Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 21, 2006

R. Droms
Cisco Systems, Inc.
A. Durand
Comcast Corporation
D. Kharbanda
J-F. Mule
CableLabs

March 20, 2006

DOCSIS 3.0 Requirements for IPv6 support
draft-mule-cablelabs-docsis3-ipv6-00.txt

Status of this Memo

Copyright Notice

Abstract

This document provides an overview of the draft requirements for IPv6 support in the CableLabs DOCSIS 3.0 specifications. Our goal is to share high-level IPv6 requirements and design architecture in draft status with the IETF community.

We first introduce the main network elements involved in the support of IPv6 in DOCSIS cable networks and expand on the deployment scenarios in scope of the DOCSIS 3.0 efforts. We elaborate on the roles played by some network elements in enabling IPv6 in DOCSIS: the broadband access device (Cable Modem), the headend or network side equipment (Cable Modem Termination System) and the various backoffice servers. Some high-level requirements are then summarized with a special focus on three network services: IPv6 provisioning and management of cable modems, IPv6 transport via a DOCSIS network using a cable modem acting as an IPv6 bridge or router, and IP multicast. Finally, we conclude with a theory of operations section to provide more details and sample flows on how an IPv6-capable cable modem acquires its IPv6 address and configuration parameters over a DOCSIS 3.0 network.

CableLabs, its members, the vendors participating in the DOCSIS specifications and the co-authors of this document are seeking general feedback from the IETF community on the overall DOCSIS IPv6 approach. The level of requirements provided in this document may vary; we also welcome feedback on where more details should be provided in future versions.

Table of Contents

1. Overview of DOCSIS 3.0 Networks

This section provides some terminology and background information on cable access networks to the readers who may not be familiar with DOCSIS networks.

The CableLabs(r) DOCSIS(r) project (Data Over Cable Service Interface Specification) defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks. CableLabs has published the DOCSIS 2.0 specification [RFI2.0], and CableLabs is currently developing the DOCSIS 3.0 specification.

In this document, we use the following terminology for a DOCSIS network:

Cable access network or hybrid-fiber/coax (HFC) network: A broadband cable access network that may take the form of either an all-coax or hybrid-fiber/coax (HFC) network. The generic term "cable network" is used here to cover all cases. It is the logical or physical portion of network between a cable modem and a cable modem termination system.

Core data network: The data network operated by a cable service provider to run DOCSIS high-speed data services. It connects the cable modem termination system to the backoffice systems and the rest of the Internet network.

Home network: the network connecting CPEs to the cable modem.

The main elements that participate in a DOCSIS network and the provisioning of DOCSIS services include:

the Cable Modem (CM): The CM connects to the operator's cable network and to a home network, forwarding packets between them. Many devices can be attached to the home network, including standalone devices and devices embedded in the CM.

Customer Premises Equipment (CPE): DOCSIS 3.0 CMs will support CPE devices and hosts that may use IPv4, IPv6 or dual stack IPv4 and IPv6. CMs may provide layer 2 bridging of Ethernet transport, but the details of this function are out of the scope of this document. Examples of typical CPE devices are home routers, VoIP telephony adapters, set-top devices, personal computers, etc.

