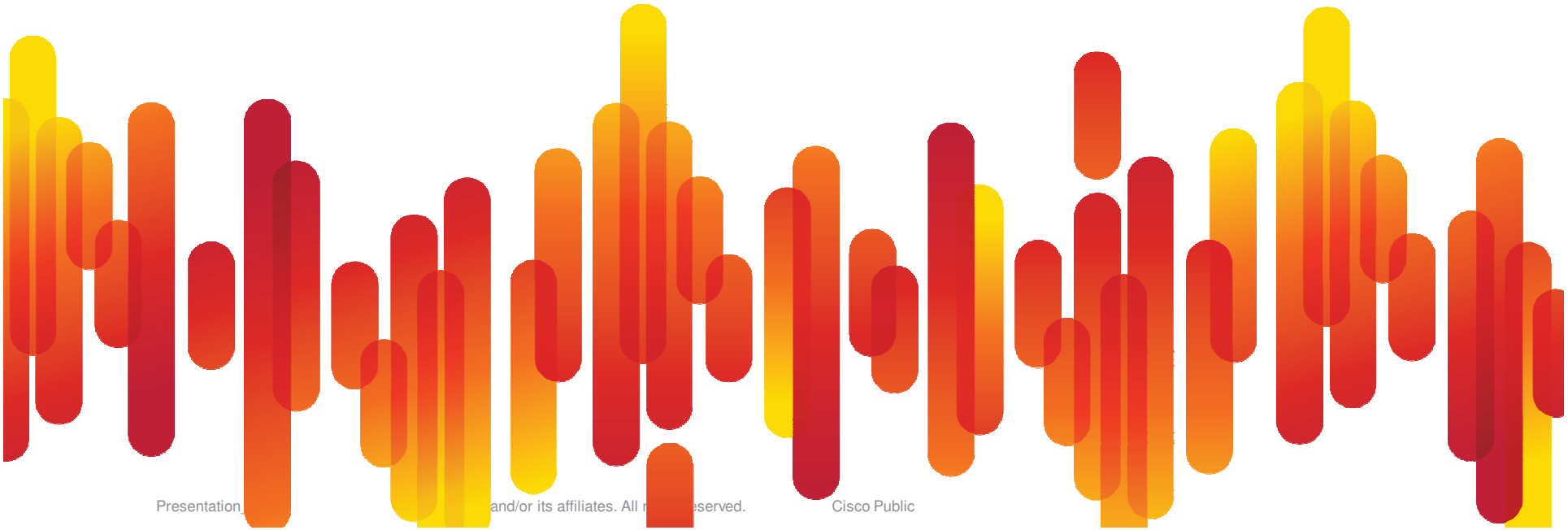
Service Provider IPv6 Deployment Overview
RMv6TF IPv6 Summit – 2011

