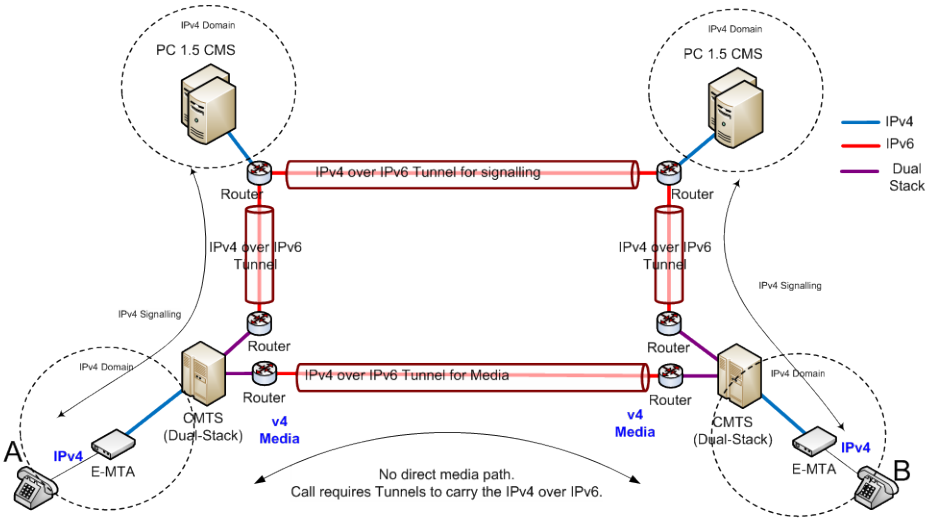

Figure 30 - PC 1.5 across IPv6 Network

Setup: The PC 1.5 CMSs and the PC 1.5 E-MTAs are on islands of IPv4 in a sea of IPv6. The E-MTAs support IPv4, the CMTS supports Dual-stack, and the CMS supports IPv4 on both sides. The connection between the CMTS and CMS is IPv6, and the connection between the two CMS is IPv6.

E-MTA Provisioning/SIP Registration: E-MTAs 'A' and 'B' is provisioned in IPv4 mode and completes registration with the CMS using IPv4.

Signaling: E-MTA 'A' completes NCS call signaling with the PC 1.5 CMS using an IPv6 tunnel to carry the IPv4 packets from the E-MTAs. E-MTA 'A's CMS routes the call to the E-MTA 'B's CMS over a tunnel. E-MTA 'B' completes NCS call signaling with the PC 1.5 CMS using an IPv6 tunnel to carry the IPv4 packets from the E-MTAs.

Media: The IPv4 media traverses the network in a tunnel (e.g., GRE, etc.). It is encapsulated at E-MTA 'A's router, decapsulated at E-MTA 'B's router. Media path is successfully established. Since both endpoints support IPv4, E-MTAs 'A' and 'B' set up an IPv4 media path with the support of tunnels to carry the signaling and media traffic over IPv6.

7 IPV6 WEB CONTENT USE CASES

Consumer adoption of IPv6 will be primarily governed by content availability. MSOs need to enable IPv6 on their content infrastructure to provide IPv6 access to web content and high-value applications like email, DNS, and FTP. In addition, providers need to interface with third-party content providers to encourage native IPv6 adoption for web content, DNS, Content Distribution Networks (CDNs), and geolocation services, while minimizing the use of white lists that restrict availability of IPv6 content.

The following sets of use cases identify how MSOs and content providers can enable IPv6 access to content. Since content delivery is not specified in any CableLabs specifications, these use cases identify the emerging best practices for MSOs.

7.1 Internal Web Content/Portal Support

This use case describes how an MSO can enable IPv6 on its web portal and offer the web content over IPv6.

7.1.1 Typical Web Services Architecture

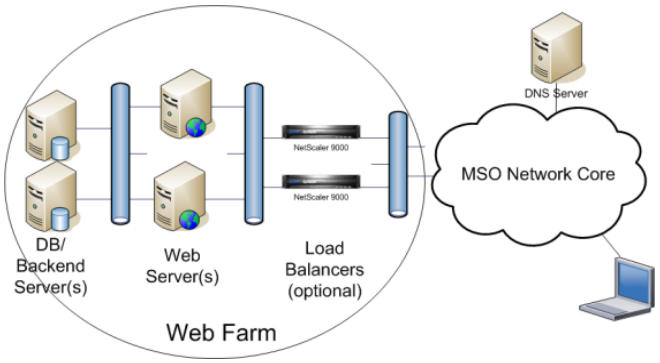

Figure 31 - Web Services Architecture

A typical web services architecture (as shown in Figure 31) consists of a set of web servers connected to a set of load balancers at the front end and a set of database servers at the backend.

7.1.2 Enabling IPv6 Web Services

This use case requires an IPv6 core network to enable IPv6 connectivity to clients.

There are two potential approaches to enable IPv6 for web services:

1. Enable IPv6 (Dual-stack or separate infrastructure for each protocol) on the load balancers, while leaving the web servers as IPv4-only.
2. Enable Native IPv6 (Dual-stack or separate infrastructure for each protocol) on the web servers. If load balancers are available, this requires them to support IPv6 as well.

With either approach, the MSO needs to configure the DNS server to offer AAAA records. The backend/database servers can stay IPv4 or be upgraded to IPv4/IPv6 dual-stack.

7.1.3 Load Balancers with IPv6 Support

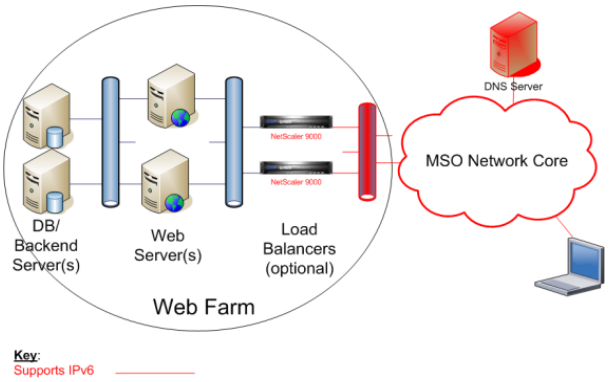

Figure 32 - Load Balancers

An IPv6 load balancer rewrites requests to the IPv4 servers. Using load balancers, (as shown in Figure 32) an MSO can provide IPv6 service while maintaining IPv4 on web servers and backend infrastructure. Citrix Netscaler, A10, F5, and other devices currently support IPv6.

The following steps enable IPv6 on the load balancers:

1. Ensure that the load balancers support IPv6.
2. Enable IPv6 on the load balancers' customer-facing interfaces.
3. Create service-mapping rules from IPv6 virtual addresses to the web server IPv4/IPv6 addresses.
4. Before providing DNS IPv6 AAAA records, test the connectivity through the load balancer.

7.1.4 IPv6-enabled Web Servers

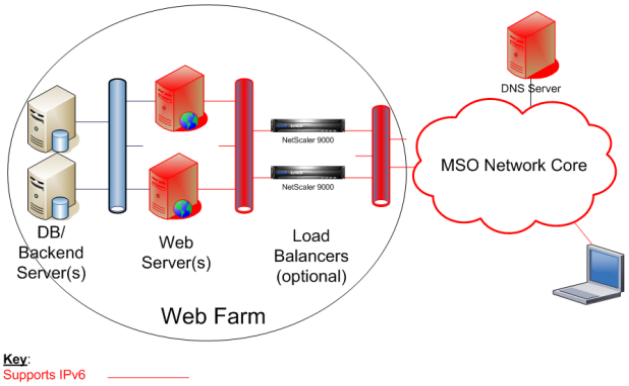

Figure 33 - Web Services Architecture

The primary function of a web server is to deliver web pages to clients over the Internet.

The following steps enable IPv6 on a web server as depicted in Figure 33:

1. Ensure that the web server OS supports IPv6.
   - The following operating systems have demonstrated IPv6 support: Windows Server 2003/2008, Windows 7, Vista, Linux, Solaris, Mac OS X, and x-BSD.
2. Verify that the web server software supports IPv6.

3. Apache, ngnix, lighttpd, Zeus, and IIS have all demonstrated IPv6 support.
4. Enable IPv6 on Ethernet interfaces using a static IPv6 Address (i.e., not using Stateless Address Auto Configuration or Stateful DHCPv6). The interface could continue to maintain an IPv4 address, as well.
5. Bind the IPv6 address to the web server via a config file setting.
6. Verify that the server is operational and supports IPv6.
7. Verify that the log processor software supports IPv6.
8. If applicable, enable IPv6 support on the load balancer.

For more information, see the RMv6TF presentation on enabling a web server: http://www.rmv6tf.org/2010-IPv6-Summit-Presentations/The%20IPv6%20Enabled%20Website-Stan%20Barber.pdf

7.1.5 IPv6-enabled DNS Servers

Once the load balancers and the web servers have enabled IPv6, MSOs must also enable IPv6 on the DNS servers to make content available to subscribers.

The following steps enable IPv6 on a DNS Server:

1. Ensure that the operating system supports IPv6.
   - Windows Server 2003/2008, Linux, x-BSD, Solaris, and Mac OSX have demonstrated IPv6 support.
2. Ensure that the DNS Software supports IPv6 transport and IPv6 AAAA records.
   - Microsoft, BIND, Nominum, and others listed at the following link are known to support IPv6: http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software.
3. Include AAAA records in DNS Zone Files.
4. Enable IPv6 on Ethernet interfaces using static IPv6 addresses, while continuing to maintain IPv4 addresses.
5. Test the DNS server.

7.1.6 Secure Web Connection

Transport Layer Security (TLS) and Secure Socket Layer (SSL) are cryptographic protocols that provide encrypted communications channels across the Internet. The main SSL/TLS functions are encrypting traffic and authenticating the owner of the website.

The TLS/SSL protocols operate as follows:

1. The user connects to a web server through a client application.
2. The client (user's browser) and server negotiate a common cipher suite.
3. The server sends its digital certificate to the client.
4. The client verifies the certificate and signature. The certificate must be signed by a Certificate Authority (CA) whose root certificate is present in client applications such as web browsers.
5. Both parties generate session keys for encryption and decryption.
6. A secure connection is established using SSL/TLS, and subsequent traffic is sent encrypted.

7.1.7 Digital Certificates

Digital certificates are electronic documents that use digital signatures to bind together public keys with an identity. Some of the important certificate fields are enumerated below (see Figure 34):

- Serial Number
- Subject (CN)
- Signature Algorithm
- Issuer
- Valid-From
- Valid-To
- Key-Usage
- Public Key
- Thumbprint Algorithm
- Thumbprint.

Two of the key fields used in SSL/TLS negotiations include the Thumbprint (Hash) and the Public Key.

Wildcard certificates can be used to secure multiple subdomains with a single digital certificate. A wildcard certificate for `*.example.com` will secure www.example.com, mail.example.com, and any other first-level subdomain of example.com.

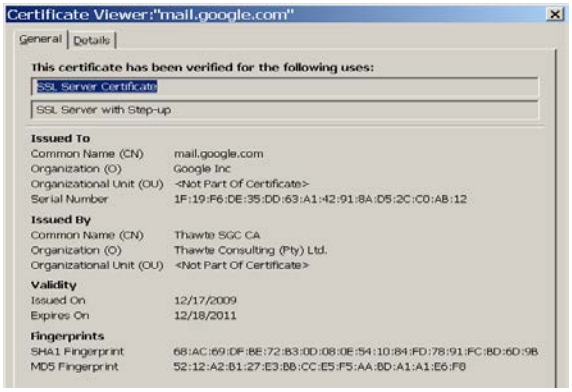

Figure 34 - Certificate Example

7.1.7.1 IPv6 Considerations

The digital certificate Subject/Common Name field is the only field affected by IPv6. The certificate is typically issued to a Fully Qualified Domain Name (FQDN). In client-server interaction, clients typically perform a reverse DNS lookup to verify that the server hostname in the certificate matches the IP address.

Some sites issue a digital certificate to an IP address rather than an FQDN. In such cases the IP address is used as the Subject/Common Name. When migrating to IPv6, a dual-stack server using an IP-based Common Name needs two certificates: one for IPv4 and one for IPv6. Such a practice increases the cost of the provider's public key infrastructure (PKI) and increases the operational complexity for the web service. Thus, the recommended best practice is to bind the digital certificate to the server's FQDN.

7.1.7.2 Enabling IPv6/SSL

The following steps are needed to enable IPv6/TLS on a web server:

1. Verify that the server supports SSL/TLS and IPv6.
2. Ensure that the server has a valid digital certificate bound to the web server's FQDN.
3. Enable IPv6 on the web server, as described in Section 7.1.
4. Install the digital certificate on the web server.
5. Populate DNS (AAAA) and Reverse DNS (PTR) entries to point to the web server or load balancer IPv6 address.

7.1.7.3 Common Problems

One of the biggest issues with SSL/TLS connections on the IPv6 internet today is the poor customer connectivity caused by broken tunnel implementations (particularly 6-to-4 and Teredo tunnels). These can lead to timeouts that cause customers to experience a very slow or broken connection.

Another common issue is that if MTU sizes are not consistent through the network, packet sizes may exceed the link MTU. If the application set the 'Do Not Fragment' bit, packets will be dropped along the hops.

Finally, if Reverse DNS lookup fails or times out because the ip6.arpa entries are not populated, it can delay or deny session establishment, again causing customers to experience slow or broken connections.

7.2 Proxy Server

A proxy server functions as an intermediary in connecting clients to servers. It is generally used to implement security and filtering policies; however, due to its position in the network, it can optionally alter the client's request or the server's response. Additionally, some proxy servers support the functionality to cache responses from the remote server to accelerate future requests. Proxy servers could also serve as protocol translators.

7.2.1 Implementation Methods

There are two ways in which to implement proxy servers.

1. Direct: Users enter proxy settings into their browsers. Subsequently, the browsers direct all traffic to the proxy server. Such implementation can be used to limit web access per administrative policies (e.g., in a school or corporate setting).
2. Transparent: Network elements automatically redirect users to the proxy server without requiring browser configuration. This type of proxy is typically used for hotspot logins, caching servers, and advanced home users who have enabled Squid (a freely available open-source proxy server).

7.2.2 IPv6 Proxy Servers

If the proxy server supports IPv6, it can be used to translate between IPv4 and IPv6. This could enable an IPv4-only user to access IPv6 web content and an IPv6 user to access IPv4 web content. As such, MSOs could include a translating proxy in a home gateway (similar to NAT46 proposals under consideration within the IETF) or include a translating proxy in an MSO server, such as a CGN.

By their nature, proxy servers only offer limited scalability, and are typically a single point of failure. Also, some proxy servers break TLS/SSL connections because the digital certificate does not match the address of the proxy server. Due to these limitations, MSOs are likely to only use proxy servers to enable IPv6 in specific limited situations.

7.3 Geolocation

Geolocation is a method to identify a user's geographic location based on the user's IP address.

7.3.1 Geolocation in IPv4

The primary sources of geolocation information are Regional Internet Registries (RIRs), such as ARIN, APNIC, and RIPE NCC. Secondary sources include the following:

- Comparing the user's public IP address with known locations of other neighboring servers and routers.
- Data mining user-submitted geographic location data.
- Examining information contributed by Internet Service Providers.
- Merging databases from different suppliers.

- Reverse DNS lookups.

The accuracy of the location information is improved by data scrubbing and statistical analysis.

7.3.2 Geolocation Uses

There are many uses for geolocation information including:

- Regional licensing used by Internet movie vendors and online broadcasters who only serve content to viewers in their licensed territories.
- Targeting local content to a specific area, such as location-based marketing.
- Prevent online fraud by restricting transactions from known harmful areas in the Internet.

7.3.3 Geolocation Providers

Geolocation services are generally offered by third-party providers. There are both free and commercial offerings, such as Google Location Services (default in Firefox), Mixer Labs (Twitter), Ip2location, Ipligence, Maxmind, and others.

7.3.4 IPv6 Implications

Geolocation services require a unique mapping between a user's IP address and location. However, certain IPv4 extensions and IPv6 transition technologies multiplex multiple users (and likely multiple user locations) behind a single IP address. For example, NAT444, NAT64, and DS-Lite break or dilute the geolocation information by moving the NAT function away from users and by mapping multiple users to the same address. Geolocation issues related to CGNs and potential solutions are covered in detail in Section 11. In this case, the address reported to the content server is the address of the NAT function, not the actual customer. Complicating the deployment of IPv6, there are currently no commercial IPv6-Geolocation services available today. However, IPv6 geolocation services will be easier to create than NAT-aware geolocation services. When transitioning to IPv6, MSOs can simplify the creation of such services by developing geographically organized addressing plans. Thus, content providers are advised to adopt IPv6 as a means of maintaining reasonable accurate location services into the future.

7.4 Content Distribution Networks (CDNs)

Content Delivery Networks or Content Distribution Networks (CDNs) are networks of servers distributed close to the edges of a network that hosts copies of popular web content. Hosting such content closer to users speeds up client access to the content. Many content providers also use CDNs to scale content distribution to large numbers of subscribers around the globe. Thus, CDNs are used for website acceleration, web caching, load balancing, and network congestion control. In the future, they could be used to offer IPv6 access to content hosted on IPv4-only servers.

7.4.1 CDN and IPv6

IPv6-enabled CDNs can make content sourced from an IPv4-only origin available to subscribers over IPv6. This can accelerate the adoption of IPv6 by providing IPv6 content before content originators are ready to upgrade their systems to support IPv6.

The CDN performs protocol conversion by enabling dual-stack (IPv4 and IPv6) support. The CDN server can then both collect and serve content using either protocol. If the content provider is only offering content over IPv4, the CDN server can use its IPv4 address to contact the server. Once the CDN server obtains content, customers can then access it through either protocol.

For the case of transition technologies that use CGNs, there is the added complexity that the user will connect to the CDN access point outside of the NAT, and not necessarily the one closest to the user. Thus, the IPv4 address reported to the CDN will be that of the NAT, not the user. Consequently, the CDN will lose visibility on geolocation information and the number of unique visitors to the site.

Some MSOs use internal CDNs; however, most CDN service is offered by third party providers, such as Akamai, Limelight, EdgeCast, AT & T, Level 3, Highwinds, Mirror Image, Internap, BitGravity, CDNetworks, and StreamZilla. Of these, only Limelight currently supports IPv6; this service is used by Netflix. Limelight's service includes Dual-stack connectivity, IPv6 transit routes, and DNS support. Akamai, BitGravity, and StreamZilla, do not currently support IPv6, but they have announced plans to support it in the near future. Other CDNs have not announced plans to support IPv6.

7.5 Web Content Providers and IPv6

One of the main roadblocks in IPv6 deployment is that customers will not adopt IPv6 until web content is available in IPv6. Hence, MSOs are encouraging content providers to offer IPv6 content.

Some providers who announced plans to deploy IPv6 early on include: Google (including YouTube), NTT, The Planet, Comcast, Choopa Hosting, Microsoft Windows Live, Word Press, Altopia, Yahoo, Verizon Business FIOS, Sprint, Giganews, eBay, Facebook, and Netflix. ATT, Qwest, AOL, Level3, Myspace, TWC, MSN, Wikipedia, and newsDemon announced plans to deploy IPv6 in 2010. On June 6 2012 many of the world's top websites enabled IPv6 support. In fact, on that day dubbed "World IPv6 Launch," multitudes of website operators, network operators and home router vendors from all over the world joined thousands of companies and millions of websites in permanently enabling IPv6.

7.5.1 Requirements for IPv6 Web Content

Third-party providers can enable IPv6 web content using the following steps:

- Ensure that IPv6 connectivity is available at the site and/or hosting provider.
- Enable IPv6 on the load balancer or web server as described in Section 7.1, Internal Web Content/Portal Support.
- Enable DNS support for IPv6. IPv6 AAAA record support is required. IPv6 transport support is desirable.

Web content providers can also certify their IPv6 readiness with the IPv6-enabled logo program: http://www.ipv6forum.com/ipv6_enabled/.

7.6 IPv6 DNS Support

7.6.1 Domain Name System (DNS) Overview

The Domain Name System (DNS) is a distributed, hierarchical naming system that maps easy-to-remember names to IP addresses. As a hierarchical system, DNS delegates responsibility for name-IP address mappings to servers authoritative for a particular domain. A DNS name server maps a domain name to an IP address by compiling a database of DNS records in a zone file. Common records include Address records (A for IPv4 and AAAA for IPv6), name server (NS) records, reverse DNS 'pointer' records (PTR), and mail exchanger (MX) records. There are also present glue records, which identify the IP addresses of the authoritative name servers for the domain. These are used to speed up DNS lookups and preventing circular lookups.

The top of the hierarchy is served by the root name servers, which are queried first as part of the recursive lookup algorithm. Below them, each domain has at least one authoritative DNS server that publishes information about the domain and any sub-domains.

7.6.1.1 Reverse DNS

Reverse DNS maps a domain name to an IP address. To populate reverse DNS, the server stores IP addresses in form of pointer (PTR) records using special domains. For IPv4, the reverse lookup domain is in-addr.arpa. For IPv6, the reverse lookup domain is ip6.arpa.

- IPv4 10.0.0.1 => 1.0.0.10.in-addr.arpa IN PTR www.example.com

- IPv6 address 2001:db8::567:89ab => b.a.9.8.7.6.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa IN PTR www.example.com

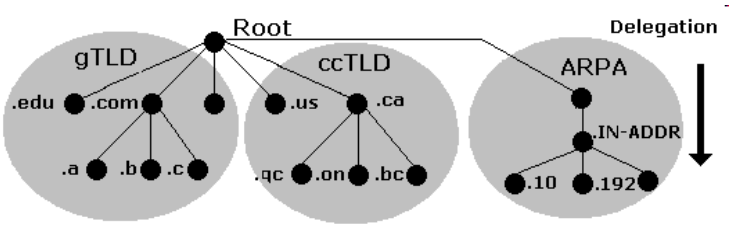

Figure 35 - DNS Root

7.6.2 DNS IPv6 Behavior

With its ability to translate human-readable domain names into machine-readable IP addresses, DNS is critical to how the Internet operates today. Given IPv6's longer addresses, it will be even more important as the adoption of IPv6 progresses. The first step towards supporting native IPv6 services is enabling IPv6 transport on caching or recursive name servers. This is generally benign, as simply enabling the IPv6 transport does not force subscribers to use it. Depending on client capabilities, a dual-stack-enabled recursive name server infrastructure can and will respond to queries for both A and AAAA DNS resource records.

Unlike enabling caching name services, enabling authoritative name servers to support IPv6 has different challenges. As with caching name services, enabling IPv6 transport on authoritative name services poses limited risk. However, the creation of IPv6 AAAA resource records for critical sites and services could prove to be problematic for subscribers with limited or misconfigured IPv6 connectivity. IPv6-capable and IPv6-enabled operating systems and applications automatically request both IPv4 (A) and IPv6 (AAAA) resource records when querying name services. If AAAA records are returned, in some cases, this will result in attempts to utilize services over IPv6, even if there is limited or no IPv6 connectivity to the remote server, resulting in potential customer service issues when key websites or email servers are seemingly not accessible. Controlling the rollout of IPv6 DNS records is essential to a successful IPv6 deployment.

7.6.3 Steps to enable IPv6 DNS

The following steps help rolling out IPv6 DNS support:

1. Ensure that the DNS Server supports IPv6.
2. Enable IPv6 transport on caching or recursive name servers, as described in Section 7.1.5.

Note: This is a low risk upgrade.

3. In a similar manner, enable IPv6 transport on authoritative name servers.
4. Add AAAA records to the zone files for the domain.

Note: This is potentially higher risk, so should be managed carefully.

5. Add the reverse DNS PTR records to the DNS system.

7.6.4 IPv6 DNS Whitelists

When migrating to IPv6, there is an opportunity to leverage the DNS infrastructure to granularly control access to IPv6 content and services. However, as discussed above, offering AAAA records to clients with limited IPv6 connectivity could result in service outages or delays in accessing content and services. Some companies are experimenting with a "white list" approach that enables IPv6 access to web content only from service providers that meet specific requirements in an attempt to mitigate the adverse impacts to their users' experience.

7.6.4.1 Content Providers using Whitelists

Most notably, Google has pioneered the "whitelist" approach in their transition to IPv6. Some background on how Google has implemented and deployed whitelist support for IPv6 can be found on its IPv6 site (see http://www.google.com/intl/en/ipv6/). Customers of ISPs that are not on the whitelist will not receive 'AAAA' records in response to DNS requests for any Google websites other than ipv6.google.com.

Yahoo proposes what they call a "Really Ugly Hack" to DNS. It intends to return 'AAAA' resource records when DNS queries arrive over IPv6 and 'A' records when the queries arrive over IPv4. Thus, it will make its content available over IPv6 only to clients capable of sending DNS queries over IPv6. This approach, however, has drawbacks. Clients running operating systems such as Windows XP can only send DNS queries over IPv4, so such clients would be limited to IPv4 service only, even if IPv6 is enabled.

A group of companies including Google, Yahoo, Netflix, and Microsoft are considering a central shared, open source DNS whitelist service. With such an approach, there would only be one whitelist and one set of whitelist criteria, as opposed to each company having its own list.

7.6.4.2 Whitelist Issues for MSOs

Whitelists present many issues to MSOs, particularly:

1. Scalability: The use of whitelists to enable IPv6 access requires MSOs to contact every content provider to exchange information about whether they can forward AAAA DNS records. This does not scale across millions of domains and autonomous networks across the Internet.
2. Management: Whitelists mean increased customer support costs for the MSOs. It is also time-consuming for MSOs to continue to monitor and maintain their IPv6 status on particular whitelists, particularly as the number of whitelists grows.
3. Numerous and varying whitelist policy requirements: MSOs cannot assume uniform behavior from all whitelist providers, and thus have to deal with multiple independent whitelist policies defining appropriate IPv6 service levels.
4. Whitelists essentially creates a two-tiered public IPv6 Internet, which segregates the Internet users into those added to privileged whitelists of large content providers and those who are not.
5. Whitelists potentially delay native IPv6 deployments by restricting subscriber access to IPv6 content, even when their system would support it.
6. Whitelists delay the ability of MSOs to learn of broken IPv6 links during initial deployment phases by forcing clients to fall back to IPv4.

Thus, whitelists are problematic for MSOs. More information on whitelist problems is available at the following link: http://www.comcast6.net/IPv6_DNS_Whitelisting_Concerns_20100416.pdf. MSOs are engaging content providers to create alternatives that facilitate customer transition to IPv6, while offering customers the best possible user experience.

7.7 IPv6 High-Value Applications

Users require support for additional IPv6 services beyond web browsing. Common services include email, FTP, Instant Messaging (IM), gaming, and peer-to-peer (P2P) applications. This section discusses the level of IPv6 support in many of these applications. Useful IPv6 application support surveys are available at http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support and http://www.ipv6.org/v6-apps.html.

7.7.1 Email

Many email applications support IPv6. The following prominent clients already support IPv6: Outlook, Thunderbird, Mac mail, and Gmail (web-based). Likewise, well-known email servers, such as Sendmail and MS Exchange, also support IPv6, and can serve as relays between IPv4 and IPv6 networks.

Both the POP and IMAP protocols work with IPv6. SMTP IPv6 Requirements are defined in [RFC3974].

Steps required to enable IPv6 on a Sendmail server are as follows:

- Build Sendmail with IPv6 options. Ensure that the APPENDDEF(`confENVDEF', `-DNETINET6 -DNEEDSGETIPNODE') option is included in the build file prior to compilation.
- Configure the sendmail.mc file to include define(`_NETINET6_')dnl.
- Install an AAAA record in the DNS for the mail server.

7.7.2 FTP

FTP support is a slightly more difficult use case for IPv6. Since FTP includes IP addresses within the protocol itself, protocol extensions to FTP are required for IPv6. These extensions are defined in [RFC2428] and [RFC6384].

IPv6 support is already widely available in many common FTP Clients and servers, including xlight, Pure-FTPd, NcFTPd, and ftp.exe.

7.7.3 Instant Messenger (IM)

IM support for IPv6 is very limited. Many common clients such as Skype, AIM, GoogleTalk, and Yahoo messenger do not yet support IPv6.

Only MS Windows Live Messenger supports IPv6 in a limited fashion. IPv4 is used for signing in to the server (authentication), exchanging presence (status), and text messages; IPv6 is only used for direct communications between clients for functions such as file transfers.

7.7.4 Gaming and Mobile Platforms

Gaming support for IPv6 is very limited. The leading game platforms, including XBOX, PS3, and WII, do not support IPv6. Also, leading online game networks, such as EA, Blizzard, Sony Online Entertainment, and Microsoft Games, do not support IPv6.

Mobile phone operating systems used as gaming platforms are beginning to offer IPv6. Apple iOS 4 and Android 4.0 introduced support for IPv6.

7.7.5 P2P File Sharing Apps

Peer-to-peer file sharing applications make up a huge percentage of the traffic on the Internet. P2P Clients are embracing IPv6 as a way to evade traffic control systems. IPv6 traffic levels surged in early 2010 when IPv6 P2P clients were released with IPv6 support. See http://www.theregister.co.uk/2009/09/10/ipv6_traffic_surge/.

The µTorrent, BitTorrent, and gtk-gnutella P2P clients support IPv6. The Gnutella (Limewire) P2P client does not support IPv6.

8 LAWFUL INTERCEPT USE CASES

Lawful interception (LI) is a telecommunications function of collecting communications network data for a Law Enforcement Agency (LEA) for the purpose of analysis or evidence. Such data generally consists of signaling or network management information and, in some instances, the content of the communications. These use cases explore IPv6 support in CableLabs Cable Broadband Intercept Specification [CBIS] and PacketCable Lawfully Authorized Electronics Surveillance (LAES) specifications.

8.1 Cable Broadband Intercept Specification (CBIS) Overview and IPv6 Accommodation

The CBIS specification [CBIS] identifies the specific interface points between the MSO and the LEA that has served the Broadband Intercept Order and enumerates the specific requirements for these interface points.

8.1.1 CBIS Outline

The following specific interfaces and logical functions have been identified and defined (as shown in Figure 36 and Figure 37) in order to meet the Law Enforcement's (LE) objectives and high-level requirements for Broadband Intercepts related to Transparency, Confidentiality, Authentication, Validation, Non-Repudiation, Correlation, Isolation, Completeness, Compression, and Encryption.

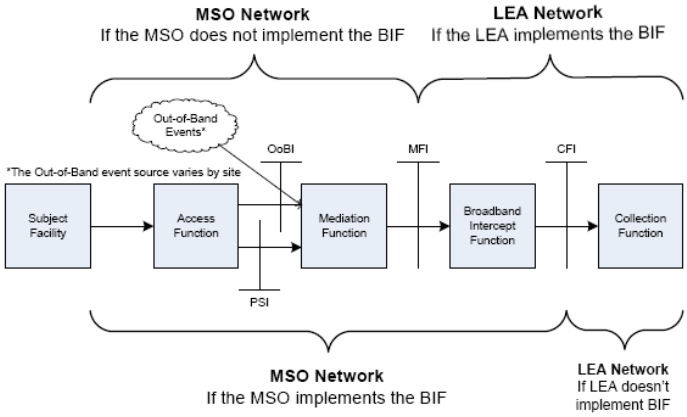

Figure 36 - CBIS Broadband Intercept Interfaces

8.1.1.1 Access Function

The access function is a site-specific means of directing data to an out-of-band interface or to a packet-stream interface. The access function may be implemented as an optical tap, a UDP data stream, a port mirror, or something else that is reliable and fast enough to manage multiple streams with no packet loss.

8.1.1.2 Mediation Function

The mediation function creates hashes and formats all events, headers and packet data depending on the type of intercept. The intercepts can be of two types: full packets or packet headers only. In either case, out-of-band data (e.g., DHCP) packets are captured. The mediation function has interfaces to collect raw data from the access function, and store formatted data at the broadband intercept function.

8.1.1.3 Broadband Intercept Function (BIF)

The broadband intercept function includes a buffer area, which is used to store 24 hours of formatted data. The BIF is an optional function for MSOs; operators may choose to implement the BIF or request that the LEA provide the BIF. The operator needs to ensure that the buffer space is sufficiently sized on an LEA-by-LEA basis.

8.1.1.4 Collection Function

The collection function provides a secure means to deliver data to LEA. It is possible for more than one LEA to have simultaneous access to such data. Some LEAs will want to set up a VPN connection, while others will use SSH and/or portable storage. For each intercept, the operator and LEA must negotiate a single common solution for the topology and protocol (e.g., IPv4 or IPv6).

8.1.2 CBIS Operation

When a Lawful Intercept Order is received by the operator, the CBIS data collection begins [CBIS]. Access to CBIS equipment is strictly controlled by law and limited to prevent disclosure of the presence of an active intercept. CBIS data collection involves the following steps:

- The operator identifies the cable modem associated with the subject facility.
- CPE devices are identified via the cable modem MIB tables.
- CBIS equipment is provisioned to capture the traffic, either by directly using CLI or using SNMP Tables, such as extractions from the dot1dTpFdbTable.
- The intercepted data is forwarded via the 'Access Function' to the 'Mediation Function'.
- CBIS has enough information to create identification tags for expected data streams.
    - For IPv4, a five-tuple consisting of source and destination IP addresses, source and destination ports and the protocol field can be created.
    - If IPv6 is in use, a six-tuple that adds the Flow Label field to the above five-tuple can be created.
- Data matching the five-tuple or six-tuple filters are formatted at the Mediation function and then passed to 'Broadband Intercept Function'. See Figure 37; the data includes both packet data and out-of-band messages.
- At the end of the intercept, the data is forwarded to the 'Collection Function' for collection by the LEA.

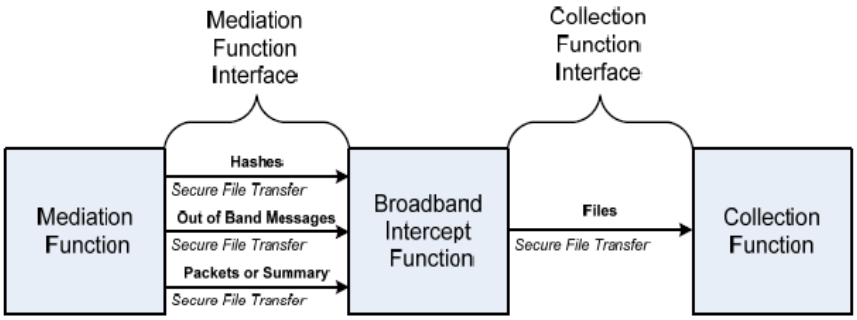

Figure 37 - CBIS Logical Network

8.1.3 CBIS IPv6 Status

In consultation with the FBI and CALEA Implementation Unit (CIU), CableLabs wrote an Engineering Change (EC) document (CBI2.0-N-10.0976-1) to add IPv6 support to the CBIS specifications. As of February 2011, the ECN has been incorporated in the CableLabs [CBIS] specification. This EC adds requirements to capture IPv6 six-

tuples, as mentioned above. The six-tuple includes the source and destination IP addresses, source and destination ports, protocol field, and IPv6 flow label. This EC also requires that DHCPv6 lease information also be captured.

After discussion with the CIU, ND and IPv6 multicast traffic are not captured. Tunneled (encapsulated) traffic is also not captured, unless the operator owns at least one of the tunnel endpoints.

8.1.4 Transition Technology Impact on CBIS

DS-Lite, NAT444, and 6RD (IPv6 Rapid Deployment) will have impacts on Lawful Intercept.

8.1.4.1 NAT444 Lawful Intercept

This use case discusses LI when the customer is behind a NAT444 deployment.

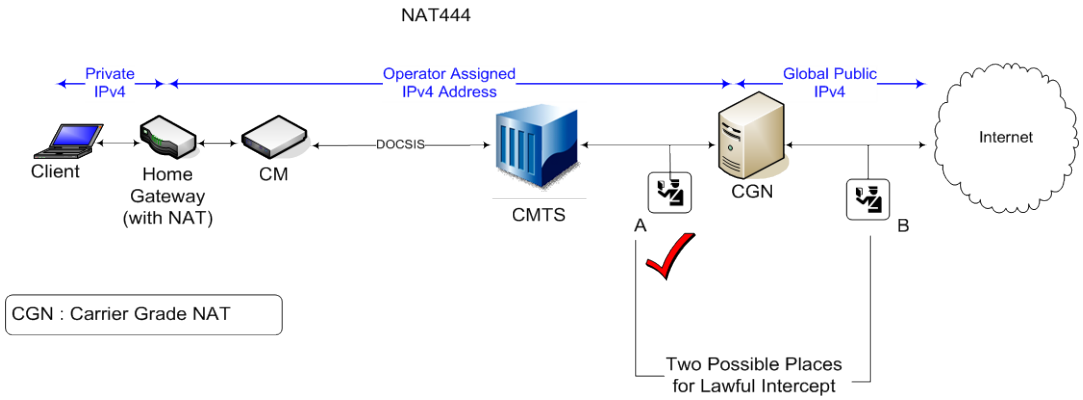

Figure 38 - NAT444: LI

NAT444 involves subjecting customer traffic to two levels of NAT translation: one at the customer home gateway, and one at the service provider CGN. The LI function can be implemented at either point A, located at the CMTS, or point B, located after the CGN function in Figure 38 above. At point A, customer IPv4 packets match an IPv4 five-tuple mapped to the customer CM, similar to current IPv4 lawful intercept. At point B, however, the source address is shared among multiple customers, so it will be difficult to map traffic to customer CM. The LI function would need to poll the CGN to obtain such a mapping.

Because interception at point A is similar to current operation and does not require complicated mappings across the CGN, the IPv6 team recommends performing inspection and interception at point A.

8.1.4.2 DS-Lite Lawful Intercept

This use case discusses LI when the customer is located behind a DS-Lite tunnel.

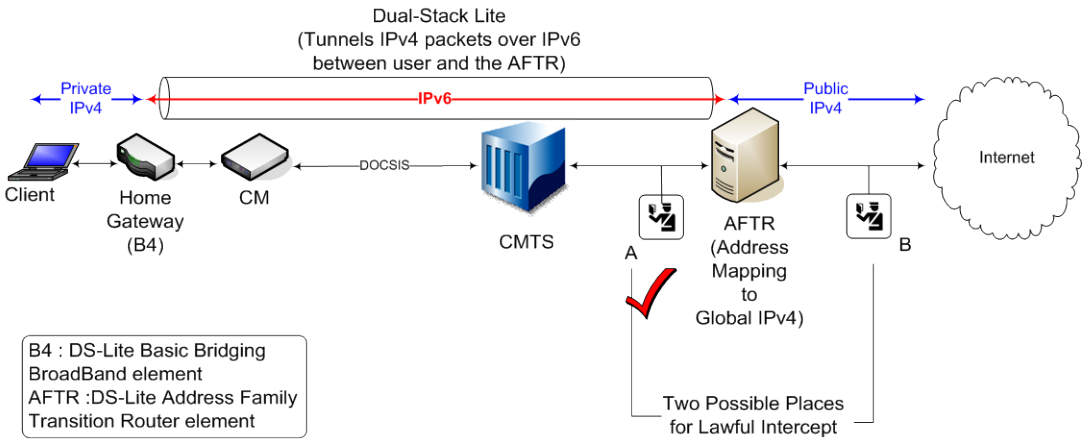

Figure 39 - DS-Lite: LI

DS-Lite encapsulates IPv4 traffic at a customer B4 device and transports it through IPv6 to a service provider AFTR, which decapsulates and translates the traffic. As with the previous use case, the LI function can be implemented at either point A, located at the CMTS, or point B, located after the AFTR function in Figure 39 above. At point A, IPv4 packets will be encapsulated within IPv6 headers that match a six-tuple tied to the customer CM. In this case, intercepted traffic will still be encapsulated, and the LEA will need to remove tunnel headers to access the data. At point B, the source address is shared between multiple customers, so it will be difficult to tie traffic to a specific customer CM. The LI function would need to poll the CGN to obtain such a mapping. As with the previous use case, because interception at point A is most similar to current operation and does not require complicated mappings across the AFTR, the IPv6 team recommends performing inspection and interception at point A. However, LEAs will need to process an extra layer of IPv6 headers in order to access the data.

8.1.4.3 6RD: Lawful Intercept

This use case discusses LI when the customer is behind a 6RD tunnel.

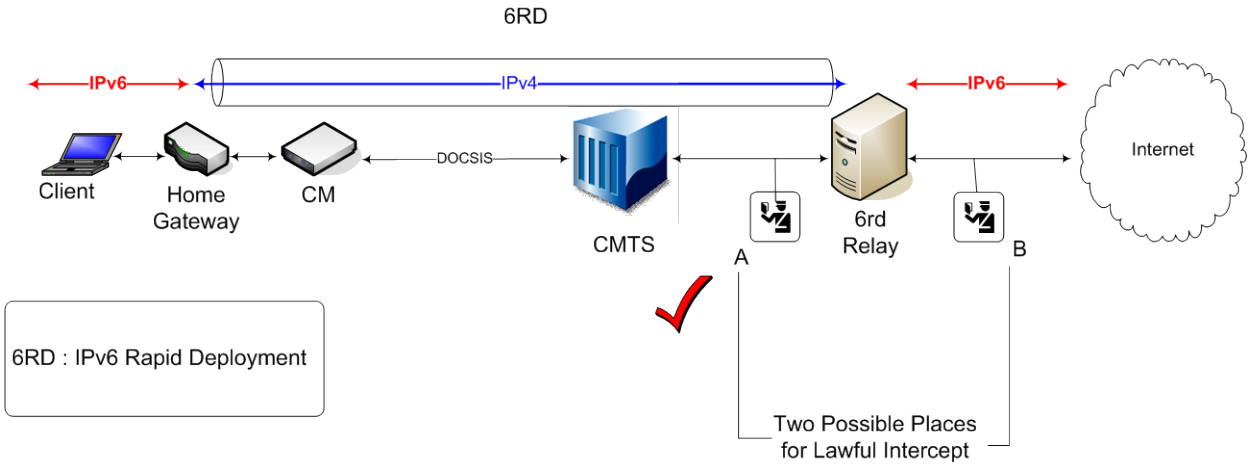

Figure 40 - 6RD: LI

6RD encapsulates IPv6 traffic at a customer home-gateway device and transports it through IPv4 to a service provider Border Router, which decapsulates the traffic. As with previous use cases, the LI function can be implemented at either point A, located at the CMTS, or point B, located after the 6RD relay/Border Router function

shown in Figure 40 above. At point A, the customer IPv6 packets will match an IPv4 five-tuple mapped to the customer CM. In this case, intercepted traffic will still be encapsulated, and the LEA will need to remove tunnel headers. At point B, IPv6 packets will be decapsulated and will match an IPv6 six-tuple tied to the customer CM (no NAT is required). Interception at point B would be similar to native IPv6.

As with the previous two use cases, because interception at point A is most similar to current operation, the IPv6 team recommends performing inspection and interception at point A. However, LEAs will need to process an extra layer of IPv4 headers in order to access the data.

8.1.4.4 General Guidelines for Data Lawful Intercept (LI) Placement

For all the three transition technologies discussed in this section, the IPv6 team recommends locating the intercept point at the CMTS, as this allows the greatest level of consistency with current operational practices across all three deployment scenarios.

8.2 PacketCable Electronic Surveillance Overview and IPv6 Accommodation

PacketCable Lawfully-Authorized Electronics Surveillance (LAES) defines requirements for intercepting voice traffic offered as part of MSOs' telephony service offerings. The LAES specifications require that both signaling information (call data) and media (call content) be captured.

8.2.1 PacketCable LAES Overview

As shown in Figure 41, the sections below introduce the concepts associated with PC LAES. Logically, these functions include the Intercept Access Function (IAF), Delivery Function (DF), Service Provider Administration Function (SPAF), Collection Function (CF), and Law Enforcement Administrative Function (LEAF). Our IPv6 analysis focuses on the Access, Delivery and Collection functions, as the Administrative Functions are out of scope.

8.2.1.1 Access Function

The Access Function is responsible for the collection of Call Content and reasonably available call-identifying information and making such information available to the Delivery Function. The Access Function is performed by the Intercept Access Points (IAPs), which isolates an intercept subject's communication or reasonably available call-identifying information unobtrusively. In a PacketCable network, many elements are designated as IAPs; see Figure 41 below.

The equipment and facilities of each subscriber include two IAPs (CMTS and S-CSCF). Call-Identifying Information reasonably available at these points is provided to the LEA. Redirected calls in the PacketCable network might not utilize the equipment or facilities of the subscriber who initiated the redirection. Accordingly, the IAP for a call that has been redirected will be either the S-CSCF/CMTS of the new destination (if redirected to another PacketCable endpoint within the same provider's network) or the MGC/Media Gateway of the PSTN interconnection (if redirected to a PSTN endpoint).

8.2.1.2 Delivery Function (DF)

The DF delivers the intercepted communication from the IAFs to the CF. It is responsible for ensuring privacy and timeliness. The DF collects and delivers Call Content (CC) and Call-Identifying Information (CII) for each intercept.

Once the DF obtains the Session Description Protocol (SDP) message, it sends a Control Point Discovery (CPD) message to obtain the IP address and protocol needed to complete the content tap. The DF configures the appropriate IAPs to set up the capture. Once it obtains data captures, the DF forwards them on to the CF.

8.2.1.3 Collection Function (CF)

The collection function is responsible for collecting intercepted CC and CII from the DF. The activation of this LEA-provided interface is the responsibility of the LEA Administrative Function. The CF is out of scope in the specification, as it is solely under the control of the LEA.

