IPv6 Technology Overview Tutorial- Part II

(With Cable Emphasis)

Speaker: Byju Pularikkal

Customer Solutions Architect, Cisco Systems Inc.

Acronyms/Abbreviations

- DOCSIS = Data-Over-Cable Service Interface Specification
- CMTS = Cable Modem Termination System
- DS = Downstream
- US = Upstream
- CM = Cable Modem
- IPv6 = Internet Protocol version 6
- ICMPv6 = Internet Control Message Protocol version 6
- DHCPv6 = Dynamic Host Configuration Protocol for IPv6
- MSO = Multiple Services Operator
- SMB = Small Business
- PDA = Personal Digital Assistant
- NAT = Network Address Translation
- CIDR = Classless Interdomain Routing
- DAD = Duplicate Address Detection
- SLA = Subnet Level Address
- VPN = Virtual Private Network
- ARP = Address Resolution Protocol
- eSAFE = Embedded Service/Application Functional Entity
- RS = Router Solicitation
- RA = Router Advertisement
- UDP = User Datagram Protocol
- DUID = DHCP Unique Identifier
- DNS = Domain Name System
- CPE = Customer Premises Equipment
- ND = Neighbor Discovery
- NS = Neighbor Solicitation
- HFC = Hybrid Fiber Coaxial
- EUI = Extended Unique Identifier
- TFTP = Trivial File Transfer Protocol
- ToD = Time of Day
- MDD = Mac Domain Descriptor
- APM = Alternative Provisioning Mode
- SNMP = Simple Network Management Protocol
- ASM = Anysource Multicast
- SSM = Source Specific Multicast
- SLAAC = Stateless Addres Autoconfiguration
- MLD = Multicast Listener Discovery

Tutorial-1: Agenda

- Structure of IPv6 Protocol
  - ➢IPv4 and IPv6 Header Comparison
  - ➢IPv6 Extension Headers
- IPv6 Addressing
  - Addressing Format
  - Types of IPv6 addresses
- ICMPv6 and Neighbor Discovery
  - Router Solicitation & Advertisement
  - Neighbor Solicitation & Advertisement
  - Duplicate Address Detection
- Multicast in IPv6
- DHCP & DNS for IPv6
  - ➢DNS with IPv6
  - ➢DHCPv6 Overview

Tutorial-2: Agenda

- Routing in IPv6
  - RIPng
  - OSPFv3
  - BGP-4 Extensions for IPv6
  - Multi-Topology IS-IS
- Tunneling
  - Automatic 6 to 4 Tunnels
  - ISATAP
- IPv6 for DOCSIS Overview
  - IPv6 Drivers in Broadband Access Networks
  - CMTS & CM Requirements for IPv6
  - MSO CPE Address Assignment Strategies

IPv6 Routing

Routing in IPv6

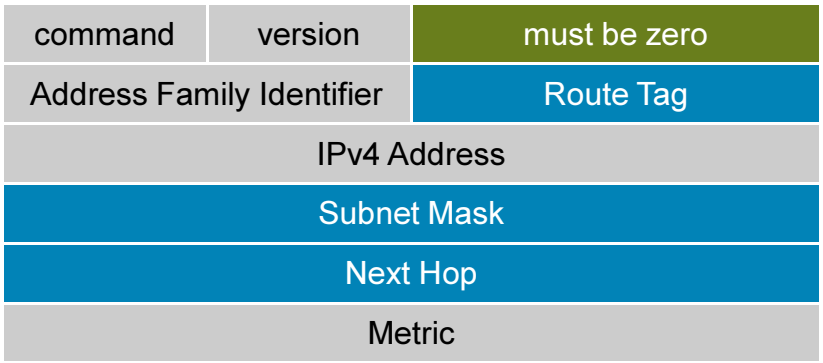
- As in IPv4, IPv6 has 2 families of routing protocols: IGP and EGP, and still uses the longest-prefix match routing algorithm

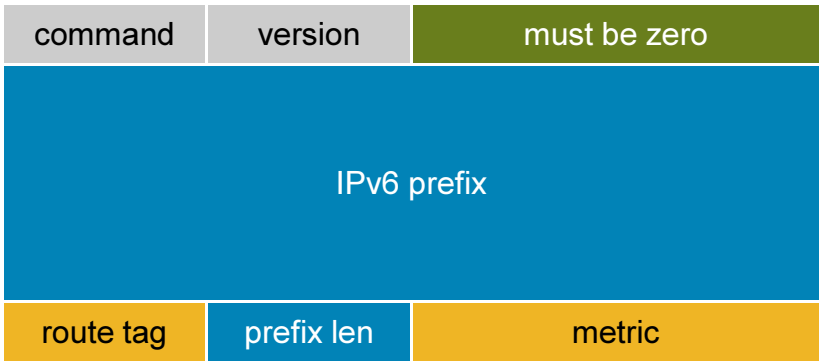
- IGP
  - RIPng (RFC 2080)
  - Integrated IS-ISv6 (draft-ietf-isis-ipv6-07)
  - OSPFv3 (RFC 2740) – (draft-ietf-ospf-ospfv3-update-19)

- EGP :
  - MP-BGP4 (RFC 2858 and RFC 2545)

RIPng (RFC 2080)

Enhanced Routing Protocol Support
RIPng Overview (RFC 2080)





- Similar characteristics as IPv4
  - ➢Distance-vector, hop limit of 15, split-horizon, multicast based (FF02::9), UDP port (521) etc.
- Updated features for IPv6
  - ➢IPv6 prefix & prefix length
- Special Handling for the NH
  - ➢Route tag and prefix length for NH is all 0. Metric will have 0xFF; NH must be link local

OSPFv3 (RFC 2740)

OSPFv3 and OSPFv2 Differences

- Protocol processing per-link, not per-subnet
- Removal of addressing semantics
- Addition of Flooding scope
- Explicit support for multiple instances per link
- Use of IPv6 link-local addresses
- Authentication method changes
- Packet format, LSA's header format changes
- Handling of unknown LSA types

OSPFv3 and OSPFv2 Similarities

packet type	Descrption
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgment

- OSPFv3 has the same 5 packet type but some fields have been changed.
- Mechanisms for neighbor discovery and adjacency formation
- Interface types
  - P2P, P2MP, Broadcast, NBMA, Virtual
- LSA flooding and aging
- Nearly identical LSA types

OSPFv3 and OSPFv2 header comparison

Version	Type	Packet Length
Router ID		
Area ID		
Checksum	Autype	
Authentication		
Authentication		

Version	Type	Packet Length
Router ID		
Area ID		
Checksum	Instance ID	0

- Size of the header is reduced from 24 bytes to 16
- Router ID & Area ID are still a 32 bit numbers
- Instance ID is a new field that is used to have multiple OSPF process' instance per link. In order for 2 instances talk to each other they need to have the same instance ID. By default it is 0 and for any additional instance it is increased, Instance ID has local link significance only
- Authentication fields have been suppressed – RFC 4552 talks about the authentication implementation in OSPFv3

BGP-4 Extensions for IPv6 (RFC 2545)

BGP-4 Extensions for IPv6

- BGP-4 carries only 3 pieces of information which is truly IPv4 specific:
  - NLRI in the UPDATE message contains an IPv4 prefix
  - NEXT_HOP path attribute in the UPDATE message contains a IPv4 address
  - BGP Identifier is in the OPEN message & AGGREGATOR attribute
- To make BGP-4 available for other network layer protocols, RFC 2858 (obsoletes RFC 2283) defines multi-protocol extensions for BGP-4
  - Enables BGP-4 to carry information of other protocols e.g MPLS,IPv6
  - New BGP-4 optional and non-transitive attributes:

    MP_REACH_NLRI

    MP_UNREACH_NLRI
  - Protocol independent NEXT_HOP attribute
  - Protocol independent NLRI attribute

BGP-4 Extensions for IPv6

- New optional and non-transitive BGP attributes:
  - MP_REACH_NLRI (Attribute code: 14)

    "Carry the set of reachable destinations together with the next-hop information to be used for forwarding to these destinations" (RFC2858)
  - MP_UNREACH_NLRI (Attribute code: 15)

    Carry the set of unreachable destinations
- Attribute 14 and 15 contains one or more Triples:
  - Address Family Information (AFI)
  - Next-Hop Information (must be of the same address family)

  NLRI

BGP-4 Extensions for IPv6

- Address Family Information (AFI) for IPv6
  - AFI = 2 (RFC 1700)
  - Sub-AFI = 1 Unicast
  - Sub-AFI = 2 (Mulitcast for RPF check)
  - Sub-AFI = 3 for both Unicast and Mulitcast
  - Sub-AFI = 4 Label
  - Sub-AFI= 128 VPN

BGP-4 Extensions for IPv6

- TCP Interaction
  - BGP-4 runs on top of TCP
  - This connection could be setup either over IPv4 or IPv6
- Router ID
  - When no IPv4 is configured, an explicit bgp router-id needs to be configured
  - This is needed as a BGP Identifier, this is used as a tie breaker, and is send within the OPEN message

