Cisco live!

February 15 – 19, 2016 • Berlin, Germany

We're ready. Are you?

1995

Migrated to USA
IPv6 First Draft

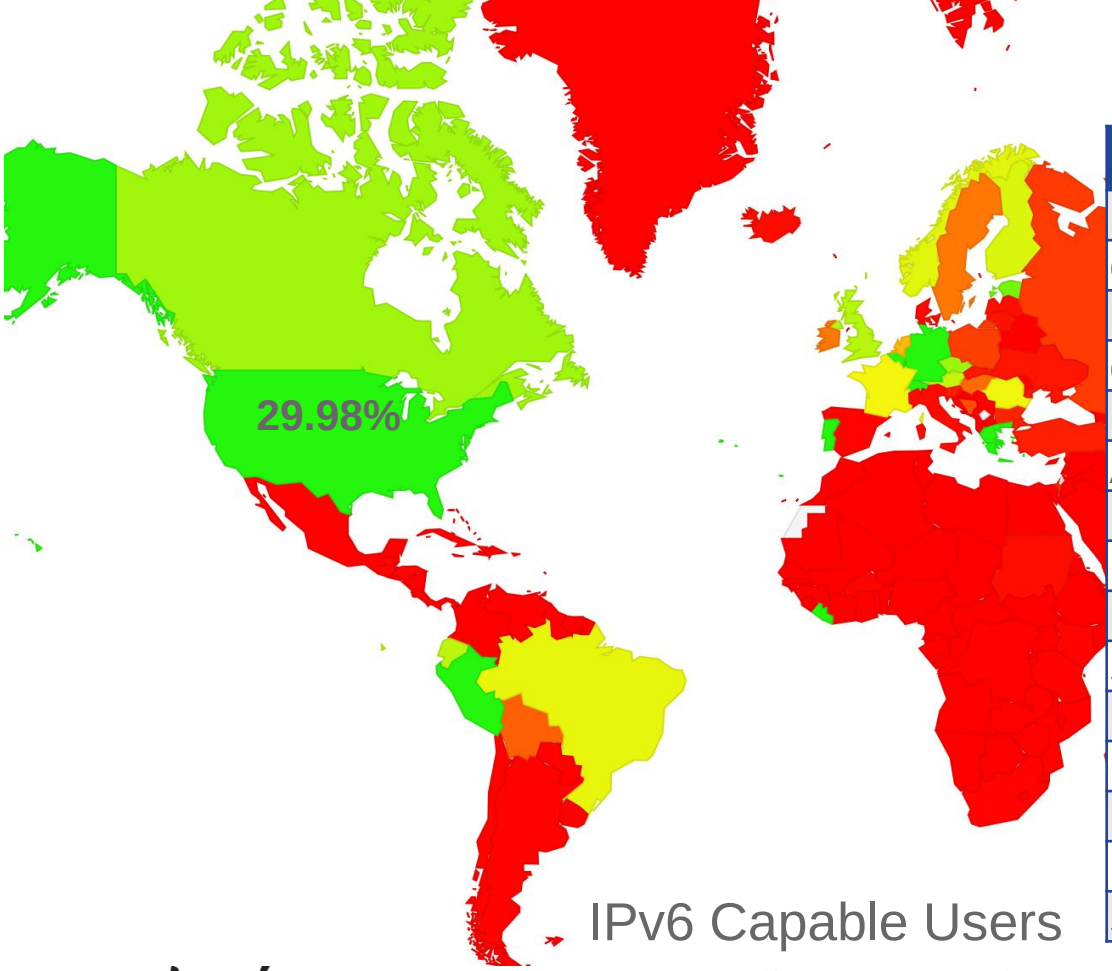
2006

Started with Cisco
Docsis3.0 Specification

2016

CiscoLive Berlin
IPv6 20th Birthday

IPv6 traffic to Google - 10%



Country	IPv6 Capable Users
Belgium	49.49%
Germany	26.39%
Norway	11.13%
Czech Republic	11.00%
Finland	9.84%
Austria	8.45%
France	6.93%
Romania	6.26%
Netherlands	5.30%
Sweden	4.45%
Ireland	4.09%
Poland	1.98%
Bulgaria	0.87%
Denmark	0.26%
Spain	0.09%

IPv6 Capable Users

Source: http://stats.labs.apnic.net/ipv6

Learn IPv6

Implement Best Practices

Enjoy the Benefits

IPv6 Deployment Best Practices for the Cable Access Network

Sreeni Inukoti, Network Consulting Engineer

Cisco live!

Agenda

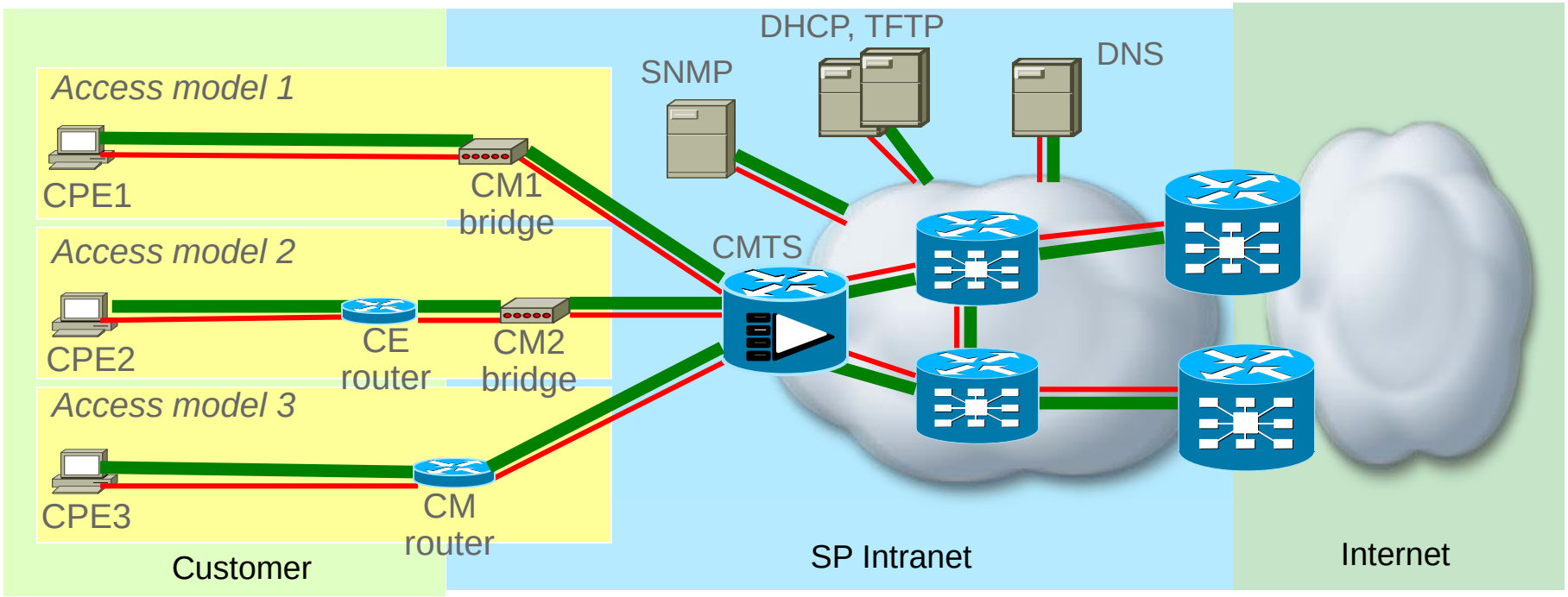
- IPv6 motivation and challenges
- IPv6 technology and usage in cable
- IPv6 for CPEs
- IPv6 for CPE routers
- IPv6 for cable modem management
- IPv6 transition strategies
- IPv6 security

IPv6 motivation and challenges

Cable’s IPv6 motivators

- Main motivator – IPv4 address depletion
- From end user’s perspective – marginal incentive to move to IPv6
- Other motivators ?

The transition to IPv6



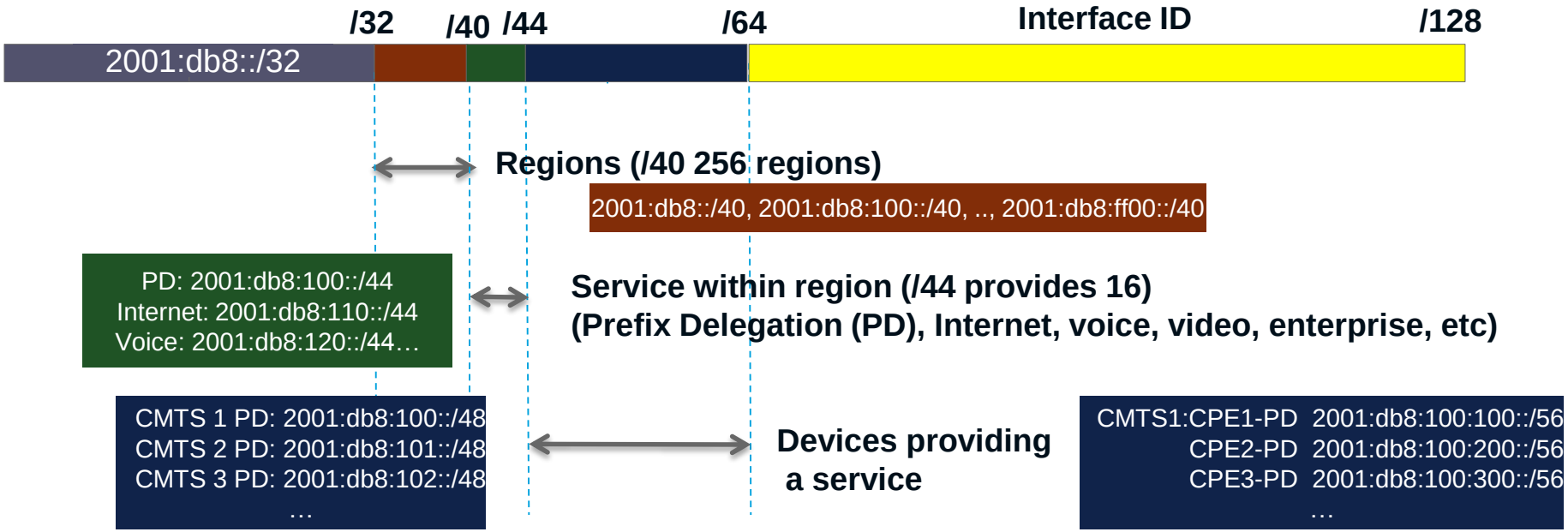
Product requirements

- For the CMTS
  - cBR-8 **(XE 3.17)**
  - uBR100012 with PRE-4/5 processors and MDF capable line cards (20x20V, 3Gx60V, wideband SPA, high density SPA) (**12.2 (33) SCI3 or 12.2(33)SCJ**)
  - uBR72xxVXR with NPE-G2 and 8x8V line cards
- DOCSIS 3.0 or DOCSIS 2.0+ cable modems
- Generally recommended to use latest releases of BAC/CNR.
  - BAC now called Cisco Prime Cable Provisioning / CPCP (**latest version 5.2**).
  - CNR now rebranded as Cisco Prime Network Registrar / CPNR (**latest version 8.3**)

IPv6 address planning

Sub-netting example (assuming - /32 for SP)

BRKRST-2667 How to write an IPv6 Addressing Plan
Wed: 2.30pm



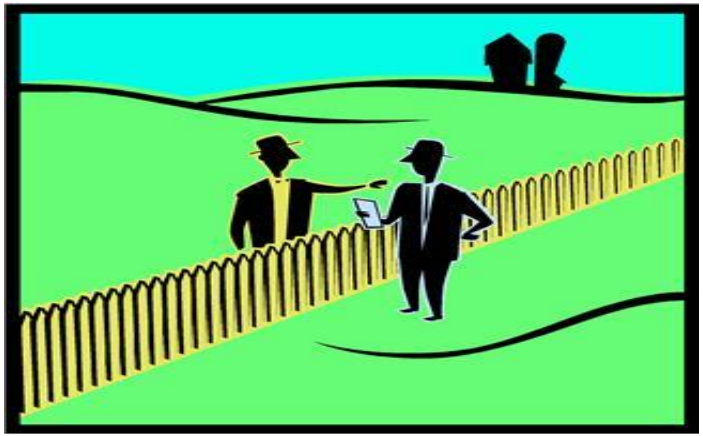
http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/IPv6_WP.pdf

IPv6 technology and usage in Cable

IPv6 neighbor discovery (ND)

- IPv6 ND RFC 4861 works over ICMPv6

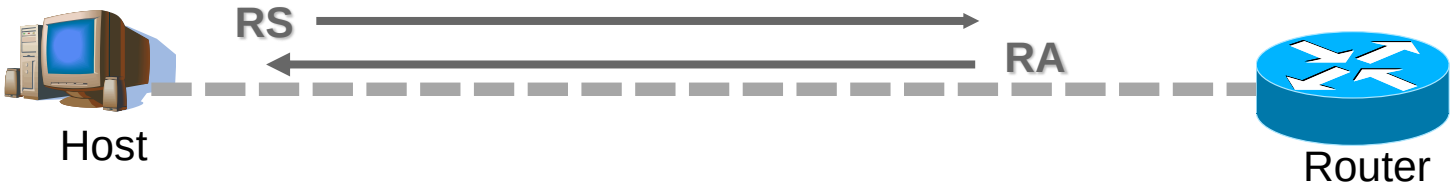
- Main functionalities :
  - Router discovery
  - Neighbor first hop discovery
  - Maintain neighbor reachability state



IPv6 neighbor discovery

Router discovery

- Router Advertisement (RA) sent periodically by router or on request upon receipt of Router Solicitation (RS)



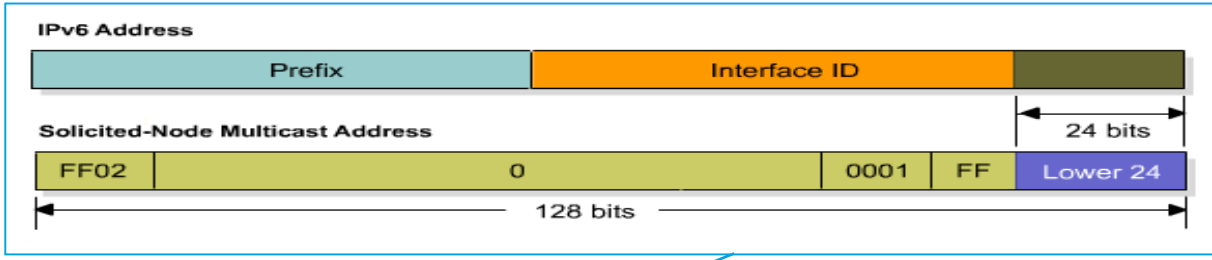

```
Routing Solicitation Packet
Definition (ICMP Type : 133)
Src = ::0 or Src GUA
Dst = All-Routers address (FF02::2)
```

```
Routing Advertisement Packet Definition
(ICMP Type : 134)
Src = Router Link-local Address
Dst = All-nodes address (FF02::1) or Dst GUA
Data= options, prefix, lifetime, autoconfig
flag
```

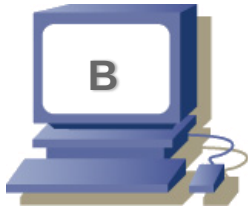
- Note: for a cable access network the CMTS will be the only valid sender of Router Advertisement messages

IPv6 neighbor discovery

L2 address resolution in IPv6



Neighbor Solicitation (ICMP Type : 135)
Src = Link-local Address of A
Dst = Solicited Node multicast Address of B
Data = LLA of A
Query = What is your link address ?



Neighbor Advertisement (ICMP Type : 136)
Src = Link-local Address of B
Dst = Link-local Address of A
Data= Link-layer addr of B

IPv6 neighbor discovery

On-link vs. Off-link

IPv4

- Address and netmask provide On-link prefix information
- If On-link, host directly communicate to resolve L2 address (ARP)
- Default Gateway is part of DHCPv4 option

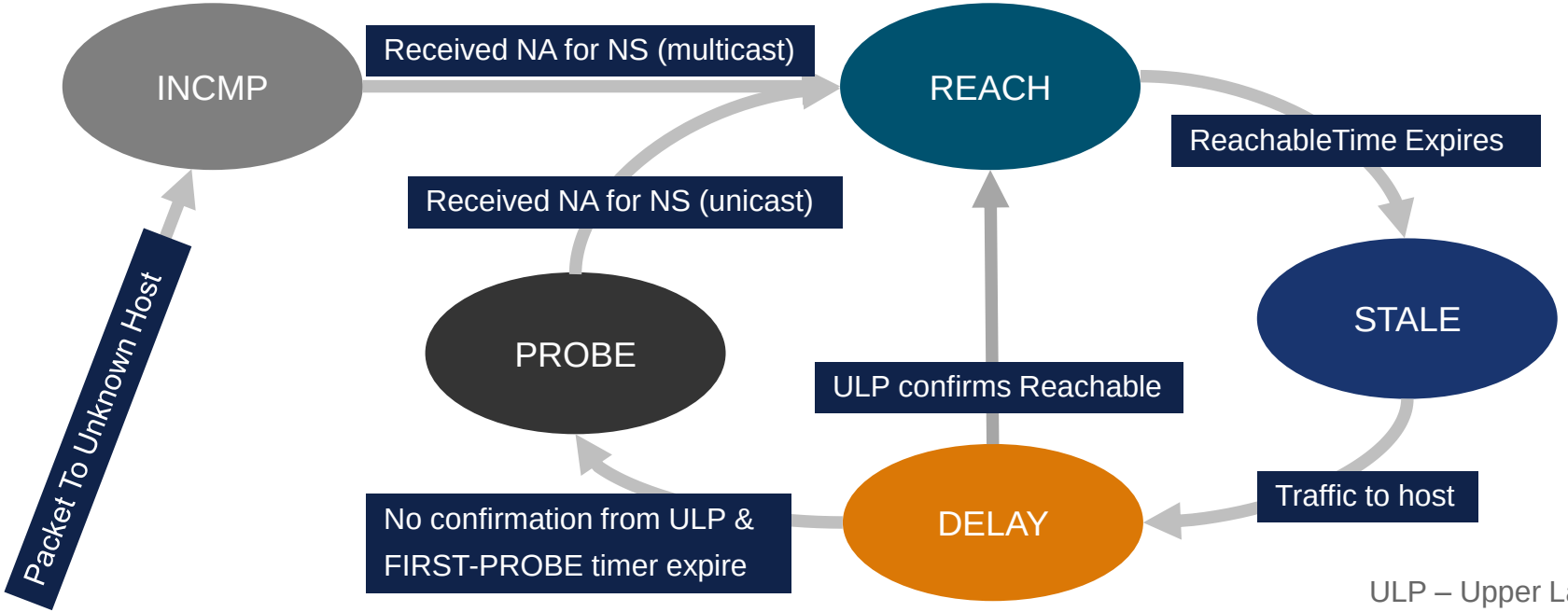
IPv6

- Address is separate from On-link. Prefixes are advertised via RA message
- If On-link, host directly communicate to resolve L2 address (NS)
- Default Gateway is part of RA