Salman Asadullah
Cisco Distinguished Engineer
IPv6 Forum Fellow

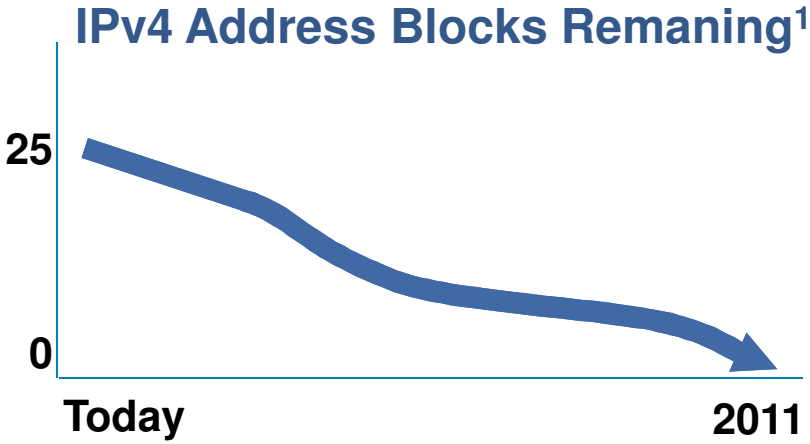


Agenda

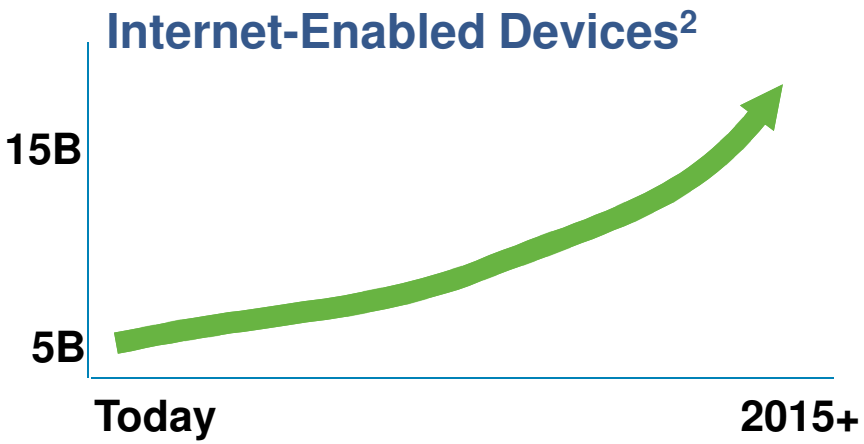
- SP IPv6 Integration Strategy
- IPv6 in Core Networks and Deployment Models
  - Native IPv4 Environments
  - MPLS Environments
- IPv6 in Access Networks and Deployment Models
  - IPv4 Translation (NAT444)
  - IPv6 Integration
  - DOCSIS 3.0 IPv6 Reference Architecture
  - IPv6 Provisioning
- Conclusion

The Growing Internet Challenge …

The gap between supply and demand for IP addresses – the key Internet resource – is **widening**