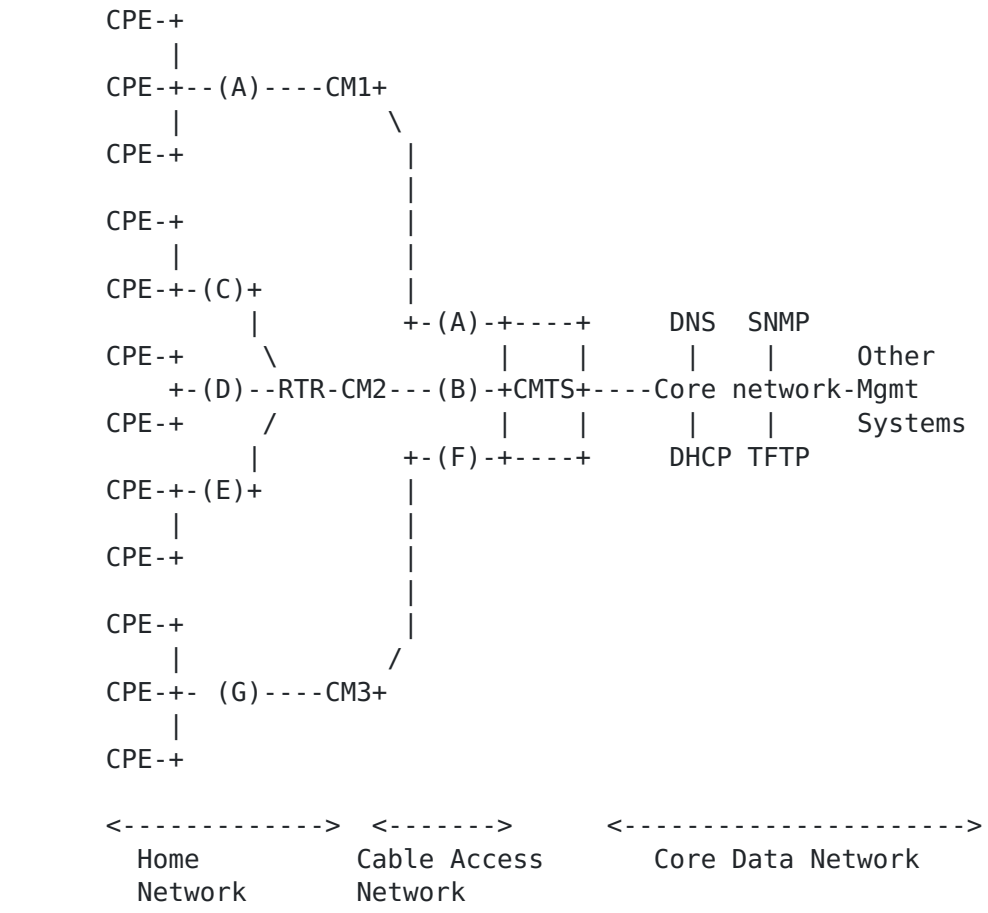
the Cable Modem Termination System (CMTS): The CMTS connects the operator's core data network with the HFC access network. At a high level, the CMTS possesses two interfaces: a Network Side Interface (NSI) connecting the CMTS to the core data network and the RF Interface (RFI) connecting the CMTS to the cable network. Its main function is to forward packets between these two domains, and between upstream and downstream channels on the cable network.

The CMTS may operate as a layer-2 bridging or layer-3 routing device. In either case, there is a "network-side routing function" provided either in the CMTS or by a separate router. The CMTS forwarding capabilities for IPv6 are described in more detail below.

various backoffice configuration services: Various services provide configuration and other support to the devices on the DOCSIS network. These services are implemented in servers connected to the core data network. In a DOCSIS 3.0 network, these servers may use IPv4, IPv6 or both as appropriate to the particular operator's deployment.

The network diagram in Figure 1 shows the various components described about. The figure illustrates three configurations:

- CPEs connected through a bridging CM (CM1)
- a CPE router (RTR) with multiple downstream links connected through a bridging CM (CM2)
- CPEs connected through a routing CM (CM3)



CM1 is a bridging CM
CM2 is a bridging CM, RTR is an external CPE router with multiple
downstream links
CM3 is a routing CM with a single downstream link

Links A, B and F are all bridged by the CMTS.

Customer 2 (CM2) is assigned 2001:DB8:2::/48
Customer 3 (CM3) is assigned 2001:DB8:3::/48

Links A, B and F are assigned 2001:DB8:0:0::/64
Link C is assigned 2001:DB8:2:1::/64
Link D is assigned 2001:DB8:2:2::/64
Link E is assigned 2001:DB8:2:3::/64
Link G is assigned 2001:DB8:3:1::/64

Figure 1: Example DOCSIS 3.0 network.

2. Motivations for IPv6 in DOCSIS 3.0

The primary motivations for enabling IPv6 support in cable operator networks may vary from one cable operator to another and depend on each cable operator's IPv6 adoption strategy.

Some cable operators view IPv6 support in DOCSIS as a critical element for CM provisioning and management to alleviate the IPv4 address space management issues.

Some cable operators view IPv6 support as a stepping stone to provide IPv6 connectivity within the home.

Some believe that the basic CM with IPv6 support should initially be a link-layer bridge while others have expressed support for a CM acting as an IPv6 layer-3 forwarding device with some router functionality.