On CMTS, communication between hosts is always via CMTS, So GUA and ULA destinations are always off-link

IPv6 neighbor discovery

Neighbor cache and Neighbor Unreachability Detection

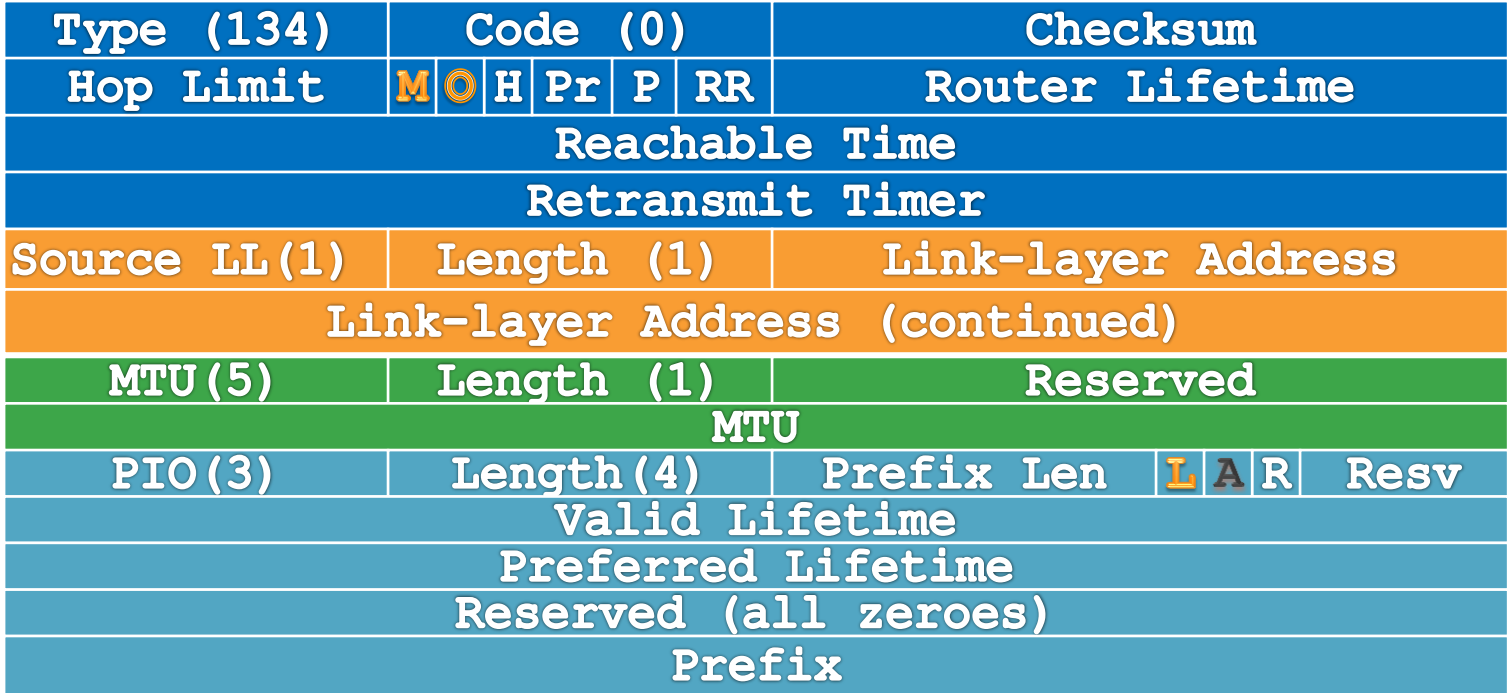


ULP – Upper Layer Protocol

```
CMTS#show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FE80::7EB2:1BFF:FE2D:DAC0                   - 7cb2.1b2d.dac0  REACH Bu99
FE80::21E:6BFF:FEFB:872                     - 001e.6bfb.0872  REACH Bu99
```

IPv6 address acquisition

Router Advertisement



M – Managed bit

O - Other

PIO – Prefix Information Option

L – On-link flag

A – Autonomous

IPv6 address acquisition

DHCPv6 message types

- DHCPv6 (RFC 3315) defines a number of message types
  - SOLICIT(1), ADVERTISE (2), REQUEST(3), REPLY (7)
  - CONFIRM(4), RENEW(5), REBIND (6)
  - RELEASE (8), DECLINE (9)
  - RECONFIGURE (10)
  - INFORMATION-REQUEST (11)
  - RELAY-FORW (12), RELAY-REPL (13)
- DHCPv6 Leasequery (RFC 5007) adds
  - LEASEQUERY(14), LEASEQUERY-REPLY(15)

IPv6 address acquisition

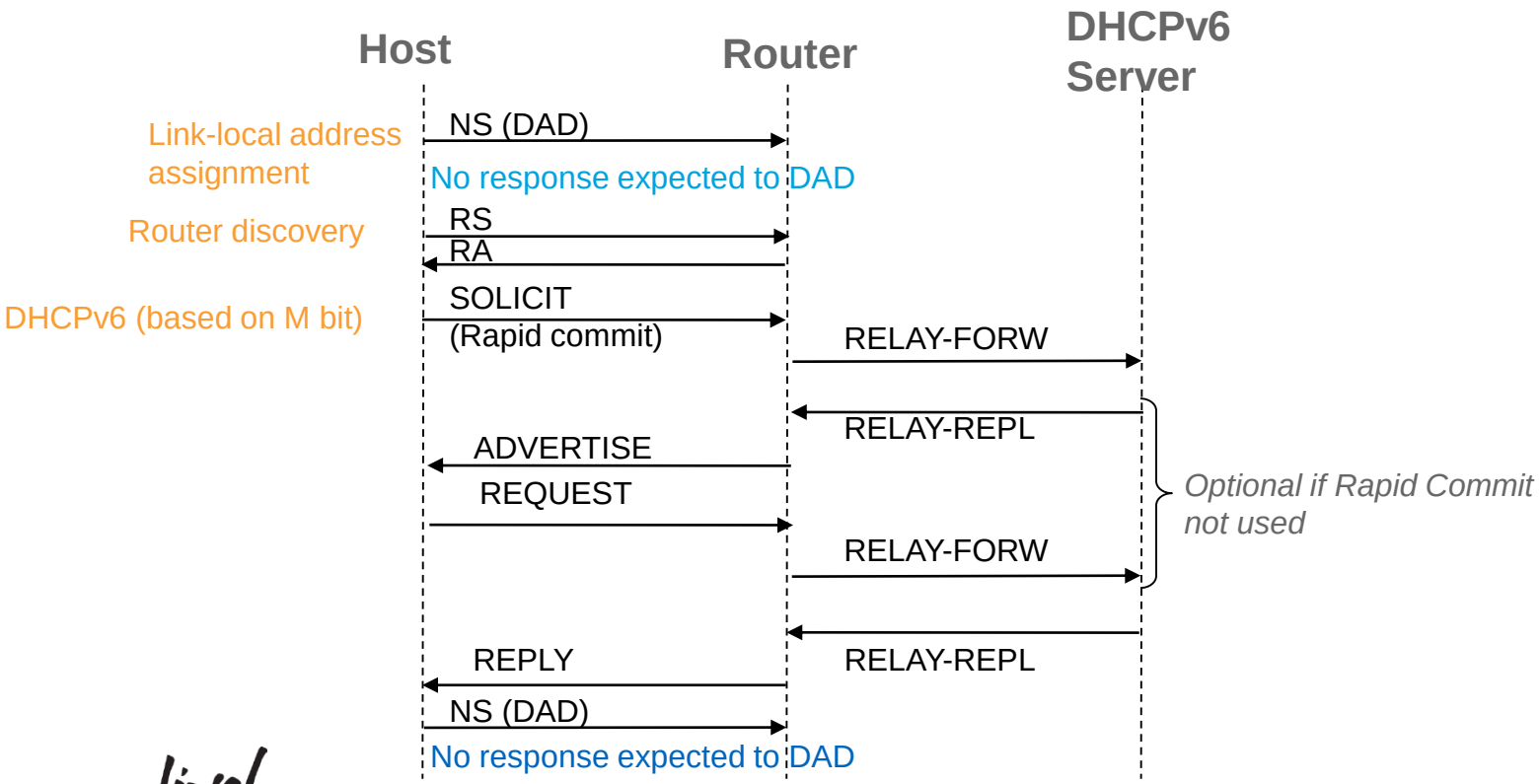
Rapid commit

- Client willing to complete DHCPv6 in two steps (SOLICIT-REPLY) includes Rapid Commit option (option 14) in SOLICIT. If accepted by the server, REPLY must contain Rapid Commit option as well.

- When Rapid Commit is used the server commits the address assignment without any knowledge on if the client actually uses it or not; should only be used with multiple servers if they are deployed such that only one server will respond to a Solicit message

IPv6 address acquisition

DHCPv6 process



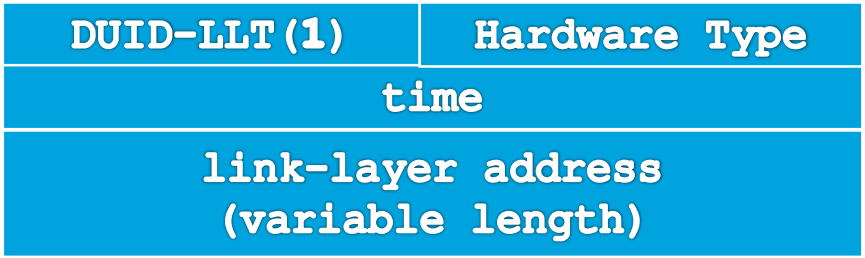
IPv6 address acquisition

DHCP Unique Identifier (DUID)

- Each client and server has a DHCP Unique Identifier (DUID) which is carried as an option and **must be unique and stable over time.**

- DUID formats or types defined by **RFC 3315**
  - Link-layer address plus time – DUID-LLT (1)
  - Vendor-assigned unique ID based on enterprise number – DUID-EN (2)
  - Link-layer Address – DUID-LL (3)

- Another type Universally Unique Identifier DUID-UUID(4) defined by **RFC 6355**



IPv6 address acquisition

Client & Server identifier options - Sample

ADVERTISE RELAY-MSG Sample with DUIDs:

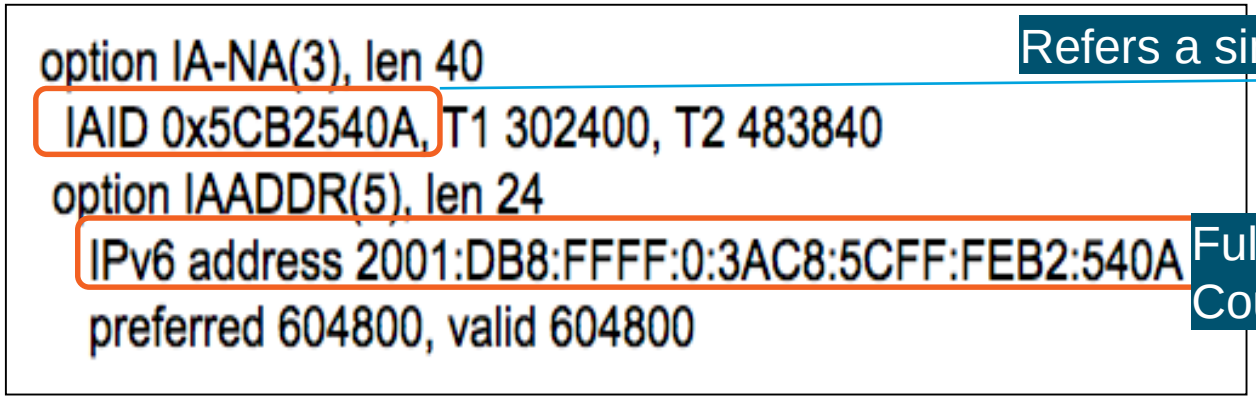
```
option RELAY-MSG(9), len 214
  type ADVERTISE(2), xid 4304265
  option CLIENTID(1), len 10
    0003000138C85CB2540A
  option SERVERID(2), len 14
    00010001134AAEE5005056B53D27
```

IPv6 address acquisition

Address options

DHCPv6 offer 3 types of Address bindings

- Identity Association Non-temporary Address (IA-NA)
- Identity Association Temporary Address (IA-TA)
- IA-PD: Identity Association Prefix Delegation (IA-PD)



IPv6 address acquisition

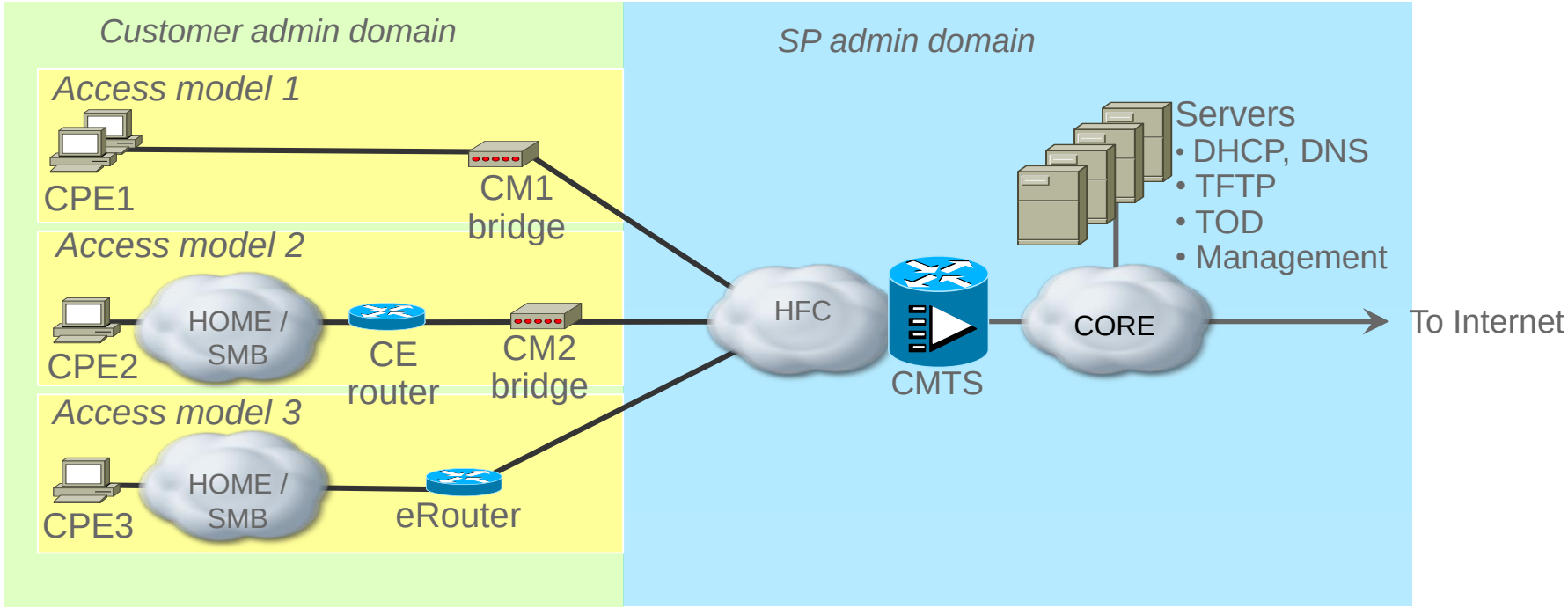
Prefix Delegation

- The **Prefix Delegation** option (IA-PD option 25) as defined by RFC 3633 has a similar structure to the IA-NA option and is **associated with one or more interfaces from the requesting router**

```
option IA-NA(3), len 40
    IAID 0x1BD6283B, T1 1800, T2 2880
    option IAADDR(5), len 24
      IPv6 address 2001:DB8:FFFE:0:B818:7159:D8F:1D4
      preferred 3600, valid 3600
  option IA-PD(25), len 41
    IAID 0x00000007, T1 302400, T2 483840
    option IAPREFIX(26), len 25
      preferred 604800, valid 1209600, prefix 2001:DB8:0:2000::/64
```

DOCSIS 3.0 IPv6 reference architecture

For Your Reference



IPv6 relevant CableLabs® specifications

For Your Reference

- DOCSIS 3.0 MAC and Upper Layers Protocol Interface (CM-SP-MULPIv3.0)
- DOCSIS 3.0 Operations Support System Interface (CM-SP-OSSIv3.0)
- DOCSIS 2.0 + IPv6 Cable Modem (CM-SP-DOCSIS2.0-IPv6)
- eDOCSIS (CM-SP-eDOCSIS)
- IPv4 and IPv6 eRouter (CM-SP-eRouter)
- PacketCable Multimedia (PKT-SP-MM)
- PacketCable 2.0 E-UE Provisioning Framework (PKT-SP-EUE-PROV)
- PacketCable 2.0 Dual-Stack IPv6 Architecture (PKT-TR-DS-IP6)
- OpenCable Host Device 2.1 Core Functional Requirements (OC-SP-HOST2.1-CFR)
- CableLabs' DHCP Options Registry (CL-SP-CANN-DHCP-Reg)

Embedded devices

- Embedded router (eRouter) is one type of embedded Service/Application Functional Entity (eSAFE) device
- eRouter is a Customer Edge (CE) router embedded with a cable modem
- RFC 7084 defines basic requirements for a CE router
- Other types of eSAFE devices include:
  - eMTA (Multimedia Terminal Adapter)
  - eDVA (Digital Voice Adapter)
  - eSTB (Set-Top Box)
- eSAFE devices undergo their own provisioning process which can be IPv4, IPv6, or dual-stack

DOCSIS 3.0 Multicast Model

Multicast DSID Forwarding (MDF)

