IPv6 for Cable Service Providers

Farhan Hamid

Cisco Systems

November, 2012

Agenda

- IPv6 motivation
- DOCSIS IPv6 migration strategies
- IPv6 in DOCSIS
  - CMTS and cable modem requirements
  - Multicast in DOCSIS
  - IPv6 provisioning for cable modem management
  - IPv6 provisioning for a CPE behind a bridging CM
  - IPv6 provisioning for an eRouter
  - IPv6 prefix delegation & prefix stability
- Questions

IPv6 motivation & Challenges

IPv6 Motivation for Cable MSOs

- Convergence of multiple services over IP is driving the addressing need for large scale
  - MSO infrastructure
  - Home/SMB networks
- CM management IPv4 address space depletion:
  - Most MSOs has been using RFC1918 private addressing for CM/STB/eMTA management
  - Even though rare, global IPv4 address was used by “some” MSOs for device management
  - Address space depletion is an issue in both the cases
- CPE IPv4 address space depletion:
  - At a ceremony held on 3 February, 2011 IANA allocated the remaining last five /8s of IPv4 address space to the Regional Internet Registries (RIRs)
  - Some MSOs may have enough addressing space available to hand out IPv4 to the subscriber for next few years, but others face an imminent shortage
- Demand from subscribers to provide IPv6 addresses and prefixes
  - The number of subscribers requesting V6 addresses may be marginal since there are no explicit benefits/incentives for them to use V6 addressing instead v4

MSO IPv6 Strategy

- Deploy IPv6 initially for management and operation of the customer devices controlled by the MSO
  - DOCSIS CM
  - Set top boxes, Packetcable MTA
- Be ready to offer customers services that take advantage of IPv6
- Architecture: Dual stack at the core, v6 at the edges for new devices
- Deployment approach: from core to the edges

  Backbone -> regional networks -> CMTS -> Devices
- MSOs would like to keep the same operational model as IPv4 (backend servers etc.)

Main IPv6 Transition Methods

- **Native Dual Stack**
  - Network stack that supports both IPv4 and IPv6
  - Widely preferred method
- **NAT 444 (“Double NAT”)**
  - Allows single IPv4 address to be shared by multiple subscribers
- **Dual-Stack Lite**
  - Tunnels IPv4 service over IPv6 network to Carrier Grade NAT
- **IPv6 Rapid Deployment (6RD)**
  - Tunnels IPv6 service over IPv4 network
- **6to4 (Tunnel Broker/Teredo)**
  - Automatic tunneling methods for IPv6 service over IPv4 network

Cable's Major IPv6 Transition Challenges

- IPv6 not backwards compatible with IPv4; can't just move IPv4 subscribers over to IPv6 networks
- Many older cable modems, set-tops, routers, TVs DVRs etc. and various other industry devices still don't support IPv6
- OSS systems must be upgraded
- Provisioning systems must be updated for DHCP distribution of large blocks of addresses
- Relatively little Web, video and gaming content is available in IPv6 format
- Poor customer awareness of incompatibility problems
- Cable operators must still support both IP protocols for indeterminate period of time
- Incorporating IPv6 upgrades into overall network upgrades
- Scaling IPv6 traffic at right pace

IPv6 & DOCSIS

Native IPv6 support pre-requisites

- Dual stack support configured in the MSO IP core
- IPv6 support by OSS / NMS systems
  - ➢CM/CPE Provisioning servers should support DHCPv6
  - ➢Network management systems should support device polling using IPv6
  - ➢Billing systems may need to be updated to support IPv6 CM/CPE addressing
- Dual stack support configured on the CMTS
- Deployment of DOCSIS 3.0 compliant CMs or DOCSIS 2.0 plus modems with IPv6 firmware
- IPv6 address assignment schemes for both residential and business subscribers

CMTS Requirements for IPv6

- CMTS a router
  - ➢Provides IP connectivity between hosts attached to CMs and the core data network
- Acts as a relay agent for DHCPv6 messages
  - ➢Inserts some options in the request. Receives some options in the response
- Participates in Neighbor Discovery (ND)
  - ➢Forward ND packets from one host to other
  - ➢Optionally implement an ND proxy service
- Generates RA messages towards the cable network (RF side)
- Multicast: ASM, SSM, Forwarding IPv6 control traffic (ND, RA etc.)
- Backward compatibility with CMs running previous versions of DOCSIS

CM (bridge) requirements for IPv6

- Address assignment through DHCPv6
- Support APM and dual stack mode
- Management via SNMP over IPv4 or IPv6 or dual stack IPv4 and IPv6
- Allow data IPv4 and IPv6 data forwarding from CPEs, regardless of how the CM is provisioned
- Support MLDv1 and MLDv2 for multicast

