Introduction to Key Technologies in DOCSIS 3.0 for Cable Operators

BRKBBA-2007

Daniel Etman

Cisco Networkers 2007

HOUSEKEEPING

- We value your feedback, don't forget to complete your online session evaluations after each session and complete the Overall Conference Evaluation which will be available online from Friday.
- Visit the World of Solutions on Level -01!
- Please remember this is a 'No Smoking' venue!
- Please switch off your mobile phones!
- Please remember to wear your badge at all times including the Party!
- Do you have a question? Feel free to ask them during the Q&A section or write your question on the Question form given to you and hand it to the Room Monitor when you see them holding up the Q&A sign.

Agenda

- DOCSIS 2.0 overview
- Modular CMTS (M-CMTS) architecture
- DOCSIS 3.0 overview
  - Downstream channel bonding
  - Upstream channel bonding
  - Multicast
  - Physical layer technologies
  - Security
  - OSSI
  - Business Services
- IPv6 in Cable
- Summary

-> DOCSIS 3.0 Intro

DOCSIS 2.0 overview

Rates

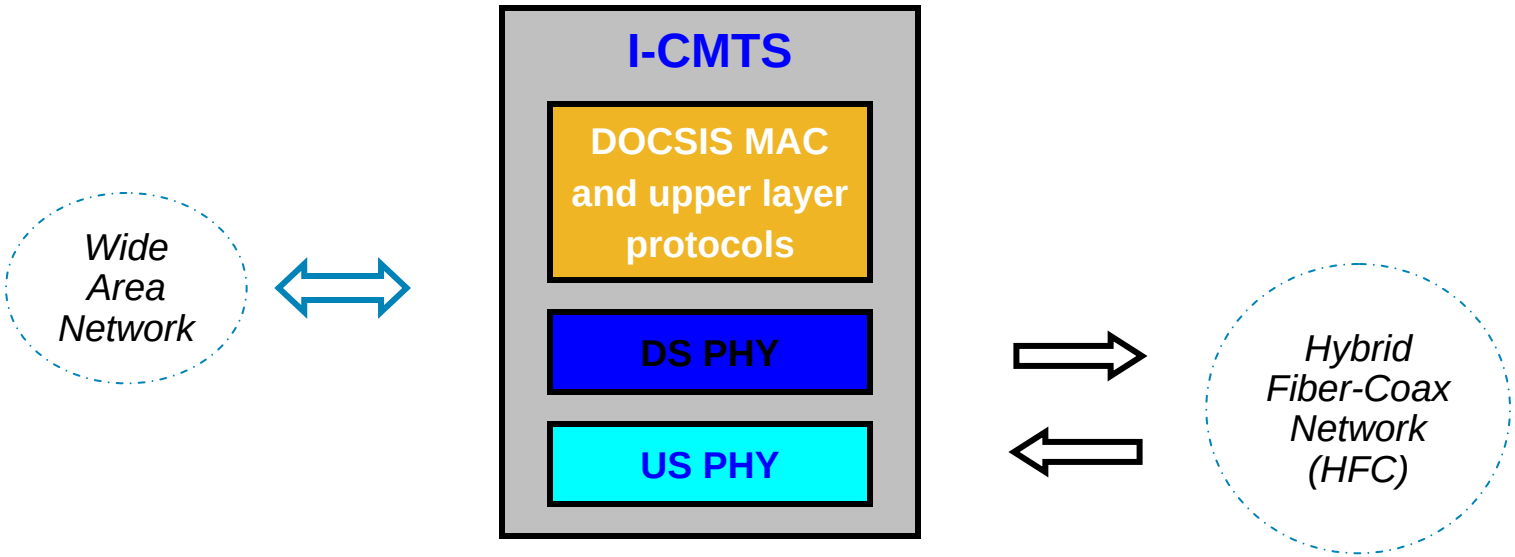
- Downstream rates
  - 6Mhz channels in the US, 8Mhz in Europe, 64QAM or 256QAM modulation
  - In the range of 26mbps/38mpbs (US), higher for Europe.
- Upstream rates
  - 200Khz-6Mhz, QPSK to 64QAM
  - In the range 320kbps to 30Mbps.
  - A flow speed is limited by the request-grant latency. That typically limits the US rates to 1-3mbps (though it can be faster with special configurations)
- Typically, out of 131 channels on the DS, only one is for DOCSIS, the rest for video (digital or analogue)

Feeds

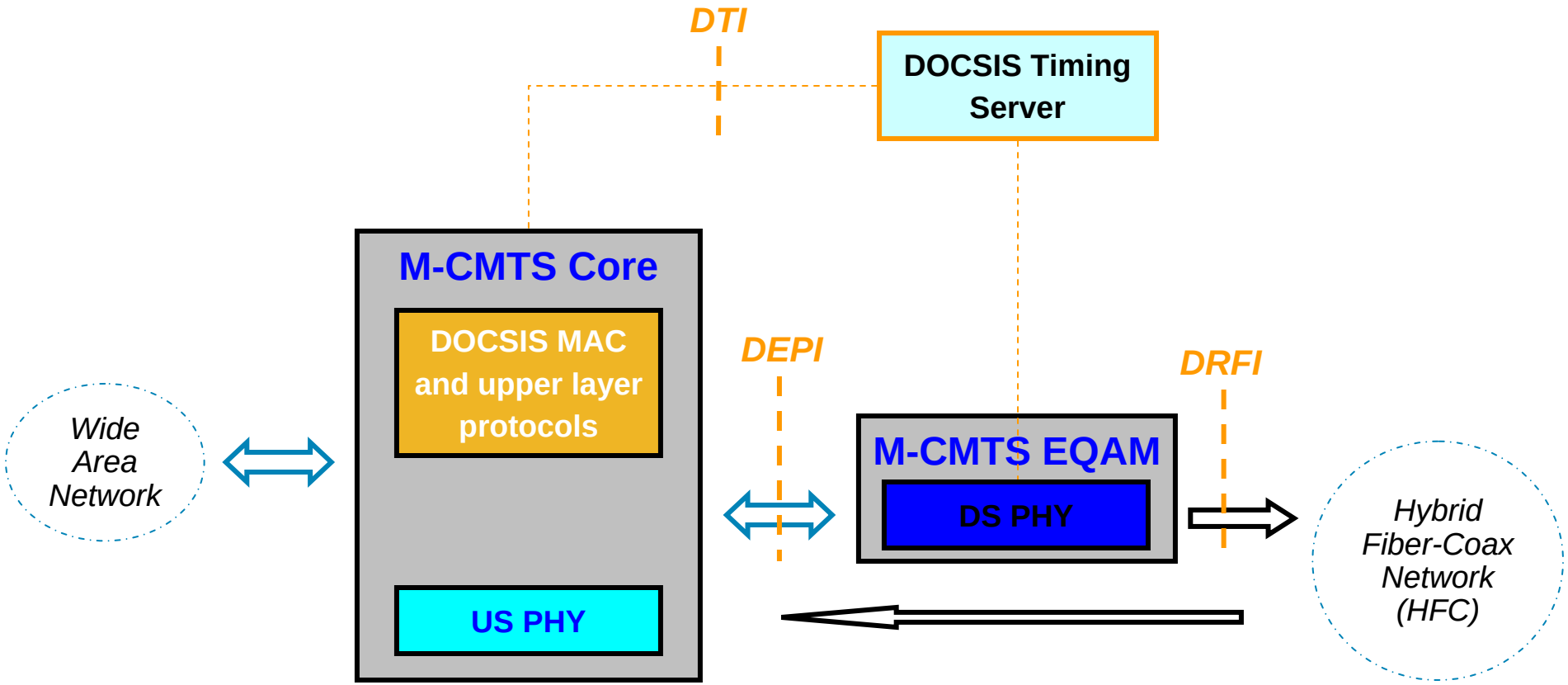
- The distribution network in optical all the way to a specific neighborhood. An FN (fibernode) converts the optical signal to an electrical signal over coax.
- An FN typically serves 500 homes (HHP – house holds passed)
- A typical DOCSIS configuration:
  - Single downstream channel is split to 4 FN
  - In this configuration about 2000 homes are passed by a DS.
  - Each FN has a single upstream frequency
  - About 800-1000 subscribers per downstream (not all homes have cable modems)