Multi-Topology IS-IS

Introduction

- Mechanism that allows IS-IS, used within a single domain, to maintain a set of independent IP topologies
- Multi-Topologies extension can be used to maintain separate topologies for:
  - IPv4
  - IPv6
  - Multicast
- Topologies need not be congruent (of course)

IS-IS Multi-Topologies Architecture
New TLVs

- New TLVs used to advertise neighbours and IP prefixes
  - TLV-229: Multi-Topologies Identifier
  - TLV-222: Multi-Topologies intermediate system
  - TLV-235: Multi-Topologies Reachable IPv4 address
  - TLV-237: Multi-Topologies Reachable IPv6 address

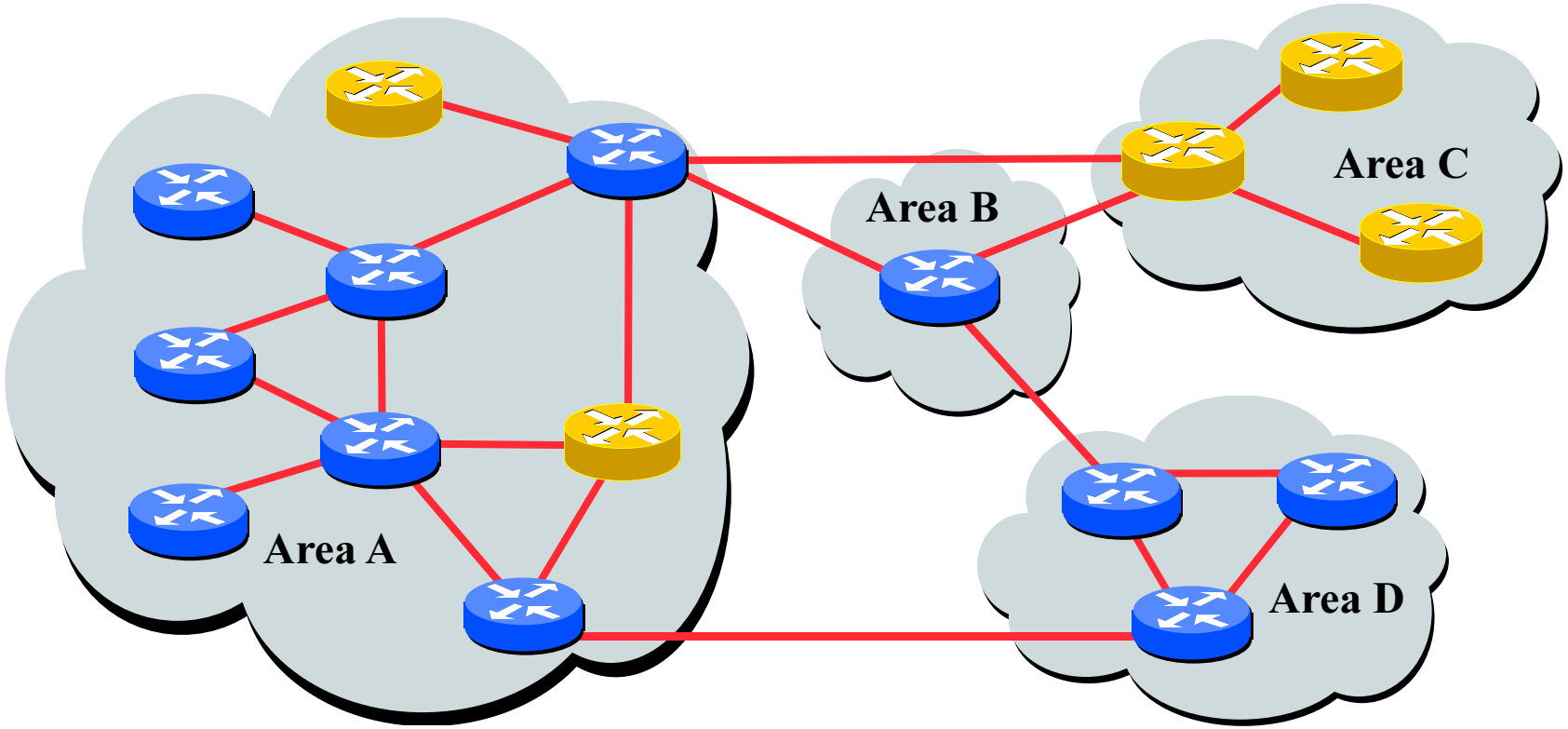
IS-IS Multi-Topologies Architecture
MT Identifiers

- Multi-Topologies Identifier describes the address family of the topology
- Reserved values are:
  - MT ID #0:Equivalent to the “standard” topology.
  - MT ID #1:Reserved for in-band management purposes.
  - MT ID #2:Reserved for IPv6 routing topology.
  - MT ID #3:Reserved for IPv4 multicast routing topology.
  - MT ID #4:Reserved for IPv6 multicast routing topology.
  - MT ID #5-#3995:Reserved for IETF consensus.
  - MT ID #3996-#4095:Reserved for development, experimental and proprietary features.

ISIS Multi Topologies Architecture Adjacencies

- Maintaining MT Adjacencies
  - Each adjacency formed MUST be classified as belonging to a set of MTs on the interface.
  - MT membership advertised in IIH packets
  - Boundaries between levels will be the same for all MTs.

Multi-Topology IS-IS



IPv4-IPv6 enable router

IPv4-only enable router

The Multi-Topology software will create two topologies inside Area for IPv4 and IPv6. IPv4-only routers will be excluded from the IPv6 topology

Tunneling

Tunneling

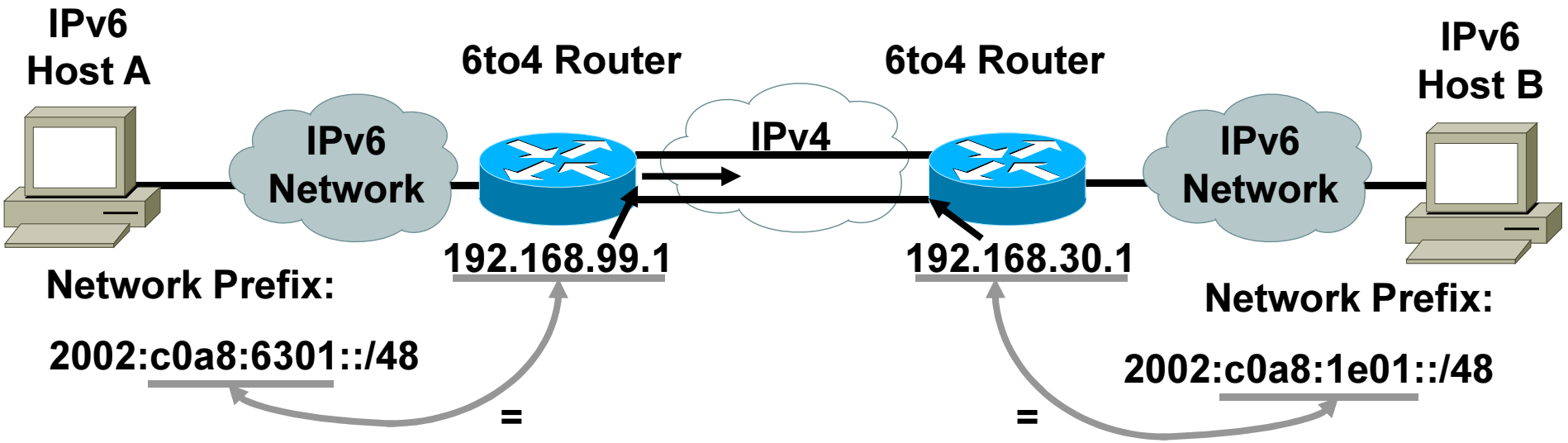
- Many Ways to Do Tunneling
- Some ideas same as before
  - Vendor specific, MPLS, IP
- Native IP over data link layers
  - ATM PVC, dWDM Lambda, Frame Relay PVC, Serial, Sonet/SDH, Ethernet
- Some new techniques
  - Automatic tunnels using 6 to 4, ISATAP and others

6 to 4 Tunneling

Automatic 6 to 4 Tunnels

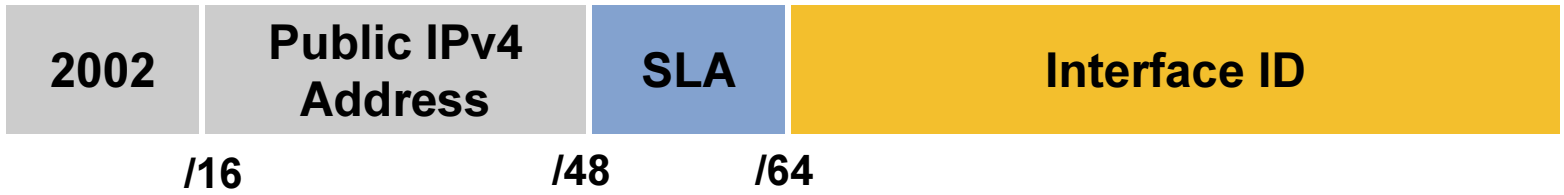
- Automatic 6to4 tunnel allows isolated IPv6 domains to connect over an IPv4 network
- Unlike the manual 6to4 the tunnels are not point-to-point, they are multipoint tunnels
- IPv4 is embedded in the IPv6 address is used to find the other end of the tunnel
- Address format is 2002:<IPv4 address>::