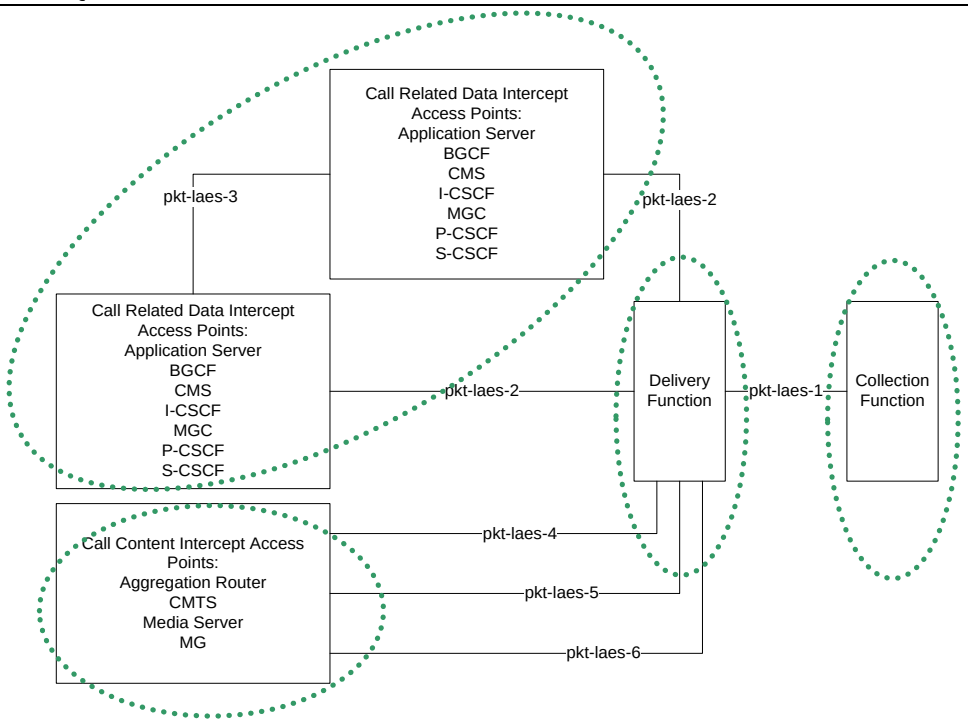

Figure 41 - PacketCable Lawfully Authorized Electronics Surveillance: Functions and Interfaces

The various interfaces between the Access, Delivery, and Collection Functions are shown in Figure 41 above, and summarized in Table 2 below.

Table 2 - PacketCable Internal LAES Interfaces

Reference Point	PacketCable Network Elements	Description
PKT-LAES-1	Delivery Function-Collection Function	Reported to Collection Function
PKT-LAES-2	Session Control Element-DF	DIAMETER based
PKT-LAES-3	Session Control Element-Session Control Element	Session Initiation Protocol (SIP) based
PKT-LAES-4	DF to Content Access Points	SNMPv3 based
PKT-LAES-5	Content Access Point to DF	Media over UDP based
PKT-LAES-6	DF to Content Access Points	Based on CPD

8.2.1.4 Interface between DF and CF

There are two main interfaces between the DF and the CF.

The Call Content Interface (CCC interface) captures the media with a timestamp. At this interface, the DF is required to support transcoding of the media to G.711. If requested, the DF can disable transcoding on a per-intercept basis. The media is captured with the original IP, UDP, and RTP headers, along with the payload.

The Call Data Collection (CDC) Interface captures events, such as call originations and call terminations, and also captures feature use for features including call waiting, call holding, and call transfer.

When the customer is behind any kind of tunnel technology, the tunnel adds a layer of headers, which can obfuscate traffic and require deep packet inspection to perform transcoding.

8.2.1.5 Intercept Access Points

Many different elements in the PacketCable network function as the intercept access points. The call-related data intercept access points are the P-, I-, S-CSCF (Call session control function), Media Gateway Controller (MGC), and Home Location Register (HLR). The call content intercept access points are the CMTS, MG (media gateway), media servers, and aggregation routers.

Note that in [CBIS], the access point is site-specific, whereas in PacketCable LAES, the access point is well-defined. The IAPs report call-related data to the DF as Intercept Event Messages, such as 'Report', 'Correlate', or 'Carrier-Info' messages. See Figure 42 below, for a simple overview of where lawful intercept takes place within the PC 2.0 network.

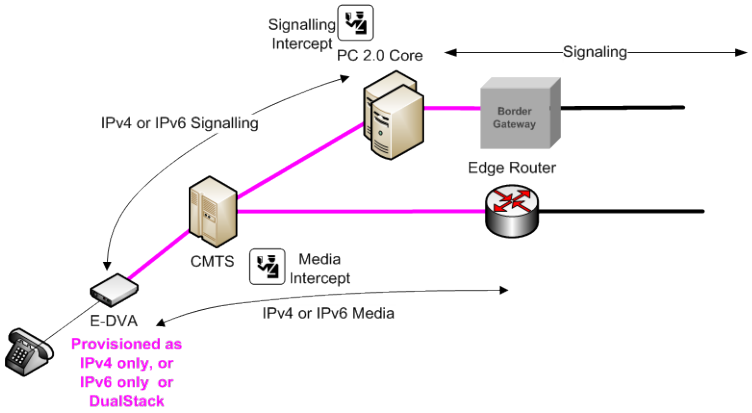

Figure 42 - Intercept Points, a Simple Overview

8.2.1.6 Call-Related Data Intercept Invocation

The call data information is sent between PacketCable network elements and the DF using Diameter accounting messages. The Diameter protocol (derived from RADIUS) is a client/server Authentication, Authorization, and Accounting (AAA) protocol. The protocol uses Accounting Request (ACR) messages, which are used to send surveillance call data messages from network elements to the DF, and Accounting Answer (ACA) messages, which are used to acknowledge an ACR.

8.2.1.7 Call Content Intercept Invocation

Invocation of call content intercept includes two steps: first is the dynamic discovery of the IAP, and the second is configuration of the TAP MIB on the IAP.

The discovery of the Content IAP is done using the Control Point Discovery (CPD) mechanism. The Delivery Function sends a CPD request message to the destination IP address of the media endpoint. The Content IAP responds with the IP address used to request the TAP MIB for content tapping along with an identifier that indicates which protocols to use.

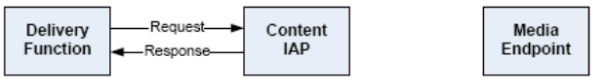

Figure 43 - Content IAP Discovery

As soon as the Delivery Function obtains the SDP and uses CDP to obtain the IP address and protocol to do the content tap, it uses the address of the media endpoint in order to set up the filter specification for content tapping per the TAP MIB. The filter specification is an IP protocol classifier that describes packets that need to be replicated, encapsulated, and transported. The setup includes configuring the interface with the destination IP address of the DF to which it should send the call content, format, transport, and call content identifier for the call to be intercepted.

The operator can specify the duration for the intercept. To set up the call content intercept, the operator creates an entry in the TAP MIB; the MIB is detailed in the PC LAES specifications.

8.2.2 IPv6 Support in PC LAES

This use case makes the following assumptions about the operator PacketCable 2.0 deployments. The MSO PacketCable 2.0 Voice network is assumed to be IPv4, IPv6, or dual-stack capable using native IP connectivity. Specifically, NAT444, DS-Lite, and 6RD will not be used for E-DVA traffic. Only Softphone traffic that traverses the data network might use such transition technologies.

IPv6 support is already available in the current CableLabs PacketCable LAES specifications. Currently, the PacketCable LAES specification defines a filter that matches the five-tuple of source IP address and prefix, destination IP address and prefix, source port range, destination port range, and protocol of packets to be captured for both IPv4 and IPv6 traffic. The TAP MIB defined for the IAPs accepts both IPv4 and IPv6 addresses. The LAES specification supports native IPv4, native IPv6, and dual-stack E-DVAs.

8.2.3 Transition Technology Impact on Softphone Lawful Intercept

An IP Softphone is a telephony application running on a PC (e.g., Skype or an MSO-provided phone client). Voice traffic goes "over the top" of the data network, and is not segmented, as with E-DVA traffic. Since Softphone traffic is transmitted in the regular data stream with other host traffic, IPv6 transition technologies such as DS-Lite, NAT444, and 6RD will impact LI for the Softphone use case.

8.2.3.1 Softphone with NAT444

This use case discusses LI when the Softphone is behind a NAT444 deployment.

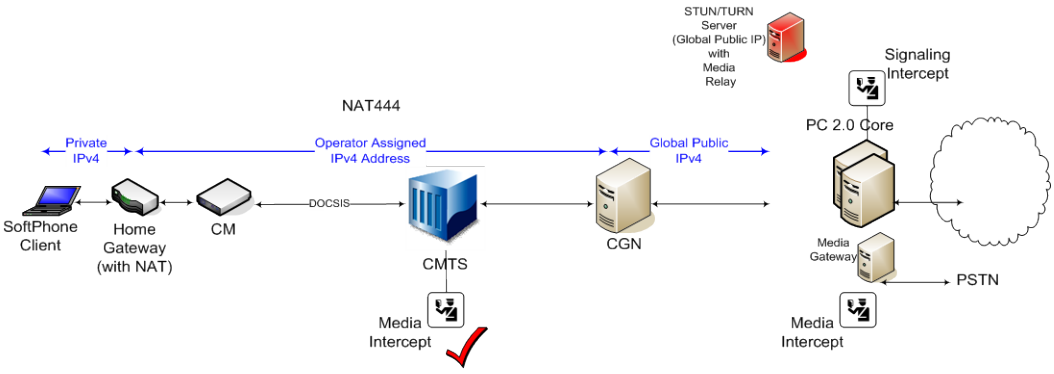

Figure 44 - Softphone with NAT444

In a network (such as the one depicted in Figure 44 above), when the user initiates a call while LI is enabled, the signaling messages traverse both the NAT at the home gateway and the CGN on the service provider network before reaching the IMS Core, where they are intercepted. The media traverses one NAT and is intercepted at the CMTS/Media Gateway. If the PacketCable 2.0 core is outside of the CGN, then the DF needs to ask the CGN for the mapping to enable CMTS to capture the appropriate media. If the PacketCable 2.0 core is located between the CMTS and CGN, the DF does not need to determine the NAT translation mapping, as both the IMS core and CMTS see the same IP address. Likewise, if the Media Gateway is on same side of the CGN as the PacketCable 2.0 Core, the DF does not need to determine translation mappings, but can simply direct the IMS core and media gateway to intercept the same call.

8.2.3.2 Softphone with DS-Lite

This use case discusses LI when the Softphone is behind a DS-Lite deployment, as depicted in the Figure 45 below.

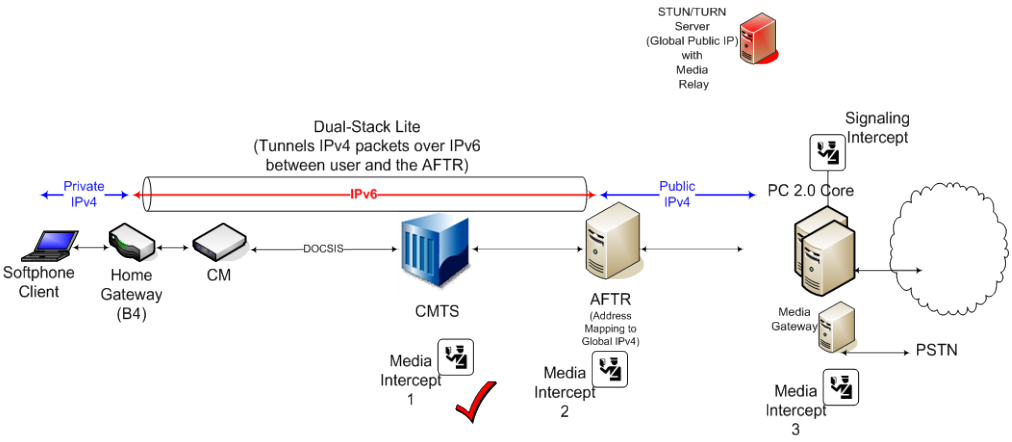

Figure 45 - Softphone with DS-Lite

When the user initiates a call with LI enabled, the signaling messages traverse the DS-Lite tunnel, are translated at AFTR, and then reach the IMS Core where they are intercepted. Likewise, the media is encapsulated at the home gateway B4 function, and can be intercepted at the CMTS (1), AFTR (2), or Media Gateway (3). If the intercept function is located at point 1, the DF needs to ask the AFTR for the translation mapping to enable the CMTS to capture the appropriate media. If the CMTS was required to transcode the media at this point, it may need to decapsulate such traffic first. If the media intercept point is located at points 2 or 3, and if Media Gateway is on the same side of the AFTR as the PacketCable 2.0 Core, the DF would not need to examine translation mappings, and the intercept point would not need to decapsulate traffic, as it would already appear as unencapsulated IPv4.

8.2.3.3 Softphone with 6RD

This use case discusses LI when the Softphone is behind a 6RD deployment.

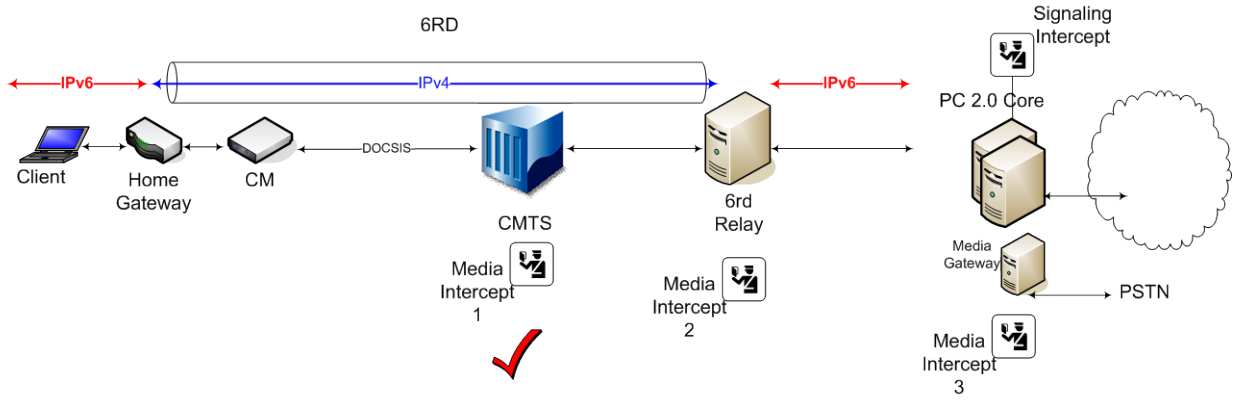

Figure 46 - Softphone with 6RD

When the user initiates a call with LI enabled, IPv6 signaling messages are encapsulated as they traverse the 6RD tunnel, and then reach the IMS Core where they are intercepted. Likewise, the media is encapsulated in IPv4 at the home gateway 6RD function, and can be intercepted at the CMTS (1), Border Router (2), or Media Gateway (3). If the intercept function is located at point 1, the DF needs to ask the BR for the IPv4-to-IPv6 mapping to enable the CMTS to capture the appropriate media. If the CMTS were required to transcode the media at this point, it may need to decapsulate such traffic first. If the media intercept point is located at points 2 or 3, and if Media Gateway is on the same side of the BR as the PacketCable 2.0 Core, the DF would not need to examine tunnel mappings, and the intercept point would not need to decapsulate traffic, as it would already appear as unencapsulated IPv6.

8.2.4 Analysis

The PacketCable LAES specification addresses support for native IPv4 and IPv6 E-DVA lawful intercept use cases, and the placement of the intercept access points are well known.

The Softphone use cases, however, require consideration of the placement of the intercept points and the PacketCable 2.0 core in relation to the CGN, AFTR, and/or BR. In all three cases, it is desirable to intercept media at the CMTS, as is done in current IPv4 practice. For NAT444, this is fairly straightforward. The PacketCable core should be located on the same side of the CGN as the CMTS, and Softphone traffic should proceed without translation. For the two tunnel cases (DS-Lite and 6RD), this placement is more complicated. Provided that it meets with LEA needs, MSOs desire to intercept encapsulated traffic at the CMTS and hand off the captured data to law enforcement for decapsulation and processing. If this approach is insufficient for law enforcement needs, then MSOs believe that the intercept point should be located at the AFTR/BR (point 2).

8.3 Data/Record Storage

There is no legal requirement for retroactive storage of network address translation mapping of customer IP addresses for customers behind a CGN or DS-Lite translation function. Any data collection or data record retention is based solely on MSO business needs. The Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA®) requires that service providers implementing the Broadband Intercept Function store 24 hours of intercept data. If the operator is not implementing the BIF, this requirement only applies to the LEA itself, and there are no additional requirements on service providers. Also, under the Digital Millennium Copyright Act (DMCA), there are no data storage or data record storage requirements imposed on operators.

9 TECHNICIAN AND OSS ACCESS USE CASES

Technician and OSS access refers to the ability of MSO technicians and OSS systems to monitor and manage IPv6 CMs/E-DVAs/eSTBs over IPv4/IPv6 networks. This section examines various use cases that fall under this topic. A few assumptions are made for the purpose of this discussion.

9.1 Assumptions

The following assumptions apply to the use case discussion in this section.

1. CM/E-DVA/eSTB is IPv6-only.
2. CMTS, headend and MSO core are dual-stack.
3. MSO corporate network is IPv4-only or dual-stack.
4. Web portal and back office could be IPv4-only or dual-stack
5. No transition mechanism exists between the CM/E-DVA/eSTB and the MSO core-

9.2 Network Diagram

The network diagram shown below applies to all the use cases discussed in this section. The MSO core and the headend are both dual-stack. The customer equipment is IPv6 only.

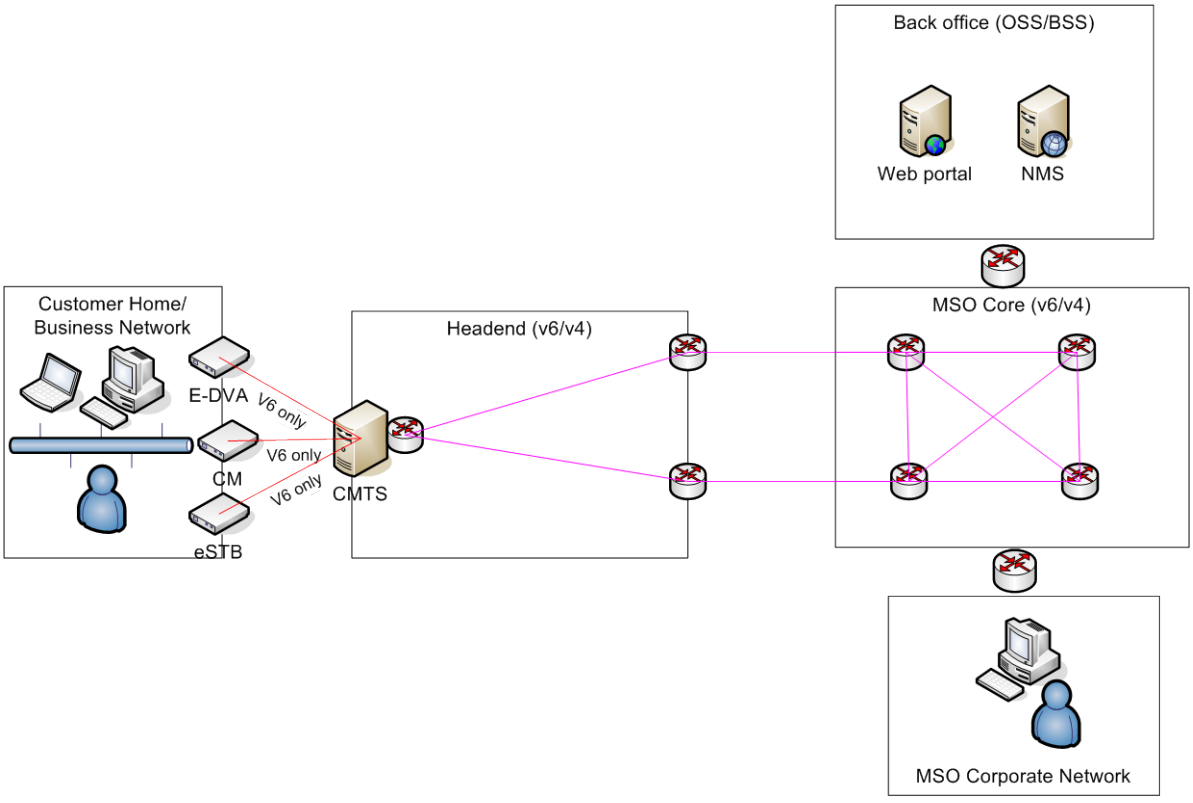

Figure 47 - Technician Access Overview

9.3 Overview of Use Cases

The Technician and OSS access use cases can be organized into the following primary categories:

1. Direct Technician Access
   - The technician accesses the CM directly (from the MSO corporate network).
   - The technician accesses the eRouter at the customer Home.
2. Indirect Technician Access
   - The technician from the MSO corporate network connects to a back office component, which in turn connects to the CM.
3. Back office automated systems access to CM
   - Automated systems that reside in the MSO back office access the CM without a stimulus from the technician.

The following subsections delve into the details of each of these use case categories.

9.4 Direct Technician Access Use Cases

This category consists of use cases where the technician accesses the CM directly (from the MSO corporate network). The category of direct technician-access use cases consists of the following scenarios:

- Technician has dual-stack connectivity
- Technician on IPv4-only MSO corporate network communicating with IPv6-only CM

In-home technician access to an eRouter device forms another use case in this section.

The following subsections examine these use cases in more details.

9.4.1 Technician with Dual-Stack Connectivity

The network diagram for this use case is shown below, and details follow.

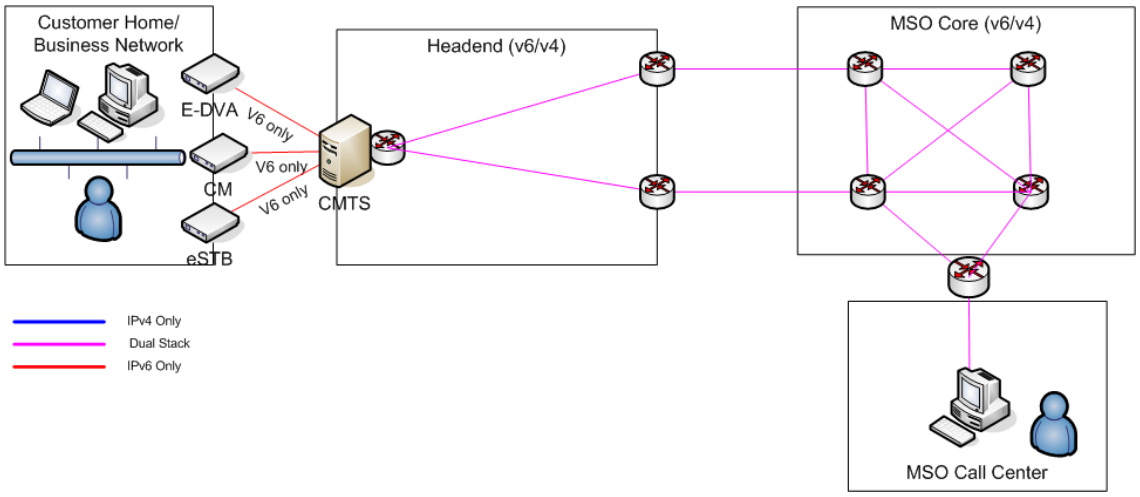

Figure 48 - Direct Technician Dual-Stack Access

In this use case, the technician has IPv4/IPv6 connectivity. The MSO core and headend network support IPv4/IPv6. The CM supports IPv6 only. The technician opens tools on PC and connects directly to the CM using IPv6. This assumes that the tools support IPv6. The use of IPv4-only tools is covered in back office use cases.

9.4.2 Technician on IPv4-only Network

In this use case, the technician on an IPv4-only network needs to access IPv6-only CM. If the technician has only IPv4 tools, they will need to connect through back office (covered below). If technician has IPv6 tools on PC, the preferred solution is to use tunneling. The most commonly used mechanisms for tunneling are Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) and 6RD/GRE. These are covered in more details in the sub-sections.

9.4.2.1 Tunneling Using ISATAP

The network diagram for this use case is shown below and details follow.

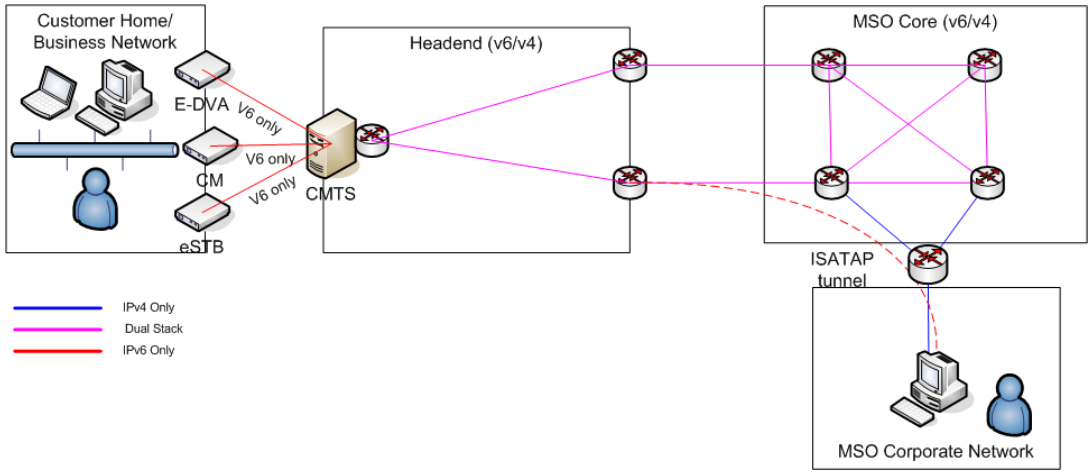

Figure 49 - Tunneling Using ISATAP

ISATAP is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network. It is useful in MSO networks when technicians have dual-stack PCs, but IPv4-only network connectivity.

ISATAP is supported in Windows XP and greater. MAC OS requires Miredo software package. The client uses DNS to determine the router address.

ISATAP is supported on many router/server platforms (e.g., Cisco and Linux).

As an example, the typical steps to configure an ISATAP Router on Linux are:

- ip tunnel add is0 mode isatap local 192.168.222.130 ttl 64
- ip link set is0 up
- ip addr add 2001:1890:1109:4102::5efe:192.0.2.1/64 dev is0
- sysctl net.ipv6.conf.all.forwading=1
- service radvd restart

As another example, the typical steps to configure an ISATAP Router on Cisco IOS are:

- interface tunnel 1
- ipv6 address 2001:0DB8:6301::/64 eui-64

- no ipv6 nd ra suppress
- tunnel source gig1/0/1
- tunnel mode ipv6ip isatap

The network operator needs to add an A record in DNS server for isatap.mydomain.com.

9.4.2.2 Tunneling Using a Gateway

The network diagram for this use case is shown below and details follow.

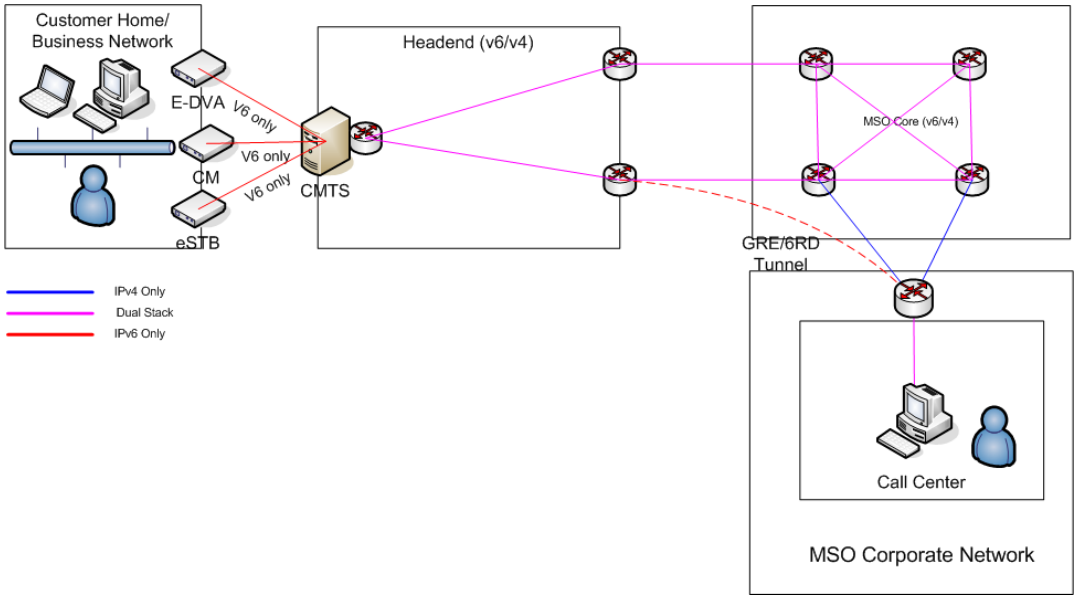

Figure 50 - Tunneling Using a Gateway

A gateway mechanism based on 6RD or GRE would be useful in certain cases. For example, the MSO call center could be IPv6-enabled before the rest of the corporate network. The gateway at the edge of the call center network may support IPv6 tunnel (6RD/GRE). The technician PCs support dual-stack.

6RD is useful when there are many sites and manual configuration is a challenge. GRE is useful when there are few sites and manual configuration is acceptable.

As an example, the typical steps to configure 6RD tunnels on Cisco routers are:

- interface tunnel tunnel-number
- ipv6 address {ipv6-address/prefix-length | prefix-name sub-bits/prefix-length}
- tunnel mode ipv6ip 6rd
- tunnel 6rd prefix ipv6-prefix/prefix-length
- tunnel 6rd ipv4 {prefix-length length} {suffix-length length}

As an example, the typical steps to configure GRE tunnels on Cisco routers are:

- interface tunnel tunnel-number
- ipv6 address {ipv6-address/prefix-length | prefix-name sub-bits/prefix-length}
- tunnel source {ip-address | ipv6-address | interface-type interface-number}

- tunnel destination {host-name | ip-address | ipv6-address}
- tunnel mode gre ipv6

9.4.3 In-Home Access to eRouter

This use case discusses how an on-site technician can get access to eRouter Web UI to debug issues or configure service in the customer home. A DOCSIS CM supports SNMP access via the CMCI port. The CM supports 192.168.100.1 as the well-known diagnostic IP address accessible only from CMCI interfaces. The eRouter, on the other hand, does not have such requirements.

9.4.3.1 Outline

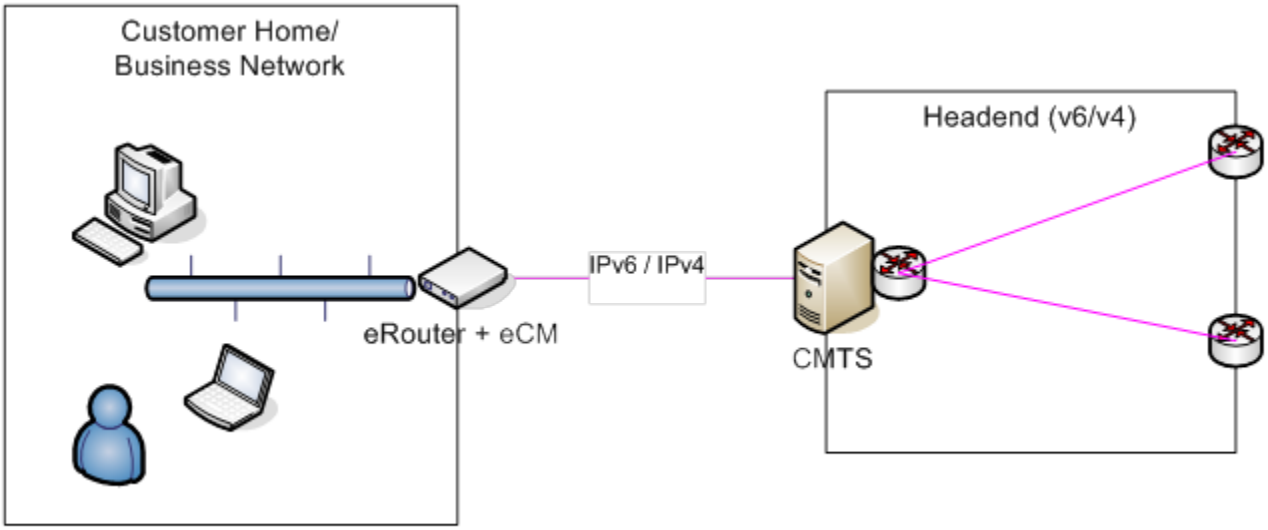

Figure 51 - In Home access to the eRouter

There are four main options for assigning an eRouter LAN Address for in-home access by a technician.

1. IPv6 Globally Unique Address (GUA)
2. IPv6 Unique Local Address (ULA)
3. IPv6 Link Local Address
4. IPv4 [RFC1918] Address

The IPv6 Globally Unique Address works only when there is an operational WAN connection. This address is operationally not advisable, as there are issues when IPv6 address cannot be renewed by eRouter. If the eCM/eRouter does not have an IP connection to the network, then the eRouter will not obtain a prefix and will not be able to delegate any addresses within the home.

The IPv6 ULA (Unique Local IPv6 Address, [RFC4193] [RFC4193]) is not advisable at this time as the use of ULAs has been reported to cause IPv6 brokenness with dual-stack servers. In the field, IPv6 brokenness is bad behavior seen in tunneled or dual-stack IPv6 deployments where unreliable or bogus IPv6 connectivity is chosen in preference to a working IPv4 connectivity. This often results in long delays, where the user has to wait for the attempted IPv6 connection to time out before using the IPv4 connection.

The IPv6 link -local address does not also fit as a solution for in-home access. It is difficult to work out the eRouter's Management address as it is based on the EUI-64 address, and the technician would need to be on the same VLAN to establish connectivity. The link-local IPv6 address also creates other difficulties when entering the eRouter link-local address into a browser. There is an interface number associated with each link-local IPv6 address that must be included for connectivity via a link-local IPv6 address.

The IPv4 private address [RFC1918] remains the most viable option. It is the traditional connection model, is well known, currently works, and is used by technicians all the time.

9.4.3.2 Recommendation

In the short term, the recommendation is to use IPv4 addresses to access the eRouter. In the long term, the recommendation would be to use IPv6 ULA when host operating systems are fixed; see [RFC6555]. Using IPv4 will remain workable in the long term.

9.5 Indirect Technician Access

In the use case, the technician connects to a back office component, which in turn connects to the CM. The web portal and back office components must be dual-stack. The network diagram is shown below and the details follow.

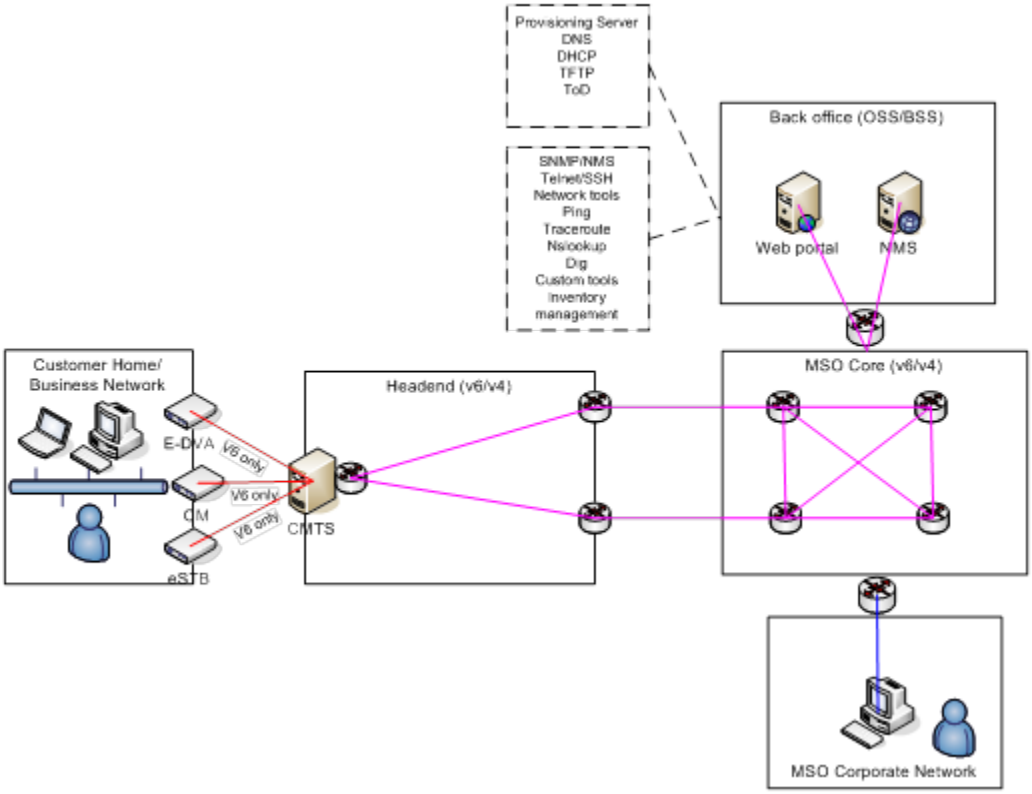

Figure 52 - Indirect Technician Access

In the use case, the technician manually accesses the CM through the back office. The technician connects to the back office system using IPv4/IPv6. The technician then uses dual-stack B/OSS tools to access customer IPv6 devices. The technician could use IPv6 literals or DNS to address the customer IPv6 CM.

When using IPv6 literals, the following considerations apply. Some tools (e.g., telnet) can handle either address family. Some tools have different versions for IPv4 and IPv6 (e.g., ping6, traceroute6). Technician training would be needed for IPv6 versions. Another option is to develop custom scripts that determine address family and call the appropriate version of the tool.

When using DNS, the following considerations apply. The tools supporting dual-stack use DNS to determine address family. The tools perform DNS lookup and calls IPv6/IPv4, depending on the type of record (AAAA or A respectively). Single-stack tools may require a wrapper to support IPv4/IPv6.

Another scenario is where the technician or customer accesses the web portal to connect to customer devices. The technician or customer can use IPv4 or IPv6 to access the portal. The web portal supports dual-stack and in turn uses IPv6 to connect to customer devices. This is discussed in Section 7.1 of this document.

9.6 Back Office Access to CM

In this use case, the automated back office systems (OSS/BSS) connect to the customer device. This case is similar to the manual technician B/OSS access use case explained above. The automated systems support dual-stack and use IPv6 literals or DNS. The tools determine appropriate address family and connect accordingly.

Custom tools developed by the service provider may need software updates. Two examples of areas of impact are shown here.

- Memory - IPv6 address binary uses 128 bits versus 32 bits for IPv4 address. The IPv6 address string uses 39 characters versus 15 for IPv4 address string.
- Databases - fields must support IPv6 addresses or domain names in addition to IPv4.

Owen Delong's "Porting IPv4 applications to IPv4/IPv6 dual-stack" presentation explains many of the considerations for updating applications to support IPv6. The presentation can be found at the following link:

- http://www.rmv6tf.org/presentations2010.htm

9.6.1 B/OSS Tools with IPv6 Support

The following is a snapshot of IPv6 support in B/OSS tools as of December 2010.

The following network tools support IPv6:

- Ping6,Traceroute6, nslookup, telnet, ssh

The following OSS tools support IPv6:

- IBM Netcool
- IBM Proviso
- Alcatel-Lucent SAM
- HP Openview with smart plug-in for advanced routing
- Cisco Works
- MG-Soft SNMP Manager

The inventory management tool, Telcordia Granite, supports IPv6. BMC Remedy does NOT currently support IPv6.

10 VIDEO USE CASES

Video services covered in these use cases include the delivery of video content, regulatory services, and applications. Video content is delivered from programmers to subscribers, and the use cases involve receiving content from the programmers, delivering video across multiple headends (often across the nation), distributing video to subscribers, and ultimately distributing video within the subscriber home. Regulatory service primarily refers to emergency alert systems (EAS) at this time. The applications that are being delivered in these use-cases include set-top applications, such as those found in Tru2Way and EBIF, as well as advanced advertising.

10.1 DOCSIS Set-top Gateway (DSG)

DSG (DOCSIS Set-top Gateway) transports Out-Of-Band (OOB) messaging between a Set-top Controller (or application servers) to an eSTB (OpenCable Host) over DOCSIS. Set-top devices use an IP session over DOCSIS for all return traffic. The DSG needs to work on both one-way (e.g., downstream-only) and two-way plant. The OOB messaging can include the channel guide, application information, Common Download, DRM, and more. The data carried within DSG Tunnels includes [SCTE65] MPEG 2 Sections, [SCTE18] Emergency Alert Messaging for Cable, OpenCable Common Download Carousel, OCAP Extended Application Information Table (XAIT) () and/or CVT (Code Version Table) data. This data is carried within DSG tunnels, which are multicast in nature. The DSG eCM receives IPv4 Multicast Tunnels. Each DSG Tunnel encapsulates IP Multicast datagram in DOCSIS frame. The destination MAC address of DSG Tunnel is known as "DSG Tunnel Address".

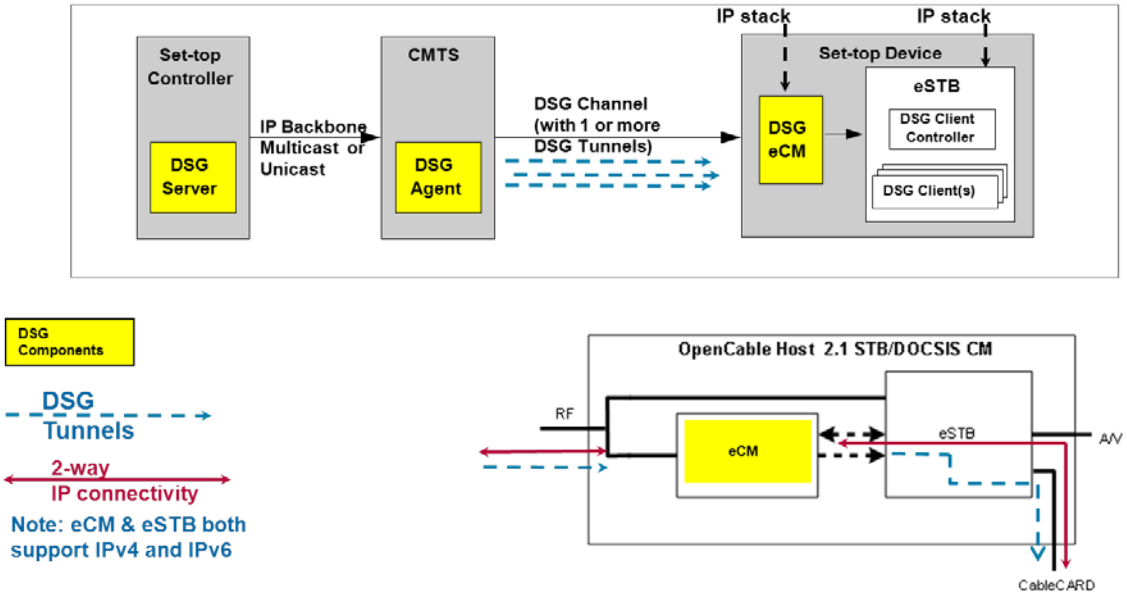

Figure 53 - DSG Components

10.1.1 DSG and MDD Provisioning Mode

DSG is capable of one-way and two-way operation. In one-way mode, it consumes DSG Tunnels, but has no upstream connection; in two-way mode, there is both upstream and downstream IP connectivity. The DSG eCM can switch between one-way and two-way modes as the plant conditions change. One-way mode has implications for IP Provisioning Mode; the behavior of DSG devices has been made consistent with standalone CMs (see Section 5.9). The DSG eCMs are required to re-read MDD when exiting one-way operation state. The MDD provisioning mode is applicable to both D3.0 and D2.0+IPv6 DSG eCMs.

10.1.2 DSG Tunnels and IPv6

The DSG Team has evaluated use of IPv6 for DSG Tunnels and agreed to continue using IPv4 for DSG Tunnels. Tunnel addresses do not need to use IPv6, even if the eCM uses IPv6 for management, because there is sufficient IPv4 Multicast Address space, and DSG is only transporting tunnel data. Additionally, it is possible to terminate IPv4 DSG tunnels to a device even when the eSTB is in IPv6-only mode.

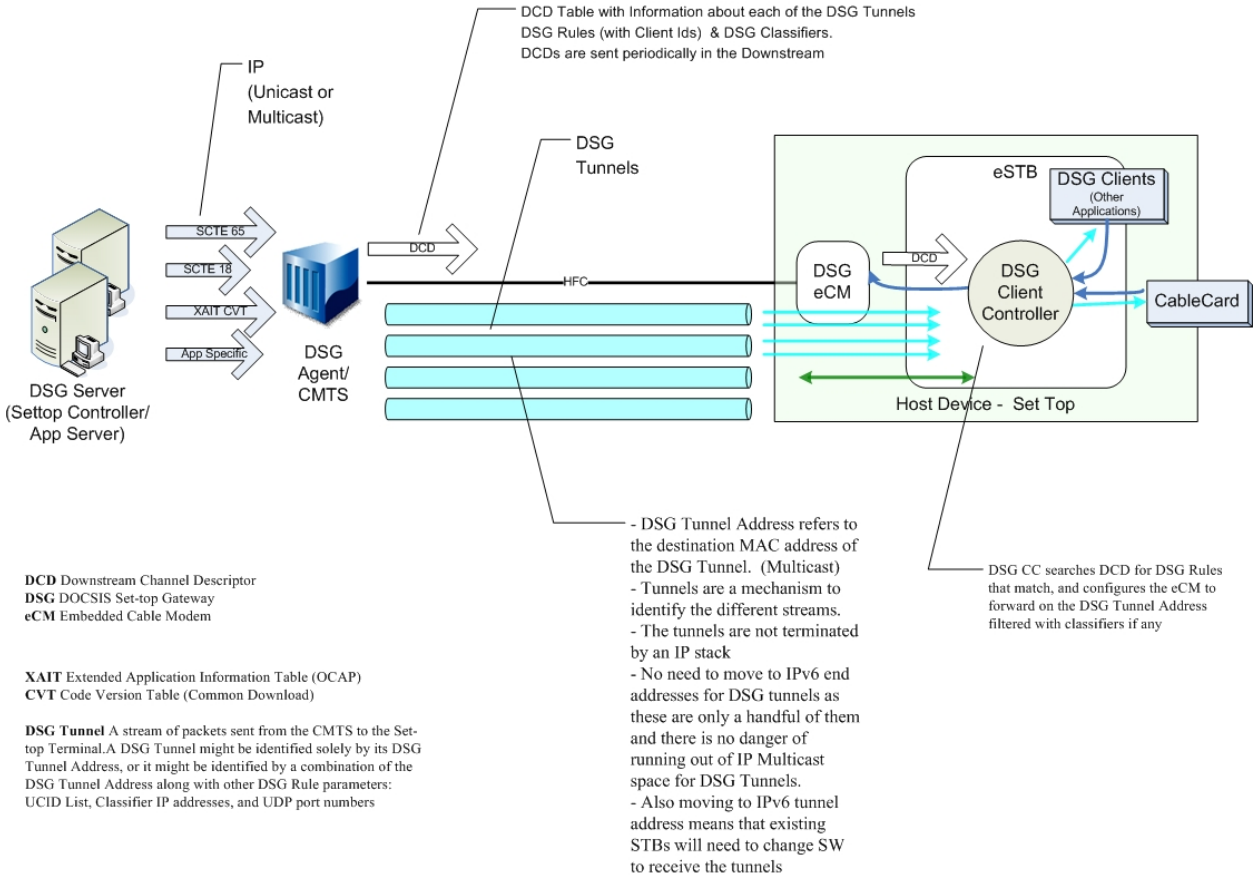

Figure 54 - DSG Tunnels terminating on an eSTB

Therefore, the proposed transition plan suggests the use of IPv4 multicast addresses for DSG Tunnels even after the CM and eSTB migrate to IPv6.