Modular CMTS

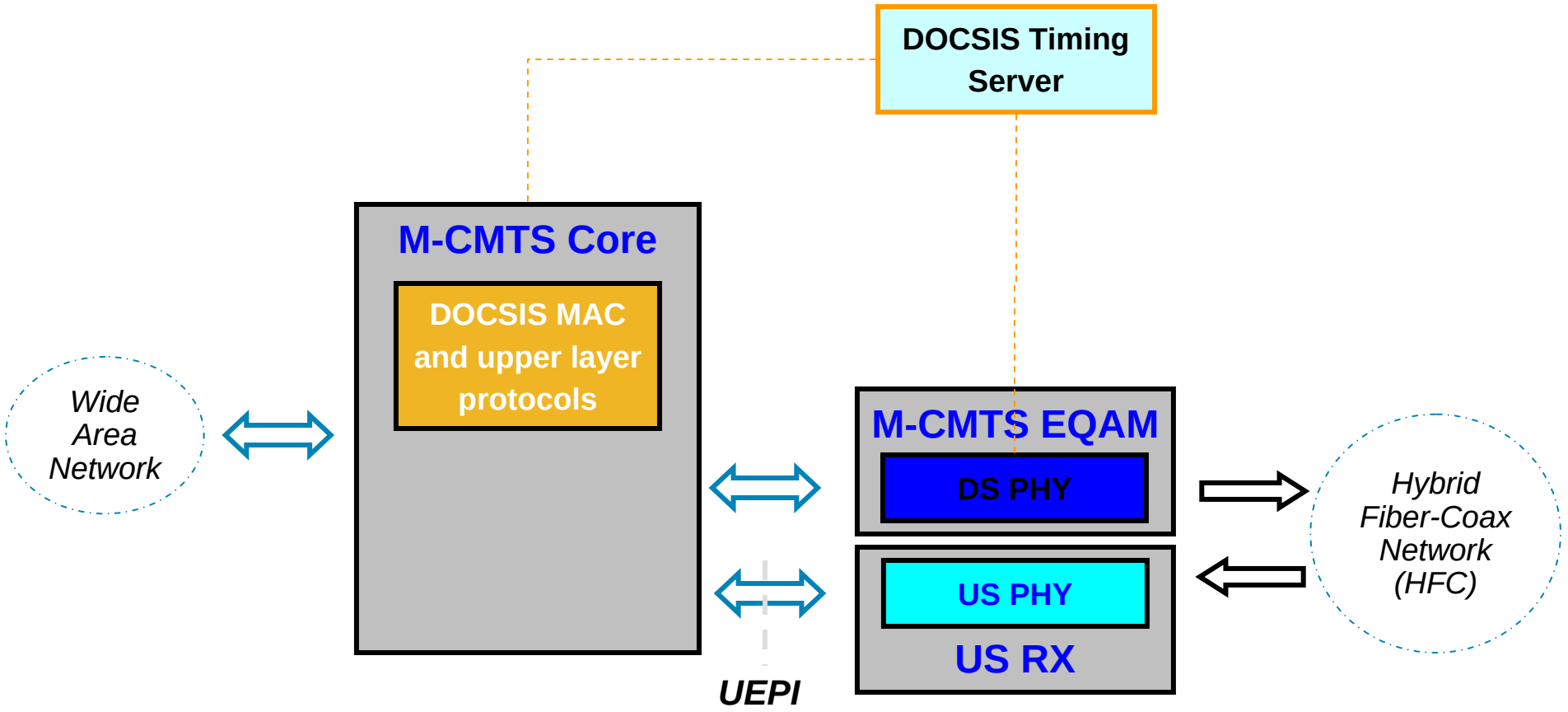
Integrated-CMTS Logical Functions



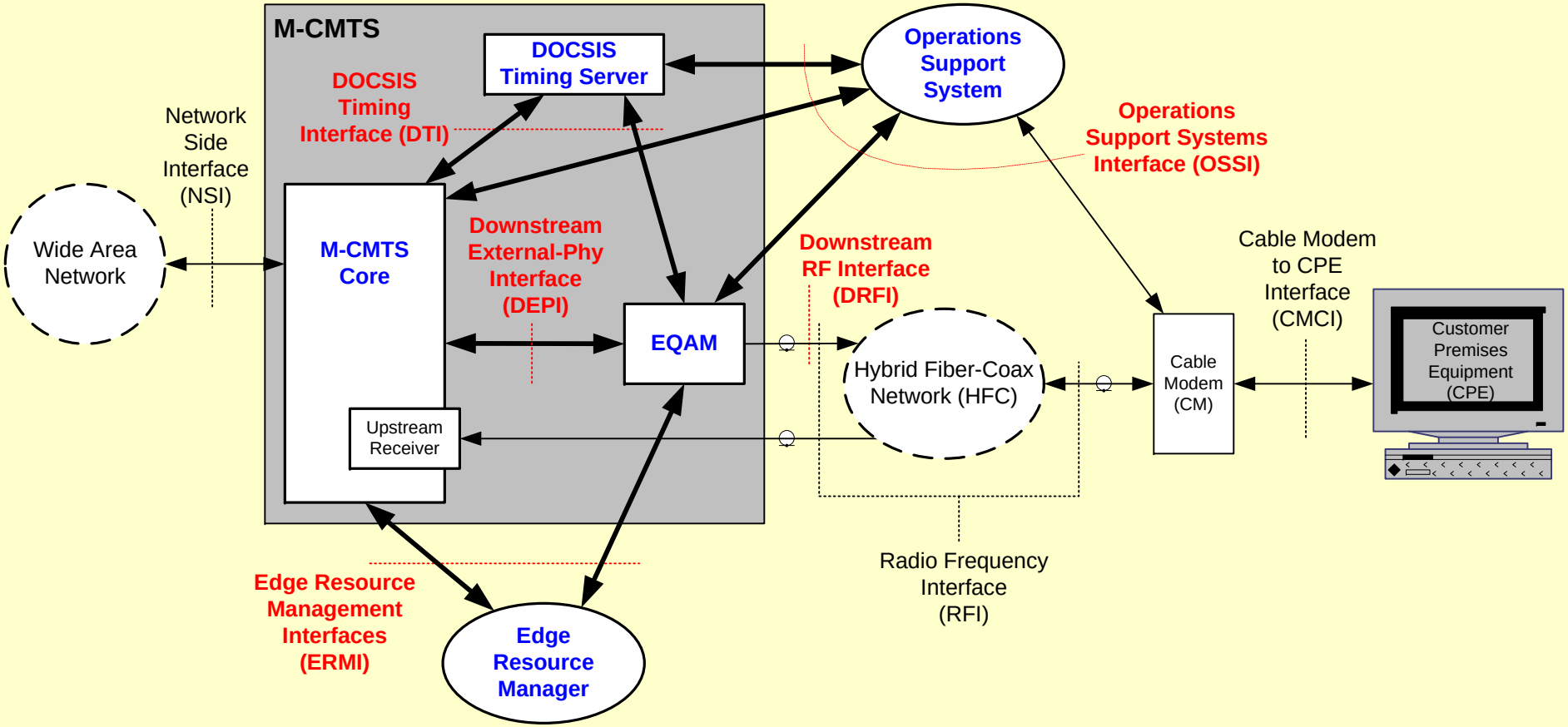
Modular-CMTS Phase 1



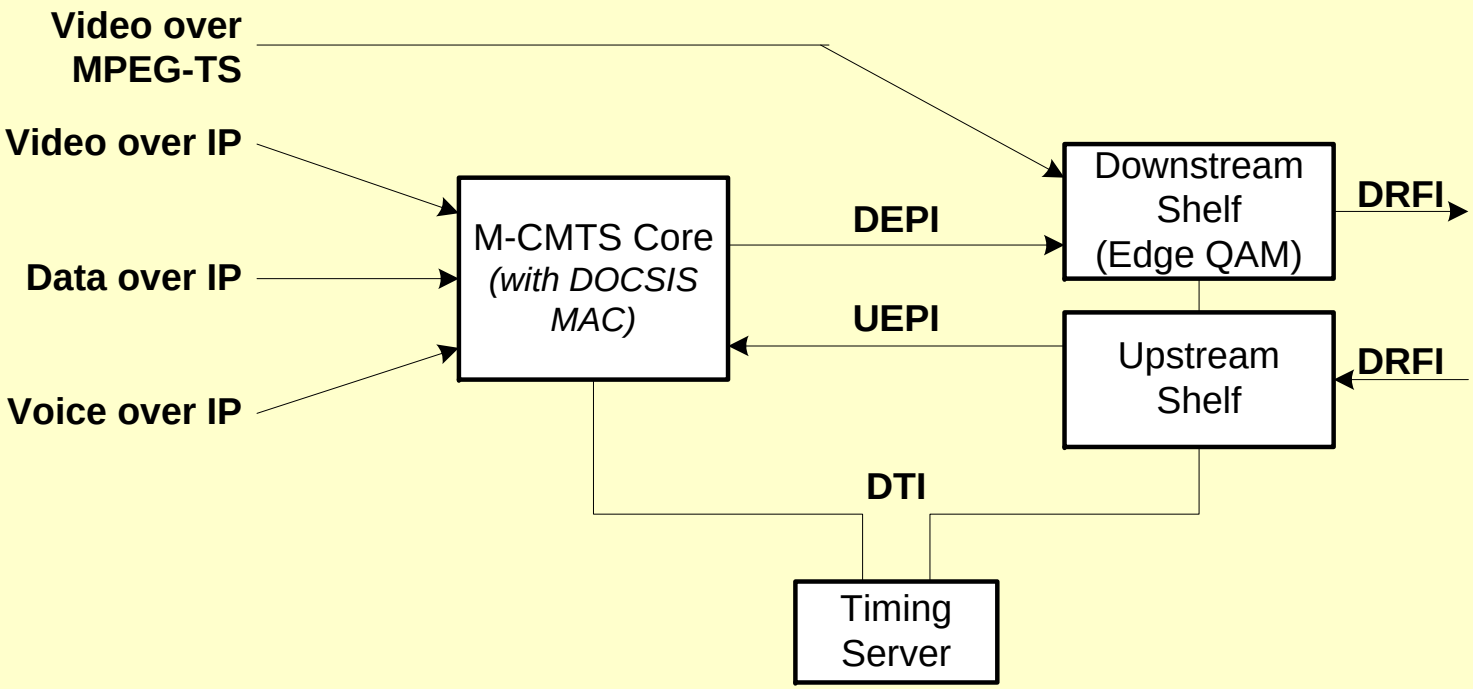
Modular-CMTS Phase 2



M-CMTS Components and Interfaces

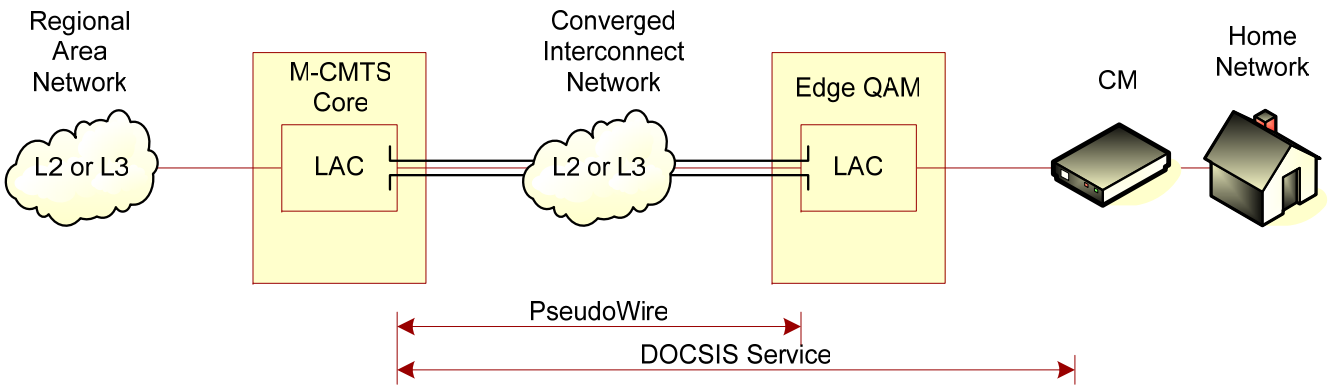


Basic M-CMTS Block Diagram



- UEPI: Upstream is an extension to DEPI and is currently under definition at Cisco.

DEPI Intro



- DEPI is an IP Tunnel, known as a pseudowire, that exists in the downstream direction between the DOCSIS MAC in the M-CMTS Core and the DOCSIS PHY that exists in the EQAM.
- The CIN (Converged Interconnect Network) may be a Layer 2 or Layer 3 network.
- The M-CMTS Core provides the DOCSIS MAC functionality, while the EQAM provides the DOCSIS PHY functionality.
- DEPI interfaces the MAC to the PHY.

DEPI Intro

- DEPI uses L2TPv3 (RFC 3931 Layer 2 Tunneling Protocol version 3) as the baseline protocol for the data path and control plane.
- DEPI uses two new pseudowire types:

  PSP (Packet Streaming Protocol) encapsulates a continuous stream of DOCSIS frames into a DEPI payload.

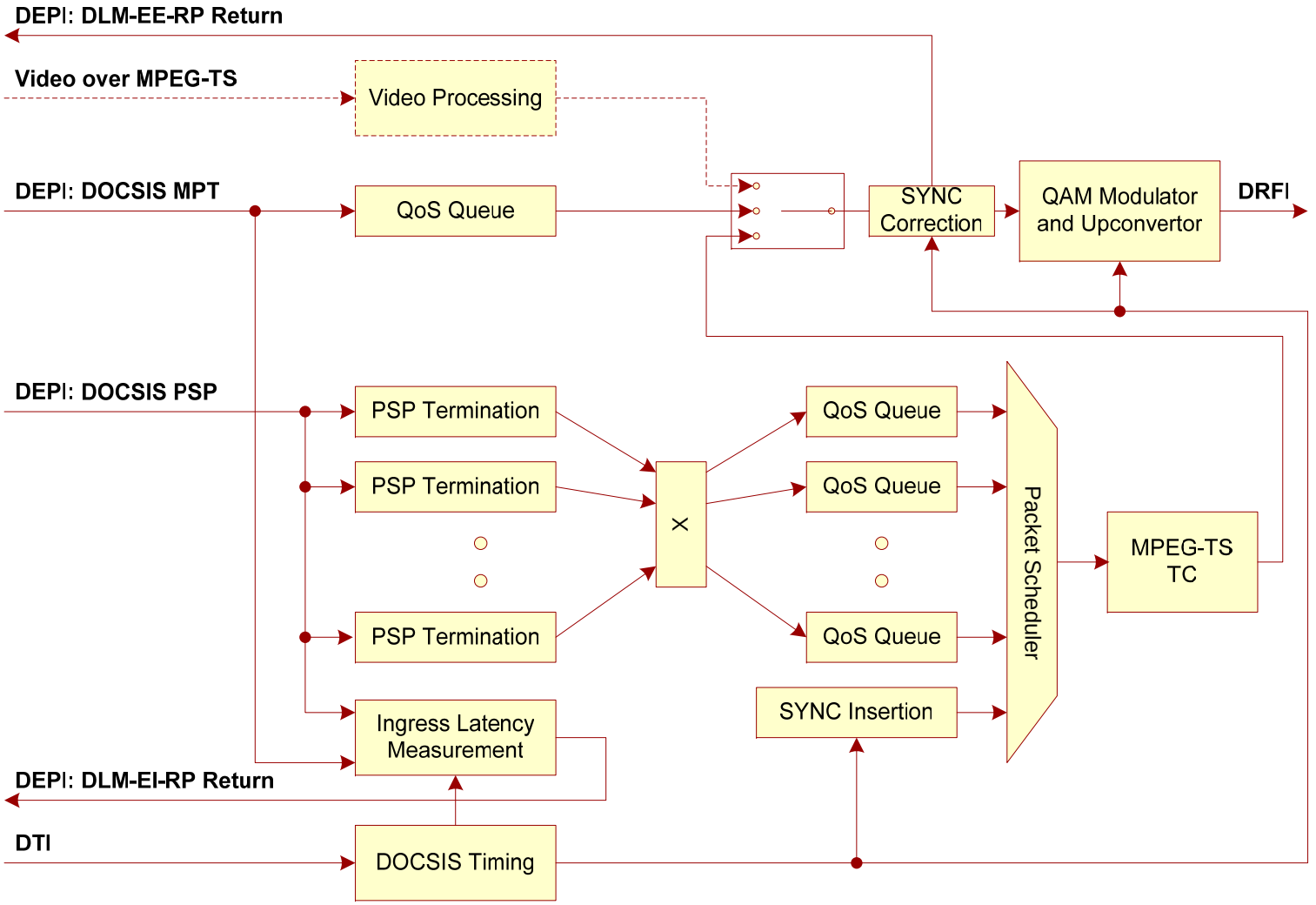
  MPT (MPEG Transport) encapsulates a group of 188 byte MPEG-TS packets into a DEPI payload.
- M-CMTS Core/EQAM must support MPT and/or PSP.
- Signaling

  DEPI has one (or more) Control Connection between the M-CMTS Core and the EQAM for configuration.

  DEPI has one session for each QAM. There are one or more sessions per control connection.