Automatic 6to4 Tunnel (RFC 3056)

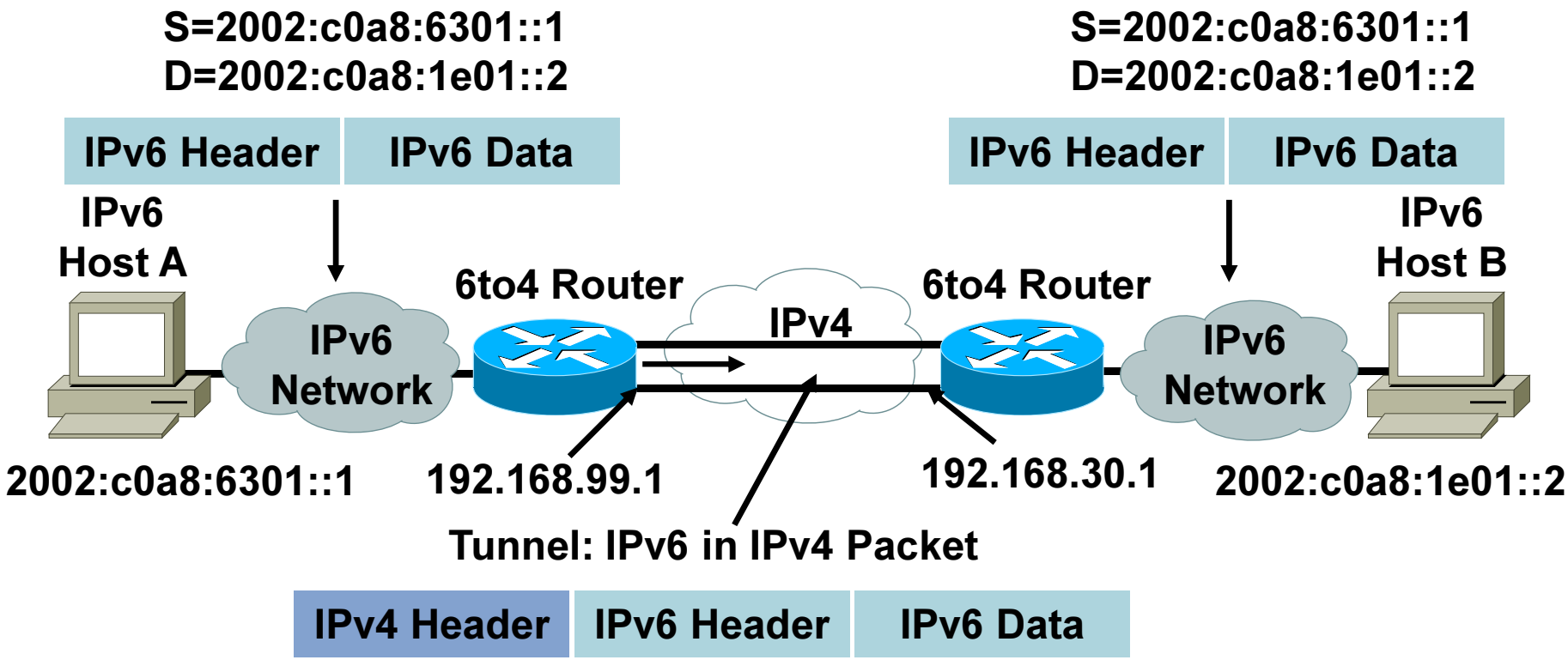


6to4:

- Is an automatic tunnel method
- Gives a prefix to the attached IPv6 network

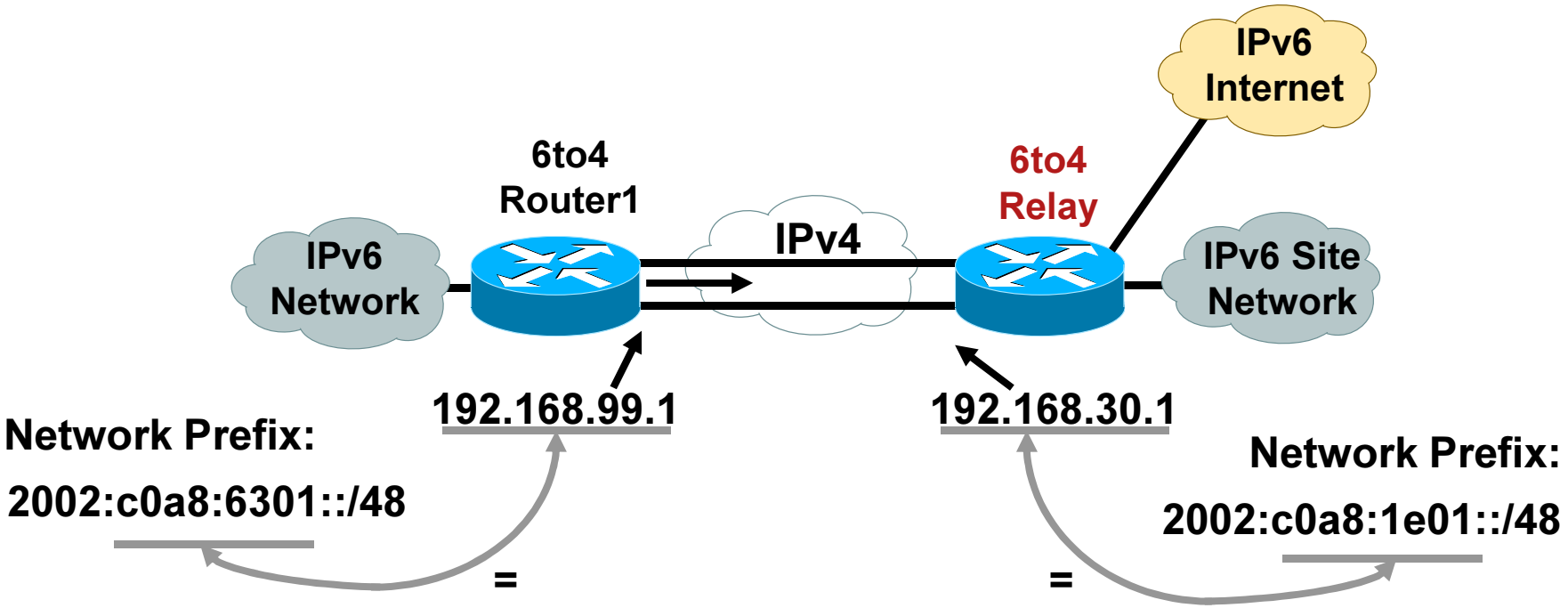


Automatic 6to4 Tunnel (RFC 3056)



S(v4)=192.168.99.1
D(v4)=192.168.30.1
S(v6)=2002:c0a8:6301::1
D(v6)=2002:c0a8:1e01::2

Automatic 6to4 Relay



6to4 Relay:

- Is a gateway to the rest of the IPv6 Internet
- Is a default router

Automatic 6to4 Tunnels

Requirements for 6to4

- Border router must be dual stack with a global IPv4 address
- Interior routing protocol for IPv6 is required
- DNS for IPv6

ISATAP Tunneling

Intrasite Automatic Tunnel Address Protocol

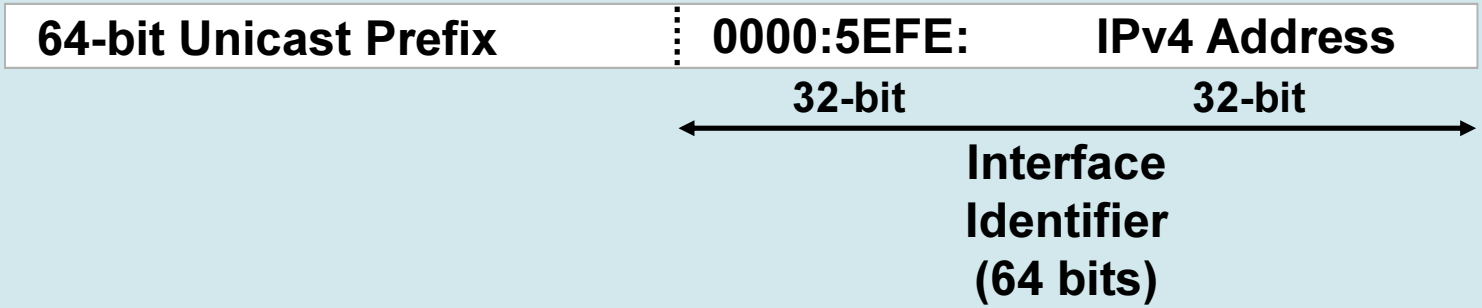
- RFC 4214
- This is for enterprise networks such as corporate and academic networks
- Scalable approach for incremental deployment
- ISATAP makes your IPv4 infratructure as transport (NBMA) network