The pool of IPv4 address blocks is **dwindling rapidly**

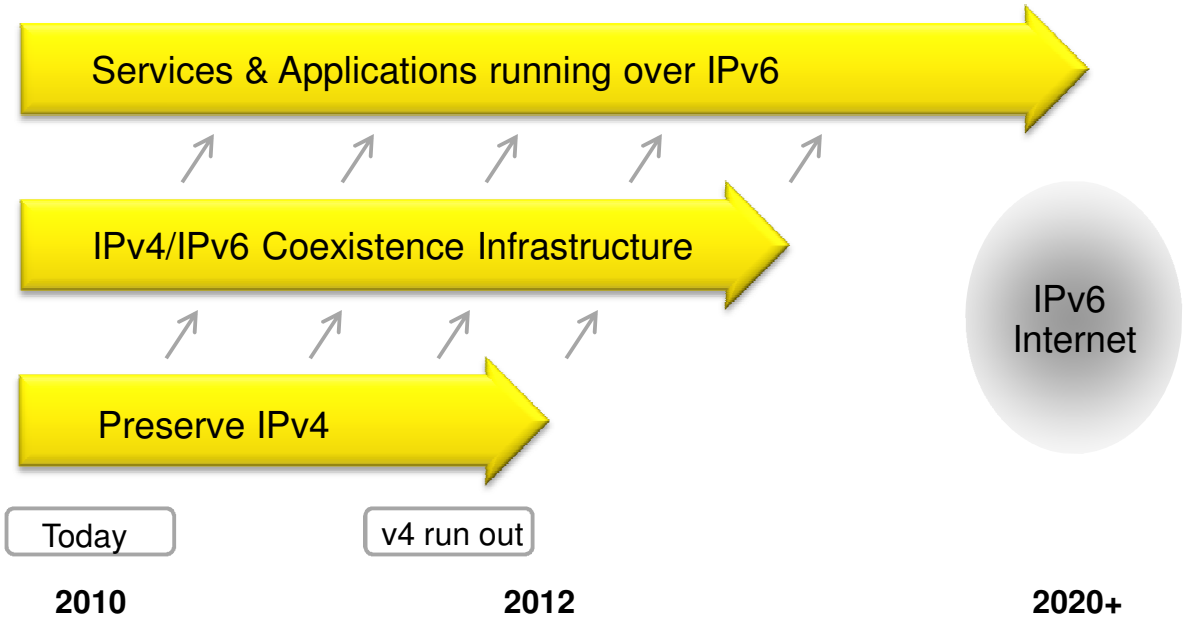


While the number of new Internet devices is **exploding**

Projected IANA Unallocated Address Pool Exhaustion: Feb-2011
Projected RIR Unallocated Address Pool Exhaustion: Sep-2011

... and Internet Evolution

Moving to 3 IP Address Families: Public IPv4, Private IPv4, IPv6



IPv6 in the SP: Drivers

- **External Drivers**

  SP customers that need access to IPv6 resources (for development or experimentation purposes)

  SP customers that need to interconnect their IPv6 sites

  SP customers that need to interface with their own customers over IPv6 (ex: contractors for DoD)

- **Internal Drivers**

  Handle some problems that are hard to fix with IPv4 (ex: managing large number of devices such **as Cell phones, set-tops, IP cameras, sensors, etc.)**

    Public IPv4 address exhaustion (~2011/2012)

    Private IPv4 address exhaustion

- **Strategic Drivers**

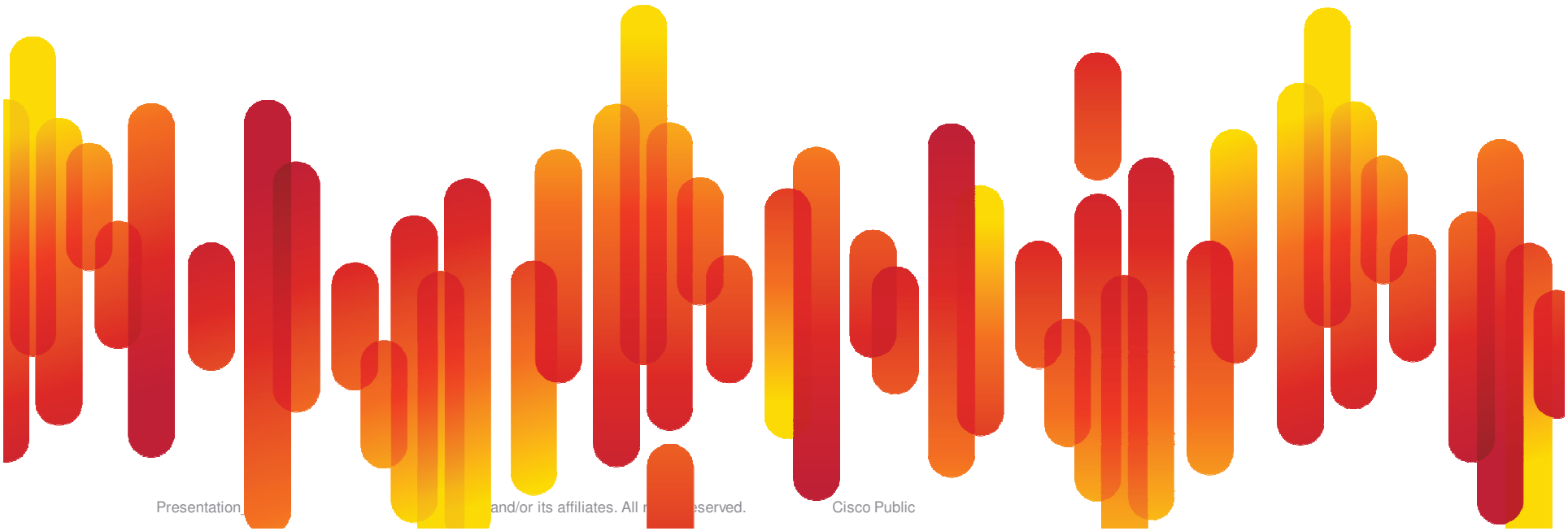
  Long term expansion plans and service offering strategies