  DEPI has one or more flows per session for QoS. (Flows are a DEPI specific concept)

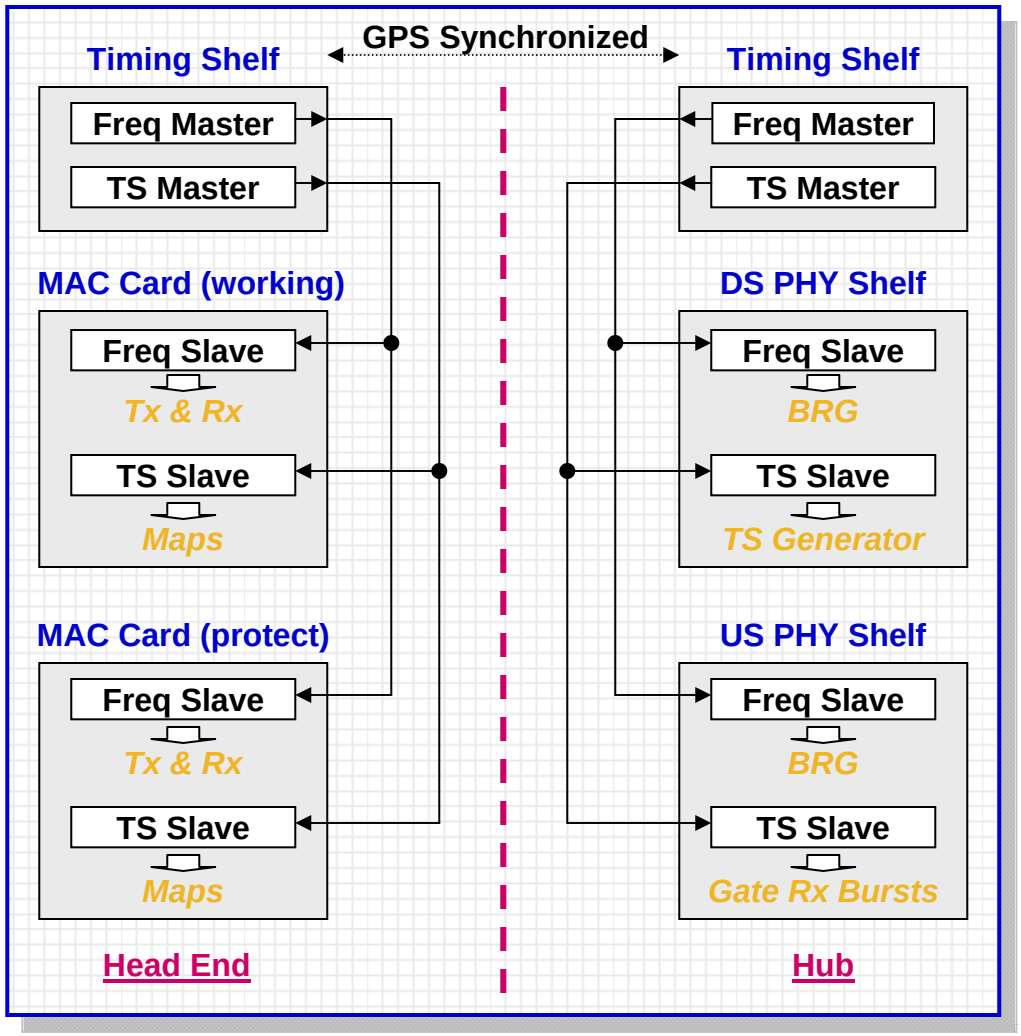
Edge QAM Block Diagram



DTI: DOCSIS Timing Interface

- A DTI Server supplies a 10.24 MHz frequency plus a DOCSIS timestamp to MAC and PHY
- MAC and PHY contain DTI Clients.
- Two-way protocol. DTI Server cancels out cable and circuit delays.

  Everyone has the same timestamp.
- Interface is UTP RJ45 Ethernet-like.



Legend
BRG = Baud Rate Generator
TS = Timestamp

M-CMTS Summary

- M-CMTS is a satellite architecture designed by Cisco that will be deployed in the 2006 (pre-DEPI) and 2007 (DEPI) timeframe.

  Separation was done between MAC and PHY.

- M-CMTS, when combined with Cisco's Wideband architecture for DOCSIS will provide:

  significantly more flexibility in configuration

  significantly lower transport cost per bit

  significantly higher data capacities than anything out there today.

- The Modular CMTS architecture and Wideband will allow DOCSIS to competitively provide the triple-play services of data, voice and video over IP.

  500+ Mbps downstream channels

  100 Mbps Downstream, 10 Mbps upstream Cable Modems.

  10x the bandwidth at 1/10 the cost

DOCSIS 3.0

DOCSIS 3.0 Subgroups

- CableLabs is most of the way through the DOCSIS 3.0 specification process. The first draft D01 has been released in February 2006. Interim Draft status I01 is scheduled for June 2006.
- There are 8 technical sub-groups.

DS Bonding	IPv6
US Bonding	Enhanced Multicast
Multi-Channel PHY	Enhanced Security
Business Services	Enhanced OSSI

Cisco has 2 engineers in each sub-group, and has more representation overall than any other vendor.

- Cisco is uniquely positioned to excel beyond the competition in each technology due to in-house expertise, authorship, and technology leverage from other parts of Cisco.

DOCSIS 3.0 Specifications

- DOCSIS 3.0 Specifications

MAC+	CM-SP-MULPIv3.0
PHY	CM-SP-PHY30-D01
SECURITY	CM-SP-SECv3.0-D01
OSSI	CM-SP-OSSIv3.0-D01
L2VPN	CM-SP-L2VPN-D04
BSoD	CM-SP-TE-D01

- Current Drafts and Interim Specifications are stored at:

  https://www.cablelabs.com/doczone/docsis/requirements/specs/current/DocZoneFolder_view

  Passwords are issued to selected vendors/providers directly from CableLabs. Access is under NDA.

New D3.0 MAC Management Messages

MDD	MAC Domain Descriptor
B-INIT-RNG-REQ	Bonded Initial Ranging Request
DBC-REQ	Dynamic Bonding Change Request
DBC-RSP	Dynamic Bonding Change Response
DBC-ACK	Dynamic Bonding Change Acknowledge
DPV-REQ	DOCSIS Path Verify Request
DPV-RSP	DOCSIS Path Verify Response
CM-STATUS	Status Report
CM-CTRL	CM Control
REG-REQ-MP	Multipart Registration Request

New D3.0 Frames, Headers, & EHDRs

Summary:

- Queue-depth Based Request Frame
- Upstream Segment Header
- Upstream Privacy EHDR with no piggyback request
- Upstream Privacy EHDR with piggyback queue-depth request
- Downstream Service EHDR
- DOCSIS Path Verify EHDR

MAC New Features

- MDD: Mac Domain Descriptor

  A MAC Management Message that defines plant topology and other parameters that are shared in a MAC domain and the CM needs to know about.

- Plant Topology

  In DOCSIS 3.0 it is mandatory that the plant topology (fiber nodes and how they are split/combined) is configured in the CMTS

- Ambiguity Resolution

  An efficient process for determining which FN a CM is physically connected to (or more precisely, which downstream service group its connected too) is possible thanks to the fact that plant topology is reflected in the MDD

MAC New Features

- Upstream/downstream bonding

  Sending packets on multiple downstreams for increased downstream throughput. Packets may be sequenced per Service Flow to ensure no out of order delivery

- DS Service EHDR – DSID and Sequence Number

  Packets are marked with a DSID which is used as a sequencing index for unicast and as a filter (and sequencing index) for multicast

- DBC-REQ/RSP/ACK: Dynamic Bonding Change

  A new message “DBC” (dynamic bonding change) to handle changing of channel assignments and DSIDs. The DSx messages are not impacted. The DBC replaces DCC for DOCSIS 3.0. DCC is only used when moving a modem to a new MAC domain (and modem will always re-initialize in such a case).

MAC New Features

- CM-CTRL: CM Control

  The CM control message is used to force various actions on the modem, such as reboot, or channel mute. It obsoletes the UP-DIS message

- CM-STATUS: CM Status Report

  In DOCSIS 3.0 we may still have a healthy connection to the CMTS even if some of the channel are in failure more. We can use this connection to inform the CMTS of the failures that it can not detect otherwise.

- DPV-REQ/RSP: DOCSIS Path Verify

  The DPV message is used to verify the state of a path (in terms of delay and packet loss samples) in the cable network, for example from the CMTS, over the CIN, the QAM and to the CM.

MAC New Features

- DS Service EHDR – Priority Field

  Packets are marked with a priority for prioritizing CMCI egress traffic – this is needed because the CM can not re-classify a packet to a flow

- Application ID

  Application ID added to the service flow definitions to help define CMTS policies such as admission control, channel assignments, bonded vs. non-bonded operation etc.

- Bonding Group Attributes

  Each bonding group has a list or attributes, for example, “high availability” or “low latency”. Each service flow is encoded with a certain set of attributes. This helps the CMTS in flows to bonding group assignment.

MAC New Features

- The CMTS controls error recovery

  In many cases where a CM is in an intermediate, or incomplete state, it is the responsibility of the CMTS to recover the modem. The modem will not take action on its own.

- Multipart REG-REQ

  Since the registration request can get fairly long it can be sent it in multiple parts.

- Receive Channel Profile

  The CM can send a set of limitations in its receive circuitry to the CMTS. The CMTS can use it for channel assignment to accommodate for these limitations.

- IUC2 obsoleted

  But still used for requests in the MSC mode (S-CDMA only) feature

Hybrid devices

- DOCSIS 3.0 is very large in scope. We are going to have “hybrid devices” that support only part of the DOCSIS 3.0 functions, for a while. DOCSIS 3.0 allows for the operation of such devices:

  To disable IPv6 set TLV5.1 to IPv4 in the MDD

  To disable AES – already handled the the current BPI standard. The CM and CMTS exchange a “cryptographic suite” as part of the authorization request. If the CM sends AES then the CMTS simply does not respond to this capability

  To disable early authentication - set TLV 6 in the MDD to see (see table 6-40 in DOCSIS 3.0)

  Commercial services – for commercial services we are required to lock the symbol clock to the baud clock. To signal that a CMTS does not support this feature (usually needed only for S-CDMA which our CMTS does not support anyway). This is signaled in the MDD.

DOCSIS 3.0- downstream channel bonding

What is downstream channel bonding ?

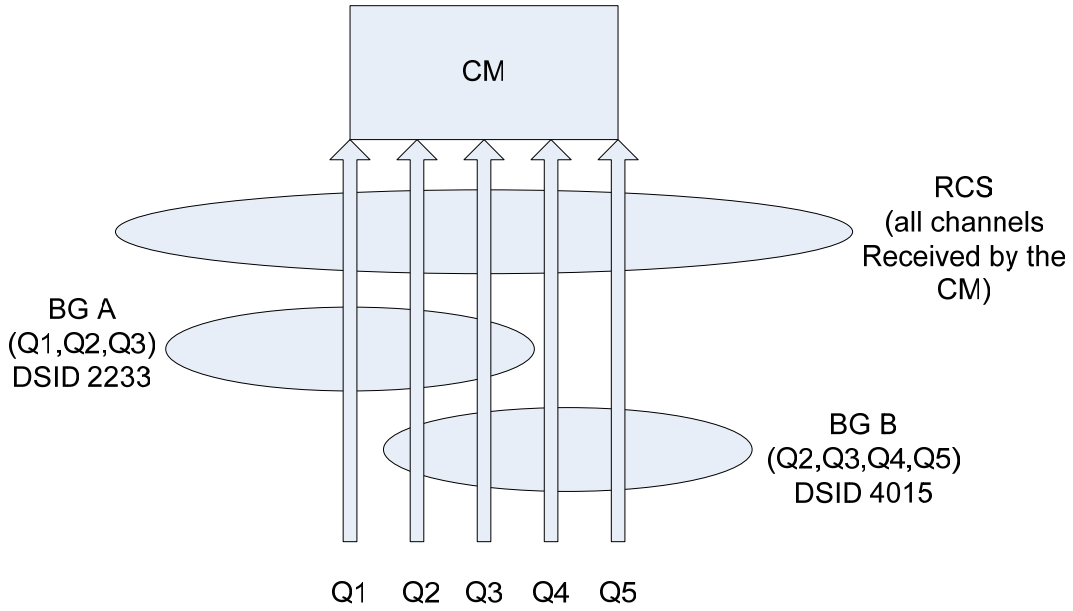
- An MLPPP like technology
- Each packet is tagged with a sequence number and a re-sequencing index:
  - The sequence number is used to place packets back in order
  - The re-sequencing index (DSID – downstream service ID) is used so that each flow, or group of flows, could be re-sequenced independently.