Intrasite Automatic Tunnel Address Protocol

- RFC 4214
- To deploy a router is identified that carries ISATAP services
- ISATAP routers need to have at least one IPv4 interface
- DNS entries are created for each of the ISATAP routers' IPv4 addresses
- Hosts will automatically discover ISATAP routers and can get access to global IPv6 network
- Host can apply the ISATAP service before all this operation but its interface will only have a link local v6 address until the first router appears

Intrasite Automatic Tunnel Address Protocol

Use IANA's OUI 00-00-5E and
Encode IPv4 Address as Part of EUI-64



- ISATAP is used to tunnel IPv4 within as administrative domain (a site) to create a virtual IPv6 network over a IPv4 network
- Supported in Windows XP Pro SP1 and others

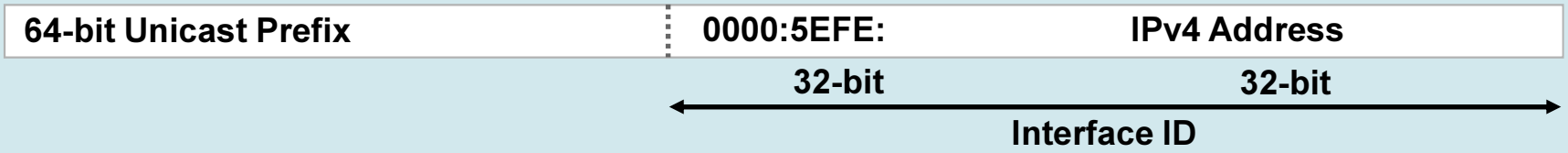
IPv6 Campus ISATAP Configuration

- Supported in Windows XP Pro SP1 and others
- ISATAP connections look like one flat network
- Create DNS “A” record for “ISATAP” = 10.1.1.1
- Use Static Config if DNS use is not desired:

```
C:\>netsh interface ipv6 isatap set
router 10.1.1.1
```

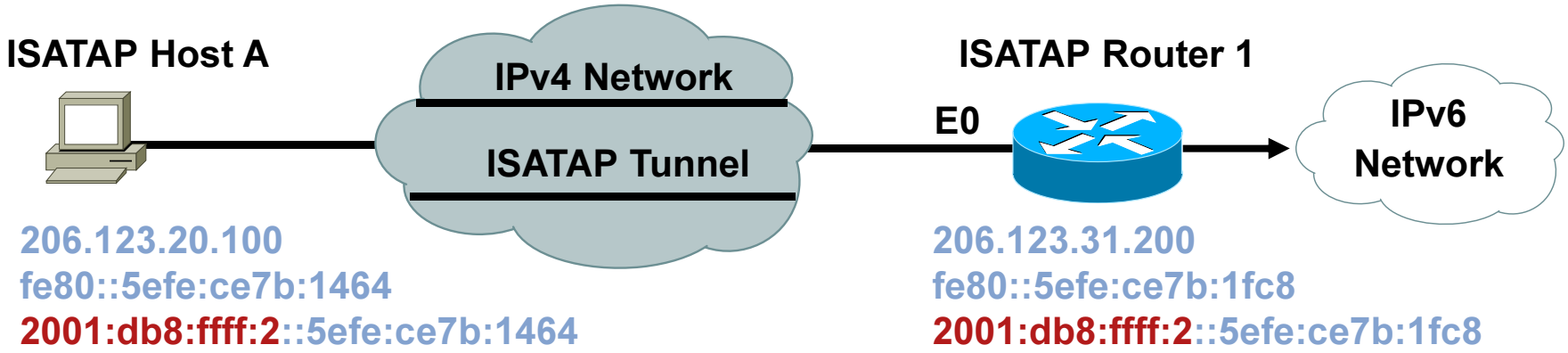
- Currently ISATAP does not support multicast!!

ISATAP Address Format:



2001:DB8:C003:111F:0:5EFE:10.1.2.100

Automatic Address Assignment of Host and Router



- ISATAP host A receives the ISATAP prefix 2001:db8:ffff:2::/64 from ISATAP Router 1
- When ISATAP host A wants to send IPv6 packets to 2001:db8:ffff:2::5efe:ce7b:1fc8, ISATAP host A encapsulates IPv6 packets in IPv4. The IPv4 packets of the IPv6 encapsulated packets use IPv4 source and destination address.

IPv6 in DOCSIS 3.0

IPv6 Drivers in Cable Access Networks

IPv6 Drivers

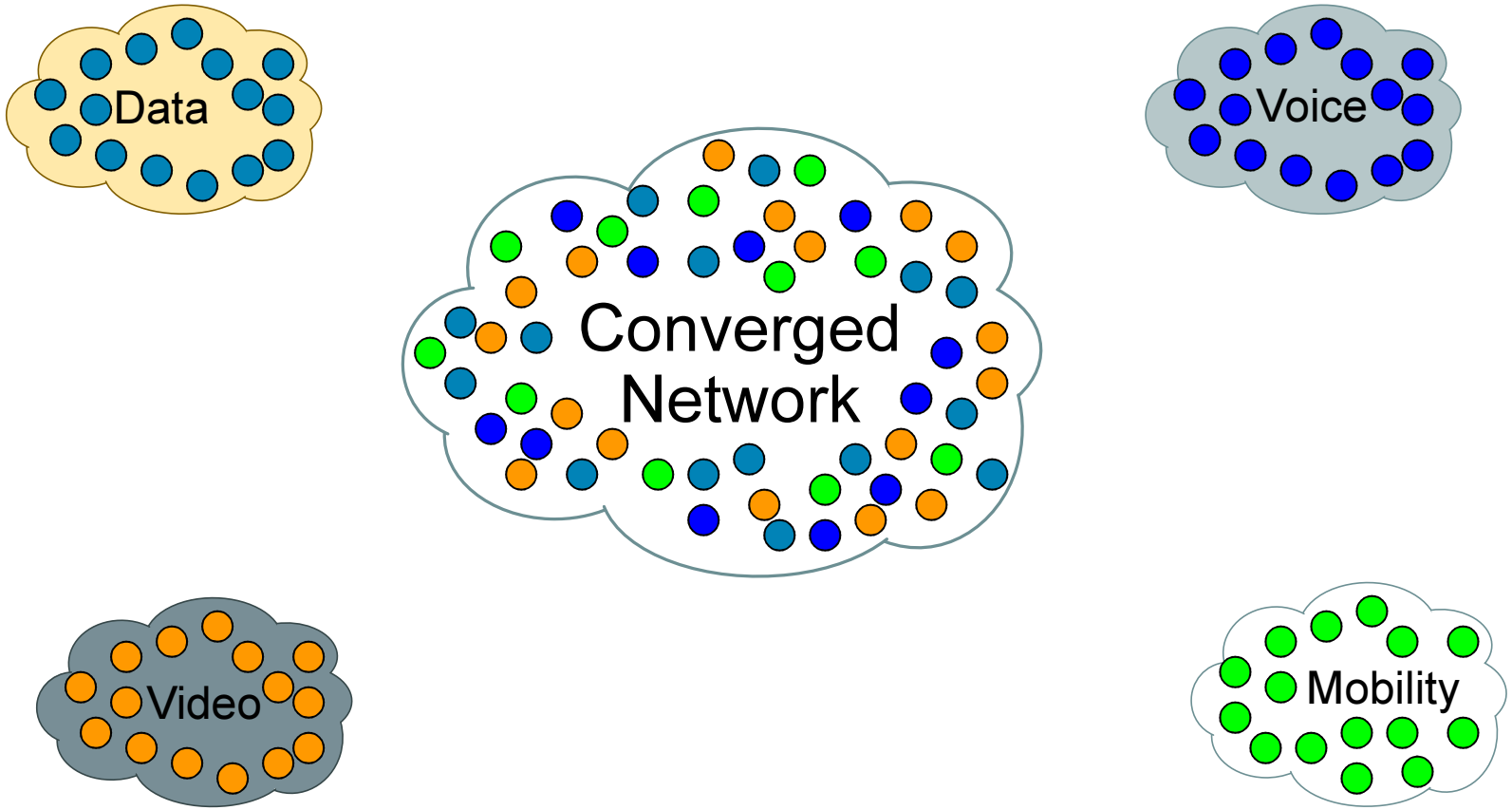
- Networks have scaled to such a degree that IPv4 address constraints are becoming a burden on network operations
  - IPv4 address exhaustion
  - All IP quad play
  - Industry consolidation
- Build infrastructure for future services
  - Global transparency
  - Plug and play home networking
  - Access transparency

Why do Cable MSO's need IPv6 *now* ?