  Preparing for new services and gaining competitive advantage

IPv6 Integration and Co-Existence

- Many ways to deliver IPv6 services to End Users, Most important is End to End IPv6 traffic forwarding as applications are located at the edge
- SPs may have different deployment needs and mechanisms but basic steps are common
  - IPv6 Addressing Scheme
  - Routing Protocol(s)
  - IPv6 Services - QoS, Multicast, DNS, …
  - Security
  - Network Management
- Resources are shared between the two protocols for both Control and Forwarding Plane. Evaluate processor utilization and memory needs
- Most vendors have good IPv6 HW forwarding performance

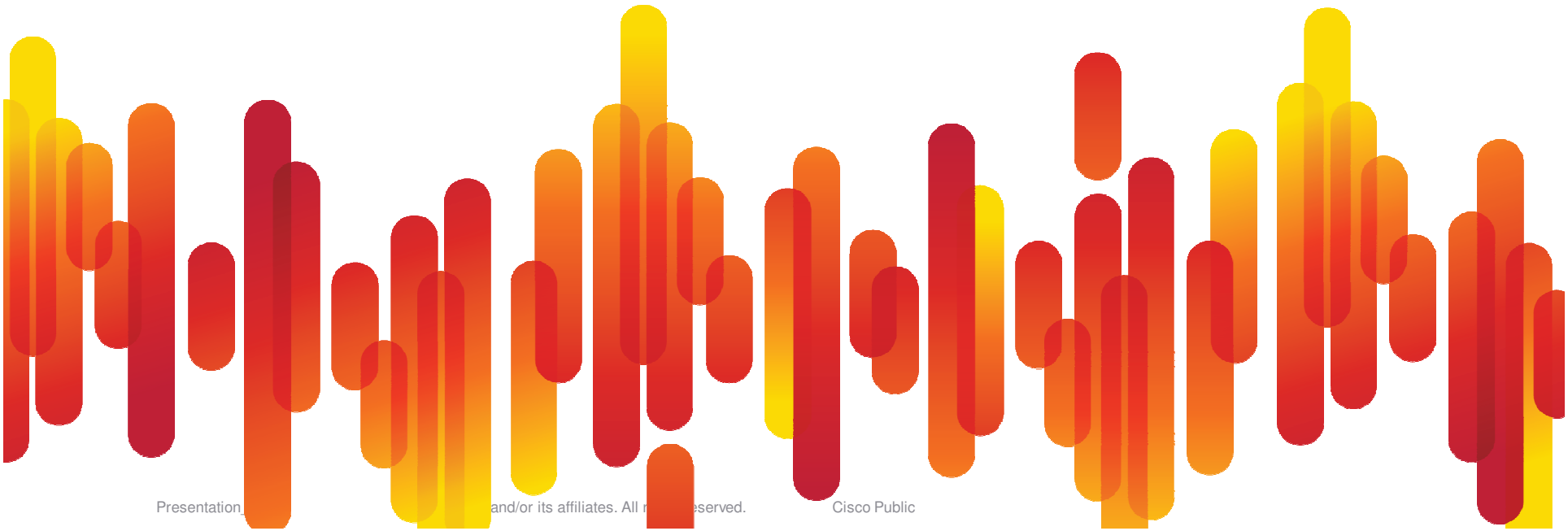
IPv6 in Core Networks and Deployment Models