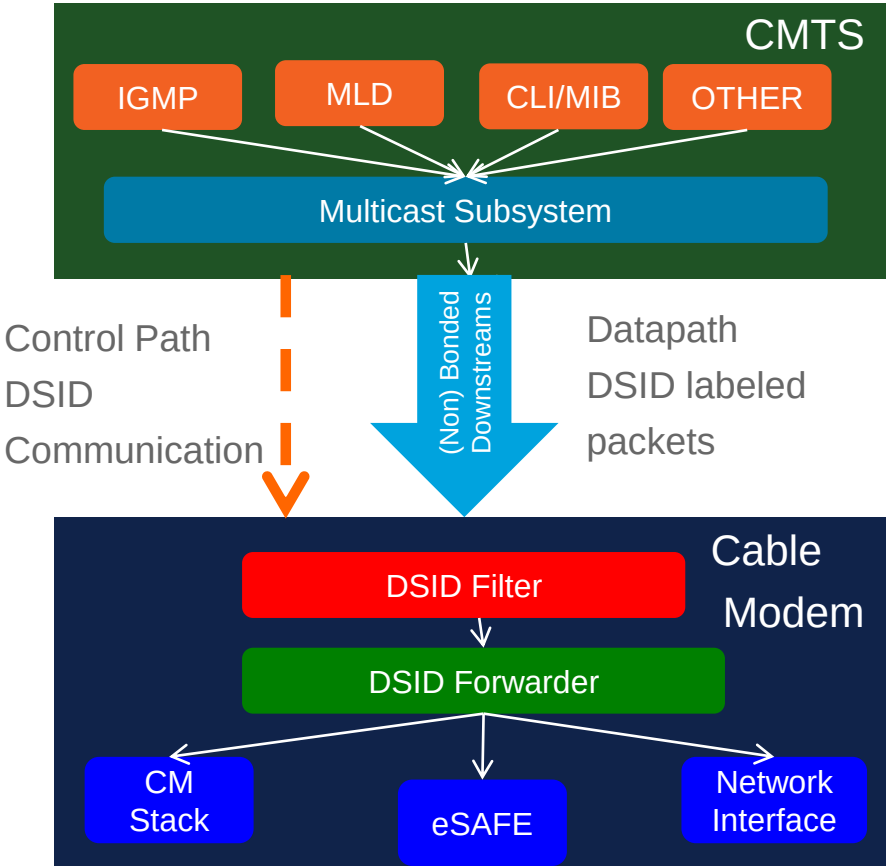
All Multicast packets are labeled with DSID

Static DSIDs:

- PreReg
- IGMPv1/v2
- IGMPv3
- MLDv1
- MLDv2

CMTS communicates DSIDs in 3-ways

- Mac Domain Descriptor (PreReg)
- REG-RSP (Other Static DSIDs)
- DBC-REQ (Dynamic DSIDs)



DSID labeled DOCSIS packet - Example

RA using PreReg

```
DOCSIS
   00.. .... = FCType: Packet PDU (0x00)
   ..00 000. = FCParm: 0
   .... ...1 = EHDRON: Extended Header Present
   Extended Header Length (bytes): 4
   Length after HCS (bytes): 94
   Extended Header
      1000 .... = Type: Reserved (8)
      .... 0011 = Length: 3
      Value: 09f018
   Header check sequence: 0x1c0d
Ethernet II, Src: Cisco_1a:0b:3f (00:12:00:1a:0b:3f), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::212:ff:fe1a:b3f (fe80::212:ff:fe1a:b3f), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
   Type: Router Advertisement (134)
   Code: 0
   Checksum: 0xccb2 [correct]
   Cur hop limit: 64
   Flags: 0xc8
   Router lifetime (s): 9000
   Reachable time (ms): 600000
   Retrans timer (ms): 0
   ICMPv6 Option (Source link-layer address : 00:12:00:1a:0b:3f)
   ICMPv6 Option (MTU : 1500)
```

```
#show cable multicast dsid Modular-Cable 5/1/0:4 static
Dsid    Stat Index    Type
0x9F014   64956       IGMPv1/v2
0x9F015   64957       IGMPv3
0x9F016   64958       MLDv1
0x9F017   64959       MLDv2
0x9F018   64960       PreReg
```

DOCSIS 2.0 + IPv6

For Your Reference

- IPv6 unsupported in DOCSIS prior to version 3.0
- D2.0 + IPv6 specification introduced to provide aspects of D3.0 required to support IPv6 for D2.0 modems
- Can operate in either MDF incapable (0) or MDF GMAC explicit (1) modes
- DOCSIS 3.0 modems operate in MDF GMAC promiscuous (2) mode

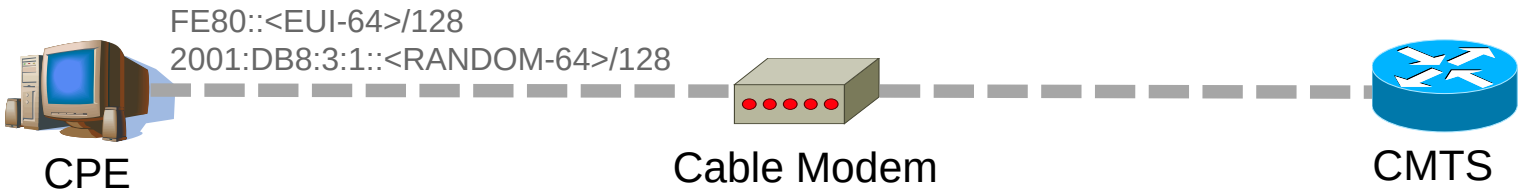
```
#show cable modem 5039.5566.31f4 ver  | inc MAC V|MDF
MAC Version                          : DOC2.0
MDF Capability Mode                  : 1
```

```
(config)#cable multicast mdf-disable ?
  DSG              DSG eCMs
  WB-Incapable-CM  Wideband Incapable modems only
```

IPv6 for CPEs

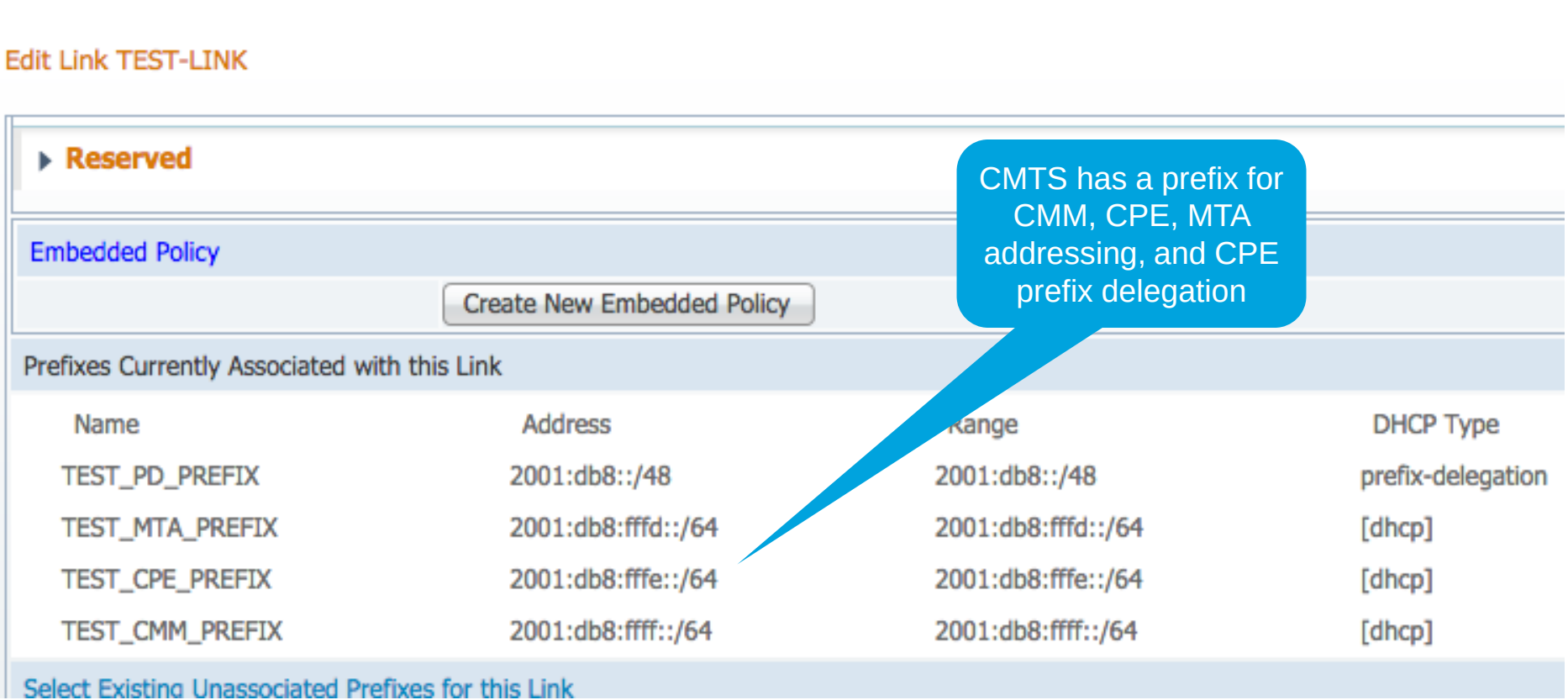
IPv6 CPE provisioning

- CPEs will have at least two IPv6 addresses
  - Link local IPv6 address
  - Link global IPv6 address learned via DHCPv6

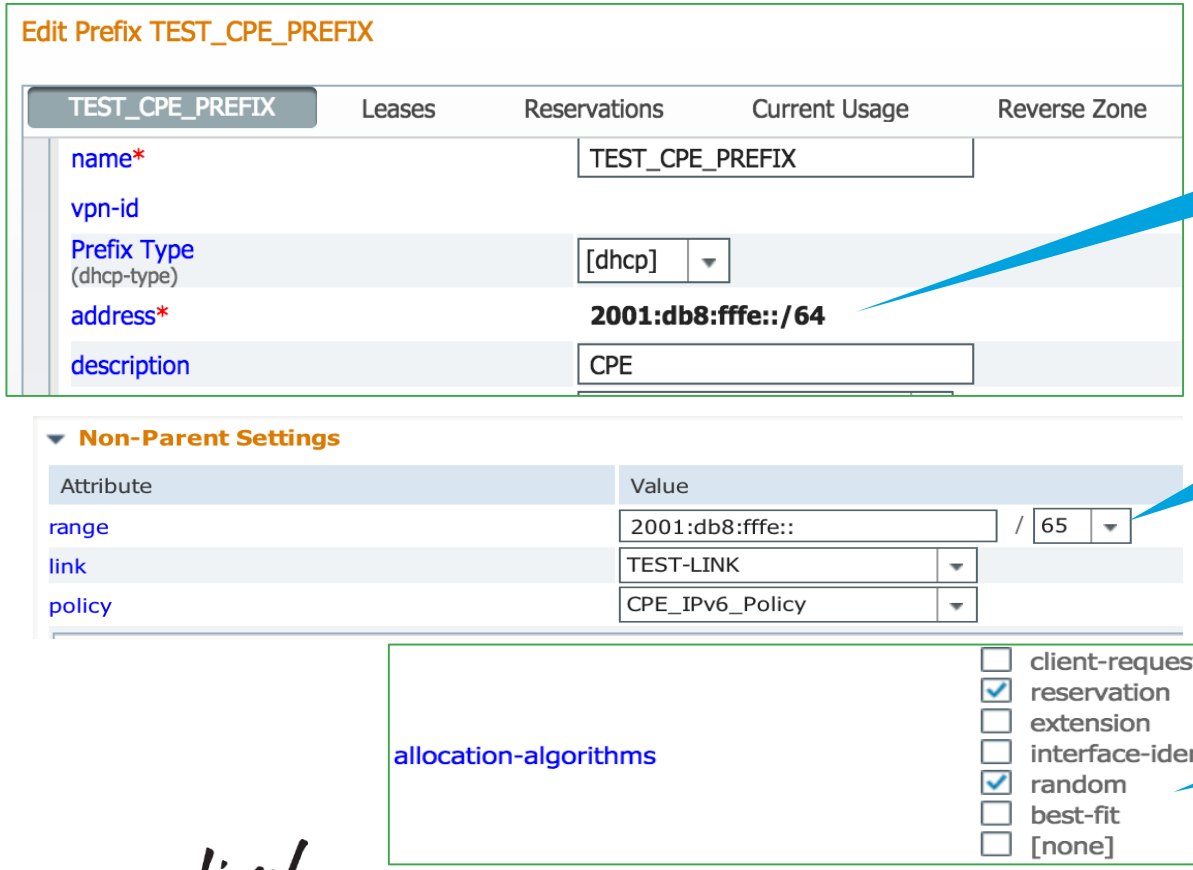


- For security reasons the SP may opt not to use the EUI-64 format for the interface-identifier portion of the global IPv6 address

CPNR example: DHCPv6 link



CPNR example: DHCPv6 prefix for CPE addresses

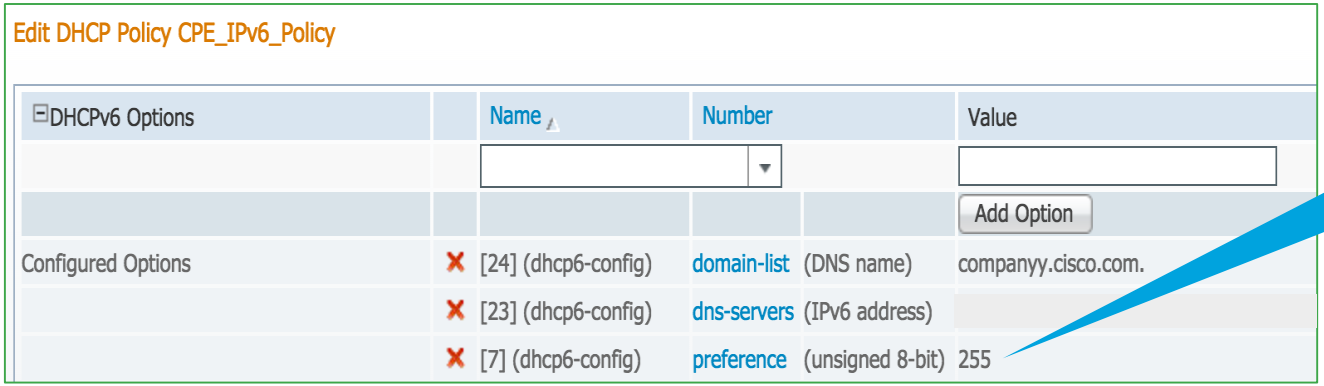


A /64 is recommended for simplicity

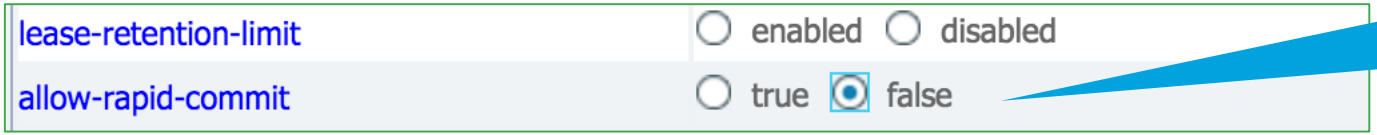
If no DHCPv6 Failover, allocate half the address range on this server; other half on the other server

Using randomly generated interface IDs provides security by not exposing the CPE manufacturer

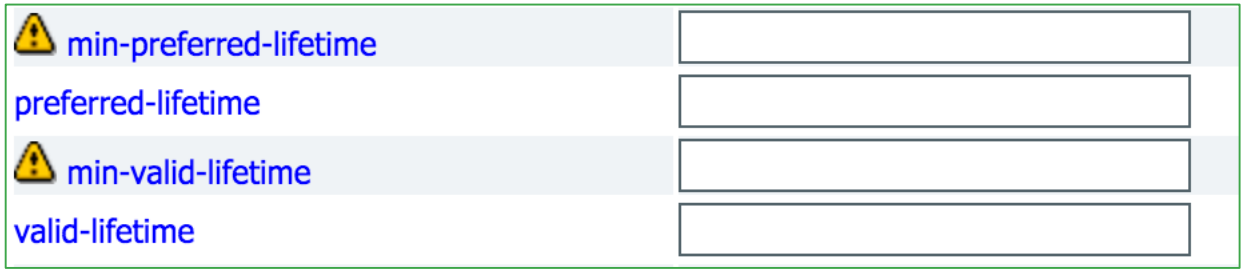
CPNR example: IPv6 policy for CPEs



Set preference option to maximum value to influence CPEs to use addresses from this server



If no DHCPv6 Failover and multiple DHCP servers Rapid Commit needs to be disabled



May opt to use longer lifetimes

Basic CMTS IPv6 configuration example

- Enable IPv6 globally

```
ipv6 unicast-routing
no ipv6 source-route
```

- Configure IPv6 on WAN and Loopback interfaces

```
interface TenGigabitEthernet0/0/0
   ipv6 address 2001:db8:1111:111D::1/127
   ipv6 nd ra suppress
   no ipv6 redirects
   no ipv6 unreachables

interface Loopback0
  ipv6 address 2001:db8:1111:FFFF::4/128
```

Infrastructure links:
- Recommended to use a separate address block for infrastructure and customers
- GUA is recommended for infrastructure links. ULA can be used but have some limitations (ex. PMTUD)

Point-to-point links:
- Current recommendation /64, /127
- Allocate /64 but configure /127.
- Some SP use /64

Loopback:
- Allocate /64 but configure /128

Basic CMTS Bundle interface configuration example

```
interface Bundle99
 no cable nd
 cable ipv6 source-verify dhcp
 cable ipv6 source-verify leasequery-filter upstream 3 5
 ipv6 address 2001:DB8:FFFD::1/64
 ipv6 address 2001:DB8:FFFE::1/64
 ipv6 address 2001:DB8:FFFF::1/64
 ipv6 traffic-filter security in
 ipv6 nd reachable-time 600000
 ipv6 nd dad attempts 0
 ipv6 nd prefix default no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 ipv6 nd ra interval 20
 ipv6 nd ra lifetime 9000
 no ipv6 redirects
 no ipv6 unreachables
 ipv6 verify unicast reverse-path
 ipv6 dhcp relay destination 2001:db8:1111:20C:29FF:FEB8:68DF
 ipv6 dhcp relay destination 2001:db8:1111:1111:250:56FF:FEB5:3D27
```

IPv6 ND configured on bundle interface

RA will not advertise any prefix since that is the only way to signal off-link to IPv6 hosts. BEST METHOD to prevent SLAAC

Traceroute tool will not work if IPv6 unreachables is disabled.