- Convergence of multiple services over IP is driving the need for large scale addressing
  - MSO infrastructure
  - Home/SMB networks
- IP is being embedded in devices that are no longer "computers" limited to IT environment
  - Sling-boxes, IP cameras, PDAs, gateways, automobiles, media centers, IP phones, etc...
- Home Networking combined with "always on" technologies like cable, dsl
  - Consumers demanding plug-and-play operation.
  - Consumer space is migrating toward a one-subnet-per-home model (instead of a shared subnet across multiple homes)
- Industry consolidation has led to mergers of IP networks with overlapping addresses
  - Managing overlapping private address spaces, network renumbering is complex and expensive …
- Next generation applications require global transparency
  - True Peer-to-peer connectivity without NAT (Presence & IM, Streaming, IP telephony etc…)
- Next generation services require access transparency
  - Seamless roaming across networks for fixed/mobile convergence

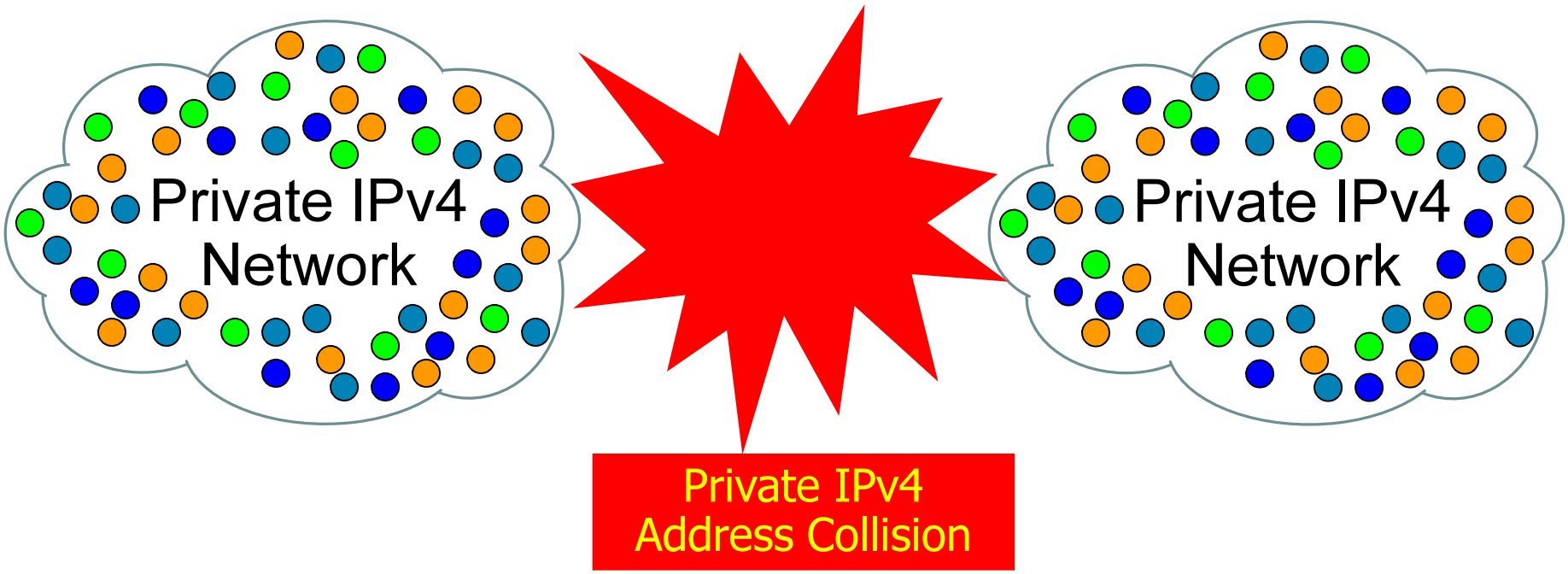
All IP Quad Play

Convergence of n IP networks calls for huge scale (nxIP) address space.



Industry Consolidation

Merger of networks with over-lapping address space calls for large, non-overlapping address space.

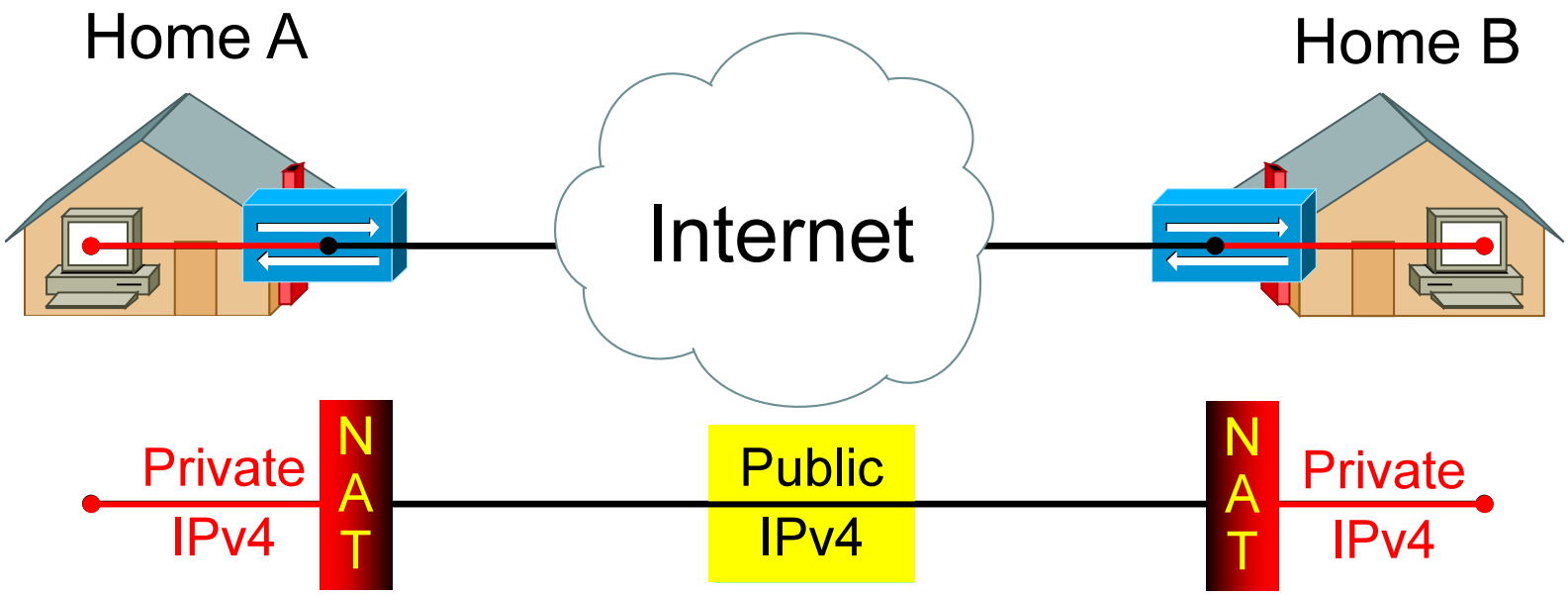


Plug-n-Play Home Networking

Premises network(s), automatic config. beyond DHCP

Global Transparency

IPv6 restores global transparency by getting rid of NAT.



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.)

CableLabs IPv6 Decision and Approach

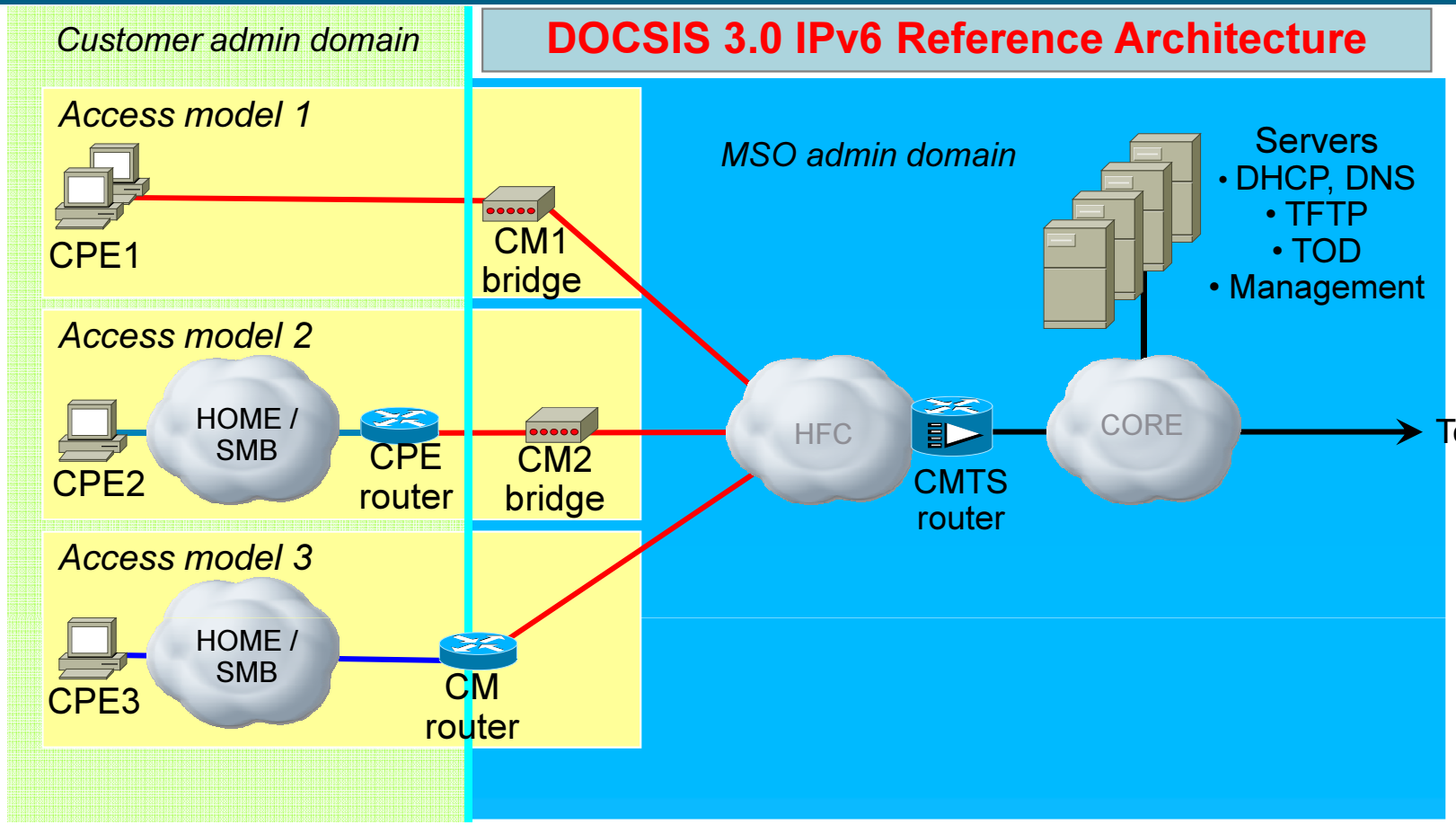
- CableLabs members put IPv6 in consideration for DOCSIS 3.0
  - IPv6 was amongst the top DOCSIS 3.0 feature candidates
- Result: DOCSIS 3.0 MUST fully support IPv6
- Rationale
  - Increased address space for CM management
  - CPE services
- Proposed phases