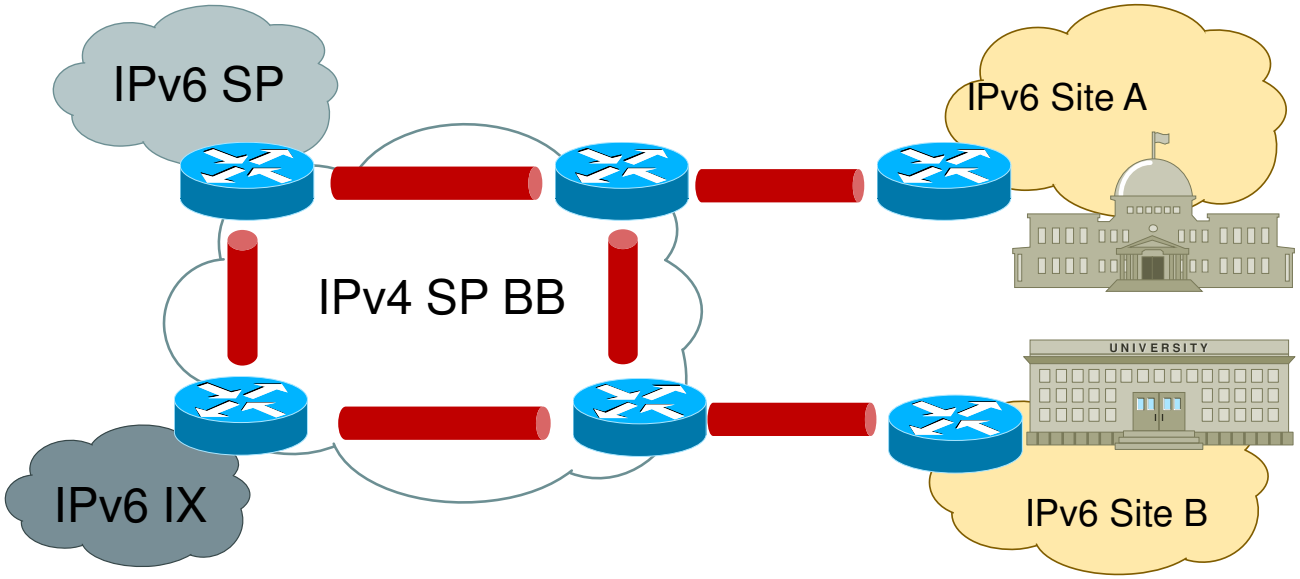
IPv6 Deployment Options — CORE

- SP Core Infrastructures – 2 Basic Paths
  - Native IPv4 core with associated services
    - L2TPv3, QoS, Multicast, …
  - MPLS with its associated services
    - MPLS/VPN, L2 services over MPLS, QoS, …
- IPv6 in Native IPv4 Environments
  - Tunneling IPv6-in-IPv4
  - Native IPv6 with Dedicated Resources
  - Dual-Stack IPv4 and IPv6
- IPv6 in MPLS Environments
  - 6PE
  - 6VPE