The main motivations for IPv6 support in DOCSIS 3.0 include:

- to provide CM and CPE operations through IPv6
- to manage IPv6-only CMs, and, dual-stack IPv4 and IPv6 CMs,
- to enable native IPv6 transport over cable access networks with a DOCSIS 3.0 CM acting as a bridge or router for IPv6 traffic.

Interoperability with other DOCSIS versions is a critical requirement to support various deployment scenarios and enable IPv6 migration with a phased approach. For example, a 3.0 CM must operate on an IPv4 DOCSIS 2.0 network and a 3.0 CMTS must be able to support all variants of DOCSIS CMs (3.0 IPv6 CM, 3.0 IPv4 CM, 2.0 IPv4 CM, etc.).

3. Theory of operations

This section describes the process for initial configuration and provisioning of a DOCSIS 3.0 CM using IPv6. The description focuses on the layer 3 provisioning, although it includes some layer 2 provisioning that controls the layer 3 provisioning. This section first highlights some of the important design choices that were made when defining IPv6 requirements for DOCSIS 3.0 cable modems. We then provide sample flows representing IPv6 message exchanges.

DOCSIS 3.0 also defines a process for CM configuration using IPv4. The details of that provisioning process are beyond the scope of this document.

As described in Section 1, a DOCSIS 3.0 CM can operate in either bridging or routing mode. In either case, the CM has a full IP stack that can support local applications and that has an IPv4 address, an IPv6 address or both assigned to an interface on the cable network. The primary use for the local applications is initial configuration, which uses DHCP, TFTP and Network Time protocol, and operational management, which uses SNMP.

A DOCSIS 3.0 CM management IP stack can operate in the following modes: IPv4 only, IPv6 mode, and dual IPv4-IPv6 mode. The operational mode of a CM is independent of the protocols forwarded by the CM to CPEs on the home network; for example, a DOCSIS 3.0 CM provisioned and managed in IPv4 supports bridging of traffic for IPv6 CPEs and vice-versa.

3.1. CM Configuration and Provisioning

During initialization, the CM receives some directives on how to establish its IP connectivity (IP provisioning mode) using a DOCSIS MAC Management Message at layer 2 containing the following information: the CM IP provisioning mode (IPv6 or IPv4), an indicator of whether the CM should enable Alternative Provisioning Mode (APM), and an indicator to enable or disable dual-stack management. APM and dual-stack management will be explained further below.

For backward compatibility reasons, if the CM does not receive a DOCSIS MAC Management Message containing the above parameters from the CMTS, the CM operates as though it is connected to a pre DOCSIS 3.0 network or legacy provisioning system. In this case, the CM performs IPv4 configuration and provisioning in DOCSIS 2.0 mode.

3.1.1. Steps in CM Provisioning

The DOCSIS 3.0 provisioning process includes the following steps:

Layer 2: The CM begins by performing layer 2 provisioning with the CMTS. The details of this provisioning process are beyond the scope of this document. As part of the layer 2 provisioning, the CM receives a message from the CMTS that controls:

* Use of IPv4 or IPv6 for CM provisioning and management

* Dual-stack management

* APM

The remainder of the provisioning process described here will assume the use of IPv6 without dual-stack management and APM. The

use of dual-stack management and APM will be described later.

Acquire IPv6 Connectivity: In this step, the CM acquires a link-local IPv6 address on the cable network and an address of larger scope to be used for the CM management applications.

The CM creates a link-local address, assigns that address to the CM management interface and uses duplicate address detection [RFC2462] to confirm that the link-local address is not already in use on the cable network.

If the CM finds that the link-local address is already in use, the CM restarts its provisioning process and a report is sent to the cable operators error logging system.

The CM then uses Neighbor Discovery (ND) [RFC2461] to locate the CMTS router and other information from a Router Advertisement (RA) message.

DOCSIS 3.0 defines that IPv6 address assignment to the CM uses DHCPv6 [RFC3315], so the 'M' and 'O' flags in the RA are set to cause the CM to initiate DHCPv6.

After receiving the RA, the CM initiates a DHCPv6 message exchange. The DHCPv6 server supplies the IPv6 address for the CM management interface, as well as other configuration information. Section 5 lists the DHCPv6 options used in CM provisioning.