  Phase 1 –CM provisioning and management over IPv6; embedded IPv6 router

  Phase 2 – Remaining IPv6 features for CPE services, for example IPv6 CPE provisioning and IPv6 service support

IPv6 Features 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)
- HFC may have management prefix for CMs and managed CPEs, and service prefix for data service
- 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



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

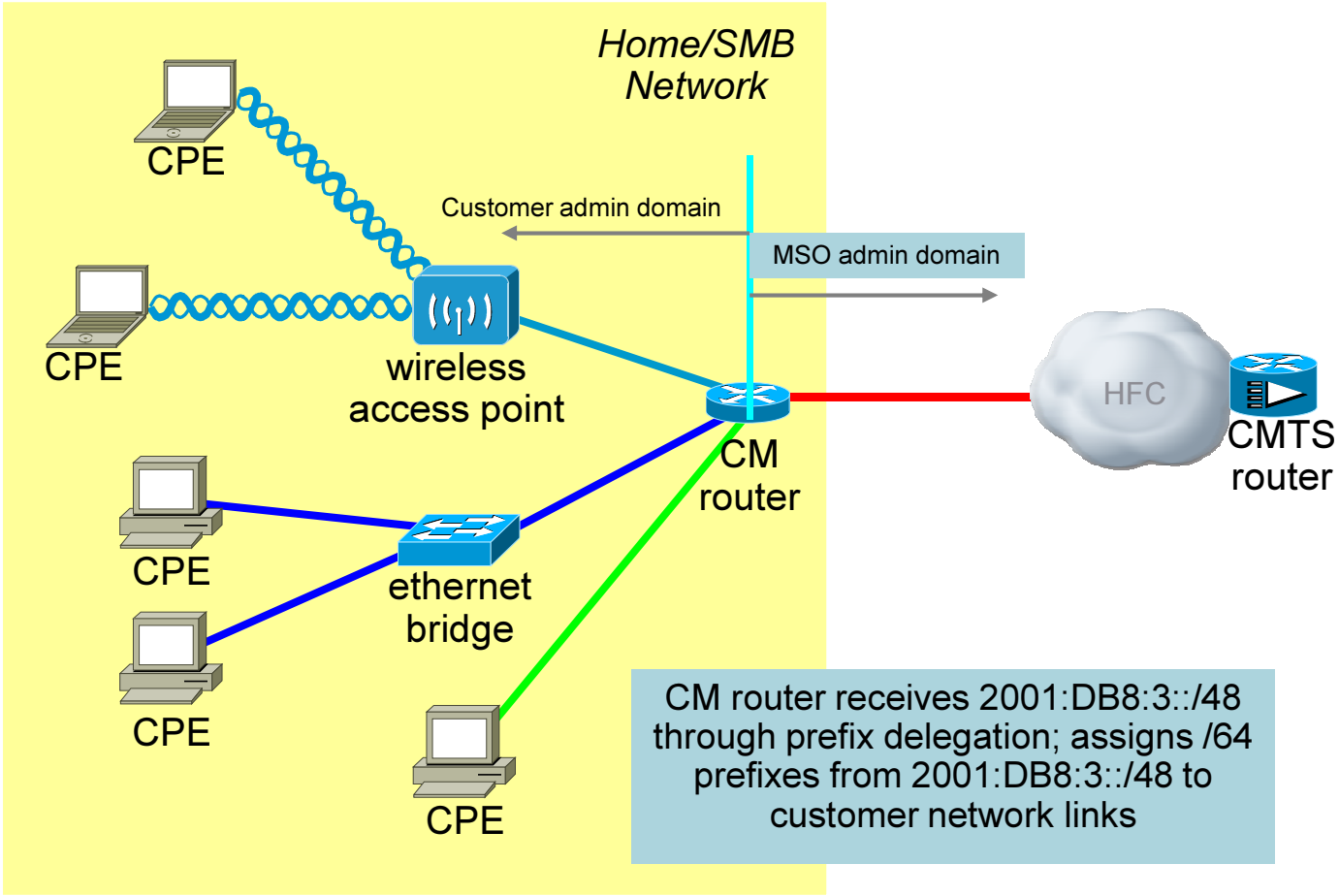
HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt) and 2001:DB8:FFFE:0::/64 (service)

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

Theory of Operations

Theory of Operations: DOCSIS 3.0

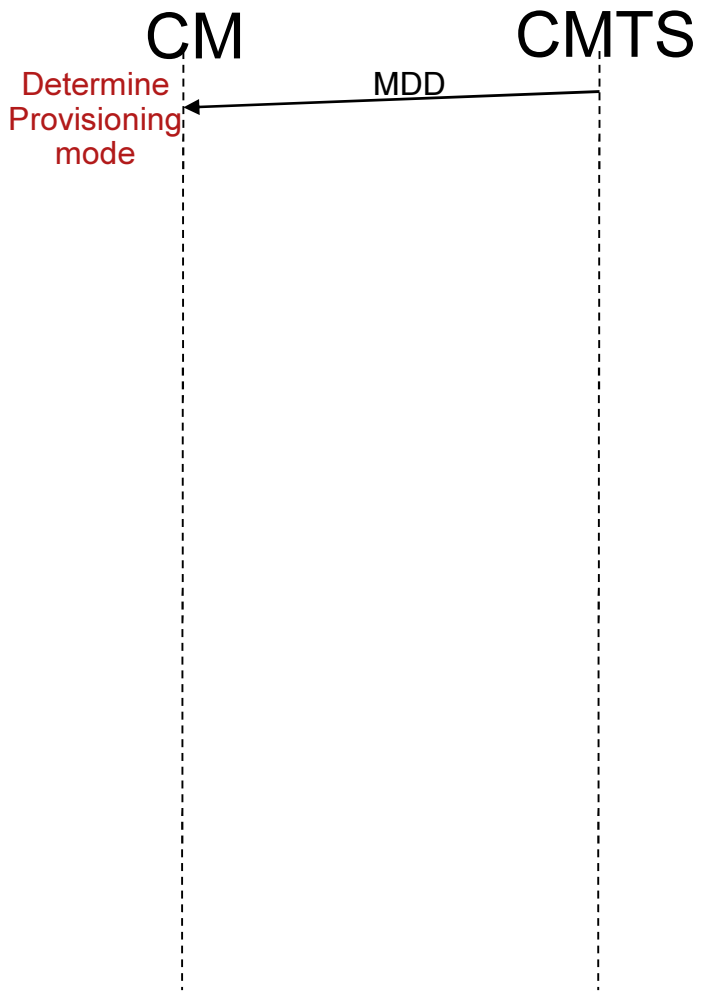
- CM can operate in either bridging or routing mode
- CM management stack can operate in
  - IPv4 only mode
  - IPv6 only mode
  - Dual mode
- CM instructed by the CMTS via an L2 message (MDD) as to what mode to use
  - If the CM does not receive any message from the CMTS it operates in DOCSIS 2.0 mode