Basic IPv6 configuration

IPv6 parameters of bundle interface

```
CMTS#show ipv6 interface bundle 99
Bundle99 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::212:FF:FE1A:B3F
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:FFFE::1, subnet is 2001:DB8:FFFE::/64
    2001:DB8:FFFF::1, subnet is
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:2
    FF02::1:FF00:1
    FF02::1:FF1A:B3F
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are disabled
  ICMP unreachables are disabled
……..
```

Link local address is auto generated from MAC address (0012.001a.0b3f) of bundle interface

CMTS is joining several IPv6 multicast groups
FF02::1 – all-nodes on the local network
FF02::2 – all routers on the local network
FF02::1:2 - all DHCPv6 agents
FF02::1:FF00:1 - solicited-node multicast for link global address
FF02::1:FF1A:B3F– solicited-node multicast for link local address

Basic IPv6 configuration

IPv6 parameters of bundle interface continued

```
……
Input features: Verify Unicast Reverse-Path, Access List
 IPv6 verify source reachable-via rx,
   0 verification drop(s) (process),
   0 suppressed verification drop(s)
  Inbound access list security
  ND DAD is disabled
  ND reachable time is 600000 milliseconds
  ND advertised reachable time is 600000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 20 seconds
  ND router advertisements live for 9000 seconds
  ND advertised default router preference is High
  Hosts use DHCP to obtain routable addresses.
  Hosts use DHCP to obtain other configuration.
```

ipv6 nd dad attempts 0 - ND DAD is disabled
ipv6 nd reachable-time 600000 – 10 minutes
ipv6 nd ra interval 20 – RA is sent every 20 seconds
ipv6 nd ra lifetime 9000 – RA's lifetime is 9000 secs (2 ½ hrs)

Hosts must use DHCPv6
ipv6 nd managed-config-flag
ipv6 nd other-config-flag

Maintaining host & network database

IPv6 CPE show commands

```
CMTS#show interface cab 6/0/0 modem ipv6
SID  Type State          IPv6 Address                              M MAC address
49   CM  w-online(pt)    2001:DB8:FFFF:0:7EB2:1BFF:FE2D:DAC0       D 7cb2.1b2d.dac0
49   CPE unknown         2001:DB8:FFFE:0:95F6:33FA:6D0F:CBCE       D 0015.587e.9d30
50   CM  w-online(pt)    2001:DB8:FFFF:0:7EB2:1BFF:FE0A:B464       D 7cb2.1b0a.b464
50   CPE unknown         2001:DB8:FFFE:0:F060:7945:20B2:188        D 406c.8f49.25c1
```

```
CMTS#show cable modem 7cb2.1b0a.b464 cpe
IP address         MAC address      Dual IP     Device Class
24.35.0.238        406c.8f49.25c1     Y          Host
```

```
CMTS#show cable modem 7cb2.1b0a.b464 ipv6 cpe
MAC Address    IP Address
406c.8f49.25c1 2001:DB8:FFFE:0:F060:7945:20B2:188
```

Maintaining host & network database

IPv6 CPE show commands

```
CMTS#show ipv6 neighbors

IPv6 Address                              Age Link-layer Addr State Interface
FE80::426C:8FFF:FE49:25C1                  35 406c.8f49.25c1  REACH Bu99
2001:DB8:FFFE:0:95F6:33FA:6D0F:CBCE        14 0015.587e.9d30  REACH Bu99
2001:DB8:FFFE:0:F060:7945:20B2:188         34 406c.8f49.25c1  REACH Bu99
FE80::144C:B972:3F42:4971                 142 001c.2512.a794  STALE Bu99
FE80::215:58FF:FE7E:9D30                  135 0015.587e.9d30  STALE Bu99
2001:DB8:FFFE:0:3084:9310:46C9:3B20        21 001c.2512.a794  REACH Bu99
```

```
CMTS#show ipv6 neighbors statistics
IPv6 ND Statistics
 Entries 40, High-water 42, Gleaned 12, Scavenged 13, Static 38
 Entry States
   INCMP 0  REACH 40  STALE 0  GLEAN 0  DELAY 0  PROBE 0
 Resolutions
   Requested 4, timeouts 3, resolved 2, failed 1
   In-progress 0, High-water 1, Throttled 0, Data discards 1
 NUD
   Requested 7966, timeouts 20, resolved 7968, failed 4
   in-progress 1, high-water 3, throttled 0, current queue 0, queue high-water 0
```

Maintaining host & network database

IPv6 ND Gleaning

- ND cache entry is initially created when device is provisioned
- ND cache entry can be lost (e.g. CLI command, CM reload) and packet forwarding in DS can't resolve L2 address
- ND gleaning allows CMTS to recover lost information without the need to reload the CPE
- ND gleaning is enabled by default and controlled with the **[no] cable nd** command under bundle interface

IPv6 for CPE routers

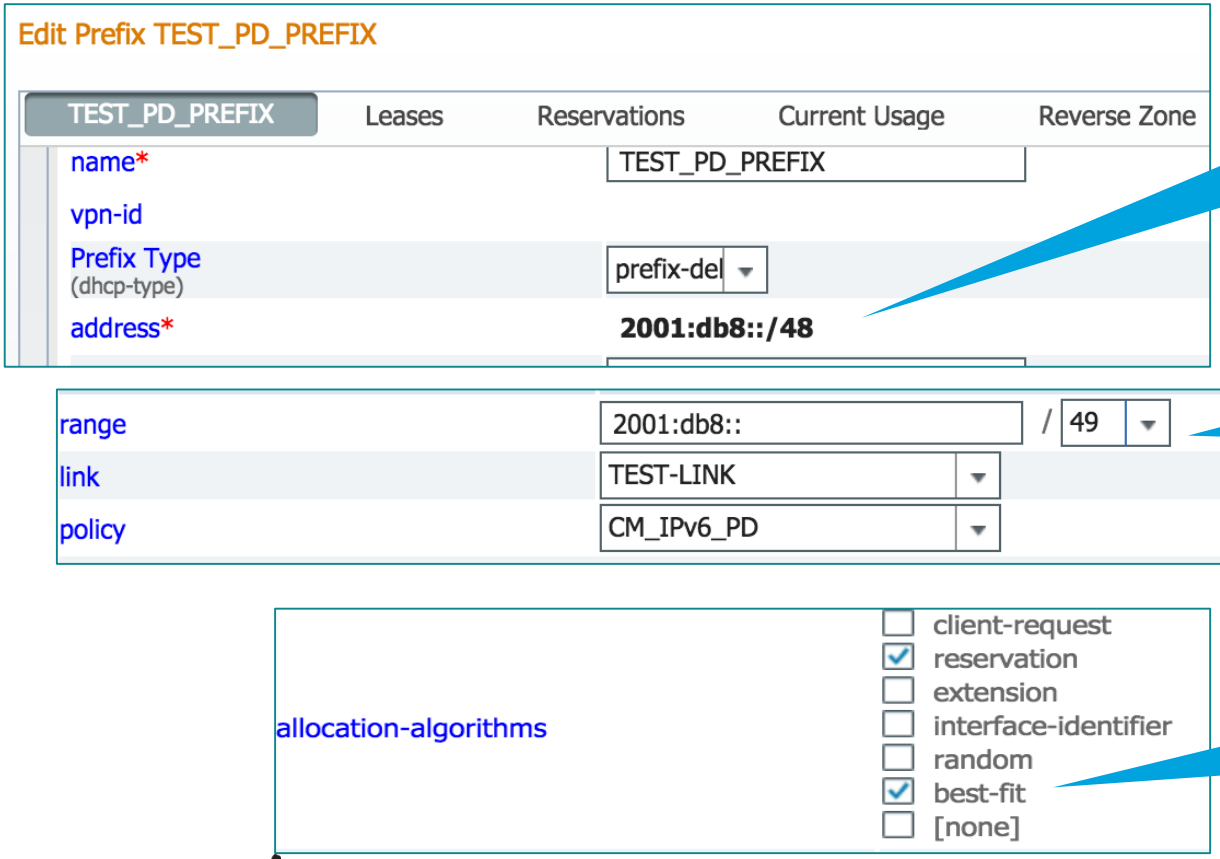
IPv6 in eRouter

Provisioning eRouter initialization mode

TLV 202 with sub-type "1" is used in Cable Modem configuration of eRouter to define eRouter initialization mode

Mode	IPv4 Behavior	IPv6 Behavior
Disabled (0)	CM bridges all traffic	CM bridges all traffic
IPv4 Protocol Enabled (1)	IPv4 traffic forwarded via NAPT	IPv6 traffic not forwarded
IPv6 Protocol Enabled (2)	IPv4 traffic not forwarded	IPv6 traffic forwarded
Dual IP Protocol Enabled (3)	IPv4 traffic forwarded via NAPT	IPv6 traffic forwarded

CPNR Example: DHCPv6 prefix for prefix delegation

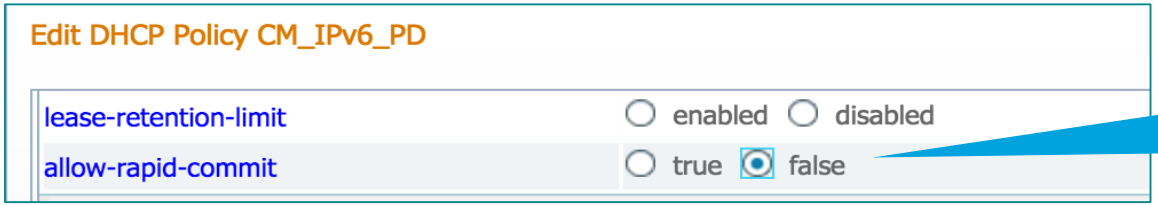


Choose a prefix length which should be more than enough for the foreseeable future

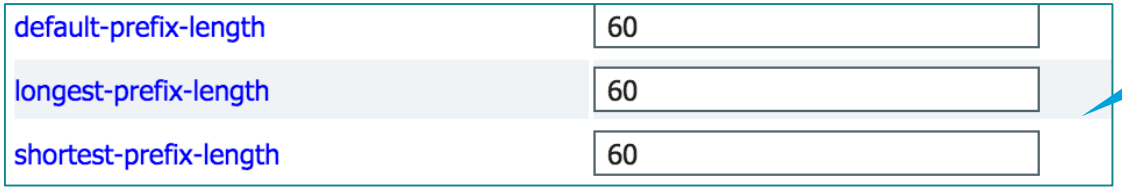
If no DHCPv6 Failover, allocate half the address range on this server; other half on the other server

The “best-fit” algorithm is used to determine the right sized prefix to delegate based upon what was requested

CPNR Example: IPv6 policy for CPE PD

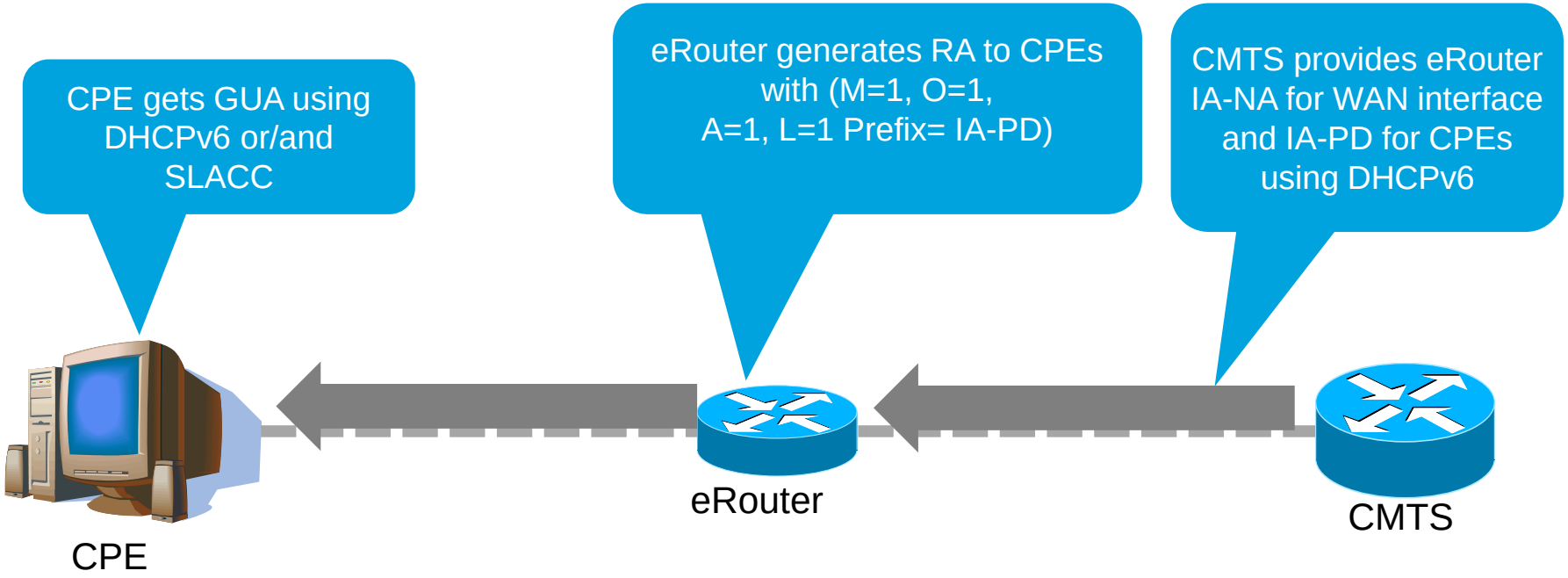


If no DHCPv6 Failover and multiple DHCP servers Rapid Commit needs to be disabled



Can define the allowable range of delegated prefix size as well as a default size

IPv6 in eRouter

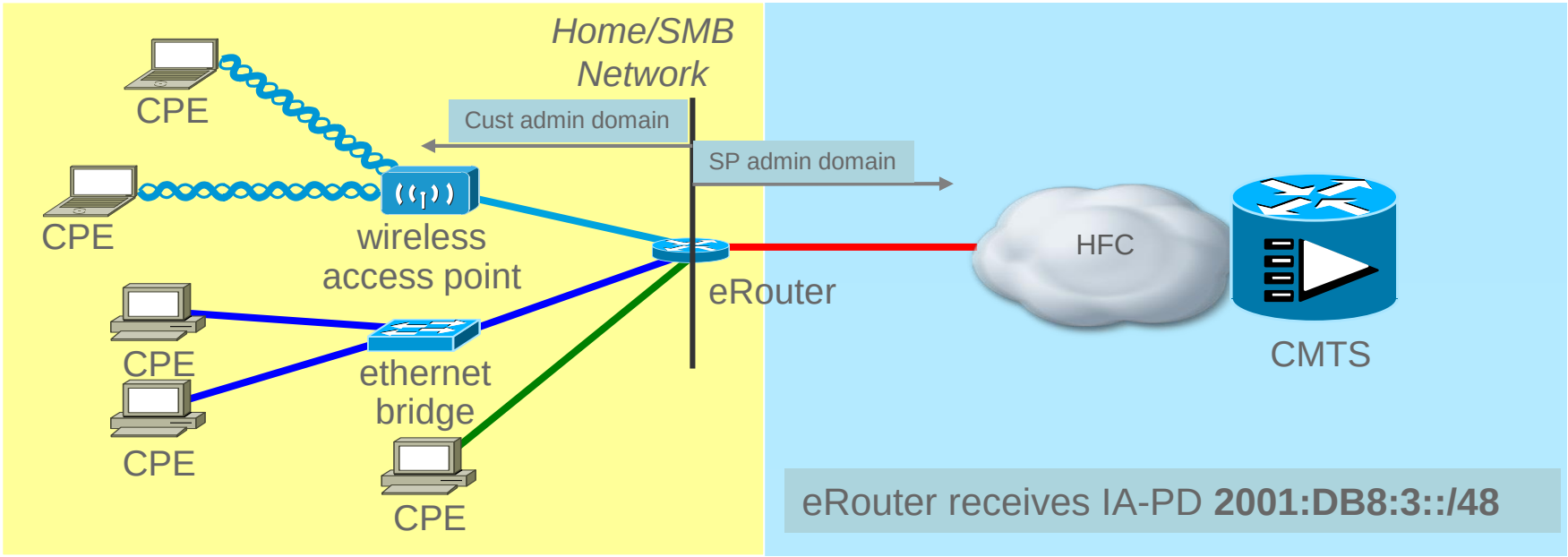


- If CPE is offered to do SLAAC then CPE might get 2 addresses per prefix (one temporary and one permanent (Host OS dependent)