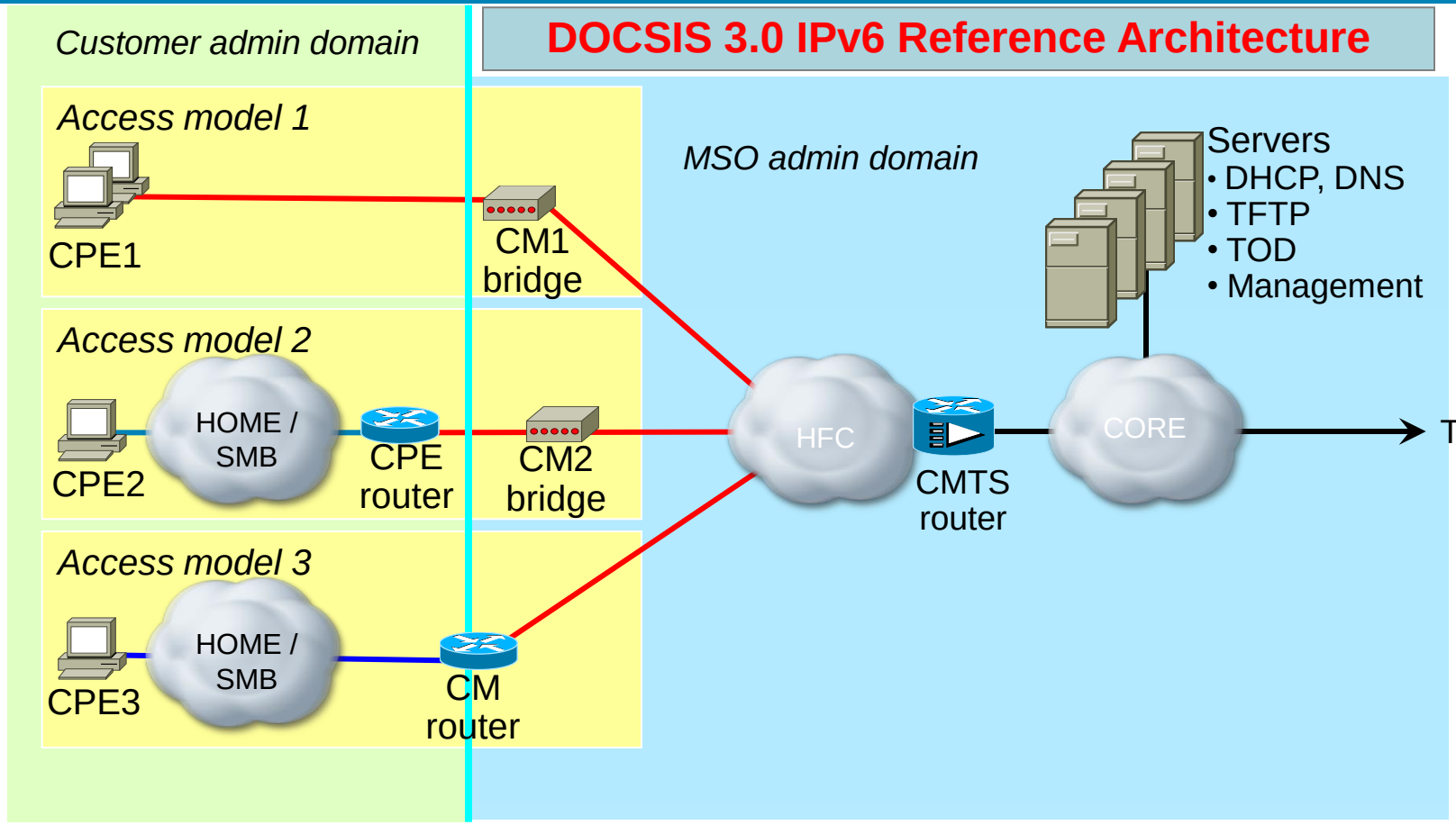
Embedded IPv6 (CM) Router requirements

- Implement DHCPv6 client for acquiring IPv6 prefix (Prefix delegation)
- Support SLAAC for CPE hosts
- Implement DHCPv6 server to support PD or address assignments to CPE hosts
- Support ND and RS queries from home CPE devices
- Support propagation of config information (DNS servers etc.) to home CPE devices

IPv6 Addressing in DOCSIS 3.0

- Customer will have premises network, not individual CPEs on HFC
  - "Lightweight router" function to be defined as eSAFE function
  - Customer will be assigned /48 prefix for sub-delegation within premises network
- CM can be provisioned and managed exclusively through IPv6
  - Relieves pressure on IPv4 address space
  - Customer can still receive IPv4 service (dual-stack network)
- DHCPv6 used for address assignment to meet MSO requirement for IPv6 address control
- Fields, options and sub-options from DHCPv4 redefined as vendor-specific options in DHCPv6

DOCSIS 3.0 IPv6 Reference Architecture



Management prefix: 2001:DB8:FFFF:0::/64
Service prefix: 2001:DB8:FFFE:0::/64
Customer 2 prefix: 2001:DB8:2::/48
Customer 3 prefix: 2001:DB8:3::/48

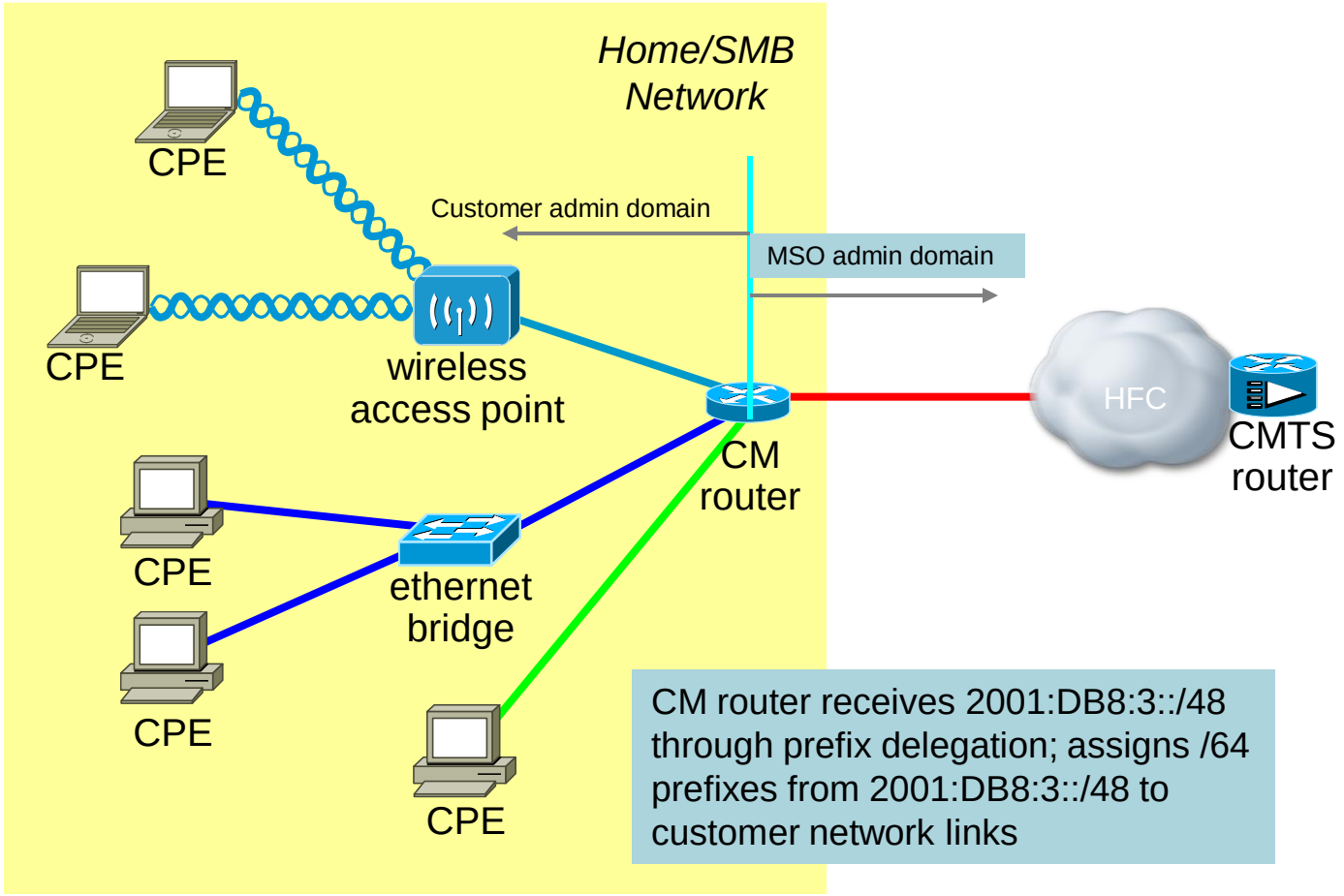
HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt) and 2001:DB8:FFFE:0::/64 (service)

Customer 2 premises link; assigned 2001:DB8:2:1::/64

Customer 3 premises link; assigned 2001:DB8:3:1::/64

Routers span customer and MSO administrative domains

DOCSIS 3.0 IPv6 Reference Architecture :Customer Premises Network



HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt) and 2001:DB8:FFFE:0::/64 (service)

Customer 3 premises link 0; assigned 2001:DB8:3:0::/64

Customer 3 premises link 1; assigned 2001:DB8:3:1::/64

Customer 3 premises link 2; assigned 2001:DB8:3:2::/64

Multicast in DOCSIS

DOCSIS 3.0 Multicast Architecture

- No IGMP snooping in the CM
- CMTS has complete control of multicast forwarding in the CM
  - Multicast filtering and replication within the CM (Based on DSIDs)
  - GMAC promiscuous operation (MDF = 2)
- DSID label used to identify a replication of a multicast stream
- Pre-registration DSID communicated in MDD message
- Static DSID(s) communicated in REG-RSP message
- Dynamic DSID(s) communicated in Dynamic Bonding Change (DBC) messages
- Two main classes of multicast traffic
  - Traffic associated with well-known IPv6 groups
  - User-joined multicast (joined using IGMP or MLD protocols)