Obtain configuration file: Once the CM has the IPv6 address assigned to its management interface, it uses TFTP (over IPv6) to download a DOCSIS 3.0 configuration file. The name and address of this file are provided through the DHCPv6 message exchange in the previous step.

Set time of day: The CM contacts a Network Time protocol server [RFC0868] to set its internal clock. The address of the Network Time protocol server is provided through DHCPv6.

Complete Registration with CMTS: After the configuration and provisioning steps are completed, the CM completes its registration with the CMTS. The CM authenticates itself to the CMTS and supplies its layer 2 and IPv6 addresses to the CMTS. The CMTS records these addresses for subsequent validation of traffic from the CM

3.1.2. Dual-stack management

To provide higher reliability for CM management through redundancy, a CM can be configured to be managed through SNMP carried over IPv4 or IPv6. In this scenario, after completing the normal configuration process, the CM obtains a second IP address to assign to its management interface. For example, if the CM has been provisioned through IPv6 and is configured to use dual-stack management, the CM uses DHCPv4 to obtain an IPv4 address, which it assigns to its management interface.

3.1.3. Alternative Provisioning Mode (APM)

A CM can be configured to use APM to improve provisioning reliability. When using APM, the CM first uses the primary provisioning protocol (IPv6 or IPv4), as specified by the CMTS. If this provisioning mode fails, the CM then tries to provision itself using the other protocol. For example, if a CM is initially configured to use IPv6 for provisioning and to use APM, if the CM is unable to contact a TFTP server over IPv6, it will restart the provisioning process using IPv4.

3.2. CM Management

Prior to registration with the CMTS, the CM is managed via both IPv4 and IPv6. For data forwarding requirements related to IPv6 prior to CMTS registration, the CM is required to:

- respond to SNMP queries and ICMP Echo packets sent to its diagnostic IP address from the CMCI port(s). The diagnostic CM IP address is a well-known IP address used only for troubleshooting purposes prior to CM registration;

- send all DHCPv4 DHCPDISCOVER or DHCPREQUEST, DHCPv6 Solicit or Request, TFTP or Time Protocol Request, or IPv6 Router Solicitation messages to its RF interface (towards the CMTS) - it must not send any of these requests to any other interface,

- not forward any packets between its RF interface and its CMCI or other any other internal interfaces (embedded eSAFE).

After successful CMTS registration, the CM applies standard packet forwarding rules. Some frame or packet filtering and processing rules may apply based on its configuration file or other requirements (for example, the CM must not forward unicast frames addressed to unknown destination MAC addresses, or, it must not accept any DHCPOFFER, ADVERTISE, etc. from the CMCI interface). The details on the packet forwarding rules are out of scope of this document.

3.3. Motivation for Use of DHCPv6

As DHCPv4 plays a key role in cable modem provisioning in today's network and the cable operator's operations, DHCPv6 is also used in IPv6 mode of operation for the cable modem to acquire its IP address from the MSO backoffice systems.

A DOCSIS 3.0 Cable Modem obtains its IP address via DHCPv6, not stateless address autoconfiguration. This design choice was motivated by several factors:

- the fact that cable networks are operated with highly managed requirements and the knowledge and control of IP address assignments is deemed important

- the importance of minimizing the changes in management and operational models (DHCP is the first gate for access network control, the binding of IPv6 addresses to DNS hostnames is critical in IPv6 and the use of stateful DHCPv6 services to perform this binding is seen by some operators as easier to implement than with SAAC)

- Due to the fact that DNS plays a more important role than in IPv4 (IPv6 addresses are so error prone to type), DHCP servers are perceived as the simplest place to perform dynamic DNS updates in both the forward and reverse DNS tree.

4. High-level IPv6 Requirements for DOCSIS Devices

Based on the deployment scenarios and cable operator motivations for deploying IPv6, the DOCSIS 3.0 specifications address the requirements for CM and CMTS operation described in this section. Some requirements are centered around CM provisioning and management using IPv6 while others are enabling native IPv6 transport for CPEs.