RFC 7084 – Basic Requirements for IPv6 Customer Edge Routers

IPv6 in eRouter

Prefix Delegation example



HFC link

Customer network link 1; assigned 2001:DB8:3:0::/64

Customer network link 2; assigned 2001:DB8:3:1::/64

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

IPv6 Prefix Delegation

DHCPv6 Solicit Packet Example

```
+- Start of RELAY-FORW (12) message (345 bytes)
|    hop-count 0,
|    link-address 2001:db8:fffe::1,
|    peer-address fe80::3ac8:5cff:feb2:540e
|  relay-message (9) option (256 bytes)
|  +- Start of SOLICIT (1) message (256 bytes)
|  |    transaction-id 13356830
|  |  rapid-commit (14) option (0 bytes)
|  |  reconfigure-accept (20) option (0 bytes)
|  |  oro (6) option (8 bytes)
|  |    17,23,24,25
|  |  vendor-class (16) option (16 bytes)
|  |    (enterprise-id 4491,
|  |    ((00:0a:65:52:6f:75:74:65:72:31:2e:30)))
|  |  vendor-opts (17) option (127 bytes)
|  |    (enterprise-id 4491,
|  |    ((device-type 2 EROUTER),
|  |    (embedded-components-list 3 ECM:EROUTER),
|  |    (device-serial-number 4 231638530),
|  |    (hardware-version-number 5 1.0),
|  |    (software-version-number 6 D3925-P15-5-v302r125
|  |    (boot-rom-version 7 2.3.0_R1),
|  |    (vendor-oui 8 0011E6),
|  |    (model-number 9 DPC3925),
|  |    (vendor-name 10 Cisco)))
|  |  client-identifier (1) option (10 bytes)
|  |    00:03:00:01:38:c8:5c:b2:54:0e
|  |  ia-pd (25) option (41 bytes)
|  |    (iaid 1555190799, t1 0, t2 0)
|  |    iaprefix (26) option (25 bytes)
|  |      (preferred-lifetime 0,
|  |      valid-lifetime 0,
|  |      prefix-length 56,
|  |      prefix ::)
|  |  ia-na (3) option (12 bytes)
|  |    (iaid 1555190798, t1 0, t2 0)
|  |  elapsed-time (8) option (2 bytes)
|  |    0
|  +- End of SOLICIT message
|  interface-id (18) option (21 bytes)
|    42:75:39:39:26:43:61:36:2f:30:2f:30:00:38:c8:5c:b2:54:0e:00:00
|  vendor-opts (17) option (22 bytes)
|    (enterprise-id 4491,
|    ((cmts-capabilities 1025 01:02:03:00),
|    (cm-mac-address 1026 38:c8:5c:b2:54:0a)))
+- End of RELAY-FORW message
```

eRouter indicating desired prefix length

IPv6 Prefix-Delegation

DHCPv6 ADVERTISE Packet Example

```
+- Start of ADVERTISE (2) message (232 bytes)
|    transaction-id 13356830
| client-identifier (1) option (10 bytes)
|    00:03:00:01:38:c8:5c:b2:54:0e
| server-identifier (2) option (14 bytes)
|    00:01:00:01:13:4a:ae:e5:00:50:56:b5:3d:27
| ia-na (3) option (40 bytes)
|    (iaid 1555190798,
|    t1 2d6h14m,
|    t2 3d14h46m24s)
|    iaaddr (5) option (24 bytes)
|       (address 2001:db8:fffe:0:e5a1:df2b:5099:2f8e,
|       preferred-lifetime 4d12h28m1s,
|       valid-lifetime 1w4d12h28m1s)
| ia-pd (25) option (41 bytes)
|    (iaid 1555190799, t1 29m4s, t2 46m31s)
|    iaprefix (26) option (25 bytes)
|       (preferred-lifetime 58m9s,
|       valid-lifetime 58m9s,
|       prefix-length 60,
|       prefix 2001:db8:0:8000::)
| reconfigure-accept (20) option (0 bytes)
| preference (7) option (1 bytes)
|    0
| vendor-opts (17) option (32 bytes)
|    (enterprise-id 4491,
|    ((time-offset 38 -5h),
|    (syslog-servers 34 fc00:1111:1111:1111:203:baff:fe67:e489)))
| dns-servers (23) option (32 bytes)
|    fc00:1111:1111:1111:250:56ff:feb5:5318,fc00:1111:1111:1111:250:56ff:feb5:5310
| domain-list (24) option (22 bytes)
|    company-v6.cisco.com.
+- End of ADVERTISE message
```

IA_NA for eRouter

IA-PD with /60 prefix length is delegated

IPv6 prefix delegation

Gleaning Process in CMTS

- CMTS as a DHCPv6 relay agent is aware of all IPv6 address assignments AND delegated prefixes
- Gleaned addresses populate the IPv6 neighbor cache and cable modem host database
- Gleaned prefix delegations automatically inserted into the IPv6 routing table as static routes and also included in the cable modem host database
- These static routes then need to be redistributed into the routing protocol to provide global connectivity (will likely want to aggregate as well)

IPv6 Prefix Delegation

PD route recovery

- Unknown IPv6 addresses for directly connected CPEs can be determined based upon the prefixes configured on the Bundle interface
- However, this is not the case with prefix delegation
  - If the static route learned during DHCPv6 gleaning is lost traffic for this prefix would most likely end up following the default route
- On uBR10002, Issue can be prevented by using the **cable ipv6 pd-route** configuration on uBR10002 platform.

```
<config> cable ipv6 pd-route 2001:db8:3::/48 Bundle99
```

- On cBR-8, CLI **cable ipv6 pd-route** is deprecated, instead **configure static summary route** to the bundle interface.

```
<config> ipv6 route 2001:db8:3::/48 Bundle99
```

Maintaining host & network database

IPv6 DHCPv6 IA_PD gleaning and IPv6 RIB

```
CMTS#show ipv6 route static
IPv6 Routing Table - default - 18 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   2001:DB8::/48 [1/0]
     via Bundle99, directly connected
S   2001:DB8::/60 [1/0]
     via FE80::3AC8:5CFF:FEB2:727A, Bundle99
S   2001:DB8:0:10::/60 [1/0]
     via FE80::3AC8:5CFF:FEB2:540E, Bundle99

CMTS#show cable modem ipv6 prefix
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP

MAC Address    Type IPv6 prefix
38c8.5cb2.727a R/D  2001:DB8::/60
38c8.5cb2.540e R/D  2001:DB8:0:10::/60
```

Maintaining host & network database

IPv6 DHCPv6 IA_PD gleaning and IPv6 RIB

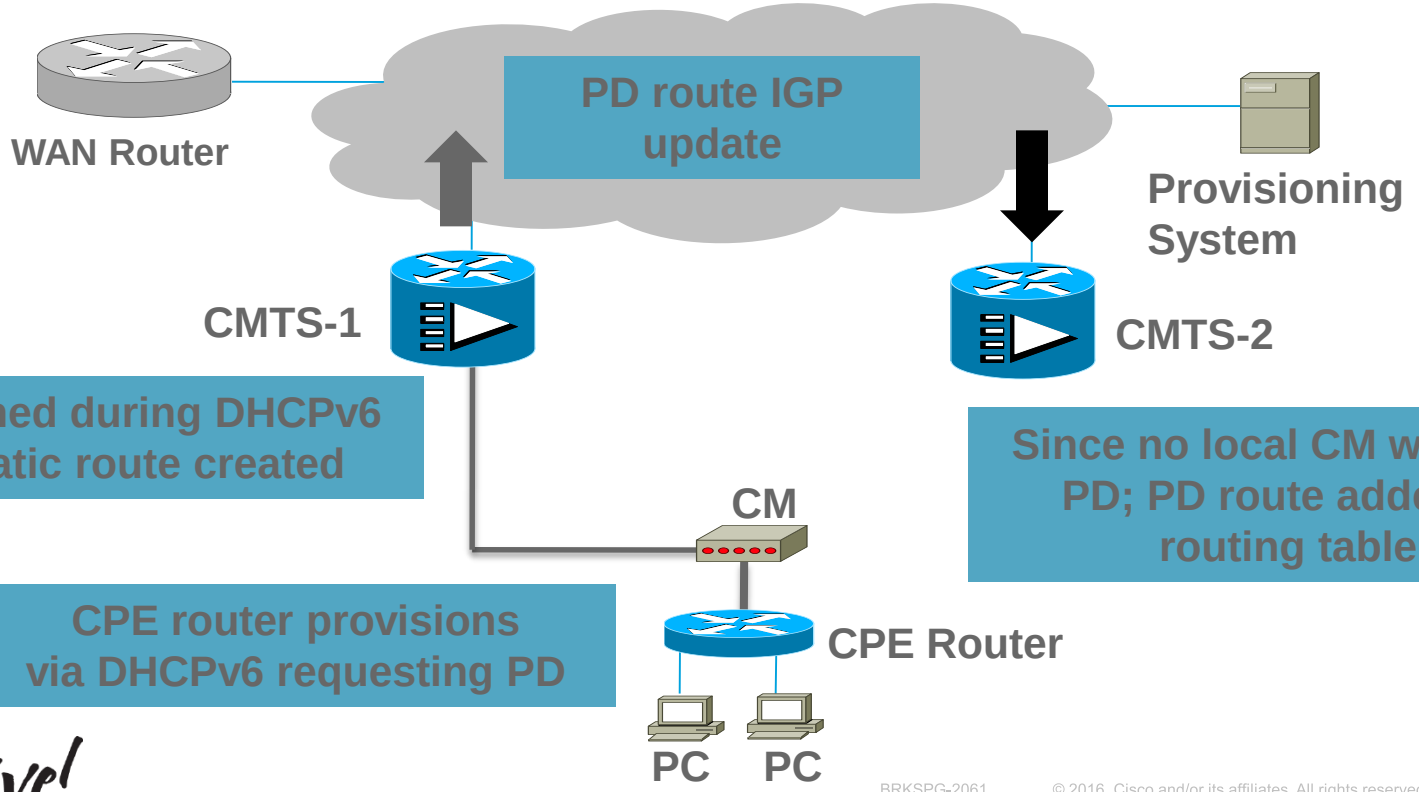
```
CMTS#show cable modem 38c8.5cb2.540a ipv6 prefix
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP

MAC Address     Type IPv6 prefix
38c8.5cb2.540e R/D  2001:DB8:0:10::/60

CMTS#show ipv6 route summary
IPv6 routing table name is default(0) global scope - 18 entries
IPv6 routing table default maximum-paths is 16
Route Source    Networks    Overhead    Memory (bytes)
connected       3           288         384
local           5           480         640
ospf 1          7           672         896
  Intra-area: 4  Inter-area: 1  External-1: 0  External-2: 0
  NSSA External 1: 0  NSSA External 2: 2
static          3           288         384
  Static: 3  Per-user static: 0
Total           18          1728        2304

  Number of prefixes:
    /0: 1, /8: 1, /48: 1, /60: 2, /62: 2, /64: 7, /128: 4
```

IPv6 prefix stability

- Typically a range of IPv6 prefixes available for delegation are allocated to a particular CMTS
- Thus if a CPE router is moved from CMTS “A” to CMTS “B” due to a node-split by the MSO it’s delegated prefix changes
  - Node-splits are where a SP alters the RF plant resulting in a portion of the customer moving to a new MAC domain in order to alleviate congestion
  - This behavior could be problematic for some end customers; such as a business customer that requires it’s addressing to remain constant

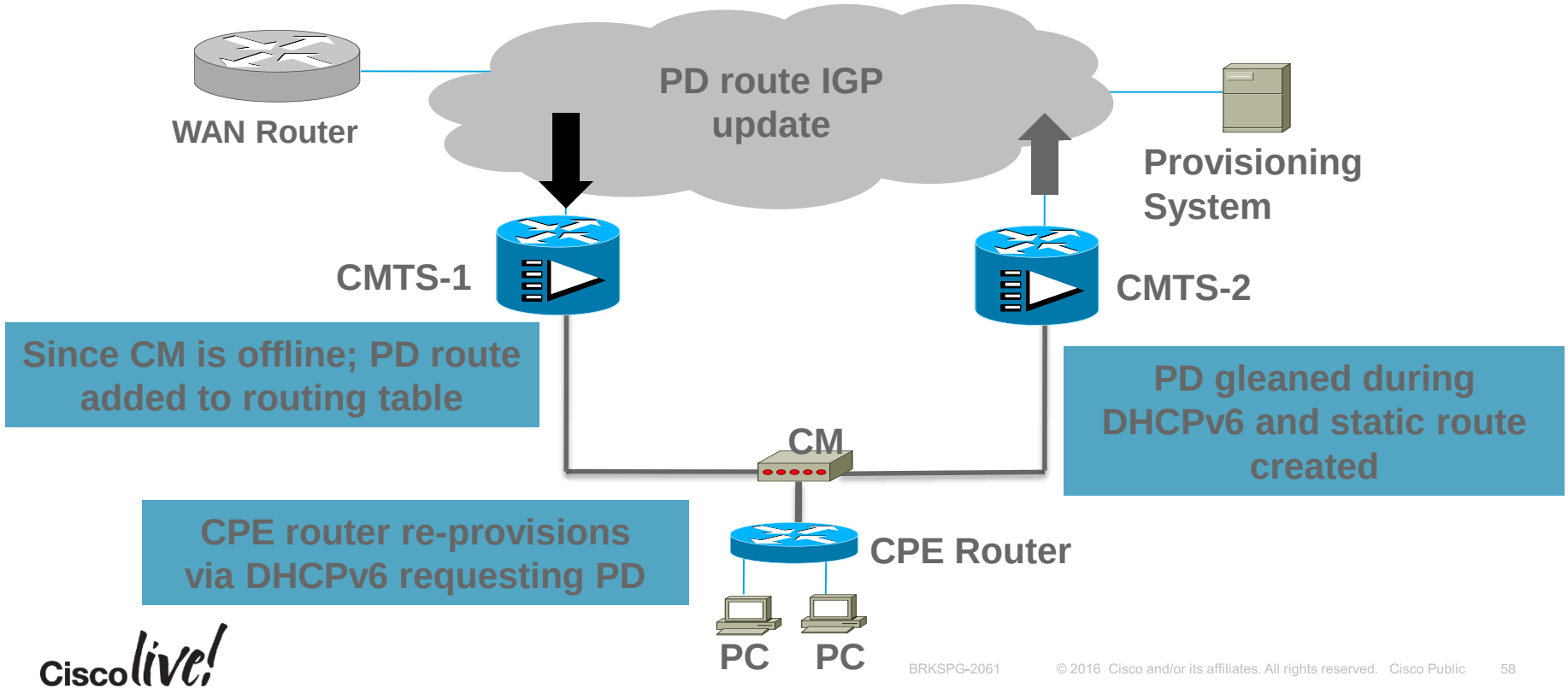
IPv6 Prefix Stability

CM and CPE router online on CMTS-1



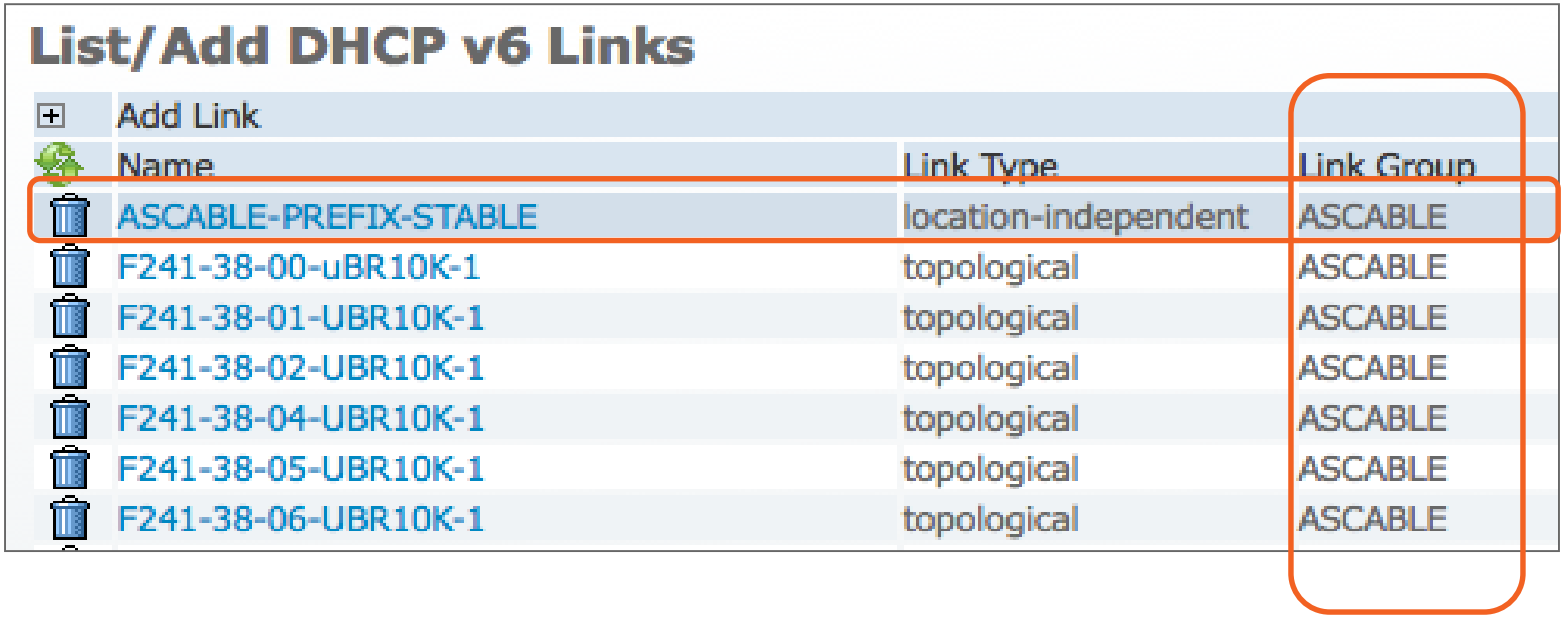
IPv6 Prefix Stability

CM and CPE router move to CMTS-2



IPv6 Prefix stability

CPNR Configuration



IPv6 Source Address Verification (SAV)

For Your Reference

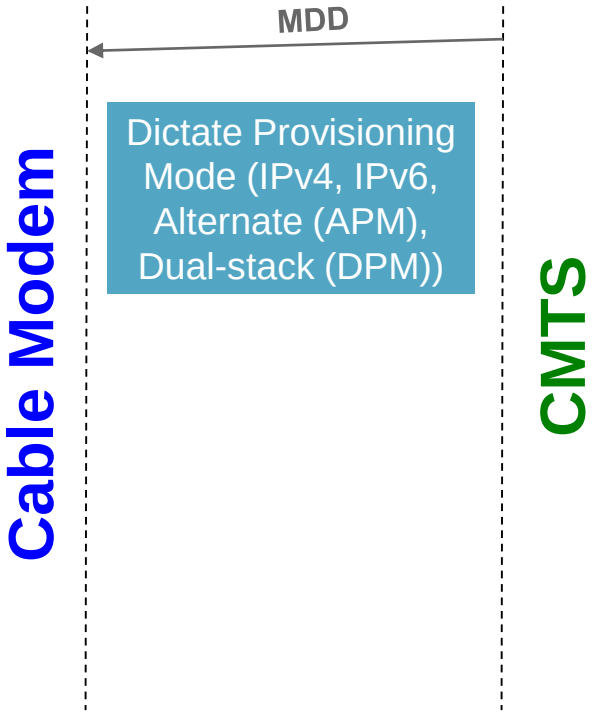
Static IPv6

- 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 the Source Address Verification (SAV) feature
  - (1) CM configuration file includes a TLV (43.7.1) that identifies the SAV Prefix group name that the CM belongs to. The prefixes in the group are configured on the CMTS. - **cable source-verify group <group-name>**
  - (2) CM configuration file includes a TLV (43.7.2) that provides the actual prefix
- Enabled with global CLI: **cable source-verify enable-sav-static**