Multicast DSID forwarding (MDF)

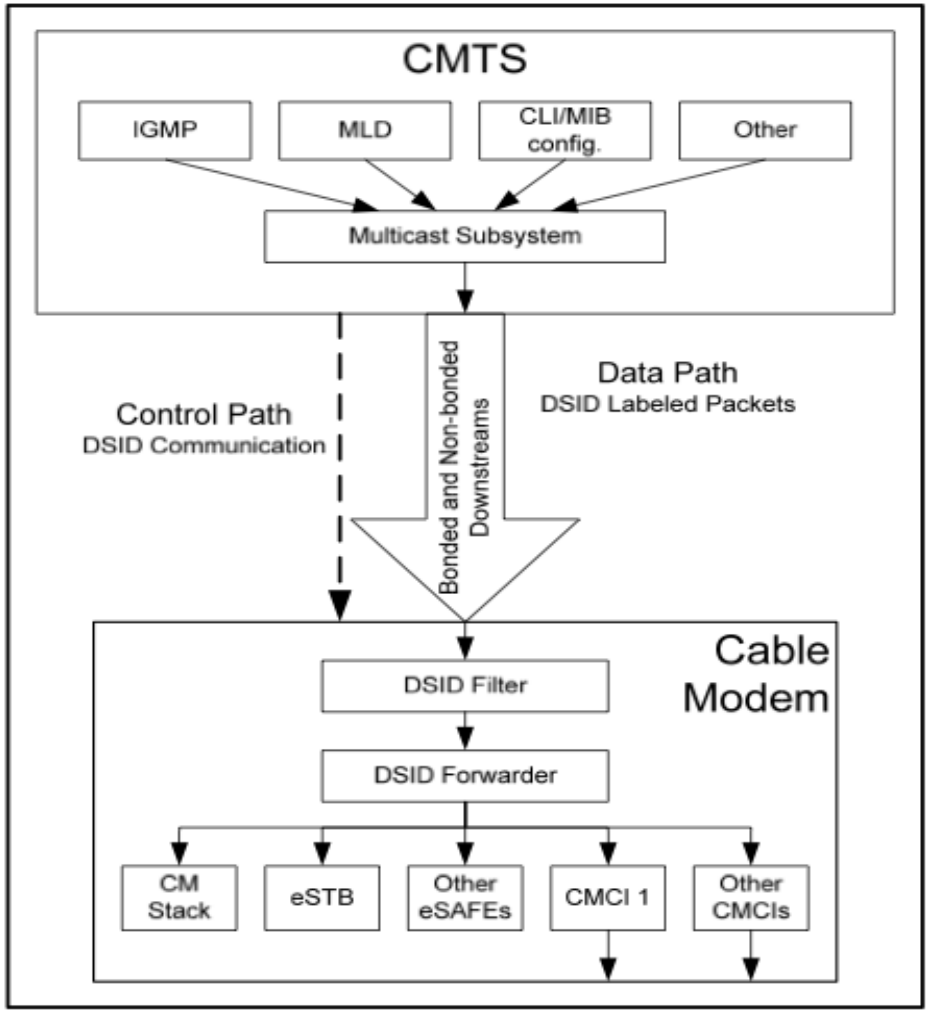


Figure 9–2 - Multicast Model

Operation when in MDF disabled mode

- MDF disabled mode (MDF = 0)

  Processes well-known IPv6 multicast addresses (D3.0 MULPI - Appendix A)

Table A–1 - Well-known IPv6 Addresses

Well-known IPv6 MAC Addresses	Well-known IPv6 Addresses	Description
33-33-00-01-00-02	FF02::1:2	All DHCP relay agents and servers
33-33-00-01-00-03	FF05::1:3	All DHCP servers
33-33-FF-xx-xx-xx	FF02:0:0:0:0:1:FFxx:xxxx	Link-local scope solicited node multicast address
33-33-00-00-00-02	FF02::2	Link-local scope all routers multicast address
33-33-00-00-00-01	FF02::1	Link-local scope all nodes multicast address

  Solicited Node multicast MAC corresponding to all unicast IPv6 addresses assigned for CM host stack

  Solicited Node multicast MAC corresponding to all unicast IPv6 addresses assigned for eSAFE host stacks

  Does not know Solicited Node multicast MAC addresses of connected CPEs; unless learned via snooping

  Mechanism for multicast forwarding of CPE IPv6 traffic is vendor proprietary

Operation when in MDF explicit mode

- MDF explicit mode (MDF = 1)
  - Used by “Hybrid” D2.0 + IPv6 cable modems
  - Forwards DSID labeled packets according to forwarding rules associated with the DSID
  - CMTS includes the GMAC (Group MAC) encoding when signaling a DSID to a CM
  - MDF explicit CM forwards downstream multicast packets with a known DSID AND a known GMAC
  - Multicast packets without a DSID label are discarded
  - Multicast packets with an unknown DSID label are discarded
  - Multicast packets with an unknown GMAC are discarded
  - Pre-Registration DSID (TLV 5.2) utilized
- CMTS may disable MDF for a modem capable of MDF explicit by setting the MDF value to “0” in the Registration Response message. This triggers the modem to revert to IGMPv2 snooping to process multicast traffic, hence IPv6 traffic CANNOT be forwarded to CPE interfaces.

Operation when in MDF promiscuous mode

- MDF promiscuous mode (MDF = 2)
  - Used by DOCSIS 3.0 CMTS AND DOCSIS 3.0 cable modems
  - CM has the ability to “promiscuously” accept and forward all GMAC addresses with known DSID labels
  - Pre-Registration DSID (TLV 5.2) utilized
  - Multicast packets without a DSID label are discarded
  - Multicast packets with an unknown DSID label are discarded
  - Filtering and forwarding based solely on DSID label; CM does not perform filtering based on GMAC address

IPv6 provisioning for cable modem management

CM provisioning

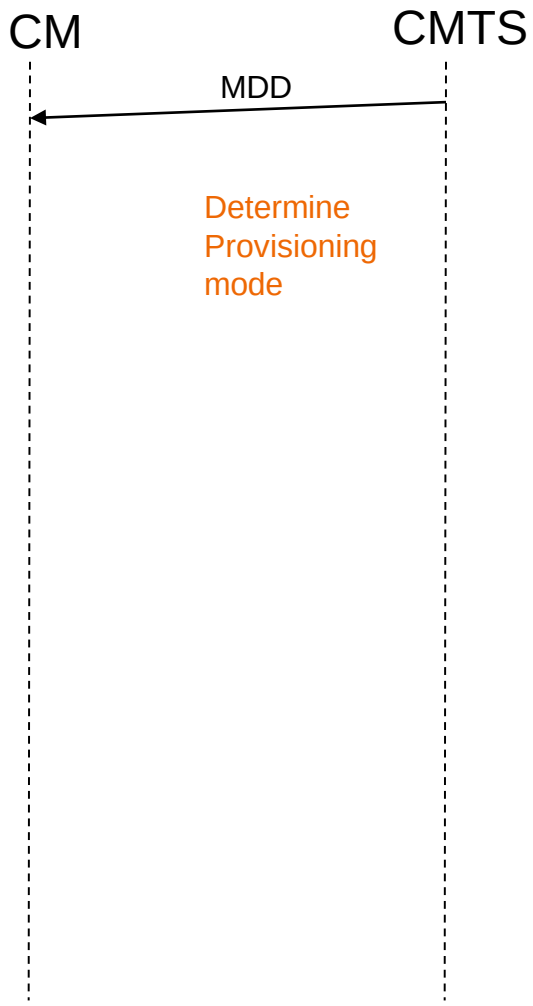
- Layer 2 provisioning
- Acquire IPv6 connectivity
- Obtain time of day
- Obtain configuration file
- Complete registration

CM provisioning

- CMTS sends a MDD message to the CM that controls the IP establishment procedure used by the CM

Type	Length	Value
5.1	1	IP Provisioning Mode (see Section 10.2.5): 0 = IPv4 Only 1 = IPv6 Only 2 = Alternate (APM) 3 = Dual-stack (DPM 4 – 255 = Reserved The CMTS MUST include this sub-TLV. The CM uses this sub-TLV as defined in Section 10.2.5.