10.1.3 Proposed Transition Plan for DSG

MSOs are following different strategies in their migration to IPv6. One logical transition plan to IPv6 for set-top devices was discussed and is described as follows:

As a first step, the DSG CMs are migrated to IPv6 addresses. As a next step, eSTB addressing can be migrated to IPv6; this is a more complicated transition, as MSO applications would need to support IPv6 prior to STB migration. As mentioned before, the DSG Tunnels continue to use IPv4 multicast addresses.

10.2 IP Simulcast (IPS)

IP Simulcast (IPS) describes architectural and technology alternatives for delivering video content to IP devices. Currently, CableLabs does not have any interface specification for the IPS architecture. The details about the

interfaces discussed in this section can be found in the IPS technical report, "IPS Video Delivery and Gateway Model."

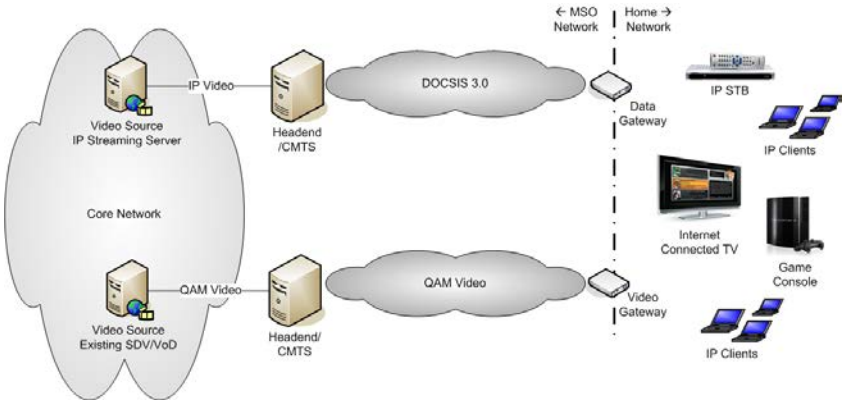

Figure 55 - IPS video Delivery Model

Video can be delivered through the Access Network either via legacy MPEG channels or via IP. In-home delivery of video uses the following IP-based technologies: Open Cable Home Networking [OCAP-HNEXT], Digital Living Network Alliance, and Universal Plug-n-Play(DLNA/UPnP) or HTTP Streaming.

The IPS technical report defines two models of IPS gateway:

- Data Gateway (D-GW) where video is delivered over IP in the access network and in the home
- Video Gateway (V-GW) which uses QAMs to receive video in the access network while delivery remains IP in the home.

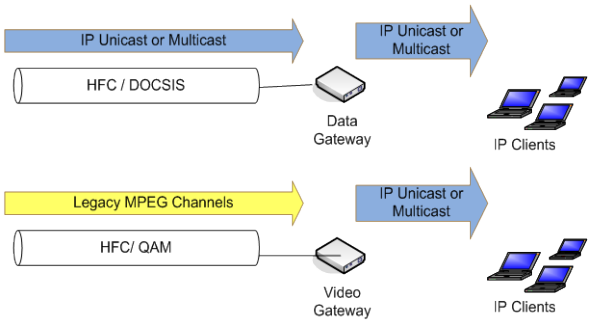

Figure 56 - IPS video deliver models

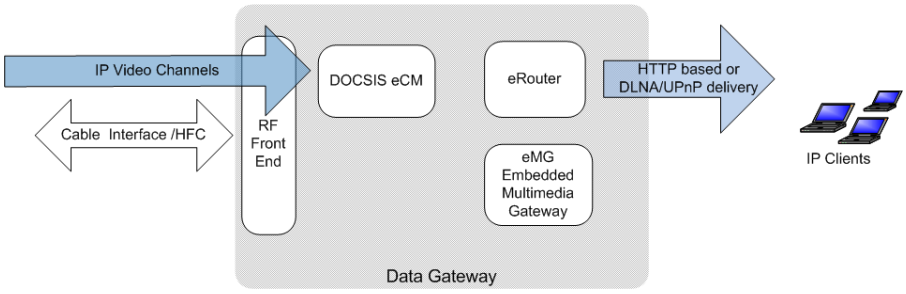

Figure 57 - IPS Data Gateway (V-GW) Reference Model

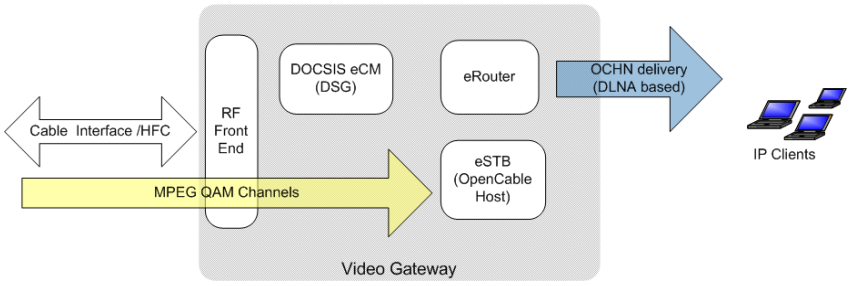

Figure 58 - IPS Video Gateway (D-GW) Reference Model

MSOs are developing their own individual product requirements; thus, our analysis is based on a current technical report on IPS, and may differ from what each MSO actually plans on deploying. There is no CableLabs specification describing the Gateway requirements and architecture.

10.2.1 IPv6 Impacts for IPS

IPS video delivery in the access network could be Multicast (either IPv4 IGMP or IPv6 MLD) or Unicast (IPv4 or IPv6). If the access network components can support IPv4 or IPv6, then the video transport over the access network can use either IPv4 or IPv6 up to the gateway in the home. The transport in the access network is independent of the IP version supported within the home network.

In the home network, IPS video delivery is usually done via Unicast (IPv4 or IPv6), but could also be Multicast, or streamed through OCHN/DLNA/HTTP. When Multicast is used in the home, support for IGMP-proxy (IPv4) or MLD-proxy (IPv6) is needed. OCHN, DLNA, and UPnP will be covered in subsequent sections in more detail.

The suggestion is to support dual-stack on V-GW and D-GW.

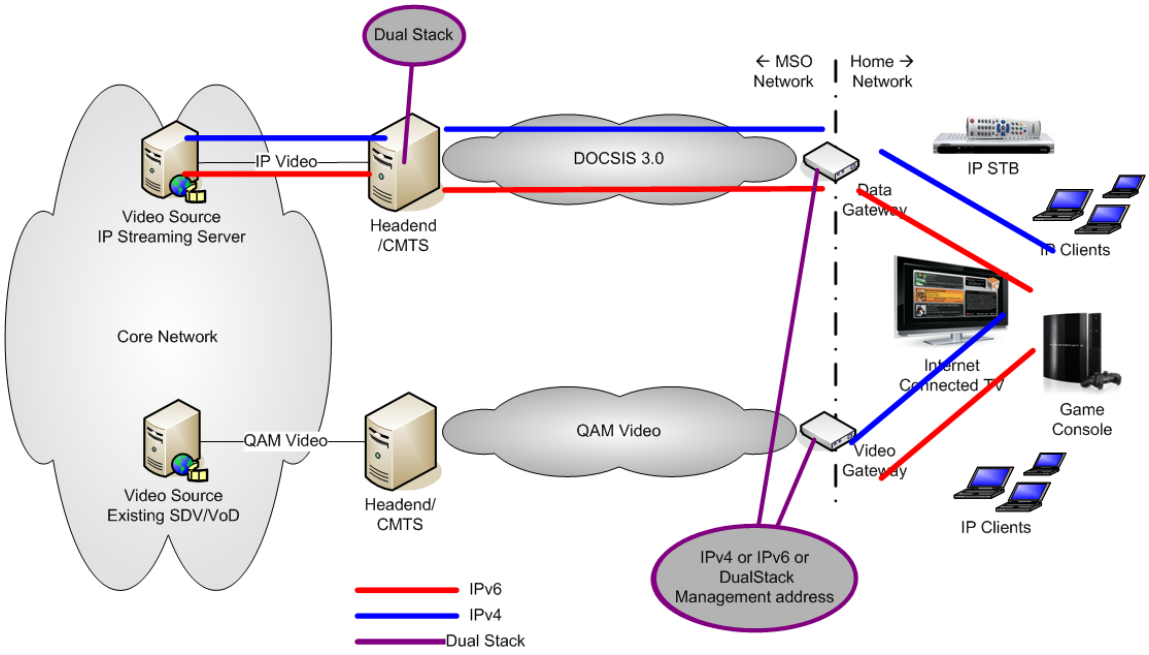

Figure 59 - IPv6 Impacts across the IPS Network

10.3 Emergency Alert System (EAS)

The EAS is a nationwide system for distributing emergency alerts through cable television systems and other public broadcasting systems. EAS support and cooperation is legally mandated for broadcast and cable television services. Traditionally, EAS alerts are received either over VHF radio (national EAS) or via telephone. The alerts are then transmitted to subscribers through legacy video/out-of-band, or via DSG or IPS.

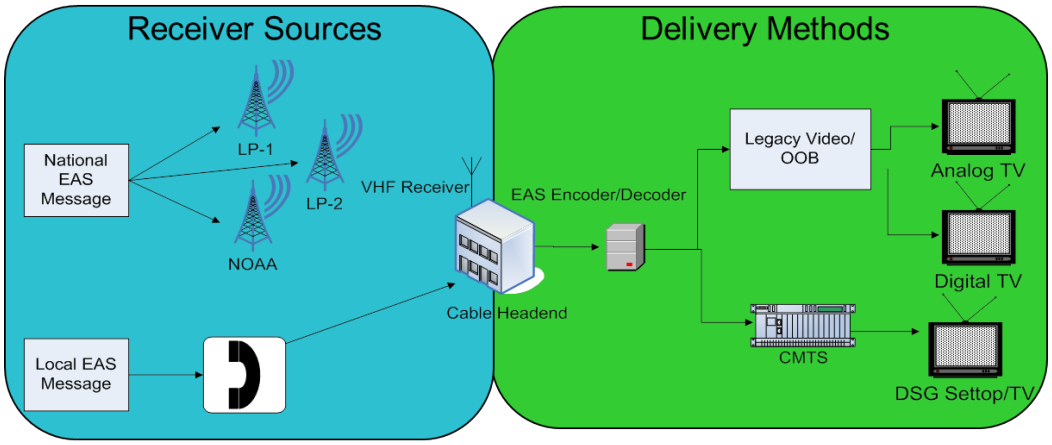

Figure 60 - Current/Legacy EAS Architecture

FEMA has adopted a new, next generation EAS called Common Alert Protocol (CAP). This is an XML-based protocol that will facilitate the transmission of alert messages in multiple formats (e.g., text, audio, and video). It also facilitates transmission of messages to persons with disabilities and non-English speakers. The FCC mandated support for CAP by 30 September, 2011. CAP does not affect the transmission of alerts to subscribers, only how they are received from authorities.

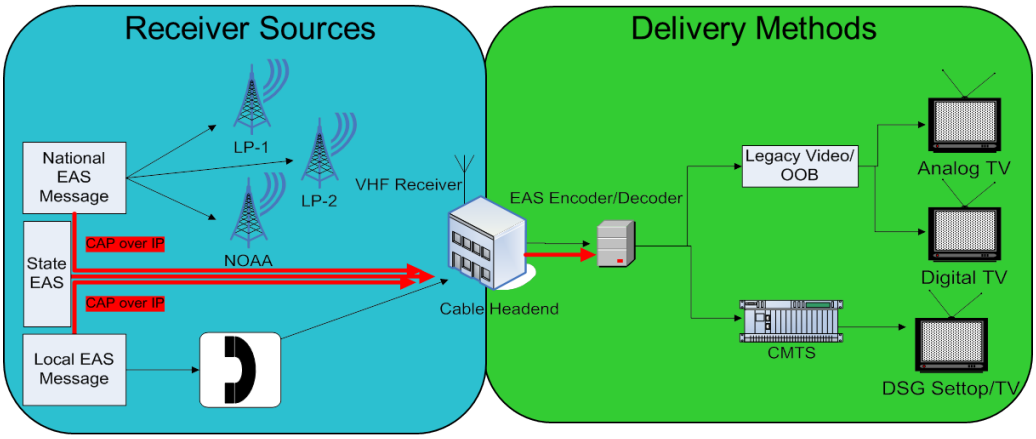

Figure 61 - Future EAS/CAP/IPAWS Topology

10.3.1 IPv6 Implications for EAS

In the current/legacy EAS, IPv6 implications are limited to subscriber delivery, and are the same implications as any other OOB information (Section 10.1.1, DSG and MDD Provisioning Mode).

When migrating to CAP EAS, the CAP receiver may need to be IPv6, IPv4, or dual-stack. In the following table, IPv6 impacts on EAS for IPS should be the same as identified for video delivery (Section 10.2.1, IPv6 Impacts for IPS).

Table 3 - EAS IPv6 Impacts

	Headend	Access	Home
V-GW Model	Signal receiver (EAS enc/dec) may need to support IPv4, IPv6, or dual-stack	Same impacts as identified for DSG	Support for EAS in DLNA, UPNP and OCHN (e.g., support for IPv4 and IPv6)
D-GW Model	Same as above	EAS/CAP delivery over IP (IPv4 or IPv6)	Support for EAS in DLNA and UPNP (e.g., support for IPv4 and IPv6)

10.4 In-Home Video Delivery

The objective of this section is to identify areas of impact to in-home video delivery when transitioning to IPv6. This includes looking at several enabling technologies.

10.4.1 Universal Plug and Play (UPnP)

UPnP is a simple, ad hoc networking framework that sits on top of the IP layer and supports zero-configuration networking and automatic discovery. It is based on open, web-based technologies and uses existing open Internet protocols (e.g., HTTP, XML, and SOAP). UPnP is independent of OS, development language, and lower-layer networking. The UPnP AV (Audio/Video) specification is of particular interest for sharing multimedia in the home (e.g., Windows Media 7 combines a UPnP-Certified AV media server and control point on the same platform).

In the diagram below, the Media Server could be devices like PCs, DVD/CD/BluRay Players, Camcorders, STBs, Tuners, Camera etc., while the Media Renderer would be devices like other PCs, TVs, and Speakers, etc.

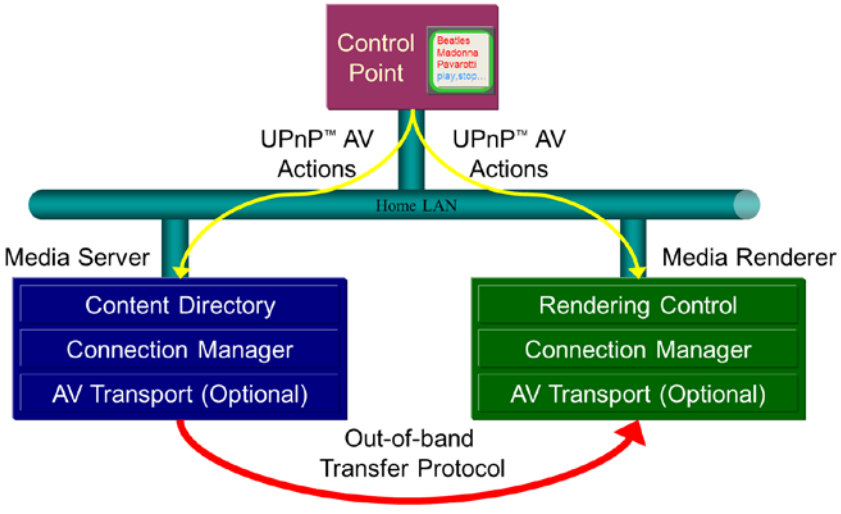

Figure 62 - UPnP AV Devices and Services

The UPnP Forum has updated the architecture to include optional support for IPv6. There are rules around address assignment and how devices advertise themselves on each network (IPv4 vs. IPv6). The architecture makes use of IPv6 link-local and site-local addresses. A UPnP Internet Gateway Device (IGD) provides IPv6 firewall control as well. More information is available in [Device Architecture v1.1, Annex A - IPv6 [UPnP]. The IPv6 requirements in

UDA1.1 are at a 'SHOULD' strength, the use of site-local unicast [RFC3879] is deprecated in favor of ULA [RFC4193], and the use of GUA in site-local multicast is restricted in favor of ULA. There is support for dual-stack IPv4 and IPv6 configuration.

10.4.2 Digital Living Network Alliance (DLNA)

DLNA has adopted UPnP Forum standards, but there is no requirement for IPv6; only IPv4.

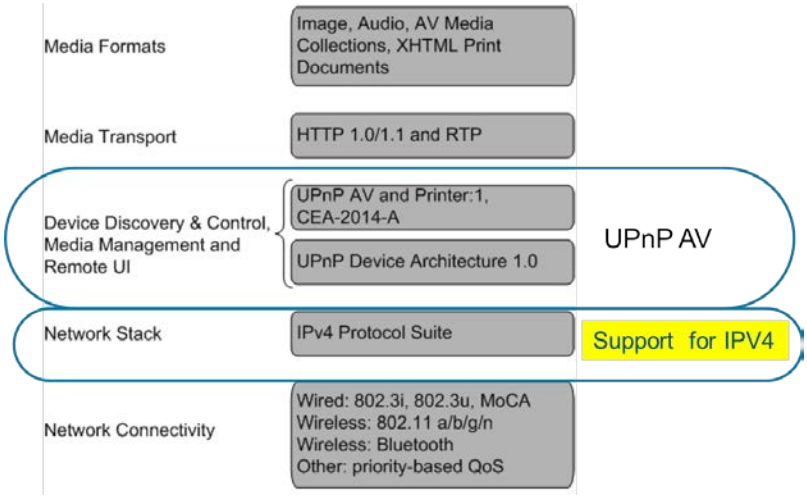

Figure 63 - Basic DLNA Architecture

10.4.3 OpenCable Home Networking (OCHN)

OCHN is a set of CableLabs specifications that utilize UPnP/DLNA Specifications as a foundation. OCHN APIs enable applications to:

- Publish or access DVR content over HN.
- Perform remote DVR scheduling.

OCHN includes HTTP support for streaming of stored content (with enhancements to DLNA-specified trick modes) and RTP support for streaming of live content. OCHN 2.0 supports multi-room DVR,, OCHN 2.5 supports Tuner Sharing and Copy/Move, and OCHN 3.0 supports streaming live content to DLNA CVP-2 devices.

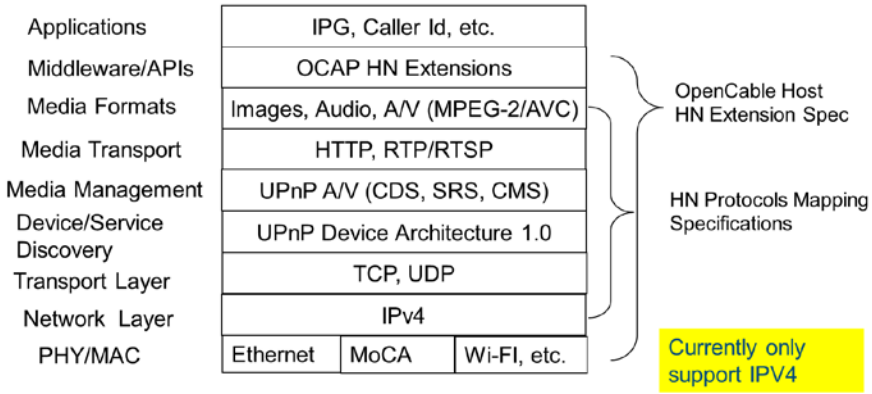

Figure 64 - OCHN Overview

10.4.4 Service Discovery Use Cases within the Home

DLNA/UPnP devices participate in the MLD protocol for any link-local and site-scope UPnP IPv6 multicast message. The Simple Service Discover Protocol (SSDP) announcements are sent to [FF0X::C]:1900. The UPnP Control points listen to these multicast addresses and ports to detect when new devices are available on the network.

The following describes different scenarios of in-home service discovery and the steps it takes to complete service discovery.

10.4.4.1 Scenario-1 One Flat IPv4 Network

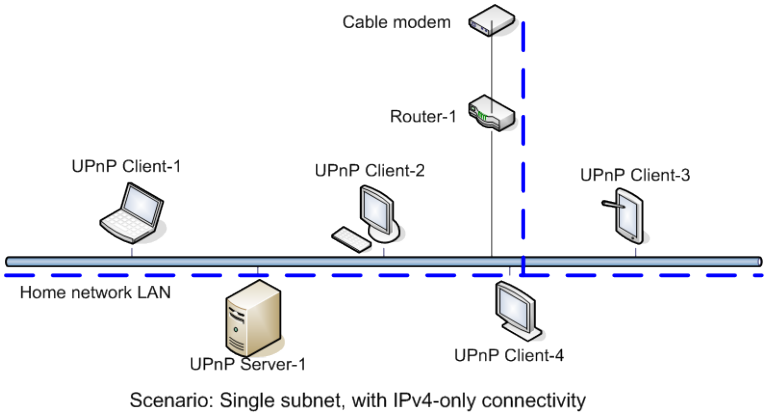

Figure 65 - One Flat IPv4 Network

- Step 0: IP-address acquisition via DHCPv4 or Auto-IP.
    - DHCP is preferred.
- Step 1: SSDP Discovery and Advertise messages are sent to specific IP-Multicast Address:Port sockets.
    - SSDP announcements are sent to [239.255.255.250]:1900.
- Steps 2-5: Client-Server use unicast SOAP/HTTP to transport media.

10.4.4.2 Scenario-2: 2 Routed IPv4 Segments

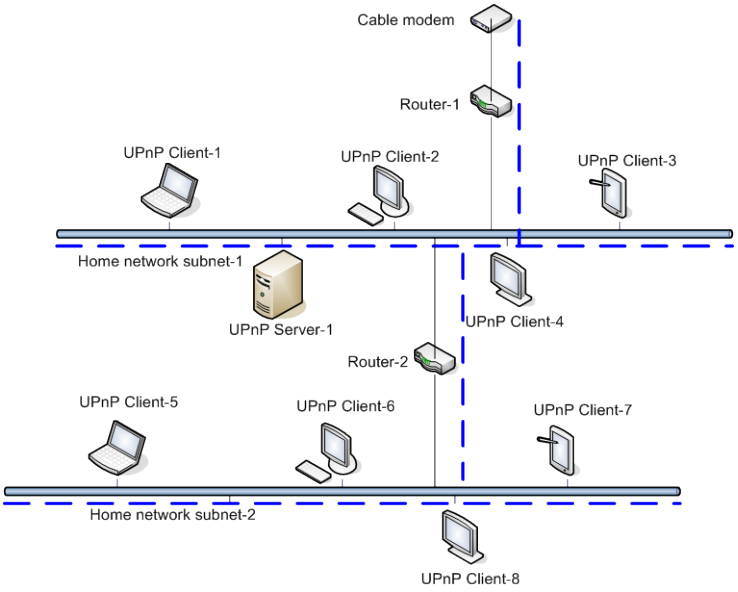

Figure 66 - 2 Routed IPv4 Segments

- Step 0: Assumes IP-address acquisition via DHCP.
- Step 1: SSDP Discovery and Advertise messages:
    - Same as Scenario-1.
    - Spec recommends SSDP messages have a TTL of 2, which allows messages to traverse two routers.
        - Spec recommends TTL to be configurable.
    - Clients are all required to send IGMP Join to ensure all routers forward messages.
    - Router-2 needs to handle multicast and/or static port forwarding configuration.
    - UPnP cannot traverse router without them.
- Both routers must install routes for both networks.

10.4.4.3 Scenario-3: One Flat Dual-Stack Network

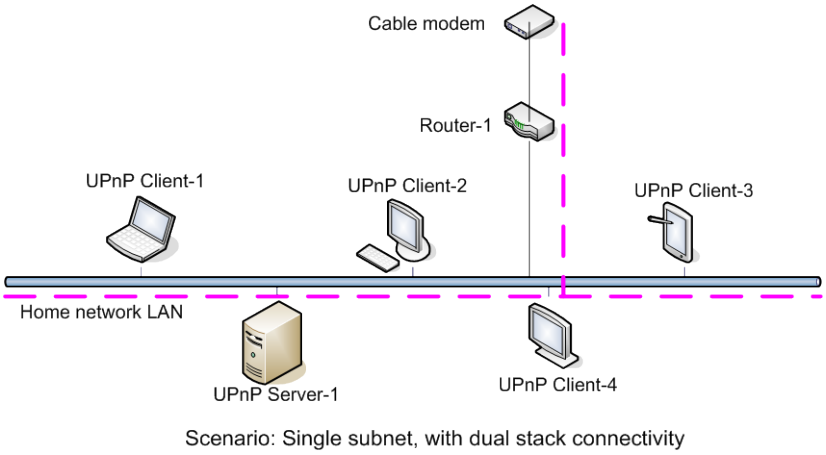

Figure 67 - One Flat Dual-Stack Network

- Step 0: IP-address acquisition:
    - IPv4: same as scenario-1 and scenario-2
    - IPv6: SLAAC (mandatory), DHCPv6 (optional), else Link-local
        - ULA is preferred over GUA in address selection
- Step 1: SSDP Discovery and Advertise messages:
    - Sent to specific IP-Multicast Address/Port sockets (TTL of 5)
        - SSDP announcements are sent to [FF0X::C]:1900
    - Clients are required to send IGMP/MLD Join to ensure all routers forward messages
- A Server device supporting dual-stack sends identical SSDP message content on both IPv4 and IPv6.
- IPv6: SSDP messages sent in site-scope multicast packets in addition to link-scope.
    - For SLAAC/DHCPv6, need a router (Router-1) else UPnP works on link-local addresses

10.4.4.4 Scenario-4 Two Routed Segments Dual-Stack Network

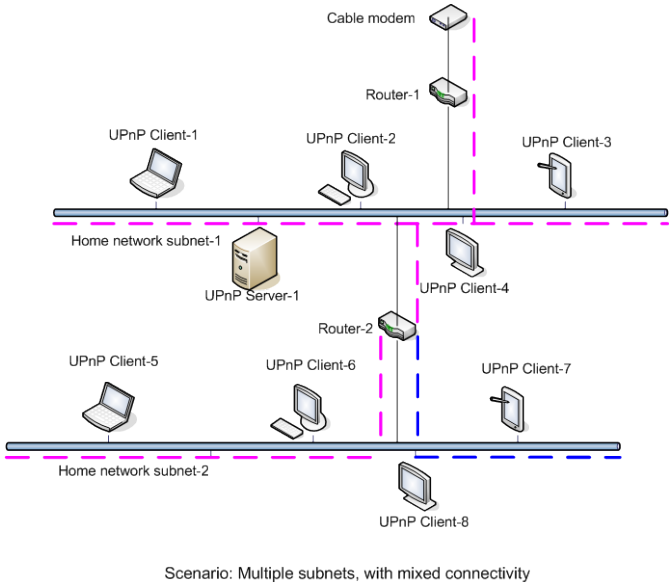

Figure 68 - Two Routed Segments Dual-Stack Network

- Step 0: IP-address acquisition:
    - Same as Scenario-3.
- Step 1: SSDP Discovery and Advertise messages:
    - Same as Scenario-3.
- IPv4-only devices: works just like in Scenario-2.
- Router-2 needs to support the following features:
    - IP-Multicast forwarding (IPv4 and IPv6)
    - Static port forwarding configuration
- Both routers must install routes for both networks.

10.4.5 In-Home Video Delivery IPv6 Impact

The lack of IPv6 support limits home network architecture options. UPnP has optional support for IPv6 in Annex A; DLNA and OCHN currently have no support for IPv6.

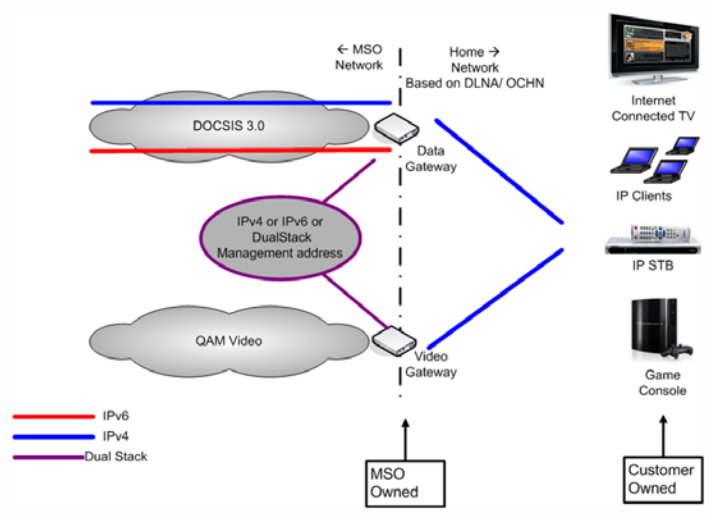

Figure 69 - In-Home Video Delivery IPv6 Impact

CableLabs has identified the lack of IPv6 support in DLNA and OCHN as an open issue and initiated discussion within CableLabs and their members.

10.4.5.1 IP stacks on the STB

An eSTB has an IP stack for interfacing with the WAN side and has potentially another LAN side IP interface dubbed the IP client. It may be necessary to separate the IP Client and the eSTB IP stacks and to add support for dual-stack on the IP client. Devices in the home are expected to operate in dual-stack mode in short to medium term and IPv6-only in long term, so dual-stack may be needed for guaranteed interoperability between MSO-provided STB (IP Client) and consumer devices (e.g., XBOX). This would require further coordination with UPnP and DLNA, however.

Members have expressed interest in having support for separate stacks for the IP stacks of the OCHN IP client and eSTB. There is also interest in supporting dual-stack for the eSTB.

10.5 Close Captioning (CC) and Parental Controls

CC is used to assist the hearing impaired by displaying textual information describing scenes and speech, which is overlaid on the video. It is a regulatory requirement that all broadcast content, analog or digital (SD or HD), support CC service. Broadcast TV service supports CC by embedding the textual information in the video (in the picture layer). For IP-streaming video, CC can be delivered as embedded in video or in a separate file using SMPTE TTML (timed text in XML) format. The SMPTE file carrying CC info may reside on the same server as video or on a separate server.

Parental Control describes a set of mechanisms that allow parents to block violent and adult content from their children. Content creators provide a content advisory rating for all content to be included in the content. The content rating is delivered via line 21 data in case of analog delivery (NTSC TV). In digital delivery of content, service providers include a content_advisory_descriptor() in the PMT, AEIT, or both. If a content_advisory_descriptor is included in content, a rating region table (RRT) is also included. For IP delivery of content in MPEG (ISOFF) format, content rating info is included in the global metadata section of the file. For HTTP streaming content with common container format (CCF) , content rating information can be delivered with metadata, with a media presentation description (MPD) file, or with both.

10.5.1 IPv6 Impacts

To support CC in IP Simulcast, the SMPTE TTML server may need to support IPv6.

To support Parental Controls (Content Rating) in IP Simulcast, the content server may need to support IPv6. For legacy video delivery, the IPv6 impacts are the same as identified for DSG use cases (Section 10.1.1, DSG and MDD Provisioning Mode) as operators use DSG to deliver parental control information.

10.6 Tru2Way ("OpenCable")

The FCC Telecom Act of 1996 requires a common receiver specification for the cable industry that separates the Conditional Access System (CAS) from receiver, brings receivers to retail stores, and fosters competition and innovation. The CableLabs project to meet these requirements was launched in 1997 and dubbed "OpenCable."

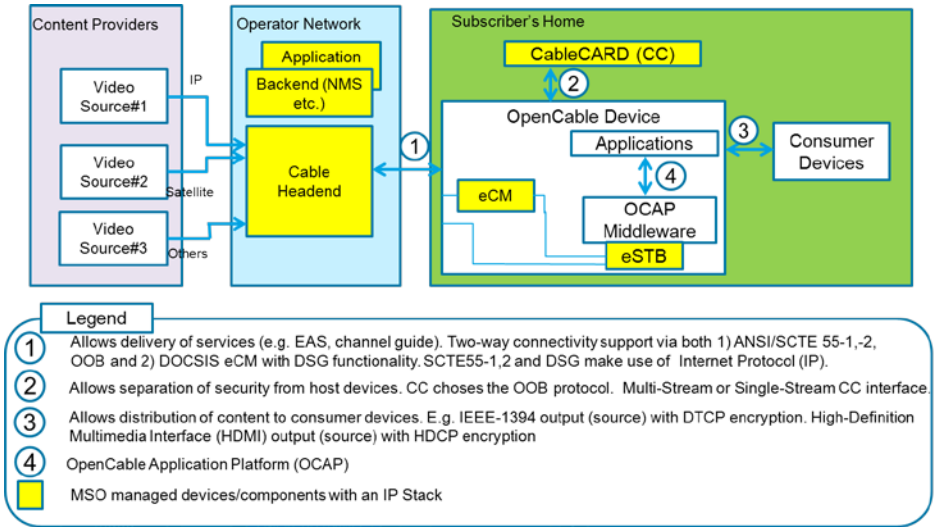

Figure 70 - OpenCable Components

10.6.1 OpenCable IPv6 Considerations

10.6.2 IPv6 Considerations for Devices in Subscriber Home

OOB communication can use either legacy methods (e.g., SCTE 55-1, -2) or DSG. Legacy methods support "IPv4-only" (the IP address is assigned to the CableCARD) while DSG supports "IPv4 only", "IPv6 only", and dual-stack.

The eSTB supports "IPv4 only" and "IPv6 only" mode (no dual-stack). An eSTB transition to IPv6 requires upgrades to the application and backend servers to support IPv6 and to the CMTS to support IPv6 (DOCSIS 3.0) and DSG. Lack of dual-stack will force all applications on the eSTB to move to IPv6 simultaneously.

The CableCARD optionally supports and uses both "IPv4 only" and "IPv6 only" mode.

The OCAP Middleware uses Java (version 1.4), which supports both IPv4 and IPv6. The applications use the IP address of eSTB.

10.6.3 IPv6 Considerations for Devices in Operators Network

OpenCable application and backend servers should support dual-stack, enabling end-to-end communication with both IPv4 and IPv6 devices. Server requirements are not covered in CableLabs OpenCable specifications. MSOs

should consider deploying Dual-Stack systems to support end to end connectivity with both IPv4 and IPv6 OpenCable devices.

10.6.4 Dual-Stack Considerations

Adding dual-stack support alleviates the requirement to move all applications to IPv6 simultaneously and, in the initial phase of transition to IPv6, it may be prudent to maintain both IPv4 and IPv6 connectivity. Also, some vendors are using eSTB IP Stack for the IP Client (see Section 10.4.5, In-Home Video Delivery IPv6 Impact).

However, dual-stack does not conserve IPv4, and today MSOs control the transition timeline for both eSTBs and App Servers, which may negate the requirement for a dual-stacked eSTB in the timeframe that it can be accomplished.

10.7 Enhanced Television Binary Interchange Format (EBIF)

Enhanced TV is a platform that enables interactivity, and EBIF is the format for interactive television applications that run on legacy and tru2way STBs. The power of EBIF is in footprint because it runs on low-end to high-end digital STBs, and all major North American MSOs are deploying EBIF (25 Million STBs deployed with ETV today). Also, Canoe is leveraging EBIF for Advanced Advertising.

EBIF enables many applications, both "bound" and "unbound." Bound applications are transported with the video stream, and are associated with a particular program. If you change the channel, a bound application will stop running. Unbound applications are not tied to any channel or program, and can run on the STB all the time, even when channels are changed (e.g., Caller ID).

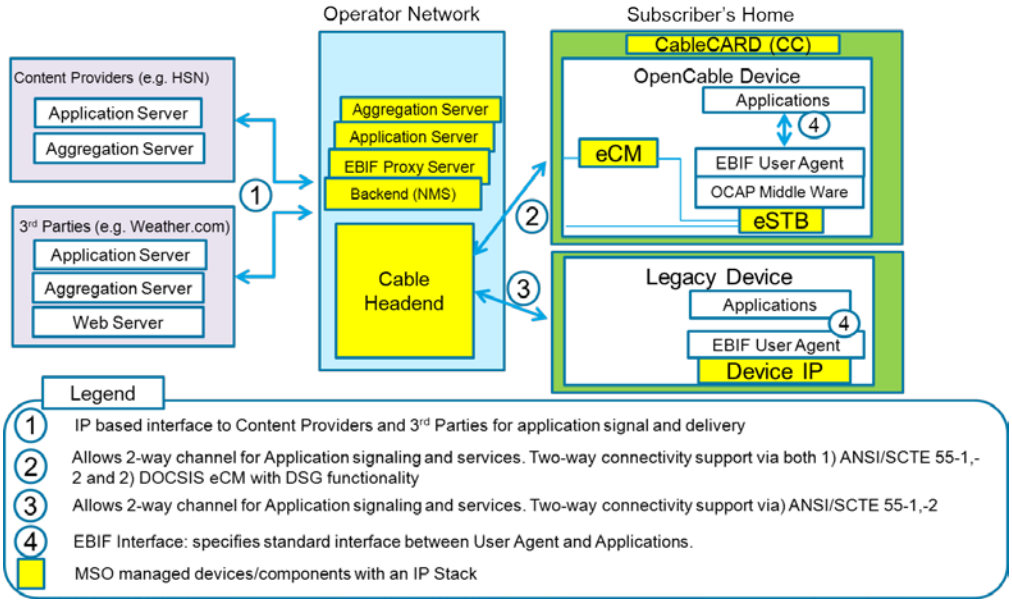

Figure 71 - EBIF Components

10.7.1 IPv6 Considerations for EBIF

EBIF user agent and applications in an OpenCable device use the IP stack of the eSTB. Since eSTB does not support dual-stack, all applications on an OpenCable device MUST transition to IPv6 at the same time. Impact to the application code itself should be minimal. EBIF user agent and applications in a legacy device use the IP stack of the device. Legacy devices only support "IPv4 only" mode (not likely to change).

MSOs should consider deploying dual-stack systems to support end-to-end connectivity with both IPv4 and IPv6 devices (OpenCable and Legacy) in subscribers' homes, content providers, and third parties. MSOs and CableLabs should consider convincing Content Providers and third parties to move to Dual-Stack as well.

10.8 Content Delivery from Programmer to Multichannel Video Programming Distributor (MVPD)

Cable operators can receive content from Programmers (e.g., CBS, HBO) through multiple means, including: satellite, terrestrial wave (microwave radio), snail mail (e.g., tape), and terrestrial link using IP or some other transport protocol. Transport mechanisms between programmers and MVPDs (MSOs) are not defined in CableLabs specifications.

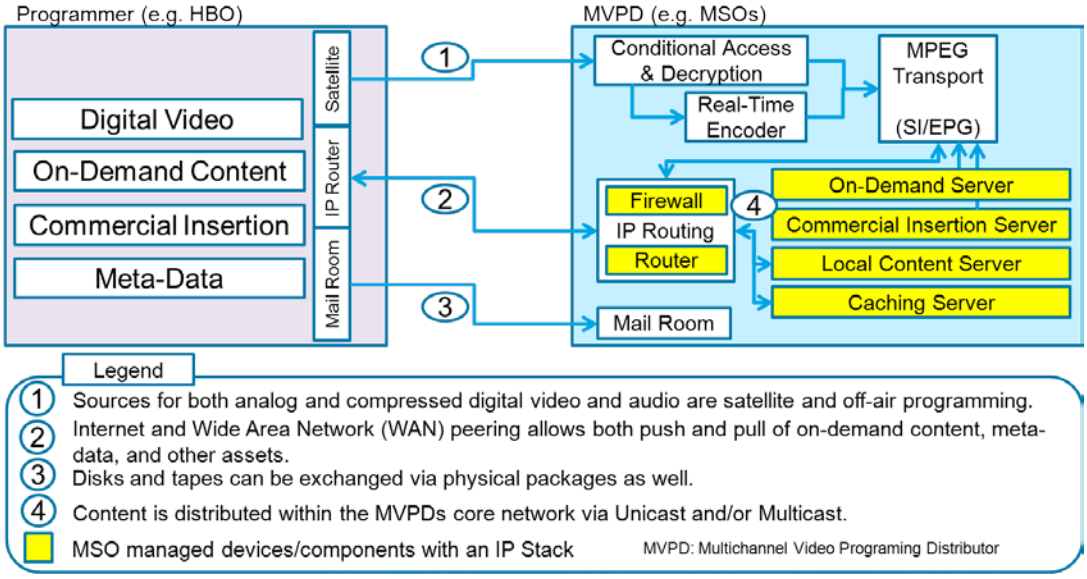

Figure 72 - Acquiring Programming Content

10.8.1 IPv6 Considerations for Acquiring Programming Content

All IP connections between programmers and MVPDs should be dual-stacked. All collectors and servers should have dual-stack support as well. Firewalls require special attention to IPv6/IPv4 feature parity. MVPDs utilizing multicast distribution within their network will need to enable MLD.

10.9 Online Content Access (OLCA)

OLCA allows MSOs to deliver online content to subscribers over IP to a variety of devices (e.g., PC, iPad, etc.). Technical requirements and architecture for the delivery of video to an MVPD customer from different online sources are defined in the CableLabs Authentication and Authorization Interface 1.0 Specification [AUTH1.0].

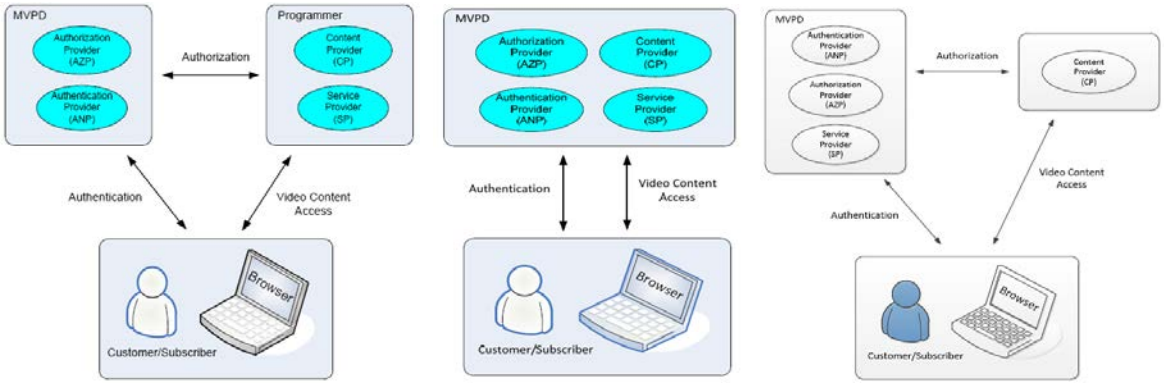

Figure 73 - OLCA Use Cases

There are several roles described within the OLCA framework [AUTH1.0]. Service Providers provide subscriber interface and access control to online video content; an MVPD, or Programmer can assume this role. Authentication Providers create, maintain, and manage customer identity information (i.e., they provide customer authentication for Service Providers). Authorization Providers create, maintain, and manage the customer authorization information (i.e., they provide customer authorization for the Service Provider). Only an MVPD can play the role of Authentication Provider or Authorization Provider. Content Providers deliver content to customers; an MVPD or Programmer can be a Content Provider. Subscribers are the customers who possess credentials for authorization and authentication.

10.9.1 IPv6 Impacts on OLCA

Authentication messaging between Service Providers and Authentication Providers uses Secure Association Markup Language (SAML 2.0) . Authorization messaging between Authorization Providers and Service Providers uses SAML 2.0, Extensible Access Control Markup Language (XACML 2.0)(). These protocols are web services and ride on top of IP networks; they have the same requirements as other web content (see Section 7, I). There is no specific IP dependency in most OLCA messages; one exception being an Authorization Query message, which includes the Subscriber IP address. The OLCA team has committed to review support for IPv6.

Transitioning OLCA to IPv6 requires discussions with content providers and CE vendors. Specific MSO steps to enable IPv6 include: enabling dual-stack on the web servers and enabling IPv6 on video-streaming servers. Once that is complete, customers will use IPv6 when available.

10.10 Advanced Advertising

Advanced Advertising is a platform to support interactive and addressable advertising, and media measurements. It is the reference architecture for a multi-MSO advanced advertising platform and defines logical entities that comprise the platform and interfaces between them. This includes a number of B2B and MSO internal interfaces. Advanced Advertising is described in CableLabs Advertising and Interactive Services Specifications.