DSID – many meanings for single field

- The DSID serves as:
  - A re-sequencing index
  - DSIDs can be used only on a specific set of QAMs
  - A tag to identify (and filter on) multicast flows
  - Associated with an interface mask on the CM for multicast replication
- How is the DSID related to service flows ?
  - Not directly related
  - Several service flows can map to one DSID
  - Several DSIDs can map to a single service flow
  - DSIDs and service flows are signaled independently, in other words, there is no messages that associated a service flow to a DSID

RCS, BG and DSIDs

- RCS (receive channel set) defines the total set of QAMs the CM needs to listen to. Many different modems can use the same RCS.
- The set of channels that packets belonging to a DSID can be sent on are a “bonding group” (BG).
- Different modems can use the same BG, but must use different DSIDs, unless used for multicast service.
- Why do we need which channels the packets are sent on ? (next slide)



Fast recovery

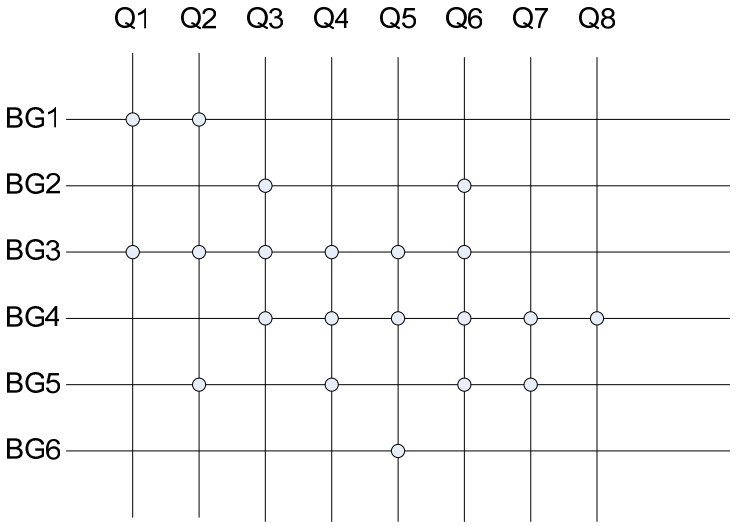
- A cable modem can receive information on QAM 1,2,3,4 (meaning the RCS is QAM 1,2,3,4).
- Packets on different channels might experience different delays. We call this differential delay “skew”
- Packets are received in increasing order on a given QAM but not across QAM.
- In the case where we know that a DSID sends packets only on 1,2,3 we can quickly recover from a missing sequence number:

  QAM 1 received sequence numbers : 1000, 1002

  QAM 2 received sequence numbers : 1007, 1008

  QAM 3 received sequence numbers : 1003, 1004
- We can immediately tell that 1001, 1005, 1006 are missing
- If we did not know that the DSID does not send packets on QAM 4, we would have had to wait a timeout period to detect the loss, because the missing packet might have appeared on QAM4

Downstream scheduling



Bonding groups are of different sizes (modem capabilities, multicast etc), Scheduling efficiently, and fairly, over partially overlapping QAMs, is the One of the main challenge for channel bonding

DOCSIS 3.0 - upstream channel bonding

Upstream MAC: Channel Bonding

- Upstream bonding

  Designed so that a single flow can consume all the BW on multiple upstreams.

- Continuous Concatenation and Fragmentation (CCF)

  An improved form of both concatenation and fragmentation that is needed for DOCSIS 3.0 operation.

Multi-SID vs. Multi-request

- Multiple outstanding grants per SID, or multiple SIDs with a single outstanding request, or both.

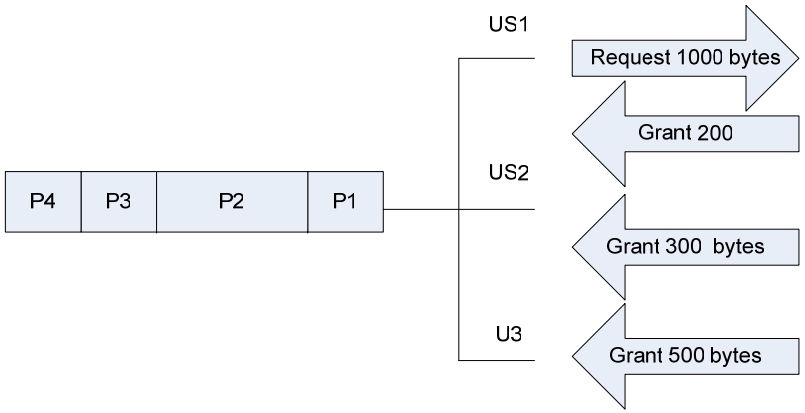
  “Multi-SID”, multiple SIDs, one grant per SID.

  - The risk : sid inflation

  “Multi-outstanding requests”

  - The risk : stale bytes in the output buffer if requests are lost. To work around this limitation its recommended to have at least 2 SIDs used for requesting – if one stalls the other still works.

CCF – continuous concatenation fragmentation



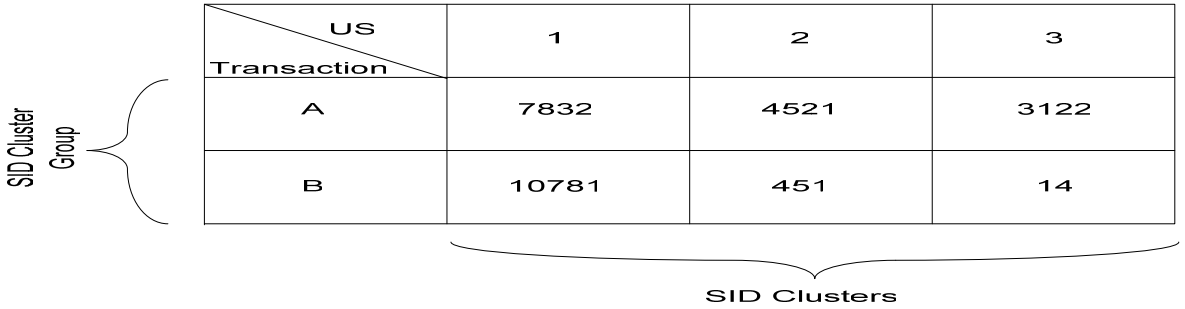
The CM has a buffer with a 1000 bytes to send. Its requests for 1000 on US1, the CM receives grants on US1, US2 and US3. The size of the grant may depend on the load on that channel

The CM does not send packets since the grant might not align with packet boundaries

Instead the CM sends “segments”

Each segment has a sequence number, and a pointer field so that individual packets Can be extracted (the pointer field is similar to the one used on the MPEG pointer In the DS

Upstream MAC: Channel Bonding



- Each SID cluster runs a “single (or multiple) outstanding request” state machine that is considered a single transaction.
- SID Clusters

  The CMTS is NOT required to assign the same SID numbers across all upstreams. This set of those single SIDs that are spread across the upstreams is called a “SID Cluster”
- SID Cluster Group

  A group of several SID clusters used to request bandwidth
- Requests made based on bytes, not minislots.

Upstream MAC: Scheduling

- CMTS is free to use all burst profiles for data

  Thanks to CCF, and to the fact that requests are made in bytes, the CMTS is free to use any IUC to grant data (IUC5,6,9,10,11) – this opens the path to new forms of spectrum management and reduces the need for logical channels.

- Allow fragmentation prior to registration

  To prevent voice jitter when large pre-registration packets (DHCP-REQ) are sent

- T4 controlled by CMTS

  Instead of polling all channels at a T4 timeout interval, the CMTS is free to send unsolicited RNG-RSP

  T4 is configurable

DOCSIS 3.0 - PHY

PHY

- Downstream bonding requiring the simultaneous demodulation of a minimum of 4 carriers in a minimum capture band of 60MHz.
- Upstream bonding requiring the simultaneous burst transmission of up to 4 carriers.
  - Upstream bonding requires new spurious emissions requirements
- Upstream frequency has been increased
  - Options for either 65MHz or 85MHz.
- Lower modulation profile eliminated,
  - Only 1.28ms/s 2.56ms/s and 5.12ms/s are used in DOCSIS 3.0.
- sCDMA active code selection (MSC - Max Scheduled Codes)
  - sCDMA active code selection requires an additional logical channel
  - Not clear if MSC is needed with a good ingress noise canceller

DOCSIS 3.0- Enhanced multicast

Enhanced Multicast

- Cisco very much fathered the D3.0 solution to use DSID as a generic D3.0 mechanism to forward and filter downstream traffic to set (groups) of CMs, and even more specific CMIM-interfaces on CMs.

- Core concept : instead of snooping IGMP at the CM (DOCSIS 2.0 style), the IGMP passes transparently through the CM, the CMTS processes it, and with a DBC message instructs the CM which filters to set and which encryption key to use. Simple change, many benefits (next slide)

What problems are being solved?

IPv4/6 Multicast	Current (DOCSIS 1.1/2.0-based)	Future* (DOCSIS 3.0-based)
Key Benefit	Bandwidth Conservation	Optimized Network Utilization & Security
Cable Modem	Protocol-aware	Protocol-agnostic
Model	ASM / IGMPv2	SSM / IGMPv3
Channel Bonding	No	Yes
QoS	Proprietary, Static	Standard, Dynamic
IPv6 Multicast	No	Yes (MLDv1/2)
VPN	BPI+ Mandatory	BPI+ Optional
Tracking of Listeners	Limited	Explicit

*** Backwards compatible**

Enhanced Multicast – non DSID filtering

- DSID HW filtering in CM is considered problem on D2.0 CMs.
- This has resulted in additional requirements that make the D3.0 multicast spec unnecessarily complex

  Need to signal MAC addresses

  May need to use BPI just for isolation (SAID HW filter)

  => Still, should be acceptable work for the CMTS
- Non-ideal upstream multicast rules:

  Complex to provide separate mac-multicast domains between different CMIM-port sets in case strong service separation between e.g.: VDOC-STB ports and other ports is required.

DOCSIS 3.0- Security

Security Objectives

- Secure provisioning of CMs
  - Unauthorized CMs can be prevented network access
- Encrypt data traffic between the CM and CMTS
  - Best effort IP data traffic
  - QoS enabled IP data traffic
  - Multicast group traffic

Early Authentication and Encryption (EAE)

- Provides enhanced security
- Authenticate CM after Ranging/before DHCP
  - Network admission control
  - Eliminate possibility of bypassing authentication by manipulating config file
- EAE Signaling: TLV 6 in MDD (MAC Domain Descriptor) Message
- Can be enabled on a per CM or per MAC domain basis
- Per CM traffic: encrypted using primary SA (security association)

Enhanced Security – Secure Provisioning

- Authentication reuse:

  Encrypt DHCP, TOD, TFTP, and REG-REQ

- CMTS TFTP Proxy

  CMTS acts as a TFTP server to the CM and as TFTP client to the provisioning server

  This allows config parameters enforcement since CMTS receives the config file first from the Provisioning Server

  Config file authorization

  TFTP options: CM MAC addr and IP addr

- DHCPv6 authentication: Lightweight protocol
- New MIC hash algorithm: MMH

Enhanced Security – Additional Features

- AES required on CM and CMTS for DOCSIS 3.0
  - DES is required for backwards compatibility
- Source-verify is now standardized
- ARP rate-limit
- Cert revocation: CRL + OCSP
- Enhanced software validation

DOCSIS 3.0- OSSI

Network Management – Features

- IPDR service definitions
  - Fault management service specifications including diagnostic log
  - Configuration service specifications including CM topology
  - Accounting service specifications including optimized SAMIS
  - Performance service specifications including spectrum measurement
  - Security service specifications including CM status
- Diagnostic Log (Cisco driving and primary author)
  - Object descriptions are for fault management
  - Included in OSSI Annex G
- Enhanced Signal Quality Monitoring (Cisco driving and primary author)
  - Based on PHY requirements, object descriptions are for performance management
  - Included in OSSI Annex J

DOCSIS 3.0- Business Services

Business Services over DOCSIS

- Emulated T1 or E1 or NxDS0 services over DOCSIS
- TE-CM, TE-CMTS, TDM Emulation Adaptors (TEA), Pseudo Wire (PW) connecting two TEAs

IPv6 in Cable Networks

IPv6 in Cable Networks

- Brief overview of IPv6
- Motivation for Cable Operators
- IPv6 in DOCSIS 3.0
  - DOCSIS 3.x Reference Architecture
- Theory of Operations (DOCSIS 3.0)
  - Provisioning
- CMTS and CM requirements for IPv6

IPv6 in Cable Networks

- Brief overview of IPv6
- Motivation for Cable Operators
- IPv6 in DOCSIS 3.0
  - DOCSIS 3.x Reference Architecture
- Theory of Operations (DOCSIS 3.0)
  - Provisioning
- CMTS and CM requirements for IPv6