IPv6 for cable modem management

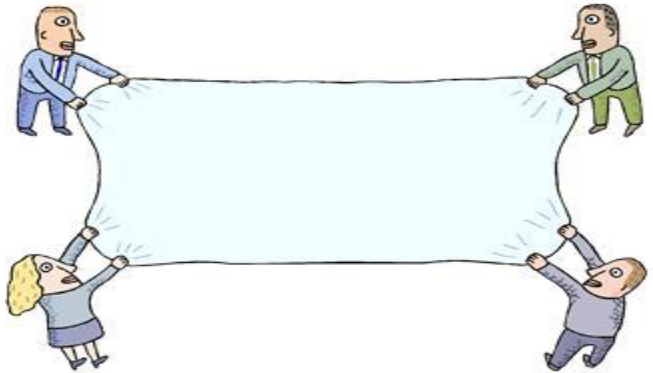
DOCSIS cable modem provisioning

- CMTS periodically sends MDD messages which dictate CM IP establishment procedure
- Controlled by **cable ip-init <>** configuration under the cable interface
- If the CM does not receive any MDD messages from the CMTS it operates in DOCSIS 2.0 mode



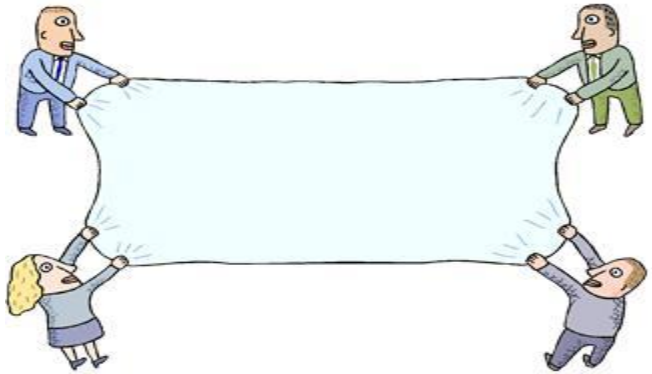
Dual-stack Provisioning Mode (DPM)

- 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
- Useful during the transition period until confidence is gained in IPv6 management infrastructure; will NOT result in freeing up IPv4 addresses
- Supported in Cisco Prime Cable Provisioning release 5.1



Alternate Provisioning Mode (APM)

- CM first attempts to provision using IPv6 and if that fails reverts to provisioning using IPv4
- If able to provision using IPv6 no IPv4 address is acquired
- Useful during the transition period until confidence is gained in IPv6 management infrastructure and unlike DPM will most likely result in the savings of IPv4 address space



MDD message example

- CMTS periodically sends MDD messages which dictate CM IP establishment procedure for all DOCSIS 3.0 and DOCSIS 2.0+ CMs

```
MDD MESSAGE
  <snip>
    dcid                          - 8
    MDD TLV, Total TLV size - 379
    MDD TLV
      Downstream Active Channel List
        Channel ID:               1
        Frequency:                687000000Hz
        Modulation Order/Annex:   256 QAM/Annex B
        Primary Capable:          Primary-Capable
  <snip>
      Downstream Active Channel List
        Channel ID:               8
        Frequency:                729000000Hz
        Modulation Order/Annex:   256 QAM/Annex B
        Primary Capable:          Primary-Capable
        CM-STATUS Event Bitmask:0x36
                                  MDD Timeout
                                  QAM FEC failure
                                  MDD Recovery
                                  QAM FEC recovery
      MAC Domain Downstream Service Group
        MD-DS-SG ID:              1
        Channel IDs:              1
                                  2
                                  3
                                  4
                                  5
                                  6
                                  7
                                  8
  <snip>
      IP Initialization Parameters
        IP Provisioning Mode:     IPv6
        Pre-Registration DSID:    585767
  <snip>
```

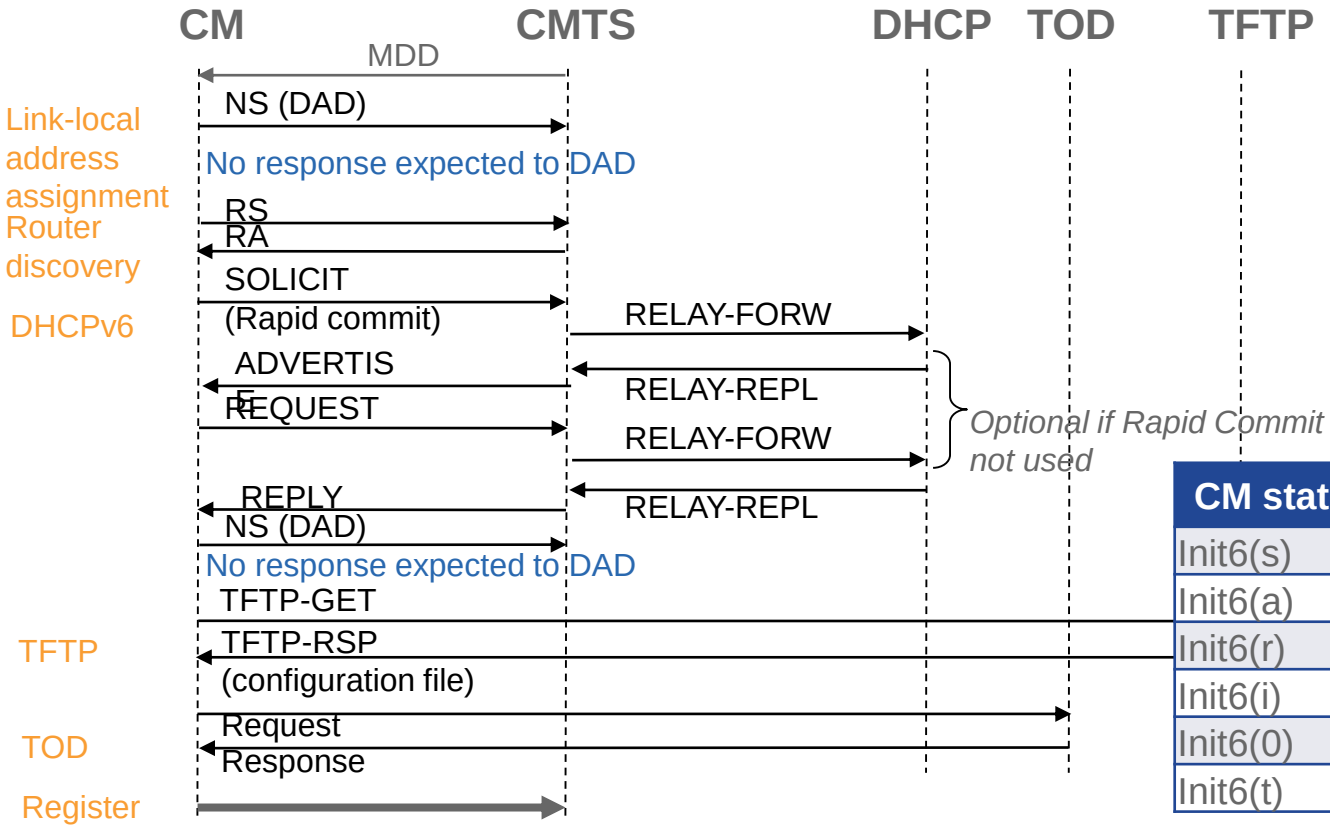
IP Provisioning Mode set to IPv6
Pre-Registration DSID included

MDD override

- **The IP provisioning mode in the MDD message will affect all DOCSIS 3.0 and DOCSIS 2.0+ modems in the MAC domain**
- Can have tighter control via SNMP setting in cable modem configuration file or SNMP Set (DOCS-IF3-MIB::docsIf3CmMdCfgIpProvMode)

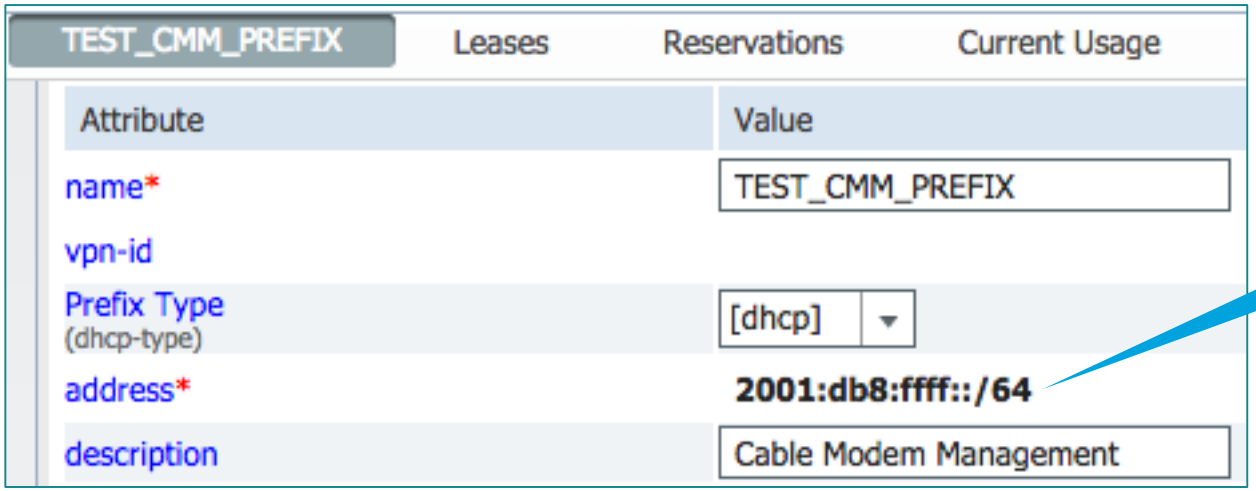
docsIf3CmMdCfgIpProvMode	Value
honorMDD (Default)	0
ipv4	1
ipv6	2
Alternate Provisioning Mode	3
Dual Stack Provisioning Mode	4

CM IPv6 provisioning and registration:



CM states	Description
Init6(s)	DHCPv6 Solicit
Init6(a)	DHCPv6 Advertise
Init6(r)	DHCPv6 Request
Init6(i)	DHCPv6 Reply
Init6(0)	TFTPv6 read request
Init6(t)	TODv6 request

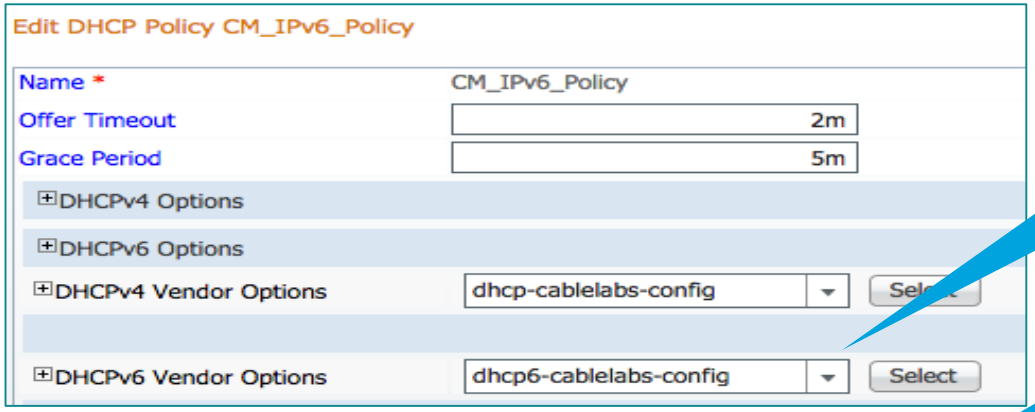
CPNR example: DHCPv6 prefix for CMM addressing



A /64 is recommended for simplicity

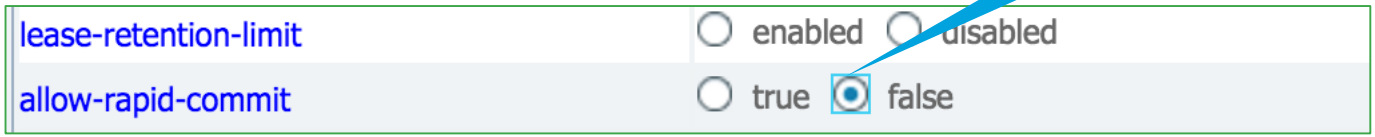
The EUI-64 interface ID format allows server redundancy w/o fear of overlap

CPNR example: IPv6 policy for CMM

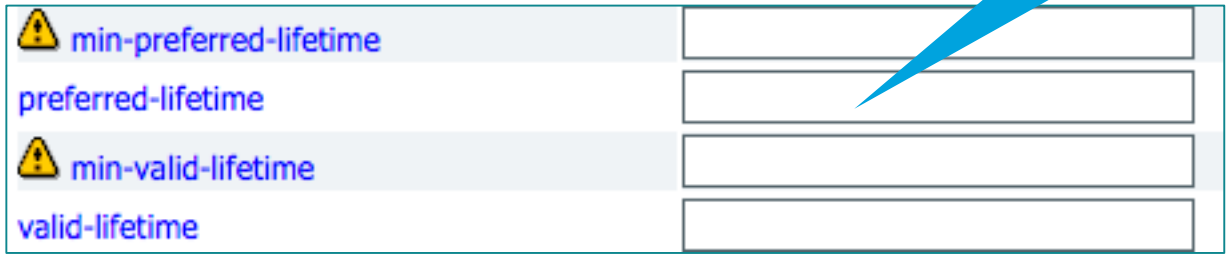


CableLabs DHCP options such as time offset, syslog server, etc. defined here

If multiple DHCP servers and no DHCPv6 Failover Rapid Commit needs to be disabled



May opt to use longer lifetimes



Basic CMTS Cable interface configuration example

- Configure Cable interfaces

```
Interface Cable6/0/0
  cable ip-init ipv6
```

cable ip-init mac-domain configuration is for CM management stack only.

This configuration NOT needed if only doing IPv6 for CPE

```
(config-if)#cable ip-init ?
  apm          Alternate Provisioning mode
  dual-stack   Dual-stack Provisioning mode
  ipv4         IPv4 Provisioning mode
  ipv6         IPv6 Provisioning mode
```

How to determine if CM is IPv6 enabled?

```
CMTS#show cable modem cab 6/0/0
                                          D
MAC Address    IP Address     I/F           MAC            Prim RxPwr  Timing Num I
                                            State          Sid  (dBmv) Offset CPE P
7cb2.1b2d.dac0 ---            C6/0/0/U1     w-online(pt)   49   0.00   1580   2   N
7cb2.1b0a.b464 ---            C6/0/0/U1     w-online(pt)   50   -0.50  1499   0   N
001e.6bfb.0872 ---            C6/0/0/U1     w-online(pt)   52   0.00   1732   0   N
0025.2e12.4b04 13.35.0.9      C6/0/0/U1     w-online(pt)   53   0.00   1490   1   N
38c8.5cb2.540a ---            C6/0/0/U1     w-online(pt)   63   -0.50  1475   1   N
```

```
CMTS#show cable modem cab 6/0/0 ipv6
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP

MAC Address    Type Interface     Mac State     D/IP IP Address
7cb2.1b2d.dac0 B/D  C6/0/0/U1     w-online(pt)   N  2001:DB8:FFFF:0:7EB2:1BFF:FE2D:DAC0
7cb2.1b0a.b464 B/D  C6/0/0/U1     w-online(pt)   N  2001:DB8:FFFF:0:7EB2:1BFF:FE0A:B464
38c8.5cb2.540a B/D  C6/0/0/U1     w-online(pt)   N  2001:DB8:FFFF:0:3AC8:5CFF:FEB2:540A
001e.6bfb.0872 B/D  C6/0/0/U1     w-online(pt)   N  2001:DB8:FFFF:0:21E:6BFF:FEFB:872
0025.2e12.4b04 B/D  C6/0/0/U1     w-online(pt)   N  ---
```

Maintaining host & network database

IPv6 ND cache

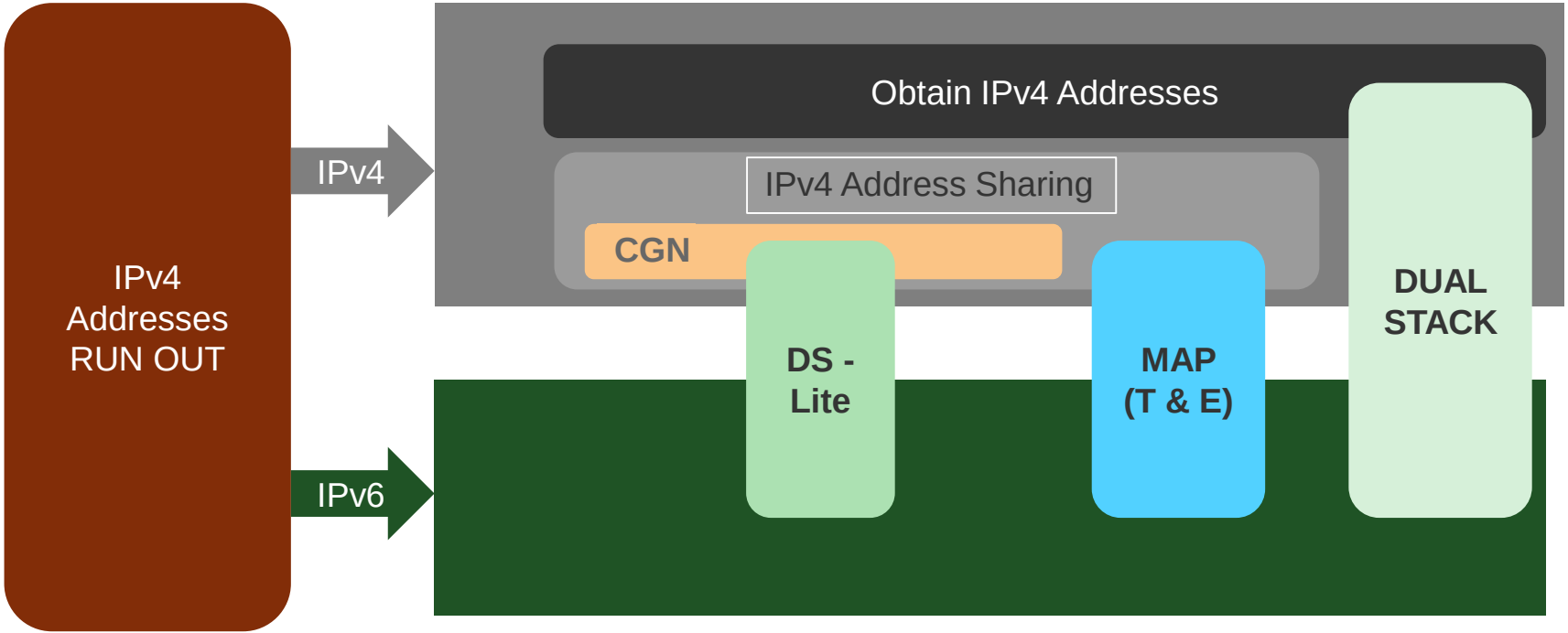
```
CMTS#show ipv6 neighbors

IPv6 Address                                Age Link-layer Addr State Interface
FE80::7EB2:1BFF:FE2D:DAC0                     - 7cb2.1b2d.dac0  REACH Bu99
FE80::21E:6BFF:FEFB:872                       - 001e.6bfb.0872  REACH Bu99
2001:DB8:FFFF:0:7EB2:1BFF:FE0A:B464           - 7cb2.1b0a.b464  REACH Bu99
FE80::3AC8:5CFF:FEB2:540A                     - 38c8.5cb2.540a  REACH Bu99
2001:DB8:FFFF:0:7EB2:1BFF:FE2D:DAC0           - 7cb2.1b2d.dac0  REACH Bu99
FE80::7EB2:1BFF:FE0A:B464                     - 7cb2.1b0a.b464  REACH Bu99
2001:DB8:FFFF:0:3AC8:5CFF:FEB2:540A           - 38c8.5cb2.540a  REACH Bu99
2001:DB8:FFFF:0:21E:6BFF:FEFB:872             - 001e.6bfb.0872  REACH Bu99
```