IPv6 in Native IPv4 Environments

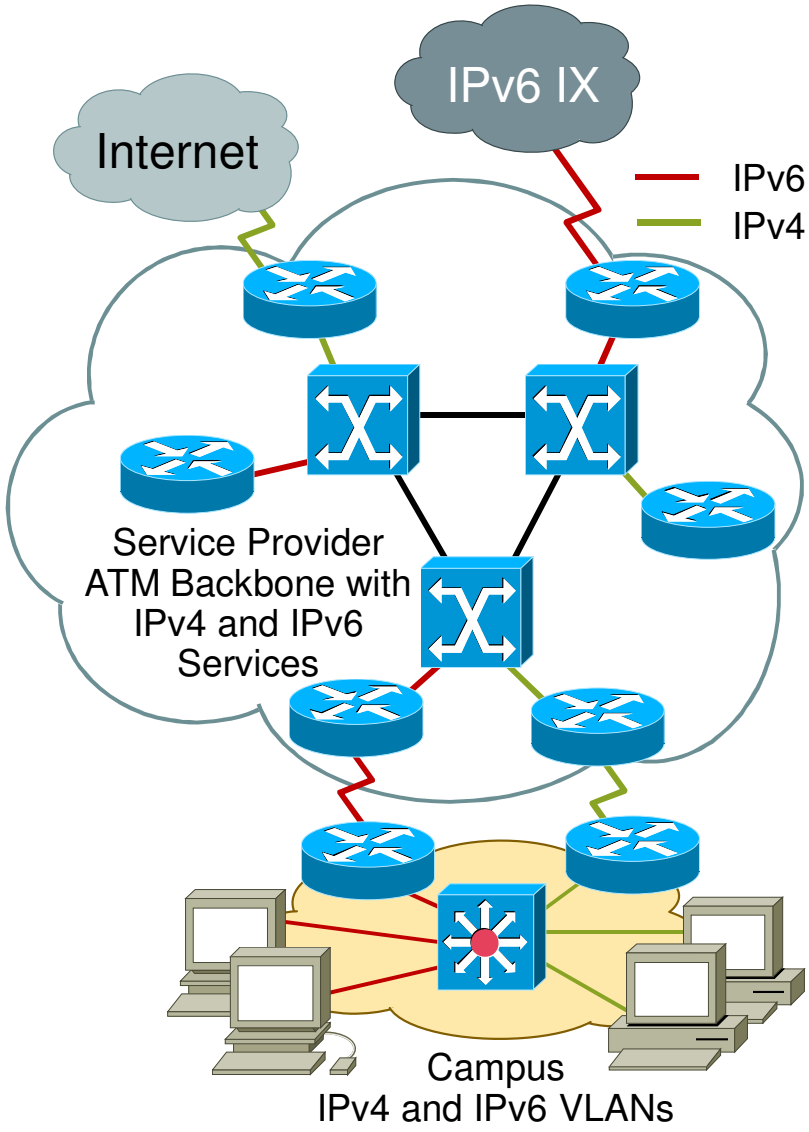


Tunnelling IPv6 in IPv4



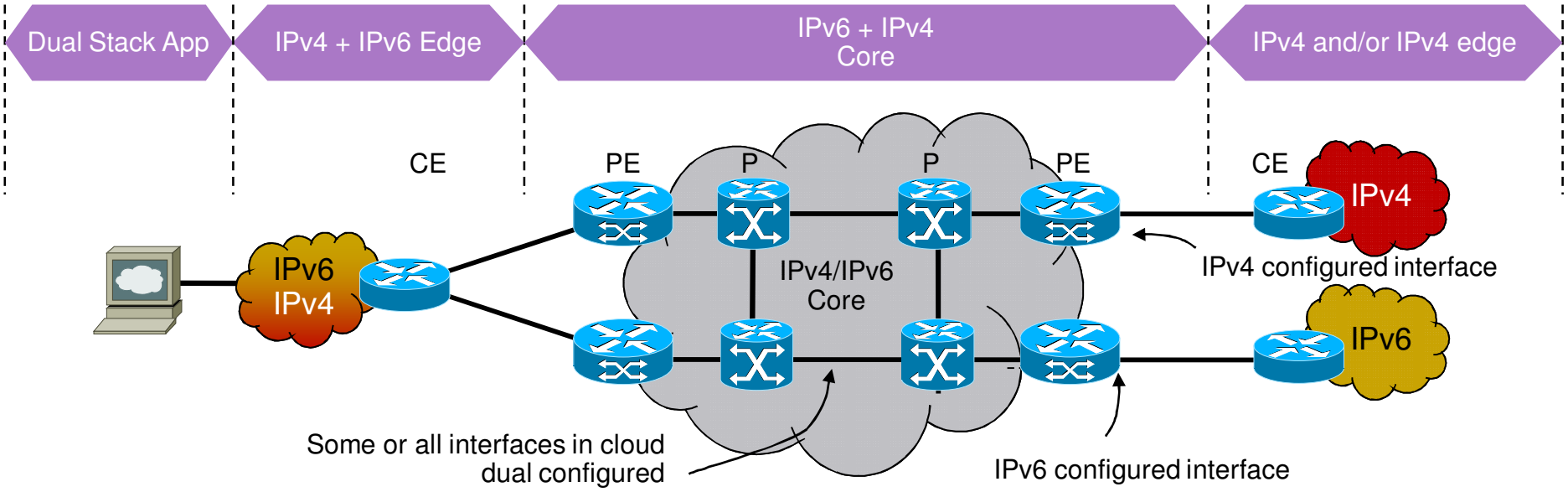
- Tunnelling Options
  - Manual Tunnels (RFC 2893), GRE Tunnels (RFC 2473), L2TPv3, …
- SP Scenarios
  - Configured Tunnels in Core
  - Configured Tunnels or Native IPv6 to IPv6 Enterprise's Customers
  - MP-BGP4 Peering with other IPv6 users
  - Connection to an IPv6 IX