IPv6
More Than Just Addresses

- New address size and format
  - 128 bit vs. 32 bit addressing, 10B vs. 250M nodes
- Equitable global assignment
- Smarter packet
  - Simplified provisioning
    - Facilities for automatic configuration beyond DHCP
  - Built-in security
    - Mandated IPSec support
  - Improved mobility
    - Seamless handover between IP sub-networks
  - QoS via flow labels*
    - Even when the packet payload is encrypted
  - Support for Anycast and enhanced Multicast

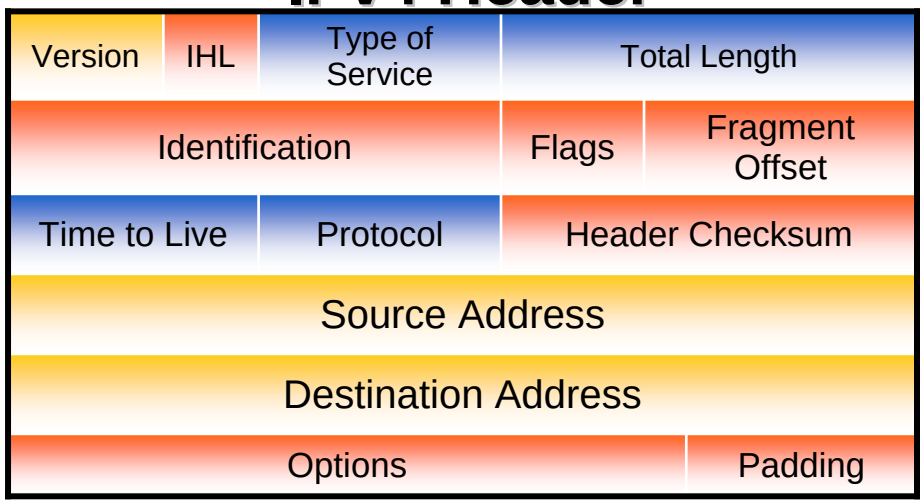
*** Not yet available from an implementation stand point**

Legacy IPv4 vs. IPv6 Comparisons

IP Service	*IPv4 Solution*	*IPv6 Solution*
Addressing Range	32-bit, Network Address Translation	128-bit, Multiple Scopes
Autoconfiguration	DHCP	Serverless Configuration, DHCP
Security	IPSec Optional	IPSec Mandated, works End-to-End
Mobility	Mobile IP	Mobile IP with Direct Routing
Quality-of-Service	DiffServ, IntServ	DiffServ, IntServ, Flow Labels
IP Multicast	IGMP/PIM/Multicast BGP	MLD/PIM/Multicast BGP,Scope Identifier
IP Anycast	--	Supported

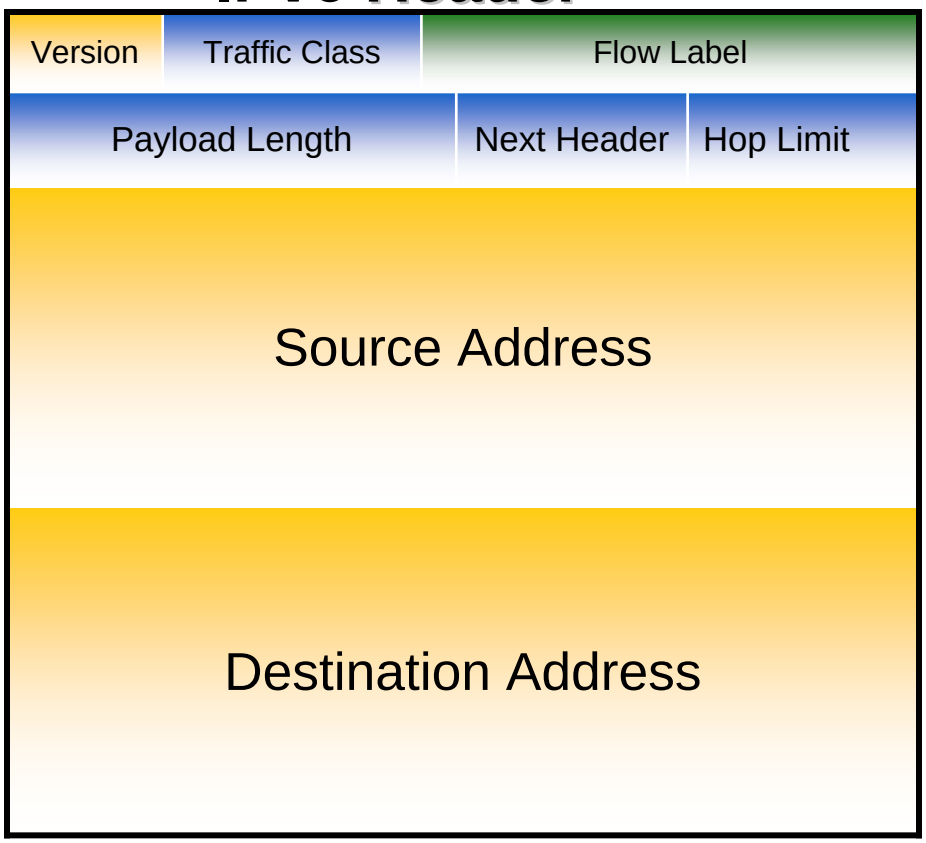
IPv4 & IPv6 Header Comparison

IPv4 Header



20 bytes (without options)

IPv6 Header



40 bytes

Legend

- **field's name kept from IPv4 to IPv6**
- **fields not kept in IPv6**
- **Name & position changed in IPv6**
- **New field in IPv6**

IPv6 in Cable Networks

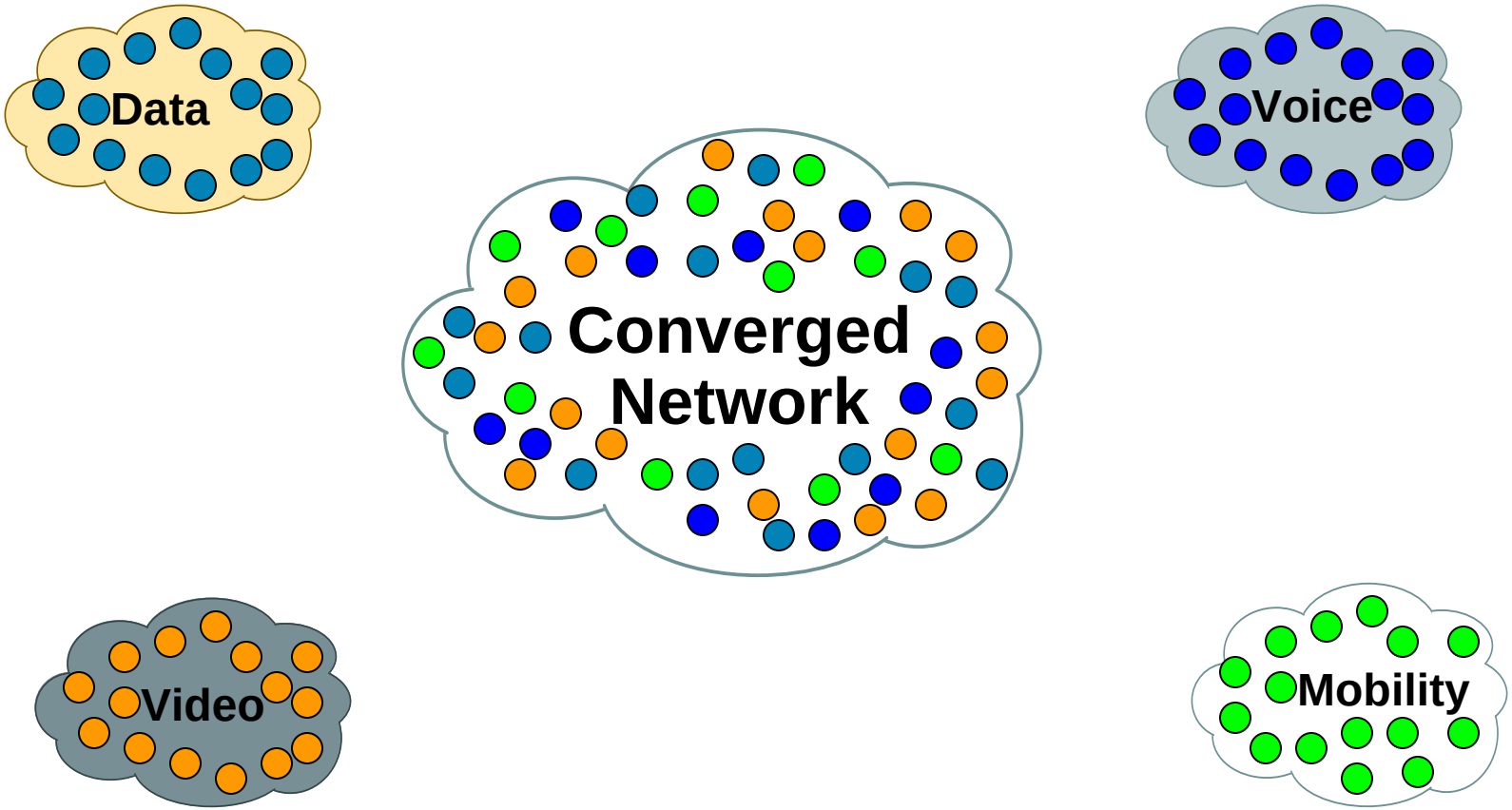
- Brief overview of IPv6
- Motivation for Cable Operators
- IPv6 in DOCSIS 3.0
  - DOCSIS 3.x Reference Architecture
- Theory of Operations (DOCSIS 3.0)
  - Provisioning
- CMTS and CM requirements for IPv6

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

- Convergence of multiple services over IP is driving the need for large scale addressing
  - MSO infrastructures
  - Home/SMB networks
- Industry consolidation has led to mergers of IP networks with overlapping addresses
  - Managing overlapping private address spaces is complex and expensive …
- Consumers demanding plug-&-play operation
  - Sling-boxes, IP cameras, PDAs, gateways, automobiles, media centers, IP phones, etc...
- Next generation applications require global transparency
  - Peer-to-peer connectivity without NAT
- Next generation services require access transparency
  - Seamless roaming across networks for fixed/mobile convergence

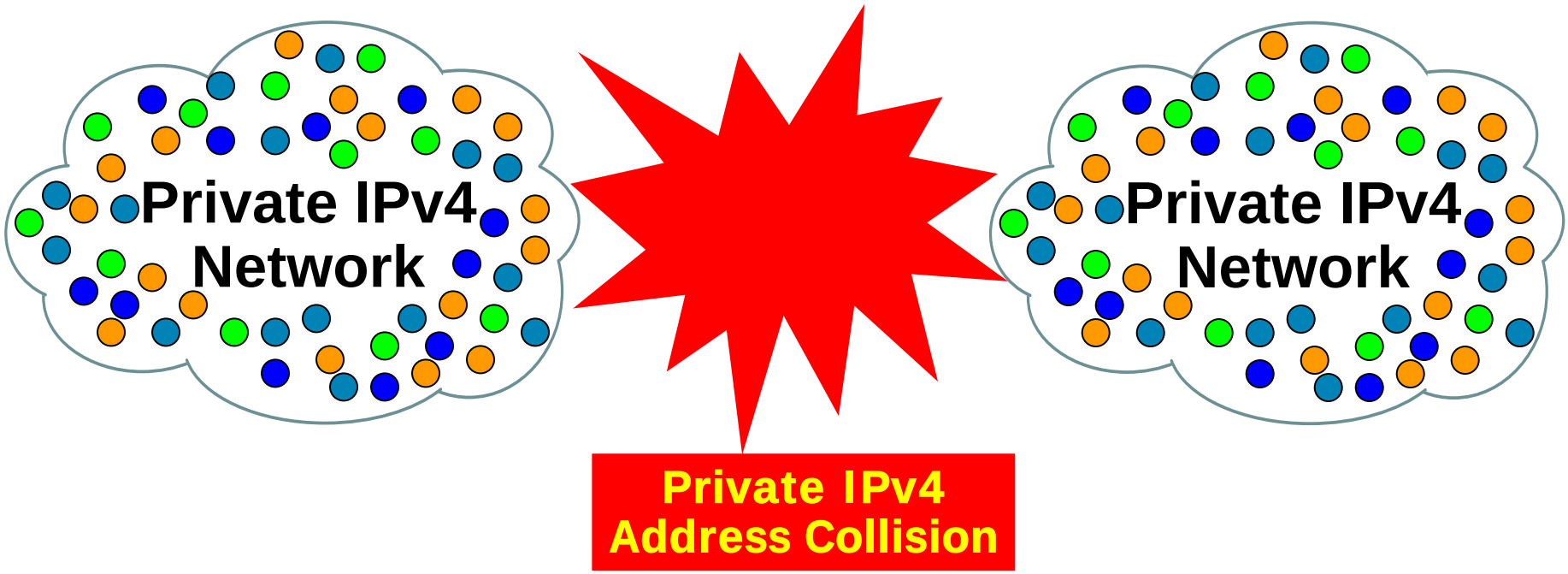
All IP Quad Play

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.