- It can be overridden by MIB in CM configuration file; covered in detail in an upcoming slide
- If the CM does not receive any MDD messages from the CMTS it operates in DOCSIS 2.0 mode



Dual Stack Management

- CM first uses DHCPv6 to acquire an IPv6 address and then uses DHCPv4 to acquire an IPv4 addresses
- If able to acquire an IPv6 address it continues the provisioning process using IPv6; otherwise it continues the provisioning process using IPv4
- Allows the MSOs to manage the CMs using SNMP carried over IPv4 or IPv6
  - ➢Useful during the transition period until confidence is gained in IPv6 management infrastructure

CM Provisioning:
Acquire IP connectivity

- DHCPv6 used for address configuration
  - Stateless auto configuration NOT used
  - M and O bits set in RAs from the CMTS
- MSOs want to have the knowledge and want to control IP address assignments
- MSOs used to DHCP. Minimizes changes in operational models
- Dynamic DNS updates can be done at the DHCP servers
  (instead of relying on CPEs and CMs)

IPv6 address acquisition
Link global address in CPE

- SLAAC cannot be used for acquiring link global IPv6 address by eCM or eRouter or bridged CPE.
- DHCPv6 is the only dynamic solution per MULPI spec.

5.2.5.2 Initialization, Provisioning and Management of CPEs

DOCSIS assumes the use of DHCP for provisioning of CPE devices. To that end the CMTS supports a DHCP relay agent which allows the operator to associate a CPE IP Address request with the subscriber Cable Modem MAC Address. This feature is also used as the basis of a mechanism that prevents spoofing of IP Addresses.

Appendix VII Notes on Address Configuration in DOCSIS 3.0

DOCSIS 3.0 specifies DHCPv6 as the method of choice to provision IPv6 addresses for CM and bridged devices. [RFC 2462] defines an alternate mechanism known as stateless address autoconfiguration, where devices build their own IPv6 address by concatenating a prefix learn through router advertisements (RA) and an interface ID derived from the MAC address. Such addresses are usually not registered within the Cable Operator, so their usage is not recommended in DOCSIS 3.0. The simplest way to prevent CM and bridged devices to use stateless address autoconfiguration is to configure router advertisement to not include any prefixes at all.

A CMTS can provide support for enforcing a deployment in which devices attached to the HFC use only DHCPv6 addresses by filtering IPv6 traffic and dropping any IPv6 datagrams whose source address has not been assigned through DHCPv6. Note that this filtering will catch manually assigned address as well as unauthorized SLAAC addresses.

Contents of DHCPv6 Solicit

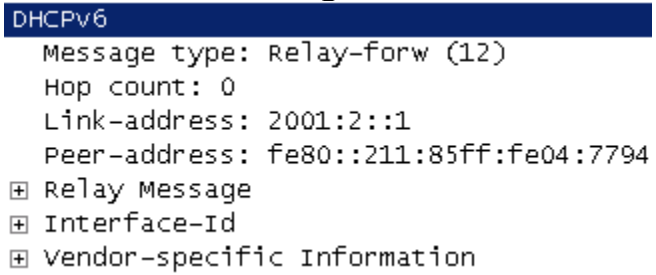
- Client Identifier option containing the DUID (DHCP Unique Identifier) for the CM as specified by RFC 3315
- IA_NA (Identity Association for Non-temporary Address) option
- Vendor Class option “4491” (CableLabs) with the string “docsis3.0”
- Vendor Specific options containing
  - TLV5 option
  - Device ID option containing HFC MAC address
  - ORO option requesting
    - Time Protocol Servers
    - Time Offset
    - TFTP Server Address
    - Configuration File Name
    - SYSLOG Server Address
- Rapid Commit option

IPv6 address acquisition
DHCPv6 in CMTS

- CMTS works as DHCPv6 relay agent

  DHCPv6 server functionality is not supported

- CMTS receives DHCPv6 packets from DOCSIS side (FF02::1:2) and forwards them to the configured DHCPv6 server.



  Link-address: the link where client is located

  Peer-address: address of client (CM, eRouter-WAN or CPE behind bridged CM)

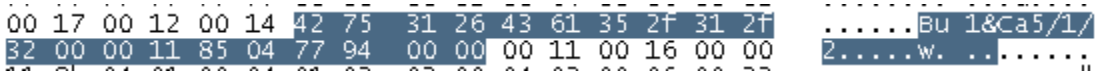
  Relay Message: relayed message (e.g. DHCPv6 SOLICIT)

  Interface-ID: interface where DHCPv6 message was received

  Vendor-specific information (Vendor = CableLabs)

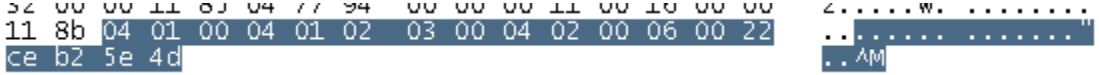
IPv6 address acquisition
DHCPv6 in CMTS contd.