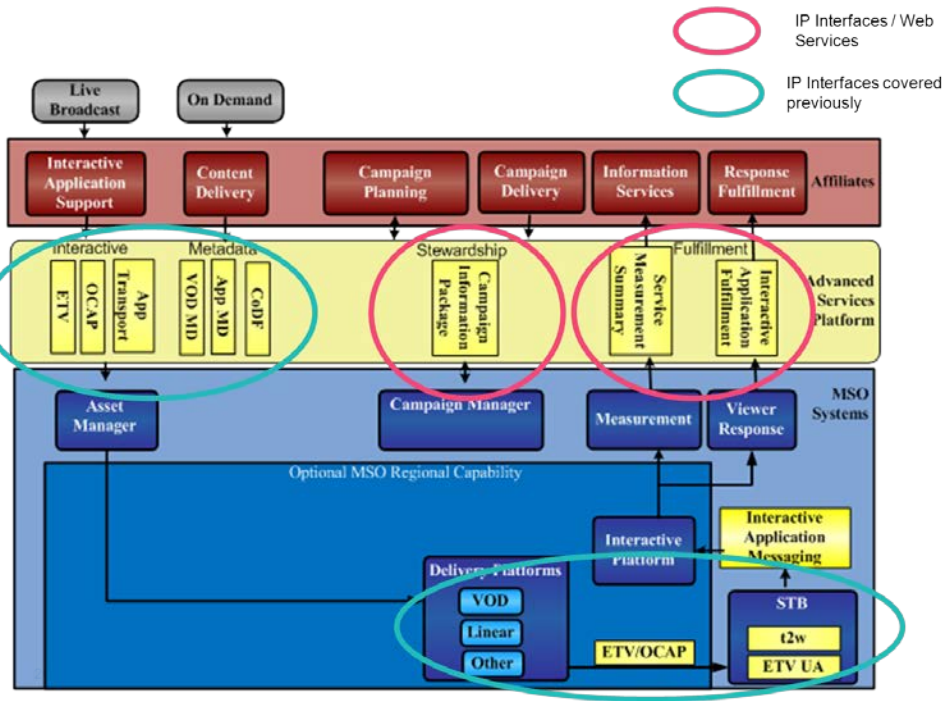

Figure 74 - Interactive Advertising

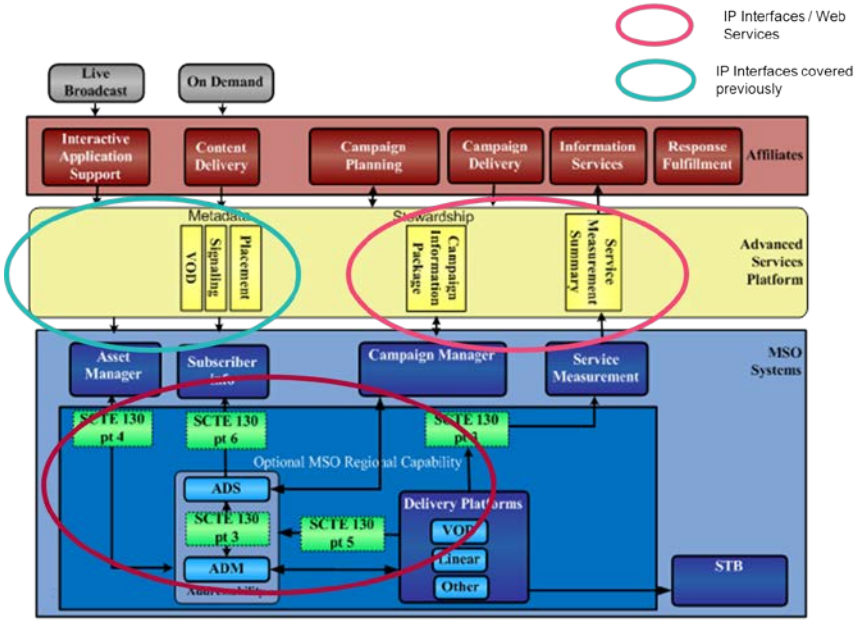

Figure 75 - Addressable Advertising

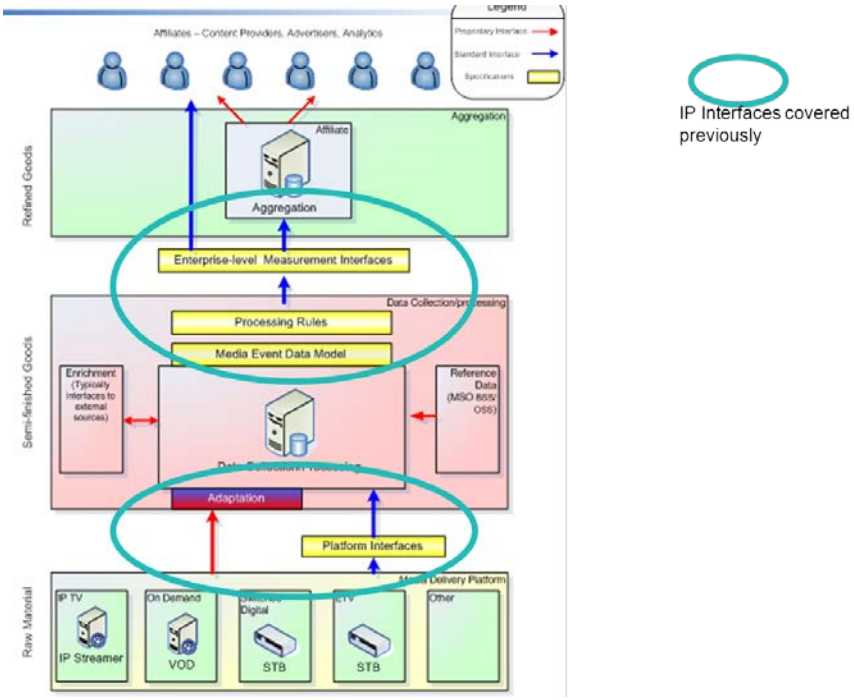

Figure 76 - Media Measurement

There are three primary advertising products currently identified within Advanced Advertising:

1. Interactive advertising includes enhanced linear content, such as vote/poll and Request for Information (RFI) applications, and access to OnDemand content from interactive applications and other advertising products based on OnDemand services.
2. Addressable advertising includes the placement of ads based on geographic, demographic, psychographic, or other parameters.
3. Media Measurements includes MSO collection of media metrics and sharing of the aggregate data with affiliates.

10.10.1 IPv6 Impacts for Advance Advertising

There are no new impacts to Advanced Advertising. B2B Connections to affiliates utilize a web services infrastructure, which is IP-version independent (see Section 7, I for IPv6 impacts). SCTE 130 inter-connections support both IPv4 and IPv6. STB connections use Linear, Tru2way (see 10.6), or EBIF (Section 10.7), and IPv6 transition impacts those technologies that were previously identified.

10.11 Linear Ad Insertion

Programmers make some advertisement time slots available for the individual MVPDs to use; these are called local avails. Local avails are signaled to the cable headend in the network feed. Analog signals are sent via DTMF tones or "Cue tones" while digital signals in MPEG are sent via SCTE 35 messages (DPI). An ad splicer responds to these signals and inserts local advertisements into the MPEG stream.

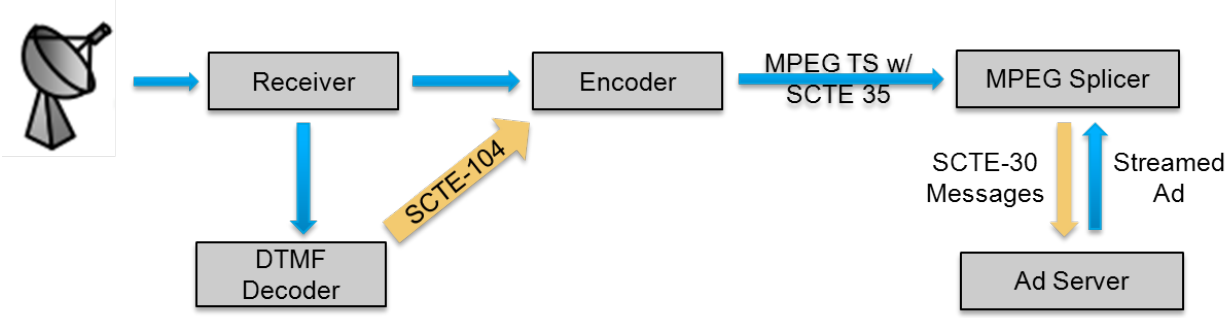

Figure 77 - Linear Ad Insertion Architecture and Components

10.11.1 IPv6 Transition Considerations for Ad Insertion

All components are within the MSO headend, content delivery to customers is over MPEG, and there is minimal IPv4 usage. The interface between the DTMF decoder and the Encoder supports IPv4 only [SCTE104]. The interface between the Ad Server and the MPEG Splicer supports IPv6 today [SCTE30]. All other interfaces are IP independent (SCTE-35 information is within the MPEG stream).

11 CGN USE CASES

11.1 Introduction

The answer to IPv4 address exhaustion is migration to IPv6, which offers virtually unlimited addresses. Because many consumer electronics in subscriber homes and many content sites only support the older IPv4 protocol, MSOs will be forced to support IPv4 connectivity through the transition period. To do this, ISPs around the world (including some MSOs) will be forced to share IPv4 addresses among subscribers using address-multiplexing technologies known as Carrier Grade NAT (CGN). The best CGN options for cable operators are NAT444 (alongside either native IPv6 or 6RD) and DS-Lite. This section covers detailed CGN use-cases.

11.2 Overview and scope

Members have indicated interest in NAT444 [ID-nat444], DS-Lite [RFC6333], and 6RD [RFC5969] as CGN/transition technologies. Other CGN technologies, such as IVI, Address plus Port aka A+P, NAT64, and DNS64 are out of scope. If the reader is interested in learning more about these out-of-scope technologies, they are defined in the following IETF documents:

- IVI is defined in [RFC6219].
- A+P is defined in [RFC6346].
- NAT64 is defined in [RFC6146].
- DNS64 is defined in [RFC6147].

It is very likely that MSOs (and all carriers) will implement the technologies needed for their transition in a phased approach over time.

Connectivity Type	Time →			
IPv4	Native	NAT444	NAT444	DS-Lite
IPv6	None	6RD *(some may skip this step)*	Native	Native

Figure 78 - Timeline of Access Technology Transition

11.2.1 Overview NAT444

NAT444 is a technique that leverages CGNs to provide IPv4 services to subscribers. It uses two NATs with three IPv4 address realms. Most commonly, there is a private IPv4 address automatically assigned to home devices from the Home Router, as there is today. Service providers then assign a second private address to the outside interface of the Home Router. The Home Router translates the subscriber-assigned private space to the operator-assigned private address for transport across the operator's access network. The operator then uses CGN to translate the subscriber's private address into a shared public address. A major advantage of this technology is that it works with existing home routers, and does not require any change on the subscribers' networks.

As NAT444 shares an IPv4 address across multiple subscribers, it offers each subscriber a limited number of ports. Since some applications simultaneously use a large number of ports, operators may need to statically reserve a relatively small number of ports per subscriber, while offering a larger number of dynamic ports on a shared basis.

Because of the port limitations imposed by NAT444, applications and gateways may need to be aware of the port restrictions. Technologies, such as NAT Port Mapping Protocol (NAT-PMP) () or Universal Port Mapping Protocol (UPMP) , can be employed to assist applications in using the correct port range.

A CPE may apply UDP hole punching or TCP hole punching for interactive services among CPEs like Voice over IP and P2P. CGN should not interfere in services using UDP hole punching or TCP hole punching.

Subscribers assign Private IPv4 Addresses [RFC1918] to home devices via the home gateway, as they do today. Service Providers then assign a second private address to the Home Gateway. The exact address range is currently a work in progress in IETF specifications, and is referred to as "IANA Reserved IPv4 Prefix for Shared Transition Space". The actual address range will need to be identified prior to deployment. The Home Gateway translates the subscriber-assigned [RFC1918] space to the operator-assigned private address for transport across the operator's access network.

The operator then uses CGN to translate the subscriber's "IANA Reserved IPv4 Prefix for Shared Transition Space" address into a shared public address, as described in [RFC6598].

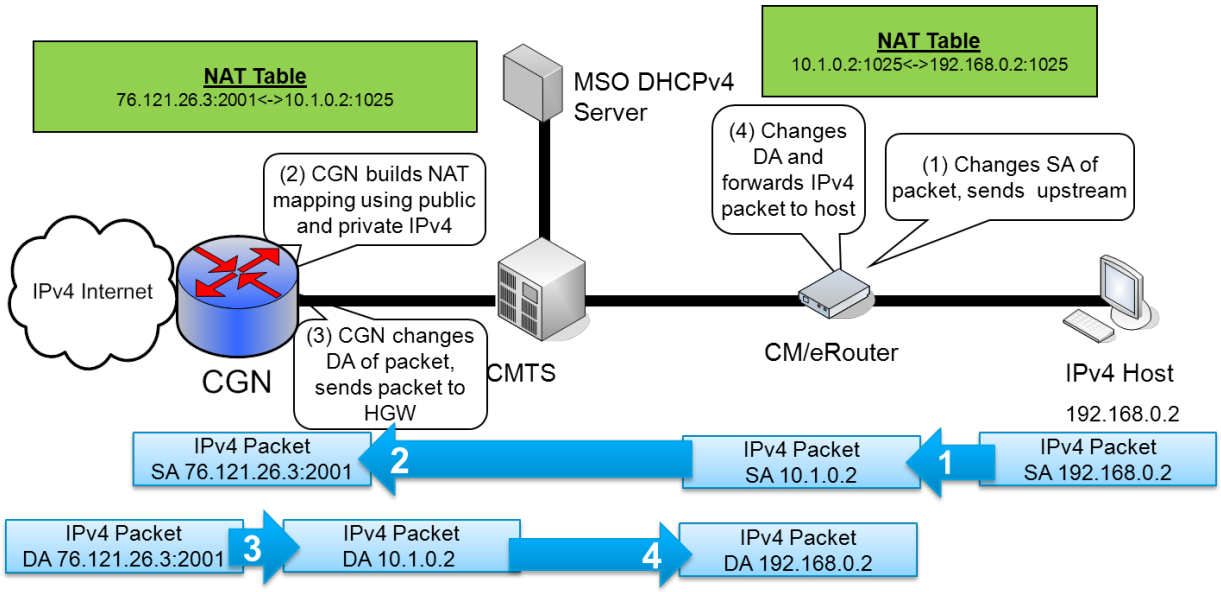

Figure 79 - NAT444 Example

11.2.2 Overview DS-Lite

DS-Lite is a technique that combines dual-stack, tunneling, and NAT translation so an operator can provide IPv4 service to customers when the network between the subscriber and operator uses IPv6. In DS-Lite, IPv4 traffic is encapsulated within IPv6 at an upgraded home gateway (or in some cases, directly at the host), and sent to a CGN. The CGN then translates the private subscriber IPv4 address into a shared public address. In order to be able to multiplex multiple subscribers who may be using the same private IPv4 address space, the CGN uses the IPv6 tunnel source address as part of its NAT translation mapping. On the other hand, IPv6 traffic can be transported natively, without address compression or mediation through a relay device. Instead of translating traffic from IPv4 to IPv6 and vice versa, the home gateways and LSN tunnel the customer IPv4 traffic in IPv6. DS-Lite avoids the complex problem of address translation at the CGN and home gateway. DS-Lite also requires an upgrade or replacement of home gateways since the majority of the installed home gateways do not support the IPv6 stack. DS-Lite is an IETF solution, which is defined in [RFC6333].

In DS-Lite, a single public IPv4 address can be shared across multiple subscribers. IPv4 traffic is encapsulated within IPv6 at a home gateway (or in some cases, directly at the host) and sent to a CGN. The CGN then translates the private subscriber IPv4 address into a shared public address. In order to be able to multiplex multiple subscribers

who may be using the same private IPv4 address space, the CGN uses the IPv6 tunnel source address as part of its NAT translation mapping.

DS-Lite can also be used with Address+Port Routing (A+P) . In such a case, the home gateway performs the A+P mechanism described above for subscriber traffic inside the A+P range. The CGN would not translate such packets, but would forward them to the IPv4 Internet.

By combining CGN and A+P, DS-Lite offers relatively high address compression. Subscribers can be given their own dedicated range of ports and access to a shared pool. DS-Lite also allows operators to deploy IPv6 to the edge of the subscriber network. Depending on where the CGN is deployed, however, DS-Lite may dictate sub-optimal traffic routing and lower scalability and reliability than a NAT solution closer to the subscriber edge.

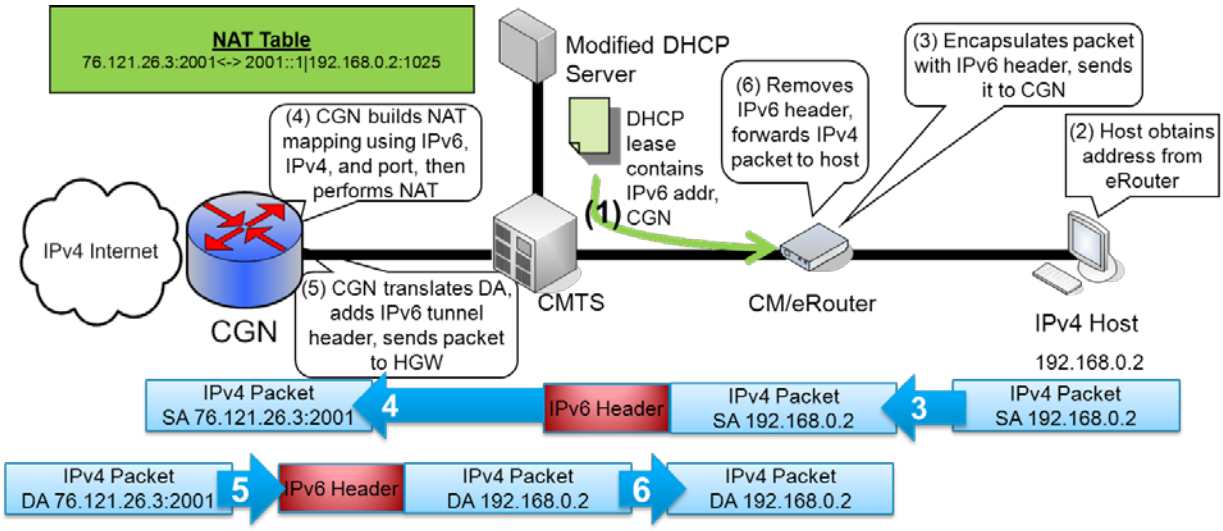

Figure 80 - DS-Lite Example

11.2.3 Overview 6RD

While 6RD is not a CGN technology per se, it is a transition technology and will most likely be used alongside a CGN, such as NAT444. The motivation for this method is to allow isolated IPv6 domains or hosts, attached to an IPv4 network that has no native IPv6 support, to communicate with other such IPv6 domains or hosts with minimal manual configuration, before they can obtain native IPv6 connectivity. 6RD tunnels IPv6 traffic to and from subscribers across the carrier's network in IPv4 tunnels. No NAT is directly involved in 6RD. 6RD is an IETF solution, which is defined in [RFC5569]. The mechanism is intended as a start-up transition tool used during the period of co-existence of IPv4 and IPv6. IETF does not perceive this as a permanent solution.

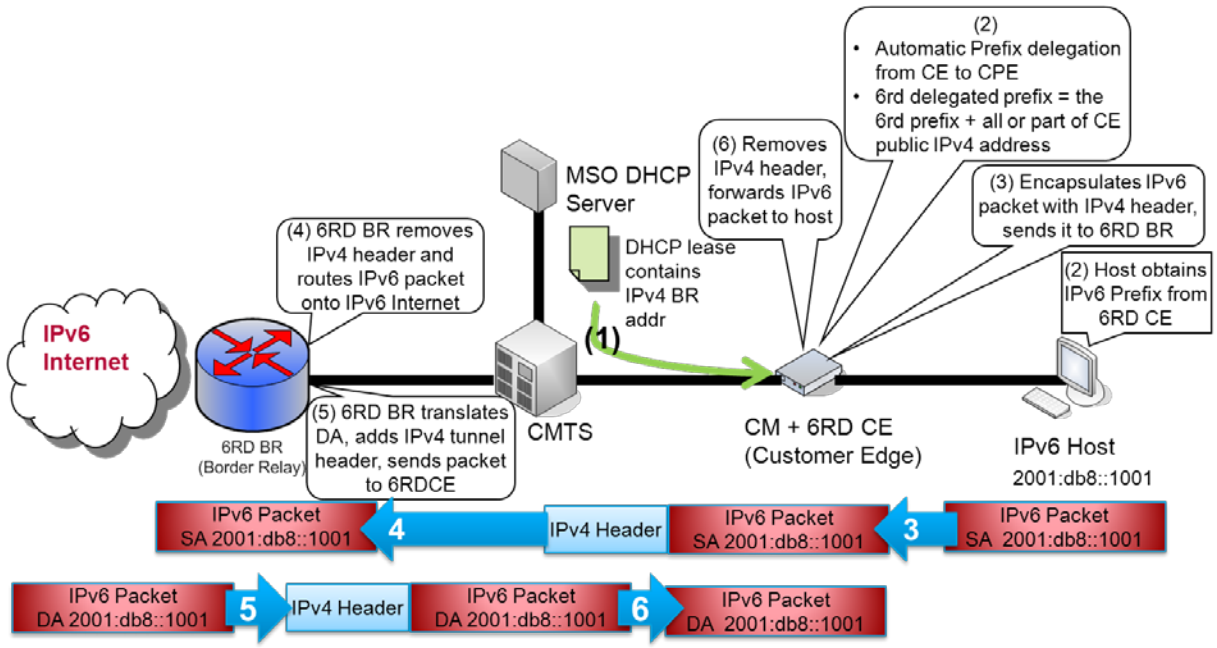

Figure 81 - 6RD Example

11.3 Deployment Considerations

11.3.1 Network Architecture

At the highest level, a CGN architecture can take one of three basic approaches: centralized, distributed, or a hybrid of the two. A pure centralized architecture places all CGN functionality in one central location within the carrier's network. A truly distributed method places CGN functionality as close to the subscriber as possible. A hybrid approach falls somewhere between these two extremes. The following sections will explore all three options and the decision points in choosing one.

11.3.1.1 Centralized Architecture

A centralized architecture places all of the CGN devices in one central location within the operator's network. This design likely offers the best ease of implementation and relative deployment cost because the network is able to start with a single CGN device and grow as needed. Additionally, because the most statistical multiplexing is gained, a centralized approach has the ability to consume the least public IP addresses for the outside of the NAT. It is also easy to place CDN or other advanced services servers inside of the NAT with a centralized approach. The downside to this design is a major impact to routing and traffic engineering, since all CGN traffic will be forced to transit this central location. It also has the largest negative impact to geolocation and all location-based services, since it makes it much harder to distinguish an individual subscriber's location behind a single network-wide NAT pool. Lastly, long-term scalability may be an issue as space, power, cooling, and bandwidth demands grow in this one location over time.

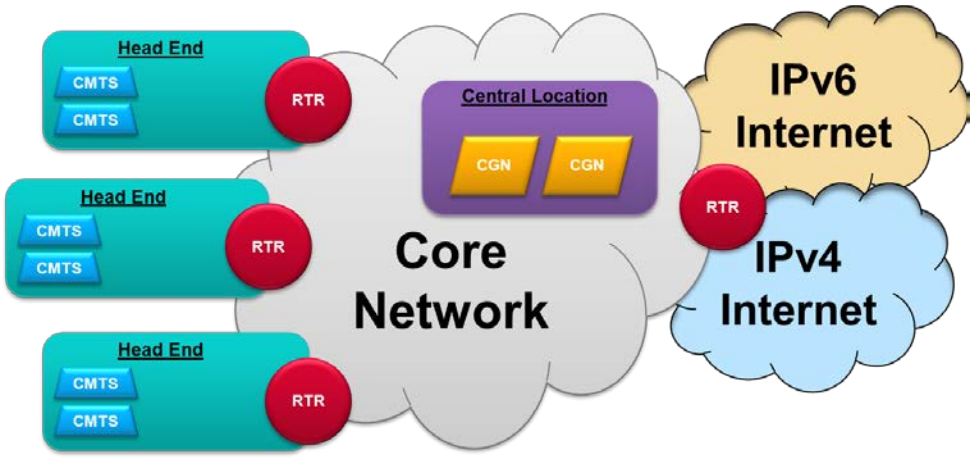

Figure 82 - Centralized Architecture

11.3.1.2 Distributed Architecture

The distributed architecture takes the opposite approach by placing CGN devices as close to the customer as possible, typically this means the local headend. By pushing the NAT closer to the end users, the distributed architecture has the lowest impact on routing, traffic engineering, and geolocation. Traffic must pass through these locations anyway. The trade-off is that a large number of CGN devices must be deployed up front, which increases the relative deployment cost and makes implementation harder. This also results in fewer subscribers per CGN device and thus potentially introduces a need for more public addresses due to the loss of the statistical multiplexing advantages of a centralized approach. Finally, CDN and other advanced services servers will likely be outside of the NAT, which is not optimal.

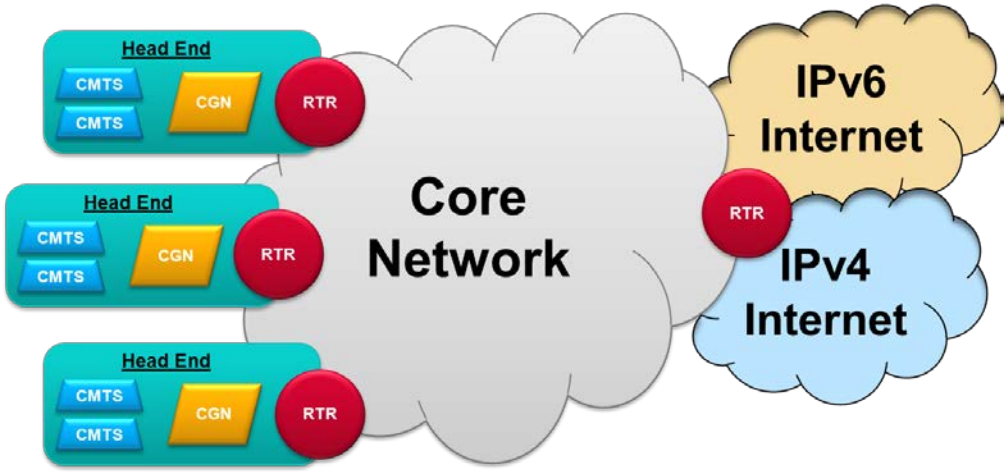

Figure 83 - Distributed Architecture

11.3.1.3 Hybrid Architecture

Another option is a phased hybrid approach, which starts with regionalized (or centralized in small networks) CGN devices and adds CGN devices as needed at local headends, as the CGN user base grows. This basic architecture offers an easy starting point and wide reach. It provides low impact to routing and traffic engineering and offers the most flexible scalability over time.

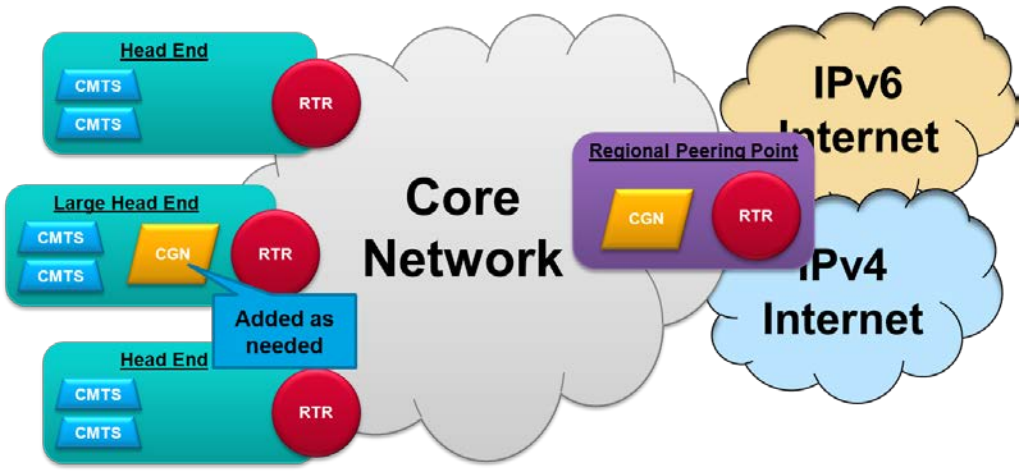

Figure 84 - Hybrid CGN Architecture (Phased Approach)

11.3.1.4 Architectural Considerations

There are many high-level constraints on a CGN system that must be considered when deciding on a basic architecture:

- Relative day 1 cost of deploying a CGN system
- Operational impact when initially deploying the chosen architecture (ease of implementation)
- Changes required in current routing infrastructure and their impact on routing
- Changes required to current traffic engineering tools and methods
- A load balancing strategy to share traffic loads between different devices is required if any more than one CGN device is to be used.
- Scalability and the ability to respond to increased traffic/subscriber growth
- Concerns regarding IP addresses include: subscriber IP addressing, the size of the private subnet needed, and the number of public addresses required.
- Granularity of geolocation information obtained when a CGN device is introduced

On-net CDN deployments must be considered to enable ease of placement of CDN servers and optimum traffic patterns for low latency.

11.3.1.5 Recommended Architecture

The CableLabs IPv6 team recommends a phased hybrid approach, which starts with Regionalized CGNs and adds CGNs as needed at local headends as the CGN user base grows. This basic architecture offers MSOs an easy starting point and wide reach. It provides low impact to routing and traffic engineering and offers the most flexible scalability over time.

See Figure 84 for an illustration of this recommended architecture.

11.3.2 Routing CGN Traffic

NAT444 CGN traffic must be identified and routed to the correct CGN without forcing all traffic through a potential bottleneck. The best approach is to classify once at the edge and use native routing or tunnels in the core.

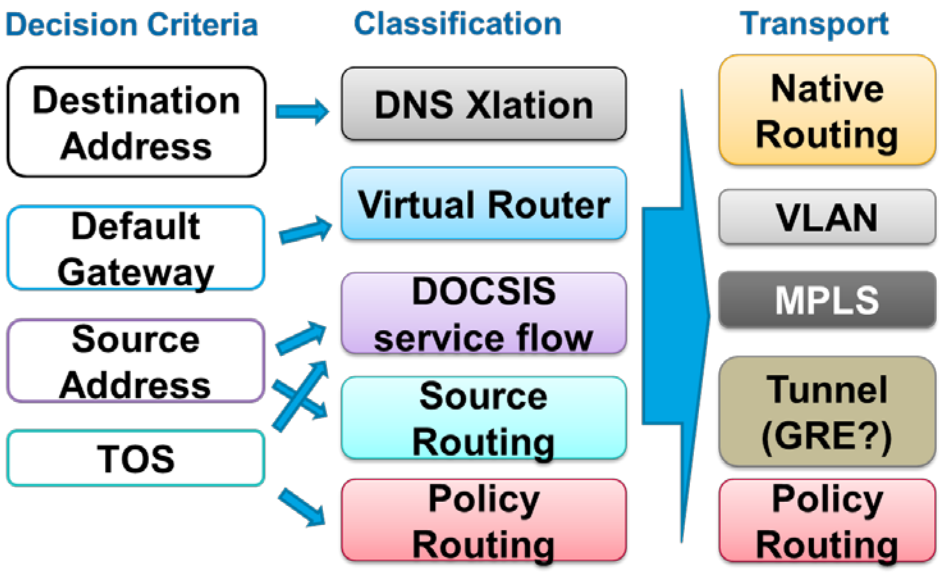

Figure 85 - Options for Routing CGN Traffic

There are several options for classification, and all are based on different decision criteria. Figure 85 illustrates these options and the various transport methods that can be used to keep CGN traffic segregated once it is identified. A few things to note here regarding the various decision criteria:

- To key on Destination Address requires DNS translation.
- Using default gateway identification requires CMTS Virtual Routing and Forwarding (VRF).
- Source address classification requires either DOCSIS L2VPN and/or source routing.
- Deciding based on Type of Service (ToS) requires either DOCSIS L2VPN and/or policy routing.
- All transport methodologies are compatible with all classification techniques.

Some examples of how to implement these options are presented in Table 4, along with a preliminary analysis of each.

Table 4 - Examples of Routing CGN Traffic

Solutions	DOCSIS L2VPN	VRF at CMTS	Source based routing	Policy based routing	DNS44
Brief Description	Classify at CM, CM assigns a service flow, CMTS assign a L2VPN (e.g., VLAN)	CPEs behind CGN are assigned a different default gateway than regular subscribers	Agg router classifies traffic based on source address	Agg router classifies traffic based on ToS (or other)	DNS resolves to CGN. CGN then translates source and destination address.
Prelim analysis	Configuration intensive Scalability issues	Good option Vendor support via proprietary options	Resource intensive (typically done in software)	Resource intensive (Software) Relies on CMTS to mark ToS	No known implementations
NOTE: Because both DS-Lite and 6RD CPE gateways build a tunnel, there are no additional routing considerations when implementing these technologies.					

11.3.2.1 VRF at CMTS

One interesting option for routing CGN traffic is using a virtual routing instance at the CMTS. This is done through a combination of DHCP and CMTS configuration. First, the DHCP server provides addresses and default route from

CGN pool within CGN address space to the CGN subscriber's Home Router. Non-CGN subscribers still receive global-scoped information (address and default route) as they do today. The CMTS is configured with one VRF for CGN traffic, and one for non-CGN traffic.

- VRF A for non-CGN traffic uses a global gateway address.
- VRF B for CGN traffic uses a gateway address within CGN scope.

Each subscriber's default route ensures that the subscriber's traffic is destined to the correct VRF. Once at the CMTS, CGN traffic is forwarded on to the CGN device(s) in one of two ways:

1. The CMTS uses MPLS to identify CGN traffic before forwarding, or
2. The CMTS has separate routing tables for each VRF, and forwards CGN traffic to one edge router or VRF and global-scoped traffic to another.

11.3.3 Redundancy

There are two methods for building redundancy into a CGN system: onsite device redundancy and site-to-site failover. Device redundancy can take several forms. 1+1 redundancy refers to one device directly supporting one other device, while N+1 redundancy refers to a single device providing backup for multiple (N) devices. In either case, the backup device can be active all the time (active/active) or it can be dormant until needed (active/passive).

For CGN device redundancy, N+1 CGN devices are installed at each regional hub. These extra devices can be configured as active/standby or active/active. In an active/standby system, the dormant standby capacity may be considered wasteful and failover will likely be slower than an active/active system. Additionally, active/active systems allow for load balancing in non-failure mode.

The next level of device redundancy is stateful NAT, which provides session continuity, allows for load-balancing, and provides the fastest failover. Stateful NAT devices share their NAT table along with all other state information so that any device in the system can continue to forward traffic initiated on any other device.

For whole-site redundancy, the best choice is typically to build in 10% additional capacity at each site, and allow the network's dynamic routing to re-route traffic when needed. For example:

- If the CGN system at a regional hub fails, dynamic routing sends failover traffic to CGN system(s) in a different regional hub.
- If the CGN system at a headend fails, dynamic routing sends traffic to the CGN system(s) located at the regional hub.

11.3.4 Load Balancing and Scalability

The first step in creating a load balancing and scaling strategy for CGN deployment is sizing the individual CGN devices (whether they are blades or stand-alone "pizza-boxes"). There are four elements that determine how many subscribers a single CGN device can support:

- New connections per second per subscriber (peak)
- Number of concurrent connections per subscriber (average)
- Necessary throughput per subscriber (average)
- Logging volume

Many of the devices being offered today offer 20 Gbps of device throughput. Manufacturers report that devices support several million (1-4 M) connections per second and tens of millions (32-128 M) of concurrent connections. Assuming that each residential subscriber consumes an average of 250 Kbps, a device offering 20 Gbps of throughput might support around 75,000 subscribers. This would allow every subscriber to have 400-1700 concurrent connections and 13-53 connections per second. While these figures are representative of several devices on the market today, individual product performance may vary.

Once the capacity of each CGN device is understood, a detailed load balancing and scaling strategy can be developed. Many of the specifics will depend on previous architectural decisions. Figure 86 shows an example of such a strategy based on a network using a hybrid/phased approach similar to what is described in Section 11.3.1.3 above, and making the assumption that each CGN device is able to support 50,000 subscribers.

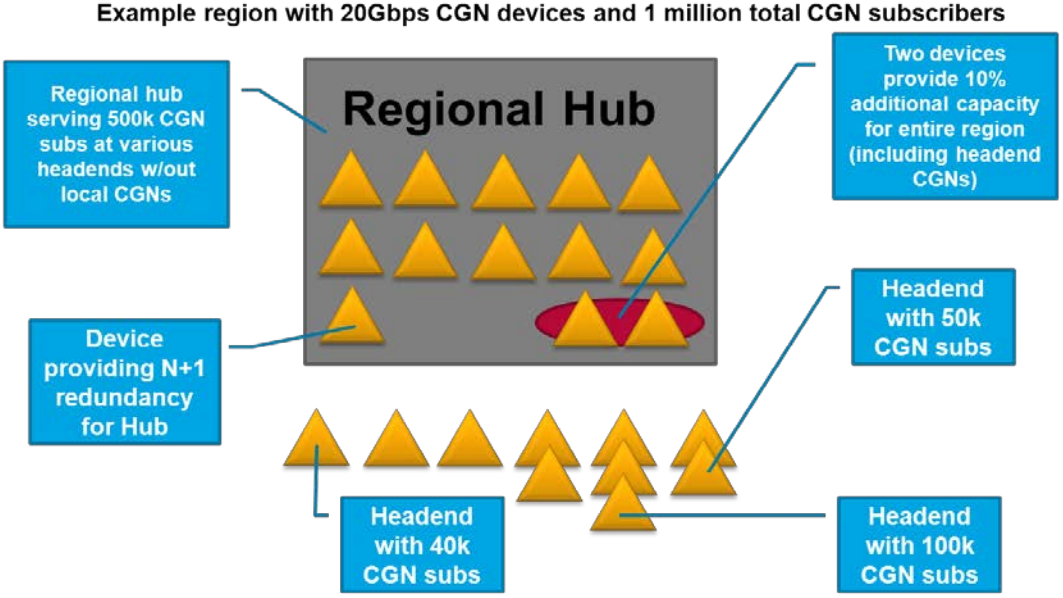

Figure 86 - Load Balancing and Scalability Example

The methodology illustrated in Figure 86 for growing a CGN infrastructure is to start with two devices at each regional hub and add an additional CGN for every 50,000 subscribers. In addition, include 10% extra capacity to absorb any potential failures in distributed CGN failures (as discussed in Section 11.3.3). Additionally, when any one headend reaches 40,000 CGN additional subscribers, it might be advantageous to add a local CGN device. Then add an additional device when the CGN subscriber count reaches 50,000 (10,000 subscriber increase) and then at every subsequent 50,000 subscriber increase. For example, a large headend would get one CGN for 40,000 CGN subscribers (approximately 200,000 total subscribers), a second CGN when the CGN subscriber pool reaches 50,000, and a third to service 100,000 CGN subscribers (approximately 500,000 total subscribers, assuming an even distribution of the 20% of subscribers who might need CGN service). This approach maintains N+1 device redundancy in every location with 50,000 or more subscribers and also builds in additional load-balancing/failure-absorbing capacity into the entire system.

11.3.5 Server Location and NAT Bypass

Optimizing local traffic and subscriber access to advanced services must be approached differently for each CGN technology. With NAT444, advanced service servers should be placed inside of the CGN and IPv6 support should be added. Dynamic routing or a VPN can then be used to bypass NAT for those servers when connecting over IPv4. For DS-Lite, simply enable IPv6 on all servers. Since all IPv4 goes through the CGN, there is no way to optimize IPv4 traffic.

11.3.6 IP Addressing

Addressing plans are required for both inside and outside IP space; the following sections address each area individually.

11.3.7 Outside Addressing

The primary concern when addressing the challenges of outside IP addressing is the compression ratio, defined as the ratio of subscribers using a CGN to the number of public IPv4 addresses supporting them:

(number of CGN subscribers) / (number of public IP addresses) = (compression ratio)

That equation simply determines how many subscribers will be placed behind a single public IP address. The higher the ratio, the fewer ports each customer will have available to them. The actual impact to each customer will depend on the protocols and services they use but as a general rule, the higher the compression ratio, the more their experience will be degraded.

The best approach is to determine how many CGN subscribers need to be supported within the planning horizon (expect a minority of users to be behind a NAT; approximately 20% at the high water mark) and also decide on an optimal compression ratio. Our analysis suggests that a compression ratio of about 8:1 will offer customers a reasonable quality of experience, while balancing against the needs of MSOs to conserve IPv4 addresses. With those two inputs into the equation, an operator can determine how many public addresses must be found.

11.3.7.1 Finding Outside Addresses

There are three methods to find public addresses for the outside of a CGN. The first is to re-purpose existing addresses by renumbering infrastructure to IPv6 or private IPv4 or by renumbering customers to inside CGN addresses. Second, there may also be opportunities to acquire new addresses from a transfer market or other secondary sources. Finally, it may be possible to reserve addresses from ARIN's current inventory by documenting plans for implementing CGN within a three-month window. In any case, outside public addresses need not be contiguous.

11.3.8 Inside Addressing

For NAT444 deployments, operators should use a single network-wide pool of inside addresses whenever possible. A large block (one /10 which is about 4M addresses) of Shared Transition Space is being reserved by ARIN and the Internet Engineering Task Force (IETF) for this purpose. That block is very likely to be the best choice for all operators (very large MSOs may need to re-use the block regionally).

From the Shared Transition Space /10, assign local (per headend) blocks (/16 per CGN device = 65k addresses) to provide operational clarity, logging, the ability to insert local CGNs, and potential geolocation benefits.

For DS-Lite any addresses are acceptable and can be reused per tunnel.

11.3.9 Geolocation

Geolocation refers to the process of identifying the physical location of a user through their connection details, primarily source IP address. This is useful for targeted advertising and location aware services. Because users connecting to the Internet from behind a CGN do not have a unique public address and instead share from a pool of source addresses, it becomes more difficult to determine their location.

Local headend CGNs will offer roughly equal granularity to what is available today, but regional (or central) CGNs will dilute geolocation data. CableLabs has proposed an idea to minimize this dilution by using separate outside pools of addresses that correspond to the per-headend private subnets. These public pools should be loose, to borrow from the next pool if needed, either borrowing from an adjacent pool or higher level pool.

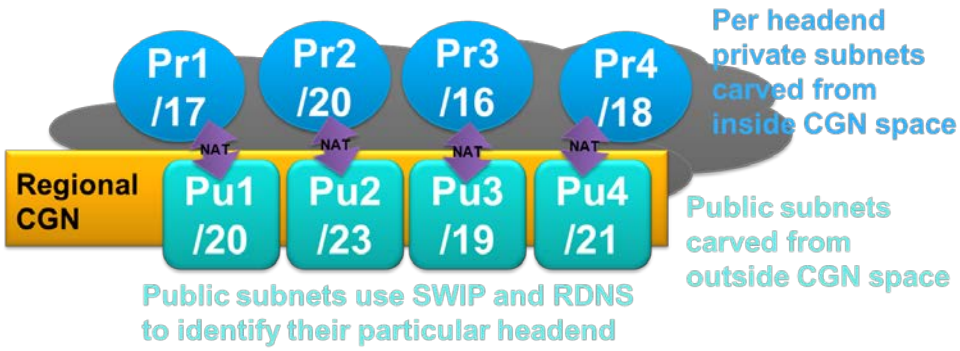

Figure 87 - Overcoming Location-Related Obstacles imposed by CGN

11.3.10 Lawful Intercept (LI)

LI is a telecommunications function of collecting communications network data for a LEA for the purpose of analysis or evidence. Such data generally consists of signaling or network management information and, in some instances, the content of the communications. The impact of CGN on Lawful Intercept operations is covered in section 8.1.4 of this document.

11.3.11 Security

There are two primary security considerations when developing a CGN architecture: filtering the inside address space at the edge of the CGN network and Denial of Service (DoS) mitigation.

11.3.11.1 CGN Inside IP Space Filtering

Because CGN inside address space is privately scoped and likely shared, operators will need to take care not to forward traffic destined to or sourced from those addresses beyond their AS (perhaps even beyond one CGN region). In order to ensure this, operators must block CGN routes from being advertised to and from peers and also block all traffic with CGN source or destination IPs at the CGN network borders. This filtering likely will not happen on the CGN device but rather on peering routers.

11.3.11.2 DoS Mitigation at the CGN

Because all traffic destined to the users behind a CGN device must pass through that device, the CGN device itself becomes a target for DOS and other IP-focused attacks from outside an operator's network. Additionally, the CGN device is also a bottleneck for attacks sourced from CGN subscriber networks, inside an operator's network. Therefore, it is highly recommended that operators consider DOS mitigation, Access Control Lists (ACL), and firewall filtering capabilities for any CGN device they plan to deploy.

11.3.11.3 IP Address Reputation

IP blacklisting is more problematic with multiple subscribers behind a single outside IP because the listing or banning of a single IP address will affect multiple users. All subscribers behind that IP are affected and any subscriber behind that IP can cause the listing. Some examples of this include:

- Secure transactions (Banking, Storefronts, etc.)
- Email spam lists (Spamhaus, etc.)
- Individual website blocking (comment spam, etc.)

In addition to the added scope, CGN makes blacklisting more difficult to troubleshoot and ultimately requires CGN logging in order to determine what subscriber caused the problem in the first place.

11.3.12 Logging

The use of CGN poses additional challenges to ISPs in responding to law enforcement requests or attack/abuse reports. In order to respond to such requests to identify a specific user associated with an IP address, an ISP will need to map a subscriber's internal source IP address and source port with the global public IP address and source port provided by the CGN, for every connection initiated by the user. An example of this identity trace back is illustrated in Figure 88.