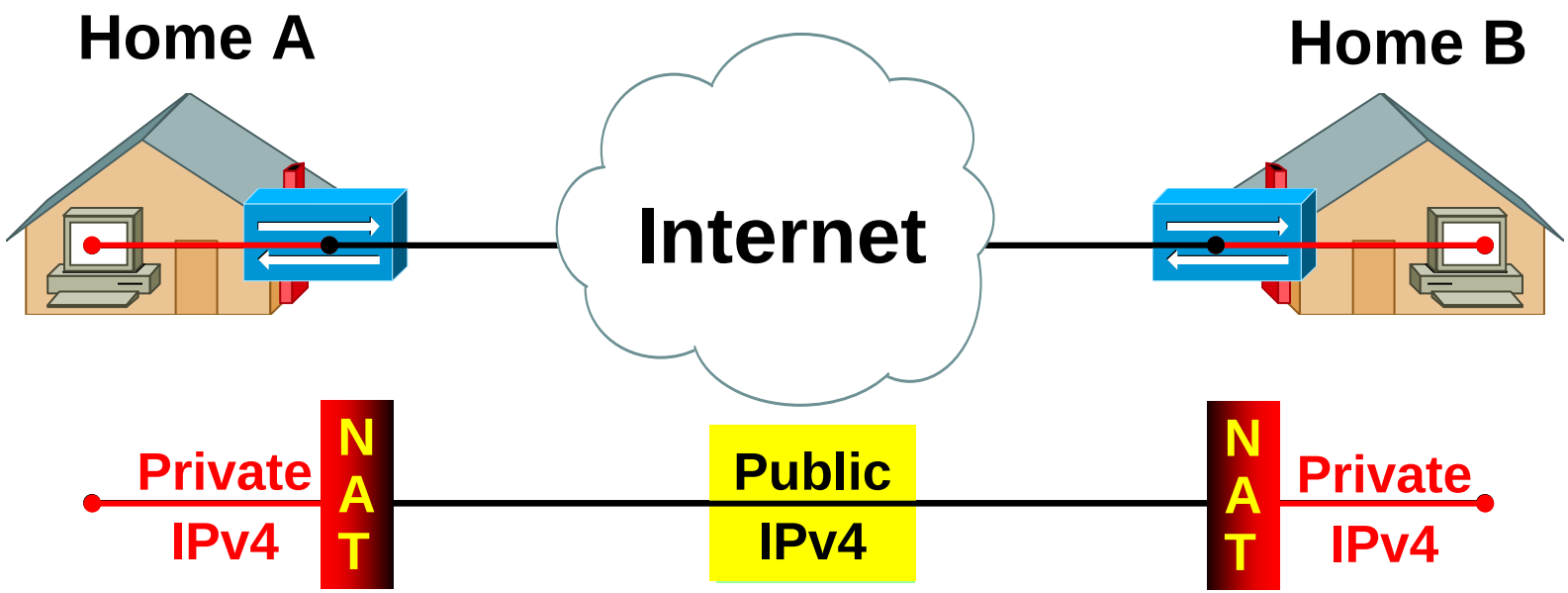


Plug-n-Play Home Networking

Premises network(s), automatic config. beyond DHCP

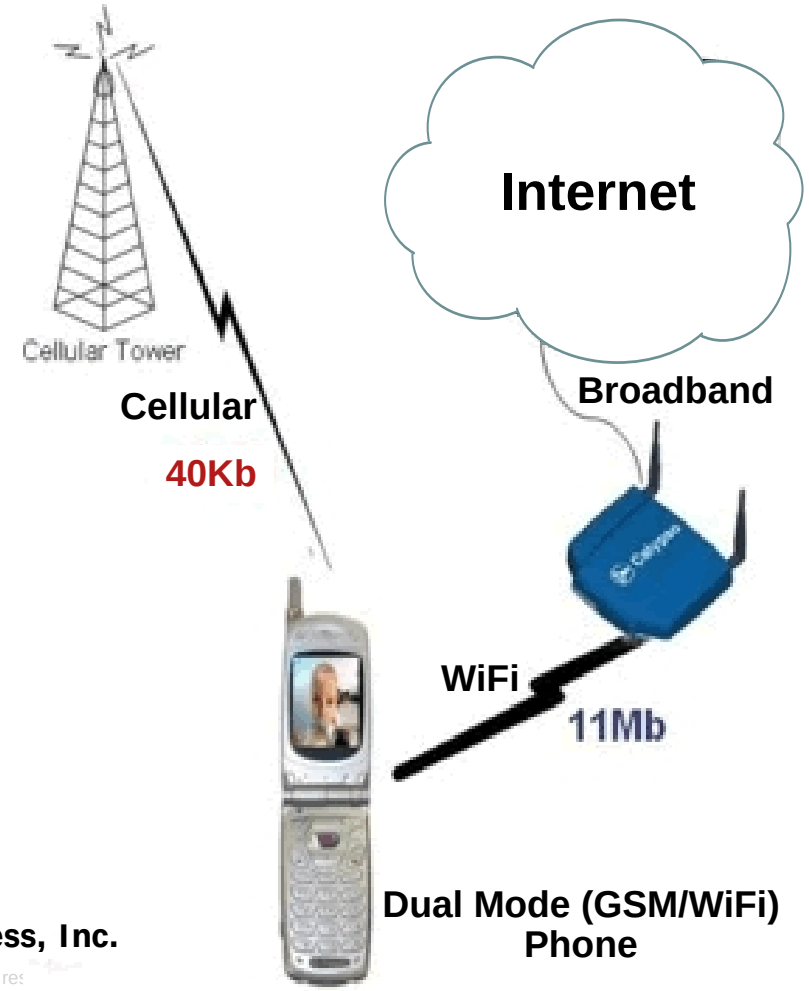
Global Transparency

IPv6 restores global transparency by getting rid of NAT.



Access Transparency

Mobile IPv6 improves mobility across access networks.



Sample Example : Calypso Wireless, Inc.

MSOs Current Status

- Frustrated with IPv4 addressing limitations - even RFC 1918
- Discussing IPv6 protocol fundamentals
- Hiring IPv6 experts and train management and operational staff
- Kicking off systems and network review for IPv6 support
- Developing testing strategy and plans for infrastructure trials
- Noticing Japan & APAC government heavily promoting IPv6
- Asking vendors → *"Got IPv6?"*

IPv6 in Cable Networks

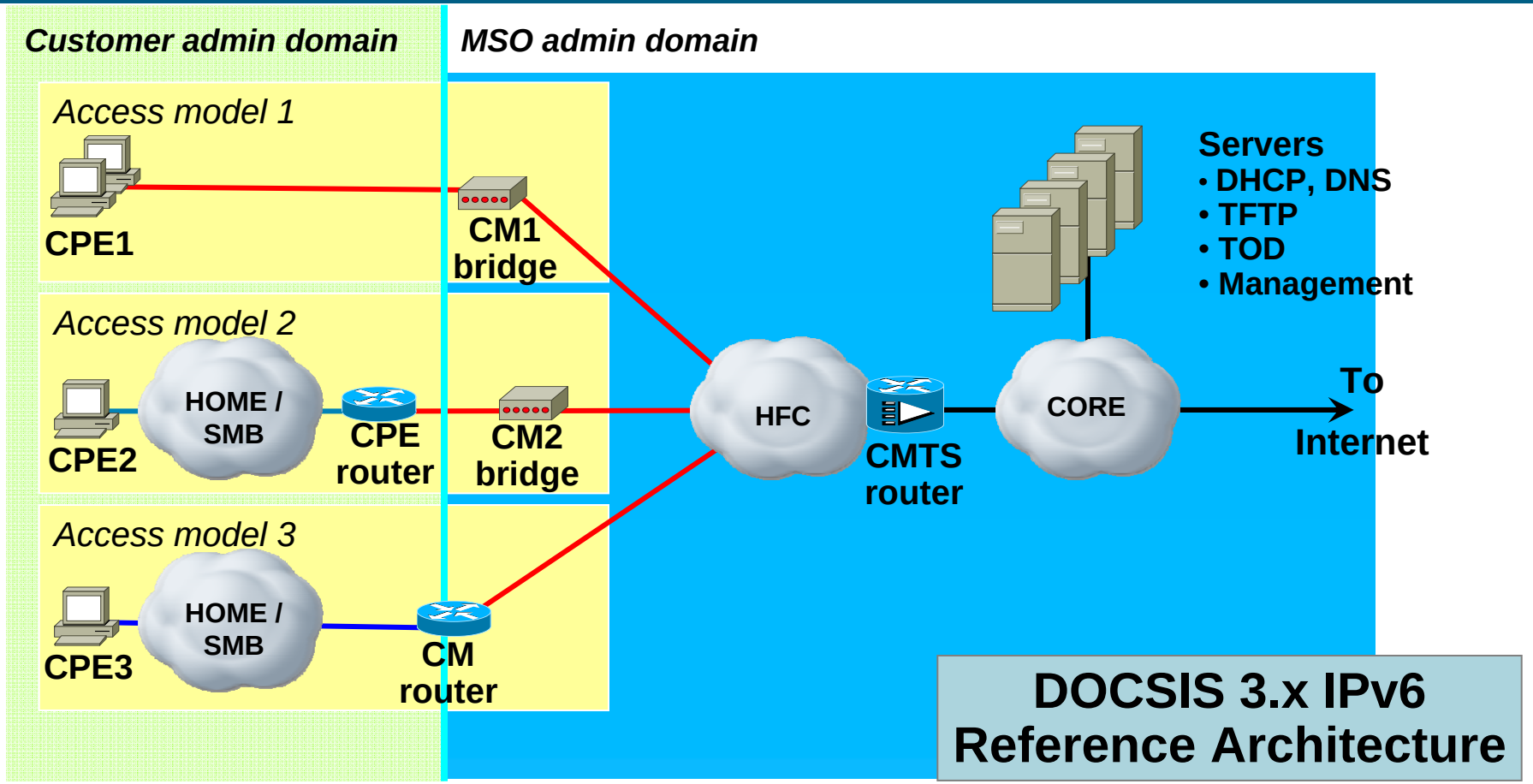
- Brief overview of IPv6
- Motivation for Cable Operators
- IPv6 in DOCSIS 3.0
  - DOCSIS 3.x Reference Architecture
- Theory of Operations (DOCSIS 3.0)
  - Provisioning
- CMTS and CM requirements for IPv6

CableLabs IPv6 Decision and Approach

- CableLabs members put IPv6 in consideration for DOCSIS 3.0
  - Cisco responded with proposal for IPv6 architecture and features
  - IPv6 was amongst the top DOCSIS 3.0 feature candidates
- Result: DOCSIS 3.x 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