- Interface-ID

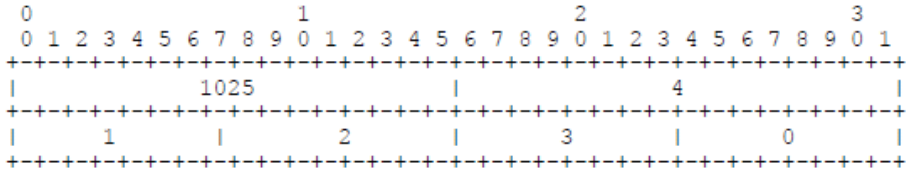


Interface name based syntax followed by CM MAC address

- Vendor (CableLabs) specific information



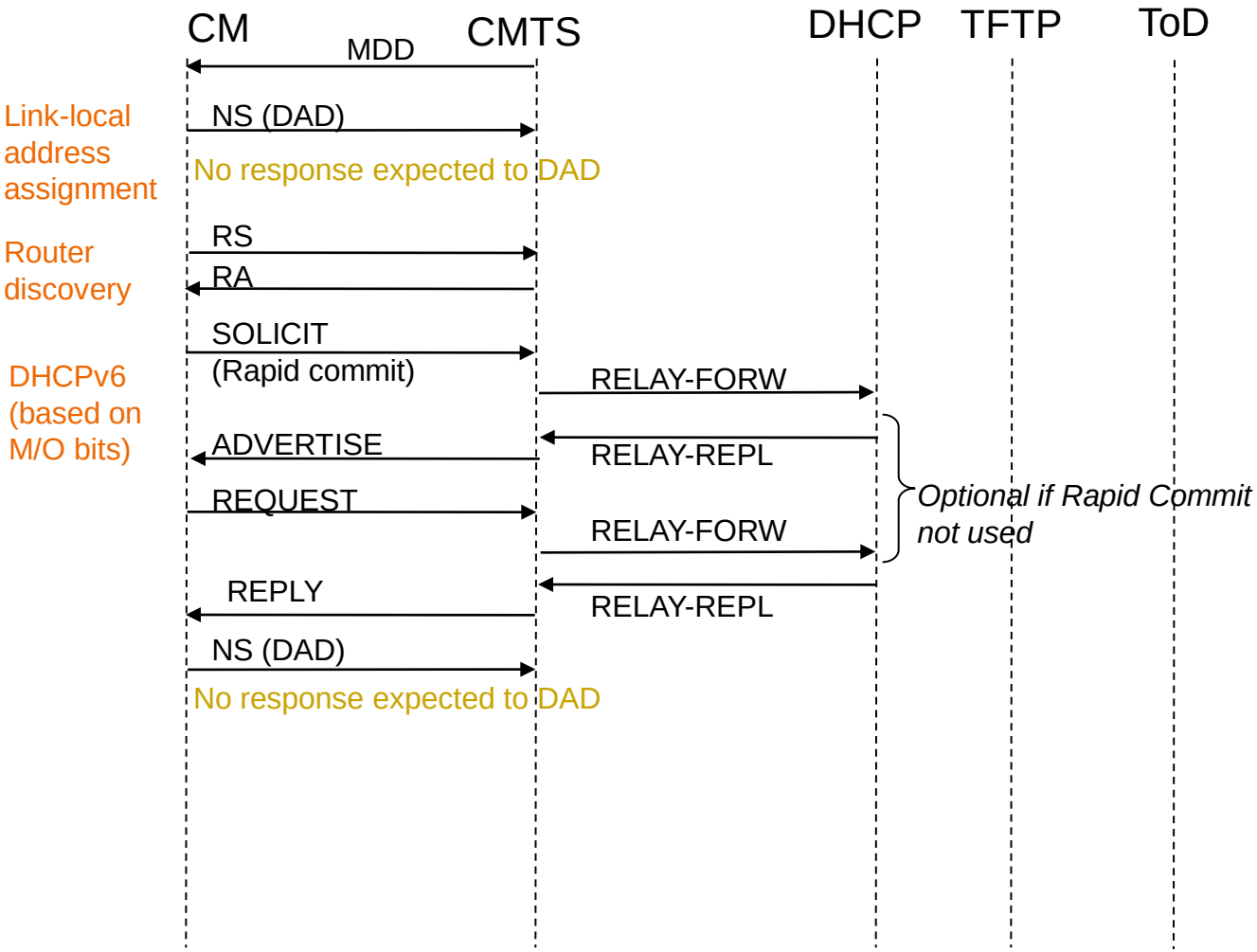
DHCPv6 Relay Agent CMTS capabilities Option (1025) that identifies CMTS as compatible with D3.0 specification.



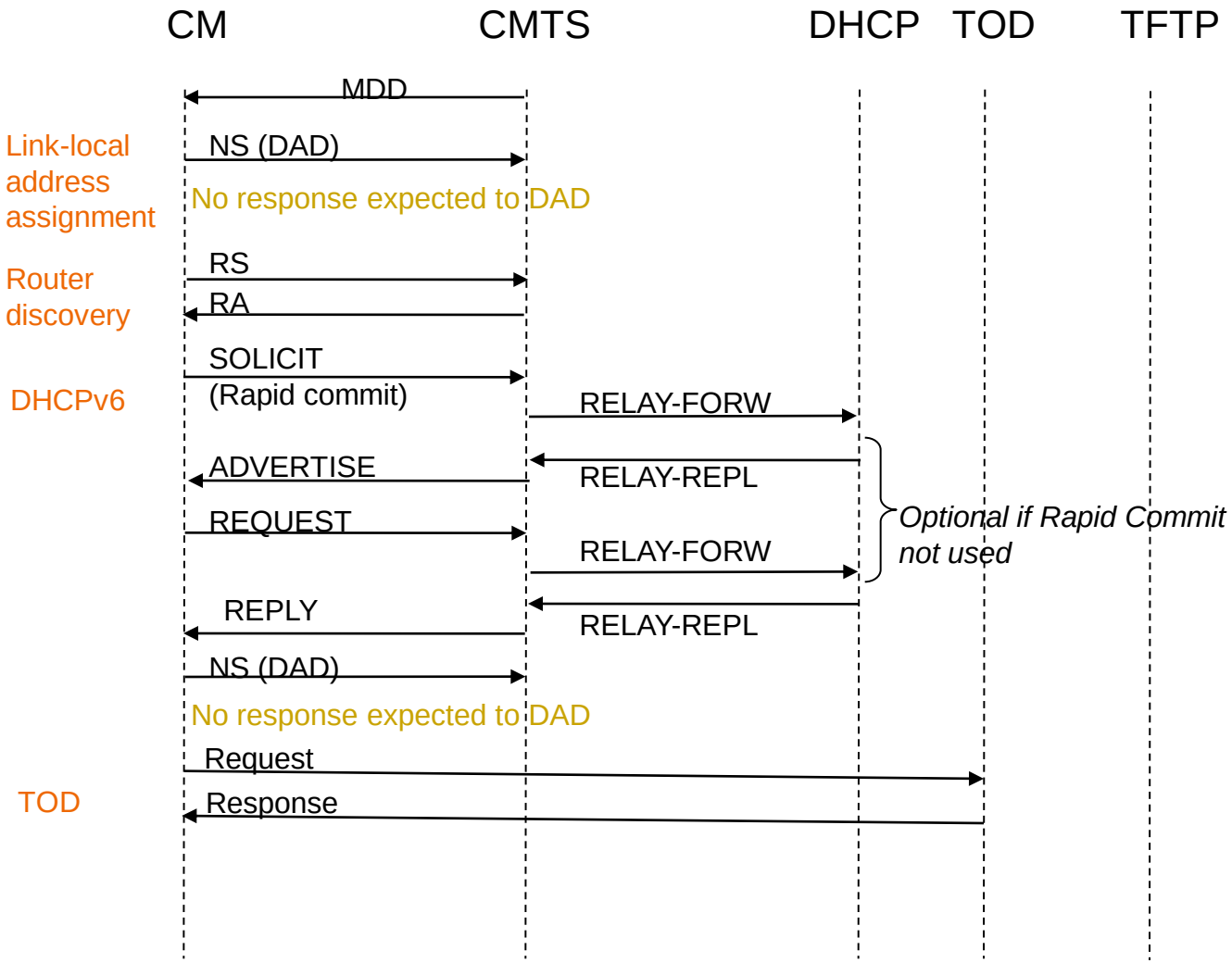
DOCSIS Relay Agent CM MAC address option (1026) that identifies relayed DHCPv6 message sourced by CM IPv6 stack or by device behind CM.