show ipv6 neighbors displays the ND cache and state follows the NUD algorithm

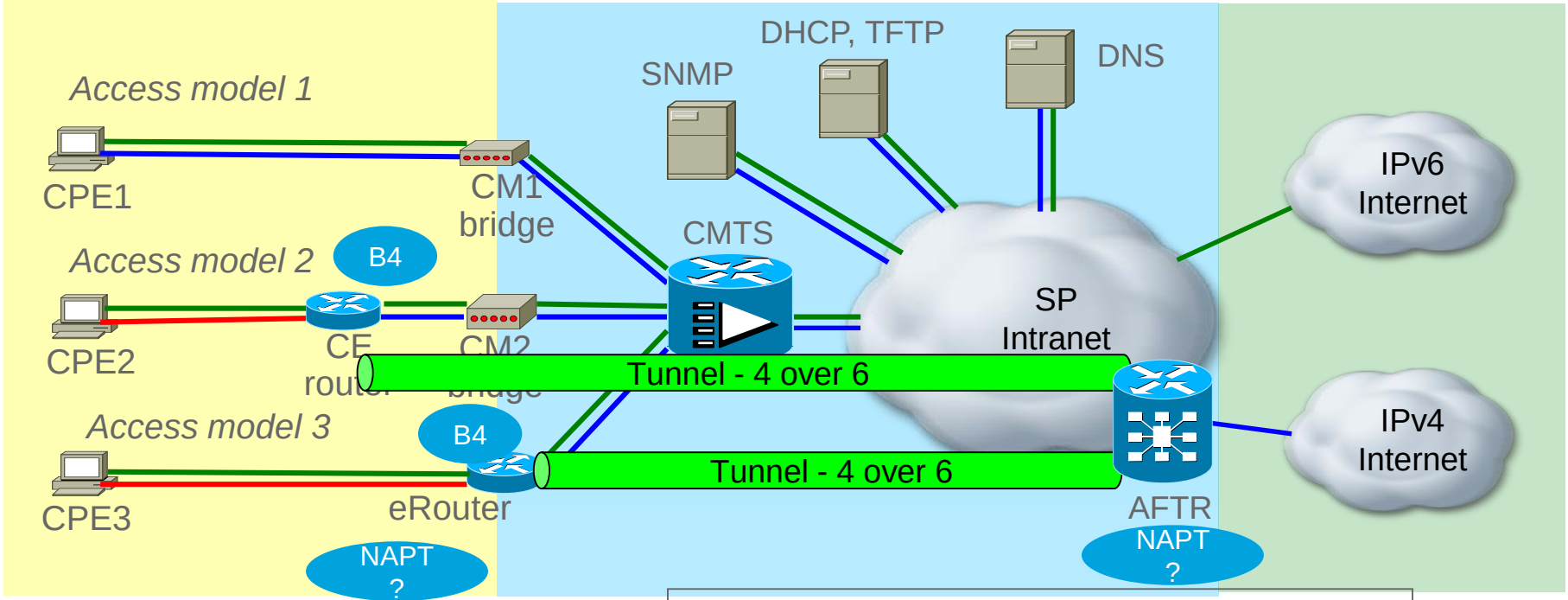
Starting with the SCG1 (ubr10k) release NUD is no longer used to maintain neighbors for cable modems; the entries are static and remain as long as the modem is online; can only removed by a **clear cable modem <> delete** or by being “offline” for the SID inactivity period of 24 hours

IPv6 transition and strategies

Transition Strategies



Transition Strategy – Service Provider “X”



Public IPv4 space used for CMM reclaimed

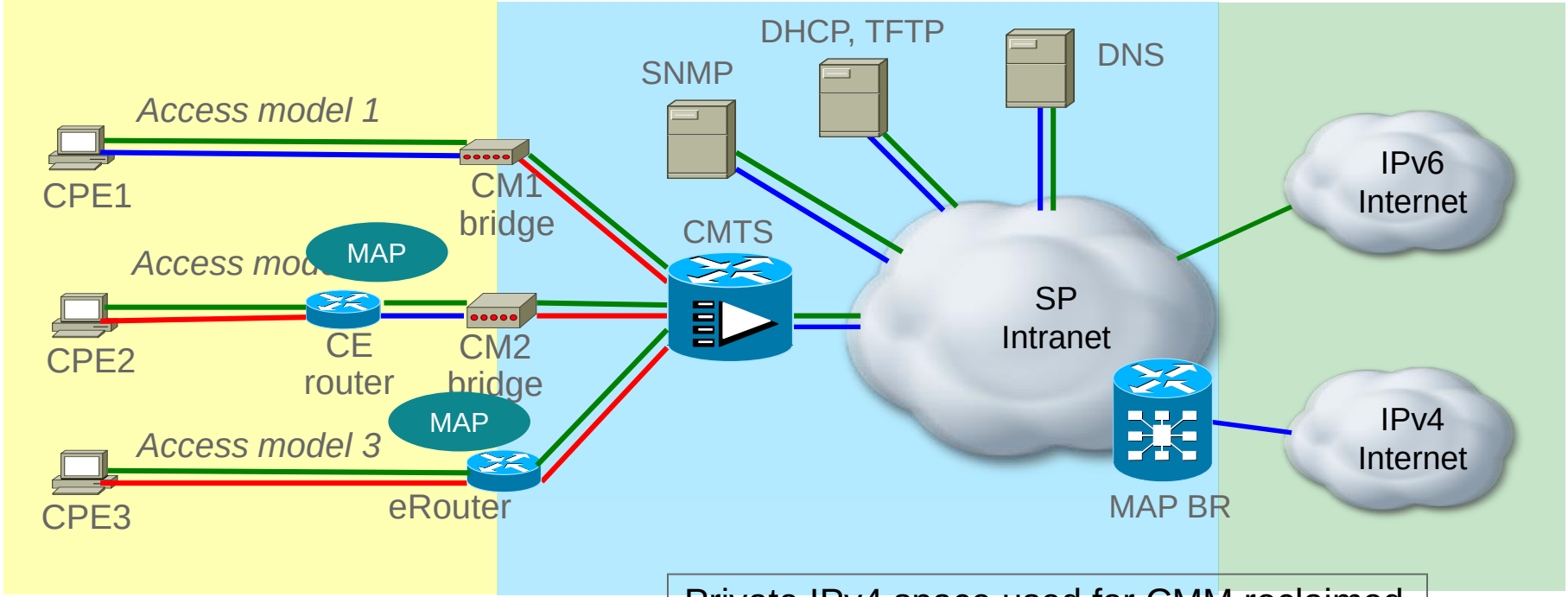
Public IPv4 space used for CPE reclaimed

Public IPv4 Private IPv4 IPv6

RFC 6333 - Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

RFC 7596 - Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture

Transition Strategy – Service Provider “Y”



Private IPv4 space used for CMM reclaimed

Public IPv4 Private IPv4 IPv6

Public IPv4 space used for CPE reclaimed

RFC 7597 - Mapping of Address and Port with Encapsulation (MAP-E)

RFC 7599 - Mapping of Address and Port using Translation (MAP-T)

IPv6 security

IPv6 Security

Features Available

- Source Verify with **DHCP** option (Lease query)
- **Access Control Lists (ACL)**
- **Cable Filter Group (FG)**
- **DOCSIS DEVICE-MIB objects**
- **Upstream Drop Classifiers (UDC)**
- **Limiting IPv6 CPEs per Cable Modem**
- **Divert Rate Limiting/ Punt Path Rate Limiting**

BRKSEC-3003 : Advanced IPv6 Security in the LAN

Source Verify with DHCP Option

- When a packet with unknown address is seen, CMTS sends a DHCPv6 Lease Query (LQ) for L2 address resolution to the DHCP server
- It is STRONGLY RECOMMENDED to disable Neighbor Discovery (**no cable nd**); similar to disabling ARP (**no cable arp**) when implementing DHCPv4 LQ

```
interface Bundle <x>
   no cable nd
   cable ipv6 source-verify dhcp
```

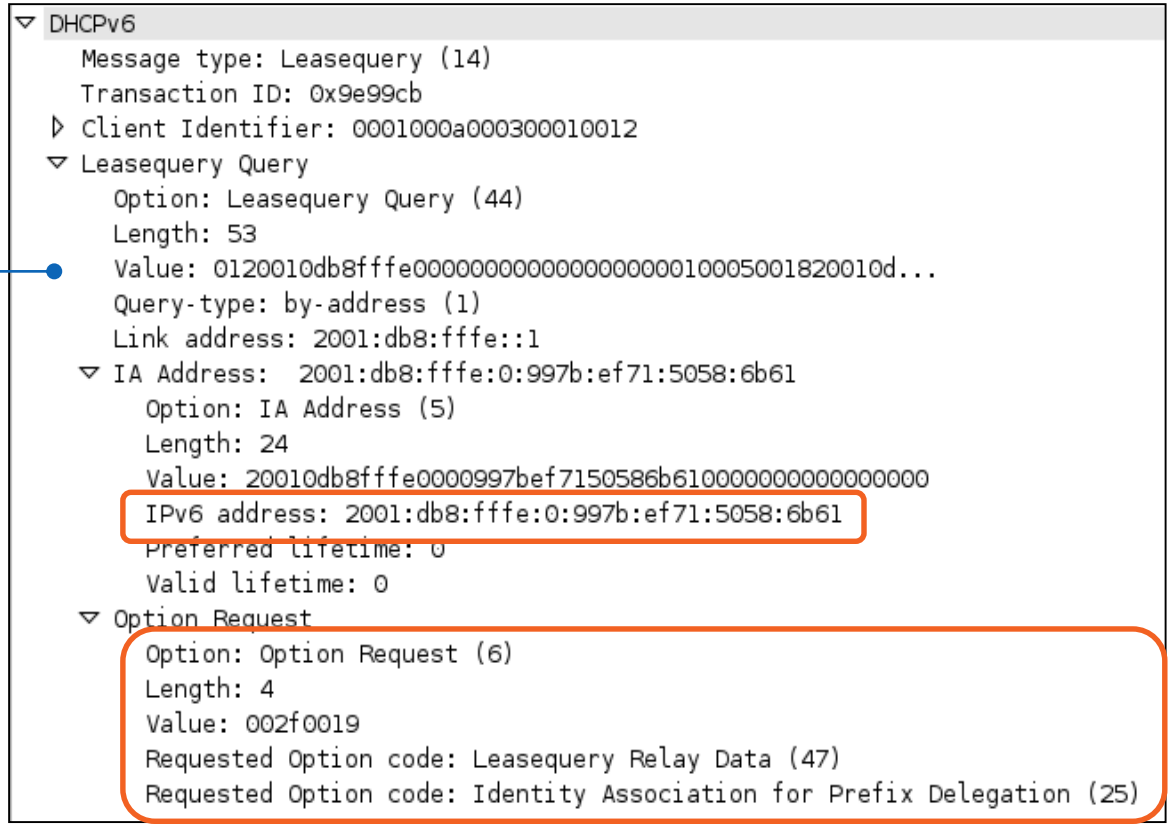
- Rate limiting SHOULD also be configured for both the upstream and downstream directions to prevent flooding the provisioning system with leasequeries

```
cable ipv6 source-verify leasequery-filter downstream 3 5
interface Bundle <x>
 cable ipv6 source-verify leasequery-filter upstream 3 5
```

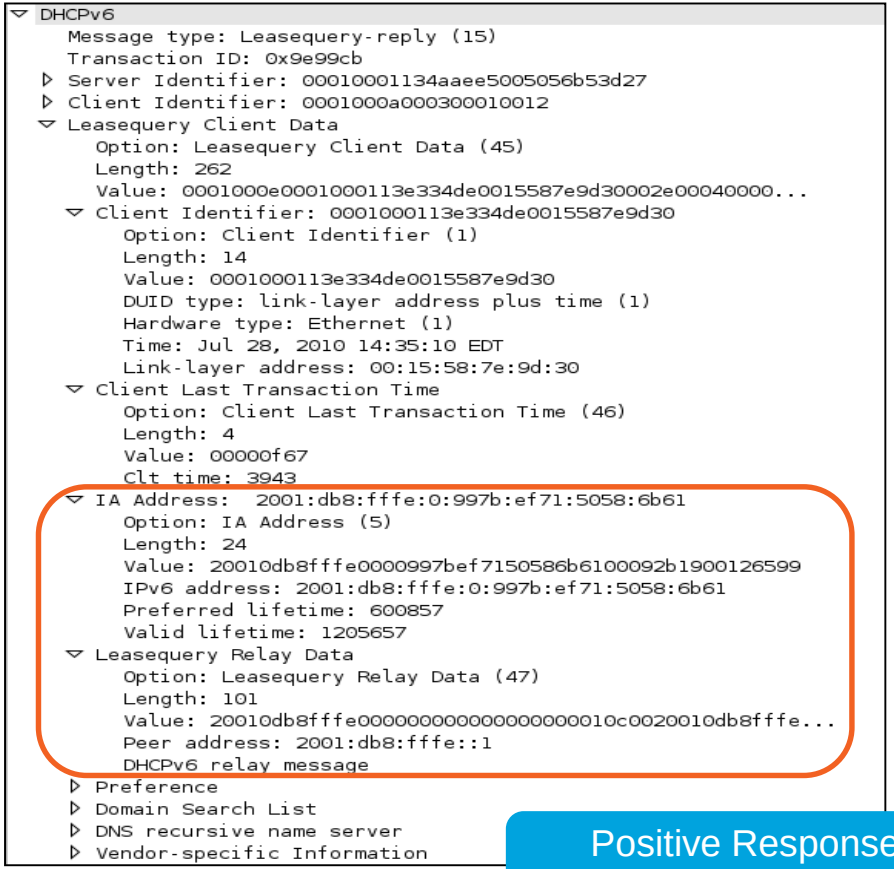
Example DHCPv6 leasequery

DHCPv6 Leasequery

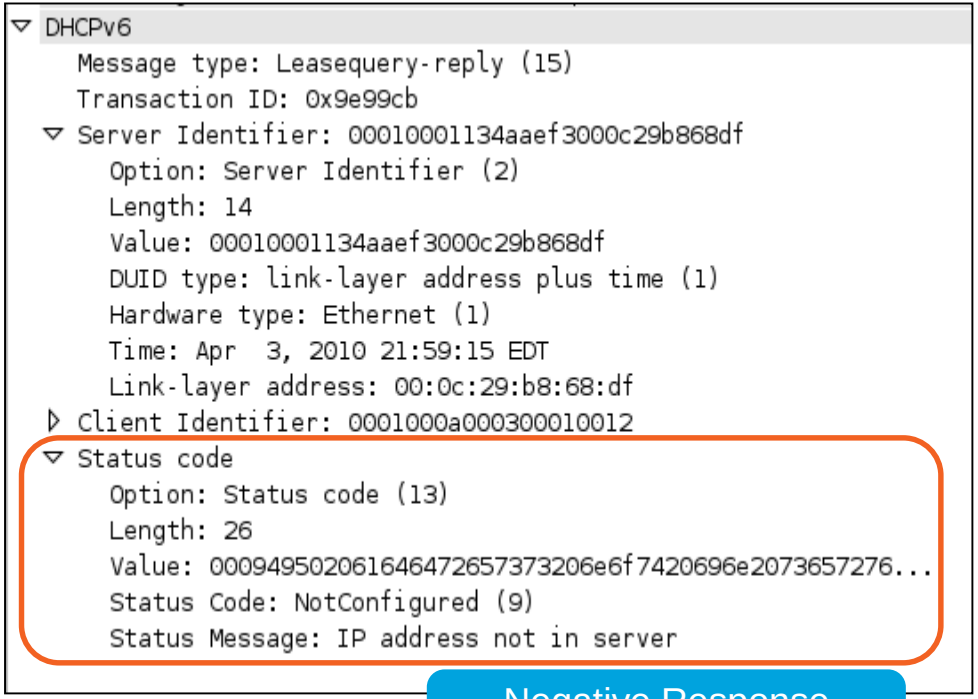
Unknown IA address included and ORO requests leasequery data as well as any delegated prefixes



Example DHCPv6 leasequery replies



Positive Response Example



Negative Response Example

IPv6 access control lists

- IPv6 Access Control Lists (ACLs) are always named lists
- To apply to a Bundle interface **ipv6 traffic-filter <name> in|out**
- Use a similar design criteria to the IPv4 ACL design:

  Allow only what's needed

  One size fits all approach as ACLs not to be often updated

  Block unexpected ICMP message types (i.e. routing headers, undetermined transport)

  Block DHCP server packets inbound

  Block access to infrastructure prefixes

  Block access to ULA prefixes

  Block unused protocols such as NetBIOS

IPv6 access control lists

- Typical IPv6 ACL use case is to restrict telnet and/or SSH access into the box; for example to block all IPv6 access

```
ipv6 access-list no-v6-access
 deny ipv6 any any
!
line vty 0 4
 ipv6 access-class no-v6-access in
```

- ACLs are also needed to restrict SNMP access to the CMTS; existing ACLs for IPv4 have no affect on IPv6 traffic thus an additional IPv6 ACL field is needed

```
snmp-server community changeme RO ipv6 no-v6-access 20
```