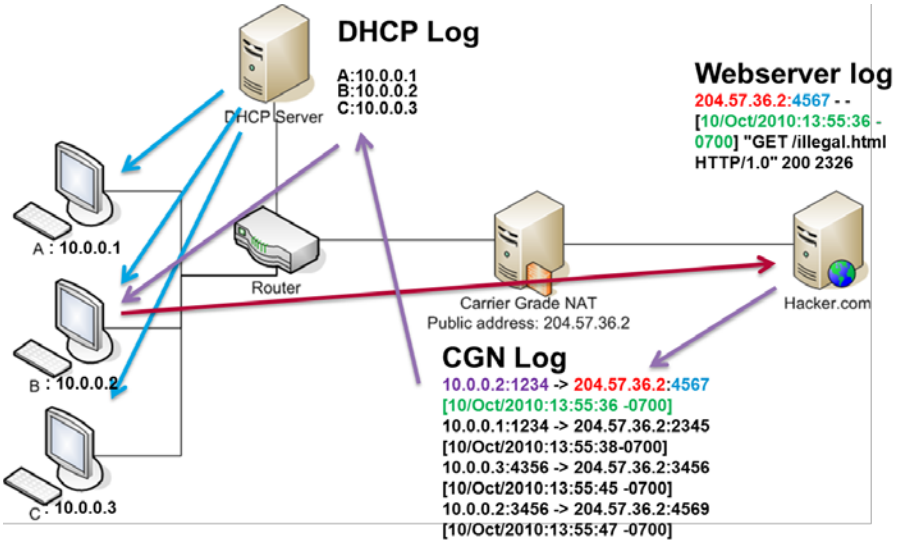

Figure 88 - CGN Subscriber Identity Traceback Illustration

This information will need to be gathered and stored for use by the provider for various downstream functions. Should the provider need to respond to security requests due to abuse from within the network (CGN-based customer), logs of the historic translations made by the CGN system would need to be available. Certain legalities may be involved when operators turn on such features due to privacy concerns related to the recording of the translation state which in turn tracks the overall usage characteristics of the customer.

CGN connection logging satisfies the need to identify attackers and respond to abuse/law enforcement requests, but it imposes significant operational challenges to ISPs. The primary goal of all operators who implement CGN with regard to logging is to reduce log volume. This can be done in several ways. The most widely supported option today is block port reservations, which can reduce logging up to 100x by reserving blocks of ports instead of individual ports. Log compression is another method that reduces volume, but not the search time. The best option is a deterministic reservation, which can almost eliminate the need for logging completely but is not supported by any vendors today.

11.3.12.1 Deterministic Port Reservation

To significantly reduce logging volumes, CableLabs proposes a technique to deterministically map internal addresses to external addresses in such a way as to be able to algorithmically calculate the mapping without relying on per connection logging.

Deterministic NAT requires configuration of the following variables:

- Inside IPv4/IPv6 address range (I);
- Outside IPv4 address range (O);
- Compression ratio (e.g., inside IP addresses/outside IP addresses) (C);

- Dynamic address pool factor (D), to be added to the compression ratio in order to create an overflow address pool;
- Maximum ports per user (M); and
- Reserved TCP/UDP port list

The compression ratio must be equal to or greater than the number of inside addresses divided by the number of outside addresses ***(C ≥ I/O)***. The inside address range divided by the compression ratio results in the number of ports per user ***(I/C = ports/user)***.

The following process is then carried out by the CGN to allocate ports:

1. Reserved ports are removed from the list of available ports on each IP address in the outside range (e.g., well known ports 1-1024).
2. Each internal IP address is allocated 1/(C+D) of the available ports. All remaining ports are allocated to the dynamic "bulk" pool.
3. When a subscriber initiates a connection, or makes some other request for ports (e.g., Port Control Protocol (PCP), they use one of the ports allocated to their internal IP address in step 2. No logging is required for these transactions.
4. If a subscriber uses all of the ports allocated to their internal IP address in step 2, they are allocated a block of ports from the dynamic "bulk" pool (up to the configured maximum ports per user). These dynamic allocations must be logged.

The primary limitation to this approach is that it requires low compression ratios.

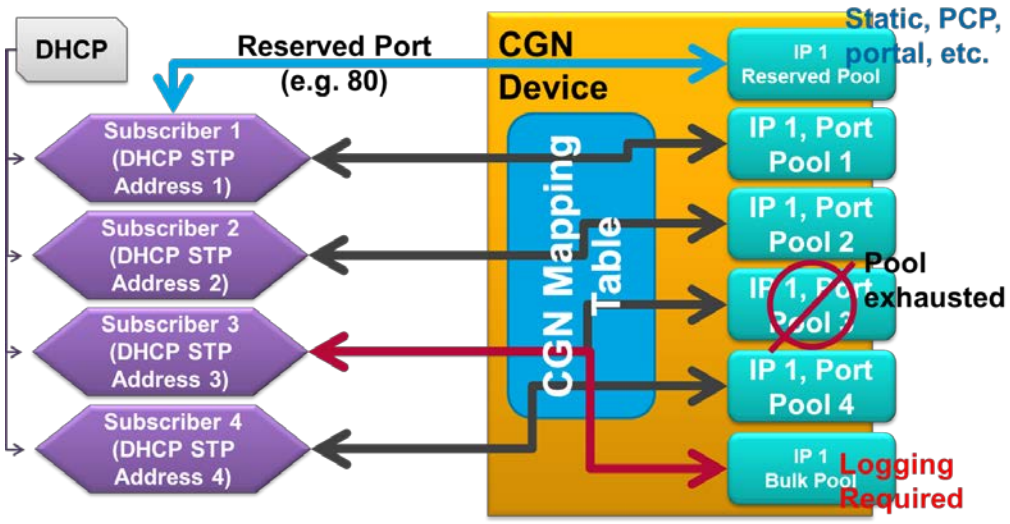

Figure 89 - Deterministic NAT Illustrated

11.3.12.2 CableLabs Logging Observations

CGN logging capabilities vary widely amongst vendor implementations. Because of the lack of standardization for CGN logging capabilities, CableLabs testing in this regard is highly observational in nature. Our testing focus was primarily on the level of detail provided, the ability to configure and control the data collected in the log file, and the ability to offload logged data to remote servers, e.g., Syslog.

Among the CGNs tested, there was relative consistency in the data elements that are reported.

- Time stamp
- Source IP/Port

- NAT IP/Port
- Destination IP/Port
- Host Name
- Event Priority/Severity

In addition to the above, there are typically vendor-specific translation codes that indicate whether a message is based on creating a new connection, freeing a port mapping, deleting a session, etc.

Vendor implementations vary in the ability to configure local log templates that control the level of data that is collected in the local log. Some implementations provide fixed templates with no ability to alter them. This placed full dependency on Syslog for altering the structure of the log messages collected, or for the amount of data that was stored. Other vendor implementations provided some degree of control for determining the type of data collected in the local log, which offered some, albeit minimal, mechanisms for controlling the amount of data to be offloaded. Event priority or severity appeared to be controlled exclusively by the Syslog server. So, for reporting of messages based on criticality, it was necessary to configure this in Syslog itself.

Another observation was that informational messages coming from the CGNs generally appear to be large. In one implementation, the average message for NAT444 was in the range of 150-450 bytes. For the same device, the average message for DS-Lite was even greater: 173-542 bytes. Given the lack of configurability for the data template, this did raise a concern about the amount of data that would be collected over time, as well as the ability to parse this data on an individual subscriber basis.

One CGN vendor that we tested had an ability to alter the contents of the local log. We saw an ability to reduce messages for NAT444 into a range that was less than 150 bytes. However, at the time of this writing, more extensive testing of this capability had not been completed.

Given our observations on the state of current products, per-connection logging will generate enormous quantities of data.

12 HOME AND ACCESS SECURITY USE CASES

12.1 Introduction, Overview, and Scope

The Home and Access Security use case provides a high-level description of the threats introduced in the cable network due to IPv6, a security analysis of the threats, and recommendations on control methods to mitigate the threats.

This use case will discuss IPv6 security issues and related considerations as it applies to the DOCSIS access network and also within the subscriber home. The use case will address various threats in the cable network as related to IPv6 and identify potential controls and recommendations on ways to mitigate the threats. The focus will be on the following three areas:

- First is the MSO headend, including any tunnel servers, CGN devices, and other security appliances at the headend. This would include analysis of threats due to transition technologies like 6RD, DS-Lite, NAT 444, and other tunneling technologies like Teredo, 6to4 etc.
- The next area would be the DOCSIS Link between the CMTS and CM and protection of these devices and the access network bandwidth against misuse and attacks.
- Lastly it will consider IPv6-enabled devices in the subscriber home, various threats faced by them (including home gateway devices), and ways to protect the home against these threats.

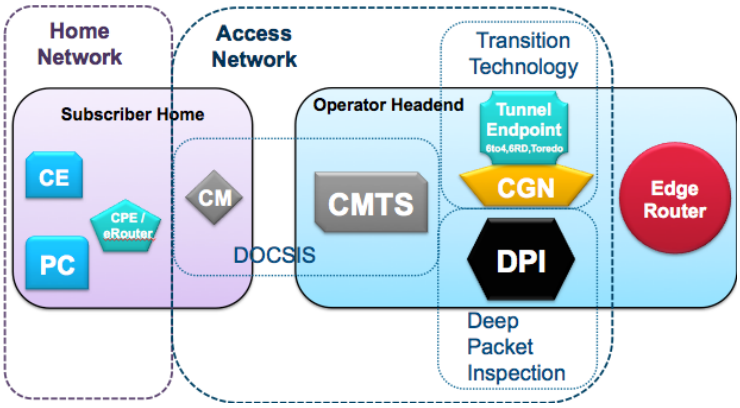

Figure 90 - Scope of Security Focus Areas

12.1.1 Security Threats under Consideration

The threats considered here are the most common security threats:

- Theft of Service (Authorization)
- Unauthorized Access (Authorization)
- Loss of Privacy (Confidentiality)
- Tampering (Integrity)
- Spoofing (Authentication)
- Denial of Service (Availability)

12.1.2 Areas Under Consideration

The following are the areas within the MSO network that are considered in the following use case.

12.1.2.1 DOCSIS/Access Network Security

These are security concerns relating specifically to DOCSIS and include the following: CMTS/CM, BPI+, UDCs and ACLs, Bandwidth Enforcement, Provisioning, DHCPv6, etc.

12.1.2.2 Home Network Security

These are security threats and considerations within the subscriber home network and include the following: Simple Security [RFC6092], Home Gateway's (CPE Router) and eRouter, Firewalls, Directly Connected Hosts, IPv6 Addressing/Privacy Extensions/ULAs, GUAs, Neighbor Discovery Protocol, DNS.

12.1.2.3 Transition Technologies

These are the possible vulnerabilities with various transition technologies, and how to best address them. This includes Protocol 41 : 6to4, 6RD, Teredo, CGN, NAT444, and DS-Lite.

12.1.2.4 Deep Packet Inspection (DPI)

These are IPv6 specific concerns with regard to DPI and includes: Protection from customer (Outbound), Protection for customer (Inbound),Tunnels, Native IPv6

12.1.2.5 Home and Access Security – Out of Scope

The following topics are out of scope: Intrusion detection Systems/Intrusion Prevention Systems, Flow Label Uses, QoS, (IVI) + (A+P), IPSec(IPv6), Client Application Security: Voice and dual-stack media (PacketCable Security), Web Content/MSO web servers, Video services, and Multicast/Anycast.

12.1.2.6 Dual-Stack Security Analysis

Dual-stack implies at least two times more security threats, since network now supports both IPv4 and IPv6. This essentially means the need for security feature parity between IPv4 and IPv6 services (i.e., the same security features that were applied to the IPv4 devices) now need to apply to IPv6 devices.

12.2 DOCSIS Security

12.2.1 Overview and DOCSIS Security Review

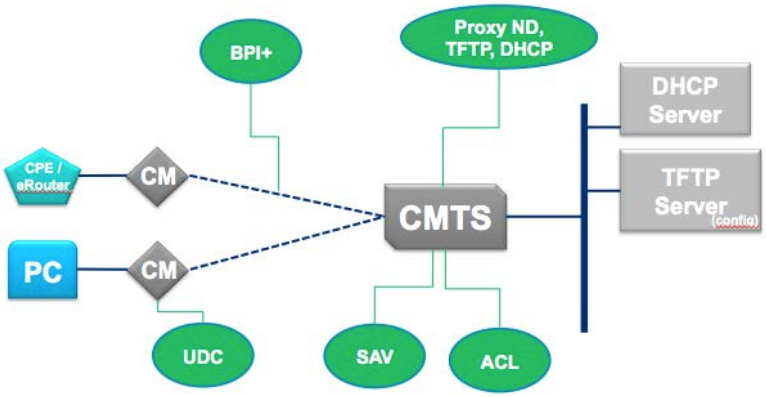

Figure 91 - DOCSIS Security Snapshot

The DOCSIS Specifications define many security mechanisms. Some of these are summarized in the diagram above and the table below.

Table 5 - DOCSIS Security Mechanisms

Control	Brief Description	Applicability
Baseline Privacy Plus (BPI+)	- CM authentication (public-key crypto) - Key exchange using BPKM - Establishing encrypted traffic sessions between CM and CMTS	IPv4, IPv6
Early Authentication and Encryption (EAE)	- Network admission control - Only authenticated CMs are allowed to continue with initialization	IPv4, IPv6
Provisioning Security	- DHCP, ToD, and TFTP protocols are secured using EAE when enabled	IPv4, IPv6
Reconfigure Key Authentication Protocol DHCPv6	- Provides protection against misconfiguration caused by a Reconfigure message sent by a malicious DHCP server.	IPv6 only
TFTP Proxy	- CMTS hides the IP address of TFTP server	IPv4, IPv6
Configuration file security	- Enforces configuration file name and content - CMTS MIC	IPv4, IPv6
Source Address Verification (SAV)	- Prevents CPEs behind CM from IP address spoofing.	IPv4, IPv6
Address Resolution Security	- Covers both ARP and ND	IPv4, IPv6
Secure Software Download	- Allows download of CM software image securely	IPv4, IPv6
At CM	- Upstream Drop Classifiers – IPv4 and v6 - IP Filtering: RFC [RFC4639] DOCS-CABLE-DEVICE-MIB	IPv4, IPv6 IPv4 only
At CMTS	- Access Control Lists - Subscriber Management MIB	IPv4, IPv6

Certain protocols should be dropped/rate-limited at earliest possible element to avoid consumption of DOCSIS network resources; mechanisms to achieve this could be Filtering or Rate-Limiting using IP classifiers and Service Flows.

12.2.2 Security Threats for DOCSIS

The main threats to DOCSIS networks are classified into the following main areas.

- Theft of Service (Authorization): This includes CM MAC Cloning, Bypassing BPI, Config File Tampering, Bandwidth Limits Via Classifiers, Server Hosting, etc.
- Unauthorized Access (Authorization): No Significant threats were identified.
- Loss of Privacy (Confidentiality): This includes Snooping user Traffic on DOCSIS network, Unauthorized access to other home networks and data.
- Tampering (Integrity): No Significant threats.
- Spoofing (Authentication): This includes IP address spoofing, Source Based Routing etc.
- Denial of Service (Availability): This includes Attack on TFTP server, Attack on DHCP Server, Malicious DHCP server: non-MSO DHCP Server, Rouge RAs, DAD DoS, ICMPv6 / ND attacks etc.

12.2.3 Theft of Service

Description of Threat: This essentially involves using MSO services without authorization.

12.2.3.1 Attack - CM MAC Cloning

This mainly involves copying the MAC address of a modem that is legitimately paid for by a subscriber. This allows the hacker to receive same level of service as paying customer on the MSO network.

12.2.3.1.1 Controls and IPv6 Impact

BPI+ authentication includes digital certificate CM MAC address validation, which helps prevent CM MAC address cloning and theft of service. Secure Software Download also authenticates download of CM software image securely.

The IPv6 Impact is indirect to the MSO.

12.2.3.2 Attack - Bypassing BPI

Hackers could modify a CM's behavior in order to bypass BPI+ authentication and steal service using MAC address cloning.

12.2.3.2.1 Controls and IPv6 Impact

Enforcing BPI+ on the CMTS will help prevent this type of attack. All traffic to all CMs must be encrypted.

Enabling Secure Software Download will also mitigate this attack.

The IPv6 Impact is indirect to the MSO.

12.2.3.3 Attack - Config File Tampering

Here the hacker modifies the CM configuration file, gets the CM to use hacked file, and obtains a higher Quality of Service (e.g., data speed) than it is authorized for.

12.2.3.3.1 Controls and IPv6 Impact

DHCP and TFTP Proxy: CMTS verifies that a CM is registering with correct parameters by learning CM provisioning information in DHCP and TFTP messaging flows.

Enabling the CMTS MIC is another method to prevent any configuration file tampering.

The IPv6 Impact is indirect to the MSO.

12.2.3.4 Attack - Bandwidth Limits via Classifiers

Here the hacker uses IPv6 to get around IPv4 rate limits and gets his traffic past the configured classifiers.

12.2.3.4.1 Controls and IPv6 Impact

The controls can be on the CM side and the CMTS side. On the CM Upstream, the MSO can use UDCs to drop certain kinds of traffic. IP Filtering can also be enabled for this purpose [RFC4639] (IPv4 only). The mechanisms on the CMTS are ACLs and the Subscriber Management MIB.

These can be configured to rate limit those traffic types.

The IPv6 Impact is direct to the MSO in that they need to create proper IPv6 Classifiers.

12.2.3.5 Attack - Server Hosting

Here the user hosts an unauthorized server behind residential CM using unauthorized service

12.2.3.5.1 Controls and IPv6 Impact

The MSO can configure the CMTS to use ACLs or UDCs on the CM to make sure this unauthorized traffic does not get through the access Network.

The IPv6 Impact is direct to the MSO in that they need to create proper IPv6 Classifiers.

12.2.4 Loss of Privacy

Description: Gaining unauthorized access to subscriber data.

12.2.4.1 Attack - Snooping User Traffic

The Security Attack is on DOCSIS network where the hacker gains access to the user traffic on the access network.

12.2.4.1.1 Controls and IPv6 Impact

The use BPI+ is paramount as it establishes encrypted traffic sessions between the CM and CMTS.

The IPv6 Impact is indirect to the MSO.

12.2.4.2 Attack - Unauthorized Home Network Access

The hacker gains unauthorized access to other home networks, and data maybe using protocols, such as mDNS, Bonjour, uPnP, etc.

12.2.4.2.1 Controls and IPv6 Impact

The main form of control to prevent these types of attacks are to use Access Control Lists ACLs and UDCs to block LAN protocols.

The IPv6 Impact is direct to the MSO in that they need to create proper IPv6 filters.

12.2.5 Spoofing

Description: Altering packets sent over the DOCSIS network with malicious intent.

12.2.5.1 Attack - IP Address Spoofing

The IP Address Spoofing attack is used as a basis for other attacks, for example DoS. The attack could also involve using unauthorized IP address space.

12.2.5.1.1 Controls and IPv6 Impact

Enforcing Source Address Verification (SAV) at CMTS to match traffic with MSO assigned address (DHCP/Static - Not SLAAC) will prevent this attack. Also the appropriate RA Configuration will help mitigate this attack.

The IPv6 Impact is direct here for the MSO, as they need to enable SAV for IPv6 and also ensure that the routers do not advertise the Prefix in RA and set M Bit.

12.2.5.2 Attack - Source Routing

This attack involves Network discovery, directing traffic back to a host with a spoofed address, and amplifying traffic in a DoS attack.

12.2.5.2.1 Controls and IPv6 Impact

The main controls for these are UDCs and ACLs.

The IPv6 impact here is direct as the MSO needs to configure devices to filter (drop) all IPv6 packets that contain routing header type 0 (RH0).

12.2.6 Denial of Service

Description: An attempt to make DOCSIS service unavailable to its intended users.

12.2.6.1 Attack - DoS Attack on TFTP service

The hacker mounts a DoS attack on the TFTP Service.

12.2.6.1.1 Controls and IPv6 Impact

The main controls for this attack is enabling Early Authentication and Encryption (EAE) on the DOCSIS network. This is a form of network admission control where only authenticated CMs are allowed to proceed with DHCP and TFTP. The TFTP transaction is secured using BPI+ when EAE is enabled. Also the CMTS supports a TFTP Proxy functionality where the CMTS hides the IP address of TFTP server. Setting the TFTP timers to appropriate values can also help to mitigate this attack.

The IPv6 impact is indirect to the MSO, as there is no separate configuration need for IPv6.

12.2.6.2 Attack - DoS Attack on DHCP Server

12.2.6.2.1 Controls and IPv6 Impact

The main controls for this attack are as follows: enabling EAE and DHCPv6 timers. This way the DHCPv6 transactions are using BPI+ when EAE is enabled. The MSO can also set out the MAX CPE setting in the CM configuration file, which will prevent traffic changed by the hacker to look like it is coming from multiple devices. Also, the CMTS DHCP Relay agent marks requests with CM Message Authentication Code (MAC) so that DoS attacks cannot succeed.

The IPv6 impact is indirect to the MSO as there is no separate configuration need for IPv6 other than using the DOCSIS 3.0 Security features.

12.2.6.3 Attack - Malicious DHCP Server: - non-MSO DHCP Server

12.2.6.3.1 Controls and IPv6 Impact

This form of an attack can be prevented by using a list of Authorized DHCP Relay Agents on CMTS. Other forms of controls are ACLs, UDCs, etc. The Reconfigure Key Authentication Protocol (RKAP) DHCPv6 also provides protection against a malicious DHCP server.

The IPv6 impact is direct to the MSO. The MSO needs to ensure that they enable RKAP on their DHCP Server, configure DHCPv6 Relay, and also configure any needed IPv6 UDCs and ACLs.

12.2.6.4 Attack - Rogue RAs

This attack is one where the hacker manages to introduce an unauthorized router on the network and uses it to send bad configuration to the clients

12.2.6.4.1 Controls and IPv6 Impact

The main forms of control here are to control access in the DOCSIS network, where the CMTS is configured to reject any RA from RF, and the CM is configured to filter out RAs going upstream.

The IPv6 Impact is direct to the MSOs.

12.2.6.5 Attack - DAD DoS

In this form of DoS attack the attacker responds to every DAD message on the network.

12.2.6.5.1 Controls and IPv6 Impact

The control to prevent this attack is a feature called ND proxy on the CMTS. Today this is an optional feature on D3.0 CMTS. When enabled, the CMTS does not forward any ND Packets received on an upstream channel to any downstream channel. The IPv6 impact is direct as the MSO needs to mandate that the CMTS support ND Proxy and also enable the ND proxy feature.

12.2.6.6 Attack - ICMPv6 Attacks

DoS/DDoS attacks on MSO infrastructure can use ICMP; these include ICMP flooding (smurf attacks, ping floods, ping-of-death, etc.)

12.2.6.6.1 Controls and IPv6 Impact

The main controls against ICMP attacks are UDCs, ACLs, etc. Also, DOCSIS 3.0 supports ICMP Classifiers, which can be used to rate limit or drop packets matching this attack. This rate limit (or drop) at the message type/code level will assist with growing IPv6 security considerations, e.g., messages like echo-request and echo-reply can be set to have lower rate limits than ND messages. The IPv6 impact is direct as the MSO needs to enable IPv6 UDCs and ACLs.

12.2.7 DOCSIS Threats and Controls Summary

Threats	Attack	Controls	IPv6 Impact
Theft of Service	CM MAC Cloning	BPI +, SSD	Indirect
	Bypassing BPI	BPI +, SSD	Indirect
	Config File Tampering	DHCP Proxy and TFTP Proxy, CMTS MIC	Indirect
	Bandwidth Limits Via Classifiers	UDC, IP Filters, ACLs	Direct
	Server Hosting	UDC and ACL Filtering, DPI	Direct
Loss of Privacy	Snooping user Traffic on DOCSIS network	BPI +	Indirect
	Unauthorized access to other home networks and data	UDC and ACL Filtering	Direct
Spoofing	IP Spoofing	SAV	
RA Configuration	Direct		
	Source Based Routing	UDC and ACL Filtering	Direct
Denial of Service	Attack on DHCP Server	DHCP Relay, EAE	Indirect
	Attack on TFTP server	TFTP Proxy, EAE	Indirect
	Malicious DHCP server: non-MSO DHCP Server	DHCP Relay Agent on CMTS	
ACLs, UDCs			
RKAP	Direct		
	Rogue RAs	DOCSIS RA Filtering	Direct
	DAD DoS	ND Proxy	Direct
	ICMPv6 / ND attacks		
IP address Cloning		UDCs, ACLs	Direct

12.2.8 DOCSIS Security Recommendations

- Enforce BPI+.
- Apply proper filtering using UDCs and ACLs:
    - Migrate to UDCs with IPv4 and IPv6 parity.
    - Update CMTS ACLs to IPv4 and IPv6 parity.
    - Drop all RH0 packets.

- Enable EAE.
- Enable TFTP Proxy and Enable Config File Learning.
- Enable Source Address Verification.
- Enable ND Proxy.
- Enable RKAP for DHCPv6 Server.

12.3 Home Network Security

12.3.1 Overview

This part of the security use case deals with security threats and related security considerations within the subscriber home network. This includes the following topics:

- Standards, such as [RFC6092], [RFC4864], and [ID-HNA_IPV6]
- Devices, such as Home Gateway's (CPE Router), eRouter, and Directly Connected Hosts
- Technologies, such as Firewalls and IPv6 Addressing/Privacy Extensions, ULAs, GUAs

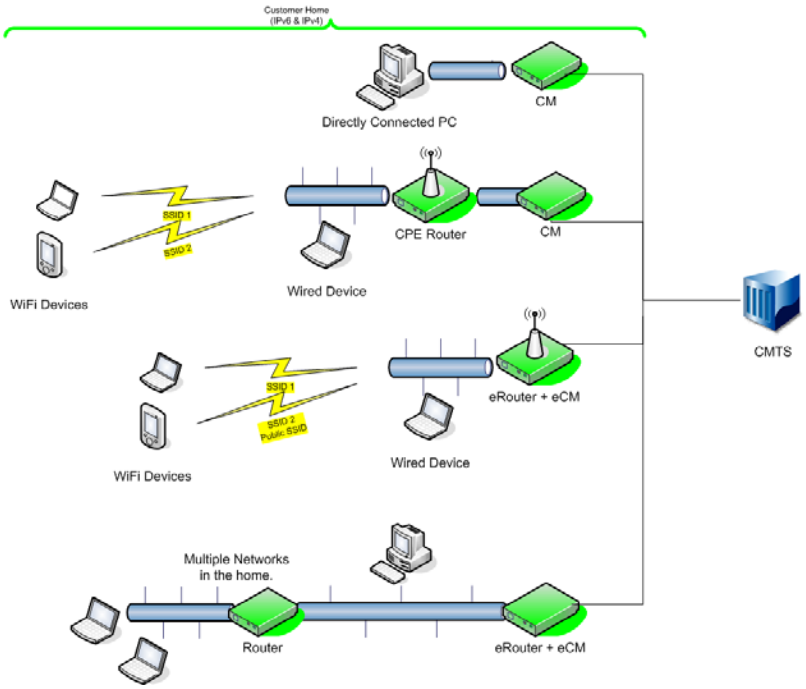

Figure 92 - Home Network Topologies

12.3.2 Scope and Out of Scope

This use case considers the following scenarios: A PC directly connected to CM, an eRouter behind CM, a CPE Router behind CM, Multiple Routers and Subnets within the home, Home Wi-Fi, and Dual-Stack Networks.

The following is considered out of scope: Multi-Homing (i.e., Dual ISP connections), DNS Server in the home, Public Wi-Fi (Wi-Fi Roaming attacks), Mobile IP (this includes mobility extensions for IPv6, PMIP).

The security threats considered for the home network are: Theft of Service (Authorization), Unauthorized Access (Authorization), Loss of Privacy (Confidentiality), Tampering (Integrity), Spoofing (Authentication), and Denial of Service (Availability).

12.3.3 Theft of Service

12.3.3.1 Attack: via Wireless – Wi-Fi

Here the hacker uses the Home Wi-Fi connection as a starting point to launch his attacks into the home network.

12.3.3.1.1 Controls and IPv6 Impact

MSOs have a few controls to easily prevent these attacks. For managed Wi-Fi deployments, the operators configure the Gateway to use secure Wi-Fi (WPA or WPA-enterprise). For unmanaged Wi-Fi, the operators suggest strongly to their customers to secure their Wi-Fi (WPA). The CPE Router could also be configured with MAC address ACLs. The IPv6 impact is indirect to the MSO.

12.3.3.2 Attack - via Wired – MOCA and Ethernet

Here the hacker uses the home-wired ethernet connection as a starting point to launch his attacks into the home network.

12.3.3.2.1 Controls and IPv6 Impact

The main controls to prevent these attacks are to use MAC address ACLs on CPE Router. The IPv6 impact is indirect to the MSO.

12.3.3.3 Attack - Network Scanning

Here the hacker determines what hosts are on the home network and uses this as a reconnaissance for other attacks. There are multiple methods to accomplish this and could include: Ping sweeps, DHCPv6 discovery, DNS scraping, etc.

12.3.3.3.1 Controls and IPv6 Impact

The main controls to prevent network scanning are as follows: Use SLAAC or "randomized/unique" DHCPv6, use filters as defined by recommendation-9 in [RFC6092] or [ID-IPv6SEC] section 3.1.7, and use of DNS masking.

The IPv6 impact to IPv6 is direct as the MSO could affect the following changes in the network. This includes use of SLAAC or a unique DHCPv6 configuration in the home network, and the MSO could configure the network to drop (not process) inbound DHCPv6 discovery packets [RFC3315] received on exterior interfaces. Also the MSO does not populate DNS records to prevent Network Scanning.

12.3.3.4 Attack - Exploiting Host vulnerability

Here the hacker exploits known host vulnerabilities to gain access to the attacked host.

12.3.3.4.1 Controls and IPv6 Impact

The main controls to prevent exploits of host vulnerability are Firewalling (filters). These could be based on [RFC6092] or [ID-IPv6SEC].

The IPv6 impact to this is direct, since the MSO could affect the following changes in the network: configuring firewalling using static rules or dynamic rules (IPS), or implementing a layered security approach.

12.3.3.5 Attack - Virus/Trojan/Malware

Here the hacker exploits infection of home network device via virus/Trojan/malware programs.

12.3.3.5.1 Controls and IPv6 Impact

The main controls against these types of attacks can be classified as host-based (i.e., antivirus software), content-based [i.e., use of HTTPS or Domain Name System Security Extensions (DNSSEC)], or home gateway-based (which can be used to filter malicious websites). The IPv6 Impact is indirect to the MSO.

12.3.3.6 Attack - Access to Local Device

The hacker tries gaining access to a device that only requires local network connectivity (sensors, appliances, etc.).

12.3.3.6.1 Controls and IPv6 Impact

The main controls here are for the MSO to configure the correct filters in the home gateway, to prevent access and the use of ULAs in the network. The IPv6 impact is direct as the MSO needs to apply proper filters to deny access to local devices on home CPE router and investigate the possibility of use of ULAs for local device communication.

12.3.4 Spoofing

12.3.4.1 Attack - Spoofed source Address

Here the hacker spoofs the source IP address on packets leaving the home network.

12.3.4.1.1 Controls and IPv6 Impact

The main controls here are for the MSO to configure the correct filters, using BCP 38 [RFC2827], and deny any traffic going upstream sourced with ULAs.

The IPv6 impact is direct as the MSO needs to only allow traffic with a valid source address to leave the home network. This configuration could be done on the Home CPE router/CM.

12.3.4.2 Attack - Spoofed Source Address

Here the hacker spoofs the source IP address on packets entering the home network.

12.3.4.2.1 Controls and IPv6 Impact

The main controls here are for the MSO to configure the correct filters, i.e., deny Bogon/Martian source addresses. The IPv6 impact is direct as the MSO needs to only allow packets sourced from 2000::/3, or only allow IPv6 blocks allocated to RIRs. This configuration could be done on the Home CPE router.

12.3.4.3 Attack - Source Routing

In this form of Source routing attack involves network discovery, directing traffic back to a host with a spoofed address, and amplifying traffic in a DoS attack.

12.3.4.3.1 Controls and IPv6 Impact

The main controls here are for the MSO to configure the correct filters on the home gateway. The IPv6 impact is direct, since the MSO needs to filter (drop) all IPv6 packets that contain routing header type 0 (RH0) on the Home CPE router.

12.3.5 Loss of Privacy and Tampering

12.3.5.1 Attack - Snooping

Here the hacker manages to snoop user traffic on wireless network.

12.3.5.1.1 Controls and IPv6 Impact

The main controls here are for the MSO to configure the use of WPA to encrypt traffic sessions between the client and AP, and if possible encrypt application traffic using TLS or IPSec between the client and the service. Also adding requirements to the home router to randomly change source address ([RFC4941], DHCPv6) over time will help against snooping attacks. The IPv6 impact is direct as the MSO needs to configure the Home DHCP server with short lease times.

12.3.5.2 Attack - Man-in-the-Middle

Here the hacker mounts a man-in-the-middle (MITM) attack on the home wireless network.

12.3.5.2.1 Controls and IPv6 Impact

The main controls here are for the customer to use some form of mutual authentication: either via Link layer (WPA) or via Application layer features (for example, TLS or IPSec). The IPv6 impact is indirect as the customer needs to enable these security features.

12.3.6 Denial of Service

12.3.6.1 Attack - Overwhelming Home Network

Here the hacker mounts an attack on the home network by using packet-flooding techniques, such as TCP-SYN flood, UDP flood, corrupted packets, etc., or spoofed multicast ping messages (Smurf attack). The hacker can also target device-specific vulnerabilities, which could include attacking devices (e.g., printer) inside the home and making them unusable (e.g., CPU exhaustion) for home users.

12.3.6.1.1 Controls and IPv6 Impact

The main controls here are for the MSO to use some form of firewall and filters [RFC2827], [RFC3704], and [RFC6092]. This includes configuration to deny certain incoming control protocols (e.g., print) from outside and deny pings to multicast addresses. Other security controls could involve efforts to monitor, trace, and report anomalous activity. Up-to-date software, virus protection, and signature database are always necessary. Advanced security controls, such as an intrusion detection system, could help with these attacks as well as rate limiting malicious IP traffic.

The IPv6 impact is direct as the MSO needs to configure filters for IPv4/IPv6 parity on the Home CPE router.

12.3.6.2 Attack - Outbound Attacks

These are attacks originating from the Home network, e.g., a PC in the home could unknowingly be part of a botnet.

12.3.6.2.1 Controls and IPv6 Impact

The main forms of security controls for the MSO are to proactively communicate with subscribers about potential problems in the subscriber network (e.g., would be of the type Comcast Constant Guard). Also ensuring that the anti-virus software is up to date to prevent botnets/malware/etc., becomes a necessity. The IPv6 impact is direct as the MSO needs to update MSOs security systems for IPv4/IPv6 parity.

12.3.6.3 Attack - Neighbor Discovery

These are situations where the hacker uses weakness in the ND Protocol to mount attacks on IPv6 clients (including things like fake RAs). The hacker could also install an unauthorized DHCPv6 Server in an attempt to attack hosts on the network.

12.3.6.3.1 Controls and IPv6 Impact

The main forms of security controls for the MSO are to educate users to secure their network in order to prevent miscreants from getting access to the home network LAN. The MSO could also setup the access network to drop unauthorized ND messages from the home network. Controls used against the Theft of Service attacks could also be applicable here.

The IPv6 impact is direct as the MSO needs to ensure security configuration on home CPE router. On the access network, turning on ND proxy at the CMTS will also help against ND attacks.

12.3.7 Home Network Threats and Control Summary

Threats	Attack	Controls	IPv6 Impact
Theft of Service	Wireless Access	Secure network using WPA, MAC Address ACLs	Indirect
	Wired Access	Secure network using MAC Address ACLs	Indirect

Threats	Attack	Controls	IPv6 Impact
Unauthorized Access	Network Scanning	SLAAC, random DHCPv6, DHCPv6 filtering, DNS Masking	Direct
	Exploiting Host vulnerability	Firewalling	Direct
	Virus Trojan Malware	Antivirus software, HTTPS, DNSSEC, Filter malicious websites	Indirect
	Local Network Device	Filters, ULAs	Direct
Loss of Privacy and Tampering	Snooping wireless Traffic	Link layer (WPA), DHCPv6 short lease times	Direct
	Man-in–the-middle Attack	Link layer (WPA)	Indirect
Spoofing	Spoofed address leaving network	Filtering per [RFC2827]	Direct
	Spoofed address entering network	Bogon/Martian filtering	Direct
	Source Routing	Filtering RH0	Direct
Denial of Service	Overwhelming home network, device requests, Smurf attacks	Filtering per [RFC2827], virus protection software, intrusion detection system, Rate limiting IP traffic	Direct
	Outbound Attacks	MSO Security Systems, virus protection software	Direct
	ND attacks	Secure Home network, ND proxy on CMTS	Direct

12.3.8 Home Network Security Recommendations

- Theft of Service, Loss of Privacy, and Tampering
    - Inform subscribers of Wi-Fi security threats and how to prevent them, and guide subscribers on how to setup a secure Wi-Fi network using WPA.
    - Wi-Fi Gateway devices must support CableLabs Wi-Fi gateway spec and SNMP MIBs, Monitor Wi-Fi network security status using these MIBs.
    - Configure DHCP Server with short lease times.
- Unauthorized Access
    - Do not populate DNS records in the MSO network.
    - Use SLAAC or a unique DHCPv6 configuration in the home network.
    - Drop inbound DHCPv6 discovery packets received on home gateway exterior interfaces.
    - Configure firewalls with IPv4/IPv6 parity and any needed additional IPv6 specifics.
    - Apply proper filters on home gateway to deny access to local devices.
    - Inform subscribers of the importance of antivirus software, HTTPS, and online safety.
- Spoofing
    - Allow only traffic with valid source addresses to transit the home gateway.
    - Configure Bogon/Martian filtering and RH0 Filtering on home gateway.
- Denial of Service

- Turn on ND Proxy on CMTS.
- Update MSO security systems for IPv4/IPv6 Parity.
- Implement firewall and filters (e.g., [RFC2827], [RFC3704], and [RFC6092]) Intrusion Detection Systems, Rate limits.

12.3.9 Firewalls and Filtering

Firewalls protect networks from unauthorized access using filtering rules. The main types of firewalls are stateless, stateful, and application layer firewalls.

The IETF has developed firewall standards/guidelines for IPv6 networks, these include the following:

1. Simple Security [RFC6092]: This is a set of recommended security capabilities for IPv6 residential CPE; it defines firewall filtering rules for IPv6 traffic.
2. Advanced Security [ID-IPv6SEC]: This supports the concept of end-to-end IPv6 reachability. It uses firewall adaptive filtering based on Intrusion Prevention System (IPS) functions.
3. Local Network Protection for IPv6 [RFC4864]: This recommends firewall functions that replace NAT security.

12.3.9.1 Simple Security

In a broadband home network, the gateway/router should be equipped with stateful firewall capabilities. The gateway/router needs to provide a default configuration where incoming traffic is limited to return traffic resulting from outgoing packets. It should also have an easy interface that allows users to create inbound 'pinholes' for specific purposes, such as online gaming.

Simple Security defines the following capabilities.

- Check all traffic to and from public Internet for basic sanity, e.g., filter for spoofs and misdirected ("Martian") packets [RFC4949].
- Allow tracking of application usage by source and destination network addresses and ports.
- Barrier against untrusted external influences on interior network by requiring filter state to be activated by traffic originating at interior network nodes.
- Allow manually configured exceptions to stateful filtering rules according to network administrative policy.
- Isolate local network DHCPv6 and DNS resolver services from public Internet.

Simple Security defines requirements in the following areas:

- Stateless Filters: Certain kinds of IPv6 packets MUST NOT be forwarded in either direction by residential Internet gateways regardless of network state. These include packets with multicast source addresses, non-routable and/or reserved prefix destination addresses, deprecated extension headers, etc.
- Connection-Free Filters: Some applications use connection-free transport protocols with no release semantics, e.g., UDP. Most application state is not carried at transport level, and state records are created when communication is initiated and are abandoned when no further communication is detected. Examples are Internet Control and Management, Upper-Layer Transport Protocols, UDP, IPsec, and Internet Key Exchange (IKE), Mobility Support in IPv6, etc.
- Connection-Oriented Filters: Connection-oriented filters are for protocols that require session establishment before data transfer. Examples are TCP, SCTP, DCCP, and Shim6.

Simple Security Additional Requirement: The cable industry consensus is that Simple Security is turned ON by default on the home gateway/router. Also by default, the internet gateway device needs to deny any protocol received on WAN (operator facing) interface not specifically allowed by configuration with the following exceptions: DHCP, ND, ICMP and established TCP and UDP flows, and IPSec (IKE/HIP). IP sec is intended to be

allowed only for IPv6; for IPv4, there should be no change from the same rules that apply today, i.e., block or drop IPsec traffic.

12.3.9.2 Advanced Security

Advanced Security is a firewall security model that allows most traffic to pass unless identified as harmful using a set of signatures; this supports the IPv6 concept of end-to-end reachability. Advanced Security uses an adaptive security policy, building on a Signature-based IPS (which requires a daily signature update). Advanced Security also uses a centralized address reputation database. It performs Local and Global correlation to prioritize attack signature inspection based on local host OS and application support, and prioritize attack signature inspection based on information received from distributed IPS on the Internet. The IETF draft [ID-IPv6SEC] provides an example set of configurable rules.

Pros: Advanced Security supports the concept of IPv6 end-to-end reachability, and implements an adaptive security policy to allow the CPE router to detect new attacks shortly after they are discovered. It is also a potential new service to offer subscribers.

Cons: A centralized database must be maintained to support IPS traffic signature and IP address reputation score, which is a big burden. Also processing and storage requirements may exceed simple residential CPE router capabilities, as the local storage requirements is expected to be > 100 MB.

12.3.9.3 Simple Security vs. Advanced Security

Simple Security defines traditional firewall filtering functions for IPv6 traffic, includes Stateless and Stateful filters, Connection and connectionless protocols, and Application layer protocols.

Advanced Security supports concept of end-to-end IPv6 reachability and uses firewall adaptive filtering based on IPS functions. It requires a remote service for keeping traffic signatures and other information up to date.

12.3.9.3.1 Requirements Summary

The cable industry consensus around the Simple Security requirements are as follows:

- Stateless Filters: *Must Support*
- Connection-Free Filters: ICMP, Upper-Layer Transport Protocols, UDP, IPsec, IKE: *Must Support*, and Mobility Support in IPv6: *Nice to Have*
- Connection-Oriented Filters: TCP, Shim6: *Must Support*, and SCTP,DCCP: *Nice to Have*
- Passive Listeners and Management Applications: *Nice to Have*

Advanced Security provides a complement to Simple Security through monitoring of traffic patterns using IPS and Local Correlation and other Configurable rules, which include: RejectBogon, AllowReturn, ProtectLocalOnly, and ParanoidOpeness. Advanced Security is not a replacement for Simple Security.

12.3.10 Miscellaneous Home Network Security Topics

12.3.10.1 Local Network Protection for IPv6 (RFC 4864)

[RFC4864] analyses the perceived advantages of NAT and discusses new tools available with IPv6. It provides methods to implement the perceived benefits of NAT with IPv6 technology and includes case studies with practical applications of IPv6 tools. It also documents standardization gaps (as of May 2007).

12.3.10.1.1 Replacing IPv4 NAT with IPv6 LNP

[RFC4864] discusses the concept of a Simple Gateway between the Internet and the Internal Network, and requires support for IPv6 and Simple Security; it also touches on user/application tracking at the home gateway for security purposes. It has recommendations on Privacy and Topology Hiding Using IPv6 and also touches on Independent Control of Addressing in a Private Network, Global Address Pool Conservation, and the topics of Multihoming and Renumbering.

12.3.10.1.2 IPv6 and Simple Security Implications

This includes built-in protections, such as privacy extensions that reduce attack profiles, and use of IPSec, as it is no longer inhibited by NAT and connections can now be initiated from either end. Also subnet ping sweeps are nearly impossible in IPv6. The recommendation is to use a stateful firewall [RFC6092] and [RFC6092].

12.3.10.1.3 Privacy and Topology Hiding Using IPv6

The recommendations here are around the use of Privacy Addresses [RFC4941] and Unique Local Addresses. It also discusses Untraceable IPv6 Addresses by injecting explicit host routes into the IGP, Use tunneling (e.g., Mobile IPv6), and Virtual LAN techniques. Typically this is a LAN management consideration and is implemented by end-users, not ISPs.

12.3.10.1.4 IPv6 Gaps Identified by RFC 4864

The main gaps identified are as follows:

- Simple Security - which is addressed in [RFC6092].
- Subnet Topology Masking - some optimizations or best practices are needed.
- Minimal Traceability of Privacy Addresses - a BCP on combining privacy addresses with topology hiding is needed.
- Site Multihoming - which is addressed by the SHIM6 WG.

12.3.10.2 IPv6 Addressing

The special IPv6 Address types considered here under the topic of security are privacy extensions and ULAs.

Global IPv6 Address assignment for a device in the home network can happen as follows:

- The IPv6 address is assigned by the DHCPv6 server, or
- Stateless address autoconfiguration.

12.3.10.2.1 SLAAC and Addressing Concerns

SLAAC uses MAC addresses to generate a 64-bit interface identifier; the interface identifier is appended to the delegated prefix for a 128-bit IPv6 address.

But SLAAC raises various concerns with the embedding of a fixed-interface identifier in the IPv6 address; mainly the IP address cannot be easily hidden. IPv6 addresses generated via SLAAC contains the same interface identifier, regardless of where a device connects. This facilitates tracking of individual devices (users) as they move across networks, and it becomes possible to correlate seemingly unrelated activity using this identifier. Note: Even the network prefix portion of an address could also serve as a constant identifier.

12.3.10.2.2 Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 4941)

[RFC4941] defines methods to create additional IP addresses based on a random interface identifier, which can be used for initiating outgoing sessions and can be defined for short time use (hours/days). The basic idea is to produce a sequence of temporary global scope addresses that appear to be random. A node highly concerned about privacy can use different interface identifiers on different prefixes.

The Privacy Address Generation Methods are as follows:

- Method #1: Stable storage present. Take the Previous ID (Initial value) and combine it with the Interface ID, Create an MD5 digest of the combination, use the leftmost 64 bits, set bit 6=0 → this is the Interface ID, ensure that the generated address does not match against previously used addresses.
- Method #2: No Storage present. This is same as the above method except that the initial value should be random.