Note: equivalent to Option-82 in DHCPv4

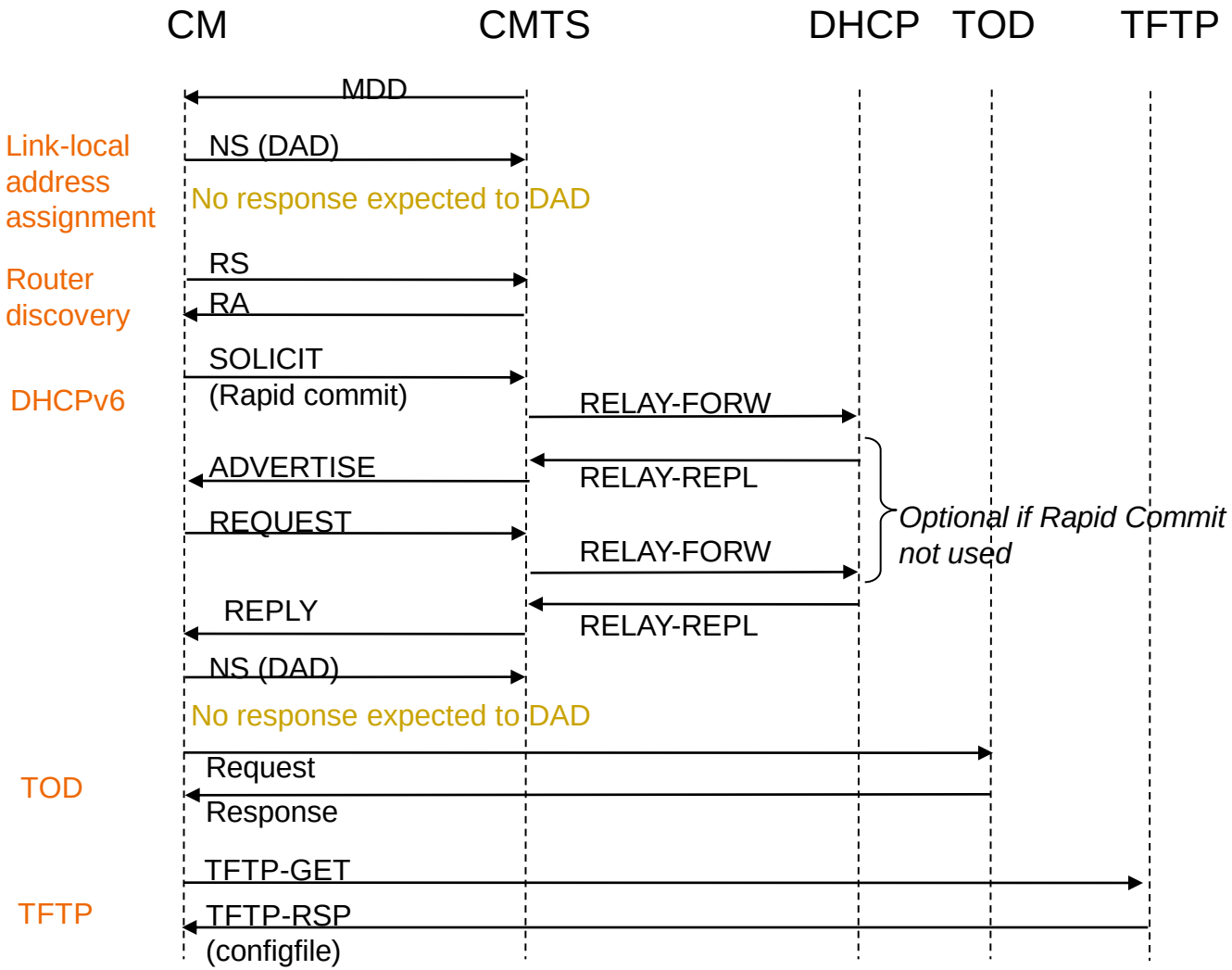
CM Provisioning:
Acquire IP connectivity



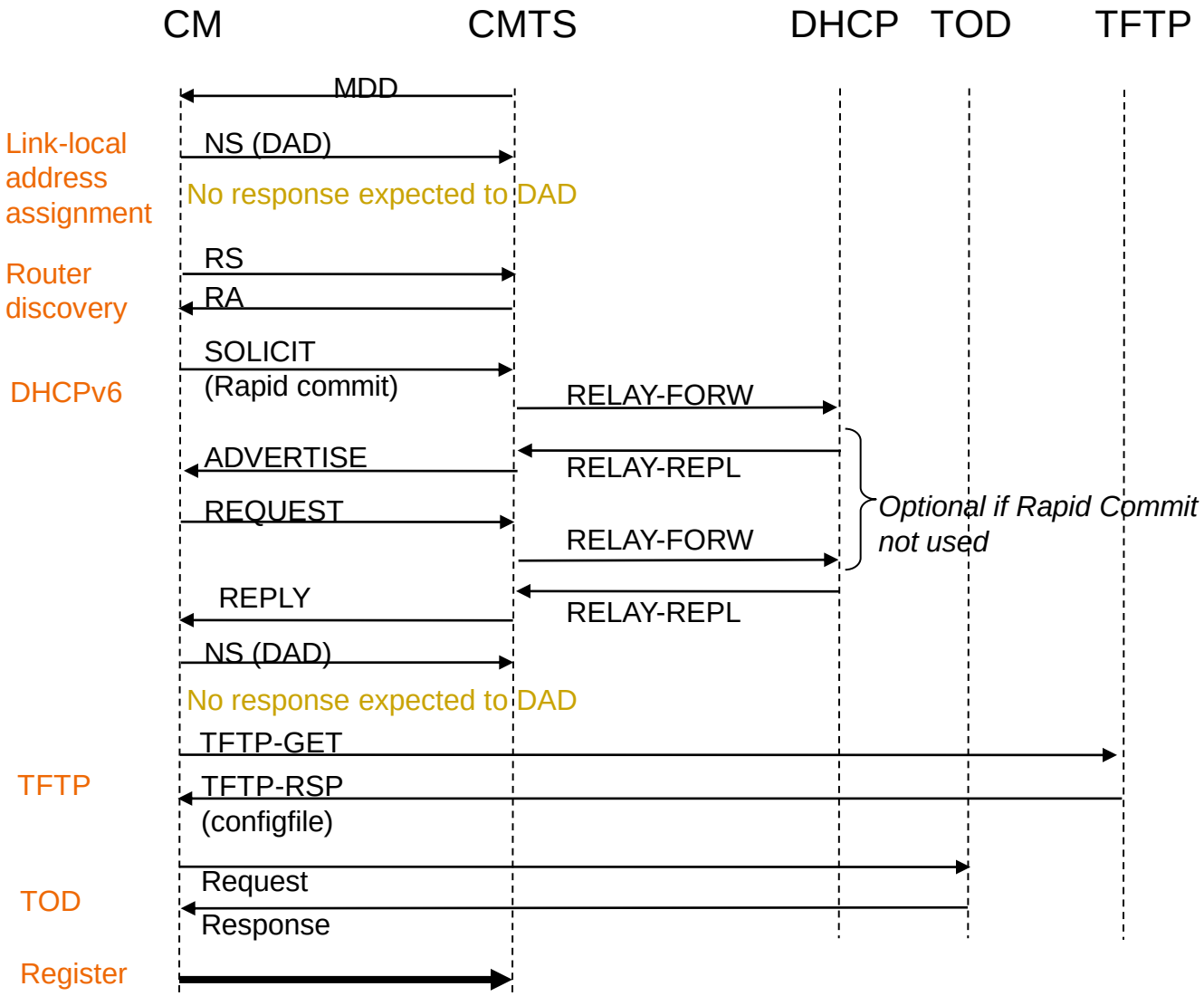
CM Provisioning:
Obtain TOD



CM Provisioning:
Obtain Configuration File



CM Provisioning:
Complete Registration



IPv6 provisioning for a CPE behind a bridging CM

IPv6 CPE provisioning

- DOCSIS CPE will typically have two IPv6 address on CMTS facing RF interface

  Link local IPv6 address generated on CM MAC address

  Link global IPv6 address learned via DHCPv6.