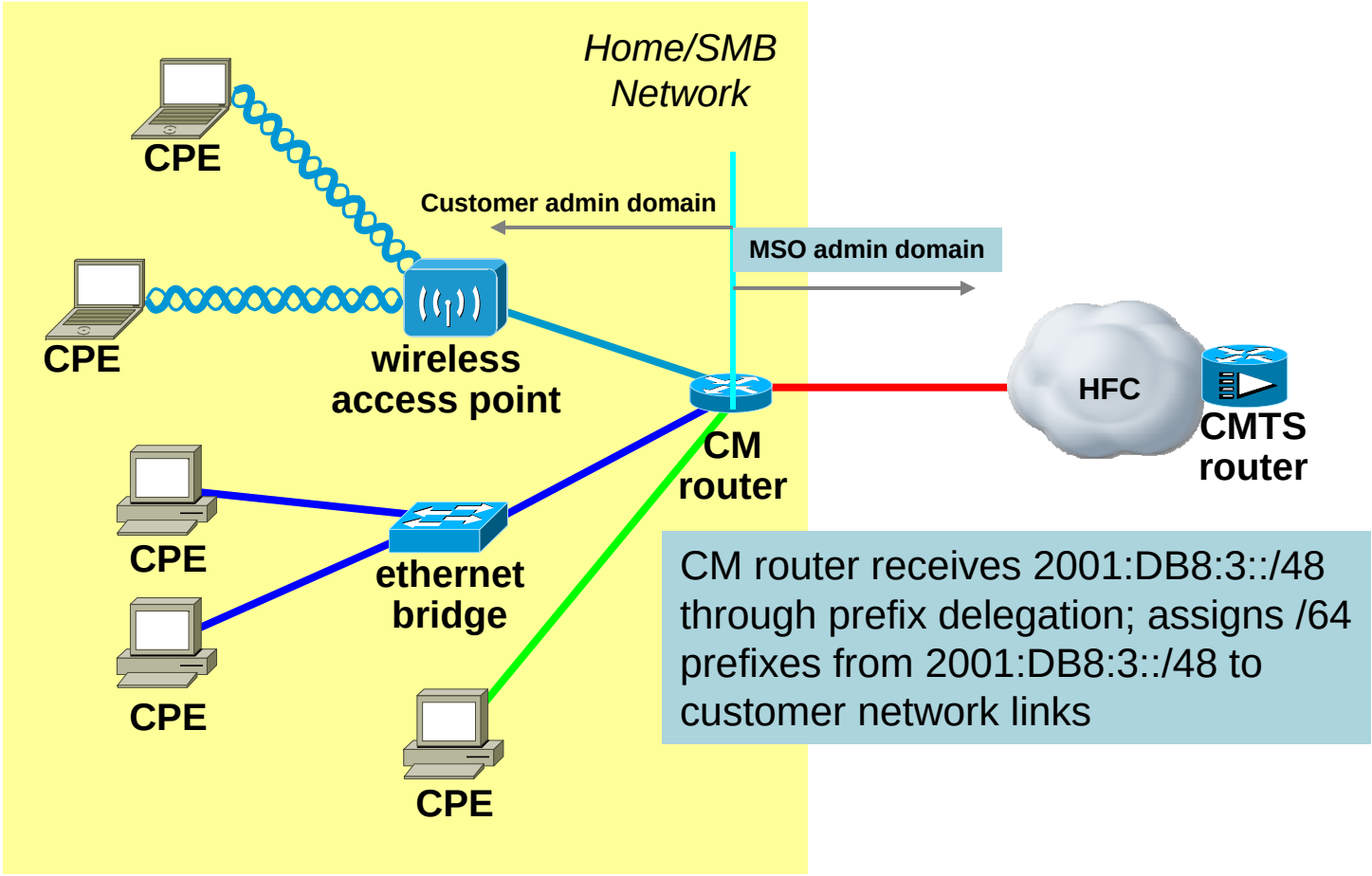
HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt) and 2001:DB8:FFFE:0::/64 (service)

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

Access Model 3 – Zoom In View



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

IPv6 in Cable Networks

- Brief overview of IPv6
- Motivation for Cable Operators
- IPv6 in DOCSIS 3.0
  - DOCSIS 3.x Reference Architecture
- Theory of Operations (DOCSIS 3.0)
  - Provisioning
- CMTS and CM requirements for IPv6

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

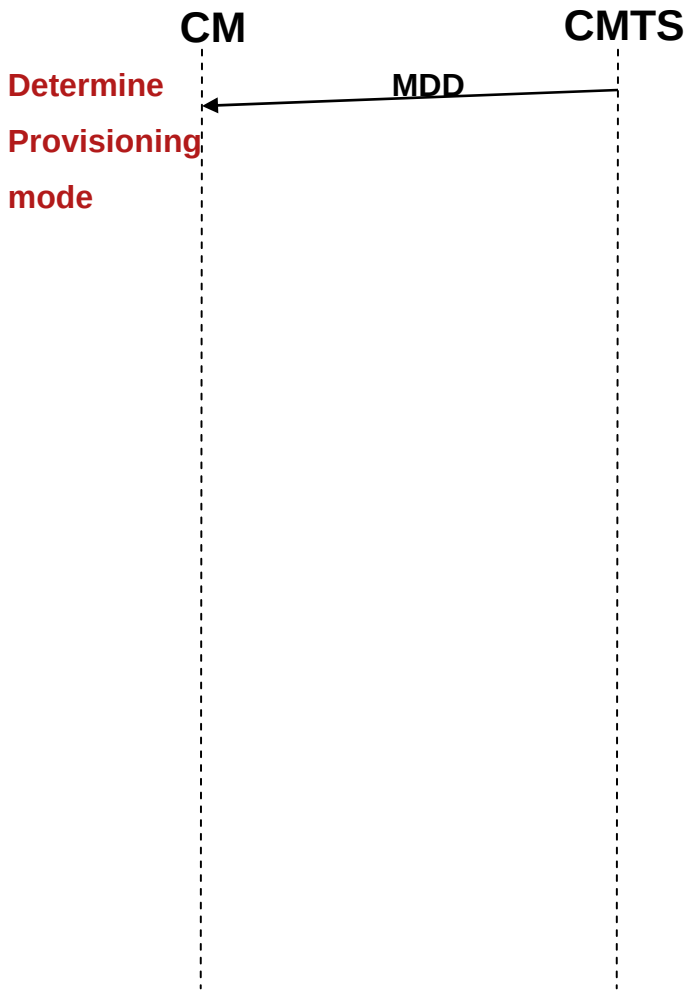
  If the CM does not receive any message from the CMTS it operates in DOCSIS 2.0 mode

CM provisioning

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

CM provisioning: Layer 2

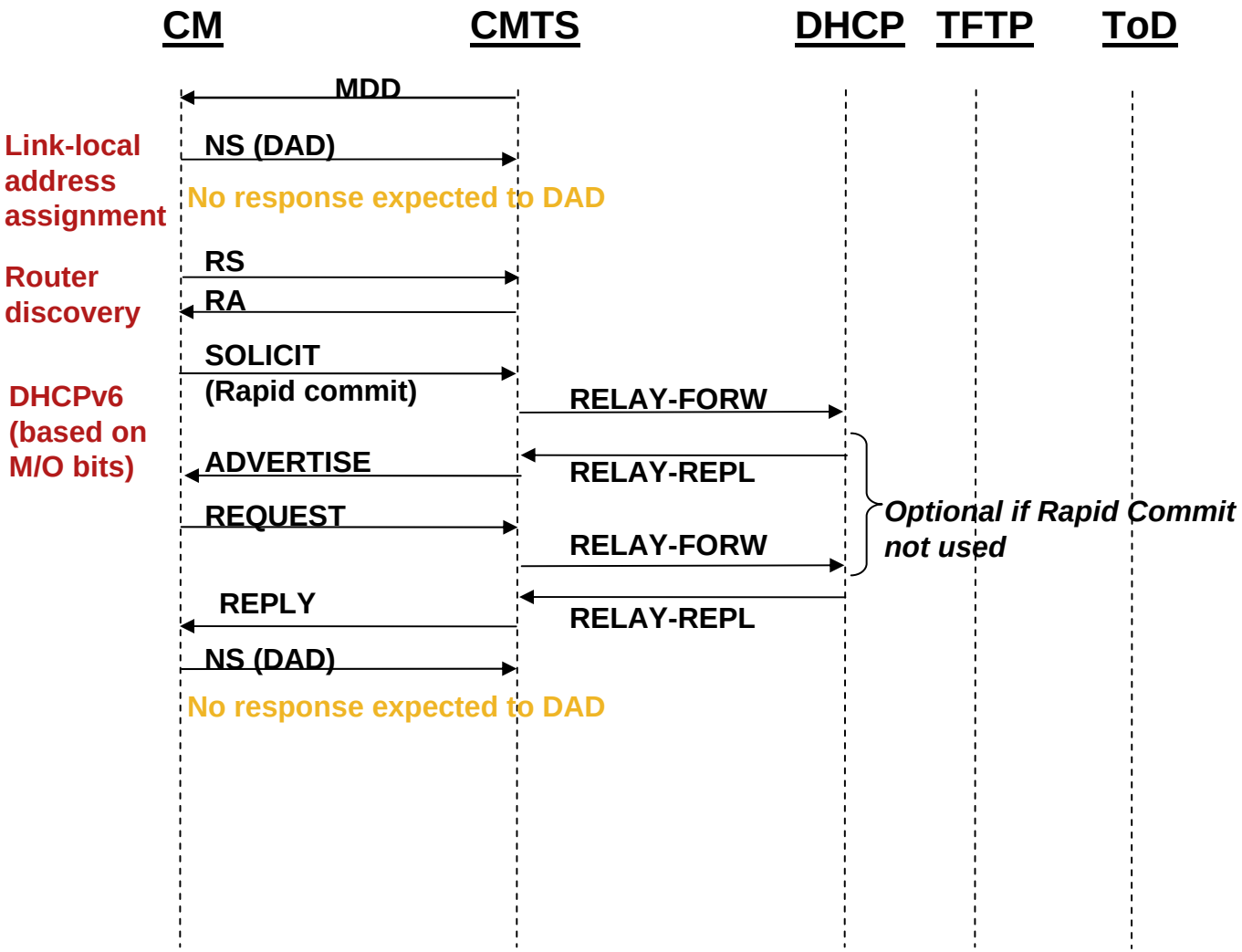
- CMTS sends an L2 message to the CM that controls
  - Use of IPv4 or IPv6 as the preferred mode for CM provisioning and management
  - Dual stack management
  - Alternate Provisioning Mode (APM): If preferred mode fails, restart provisioning in the alternate mode



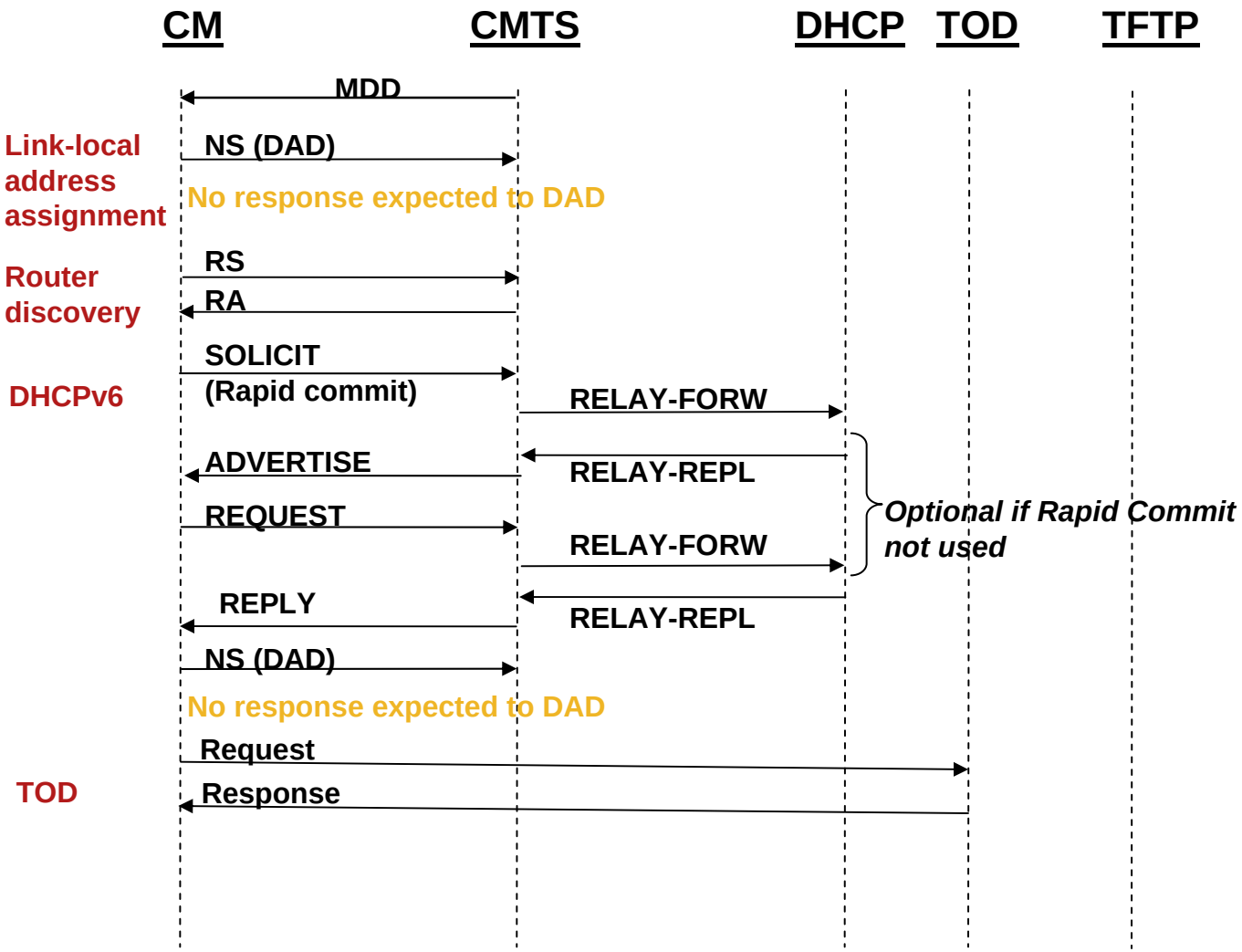
CM Provisioning: Acquire IP connectivity