[RFC4941] defines other rules around lifetimes of temporary addresses, performing DAD on generated addresses and deprecating temporary addresses, and generating new ones, etc.

12.3.10.2.3 Impacts of Privacy Extensions

Privacy Extensions create some big impacts on the network; the first is to affect the balance between two somewhat opposing needs protecting individual privacy versus effectively maintaining and debugging a network. When IP Addresses are changing over time, it makes it difficult to track/isolate operational problems. It becomes difficult to determine if the behavior is caused by a single errant machine or a number of them.

In the MSO network, privacy addresses do not seem to be a significant impact, other than seeing numerous addresses. Also Privacy Extensions are more applicable to devices behind an eRouter/CPE Router device.

Currently the level of support for Privacy addresses in host devices is not so widespread:

- On Windows devices it is enabled and used by default,
- On MAC or Linux platforms it is disabled by default, the generation of the privacy addresses and the preferred use can be activated,
- On the iPhone and Android OSes it is disabled by default.

12.3.10.2.4 Unique Local Addresses (ULAs)

[RFC4193] defines an IPv6 unicast address format that is globally unique and is intended for local communications only. The ULA is a globally unique prefix (high probability of uniqueness) It is a well-known prefix to allow for easy filtering at site boundaries, and if accidentally leaked outside of a site via routing or DNS, there is no conflict with any other addresses. In practice, some applications may treat these addresses like global scoped addresses, which is a real issue in deployment and it causes "IPv6 brokenness".

ULAs Security and Control

Local IPv6 addresses are created using a pseudo-randomly allocated global ID. ULAs use the FC00::/7 prefix, with the L bit set to 1, a 40-bit global identifier (pseudo random), a 16-bit Subnet ID, and the 64-bit Interface ID. ULAs are designed to be routed inside of a site, similar to other types of unicast addresses. The default routing configuration must filter out any ULAs, both incoming and outgoing. ULAs do not provide any inherent security to nodes; it may be used with filters at site boundaries to keep ULA traffic inside of site, but it is no more or less secure than filtering any other type of global IPv6 unicast address.

The main recommendation on ULAs is that MSOs do not want to allow traffic to/from unknown ULAs traveling on the MSO network. The best practice is to filter ULAs at both boundaries: at the customer edge filter out unknown ULAs (filtering could be at CMTS), and at the MSO-Internet edge filter out all ULAs.

12.3.10.3 Host Security Threats and Controls

Two of the main home-network security threats apply to host devices These are 'Unauthorized Access,' which includes exploiting host vulnerability and malware attacks, and 'Denial of Service,' which includes overwhelming the host processor with requests and ND attacks (redirection, duplicate address detection).

These attacks can come within the home network via unauthorized access to the wireless (Wi-Fi) network or via host devices infected with malware. The hosts can be protected by the following controls: turning on Wi-Fi WPA security, installing anti-virus software on the host, turning on the host firewall, Secure ND (SEND), etc.

12.3.10.3.1 Secure Neighbor Discovery (SEND) [RFC3971]

Neighbor Discovery Protocol (NDP) defined in [RFC4861] and [RFC4862], defines specific functions like ND, Address auto-configuration, Router Discovery (RD), Neighbor Un-reachability Detection (NUD), Address Resolution, Duplicate Address Detection (DAD), Redirection, etc.

SEND (defined in [RFC3971]) new Options to the base ND protocol; for example, Cryptographically Generated Addresses (CGA) Option, RSA Signature Option, Timestamp Option, Nonce Option, and Certification Path Solicitation, etc. DOCSIS devices do not support SEND today, and there is limited Device and OS support among Windows and MAC-based platforms.

12.3.10.3.2 Cryptographically Generated Addresses (CGA) RFC 3972

[RFC3972] defines Cryptographically Generated Addresses and how to generate a CGA from cryptographic hash of a public key and auxiliary parameters. It also describes how to verify association between public key and CGA, how to sign a message sent from CGA, and how to verify the signature. The protection works without a certification authority or any security infrastructure.

12.3.10.4 DNS in the Home

Home networks are evolving and increasingly signaling the need for DNS in the Home. The increased number of devices in the home communicating with each other, the fact that IPv6 addresses are not easy to remember, and the fact that more devices in the home means more IP addresses to remember, all make the case for having a DNS server inside the home. In the past, devices in the home were limited to home PCs, while nowadays it easily includes PCs, Tablets, Smart Phones, internet-enabled TVs, Media Servers, printers etc. Past applications were limited to Web surfing, email, IM, and Voice, while nowadays it includes Web surfing, email, IM, Voice, Social media, video conferencing, media streaming, home security, and automation, etc. The protocols in use in the past were TCP, UDP, HTTP, IPv4, but now we routinely see TCP, UDP, HTTP, DLNA, UPnP, IPv6, IPv4 etc. Also, the traffic in the past was limited to be between the devices in the home and on the internet, whereas currently it is between the devices inside the home and on the internet.

12.3.10.4.1 Solution - DNS Server inside the Home

12.3.10.4.1.1 Conventional DNS or Unicast DNS

This requires home users to setup a DNS server inside the home; a CPE router could support this functionality. This conventionally configured name-to-address translation is either done manually or using DDNS.

Security Threats here could be Forged DNS data, and the Potential Solution for that would be DNSSEC (Self Signed). Other security threats, such as unauthorized updates to a DNS Server, could be countered by using a secure DNS Dynamic Update or an Administrative username and password.

One of the main assumptions here is that the subscriber is not interested in advertising the home domain outside the home and, hence, does not need it.

12.3.10.4.1.2 Multicast DNS [ID-MCAST-DNA]

Multicast DNS (mDNS) supports Zero Configuration name-to-address translation via address lookup of peers on the local link. It uses the Special-Use (".local.") Domain Names. Each device on the link supports DNS resolver and responder and supports both multicast and unicast queries and responses. It also provides automatic name conflict resolution in the local network.

12.3.10.4.1.3 DNS-Based Service Discovery [ID-DNS-SRV]

The idea here is mainly around service discovery using DNS SRV, TXT RR. It works with both mDNS and conventional DNS. It also supports a Zero Configuration approach with mDNS. The conventional DNS server can be populated manually or by DDNS. It allows for service discovery in "local" or any other domain.

The security threats are similar for mDNS and DNS-based Service Discovery. One potential threat could be a host not cooperating in resolving name conflicts. The main control for this would be to ensure only authorized devices participate in these protocols. Also for other security threats such as forged DNS data for "local" or "global" entries, DNSSEC provides a good mitigating factor.

12.4 IPv6 Transition Technologies

12.4.1 Introduction and Scope

This section of the use case deals with IPv6 transition technologies and discusses vulnerabilities with various transition technologies and how to best address them. It will cover threats using unmanaged IPv6 technologies, such as Teredo and Protocol 41 (e.g., 6to4). It will also cover threats to transition technology devices in headend that implement technologies, such as NAT444, DS-LITE, 6RD, how to protect CGN devices, access controls, and

logging control. For this discussion, the following topics are out of scope: NAT64/DNS64, Proxy, STUN, TURN, and ICE.

The security threats under consideration are the same as the other use case and include: Theft of Service (Authorization), Unauthorized Access (Authorization), Loss of Privacy (Confidentiality), Tampering (Integrity), Spoofing (Authentication), and Denial of Service (Availability).

There are various security issues due to the presence of IPv4 to IPv6 Transition Mechanisms [RFC4942]. IPv6 Transition/Coexistence Mechanism-Specific Issues include traffic avoiding ingress filtering checks, the possibility of attacks to the tunnel interface, and lower security due to the fact that there is no pre-configured association between endpoints. Other security issues due to automatic Tunneling and Relay opens up vulnerabilities, as automatic tunneling allows the de-encapsulation of traffic sourced from anywhere in the Internet within the security boundary. Also, tunneling IPv6 through IPv4 networks may break various IPv4 Network Security Assumptions. For example, there is a need to separate IPv4 and IPv6 firewalls, with tunneled IPv6 traffic arriving encapsulated in IPv4 packets routed through the IPv4 firewall before being decapsulated, and then passing through the IPv6 firewall.

The following table describes the various transition technology types.

Table 6 - IPv6 Transition Technologies

Name	Type	RFC	Brief overview
Dual-Stack	Native	[RFC4213]	Hosts and routers support and operate both IPv4 and IPv6 stacks.
Static Tunnels	Tunnel	[RFC2473]	Manual tunneling of IPv6 in IPv4
Teredo	Tunnel	[RFC4380]	Automatic tunneling of IPv6 into UDP (IPv4), allows connectivity between IPv6 networks over IPv4.
6to4	Tunnel	[RFC3056]	Automatic tunneling of IPv6 into IPv4, allows connectivity between IPv6 networks over IPv4. Uses third-party infrastructure to terminate tunnels.
6RD	Tunnel	[RFC5569]	Automatic tunneling of IPv6 into IPv4 allows connectivity between IPv6 networks over IPv4. Uses operator infrastructure to terminate tunnels.
ISATAP	Tunnel	[RFC4213]	Automatic tunneling of IPv6 into IPv4 allows connectivity between IPv6 networks over IPv4 intranet. Used inside an enterprise.
DS-Lite	Tunnel + Address Sharing	[RFC6333]	Automatic tunneling of IPv4 into IPv6 allows connectivity between IPv4 networks over IPv4 internet.
IPv4/IPv6 Translation	Translation	[RFC6144], [RFC6145]	Allows translation from one protocol to another Stateless/Stateful.
DNS64	Translation	[RFC6147]	DNS64 is a mechanism for synthesizing AAAA records from A records.
DNS46	Translation	[ID-DNS46]	A DNS translator that translates AAAA record to A record
IVI	Translation	[RFC6219]	Allows prefix-specific translations from one protocol to another. Stateless.
NAT444	Address Sharing	Many IETF drafts	Allows continuation of IPv4 services after the IPv4 address exhaustion.

Name	Type	RFC	Brief overview
			Allows operators to assign a single public IPv4 address to multiple subscribers.
A+P	Address Sharing	[RFC6346]	Allows continuation of IPv4 services after the IPv4 address exhaustion. Allows assigning the same IPv4 address to multiple clients, each with its assigned port range.

12.4.2 Tunneling Technologies

12.4.2.1 Security Concerns with IP Tunneling and Recommendations [RFC6169]

12.4.2.1.1 Tunnels May Bypass Security

Tunnels bypass network security domains, One way to control this threat is to disable all Tunnel Traffic and prefer native access for the customer. If the tunnels are bypassing IP Ingress and Egress Filtering, the recommendation would be that the Tunnel servers and Clients should apply ingress and egress controls. To prevent any source routing after the Tunnel Client, Tunnel clients should enforce a policy to discard tunneled IP packets that specify additional routing.

12.4.2.1.2 Challenges in Inspecting and Filtering Content of Tunneled Data Packets

It is very inefficient to perform Selective Network Filtering of All Tunneled Packets. The recommendation for networks with specific security policies would be to disable those tunneling protocols or to filter all tunneled traffic at network boundary (using source/destination port, IP protocol field, etc.). Due to the problems with Deep Packet Inspection of Tunneled Data Packets, tunneling across the (as opposed to tunneling to) security boundary is not recommended.

12.4.2.1.3 Increased Exposure Due to Tunneling

NAT holes increase the attack surface in any network The exposure of a NAT Hole can open up security breaches, and the main recommendation is to minimize tunneling use. Public tunnels widen holes in restricted NATs; therefore, the recommendation here would be that the tunnel client run a host firewall on the tunnel interface.

12.4.2.1.4 Tunnel Address Concerns

Due to known tunneling protocols, it is feasible to guess tunnel addresses, so using tunnel endpoint addresses that are not easily guessable (e.g., using any unused fields in the address). Also an attacker can profile targets based on the tunnel address, so it is recommended to randomize server settings and tunnel client ports.

12.4.2.1.5 Attacks Facilitated by Changing Tunnel Server Setting

A man-in-the-middle attack can be mounted by changing the client's server setting or changing the DNS responses.

The recommendations against such attacks are any anti-phishing and anti-fraud provisions, software that specifically monitors for tunnel server changes, enforcing the client to authenticate either tunnel server or at least the means by which tunnel server's IP address is determined.

12.4.2.1.6 Mechanisms to Secure Use of Tunnels [RFC6169]

[RFC6169] includes recommendations, such as operating on-premise tunnel servers/relays, so the tunneled traffic does not cross border routers. Setting up internal routing to steer traffic to these servers/relays is advisable. Lastly, setting up firewalls [RFC2979] to allow known and controllable tunneling mechanisms and disallow unknown tunnels would help prevent attacks using tunneling technologies.

12.4.2.2 Teredo: Threat Analysis - Attacks and Controls

Teredo encapsulates IPv6 packets within IPv4 UDP packets, and it gives IPv6 connectivity to hosts on IPv4 Internet with no direct native IPv6 connection. Teredo is a last-resort transition technology, and was developed by Microsoft. It allows automatic IPv6 tunneling by encapsulating IPv6 packets within IPv4 UDP packets [RFC4380].

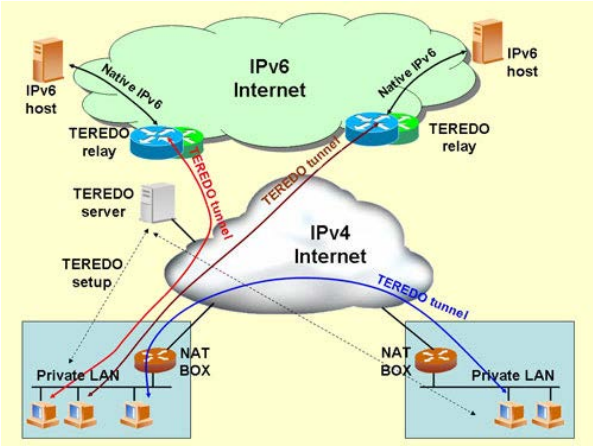

Diagram Source http://www.ipv6tf.org

Figure 93 - Teredo Components

The Teredo client is assigned an IPv6 address with a Teredo prefix (2001:0::/32). The Teredo server is an IPv6/IPv4 node, and it uses UDP port 3544. The server is used by Teredo clients to auto-detect any kind of NAT, and assists in address configuration of Teredo clients. It facilitates initial communication between Teredo clients or between Teredo clients and IPv6-only hosts. A Teredo relay is an IPv6/IPv4 router and can forward packets between Teredo clients on an IPv4 Internet (using a Teredo tunneling interface) and IPv6-only hosts.

12.4.2.2.1 Theft of Service

Theft of service could include exceeding bandwidth caps or the unauthorized use of provider relays/endpoints. The security control methods include ensuring that tunneled traffic is counted; adjust rate-limiting filters or apply proper filters to only allow internal source or destination addresses to use relays/endpoints.

12.4.2.2.2 Unauthorized Access/Spoofing

Unauthorized access/spoofing attacks could include tunneling IPv6 traffic past IPv4-aware firewalls and other controls, multiple layers of encapsulation (i.e., v4-in-v6-in-v4), protocol masking, and other attacks. The security recommendations here are to add or adjust DPI and relays to monitor tunneled traffic for IPv6 attacks. Inserting relays/endpoints to ensure control points will prevent these attacks and filter out all Teredo traffic.

12.4.2.2.3 Denial of Service (DoS)

DoS attacks could include flooding the provider-managed tunnel endpoints. The main control for this would be to adjust the configured filters with appropriate rate limits, installing BOGON and uRPF checks, or installing an IPS.

12.4.2.2.4 Loss of Privacy/Tampering

The attacks here could be in the form of a malicious relay, which sucks in all user traffic when the hacker manages to install Anycast routes within MSO networking infrastructure. The main control against such attacks is to install a tunnel relay on the MSO network and block routes to the injected anycast address.

12.4.2.3 6to4 Threat Analysis: Attacks and Controls

Protocol 41 enables direct encapsulation of IPv6 datagrams within IPv4 packets and is indicated by IP protocol number 41 [RFC2473]. Most tunnels use IPv4 protocol 41 encapsulation, where the data payload is just the IPv6 packet itself (e.g., 6to4, 6RD).

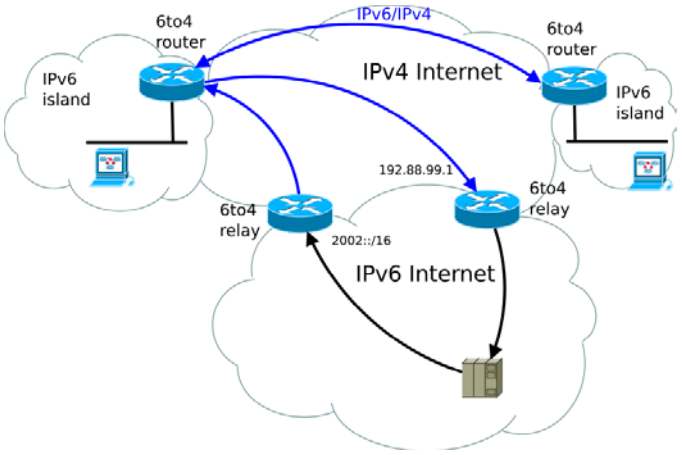

Diagram Source: http://en.wikipedia.org/wiki/File:6to4.svg

Figure 94 - 6to4 Architecture

12.4.2.3.1 DoS Attacks

Neighbor Discovery attacks where the traffic received by the 6to4 relay or router includes link-local IPv6 addresses in the 6to4 tunnel. The control against this attack would be to silently discard these packets.

Spoofing traffic to 6to4 nodes, originates from either native IPv6 or from an IPv4 or 6to4 network. The hacker uses a forged IPv6 address to launch a DoS attack on 6to4 network. Response from 6to4 network triggers a reflection DoS attack. The security controls here are that IPv6 and IPv4 operators implement address filtering before transmitting out of their networks. Also, verifying the source IPv6 address prefix so that it includes the source IPv4 address can prevent this attack. (This requires ISP tunnel relays for this to work).

Local IPv4 broadcast attacks can be launched where the IPv4 address within an IPv6 address is a broadcast or multicast address. A simple control for this would be that 6to4 routers/relays should drop the 6to4 packets with broadcast or multicast IPv4 address.

12.4.2.3.2 Theft of Service

This could include hackers using the 6to4 infrastructure against operators permission. Hackers can force traffic to go to a specific relay using the IPv4 address of the relay (instead of anycast address) or using the routing header to route IPv6 packets to reach specific 6to4 relays. The controls include preventing the use (block/filter) of the actual relay IPv4 address, instead of 192.88.99.1, or filtering out packets with a routing header.

12.4.2.4 6rd Threat Analysis Attacks and Controls

12.4.2.4.1 Denial of Service (Availability)

DoS attacks could prevent communication between the node (e.g., 6RD relay, CPE) under attack and other nodes.

The security controls are firewall and filtering support on the CPE and the Border Relay (BR).

For example, the CPE must drop incoming 6RD frames if the source IPv4 address in the frames is not the same as the configured IPv4 address for BR. The CPE disallows tunneling of IPv6 frames with link-local, site-local, ULA, and any multicast addresses, and the CPE enforces IPv6 Simple security.

The 6RD BR must drop 6RD frames from the customer if a source IPv6 address in the frame is not from an operator-assigned 6RD prefix. The BR must drop any incoming frames with destination IPv6 prefix not used for 6RD. The BR disallows frames with IPv4 private, broadcast, and loopback addresses or frames with inconsistent source-IPv6 delegated prefix and IPv4 address. The BR performs reverse path forwarding checks.

The CMTS could also perform SAV on the IPv4 address.

12.4.2.4.2 Theft of Service

This includes unauthorized use of service (e.g., 6RD relay) by a hacker. The control would be to configure filters at the CM/BR and disallowing 6RD traffic from subscribers not authorized to use 6RD relay services.

12.4.2.4.3 Loss of Privacy/Tampering

A third party may be able to configure a CPE to use a 6RD relay that is not hosted by the operator and snoop/tamper traffic. To prevent this, an operator may want to block 6RD protocol traffic not destined to its own BR relays.

12.4.2.4.4 Spoofing (Authentication)

Unauthorized use of the BR platform to launch an attack on IPv6 sites. The basic controls here are to harden the BR system, and the other security controls from the 6to4 spoofing attack also apply here.

12.4.3 Address Sharing Technologies

12.4.3.1 NAT 444, DS-Lite Threat Analysis Attacks and Controls

Theft of Service could include unauthorized use of public IP addresses by a hacker. This can be easily prevented using SAV at the CMTS.

Denial of Service could include flooding the provider-managed CGN. Such an attack could be based from inside the network using traffic and/or session/port overload techniques, or from outside network using traffic overload techniques. The main controls here are to adjust and configure the appropriate filters like BOGON and uRPF checks. The AFTR/CGN device can limit port usage per customer or enable session limiting or rate limiting techniques.

Unauthorized Access attacks involve gaining access to prohibited protocols and using the shared identity for malicious activity. The security control is to apply proper filters, all current IPv4 filtering and firewalling should apply to CGN Traffic as well, and the CGN (DS-Lite) needs to be inside a firewall.

12.4.3.2 CGNs and Position of LI, IPS, and Firewall

When deploying CGN devices in the network, the media intercept point needs to be determined (current consensus is to keep the point at the CMTS itself).

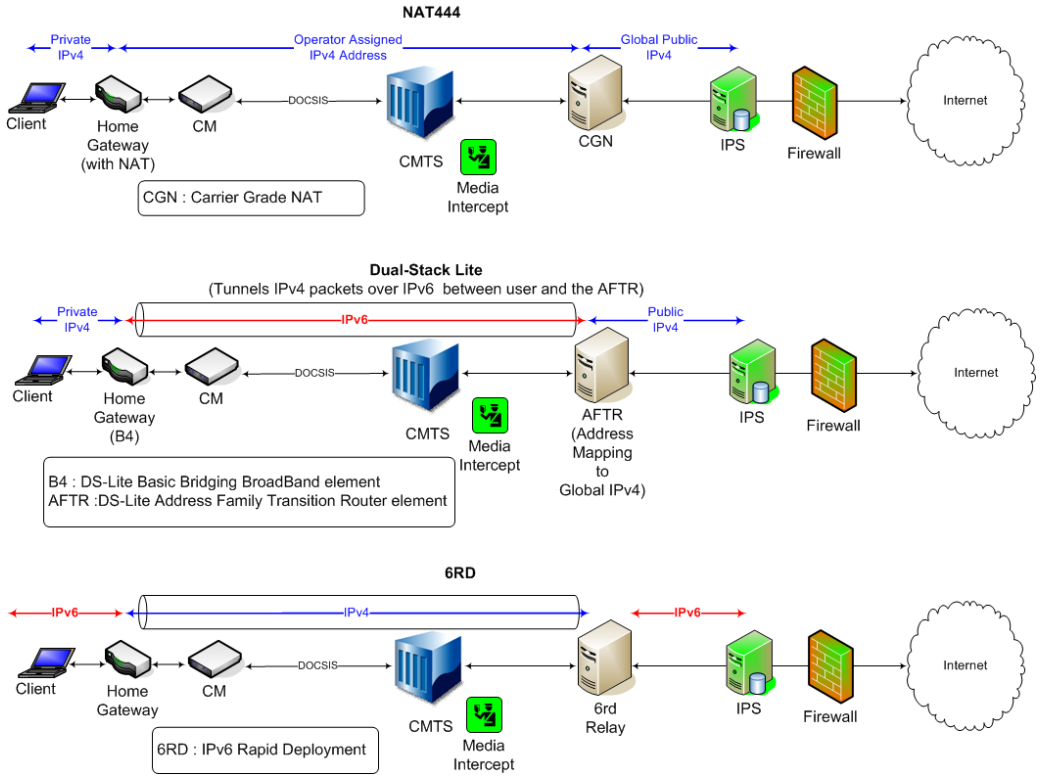

Figure 95 - Media Intercept Position

12.4.3.2.1 IPS/Firewall for user-to-user traffic behind CGNs

The following options are used for eliminating security threats for user-to-user traffic that is behind the same CGN device:

- Rely on host and CPE firewalls.
- Deploy IPS/Firewall appliances close to routers used for user-to-user traffic forwarding:
    - For DS-Lite and 6RD, this router is AFTR and BR respectively,
    - For NAT444, this router is different for different operators.
- Route user-to-user traffic through IPS/Firewall north of CGN.

Any user-to-user (local) traffic protection provided today by the MSO for IPv4 should continue into IPv6.

12.4.3.3 CGN Device Protection

It is important to control access to CGN devices, as these track traffic sessions to some extent and can bring up privacy issues. CGN logs contain sensitive information about subscriber network usage (source and destination addresses). This includes configuration settings to control CGN device behavior.

General device access controls include incorporating security layers (building, room, server), multifactor authentication (authenticate admins multiple ways), separation of duties (requires more than one person to access device), etc.

Access control to the log information can be achieved by encrypting log data and sending syslog events only to authenticated servers over a secure/encrypted link. Techniques, such as Deterministic NAT, can also eliminate most logging in CGN devices.

12.5 Provisioning Server and CMTS Security

This section identifies a couple of issues that were noticed on some IPv6 deployments.

12.5.1 DHCPv6 Issue (Windows Clients)

This issue is when Windows clients overwhelm a DHCPv6 server by implementing behavior that is not compliant with the RFCs.

The windows client, even when denied an IPv6 addresses by the DHCPv6 server, keeps initiating DHCPv6 requests every 400 seconds. When the ADVERTISE is sent and gets back no IA_NA (no addresses available status), the Windows DHCPv6 client will send six exponentially backed-off SOLICITs every 6.5 minutes. This essentially amounts to a significant form of DoS on the DHCPv6 server, especially when multiplied by even a relatively small population of DHCPv6 clients directly connected to a CM (i.e., no home router). Also, if the IPv6 DHCP server is the same device as the IPv4 DHCP server, this issue will affect all DHCP services. The main issue is that devices do not perform any back off when talking with the DHCP server. Between the six SOLICIT messages, the backoff is exponential (0,1,2,4,8,16) and then 6.5 minutes all over again. This is non-RFC-compliant behavior.

There are a few potential approaches to resolving this DHCPv6 Issue. One idea is to make M and O bits relevant in the RFCs; this is the preferred option and in addition would need text to correct [RFC4861]. Another idea is to make DHCP timers relevant when the server says no addresses are available. These recommendations will take some time to appear in practice.

Another solution during IPv6 rollout testing would be to filter DHCPv6 messages upstream for devices that are not expected to get IPv6 addresses. Obviously this is not preferred because this is the equivalent of disabling IPv6.

12.5.2 CMTS ND Table Issue

This was a vendor-specific protocol implementation issue. A CMTS vendor had a limitation of 4k entries in the Neighbor table. When that number is reached, the CPU utilization goes sky high, though this bug was recently fixed.

However MSOs are seeing a similar behavior with IPv4 where the ARP table fills in very rapidly due to scanning attacks from the outside. The method to overcome this issue is to make sure that the CMTS can handle an overflow of ND queries due to either an external attack or a local scanning. This is not an easy problem to solve, as legitimate queries are hard to separate from bad ones. The IETF had discussions on this some time ago, and the basic idea there was to rate-limit the requests when a threshold (% of table) was reached.

12.6 Deep Packet Inspection

12.6.1 DPI Introduction and Background

Traditional firewalls limit access between networks using traffic filters. These can be either stateless or stateful. Stateless filters are where certain packets must not be forwarded regardless of state (multicast source address, non-routable, deprecated, or protocol). Stateful filters allow or deny traffic based on connection state monitoring at Layer 3 and 4 (e.g., TCP and UDP), and do not allow any unsolicited inbound traffic.

Intrusion prevention system/Intrusion detection system (IPS/IDS) are more adaptive security technologies. They monitor network traffic for malicious activity; that is, all traffic passes through unless identified as harmful. The IDS logs and notifies while the IPS also stops and blocks harmful traffic. The IPS/IDS uses the following methods for attack detection. Signature-based detection uses heuristics and patterns that can be attack-based and/or vulnerability-based. Statistical anomaly-based detection baselines the network behavior and then monitors for changes. Stateful Protocol Analysis Detection identifies deviations of protocol states using predetermined profiles.

DPI combines stateful firewall and IPS/IDS functionality; it allows operators to recognize patterns in network traffic. 'Signatures' are defined in advance and distributed to the DPI engines in the network. The DPI looks through Layers 2-7, including packet payload and identifies specific types of application traffic and attacks. DPI information can be used to manage network traffic, and when anomalies are detected, network operators are notified and malicious traffic can be immediately dropped when detected.

12.6.1.1 DPI Uses and Deployment

DPI enhances network security by detecting various protocol attacks, such as DoS/DDoS, port scanning, viruses and worms, and spam and phishing. DPI supports lawful interception. It also helps define traffic management policy and enforcement. DPI can be deployed at the network edge/boundaries or deeper within the network; it can be deployed inline with real time traffic, or the traffic can be mirrored to the DPI engine.

DPI helps identify specific application traffic usage, helps manage network resources, detects and blocks specific security attacks, and supports lawful intercept.

But inline DPI can be a choke point if it does not have sufficient bandwidth/processing capacity or if it malfunctions, and it may raise concerns about subscriber privacy and network neutrality.

12.6.2 DPI and IPv6

Any MSO deploying DPI engines will need to ensure feature parity between IPv4 and IPv6 for all current uses of DPI, such as security, traffic management, CALEA LI, etc.

Tunnels should terminate at security boundaries as monitoring tunneled traffic is difficult and complex, even with DPI, and some vendors have been known to mishandle tunnel traffic (e.g., Protocol 41).

12.7 Security Use Case Summary

Figure 96 gives a high-level overview of all the security techniques and controls available at each device within the MSO network, specifically the home and the access network.

Figure 96 - Summary of Security Controls at each Device

13 ADVANCED HOME NETWORKING USE-CASES

Home networks are becoming more advanced. The introduction of IPv6 and nearly unlimited public address space within the home will only serve to expedite and expand this trend. There are many emerging use cases for the home networks, which are driving this increased complexity and the need for more advanced home network solutions.

The need to separate guest users from home users for privacy and security is one such use case. Another emerging requirement for multiple wireless networks is the drive towards community Wi-Fi options, where the Wi-Fi gateways in subscribers' homes are used to provide Wi-Fi roaming services without interfering with the subscribers' services. Similarly, there is a push for home gateways to provide Femto cells for cellular services and other heterogeneous link-layer technologies (e.g., low-powered sensor networks and Ethernet), all with different requirements. Video content sharing and streaming (including multicast IP video streaming) between the devices inside the home and from the Internet, place additional demands on home networks. Smart grid, home automation and security, telecommuting and corporate IT requirements (e.g., security and network separation), residential multi-homing, and the ever-increasing number of devices in the subscriber's home. including machine-to-machine (M2M) communication (the Internet of Things) all also contribute.

The following sections provide some considerations and solutions for the ever more advanced home networks of the future. Home network architectures are investigated in depth, followed by service discovery, IP video gateways (in-home video distribution), and home routing protocols.

13.1 Home Network Architectures

The basis of every network is its fundamental architecture. What is the expected physical topology? How are addresses distributed and traffic forwarded? In home networks these challenges are all exacerbated by the need for the network to be auto-configuring, with as little user interaction as possible. This section works through the expected home network architectures from simplest to most complex.

13.1.1 Directly Connected Host

The simplest possible architecture is that of a directly connected host. This is the case of a single subscriber device (laptop, tablet, desktop, smartphone, etc.) connected directly to the CM. In this scenario, the device communicates directly with MSO DHCP servers, so SLAAC is not used at all.

There is a potential issue when adding IPv6 in this architecture. In certain cases, the DHCPv6 client in a subscriber device makes continuous retries per RFC 3315, which are excessive in a phased roll-out (IPv6 enabled on DHCPv6 server before all clients are provided IPv6 addresses). Luckily there is a potential solution currently in development within the IETF see [ID-MAX_SOL_RT]. This solution raises the SOL_MAX_RT value from 120 to 3600 seconds by default, and allows a DHCPv6 server to override the client default of SOL_MAX_RT.

13.1.2 "Baseline" Architecture

In this next step up in home network architecture complexity, a single home router is connected to the CM and supports a single home network (single LAN). This architecture is called "baseline" because it is the current de-facto standard. In this case, IPv6 would also be enabled. This means that all IPv4 hosts are on one IPv4 network, and all IPv6 hosts are on one IPv6 network with dual-stack hosts that belong to both. An example is illustrated in Figure 97 below.

One thing to note is that today's subscriber can cascade many CPE routers behind the operator-connected home router to allow additional IPv4 networks. This creates a NAT44*4 environment and is not possible when using IPv6 because NAT is not the default mode of operation. More sophisticated users likely route [RFC1918] space within the home; these users will likely be capable of manually configuring their IPv6 networks as well. It is understood that cascaded a NAT breaks known service discovery protocols.

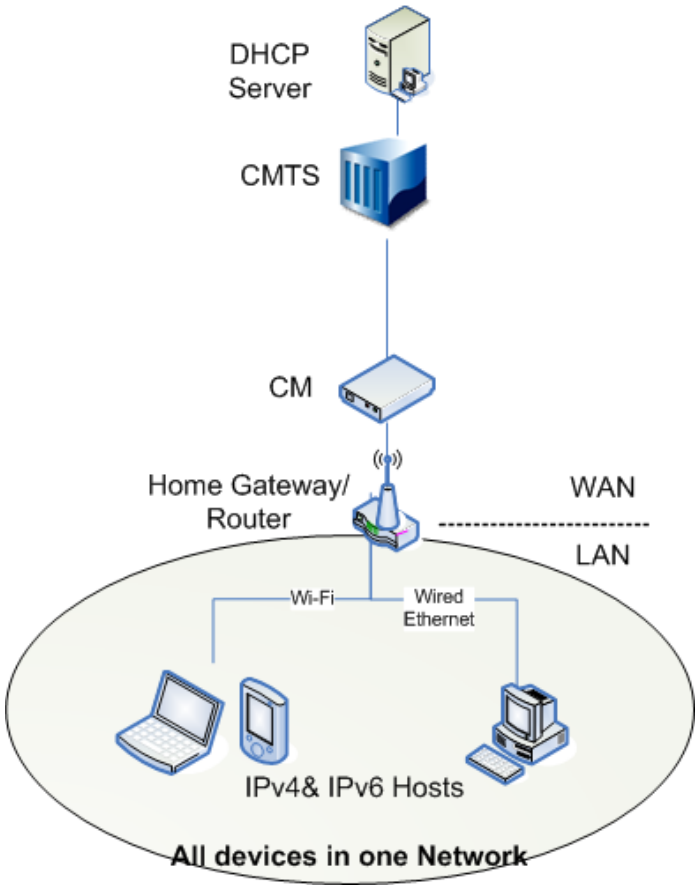

Figure 97 - Example "Baseline" Home Architecture

13.1.2.1 Baseline IPv4 Provisioning

IPv4 is provisioned in the baseline network in two general steps. First, the operator-facing interface (aka WAN interface) on the CPE router obtains a globally routable unicast IP address from the Service Provider using DHCP, which also includes information about the DNS server, default route, host name, etc. Next, the customer-facing interface (aka LAN interface) on the CPE router assigns unicast private IP addresses to the devices on the LAN using DHCP, which also includes DNS server, default route, host name etc.

13.1.2.2 Baseline IPv4 Forwarding

Because there is a single IP LAN, the CPE router performs layer 2 switching to forward traffic between various devices on the LAN. The LAN may include multiple physical interfaces such as Wi-Fi, Ethernet, Zigbee, and others. Devices on the various LANs belong to the same IP network and connect to a single IP interface (dual-stack devices belong to both the IPv4 and IPv6 network, and connect to both the IPv4 and IPv6 interface).

The CPE router does perform IP routing and NAPT to forward the traffic between devices on the LAN and Internet (traffic traveling from LAN to WAN and from WAN to LAN).

13.1.2.3 Adding IPv6 to "Baseline" Network

In order to add IPv6 to a baseline home network, the CPE router MUST support IPv6 on both its LAN and WAN interfaces. Subscriber devices MUST also support IPv6 to use the IPv6 network. Remember that adding IPv6 creates a new logical IP network (dual-stack networks are inherently multi-homed), and that although hosts share a common physical infrastructure, IPv4-only nodes and IPv6-only nodes cannot communicate.

Unlike IPv4, IPv6 traffic is not expected to be NATed. This means that security for IPv6 traffic (e.g., simple security) is required and there may be an increased impact to subscribers when renumbering IPv6.

Routers and hosts on a dual-stack network must be capable of handling multiple addresses (adds GUA IPv6, link-local IPv6, etc., to existing [RFC1918] IPv4).

Baseline IPv6 networks MUST support stateless IPv6 configurations (SLAAC, Stateless DHCPv6), but they may not support stateful configurations.

13.1.2.4 Key Limitations

The key limitations of the baseline architecture are the single layer 2 broadcast domain and the single IP network(s). A single L2 broadcast domain is not optimum for the increasing number of devices in the home. The addition of heterogeneous link-layer technologies (e.g., low-powered sensor networks and Ethernet) with different requirements does not allow L2 security zones or walled gardens. Having only one IPv4 and one IPv6 network means that guests have network connectivity to all connected devices, which increases the potential for unauthorized access to devices in the home. This baseline architecture provides limited support for new and emerging services in the home.

13.1.3 "Single Router" Architecture

Like the baseline architecture, the "single router" architecture includes a single home router and a single WAN interface. Where the two differ is that the single router architecture includes multiple LAN IP interfaces and multiple home networks (LANs). Due to this, the router is required to route traffic between networks (rather than just switch). IPv4 and IPv6 networks are still independent. This architecture is defined in [RFC6204] and [eRouter] and is illustrated below in Figure 98.

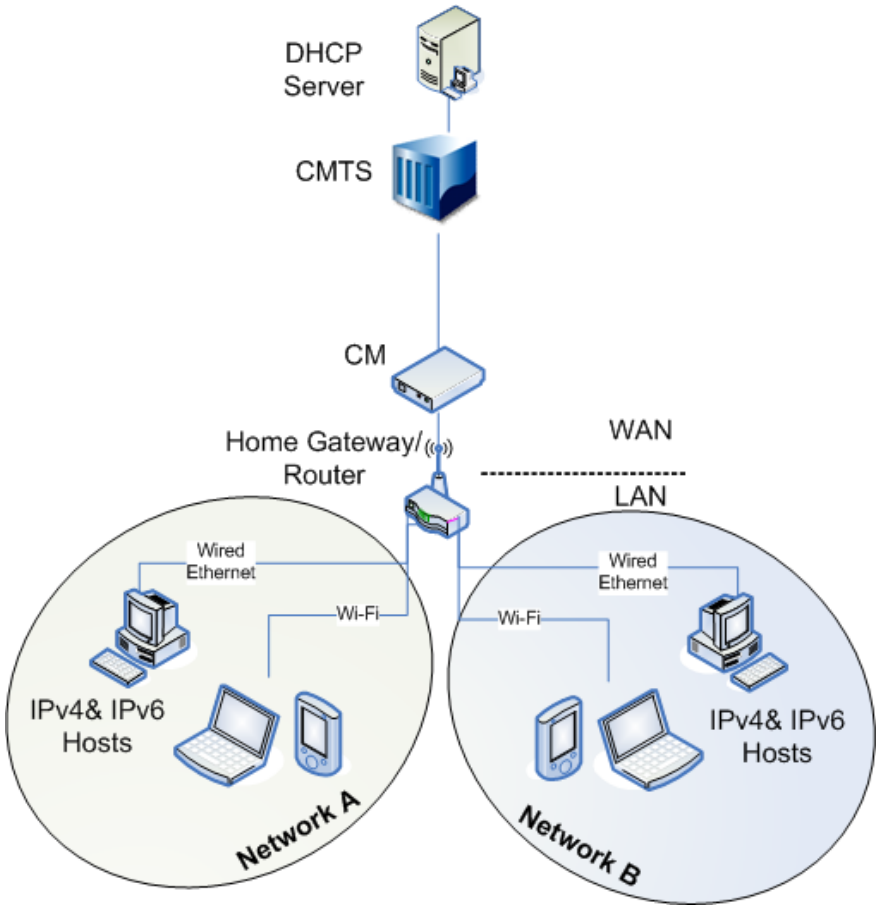

Figure 98 - Example "Single Router" Home Network Architecture

13.1.3.1 IPv4 in the Single Router Architecture

IPv4 works the same as the baseline architecture. By default there is a single IPv4 network with NAPT. Multiple IPv4 networks may be possible but this is not clearly defined in eRouter or [RFC6204]. Cascading routers is still possible without additional configuration, noting that this creates NAT44*4 and breaks IPv4 service discovery.

13.1.3.2 Home Router Provisioning (IPv6)

To provision IPv6 in the Single Home Router network, the home router must first create its link-local addresses for the WAN and all LAN interfaces. This is done using an EUI-64 ID and requires that the home router perform DAD, to ensure that the addresses are unique. Next, the home router performs Router Discovery on its WAN interface, using its WAN link-local address as the source address. Once the home router has discovered its upstream router, it must initiate a DHCPv6 exchange with it to complete provisioning. This includes both DHCPv6 address assignment (the IA_NA) and DHCPv6 prefix delegation (the IA_PD). Both IA_NA and IA_PD are done as a single DHCPv6 session. To ensure that IPv4 and IPv6 requests (and multiple requests over time) from the same home router are recognized as such by the DHCP server(s), the home router uses a persistent DHCP unique identifier (DUID). As defined in [eRouter] and [RFC6204], the home router includes the DNS recursive name server option and the reconfigure accept option. When the home router receives its WAN address in the IA_NA, it performs DAD and joins the all-node and solicited-node multicast addresses. For the IA-PD, the home router requests a prefix large enough to provide one /64 for each LAN interface, rounded up to the nearest nibble (4 bits). Once it assigns a /64 to each LAN interface (and installs routes for them), it installs a null route for the aggregate, nibble-aligned prefix to avoid forwarding unnecessary traffic. If the prefix provided by the DHCPv6 server is too small to assign a /64 to each of its LAN interfaces, a single /64 is assigned for all LAN interfaces. As noted previously, a phased IPv6 deployment may require DHCPv6 tweaks similar to what is proposed in [ID-MAX_SOL_RT].

13.1.3.3 Key Limitations

There are several key limitations of the Single Router home-network architecture. First, service discovery becomes an issue whenever multiple networks are introduced into the home network. A major reason for this complication is that in-home multicast are not defined in [eRouter] or in [RFC6204]. Downstream multicast is required by [eRouter], and MLD is listed as optional in [RFC6204] however. Another general limitation is that adding IPv6 to any network emphasizes the need for local name service. IPv4 support is also a limitation since IPv4 is not covered at all in [RFC6204] and multi-network IPv4 is not defined in [eRouter]. Finally, and perhaps most poignantly, adding additional, cascading IPv6 routers requires IPv6 prefix sub-delegation (no NAT), and there is currently no mechanism defined to achieve this.

13.1.4 Multi-Router Architectures

Devices in the home are evolving in scale and diversity and this is driving subscribers to add routers within the home network. Multiple home IPv6 routers require sub-delegation unlike advanced home networks in IPv4, which use cascaded NAT or manual setup. There is no NAT in IPv6, and we need to avoid manual configuration for most users. This drives the need for a working zero-configuration multi-router home network architecture.

As CableLabs investigated such an architecture and the mechanisms to enable it, several basic assumptions were made:

- Each home network has a single ISP connection and no IPv6 NAT/NAPT.
- Each home router requires at least one /64 (one per LAN interface).
- Routers are plugged in "right side up" (WAN interface connected to LAN interface of upstream router).
- Routers do not act as clients on LAN interfaces.
- Hosts can accept multiple addresses ("Internal multi-homing").

The following constraints or requirements were also assumed:

- The CPE Edge Router (CER) sends an aggregated prefix request to ISP. This means that the ISP does not see individual /64 prefixes allocated within home. The delegated prefix is then divided into multiple subnets by the CER.

- Prefix delegation (and sub-delegation) should be automatic.
- Addition of a new Internal Router (IR) should not affect the existing topology.
- The selected assignment mechanism should be reasonably efficient.
- Home network architecture should be self-configuring, that is they should minimize or eliminate manual configuration.

13.1.4.1 Multi-Router Addressing Schemes

The expected physical topology and preferred addressing scheme (logical topology) need to be understood in order to select the best architecture and associated sub-delegation/routing mechanism(s).

This section examines the expected physical topology and describes several possible addressing schemes. The next section (13.1.4.2) digs into requirements and suitable mechanisms to enable the selected addressing scheme(s).

Based on these assumptions, the general physical topology will be an inverted tree with a single root (the CER). An example of this is illustrated in Figure 99.