CM provisioning

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

CM provisioning: Layer 2

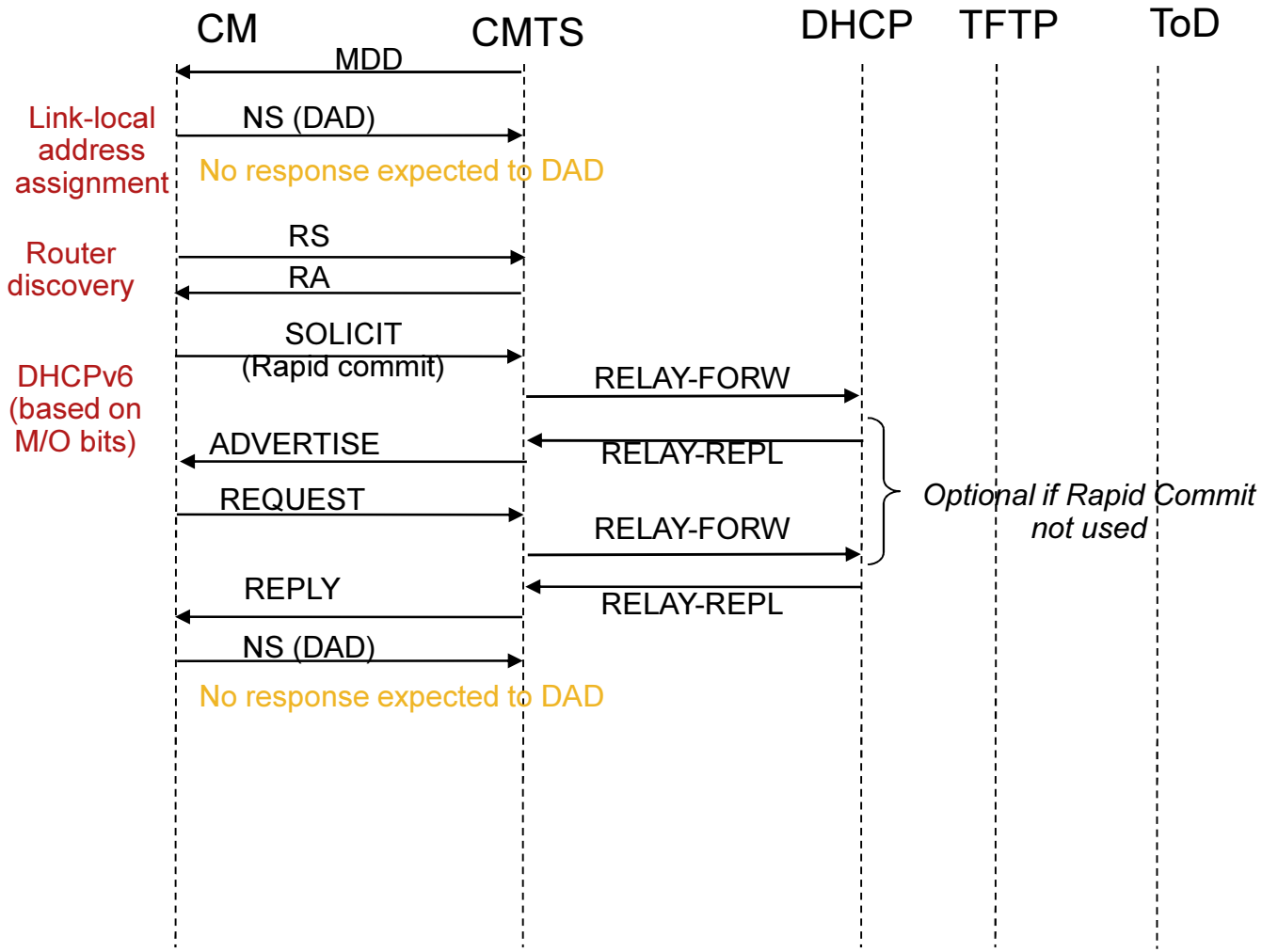
- CMTS sends an L2 message to the CM that controls
  - Use of IPv4 or IPv6 as the preferred mode for CM provisioning and management
  - Dual stack management
  - Alternate Provisioning Mode (APM): If preferred mode fails, restart provisioning in the alternate mode



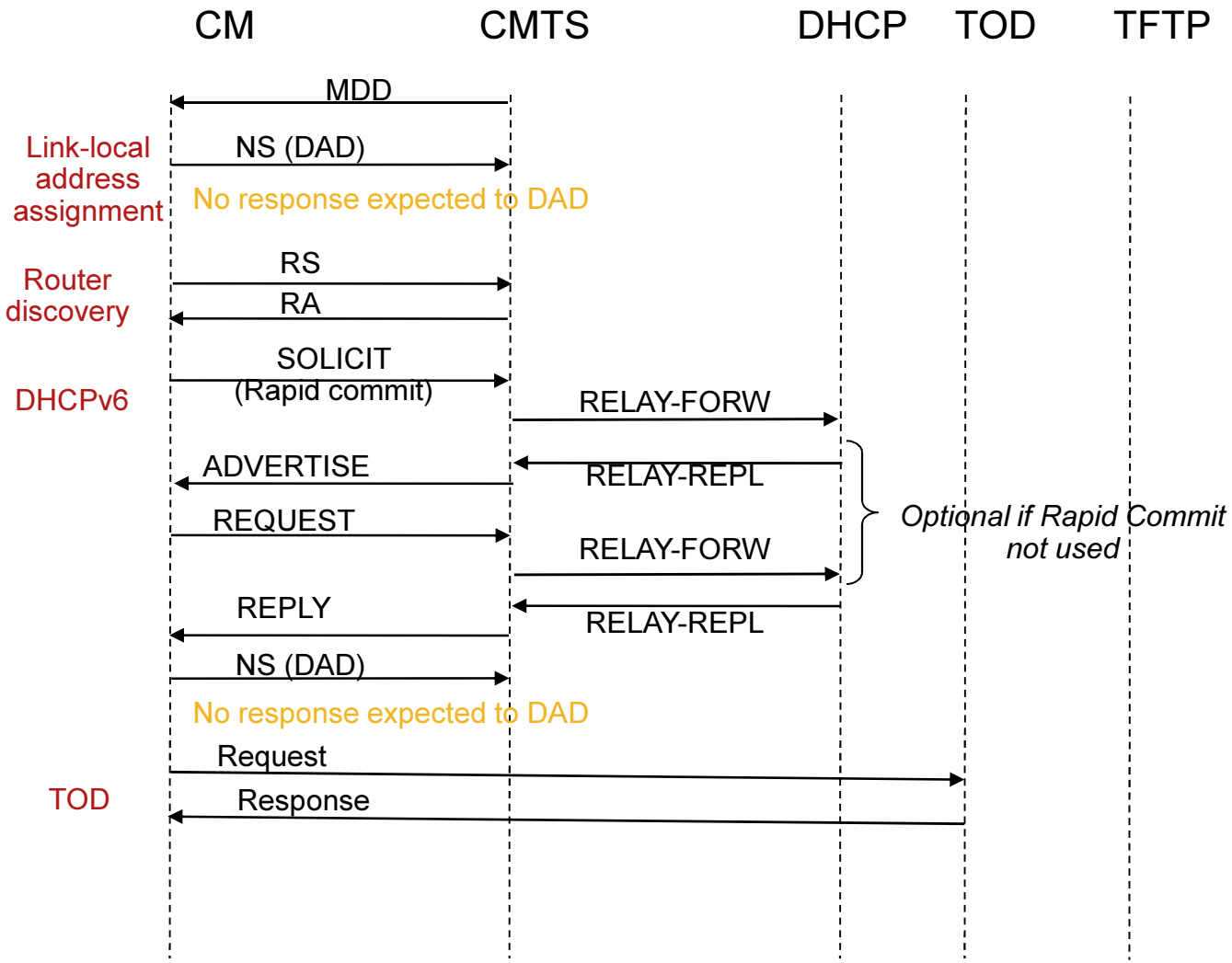
CM Provisioning: Acquire IP connectivity

- DHCPv6 used for address configuration
  - Stateless auto configuration NOT used
  - M and O bits set appropriately 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)