Cable operators have identified the following requirements for IPv6 in DOCSIS 3.0:

- IPv6-only operation

- IPv6 provisioning with dual-stack management

- Fallback from IPv6 to IPv4 provisioning

- Backward compatibility with devices qualified for previous DOCSIS versions

- Control of CM provisioning modes by cable operator
- Provisioning, management and operation of embedded router
- Provisioning and operation of CPE router

4.1. CMTS Requirements for IPv6

The CMTS provides IP connectivity between hosts attached to the cable modems (the hosts attached to the CMs can communicate only via the CMTS) and between the CM and the core data network.

The CMTS can act as a bridge or router: it performs data forwarding in transparent bridging or network-layer forwarding mode, or a combination of the two. The link-layer requirements applicable to CMTS are out of scope of this document.

For IPv6, the CMTS participates in Neighbor Discovery (ND) [RFC2461]. The CMTS must either forward ND packets from one host to the other, or facilitate a proxy ND service, which responds on behalf of other hosts. A proxy ND service on the CMTS also reduces the possibility of potential denial of service attacks because the ND messages are not forwarded to hosts (untrusted entities). The implementation of the proxy ND service is vendor dependent and not specified by the CableLabs specifications.

The CMTS acts as a relay agent for DHCPv6 messages. The CMTS adds specific DHCPv6 relay agent options to pass information about the type and location of CMs and CPEs to the DHCPv6 server(s). The CMTS also receives DHCPv6 relay agent options from the DHCPv6 server regarding the assignment of prefixes and addresses to CPEs.

The network-side routing function generates Router Advertisement (RA) messages [RFC2461]. In the case of a routing CMTS, the RAs are forwarded directly to the cable network. In the case of a bridging CMTS, the network-side routing function is provided b y a separate router, which forwards the RAs to the RFI interface for appropriate forwarding by the bridging CMTS.

When the routing CMTS forwards well-known IPv6 multicast packets from the NSI to RFI, the CMTS terminates and applies appropriate processing.

4.2. Cable Modem Requirements for IPv6 Support

The DOCSIS 3.0 CM must support operations in IPv4, IPv6, or both IPv4 and IPv6 including:

- Device provisioning for the CM through IPv6 or IPv4. The choice of provisioning mode is controlled by the cable operator through the CMTS. A mode is also defined when provisioning will fall back from one IP version to the other in case of failure. This behavior is required to support a variety of operating environments and failure conditions.

- IPv6 address assignment through DHCPv6 [RFC3315]; Section 3gives some of the reasons that led to this choice and how it compares with today's IPv4 address assignment mechanism through DHCP.

- Element management through IPv6, IPv4, or dual-stack IPv4 and IPv6. The mode of element mode management is controlled by the cable operator through the CMTS.

- Data forwarding of IPv4 and IPv6 traffic from and to CPE through the CM regardless of how the modem is provisioned for the cable operator's management purposes.

4.3. Embedded IPv6 Router Requirements

A DOCSIS 3.0 CM integrated device may include an embedded IPv6 router. This section highlights some of the critical requirements an embedded DOCSIS IPv6 router must support.

For IP-level requirements (IPv6 Routing, Forwarding, Multicast, etc.), the embedded router must:

- support Neighbor Discovery and Router Solicitation queries from IPv6 CPE hosts

- forward IPv6 packets to multiple stand-alone IPv6 CPE Routers for a single global IPv6 prefix

- support propagation of other configuration information such as the addresses of DNS servers

- support Multicast Listener Discovery (MLD) proxy for MLDv1 and MLDv2

For Provisioning and Management, the embedded router must:

- implement a DHCPv6 client to acquire Prefix from the cable operator's network and obtain its global-scope IPv6 management address(es)

- support IPv6 Stateless Autonomous Auto-Configuration (SAAC) for CPE hosts

- implement a DHCPv6 Server with IPv6 Prefix Delegation to CPE hosts

- support router configuration via TFTP and other optional protocols (like HTTPS)

- support SNMPv3 and IPv6 MIBs including the IETF Host and Router MIB modules along with the ability to enable or disable the IPv6 router functionality

The QoS requirements are being defined and are left out of scope for now. They will be added in a future revision of this I-D.

4.4. IPv6 Multicast Support

DOCSIS 3.0 provides enhanced support for IP Multicast with the addition of several new capabilities. The main features in-scope of this document include support for Source Specific Multicast (SSM) [ID-SSM-ARCH] (forwarding of SSM traffic for MLDv2) and IPv6 multicast transport (multicast traffic including Neighbor Discovery (ND), Router Solicitation (RS), etc.).