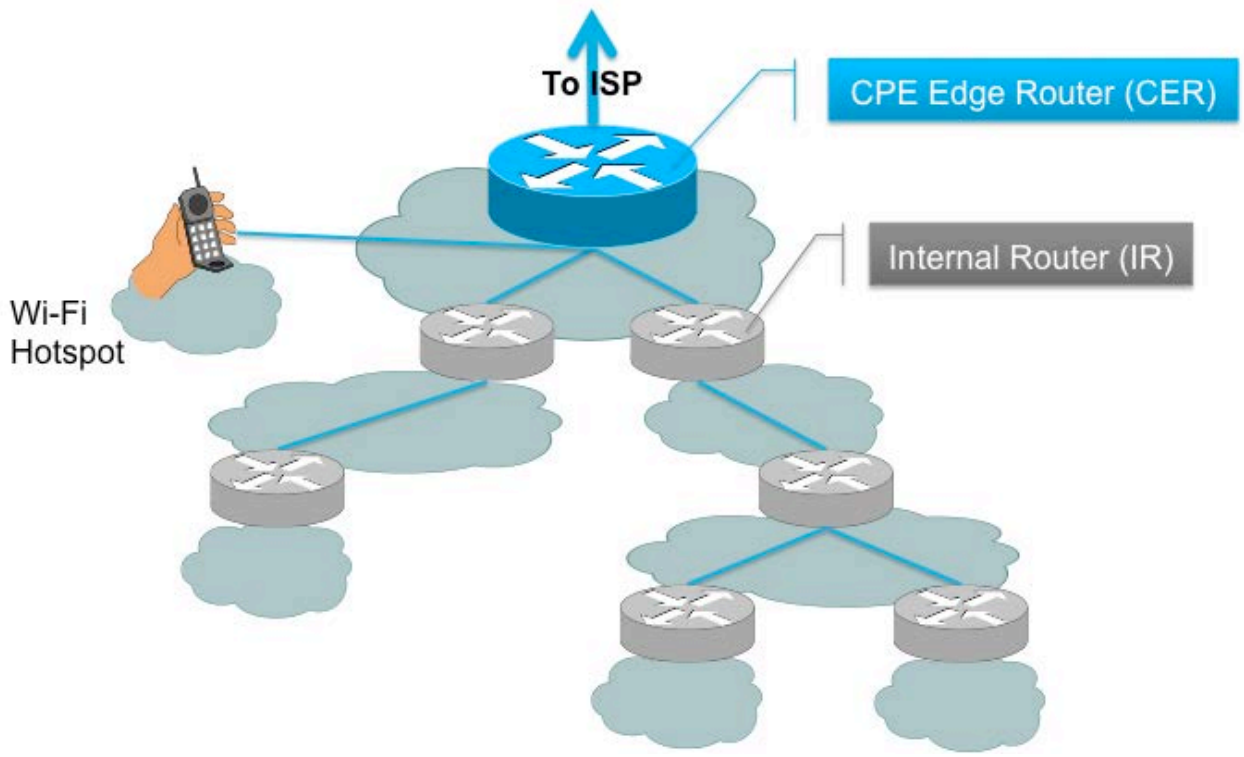

Figure 99 - Example Expected Physical Home Network Topology

Within this expected physical topology, there are several possible addressing schemes. They fall into two general categories: hierarchical and non-hierarchical.

Hierarchical addressing schemes ensure that the prefix any given router receives is a subnet of upstream router's prefix. This forces aggregation at every level within the hierarchy. One variant of this is the "uniform hierarchy" in which routers receive the same prefix size across a given level (e.g., all routers 2 hops from the CER get a /58). An example uniform hierarchy is shown in Figure 100.

In non-hierarchical networks, aggregation is not as much of a concern since any given prefix may or may not come from the upstream router's prefix. This methodology is more efficient however; routers get only the prefix size they need, regardless of position (e.g., any router with two IP interfaces gets a /63).

From these two general categories, CableLabs developed six individual addressing schemes: Uniform Static Hierarchical, Uniform Dynamic Hierarchical, Non-Uniform Dynamic Hierarchical, Dynamic Non-Hierarchical, Flat, and Overlay. The pros and cons of each of these were investigated and are documented in Figure 101. For more detail on each of the schemes examined, see the use case slides.

After weighing these six addressing schemes, the Uniform Dynamic Hierarchy and Flat schemes were eliminated. The team worked to develop addressing mechanisms for the remaining four.

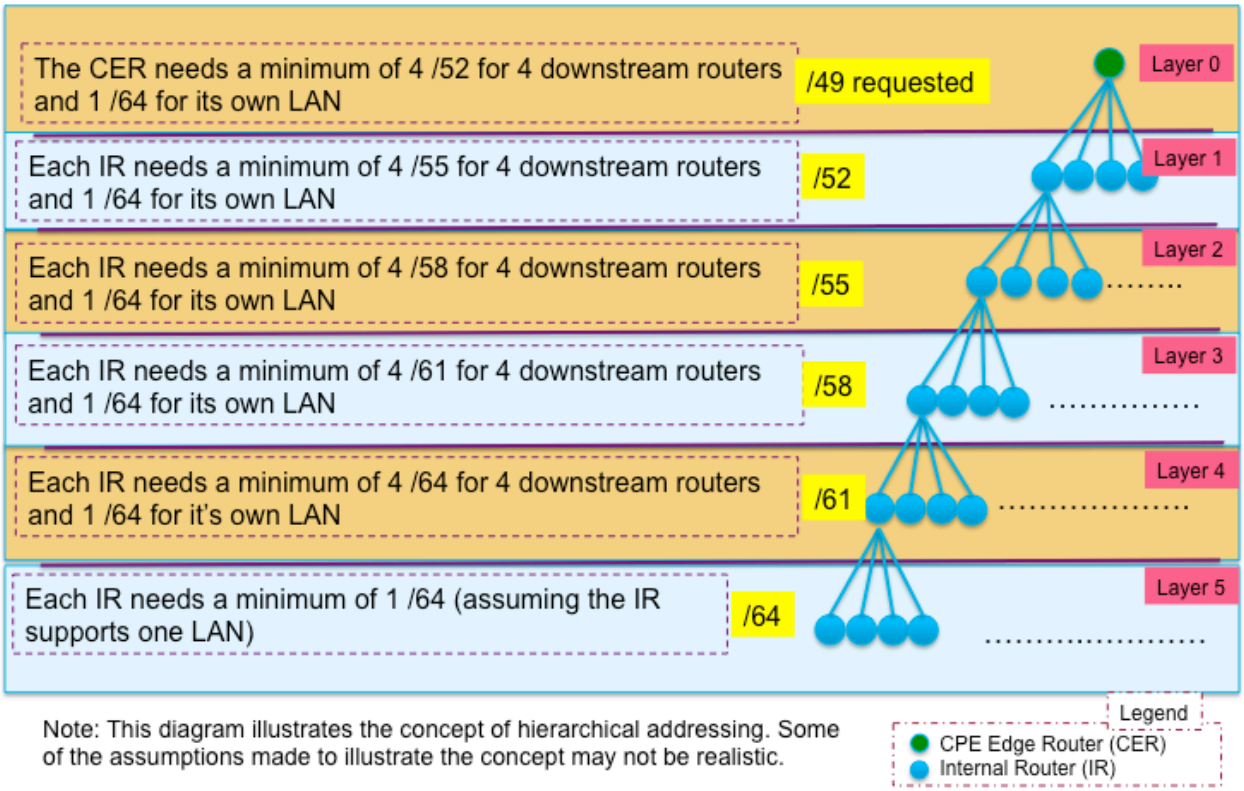

Figure 100 - Example (4x5) Uniform Hierarchical Addressing

Scheme	Pluses	Limitations
Uniform Static Hierarchy	Hierarchical, Intuitive, Simple Algorithm	Most Waste, Least Flexible, Set Prefix, Manual Configuration
Uniform Dynamic Hierarchy	Hierarchical, Dynamic, Intuitive, Simple Algorithm	Waste, Inflexible, Renumbering, Prefix Requests, Race Condition
Non-Uniform Dynamic Hierarchy	Hierarchical, Flexible, Efficient	Waste, Renumbering, Prefix Requests, Race Condition
Dynamic No Hierarchy	Efficient, Flexible, Conceptually Simple	Complex Routing, Renumbering, Prefix Requests
Flat	Hidden Topology, Most Efficient, Most Flexible, Operationally Simple	No Layer 3 Separation (Overlay solves this)

Figure 101 - High-Level Home Network Addressing Schemes

13.1.4.2 Multi-Router Addressing Mechanisms

This section explores requirements and suitable mechanisms to enable the selected addressing schemes. Figure 102 shows the 9 mechanisms evaluated by CableLabs and the addressing schemes they enable.

Static Uniform Hierarchical	Dynamic Non-Uniform Hierarchical	Dynamic Non-Hierarchical	Overlay
Default Configuration	Router Capabilities Protocol (new)	Unicast DHCPv6	Tunneling
Hop by Hop DHCPv6	ULA First	Routing Protocol	NAT66
		DHCPv6 Relay	

Figure 102 - Addressing Mechanisms

Figure 103 provides a detailed analysis of the nine addressing mechanisms. In this diagram, scheme indicates the addressing scheme applied, and the option column contains the addressing mechanism being evaluated. TtD stands for Time to Develop and is a rough estimate of the amount of time needed to see the mechanism in consumer products; it includes both standards work and implementation time. Hardware impact is an estimate of the memory and processing demands. CER ID is short for CPE and is either required (needed in addition to the addressing mechanism), or included (present in the mechanism). Prefix size is a measure of efficiency; some schemes/mechanisms require much larger prefixes than others for the same network. The Prefix Response column indicates the requirement on MSOs to respond to IA_PD hints, i.e., to provide requested prefix sizes. The possible values for Prefix Response are Strict (a specific prefix size is required), Loose (it's best to respond to the hint), and Any (any MSO prefix of adequate size is acceptable). Flexibility estimates the ability for the home network

topology to be unique and tolerant to change. The final column ranks IPv4 friendliness; whether the mechanism provides a solution for IPv4 (other than NAT stacking) in addition to IPv6.

Scheme	Option	TtD	Hardware Impact	CER ID	Prefix Size	Prefix Response	Flexibility	IPv4
Static Uniform Hierarchy	~~Default~~	2-4yr	Low	Incl.	Large	Strict	Low	v4 PD
	Hop by Hop	0-2yr	Low	N/A	Large	Any	Low	v4 PD
Dynamic Non-Uni Hierarchy	~~RC~~	3-5yr	High	Incl.	Medium	Loose	Medium	v4 PD
	~~ULA First~~	0-2yr	Medium	Req.	Medium	Loose	Medium	v4 PD
Dynamic Non-Hierarchy	~~Unicast DHCPv6~~	2-4yr	High	Req.	Medium	Loose	High	v4 PD
	~~Routing Protocol~~	2-4yr	High	Incl.	Medium	Any	High	v4 PD
	DHCPv6 Relay	0-2yr	Medium	Req.	Medium	Loose	High	v4 PD
Overlay	Tunneling	2-4yr	Low (+tunnel)	Req.	Small	Any	High	Works
	NAT66	0-2yr	Low	Req.	Small	Any	High	v4 PD

Figure 103 - Detailed Home Network Addressing Mechanism Analysis

Following this detailed analysis, four options remained to be examined further:

- GUA PD (global unicast address prefix delegation) or hierarchical DHCPv6 PD,
- ULA PD + NPT (unique local address prefix delegation plus network prefix translation) or hierarchical DHCPv6 PD + NPT,
- ULA PD + Tunnels or hierarchical DHCPv6 PD + Tunnels, and
- GUA Relay or DHCPv6 Relay.

The following sections describe each of these mechanisms.

13.1.4.2.1 GUA PD (Hierarchical DHCPv6 PD)

Figure 104 provides an illustration of the GUA PD addressing mechanism; the provisioning steps and failure cases are detailed below.

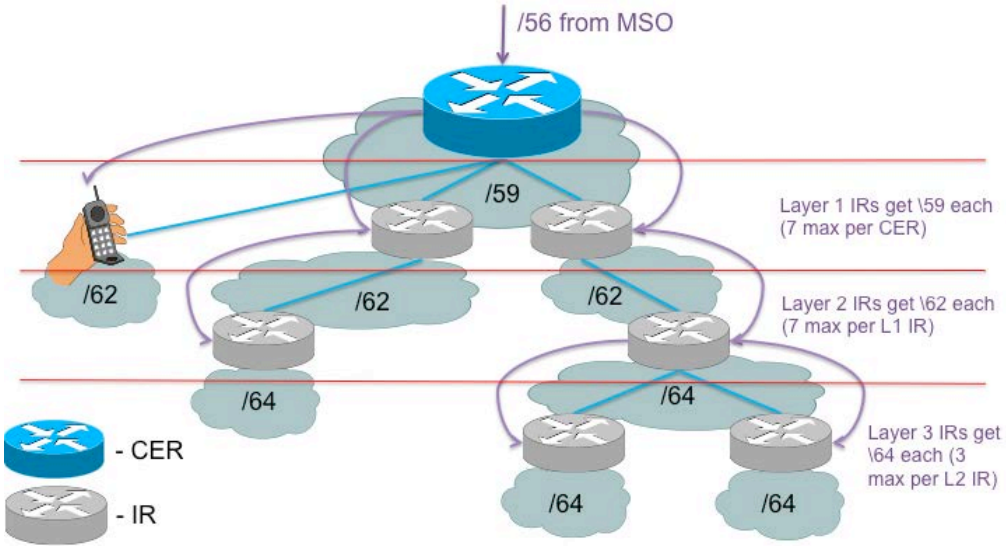

Figure 104 - Hierarchical DHCPv6 PD

Provisioning starts when the CER receives an RA with the M and O bits set to 1. The CER then initiates DHCPv6 with the MSO DHCPv6 server. The CERs request contains IA_NA, IA_PD, and CER_ID options. The IA_PD option includes a prefix size hint for the largest prefix it can handle (e.g., /48). The MSO DHCPv6 server responds with a WAN IPv6 Address (IA_NA), a home IPv6 Prefix (IA_PD), e.g., /56, and a blank or :: CER_ID option [ID-CER-ID].

Once the DHCPv6 exchange with the MSO server is complete, the CER advertises its RA with the M and O bits set to 1 into all LAN segments. Level 1 IRs then initiate DHCPv6 with CER. The L1IRs send the IA_PD and CER_ID options. The IA_PD again includes a hint for the largest prefix the requesting router can handle. The CER responds with the IRs IPv6 Prefix (e.g., /59) and a CER_ID option containing the CER's LAN IP.

At this point, the L1IRs advertise their RA with the M and O bits set to 1, and the Level 2 IRs and all IRs in subsequent levels follow the same procedure as above. Prefix delegation ends when there are no more DHCP (IA_PD) requests or a router runs out of prefixes to delegate

Finally, all home routers (CER and IR) install a default route based on the RAs they received. All home routers (both CER and IR) record which client each delegated prefix is handed out on (this prefix/address tuple is used to construct routing table). All IRs then turn off their internal firewall, as all firewall responsibilities are at the edge of the home network on the CER.

There are several possible failure cases. Running out of prefixes to delegate at any level is one such case. Turning the offending router, and all downstream routers, into bridge(s) could solve this. Another possible failure occurs when an IR does not support the CER identification option. In this case, routers below the offending router think they are the CER and maintain firewalling. Manually (or automatic option) disabling the firewall on such downstream IRs would solve this issue. A router that does not support forwarding packets when the ingress and egress interfaces are the same would also cause a failure, but this is expected to be rare. Lastly, sub-optimal routing could be experienced in a home network where ICMP redirects are not supported by CER/IRs.

It should be noted that [ID-Prefix-Alloc] outlines an addressing mechanism that is basically inline with the CableLabs-defined GUA PD mechanism detailed here. Adding a pointer to [ID-CER-ID] to enable the disabling of IR firewalls would make the comparison more complete.

13.1.4.2.2 ULA PD + NPT (Hierarchical DHCPv6 + NPT)

Figure 105 illustrates the basic elements of a ULA PD + NPT home network addressing mechanism. This method combines [RFC6296] network prefix translation with a hierarchical DHCPv6 distribution of ULA.

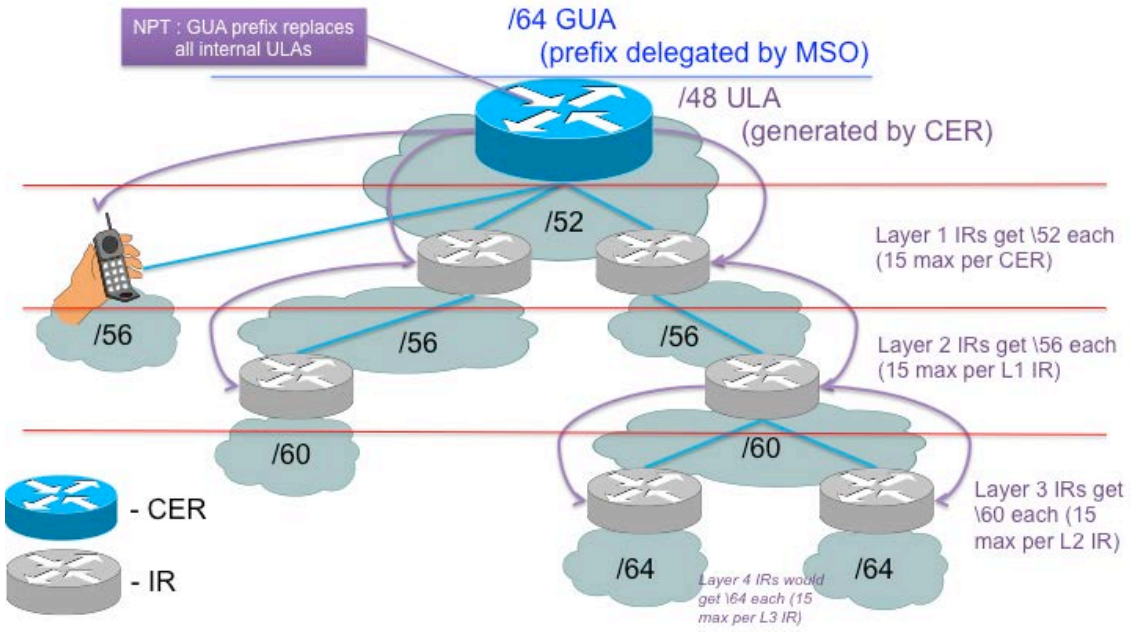

Figure 105 - Hierarchical DHCPv6 PD + NPT

To provision a ULA PD + NPT home network, the CER first receives GUA from the MSO DHCP server. This is initiated when the CER Receives an RA from the MSO network with the M and O bits set to 1. The CER then initiates DHCPv6 with the MSO DHCPv6 server. The CERs request contains IA_NA and IA_PD options. The IA_PD option includes a prefix size hint for the largest prefix it can handle (e.g., /48). The MSO DHCPv6 server responds with a WAN IPv6 Address (IA_NA) and a home IPv6 Prefix (IA_PD), e.g., /64.

At this point, the CER identifies itself based on the fact that it received a GUA prefix (in the RA and via DHCP), which means it is directly connected to the MSO network and thus is the edge router. This prompts the CER to create a pseudo-random ULA /48 prefix [RFC4193] and start ULA provisioning. The CER now advertises its RA (including the ULA Prefix) with the M bit set to 0 and the O bit set to 1. The M bit set to 0 signals to all Level 1 IRs that they should provision their WAN interface using SLAAC and the provided ULA prefix.

L1IRs then perform DHCPv6 with CER, including just the IA_PD option (with hint). The CER responds with the IR ULA Prefix (IA_PD), e.g., /52. L1IRs now advertise their own RA with the M bit set to 0 and the O bit set to 1. L2IRs and any subsequent levels then follow same procedure as above for L1 IRs. Prefix delegation ends when there are no more DHCP (IA_PD) requests or a router runs out of prefixes to delegate.

The final step of provisioning is routing tables. First, all home routers (CER and IR) install a default route based on the RAs received. All home routers (CER and IR) also record which client each delegated prefix is handed out to (this prefix/address tuple is used to construct the router's routing table). Finally, all IRs then turn off their internal firewall as all firewall responsibilities are at the edge of the home network on the CER.

CableLabs has identified several failure cases related to ULA PD + NPT. Perhaps most problematic, stateless NPT [RFC6296] doesn't support the specific use case described here. NPT requires that the inside and outside prefixes must be the same length. If the prefix lengths differ, the longer (smaller) of the two will limit the ability to use subnets in the shorter (larger). For example, if the MSO provides a /64 GUA prefix to the CER, only one /64 of ULA will be able to be utilized within the home network. A stateful NPT or NAT could solve this, but requires a new RFC.

Beyond that, NAT traversal in general is still an issue with NPT. Potential solutions include all of the current NAT traversal methods, such as STUN, TURN, ICE, ALGs, etc. And, of course, all of the failure cases from previous use cases also apply: running out of prefixes to delegate at any level, routers not supporting the forwarding of packets when the ingress and egress interfaces are the same, ICMP redirects not supported, etc.

13.1.4.2.3 ULA PD + Tunnels (Hierarchical DHCPv6 PD + Tunnels / AKA: Overlay)

This section describes the CableLabs-invented overlay network (ULA PD + Tunnels). Figure 106 provides a basic illustration of this mechanism. Provisioning steps and failure cases are detailed below.

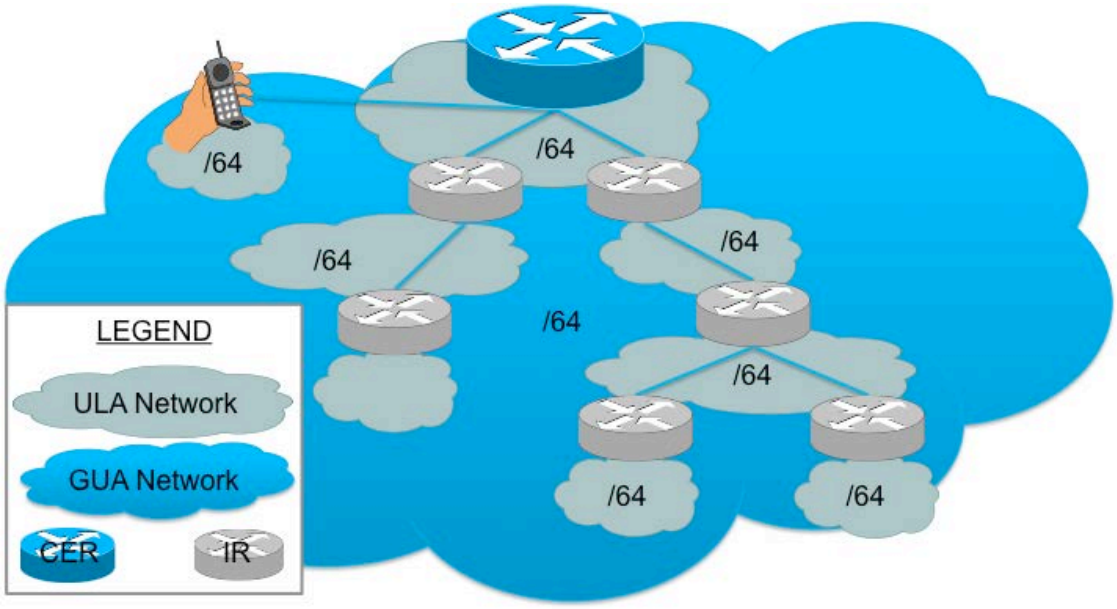

Figure 106 - Hierarchical DHCPv6 PD + Tunnels (Overlay)

Provisioning again starts when the CER receives an RA with the M and O bits set to 1. The CER then initiates DHCPv6 with the MSO DHCPv6 server. The CERs request contains IA_NA, IA_PD, and CER_ID options. The IA_PD option includes a prefix size hint for the largest prefix it can handle (e.g., /48). The MSO DHCPv6 server responds with a WAN IPv6 Address (IA_NA), a home IPv6 Prefix (IA_PD), e.g., /64, and a blank or :: CER_ID option [ID-CER-ID].

The CER then creates a pseudo-random ULA /48 prefix [RFC4193] and starts ULA provisioning. The CER advertises its RA (including the ULA Prefix) with the M bit set to 0, the O bit set to 1, and the A bit set to 1. This signals attached routers to initiate DHCPv6 PD and SLAAC. The Level 1 IRs provision their WAN interface using SLAAC and the provided ULA prefix.

L1IRs then perform DHCPv6 with CER, including the IA_PD (with hint) and CER_ID options. The CER responds with the IR ULA Prefix (IA_PD), e.g., /52, and the CER's GUA LAN IP (CER_ID). L1IRs now advertise their own RA with M=0, O=1, and A=1. L2IRs and any subsequent levels then follow the same procedure as above for L1 IRs. Prefix delegation ends when there are no more DHCP (IA_PD) requests or a router runs out of prefixes to delegate.

Next, all IRs establish IP tunnels to the CER using generic packet tunneling in IPv6 [RFC2473]. These tunnels are built from the IRs ULA WAN IP to the CER's GUA IP (obtained in the CER_ID). The CER then establishes IP tunnels back to each IR (the CER sees each IRs ULA address as the source of the incoming tunnels); this creates bi-directional virtual links.

Once these tunnels are established, the IRs advertise a new RA (M=1) with two PIOs. The first PIO is for the ULA prefix and indicates that hosts should perform SLAAC, and that the prefix is on-link (A=1, L=1). PIO number two is for the GUA prefix, it instructs hosts to perform DHCPv6 and informs them that the prefix is not on-link (A=0, L=0). The /64 GUA prefix advertised in the second PIO is derived from the CER_ID. IRs relay all IA_NA requests up their tunnel to the CER. In this way, hosts receive GUA via IA_NA from the CER over a tunnel. In order to provision downstream routers with ULA prefixes, IRs relay IA_NA and directly answer IA_PD requests.

The resulting logical "overlay" GUA network is illustrated in Figure 107.

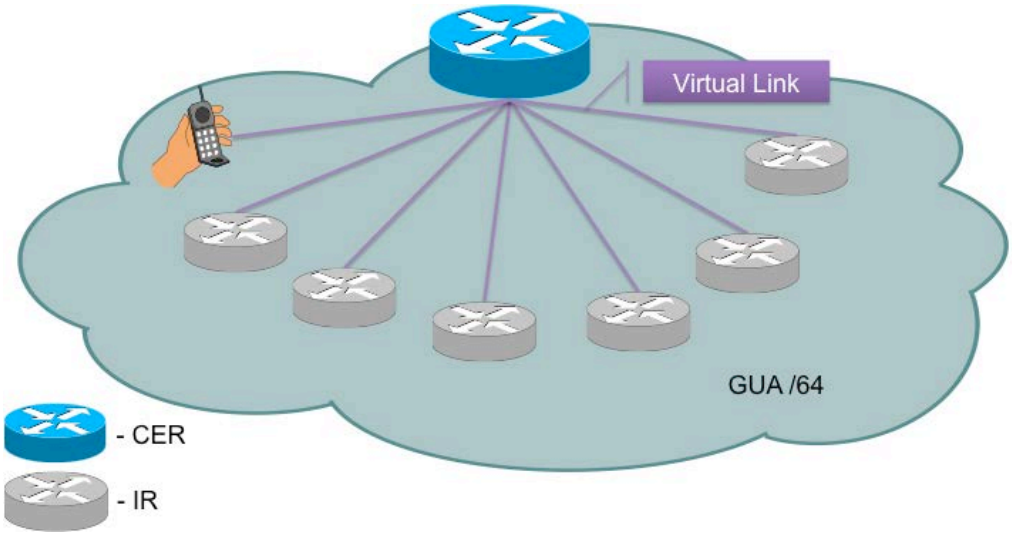

Figure 107 - Logical GUA Topology for Overlay Network

Routing is provisioned based on RA and DHCP information. The CER starts by installing a default route based on the received MSO RA. Then IRs install a default ULA router based on the RAs they've received. Next "Up" routes for ULA FC00::/7 and the CER_ID are installed by the IRs. All home routers (CER and IR) record which client (IR) each delegated ULA prefix is handed out to. and this prefix/address tuple is used to construct their ULA routing tables. The IRs also install a ::/0 default route on their virtual link to the CER and the CER records which relay (IR) each GUA IA_NA is handed out to (as with the IRs and ULA, this GUA address/tunnel tuple is used to construct the CERs GUA routing table). Example IR and CER routing tables are illustrated in Figure 108 and Figure 109, respectively.

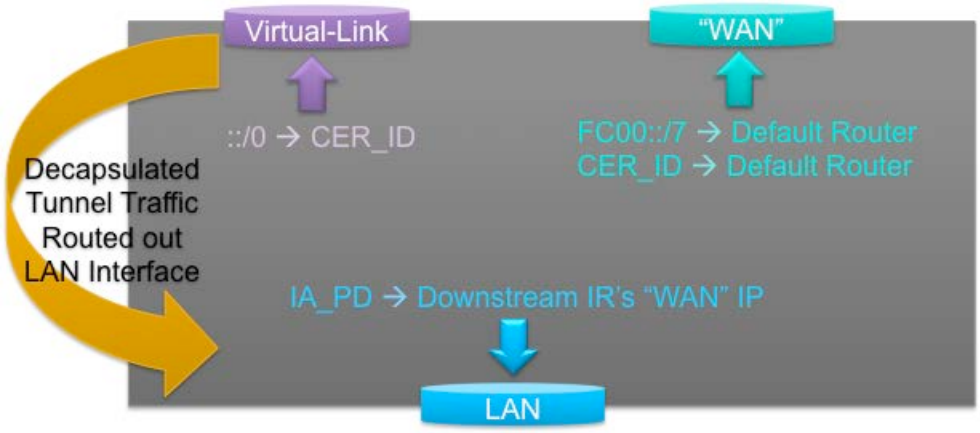

Figure 108 - IR Routing Table for Overlay Network

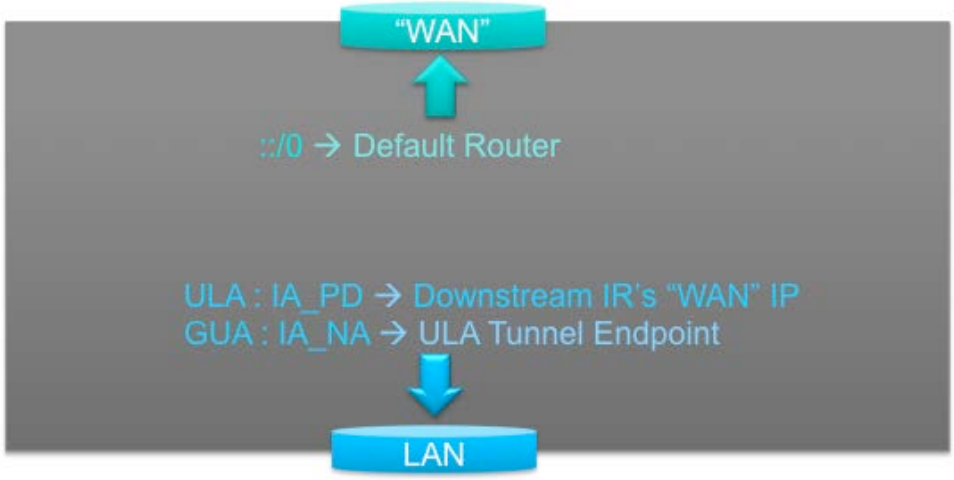

Figure 109 - CER Routing Table for Overlay Network

In all network architectures there are conditions that may cause a failure; CableLabs has identified several failure conditions for this "overlay" network. Most obvious is a home router that doesn't support tunneling that is being introduced to the home network. This would result in no GUA connectivity for directly attached hosts, with no known workarounds. There is also a concern that setting the M bit to 1 in the dual-PIO (ULA and GUA) RA may cause hosts to not do SLAAC (despite the A bit in the PIO being set to 1). Hosts need to be tested to determine the scope of this potential issue. Since the CER must provide GUA to each and every host in the home, there is a possibility that it could exhaust DHCP "slots." CER DHCP implementations will need to keep this in mind when determining DHCP memory allocations. Another potential issue specific to this addressing mechanism could occur in the event that the CER fails. A sudden restart of the CER could mean that all DHCP state (and thus routing information) would be lost. Storing bindings in non-volatile memory to preserve this state across resets could solve this. Using short lease times on GUA could also limit the impact of such a failure, since hosts would send DHCP messages to the CER frequently. Previous failure cases appear again here as well. Running out of prefixes to delegate and having an IR that doesn't support the CER identification option are both potential issues with existing workarounds.

13.1.4.2.4 GUA Relay (DHCPv6 Relay)

The final addressing mechanism investigated in detail is GUA Relay, which relies on the DHCPv6 Relay Agent functionality defined in [RFC3315]. Here again, Figure 110 provides a visual example, and this section provides the detailed provisioning process as well as an analysis of potential failure cases.

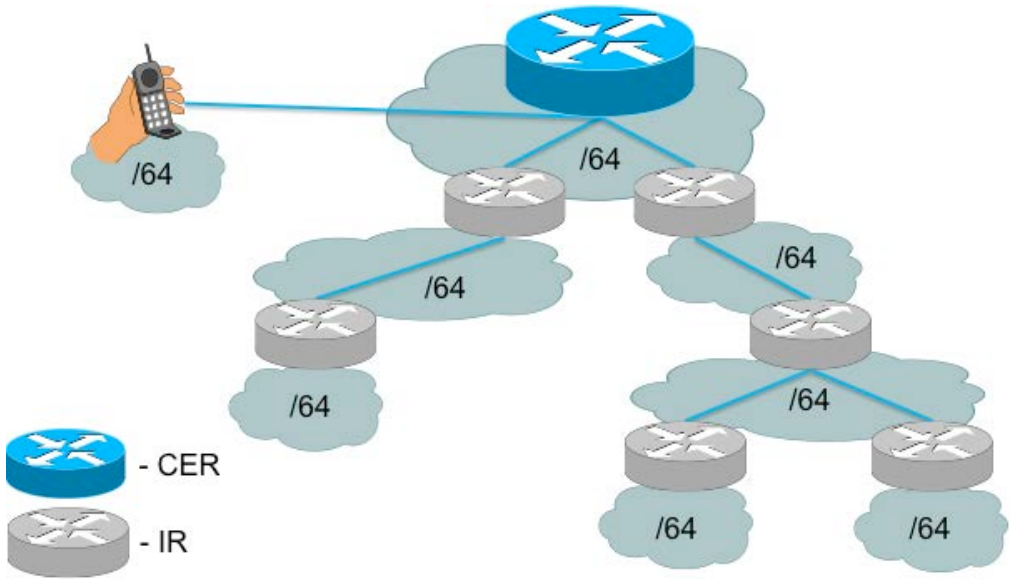

Figure 110 - DHCPv6 Relay

Provisioning starts familiarly; the CER receives an RA with the M and O bits set to 1 prompting it to initiate DHCPv6 with the MSO DHCPv6 server. The CERs request contains the IA_NA, IA_PD, and CER_ID options. The IA_PD option includes a prefix size hint for the largest prefix it can handle (e.g., /48). The MSO DHCPv6 server responds with a WAN IPv6 Address (IA_NA), a home IPv6 Prefix (IA_PD), e.g., /56, and a blank or :: CER_ID option [ID-CER-ID].

Once the DHCPv6 exchange with the MSO server is complete, the CER advertises its RA with the M and O bits set to 1 into all LAN segments. Level 1 IRs then initiate DHCPv6 with CER. The L1IRs send the IA_PD and CER_ID options. The IA_PD again includes a hint telling the CER how many /64s it requires (how many LAN interfaces). The CER responds with the IRs IPv6 Prefix (e.g., /64) and a CER_ID option containing the CER's LAN IP.

At this point the L1IRs advertise their own RA with M and O bits set to 1 and the Level 2 IRs initiate DHCPv6. L2IRs send the IA_PD (with hint) and CER_ID options. They may use SLAAC or may send IA_NA as well, this choice does not affect the mechanism. L1IRs respond with the CER's LAN IP using the CER_ID option and also relay the IA_PD request out their WAN/upstream interface. This allows the CER to respond to the IA_PD request with the L2IRs IPv6 Prefix (e.g., /64). This response is relayed by L1IRs to the client or relay that the corresponding request was received from.

Now L2IRs advertise their RAs with the M and O bits set to 1 and the Level 3 IRs and any subsequent levels follow the same procedure. Prefix delegation ends when all IRs have received a prefix.

Routing tables are provisioned fairly simply in this mechanism. First, all home routers (CER and IR) install a default route based on the RA(s) they receive. Then prefix-address tuples are used to construct routing tables. The CER determines tuples by recording which relay each delegated prefix is handed to. IRs create tuples by inspecting the contents of all relayed IA_PD responses and recording both the prefix contained and which client/relay the message is relayed to.

Failure could occur if the CER runs out of prefixes to delegate. To solve this, the CER could simply request a larger prefix. Another option is to turn additional routers into bridges. If an IR doesn't support the CER identification option, downstream routers may think that they are the CER. Adding prefix size to the CER identification process may solve this. Finally, if an IR reboots it loses its routing table. This is particularly problematic because the table is built on snooped DHCP information. Storing the routing table in nonvolatile memory, which persists across resets, could eliminate this problem. Also, home routers could be configured to send lease queries on boot and IRs to respond to lease queries from upstream routers with snooped relay information.

13.1.4.3 Multi-Router Architecture Summary:

GUA PD is a straightforward solution, which is already in progress within the IETF [ID-Prefix-Alloc].

Advancement of ULA PD + NPT would require a new stateful NPT RFC since the existing RFC ([RFC6296]) does not satisfy the use case. This is likely a long (and hard fought) process, which may even require a reference implementation before it can go anywhere.

ULA PD + Tunneling is a viable approach that supports the smallest prefix requirement. Standardization would require a new IETF Homenet Internet draft.

DHCPv6 Relay is another viable option that supports an intermediate prefix size. It has been submitted to the IETF as [ID-Home-Relay].

13.1.5 Other Home-Network Architecture Considerations

CableLabs and members identified two additional areas of concern with regard to home network architectures above addressing schemes and mechanisms. This section takes a deeper look into both CER identification and the use of ULA.

13.1.5.1 CER Identification

As noted in Section 13.1.4, many addressing mechanisms require identification of the CER. CableLabs identified several high-level approaches to CER identification: Static, IGP or other peer-to-peer topology discovery mechanism, top-down messages, and automatic determination based on prefix and/or route information.

Static CER identification accurately identifies the CER at network installation time, is lightweight, and does not require new router development. The downside is that static configuration is prone to error, likely to become out-of-date as the network changes and grows over time, and users need to understand IPv6 addressing to make the configuration.

Topology discovery could be achieved in one of two ways. The first is with an IGP like OSPFv3, RIPng, etc. These protocols are well-known for enterprises and service providers and provide good topology information. They are, however, also heavyweight (resource intensive) and present configuration challenges in a home environment. The other option is site-specific multicast (SSM). This method would have IRs/CERs send out SSM messages to identify topology, similar to spanning tree. This allows for a comprehensive topology to be discovered, similar to link-state IGP. Unfortunately, it would require 6man IETF development, which would be slowed even further since its a new approach for router vendors.

The top-down message approach might look something like the [ID-UP-PIO] with traceroute added in. This mechanism would be lightweight, provide good topology information, and identify each home routers place in hierarchy. On the downside; it too requires IETF (6man) development, it is best for hierarchical topologies, and it requires traceroute to identify CER.

Top-down messages could also use a DHCP option. To do this, home routers would request the CER_ID DHCP option [ID-CER-ID], and the CER would insert its own address; subtended routers would simply copy the CER option for downstream requests (all routers receive the CERs address). This method requires no end-user configuration, directly identifies CER, and works with all topologies. It does require IETF (dhc) development, however, and could lead to split trees/reconvergence delay depending on the home router attachment order (the order that routers are added to the home network).

Finally, automatic determination could be achieved in several ways. Prefix length and traceroute could be combined, but this would only work with hierarchical topologies, and would require consensus on depth/width and default prefix size. Alternatively, home routers could match their received RA with the DHCP server address. If the DHCP server address matched the router address in the RA, then the DHCP server is the CER (and the receiving router is not). Here again, however, this mechanism only works in hierarchical topologies, and it would not work with DHCP relays.

In summary, there are three viable short-term approaches: IGP, DHCP option, and static. Of the three, CableLabs recommends using a new DHCP option because it is lighter weight than an IGP, offers relatively fast development

time, requires no user configuration, and the specifics can be tuned. As such, CableLabs has submitted [ID-CER-ID].

13.1.5.2 ULA

ULA (Unique Local Addresses) are defined in [RFC4193]; they have an IPv6 unicast address format, are globally scoped, and are intended for local communications. Local IPv6 addresses are created using a pseudo-randomly allocated global ID with a prefix of FC00::/7, the L bit set to 1, and a 40-bit global identifier (the pseudo-random bit). Using a well-known prefix (FC00::/7) allows for easy filtering at site boundaries, which is important because ULA are designed to be routed inside of a site, similar to other types of "private" unicast addresses (e.g., [RFC1918] for IPv4). This creates a need for a "ULA boundary" because traffic sourced or destined for a ULA address is not relevant on the Internet.

The ULA boundary serves to block or NAT ULA traffic at the CER. ULA filtering could, therefore, cause brokenness if hosts attempt to communicate across this boundary (e.g., with servers on the Internet) using ULA addresses. Even with ICMP messages returned, the host is unlikely to switch to GUAs. With NPT (NAT) instead of filtering, ULAs behave much like IPv4 [RFC1918] addresses.

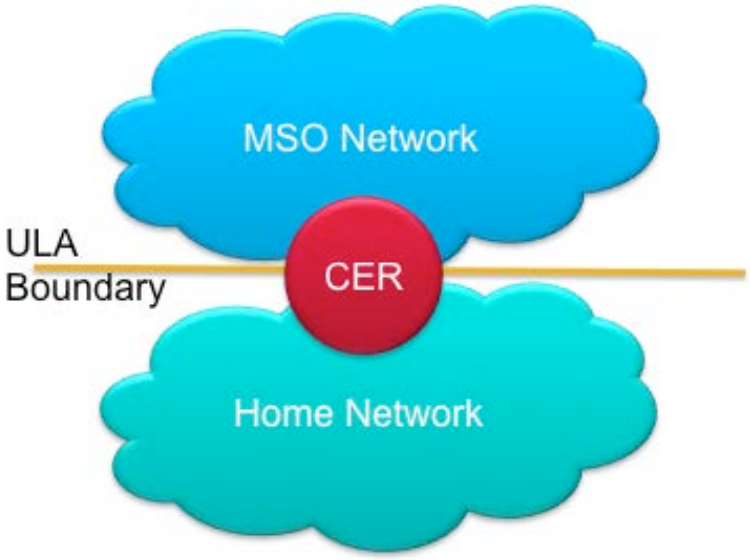

Figure 111 - ULA Boundary

Many members have been hesitant to support the deployment of ULA in home networks. CableLabs examined the benefits and potential issues with ULA addressing in home networks to provide a basis for future decisions in this space.

In the "pro" column, ULAs support routing inside the home similar to [RFC1918] space, they can be used for operation of the internal network regardless of WAN connectivity (e.g., during an ISP outage). Because they are locally generated, there is no renumbering needed, which provides inherent prefix stability for home networks as well. This in turn facilitates Service Discovery in the home (stable internal addressing means easier service directory creation and maintenance). ULAs also support home-network privacy by allowing topology hiding and internal-only hosts (ULA only, no GUA). There is also the possibility for GUA prefix size flexibility for MSOs when using ULA in the home because home-network addressing is not tied to the GUA prefix directly. There are two ways to take advantage of this: NPT 66 (IPv6-to-IPv6 Network Prefix Translation) [RFC 6296] and the Overlay network (ULA + GUA-Tunneling).

There is one potentially major downside to using ULA in the home; hosts may try to use ULAs to connect to the Internet. Improper Source Address selection leads to what the industry has dubbed "IPv6 brokenness." This arises because ULA is globally scoped but only locally significant (ULAs do not allow Internet connectivity). Much of this issue stems from [RFC3484], which was written 2.5 years before ULAs were defined, so its address selection algorithm doesn't consider ULAs at all. Luckily there is an update in progress within the 6man working group at the IETF that better handles ULA vs. GUA selection, but will take time for host implementation [ID-3484bis].

The bottom line is that ULAs are intended to act as [RFC1918] for IPv6 and provide stable home network topology regardless of ISP connectivity. Unfortunately, today, improper host address selection leads to brokenness. NPT (NAT) can address this brokenness, but it brings with it the challenges of NAT.

If ULAs are used in the home network, a method for generation and distribution must be determined. Because ULAs are locally significant, they must be generated and distributed locally (i.e., MSOs will not provide ULA). CableLabs identified two approaches to ULA distribution in the home.

Each individual home router could generate its own ULA prefix. This approach does not require prefix delegation (since each router creates its own prefix) and allows non-hierarchical routing. There is a small chance of duplicate prefixes, but more importantly this method would require a routing protocol to signal each independently generated prefix to all routers in the home network.

The other method is for the CER to delegate a single "unified" ULA prefix to all IRs within the home network. This does not require routing protocol, but does need prefix delegation, and it can support hierarchical routing. An added benefit is that it guarantees prefix uniqueness within the home.

CableLabs recommends this latter unified prefix because it offers a lightweight and stable topology, uses homenet mechanisms designed for GUAs, and no routing protocol is required.

13.1.6 Timeline

CableLabs expects home network architectures to evolve over time. They are emerging now, based on [eRouter] and [RFC6204], and will grow in complexity as more routers are needed. These multi-router topologies will require CER identification and an addressing mechanism. The likely addressing mechanism will be GUA PD (Hierarchical DHCPv6 PD) similar to what is outlined in [ID-Prefix-Alloc] today. Currently CableLabs sees no need for an in-home routing protocol but advises members to watch the IETF Homenet working group as home networks evolve.

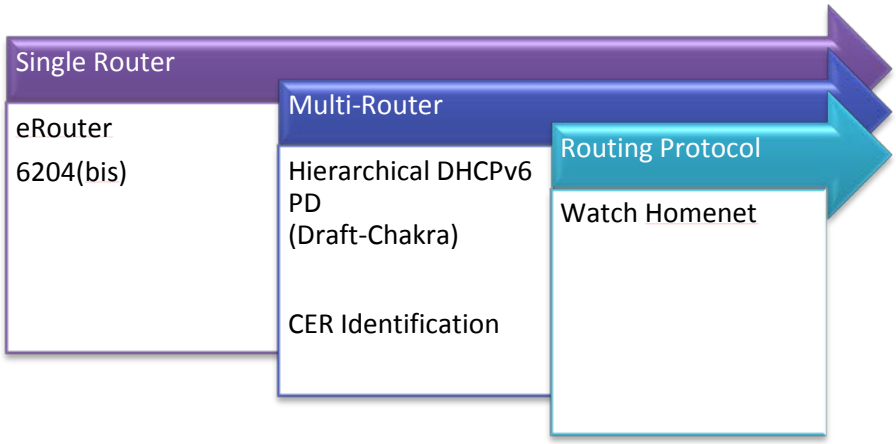

Figure 112 - Timelines for Future Home-Network Architectures

13.2 Service Discovery

Wikipedia describes service discovery as follows: "Service discovery protocols are network protocols which allow automatic detection of devices and services offered by these devices on a computer network."

While exploring service discovery options for home networks, CableLabs made several general assumptions about the networks and services involved.