- DAD is always used to check uniqueness of acquired IPv6 address

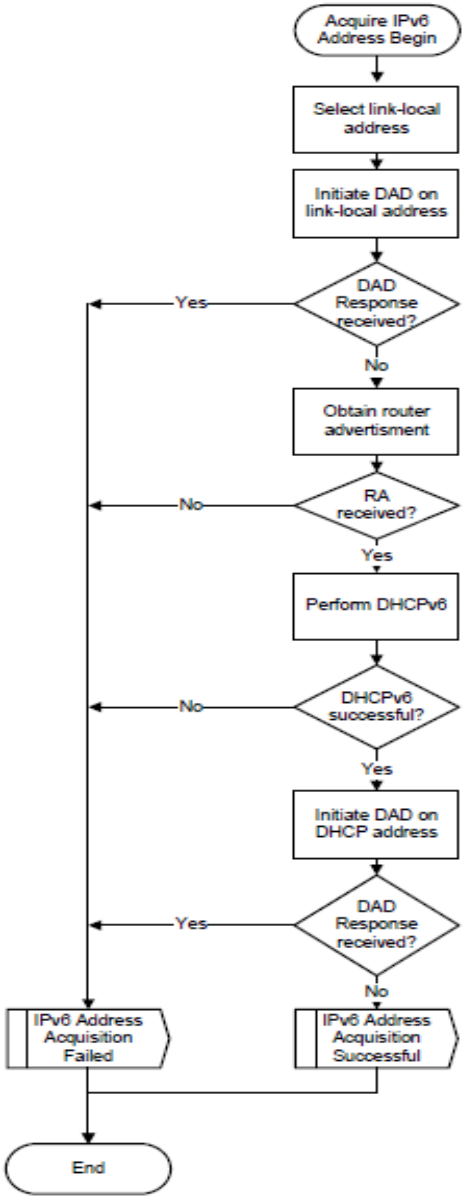


Figure 10–22 - IPv6 Address Acquisition

IPv6 address acquisition
Static IPv6 and SAV

- In case of business customers, static IPv6 addressing may be required
- The CMTS learns about a static IPv6 CPE when the static IPv6 CPE sends any data (including an NS(DAD)) to the CMTS.
- CMTS checks the IPv6 source address using Source Address Verification (SAV) feature

  (1) CM configuration file incl. TLV that identifies the SAV Prefix group name that the CM belongs to. The prefixes in the group itself is configured on the CMTS.

  (2) CM configuration file incl. TLV that provides the actual prefix

  CMTS checks if the source IPv6 address of the static CPE falls within an IPv6 subnet prefix and adds CPE to the ND cache.

IPv6 provisioning for an eRouter

IPv6 in eRouter
CableLabs specification

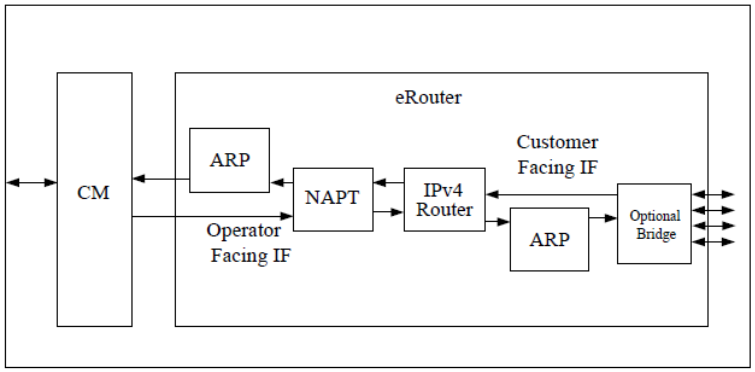


Figure 9-1 - eRouter IPv4 Forwarding Block Diagram

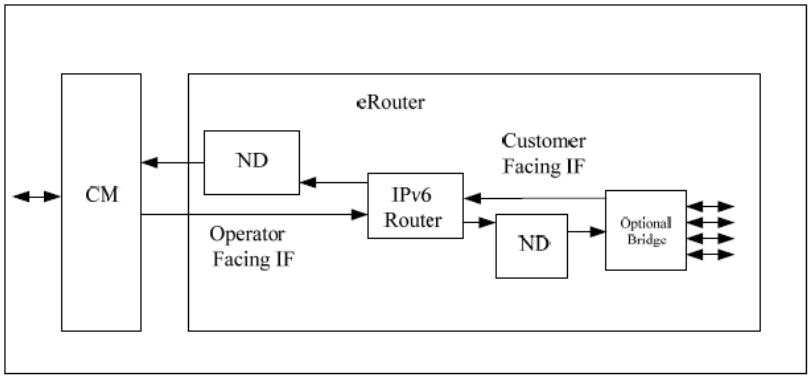


Figure 10-1 - eRouter IPv6 Forwarding Block Diagram

- CableLabs eRouter defines a set of features for both IPv4+IPv6 eRouter
- IPv4
  - IPv4 Router with NAPT and Application Layer Gateways (ALG)
  - IGMPv2/v3 proxy
- IPv6
  - IPv6 routing without NAPT or ALG
  - MLD proxy

IPv6 in eRouter
eRouter mode of provisioning

Table 6-1 - eRouter Modes

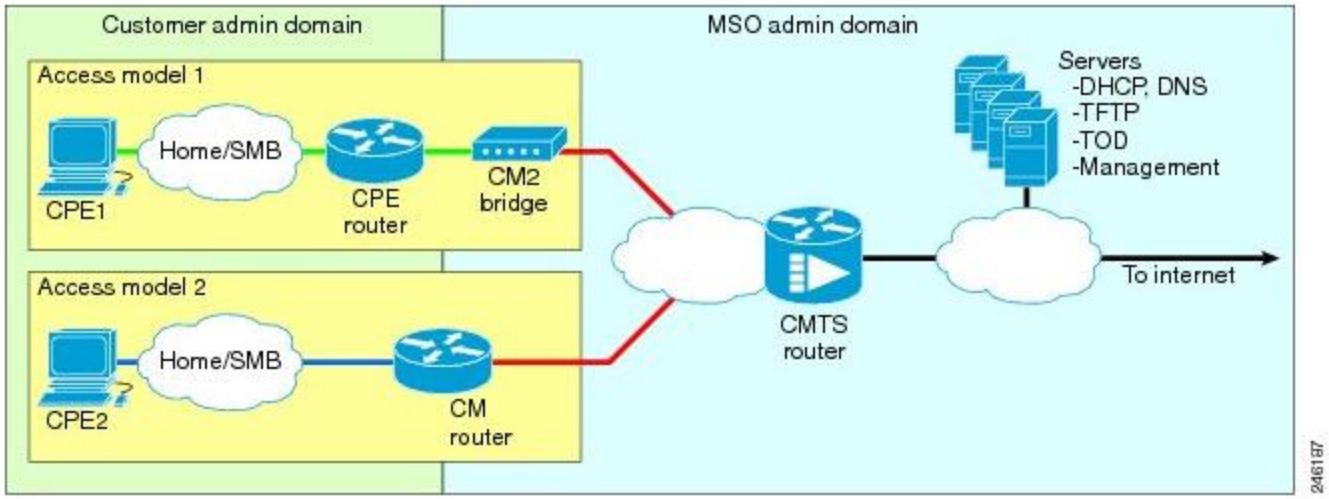
Mode	IPv4	IPv6
Disabled	CM bridges all traffic per MULPI spec.	CM bridges all traffic per MULPI spec.
IPv4 Protocol Enabled	eRouter forwards IPv4 traffic with NAPT.	eRouter does not forward IPv6 traffic.
IPv6 Protocol Enabled	eRouter does not forward IPv4 traffic.	eRouter forwards IPv6 traffic.
Dual IP Protocol Enabled	eRouter forwards IPv4 packets using NAPT.	eRouter forwards IPv6 packets.