DOCSIS 3.0 supports both the traditional form of IP Multicast, Any Source Multicast (ASM) [RFC1112], as well as Source Specific Multicast (SSM) which is particularly relevant for broadcast-type IP multicast applications. MLDv2 for IPv6 [RFC3810] is required for SSM.

The membership reports are passed transparently by the CM towards the CMTS. The CMTS operates as an MLD querier, and as an IPv6 multicast router for a routing CMTS or listener (snooping switch) for a bridging CMTS. In IPv6 multicast, both the "Any Source Multicast" (ASM) and the "Source Specific Multicast" models are supported.

Specific requirements exist on the CM and CMTS to properly handle IPv6 multicast. For example, in order to successfully obtain its IP address and register with the CMTS, the CM needs to receive certain multicast packets such as those used for DHCPv6, router discovery and duplicate address detection. Another example of IPv6 multicast requirements is that a CMTS MUST forward downstream IPv6 multicast traffic to CPE devices joined through MLDv2. Also, the CM must forward IPv6 registration multicast traffic for CPEs behind the CM.

More details on IPv6 multicast support may be provided in future versions of this document. Other multicast capabilities are included in DOCSIS 3.0 but they are out of scope of this document.

5. DOCSIS 3.0 DHCPv6 Requirements

This section lists the main IETF DHCPv6 client and relay agent DHCP options used for CM IPv6 provisioning. It provides more details on how DHCPv6 is used to acquire configuration parameters.

DHCPv6 Client options include:

Published IETF RFCs: as defined in [RFC3315] and [RFC3633]
- Client Identifier option (DUID)
- IPv6 address assignment (IA_NA, IA_TA)
- Prefix assignment (IA_PD)
- Rapid commit
- Reconfigure accept
- Option request

Current IETF Internet-Drafts (in DHC wg):
- RFC 868 Time Protocol servers
- Time offset

CableLabs vendor specific options:
- These sub-option parameters are defined as part of the DHCPv6 Vendor-specific Information option defined in section 22.17 of RFC 3315, under the CableLabs enterprise number:
- DOCSIS version identifier
- CM capabilities
- TFTP servers
- TFTP configuration file name
- syslog servers
- Device ID (MAC address)

The DHCP Relay agent options include:

Published IETF RFCs:
- Interface-ID

Current IETF Internet-Drafts (in DHC wg):
- Subscriber-ID option
- Assignment information

CableLabs vendor specific options:
- CMTS capabilities: additional CMTS capability strings are defined which contains the DOCSIS version of the relay agent.
- CM MAC address

6. Open Issues

This could be a section where we seek more guidance or provide a more direct view on how we have taken some IPv6 requirements.

7. Acknowledgments

This document is based on the work of a large number of people and contributors participating in the CableLabs DOCSIS project. The authors would like to recognize and thank the following for their assistance and contributions:

Jason Combs and John Brzozowski of Comcast, Ron da Silva and Chris Williams of Time Warner Cable, Victor Blake of Advance New House, Kirk Erichsen of Adelphia, Ben Bekele of Cox Communications, Doc R. Evans and Dan Torbet of Arris, Margo Dolas and Cliff Danielson of Broadcom, Amol Bhagwat of CableLabs, Diego Mazzola of TI and Madhu Sudan of Cisco.

8. Security Considerations

None.

9. Normative References

[RFC0868] Postel, J. and K. Harrenstien, "Time Protocol", STD 26, RFC 868, May 1983.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

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

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

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

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

[RFI2.0]   CableLabs, "CableLabs Data-Over-Cable Service Interface Specifications: Radio Frequency Interface Specification SP-RFI2.0-I09-050812", December 2005.

Authors' Addresses

Ralph Droms
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
USA

Phone: +1 978 936 1674
Email: rdroms@cisco.com

Alain Durand
Comcast Corporation
1500 Market Street
Philadelphia, PA 09102
USA

Email: alain_durand@cable.comcast.com

Deepak Kharbanda
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: d.kharbanda@cablelabs.com

Jean-Francois Mule
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: jfm@cablelabs.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).