- 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)

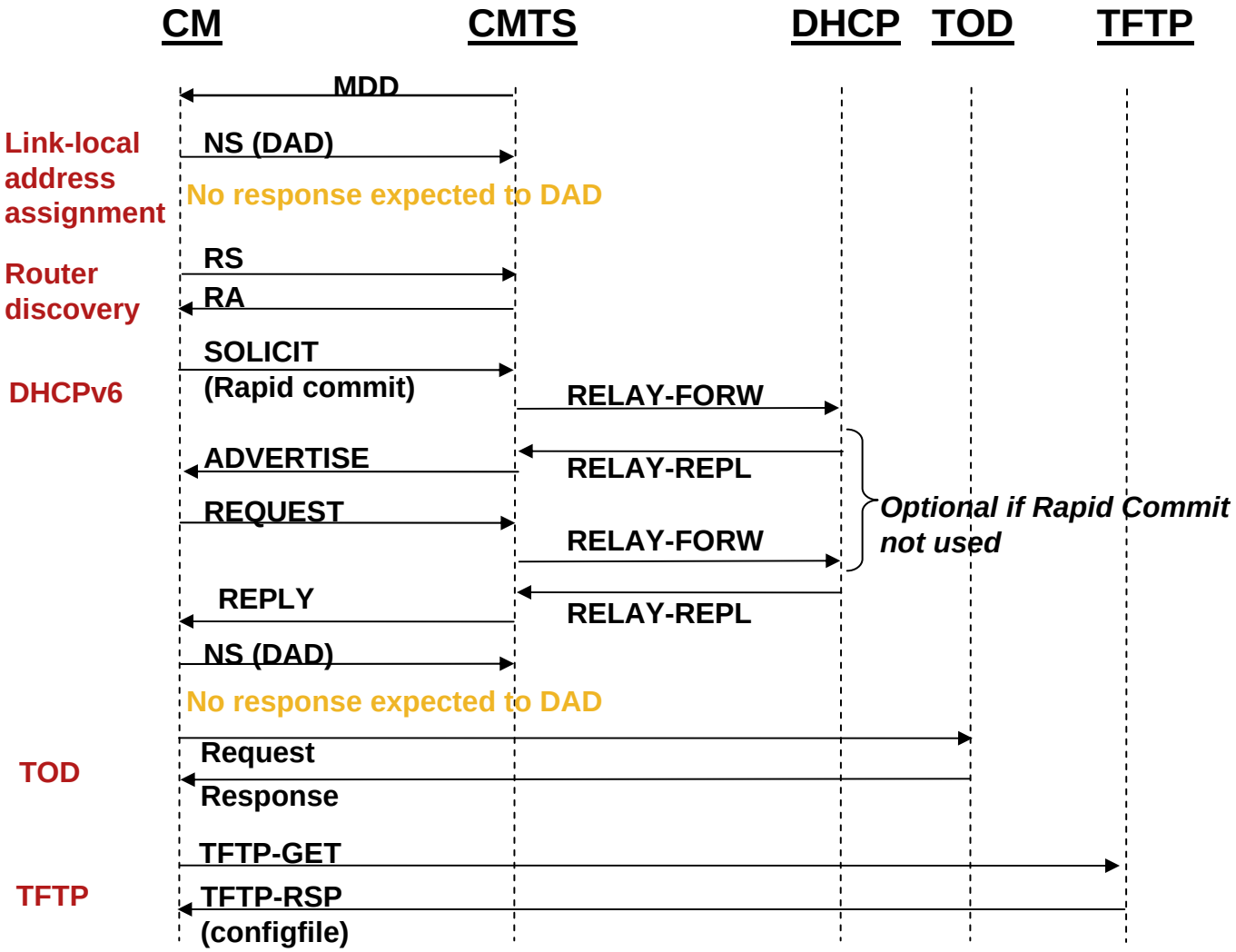
CM Provisioning: Acquire IP connectivity



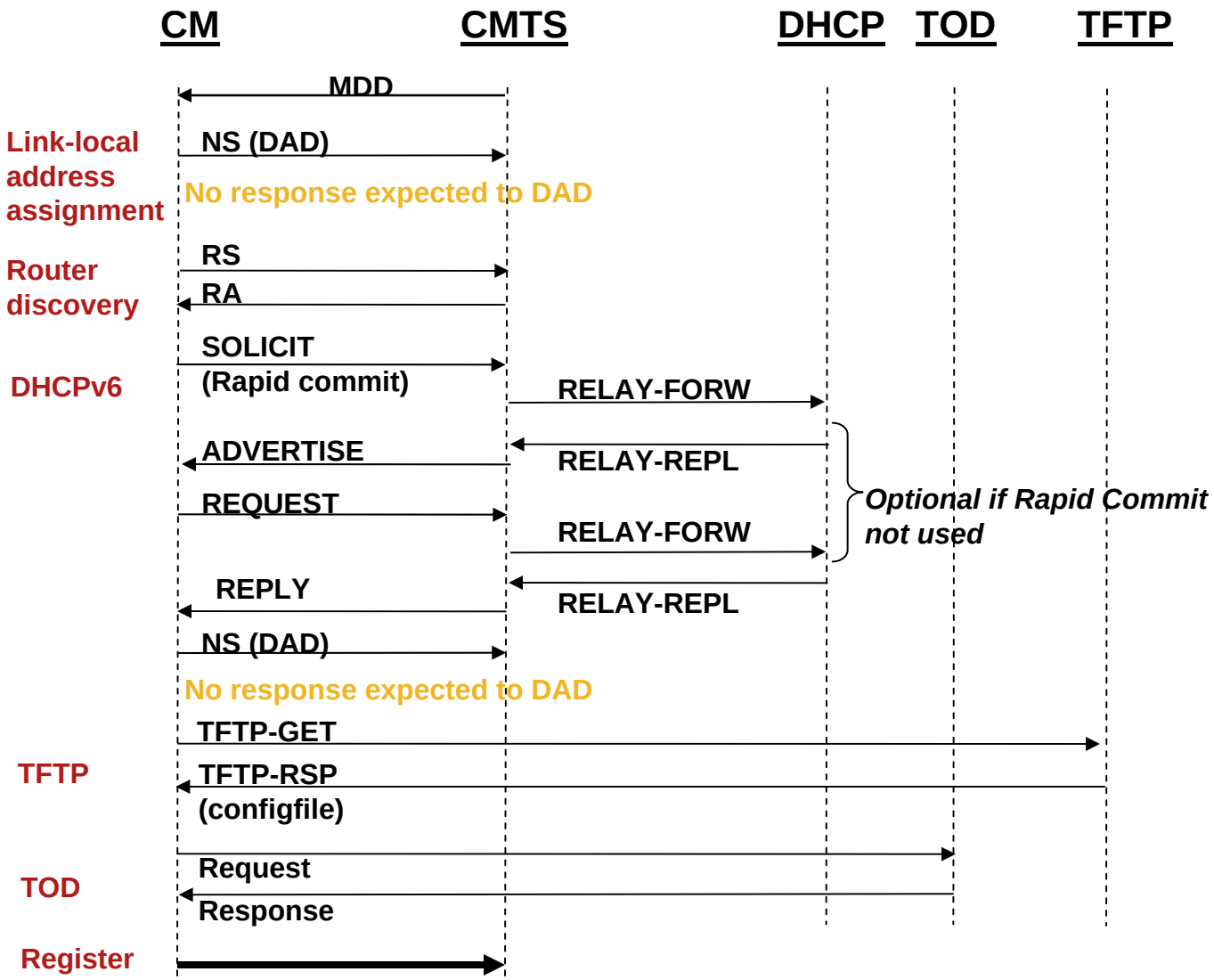
CM Provisioning: Obtain TOD



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)

IPv6 in Cable Networks

- Brief overview of IPv6
- Motivation for Cable Operators
- IPv6 in DOCSIS 3.0
  - DOCSIS 3.x Reference Architecture
- Theory of Operations (DOCSIS 3.0)
  - Provisioning
- 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

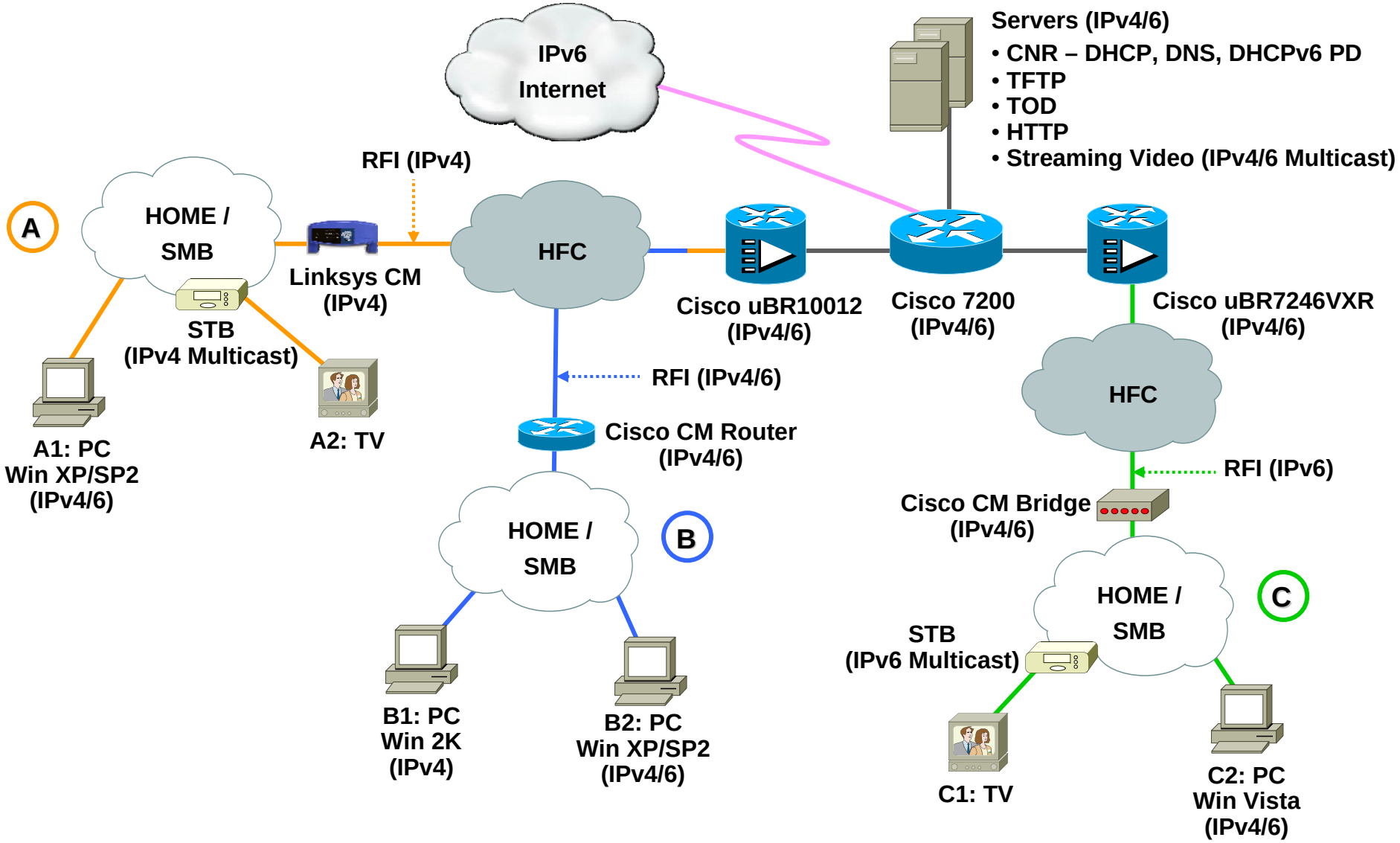
CM (bridge) requirements for IPv6

- 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

Cisco IPv6 Demo Topology



-> DOCSIS 3.0 Intro

Summary

Concluding Remarks

- DOCSIS 3.0/M-CMTS

  Promises significant cost reduction and bandwidth increase

  Enhanced security, enhanced network management, enhanced multicast, business services

  Adds IPv6: potential to reduce MSO operational costs and enable next generation applications

  Is backward compatible with existing DOCSIS standards

  Allows for a phased deployment

Meet the Experts
IP NGN Architectures and Technologies

- Oliver Boehmer
  Network Consulting Engineer

- Moustafa Kattan
  Consulting Systems Engineer

- Yves Hertoghs
  Distinguished System Engineer

- Ed Draiss
  Product Manager

Recommended Reading

BRKBBA -2007

- Continue your Networkers learning experience with further reading from Cisco Press.
- Visit the on-site Cisco company store, where the full range of Cisco Press books is available for you to browse.

Q and A