- eRouter provisioning mode is controlled via TLV 202 in the CM configuration file; sub-type “1” is for eRouter Initialization and is one byte in length with the following possible values:

Value
0: Disabled
1: IPv4 Protocol Enabled
2: IPv6 Protocol Enabled
3: Dual IP Protocol Enabled
4-255: Invalid

Ex: GenericTLV TlvCode 202 TlvLength 3 TlvValue 0x010103; /* dual IP */

IPv6 address acquisition
IPv6 CPE Router architecture



- IPv6 router acquires the following information from DHCPv6 server
  - WAN interface IPv6 address (IA_NA)
  - IP address space to provision its LAN interfaces (IA_PD)
- IA_PD is routed subnet from CMTS perspective

IPv6 in eRouter

IPv6 provisioning of operator facing interface

After the CM has completed provisioning, if the eRouter is operating in the IPv6 Protocol Enabled Mode or the Dual IP Protocol Enabled Mode, the eRouter MUST use DHCPv6 [RFC 3315] in order to obtain an IP address for its Operator-Facing IP Interface and any other parameters needed to establish IP connectivity, as illustrated in Figure 8-1.

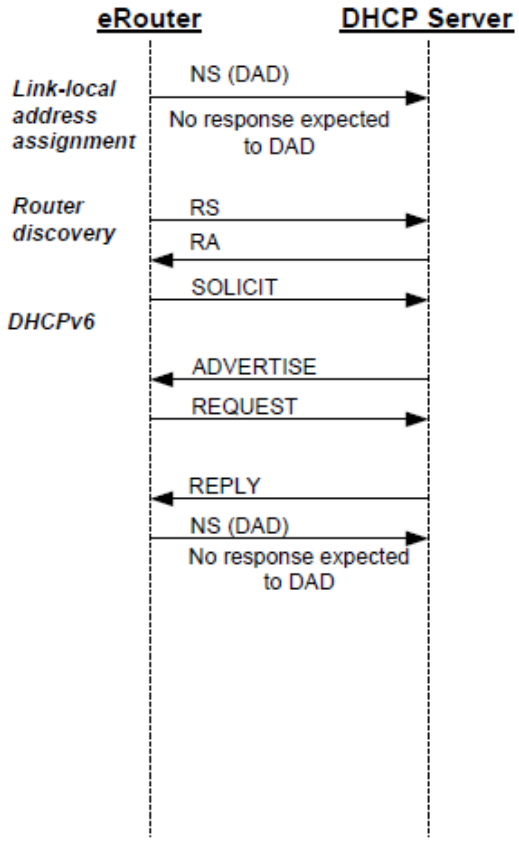


Figure 8-1 - IPv6 Provisioning Message Flow

Link local = FE80:: + EUI-64

DAD to confirm uniqueness (NS/NA)

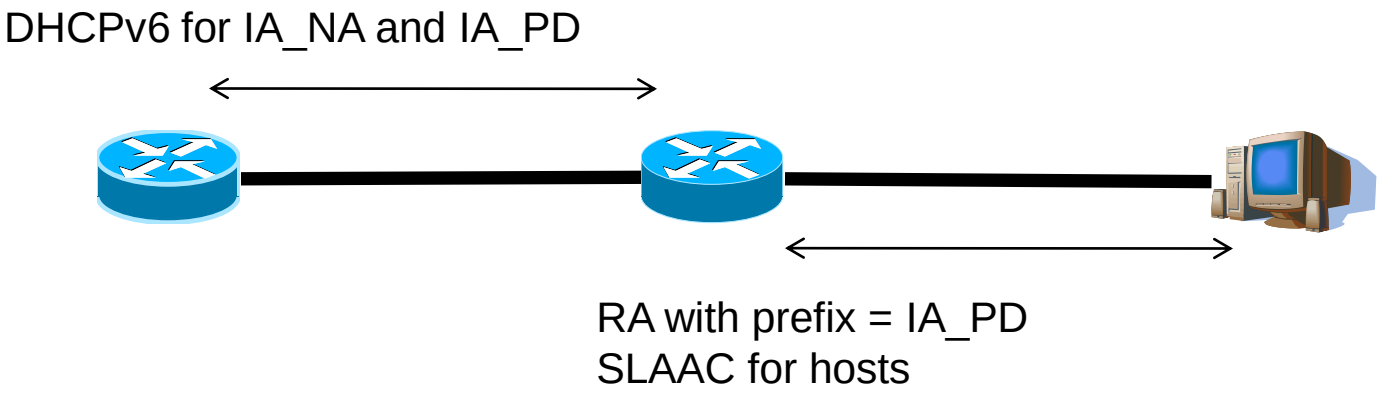
Router discovery (RS/RA)

DHCPv6 incl. PD option and Rapid Commit (MUSTs in Solicit, PD MUST in Advertise/Reply)

DAD to confirm uniqueness of DHCP address

IPv6 in eRouter
Local interfaces and CPEs

- Local interface link-local IPv6 address auto generated (EUI-64)
- eRouter assigns a global IPv6 address to CPE-Facing Interface based on a prefix derived from IA_PD
- eRouter generates RA (M=0, O=1, prefix = IA_PD with A=1)
- CPE will use SLAAC to get IP address
- Per RFC 5006/6106, RA also contains DNS server IP addresses
- DHCPv6 server functionality; either stateful for address assignment or stateless for additional information e.g. DNS



IPv6 prefix delegation & prefix stability

IPv6 Prefix Stability

- An IPv6 CPE router behind the CM is allocated an IPv6 Prefix when the CPE router gets online.
- For business services the MSO would like this Prefix to remain stable even when the CM of the CPE router moves from one CMTS to another.
- A CM can move between two CMTS's in a RF node-split provisioned between the two CMTS's.
- Problem is specific to IPv6 because IPv4 does not support Prefix Delegation. IPv4 instead supports NAT.

D3.0 MULPI Solution

- An IGP such a ISIS operates between the two CMTSs.
- The IGP updates a Prefix add/delete from one CMTS to another.
- The CMTS that receives the IGP update for a Prefix checks if the Prefix belongs to a CM that is offline or online.
- If the CM is online, the Prefix is attached to this CM's CPE.
- If the CM is offline, the Prefix is deleted on the CMTS.
- After CM move, this solution assumes the CPE router will reset and thus the new CMTS gleans the PD and sends a routing update to the old CMTS to purge the PD. Note CNR allocated the same prefix to the CPE router even when the CPE's CM has moved to another CMTS.

Thank you.