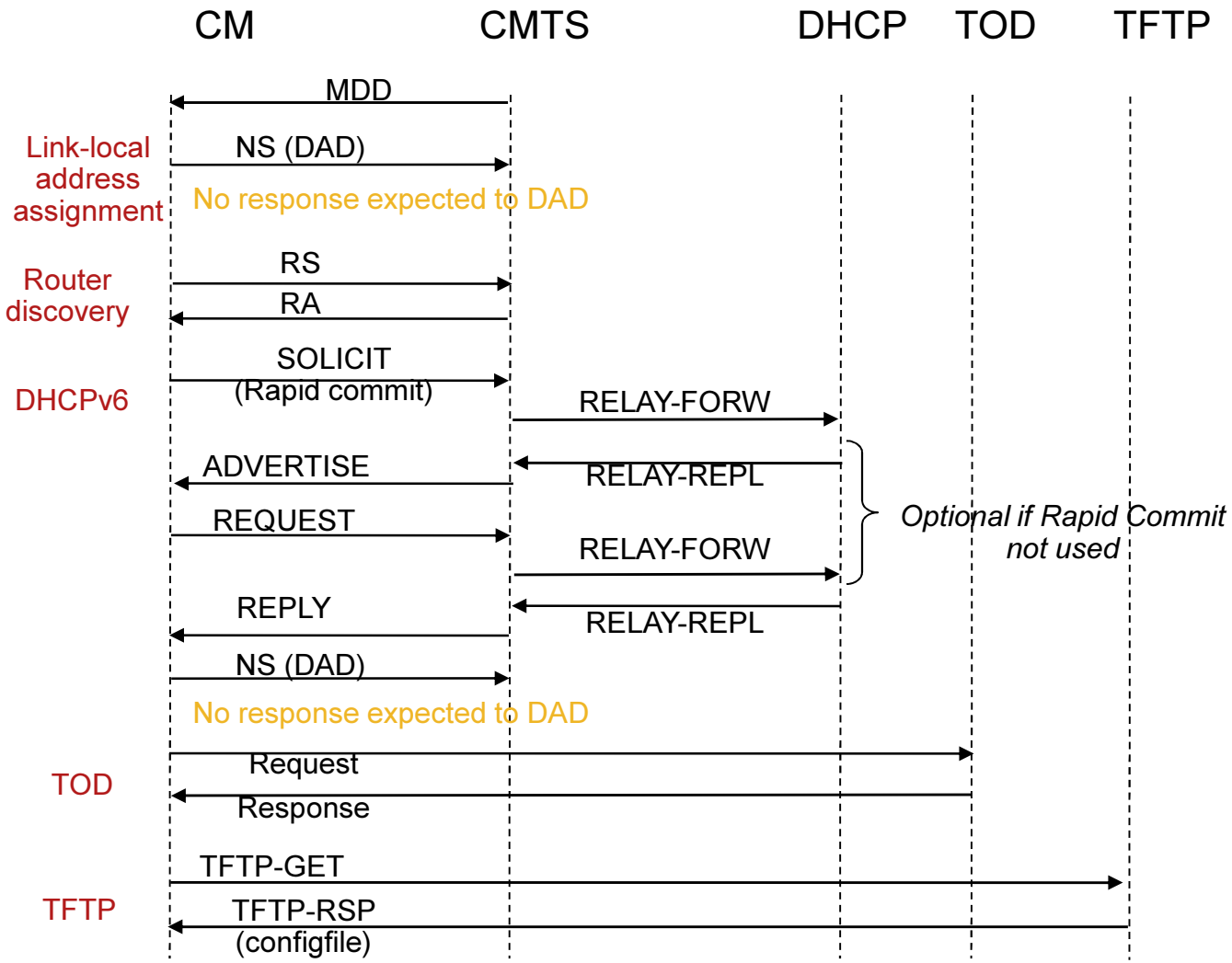
CM Provisioning: Acquire IP connectivity



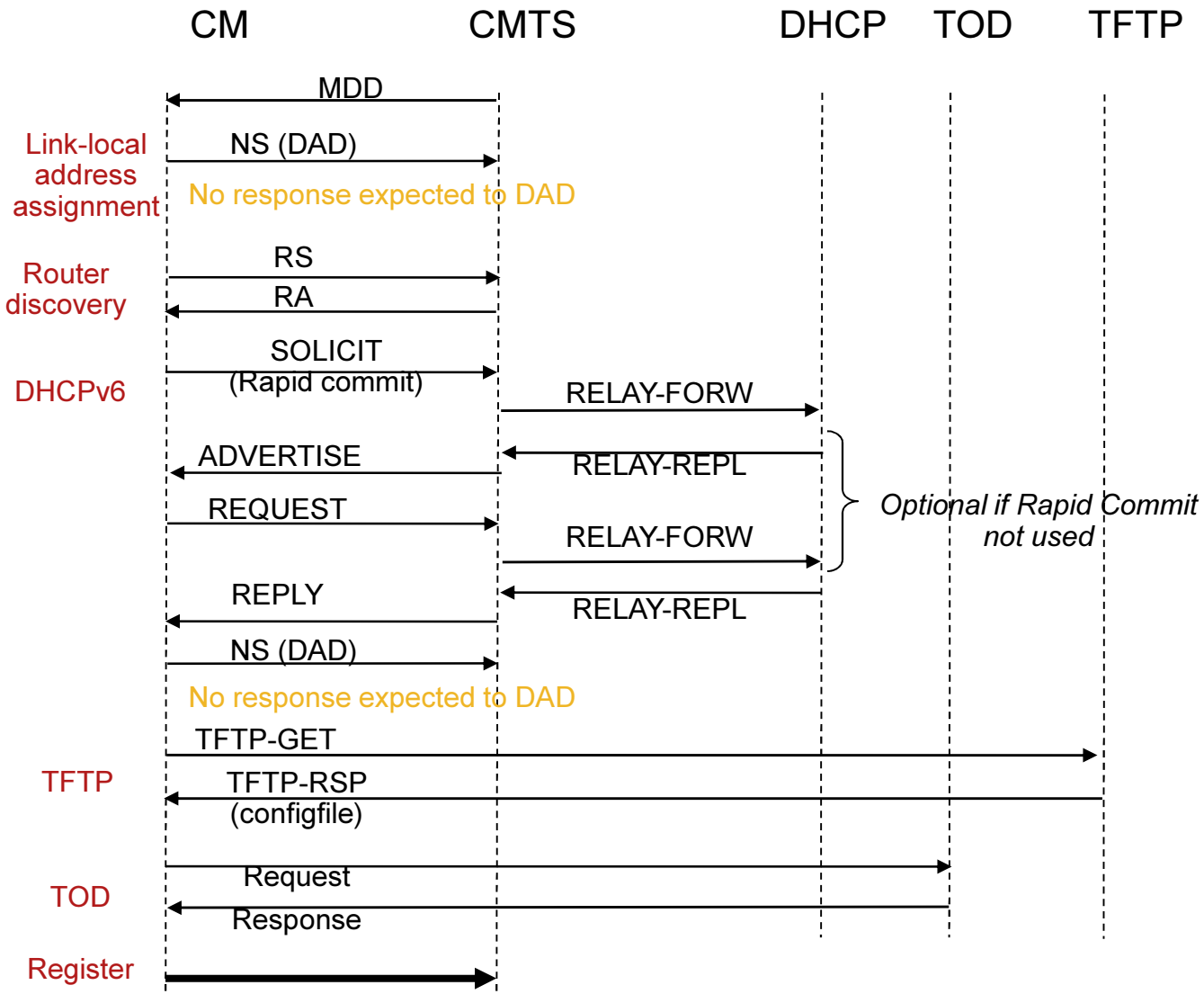
CM Provisioning: Obtain TOD



CM Provisioning: Obtain Configuration File



CM Provisioning: Complete Registration



Dual Stack Management

- CM directed to use dual stack management via MDD message
- After registering with either IPv4 or IPv6 address, the CM acquires the additional IP address type using DHCP
- Allows the MSOs to manage the CMs using SNMP carried over IPv4 or IPv6
  - Useful during the transition period

Alternate Provisioning Mode (APM)

- To improve provisioning reliability
- CM first uses primary provisioning protocol (IPv6 or IPv4) as specified by MDD message
- If primary provisioning mode fails, the CM tries to provision itself using the other protocol
  - e.g., if primary mode is IPv6 and it fails, CM restarts provisioning in IPv4 mode (only if APM is configured)

CMTS and CM Requirements for IPv6

CMTS Requirements for IPv6

- CMTS can be a bridge or 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

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
- Support MLDv1 and MLDv2 for multicast

MSO CPE Address Assignment Strategies

Dual Stack CPE with Public V6 & V4 Addresses

- IPv4 applications and Internet services will continue to exist for a foreseeable future
- In the end to end dual stack model, the end subscribers will be provided with a global IPv6 address as well as a global IPv4 address
- CPEs can use, IPv6 address to access the V6 part of the Internet and IPv4 address to access the V4 part of the Internet and services
- Cable Modem management may use, IPv6/IPv4 or dual stack
- With this approach, provider side large scale NAT will not be a requirement

Single IPv6 only stack for the CPEs

- This approach may be taken by MSOs whose public V4 address space available for the CPE side addressing is very limited
- In this as well, the core infrastructure nodes may be configured to run in dual stack mode
- Each customer side CPE device will be assigned with a single global IPv6 address
- Cable Modem management may use, IPv6/IPv4 or dual stack
- V6 enabled applications from the CPE side can seamlessly access the V6 part of the Internet
- Some kind of large scale 6-to-4 NAT will have to be done on the customer side to facilitate the V4 Internet access

Dual Stack CPE with Public V6 & private V4 Addresses

- This is another approach MSOs may take if they have very limited public IPv4 address left out for CPE side addressing
- Core infrastructure will be configured to run in dual stack mode
- Each customer side CPE device will be assigned with a single global IPv6 address & a single private IPv4 address
- V6 enabled applications from the CPE side can seamlessly access the V6 part of the Internet
- In order to support V4 based Internet services, some kind of large scale 4-4 NAT will need to be done on the provider side

Q & A