It is assumed that there will be multiple subnetworks/LANs and routers (CER and IRs) in each home network. Home networks are expected to have multiple Layer 1 and Layer 2 protocols (e.g., Ethernet, Wi-Fi, MoCA, etc.). Finally, home networks are assumed to be dual-stacked (configured for both IPv4 and IPv6) and have arbitrary topologies that generally fit the model of a single-ISP inverted-tree with loops possible.

It is further assumed that there will be multiple service types (e.g., media, printers, security and automation, etc.), multiple devices per service (e.g., more than one media server), and multiple gateways (e.g., distinct Internet and IP video gateways). Machine-to-machine communication within home (e.g., auto-configuring sensor network) is also expected.

Based on these assumptions, CableLabs identified several basic requirements that a home network service discovery protocol must meet. To start with, service discovery must work across the entire home network (i.e., a site-local rather than link-local mechanism). Service discovery is needed for all services expected within the home (e.g., audio, video, print, security and automation). The home network must support media delivery from inside and outside of home (e.g., a media server within home and IP video delivery from the Internet). Service discovery must also support auto-configuration (both M2M and human controlled).

Taking all of that into consideration, CableLabs further investigated the primary challenges to providing this type of service discovery in the home. First and foremost, multi-router service discovery is today largely untested as the previous focus appears to have been specifically on local link communication. Also, there are many different types of devices in the home from various vendors, some with proprietary implementations (e.g., UpnP, CE Devices, Bonjour, Apple). Finally, most home routers block multicast by default and even the new IPv6 CPE router standards, [eRouter] and [RFC6204], are silent on LAN-to-LAN multicast.

There are four potential protocols for home network service discovery. Simple Service Discovery Protocol (SSDP) is part of UPnP and appears to be a viable option today due to the facts that it is dual-stack, can use both link and site scope multicast messages, is an open standard supported by many big and small CPE vendors, and is stable and well defined with multiple implementations. DNS Service Discovery (DNS-SD) is typically used with mDNS (as in Apple's Bonjour), which needs its multicast scope expanded beyond link-local (dropping mDNS likely requires an in-home DNS server). On the plus side, DNS-SD is dual-stack, uses standard DNS messages, is documented in published IETF drafts, and is implemented by Apple with software available for other platforms. Local Multicast Name Resolution (LLMNR) was investigated but is only useful for name resolution and does not include a mechanism for service discovery. Service Location Protocol (SLP) rounds out the options. SLP is a comprehensive service discovery framework that uses administrative scope (site-local) multicast messages and is documented in published RFCs. Unfortunately, it is IPv4-only and has very little current consumer electronics (CE) support.

13.2.1 Service Discovery Timeline

UPnPs SSDP is the most viable option for in-home service discovery today, although multicast support in-home routers needs to be enhanced and tested. Longer term, DNS-SD may be useful as well, once coupled with a site-scoped multicast DNS or some form of in-home DNS server.

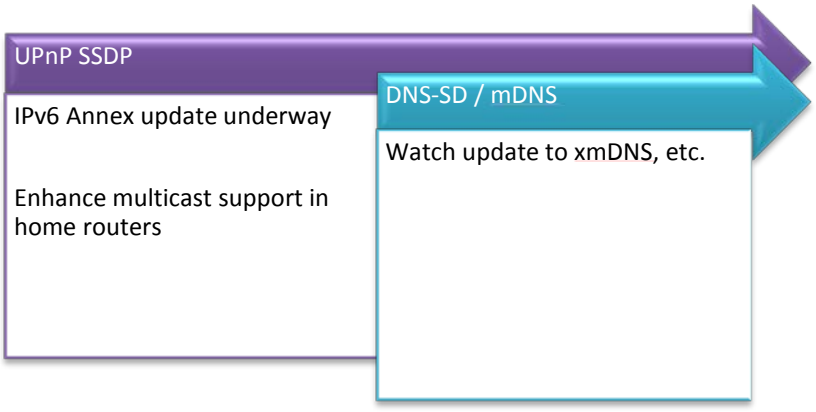

Figure 113 - Service Discovery Timeline

13.3 IP Video Gateway

IP video gateways are used by MSOs to provide IP video service streamed to tablets, IPTVs, smart phones, etc., within the subscriber home. The MSO may or may not provide Internet service to IP video service customers,

opening the potential for a dual-gateway scenario (separate data and video gateways). In any case, the MSO-provided video must transit the MSO-provided video gateway for ensured QoS, DRM compliance, etc. In the same home, Internet traffic must continue to transit the data gateway (provided by the MSO or a third party) as there will be no data path through the video gateway. CableLabs has identified three scenarios to address this problem space: a combined gateway, independent gateways, and hierarchical gateways. All three are reviewed in detail in the following sections.

13.3.1 Combined Data and Video Gateway

In this first scenario a single MSO-provided device includes both data and video gateways. This combined gateway acts as the CER for the customer's home network. It manages the home network LAN (DHCP, DNS, etc.) and provides the default gateway for all traffic leaving the home. The combined gateway routes both data and video streams intelligently, sending them "up" or "out" the appropriate interface. This combined gateway also provides service discovery functions for all MSO-provided video. See Figure 114 for an illustration of this scenario.

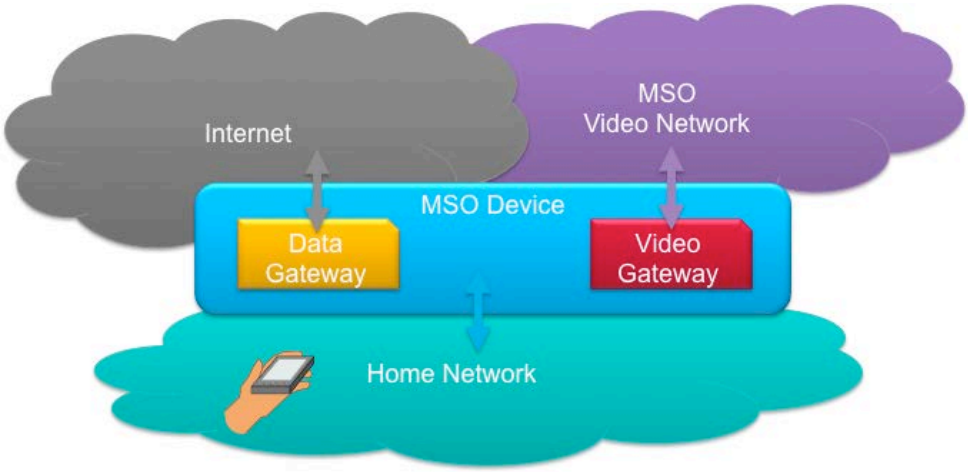

Figure 114 - IP Video Gateway Scenario 1: Combined Gateway

This scenario is simple and efficient, providing a single device and a single addressing space within the home. The combined gateway also provides MSOs with most control and enables a single service discovery domain. However, it also requires the availability of combined gateway devices (not available today) and requires that MSOs provide both data and video services, which won't always be the case.

13.3.2 Independent Gateways

In the second scenario, the data provider deploys a data gateway, the video provider deploys a video gateway, and each gateway manages its own distinct home network. In this scenario, the customer must move devices between the two networks. Combining these parallel networks is not practical because hosts only accept addresses from a single DHCP server. The video gateway is responsible for providing service discovery functions for the MSO-provided video while the data gateway may or may not participate in LAN service discovery. This scenario is illustrated below, in Figure 115.

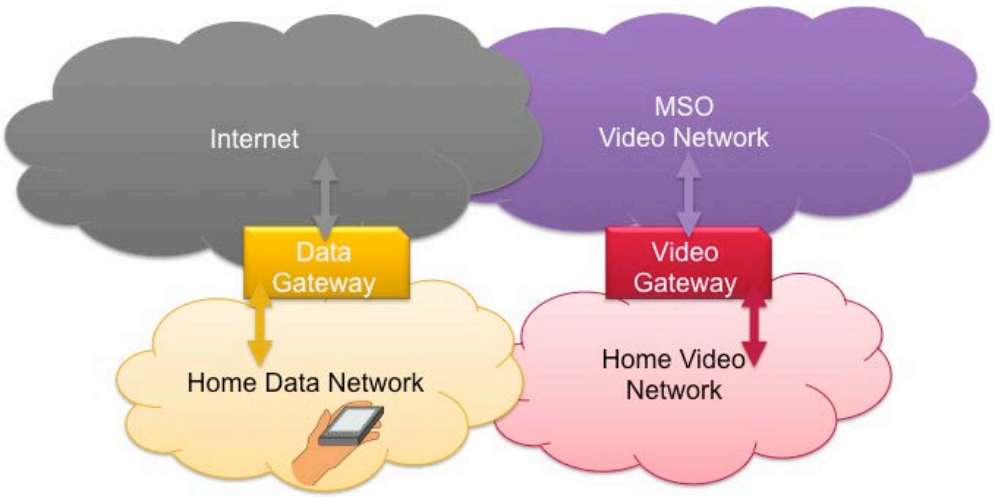

Figure 115 - IP Video Gateway Scenario 2: Independent Gateways

The independent gateway scenario is simple to deploy for each service and/or provider, and uses simple, single-purpose devices. The main problem with this approach is that customers must move devices between networks because data/Internet service is not available on video network and vice versa (no browsing while watching). Another drawback is that this scenario splits service discovery into two domains (one per network). The independent gateway scenario is also prone to user error. Connecting the two networks together would result in non-deterministic behavior and not all users are familiar with switching their device between networks.

13.3.3 Hierarchical Gateways

Similar to the last scenario, in the hierarchical gateway scenario the data provider deploys a data gateway, and the video provider deploys a video gateway. However, in this case, the hosts and the video gateway all join the data gateway managed network. This means that DHCP, DNS, etc., are all provided by data gateway, which acts as the sole CER for the home. Three options have been identified by CableLabs for routing the video traffic: Proxy, NAT, and Reverse PD. All three are covered in detail below. In this scenario the video gateway should be capable of acting as the CER when there is no data gateway present to ensure that video service works regardless of the presence of Internet/data service. The video gateway is responsible for providing service discovery functions for MSO-provided video, but the data gateway should participate in LAN service discovery as well, when possible. Figure 116 provides an illustration of this scenario.

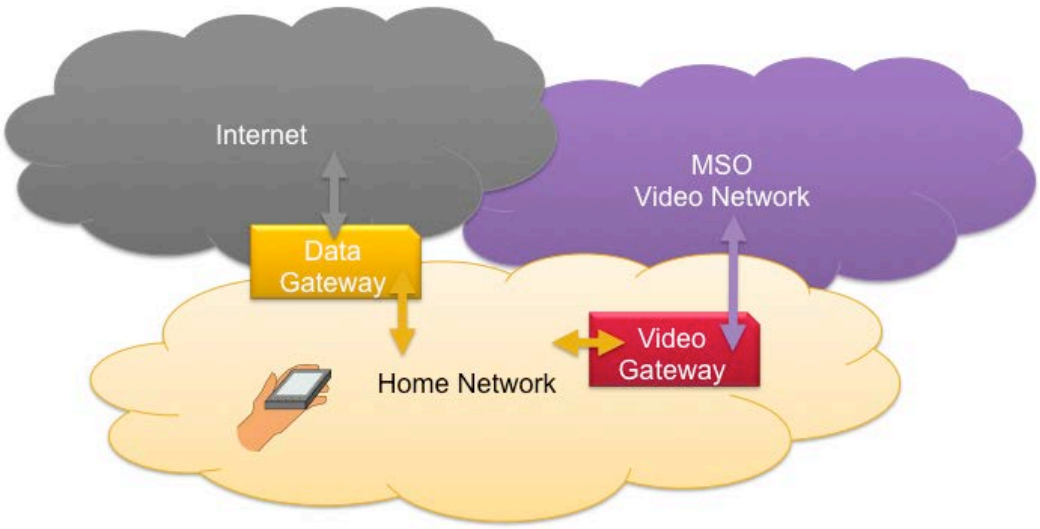

Figure 116 - IP Video Gateway Scenario 3: Hierarchical Gateways

Like the independent gateway scenario, the hierarchical gateway scenario is simple to deploy for each service and/or provider and uses simple, single-purpose devices. This scenario adds the benefits of a single home network and single service discovery domain to that, however. The downsides associated with those gains are that the customer must connect the video gateway correctly to the data gateway and to the video WAN (MSO network). This third scenario also requires vendor development due to the more complex routing for the MSO video service, and the fact that the video gateway needs to be able to distinguish stand-alone (single-gateway) vs. hierarchical (dual-gateway) environments.

As mentioned above, there are three hierarchical gateway implementation options. The first is NPT, where the video gateway performs prefix translation between the home and the MSO network. The next option is a potential enhancement to DHCPv6 developed by CableLabs called reverse PD (prefix delegation) in which the video gateway sends the MSO-assigned prefix information "up" to CER/DHCP server. The final implementation option is to use a back-to-back service proxy. The following sections cover these three methods in more detail.

13.3.3.1 Hierarchical Gateway with NPT

There are actually two ways to implement NPT in the hierarchical gateway scenario; dual-NPT and NPT with Route Information Object (RIO).

13.3.3.1.1 Dual NPT

With dual NPT, the video gateway uses MSO addresses on the MSO interface and Internet addresses (assigned by the data gateway) on its LAN interface. The video gateway then performs NPT in both directions. The video gateway advertises all available MSO video services into the LAN with NPT addresses. Clients establish sessions with the MSO video network through the video gateway directly. This is illustrated in Figure 117.

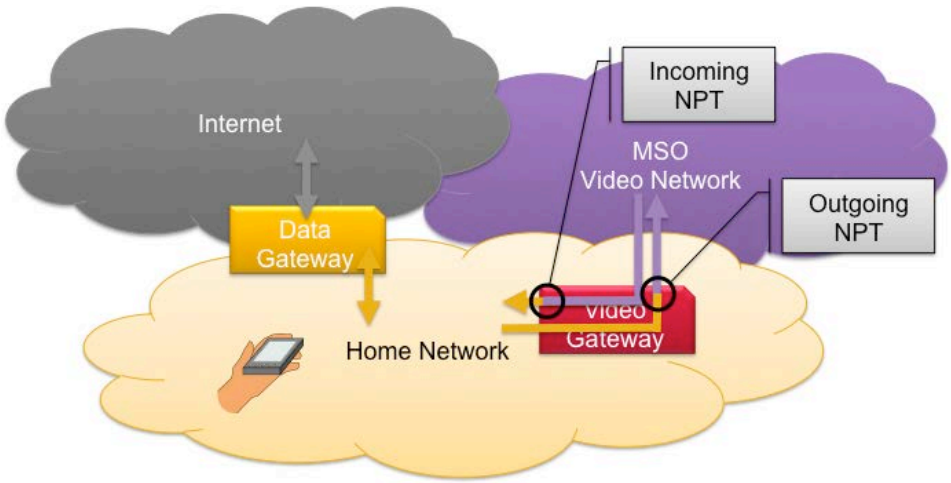

Figure 117 - IP Video Gateway Scenario 3.1: Hierarchical Gateway with Dual NPT

The dual NPT approach benefits from needing no special routing in the LAN nor interaction from the data gateway. It allows for a relatively simple video gateway and clients interact directly with the MSO network. However, its NAT and the video gateway may actually require an Application Layer Gateway (ALG) for many video services to function properly.

13.3.3.1.2 NPT and RIO

When combining a single instance of NPT with RIO, the video gateway again uses MSO addresses on the MSO interface and Internet addresses on its LAN interface. The video gateway then advertises the MSO prefix to hosts in the home network as route info in an RA using the RIO defined in [RFC4191]. The video gateway still performs NPT on outbound traffic, but does not need to do so on inbound traffic in this case since the MSO video services are advertised into the LAN with MSO addresses. Clients establish sessions with the MSO video network via the video gateway directly. Figure 118 provides an illustration.

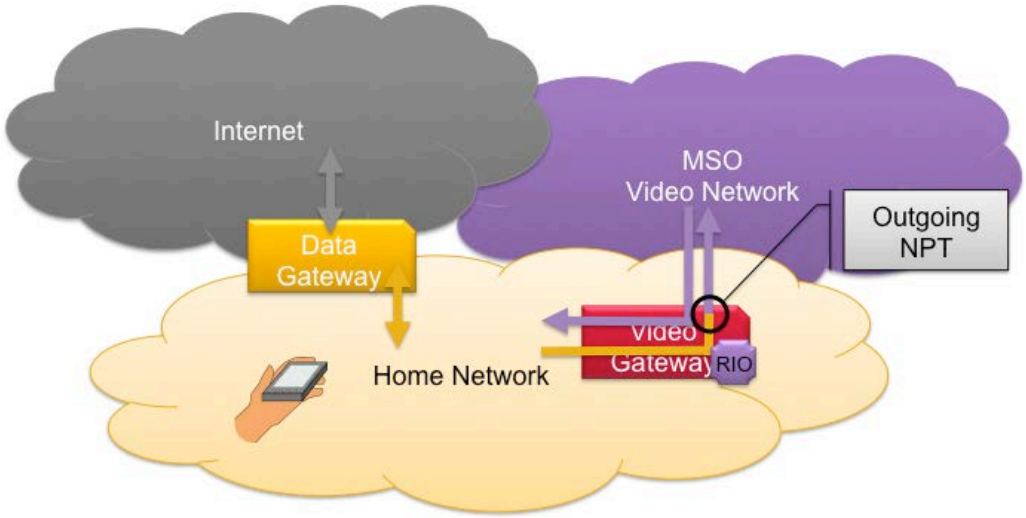

Figure 118 - IP Video Gateway Scenario 3.2: Hierarchical Gateway with NPT and RIO

Here again, no interaction from the data gateway is needed, and because clients interact directly with the MSO network a relatively simple video gateway is allowed. It's still NAT though and the video gateway may still require one or more ALGs. Furthermore, this method requires that all hosts support the RIO (type "c" hosts in [RFC4191] parlance). It also requires a flat network or CER/IR processing of the RIO.

13.3.3.2 Reverse PD

In the reverse PD case, the video gateway (dhcp client) advertises the MSO-assigned video prefix to the data gateway (dhcp server). This video prefix is the one to be used by clients on the LAN to reach video network and therefore must be routed to the video gateway. The data gateway then hands out addresses to clients from both prefixes so that all hosts acquire two addresses, one on the data network and one on the video network. The video gateway advertises all MSO video services into LAN with MSO video network addresses. Clients establish sessions with the MSO video network via video gateway, but traffic is routed through the data gateway first (it's the default router), and clients must use the video prefix address (requires good host address selection). The data gateway, of course, still handles traffic to the Internet, and clients use the data prefix address for these communications. An illustration of this model is shown in Figure 119 below.

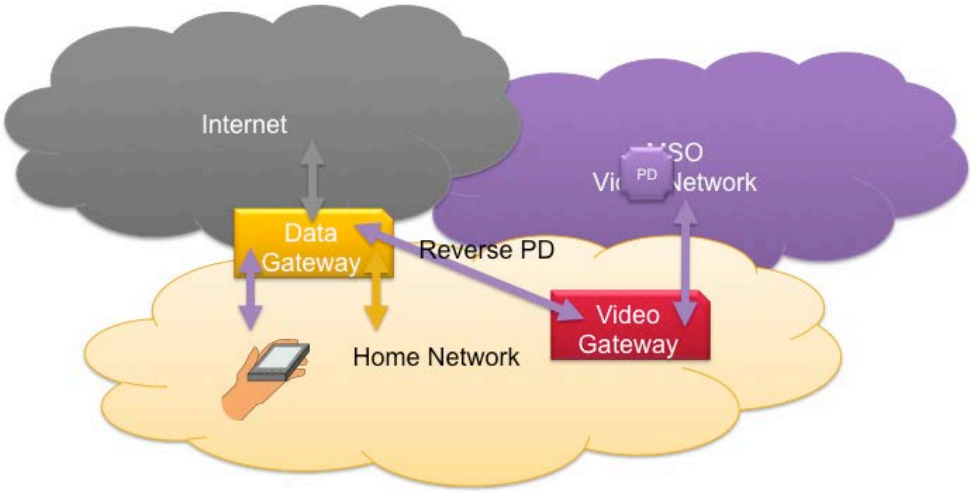

Figure 119 - IP Video Gateway Scenario 3.3: Hierarchical Gateway with Reverse PD

One of the primary advantages of reverse PD is that it removes the need for NPT and still allows a simple video gateway since clients interact directly with the MSO network and there is no need for an ALG. Unfortunately, since this was just invented at CableLabs, it needs protocol development (reverse PD needs to be added to DHCPv6). Perhaps an even larger hindrance is the fact that this method requires interaction with data gateway, which may not be under MSO control or management. Finally problems with host address selection would also manifest themselves in such a network.

13.3.3.3 Proxy

The final option identified by CableLabs to support the hierarchical gateway scenario requires the video gateway to act as full video service proxy. The video gateway advertises all MSO video services into LAN from its LAN address, and clients then establish sessions with the video gateway (not the MSO network). The video gateway closes the loop by establishing back-to-back sessions with the MSO network. In this model, the video gateway uses MSO addresses on the MSO interface and Internet addresses (provided by the CER/data gateway) on its LAN interface. See Figure 120 for an illustration representing this model.

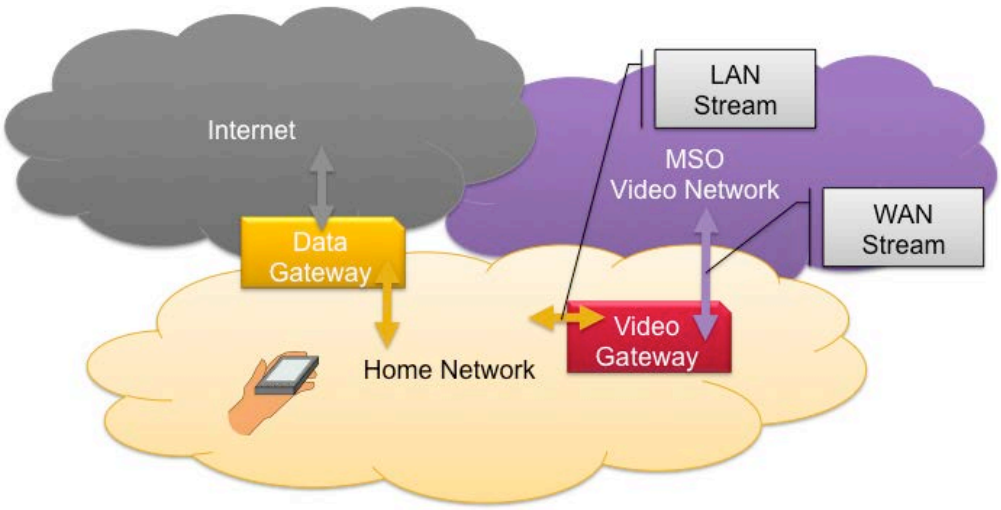

Figure 120 - IP Video Gateway Scenario 3.4: Hierarchical Gateway with Proxy

No special routing is required in LAN when using the proxy technique, and the video gateway provides a clear demarcation between the home and MSO networks. One of the less obvious benefits of this model is that the LAN and WAN video sessions are independent, so the WAN session could switch between multicast and unicast and/or the LAN and WAN sessions could be different protocols, both without any disruption to the customer. Another plus is that no interaction from the (potentially third party) data gateway is needed. The downside is that this method requires a fairly advanced video gateway that must be capable of performing full back-to-back proxy for both service discovery and video streaming.

13.3.4 Timeline

The combined gateway is a single device that provides simplicity but lowers flexibility. Independent gateways create separate networks that are likely to provide a poor user experience. Hierarchical gateways provide flexibility, but add complexity and offer multiple options for implementation: NPT, Reverse PD, and Proxy.

The Proxy and dual NPT methods of the hierarchical gateway scenario are both feasible options today with NPT, plus RIO possibly becoming an attractive replacement for dual NPT once most devices support the RIO.

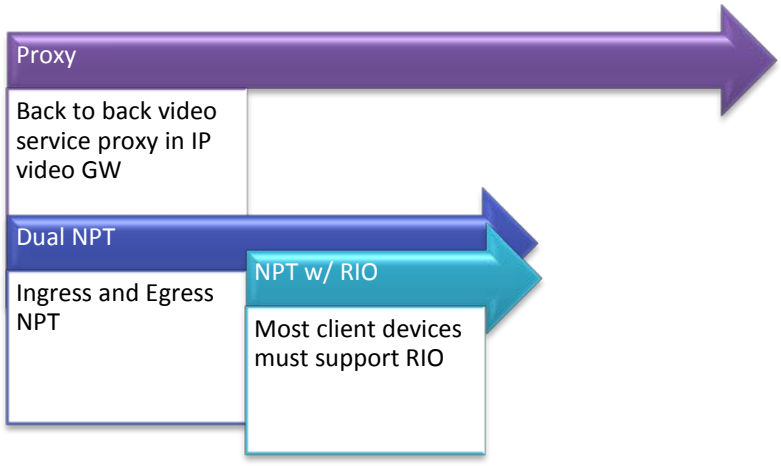

Figure 121 - Proxy and Dual NPT Methods of the Hierarchical Gateway Scenario

13.4 Home Routing Protocol

CableLabs and engaged members agree that a home routing protocol is unnecessary at this time. If there is a need for a home routing protocol in the future, what's our best bet? CableLabs examined multiple options gathered from several IETF working groups: Homenet, 6LoWPAN, MANET, etc. The routing protocols investigated were:

- OSPF – Open Shortest Path First
- IS-IS – Intermediate System to Intermediate System
- RIPng – Routing Information Protocol next generation
- UP-PIO - Finding Up in an Unmanaged Network
- RPL - IPv6 Routing Protocol for Low-Power and Lossy Networks
- OLSR – Optimized Link State Routing Protocol
- AODV - Ad hoc On-demand Distance Vector Routing Protocol
- LOAD – 6LowPAN On-demand Distance Vector RP
- DYMO-Low - Dynamic Manet On-Demand for 6LoWPAN RP
- Hi-Low – Hierarchical Routing over 6LoWPAN

These protocols were all weighed against the requirements documented in [ID-Routing-Req]:

- Reachability between all nodes in the home network
- Border detection
- Robust to routers being moved/added/removed/renumbered
- No configuration required
- Best-path is a non-requirement
- Support for multiple upstream networks is a requirement
- Cannot assume hierarchical prefix delegation in the home
- Failover (multiple upstream paths to one destination)
- Prevent looping
- Should be a lightweight solution
- Must handle multi-dwelling units
- Must be resilient to running on wireless networks
- Robustness in the face of unintentional joining of networks

There are many feasible options, two of the primary decision points are:

- Link State, Distance Vector, or Ad Hoc routing protocol?
- Which of the various optimizations are most beneficial?

Additional protocol work is needed regardless of choice. CER Identification is lacking and needed by most, and further protocol work is also needed by most protocols to support full auto-configuration and specific home network requirements. Vendor implementations are still needed in all cases.

In the end, hierarchical DHCPv6 Prefix Delegation [ID-Prefix-Alloc] is easier to implement than any routing protocol, and routing protocols are likely only needed when multi-homing home networks. Residential multi-homing is not believed to be likely at this time, but a routing protocol may also be needed for loop prevention. In any case, any home routing protocol is likely to take significant time to reach consensus within the IETF (homenet working

group), and other solutions are likely to be available sooner. This does not preclude adding a routing protocol into the home network when standardization is complete.

14 REQUIREMENTS

This section defines requirements for providing IPv6 services in a cable environment. General requirements are applicable to all devices (e.g., cable modems, CMTSs, and servers). In addition, device-specific requirements sections provide additional requirements for devices. When designing IPv6 products, device manufacturers should first consider the general requirements applicable to all devices, and add support for requirements applicable to their class of device.

14.1 General Requirements

This section lists IPv6 requirements applicable to all devices.

- MUST support the following RFCs:
    - [RFC2460], Internet Protocol v6 (IPv6) Specification
    - [RFC4861] Neighbor Discovery for IPv6
    - [RFC4862], IPv6 Stateless Address Auto-configuration

14.2 Cable Modem Requirements

This section lists IPv6 requirements applicable to cable modems supporting DOCSIS 2.0+IPv6 and DOCSIS 3.0 specifications.

14.2.1 DOCSIS 2.0+IPv6 CM

- MUST support DOCSIS 2.0+IPv6 Cable Modem Specification, [DOCSIS2.0-IPv6].
- MUST support IPv6 management as defined in the OSSIv3.0 Specification, [OSSI].
- MUST support Provisioning Mode Override, as defined in [OSSI] and [DOCSIS2.0-IPv6].

14.2.2 DOCSIS 3.0 CM

- MUST support MAC and Upper Layer Protocols Interface Specification, [MULPI].
    - In particular, MUST support Upstream Drop Classifiers.
- MUST support OSSIv3.0 Specification, [OSSI].
- MUST support Provisioning Mode Override, as defined in [OSSI].
- MUST support all DOCSIS Security features as defined in [SECv3.0], including BPI+, Secure Software Download, Max CPE Setting from the CM config file.

14.2.3 DSG CM

- MUST support DOCSIS Settop Gateway [DSG].
- DSG eCM MUST be DOCSIS 3.0 or D2.0+IPv6.

14.3 IP Simulcast Gateway Requirements

- Data Gateway MUST support Dual-stack for the access and in-home video delivery.
- Video Gateway MUST support Dual-stack for in-home video delivery.

14.4 eSTB Requirements

- MUST support OpenCable Host Device 2.1 Core Functional Requirements specification [HOST2.1-CFR].
- MUST support IPv6-only mode of operation.

14.4.1 OCHN Extension Requirements

- MUST support OCHN (which points to DLNA and UPnP).

14.5 CMTS Requirements

This section lists IPv6 requirements applicable to DOCSIS 3.0 CMTSs.

- MUST support MAC and Upper Layer Protocols Interface Specification, [MULPI].
    - MUST support DHCPv6 relay agent.
    - MUST support ND Proxy.
- MUST support OSSIv3.0 Specification, [OSSI].
- MUST support ingress and egress access lists for the RF interface.
- MUST support CPE IPv6 traffic forwarding.
- MUST support IGMPv3 [RFC3376] and MLDv2 [RFC3810].
- MUST support ICMPv6 [RFC4443].
- MUST support OSPFv3 [RFC5340] or IS-IS [RFC5308] for IPv6.
- MUST support IPv6 transport of SNMP and syslog messages.
- MUST support Data Lawful Intercept requirements identified in [CBIS].
    - MUST be capable of identifying and capturing encapsulated traffic (e.g., 6RD and DS-Lite traffic).
- MUST support Voice Lawful Intercept requirements identified in [ES INF] and [ES DCI]
- MUST support DHCP snooping as described in Section 5.9.2.3.
- MUST support, all DOCSIS Security features as defined in [SECv3.0], including DHCP Relay Agent and TFTP Proxy, CMTS MIC, Early Authentication and Encryption, ACLs, SAV, RA Configuration, Ability to filter various packets (e.g., RH0), Reconfigure Key Authentication Protocol (RKAP) DHCPv6.

14.5.1 DSG CMTS

- MUST support DOCSIS Settop Gateway [DSG].
- MUST support above D3.0 CMTS requirements.

14.6 eRouter/Home Gateway Requirements

This section lists IPv6 requirements applicable to eRouters and retail home gateways.

- MUST support IPv6 provisioning of CPE devices as specified in [eRouter].
- MUST support IPv6 address assignment, as specified in [eRouter].
- MUST support [RFC4361] to make the DHCPv4 client identifier identical to the DHCPv6 DUID.
- MUST provide DHCPv6 service on CPE-facing interfaces, as described in [eRouter].

- MUST provide IPv6 traffic forwarding, as described in [eRouter].
- MUST support a firewall. Configuration and operation of the firewall is outside of the scope of this document.
- MAY support DS-Lite [RFC6333].
  - MAY support the [RFC6106] Recursive DNS Server Option.
- Retail Home Gateways SHOULD support Requirements for IPv6 Customer Edge Routers, [RFC6204].
- DLNA and UPnP Gateways.

14.6.1 Security Requirements

- MUST support Simple Security [RFC6092].
- If the Home Gateway supports a Wi-Fi interface, it MUST support some form of secure Wi-Fi (WPA or WPA-enterprise).
- MUST support Simple Security [RFC6092], and it MUST be on by default.
  - Stateless Filters MUST support all as defined in [RFC6092].
  - Connection-Free Filters:
    - MUST support ICMP, Upper-Layer Transport Protocols, UDP, IPsec, IKE.
    - MAY support: Mobility in IPv6.
  - Connection-Oriented Filters:
    - MUST support TCP, Shim6.
    - MAY support SCTP and DCCP.
  - MAY support Passive Listeners and Management Applications.

  At a high level these include: dropping inbound DHCPv6 discovery packets received on exterior interfaces, ability to configure Static and dynamic Firewall rules, check for valid Source addresses, allow for only allocated IPv6 blocks, filter RH0 traffic, Support MAC address ACLs, etc.
- MUST support ability to configure the home DHCP server with short lease times.
- MAY support ULAs on the Local Network and ULA filtering.
- MAY support Advanced Security [ID-IPv6SEC] and the Intrusion Detection and Prevention concepts from it.

14.7 Dual-stack E-DVA Requirements

This section lists IPv6 requirements applicable to PacketCable 2.0 E-DVA devices.

- MUST support PacketCable 2.0 specifications.
- MUST be capable of routing both IPv4 and IPv6.
- MUST support dual-stack implementation.
- MUST support IPv4 and IPv6 stacks simultaneously for media.
- MUST support the ability to independently configure preference of the IP address family used for provisioning, signaling, and media (SDP).

14.8 PC 2.0 Core (e.g., x-CSCF) Requirements

This section lists IPv6 requirements applicable to PacketCable 2.0 Core devices (e.g., P-CSCF, I-CSCF, SCSCF, BGCF, UGC and Application Servers).

- MUST support PacketCable 2.0 specifications.
- MUST be capable of routing both IPv4 and IPv6.
- MUST support dual-stack implementation.
- MUST support IPv4 and IPv6 stacks simultaneously.

14.9 TrGW Requirements

This section lists IPv6 requirements applicable to Translation Gateways.

- MUST be capable of routing both IPv4 and IPv6.
- MUST support Dual-stack implementation.
- MUST support IPv4 and IPv6 stacks simultaneously.

14.10 SBC Requirements

This section lists IPv6 requirements applicable to Session Border Controllers.

- MUST support Dual-stack implementation.
- MUST support IPv4 and IPv6 stacks simultaneously.

14.11 Server Requirements

This section lists IPv6 requirements applicable to MSO back-end servers.

14.11.1 Common Requirements for All Servers

- MUST support the following RFCs:
    - [RFC1981] Path MTU Discovery for IPv6.
    - [RFC2460] Internet Protocol v6 (IPv6) Specification.
    - [RFC3596] DNS Extensions to Support IPv6.
    - [RFC4291],IPv6 Addressing Architecture.
    - [RFC4443] Internet Control Message Protocol (ICMPv6).
    - [RFC5569] Neighbor Discovery for IPv6.
    - [RFC4862] IPv6 Stateless Address Auto-configuration:
        - MUST support [RFC4862] auto-configuration of link-local addresses.
        - MUST support manual configuration.
        - MUST support disabling auto-configuration.
- Servers that are manageable using SNMP MUST support the following IPv6 MIBS:
    - [RFC3410] Introduction and Applicability Statements for Internet Standard Management Framework.

- [RFC3411] An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.
- [RFC3412] Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
- [RFC3413] Simple Network Management Protocol (SNMP) Applications.
- [RFC3414] User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- [RFC3415] View-based Access Control Model (VACM) for the simple Network Management Protocol (SNMP).
- [RFC3416] Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).
- [RFC3417] Transport Mappings for the Simple Network Management Protocol (SNMP).
- [RFC3418] Management Information Base for the Simple Network Management Protocol (SNMP).

14.11.2 DHCP Server

- MUST parse the following options sent by the CM and defined in [CANN DHCP-Reg]:
  - Option 16 - containing enterprise number 4491 (CableLabs) and the DOCSIS version.
  - Option 17 - containing the device type.
- MUST provide CableLabs Vendor-specific information options (option 17) defined in [CANN DHCP-Reg], specifically the following options:
  - Time Protocol Servers option (37).
  - Time Offset option (38).
  - TFTP Server Addresses option (32).
  - Configuration File Name option (33).
  - Syslog Server Addresses option (34).
  - CL ERouter Container Option (1027).
- MUST support PacketCable-specific options specified in [CANN DHCP-Reg]:
  - CL_V4OPTION_CCCV6 (123).
  - CL_V4OPTION_IP_PREF (124).
  - CL_OPTION_CCC (2170).
  - CL_OPTION_CCCV6 (2171).
- MUST be able to send options defined in [CANN DHCP-Reg] specification.
- MUST support [RFC3315], [RFC3633], and [RFC6346].

14.11.3 DNS Server

- MUST support the following RFCs:
  - [RFC2874] DNS Extensions to Support IPv6 Address Aggregation and Renumbering.
  - [RFC3226] DNSSEC and IPv6 A6 aware server/resolver message size requirements.

- [RFC3363] Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS).
- [RFC4291] Internet Protocol Version 6 (IPv6) Addressing Architecture.
- [RFC3596] DNS Extensions to Support IP Version 6.
- [RFC4033] DNS Security Introduction and Requirements.
- [RFC4034] Resource Records for the DNS Security Extensions.
- [RFC4035] Protocol Modifications for the DNS Security Extensions.
- [RFC4470] Minimally Covering NSEC Records and DNSSEC On-line Signing.
- DNS Masking.

14.11.4 Time Server

- Servers providing ToD service MUST support [RFC0868].
- Servers providing NTP service MUST support [RFC5905].

14.11.5 TFTP Server

- MUST support [RFC1350].

14.11.6 Network Management Server

- MUST support the following additional RFCs:
  - [RFC3419] Textual Conventions for Transport Addresses.
  - [RFC3584] Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.
  - [RFC3410] Introduction and Applicability Statements for Internet Standard Management Framework.
  - [RFC3411] An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.
  - [RFC3412] Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
  - [RFC3413] Simple Network Management Protocol (SNMP) Applications.
  - [RFC3414] User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
  - [RFC3415] View-based Access Control Model (VACM) for the simple Network Management Protocol (SNMP).
  - [RFC3416] Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).
  - [RFC3417] Transport Mappings for the Simple Network Management Protocol (SNMP).
  - [RFC3418] Management Information Base for the Simple Network Management Protocol (SNMP).
  - [RFC3419] Textual Conventions for Transport Addresses.
  - [RFC3584] Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.

- [RFC3826] The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.
- [RFC1901] Introduction to Community-based SNMPv2 (Informational).
- [RFC1157] A Simple Network Management Protocol.
- [RFC2578] Structure of Management Information Version 2 (SMIv2).
- [RFC2579] Textual Conventions for SMIv2.
- [RFC2580] Conformance Statements for SMIv2.
- [RFC2786] Diffie-Helman USM Key Management Information Base and Textual Convention.

14.11.7 Syslog Server

- MUST support [RFC5424].

14.11.8 SMTP Server

- MUST support [RFC3974], SMTP in Dual-stack Environments.

14.11.9 FTP Server

- MUST support [RFC2428] and [RFC6384].

14.11.10 PacketCable Key Distribution Center (KDC) Server

- MUST support [RFC4120] The Kerberos Network Authentication Service (V5).

14.11.11 Tunnel Server

- SHOULD support ISATAP [RFC5214].
- SHOULD support GRE [RFC2784].

14.11.12 Common Alert Protocol (CAP) Server for EAS

- MUST support Dual-stack.

14.11.13 DSG Server

- No new Requirements identified for IPv6.

14.11.14 IP Streaming Server

- MUST support Dual-stack.

14.11.15 EBIF Application/Aggregation Server

- MSOs should consider deploying dual-stack systems to support end-to-end connectivity with both IPv4 and IPv6 devices (OpenCable and Legacy) in subscriber home, content providers, and third parties.

14.11.16 OLCA Authentication/Authorization Server

- MSOs should consider deploying dual-stack systems to support end-to-end services.

14.11.17 Advanced Advertising Servers

- MSOs should consider deploying dual-stack systems to support the Advanced Advertising Architecture.

14.12 CGN Device Requirements

14.12.1 Functional Requirements

- A CGN device needs to support the full CGN lifecycle.
    - This may include multiple technologies over several years.
- MUST support [RFC6264] (Incremental Carrier-Grade NAT for IPv6 Transition).
    - MUST support NAT 444.
    - MUST support DS-Lite [RFC6333].
    - SHOULD support 6RD [RFC5569] and [RFC5969].

14.12.2 Security Requirements

- MUST support DOS Mitigation.
    - A CGN device needs to mitigate attacks directed at or through it.
        - Syn proxy, active verification, connection limiting, anomaly recognition, aggressive aging, Unicast RPF, granular rate limiting, dynamic filtering, protocol analysis, etc.
- MUST support ACLs for incoming and outgoing traffic.
    - A CGN device needs to provide at least the basic firewalling ability.
        - Static filtering, rate limiting, white and black listing, etc.
        - MUST NOT require reset or traffic interruption to configure and apply configuration.
        - MUST support Encryption of log data.
        - MUST support sending of encrypted syslog data to servers after authenticating them.
        - Perform BOGON and uRPF checks.
        - Ability for AFTR/CGN to limit port usage per customer.
        - Ability for AFTR/CGN to support session limiting per customer.
        - Ability for AFTR/CGN to support rate limiting per customer.

14.12.3 Session Logging and Retrieval Requirements

- MUST be capable of handling up to 32 MB of logging per user per day.
- MUST support Syslog for remote/off-device logging.
    - MUST support 500,000 log messages per user per day.
- SHOULD support IPDR for remote/off-device logging.
- MUST support bulk port reservation.
    - SHOULD support 100-port blocks.

- MUST support at least two log facilities.
    - One for remote logging and one for local logging.
- SHOULD support Deterministic NAT.
- SHOULD support customized logging.

14.12.4 Application Layer Gateway (ALG) Requirements

ALG changes application-specific information embedded within packet as it transits the CGN since some applications embed IP address and port information.

- MUST support ALGs for top subscriber applications such as FTP, SIP, IPSec, Smooth Streaming, ASF, QuickTime, etc.

14.12.5 Resiliency Requirements

- MUST support 1+1 Stateful NAT.
    - Communicate NAT table updates between the primary and backup CGNs.
    - SHOULD support N+1 Stateful NAT.
- MUST support Fail Open.
    - Passes traffic transparently during failure.
- MUST support 99.99% availability.

14.12.6 Management Requirements

- MUST support FTP and HTTP for file transfer.
    - MUST support SFTP and HTTPS.
- MUST support SNMPv3 including:
    - Interface utilization (bytes and packets / in and out)
    - Session count (number of current connections)
    - Sessions established per second
    - Outside IP/port utilization
    - Overflow port usage
    - High water marks (for all)
    - Top talkers (for all)
- MAY provide access to packet size histogram data.
- MAY support Netconf for device configuration.
- MUST support multiple level of user accounts.
    - R/RW/RWX
- MUST support both HTTP and CLI based interface.
    - MUST support SSH.
    - MUST log user access on independent log facility.

    - MUST log log-ins and configuration changes.
- SHOULD support an XML based interface.
- MUST support both RADIUS and TACACS+.

14.13 6to4 Relay, 6RD Relay Security Requirements

- 6to4 MUST support:
    - Ability to identify and discard ND attack traffic.
    - Verify source IPv6 address prefix includes the source IPv4 address.
    - 6to4 routers/relays should drop the 6to4 packets with broadcast or multicast IPv4 address.
    - Prevent use (block/filter) of actual relay IPv4 address instead of 192.88.99.1.
    - Filter out packets with a routing header.
- 6RD relay MUST support:
    - BR must drop 6RD frames from customer if source IPv6 address in frame is not from an operator assigned 6RD prefix.
    - BR must drop any incoming frames with destination IPv6 prefix not used for 6RD.
    - BR disallows frames with IPv4 private, broadcast and loopback addresses.
    - BR disallows frames with inconsistent source IPv6 delegated prefix and IPv4 address.
    - Reverse path forwarding checks.

14.14 MSO Firewall

- MUST support setting up of firewalls [RFC2979] to allow known and controllable tunneling mechanisms and disallow unknown tunnels.
- Support appropriate filters to only allow internal source or destination addresses to use relays/endpoints.
- Ability to filter certain kinds of tunneled traffic, e.g., Teredo.
- Ability to block routes to injected anycast address.
- IPS/IDS capability would be nice to have.
- All current IPv4 Filtering and firewalling should apply to CGN Traffic as well.

14.14.1 DPI Servers

- MSOs should consider deploying dual-stack systems to support both IPv4 and IPv6 DPI.
- Ensure feature parity between IPv4 and IPv6 for all current uses of DPI.
    - Security
    - Traffic Management
    - CALEA LI
- Ensure implementations handle tunnel traffic (e.g., Protocol 41) correctly.

14.15 Other Requirements

14.15.1 MSO Recommendations Related to Security

14.15.1.1 Miscellaneous Recommendations

- Encourage customers to secure their Wi-Fi.
- MSO does not populate DNS records of customers.
- Deploy host-based antivirus software.
- Encrypt application traffic using TLS or IPSec between the client and the service.
- Update MSOs security systems for IPv4/IPv6 parity.

14.15.1.2 Tunnel Traffic Protection Recommendations

- Tunnels should terminate at security boundaries.
- Operating on-premise tunnel servers/relays so that the tunneled traffic does not cross border routers.
- Setting up internal routing to steer traffic to these servers/relays.

14.15.1.3 CGN Recommendations

- CGN(DS-Lite) needs to be positioned inside firewall.
- General CGN device access controls:
    - Security layers (building, room, server)
    - Multifactor authentication (authenticate admins multiple ways)
    - Separation of duties (requires more than one person to access device)
- Access control to log information:
    - CGN Device Protection to protect access to the logs etc.
    - Encrypt log data.
    - Send syslog events only to authenticated servers over a secure/encrypted link.

15 FEATURES UNDER DEVELOPMENT

This section tracks proposed IPv6 updates to CableLabs specifications. It provides an advanced look at new features, updates, and other enhancements.

15.1 IPv6 Home Networking

- Adding support for IPv6 in DLNA (work in progress).
- Enhancing support for IPv6 in UPnP (work in Progress).