Cable Filter Groups

- Cable filter groups allow per device filters and can be applied via CMTS configuration, SNMP operation, or TLVs in the modem configuration file.
- Individual filter group entries (indices) apply to either IPv4 or IPv6; a single entry DOES NOT apply to both. **IPv6 filter criterion include : source/destination addresses and prefix lengths, flow label, and IP version.**
- On uBR10012, ACL and cable filter groups can not be used simultaneously. cBR-8 does not have this restriction

```
****** Add an index to the CPE upstream Filter Group to drop IPv6 that match the rule *****
cable filter group 2 index 18 v6-dest-address 2001:db8::
cable filter group 2 index 18 v6-dest-pfxlen 32
cable filter group 2 index 18 ip-version IPv6
cable filter group 2 index 18 match-action drop

****** Either explicitly assign this FG in the CM configuration file (TLV37) or use the default FG *****
cable submgmt default filter-group cpe upstream 2
cable submgmt default active
```

Controlling CPE IPv6 traffic – DOCSIS DEVICE-MIB

- Once the CMTS is configured for IPv6 and starts sending Router Advertisements any CPE behind an IPv6 capable cable modem is able to attempt to obtain IPv6 network connectivity
- Most client devices are enabled for IPv6 by default and are just waiting for the RAs
- In pilot phase, SP may allow only certain modem types can have IPv6 CPE or restrict number of IPv6 CPEs

Controlling CPE IPv6 traffic – DOCSIS DEVICE MIB

- Can set the DOCSIS DEVICE-MIB objects docsDevFilterLLCUnmatchedAction and docsDevFilterLLCTable in the CM configuration file to explicitly block IPv6 to/from the modem's Ethernet port.
- Below is an example where IPv4 (Ethertype 0x0800 – 2048 in decimal) and ARP (Ethertype 0x0806 – 2054 in decimal) are allowed and any unspecified Ethertype (such as IPv6) are denied

```
11 (SNMP MIB Object) = docsDevFilterLLCUnmatchedAction.0 (Integer) = 1
11 (SNMP MIB Object) = docsDevFilterLLCStatus.1 (Integer) = 5
11 (SNMP MIB Object) = docsDevFilterLLCIfIndex.1 (Integer) = 0
11 (SNMP MIB Object) = docsDevFilterLLCProtocolType.1 (Integer) = 1
11 (SNMP MIB Object) = docsDevFilterLLCProtocol.1 (Integer) = 2048
11 (SNMP MIB Object) = docsDevFilterLLCStatus.1 (Integer) = 1
11 (SNMP MIB Object) = docsDevFilterLLCStatus.2 (Integer) = 5
11 (SNMP MIB Object) = docsDevFilterLLCIfIndex.2 (Integer) = 0
11 (SNMP MIB Object) = docsDevFilterLLCProtocolType.2 (Integer) = 1
11 (SNMP MIB Object) = docsDevFilterLLCProtocol.2 (Integer) = 2054
11 (SNMP MIB Object) = docsDevFilterLLCStatus.2 (Integer) = 1
```

Upstream Drop Classifiers

- Classifiers used by CM to filter upstream traffic. IPv6 filtering can be applied per Cable Modem
- Can not be used along with docsDevFilter.
- Can be assigned three ways
  - Statically via cable modem configuration file (TLV 60) – Classifiers are NOT sent by CM in REG-REQ-MP message
  - Dynamically by CMTS through group id referenced in CM configuration file (TLV 62) – Classifiers are sent by CM in REG-REQ-MP message – Not supported
  - Dynamically managed by CMTS via Dynamic Service Change (DSC) messages
- Supported on uBR10k from SCG5 release. On cBR-8, supported from day 1.

```
****** UDC support enabled per Cable interface *****
cable udc-capability
```

Limiting IPv6 CPEs per modem

- Subscriber management mechanisms similar to IPv4 (DOCSIS TLVs 35 & 36); defined by DOCSIS 3.0 OSSI & MULPI (**DOCSIS TLV 63 – Max CPE IPv6 Addresses**)

```
<ubr10k>
cable modem v6-max-cpe-prefix <>
```

```
<cbr-8>
cable submgmt default max-ipv6-cpe <>
cable submgmt default active
```

- This maximum is the total number of CPE IPv6 delegated prefixes and CPE addresses (**including link-local**) that can be learned from a modem
- Permitted IPv6 prefixes and addresses can also be configured for a cable modem using DOCSIS TLVs 61 and 67 respectively
- Interaction with DOCSIS TLV 18 (Maximum Number of CPEs) which is number of CPE MACs granted access during a CM epoch

Divert Rate Limiting (DRL) on ubr10k platform

- DRL protects the uBR10012 PRE from having to process large amounts of traffic draining CPU resources.
- Existing cable side configuration is on a per SID basis and covers all types of traffic (IPv4 and IPv6).

```
Interface cable x/y/z
cable divert-rate-limit rate 4 limit 30
```

- The WAN side configuration is configured on a divert code basis and thus new ones are used for IPv6.

```
service divert-rate-limit ipv6 ipv6_rp_dest rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_glean rate 1 limit 4
service divert-ra trusted-site-ipv6 FC00:1111:1111::/48 traffic-class 0x0 mask 0x0
```

Divert Rate Limiting (DRL) on ubr10k platform

- From SCH3 release, aggregate max-rate limit can be configured per divert-code

```
service divert-rate-limit max-rate wan ipv6_fib_glean rate 5000 limit 1000
service divert-rate-limit max-rate wan ipv6_fib_punt rate 5000 limit 1000
service divert-rate-limit max-rate wan ipv6_fib_dest rate 40000 limit 4000
```

- From SCJ release, below additional IPv6 divert-codes introduced
  - icmpv6 – IPv6 ICMP
  - Ipv6_nd_na_mcast
  - Ipv6_nd_na_ucast
  - Ipv6_nd_ns_mcast
  - Ipv6_nd_ns_ucast
  - Ipv6_rp_dest_precedence
  - Ipv6_src_linklocal

Punt Path Rate Limiting (PPRL) on cBR-8 platform

- PPRL protects the cBR-8 RP from having to process large amounts of traffic draining CPU resources.
- Cable side configuration is on a per SID basis and covers all types of traffic (IPv4 and IPv6).

```
platform punt-sbrl subscriber rate 16
```

- Per punt cause rate limiting on the WAN side configuration covers all traffic IPv4 and IPv6.

```
platform punt-policer 24 10
platform punt-policer 24 10 high
platform punt-policer 100 10

platform punt-sbrl wan punt-cause 10 rate 4
platform punt-sbrl wan punt-cause 11 rate 4
platform punt-sbrl wan punt-cause 24 rate 4
```

Punt-cause	Description
10	Subsequent packets, when RP resolving address
11	Packets to CMTS
24	Packets received for unknown address
100	Src verify inconclusive

PPRL on cBR-8 platform ..cntd

- Update copp_policy to control IPv6 traffic from trusted and untrusted sites

```
ipv6 access-list trusted_ipv6
 permit ipv6 <PERMIT-IPV6> any
class-map match-any sbrl_trusted_ipv6
 match access-group name trusted_ipv6
```

```
ipv6 access-list untrusted_ipv6
 permit ipv6 <PERMIT-IPV6> any
class-map match-any sbrl_untrusted_ipv6
 match access-group name untrusted_ipv6
```

```
policy-map copp_policy
  class sbrl_trusted_ipv6
    police rate 1000 pps conform transmit exceed transmit
  class sbrl_untrusted_ipv6
    police rate 1000 pps conform drop exceed drop
```

```
control-plane
  service-policy input copp_policy
```

Key Takeaways

- Deployment Approach - Core to Edge
- Hierarchical Address planning – Top to Bottom approach
- Multicast Control Messages timers – Tuning
- Prefix Delegation for CPE router – Create Static Routes
- Transition strategy – DS-Lite or MAP
- Implement Source Verify with DHCP – Trust your DHCPv6 server
- Implement FG/ACL, docsDevFilter/UDC – Enhance Security
- Punt Packets Rate Limiting – Reduce Control Processor CPU

Learn IPv6

Implement Best Practices

Enjoy the Benefits

Call to Action : Learning more about IPv6

BRKRST-2616	Addressing Networking challenges with latest Innovations in IPv6	Tue 16 11:15:00
COCIP6-1013	IPv4 Address Exhaustion and IPv6 Progress across Cisco IT	Tue 16 11:15:00
BRKRST-2116	Intermediate - IPv6 from Intro to Intermediate	Tue 16 14:15:00
DevNet-1275	Developing Better Applications with IPv6	Tue 16 16:30:00
BRKRST-2022	IPv6 Routing Protocols Update	Tue 16 16:45:00
BRKSPG-2603	Intermediate - How to Securely Operate an IPv6 Network	Tue 16 16:45:00
LABIPM-2007	Intermediate - IPv6 Hands on Lab	Wed 17 09:00:00
CCSIP6-2006	BMW: Enterprise IPv6 adoption	Wed 17 11:30:00
LABSPG-7122	Advanced IPv6 Routing and services lab	Wed 17 14:00:00
BRKIP6-2100	IPv6-centric application development	Wed 17 14:30:00
BRKRST-2667	How to write an IPv6 Addressing Plan	Wed 17 14:30:00
BRKSPG-2300	Service Provider IPv6 Deployment	Wed 17 16:30:00
PNLCRS-2307	Don't Be Left Behind: Consumer Internet Traffic is Shifting to IPv6, Will your Organization Follow?	Wed 17 16:30:00
BRKRST-2312	Intermediate - IPv6 Planning, Deployment and Operation Considerations	Thu 18 09:00:00
BRKSPG-2061	IPv6 Deployment Best Practices for the Cable Access Network	Thu 18 09:00:00
BRKCOL-2020	**IPv6 in Enterprise Unified Communications Networks**	**Thu 18 11:30:00**
BRKSEC-3003	**Advanced IPv6 Security in the LAN**	**Thu 18 11:30:00**
BRKRST-3123	**Segment Routing for IPv6 Networks**	**Thu 18 14:30:00**
BRKSEC-3200	**Advanced IPv6 Security Threats and Mitigation**	**Thu 18 14:30:00**
BRKRST-2301	**Intermediate - Enterprise IPv6 Deployment**	**Fri 19 09:00:00**

Lunch and Learn:

- Service Provider IPv6: Tue 16 12:45
- IPv6 in the Enterprise: Thu 18 13:00

Walk-in Self-Paced Lab:

LABCRS-1000 Intro IPv6 Addressing and Routing Lab

Experiment with IPv6-only WiFi:

SSID: CL-NAT64

WPA passphrase: cl-nat64

SLAAC + stateless DHCP

NAT64 included to access legacy

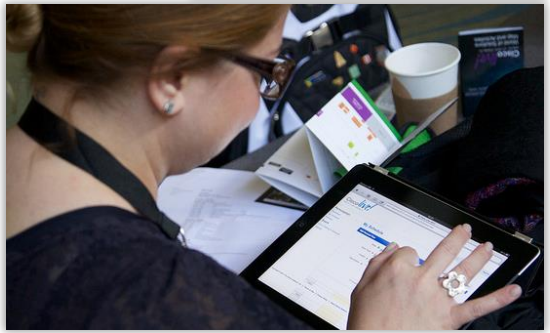
Ask all World of Solutions exhibitors for their IPv6 support ☺

Cisco live!

Complete Your **Online Session Evaluation**

- Please complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt.

- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations



Cisco live!

Thank you

We’re ready. Are you?

Appendix

General IPv6 checklist

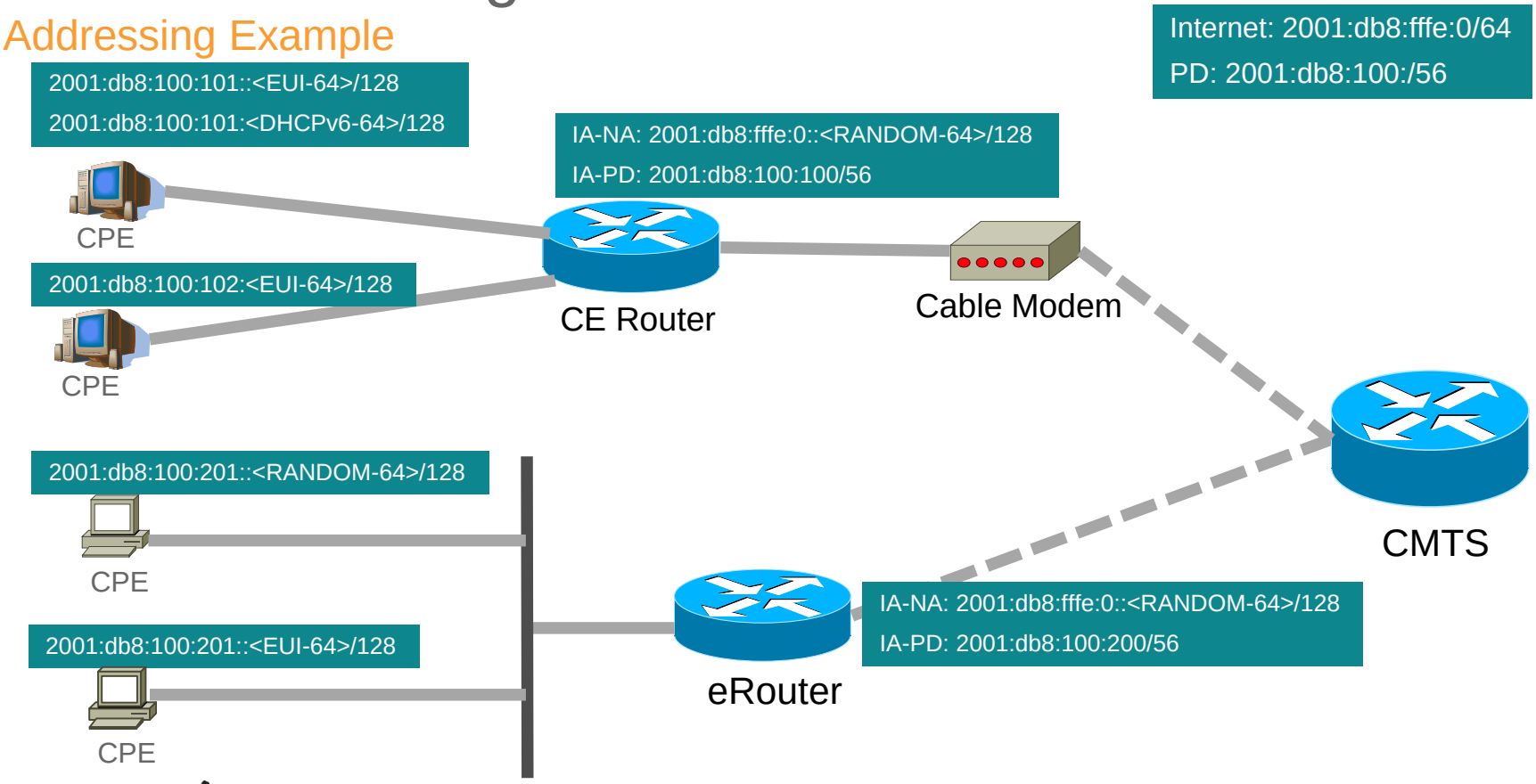
- Hardware and software upgrades
  - Are OSS and NMS systems IPv6 ready?
  - Use of DOCSIS 2.0+?
- Infrastructure IPv6 addressing strategy
  - Global and/or unique local addressing for infrastructure or perhaps link-local only
  - If global addressing for infrastructure - separate address block from customer addressing?
  - Prefix size for p2p links - /64, /127?
  - Block for loopbacks (loopbacks configured with /128)
  - Need to support customers with Provider Independent (PI) addressing
- IPv6 routing
  - ISIS (single topology or multi-topology), OSPFv3, MP-BGP, static

IPv6 for CPEs checklist

- IPv6 only or dual-stack? If IPv6 only methodology for translation?
- Will both DOCSIS 3.0 and DOCSIS 2.0+ modems be used?
- Do the provisioning systems support IPv6?
- Redundant provisioning systems? How to handle DHCPv6 failover?
- Preventing SLAAC
- Mechanisms to control which modems can have IPv6 CPEs?
- Security considerations for interface identifier addressing
- Support for multiple GUAs?
- Support for static CPE addressing?

IPv6 Prefix-Delegation

Addressing Example



IPv6 for prefix delegation checklist

- eRouters and/or standalone CE routers?
- How to control which devices can be used?
- Redundant provisioning systems? How to handle DHCPv6 failover?
- Size of delegated prefixes? /64s only?
- Prefix delegation beyond basic residential service – recursive prefix delegation
- Use of prefix stability?
- If prefix stability used size of prefix range for CMTS group?

IPv6 for CMM checklist

- Is public IPv4 addressing currently used?
- Will both DOCSIS 3.0 and DOCSIS 2.0+ modems be used?
- IPv6, DPM, or APM?
- Do the provisioning systems support IPv6?
- Same provisioning systems for IPv4 and IPv6?
- Redundant provisioning systems? How to handle DHCPv6 failover?
- Do the NMS applications support IPv6?
- Use of MDD Override to control which modems can provision IPv6?
- Enabling SNMP over IPv6 access on the modems

IPv6 security checklist

- Use of cable source verify and DHCPv6 lease query
- Use of access control lists, cable filter groups
- Securing the CMTS (Telnet, SSH, SNMP)
- Use of DRL or PPRL to protect the CMTS CPU
- IPv6 for voice?
- IPv6 multicast?

IPv6 for PacketCable 2.0

- Works with PCMM to provide dynamic QoS
- For uBR10002 platform, PCMM for IPv6 supported from SCJ release.
- With PacketCable the eDVA undergoes it’s own provisioning process independent from the cable modem
- Just like the cable modem the eDVA can be IPv4 only, IPv6 only, or dual-stack
- The protocol used by the eDVA for management & signaling can be different than what is used for the payload
- Cisco Prime Cable Provisioning supports PacketCable 2.0 with IPv6 as of release 5.1 (Basic mode provisioning)

IPv6 multicast

- CMTS global configuration **ipv6 multicast-routing** is needed to support user joined (i.e. MLD) multicast traffic; not required to support IPv6 multicast as used for neighbor discovery or routing protocols
- Globally enabling **ipv6 multicast-routing** enables MLD and PIM on all interfaces
- How to handle multicast when receivers can be either IPv4 or IPv6?