Native IPv6 over Dedicated Data Link



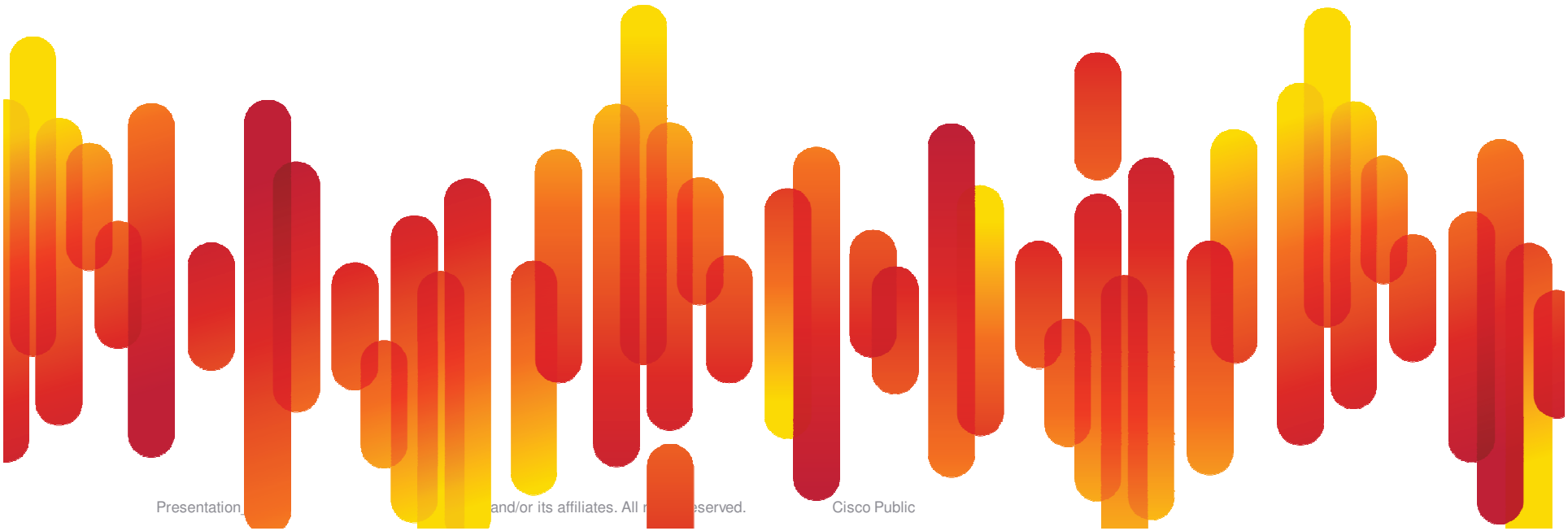
- ISP Scenario
  - Dedicated Data Links between Core routers
  - Dedicated Data Links to IPv6 Customers
  - Connection to an IPv6 IX

Dual Stack IPv4 and IPv6



- All P + PE routers are capable of IPv4+IPv6 support
- Two IGPs supporting IPv4 and IPv6
- Memory considerations for larger routing tables
- Native IPv6 multicast support
- All IPv6 traffic routed in global space
- Good for content distribution and global services (Internet)

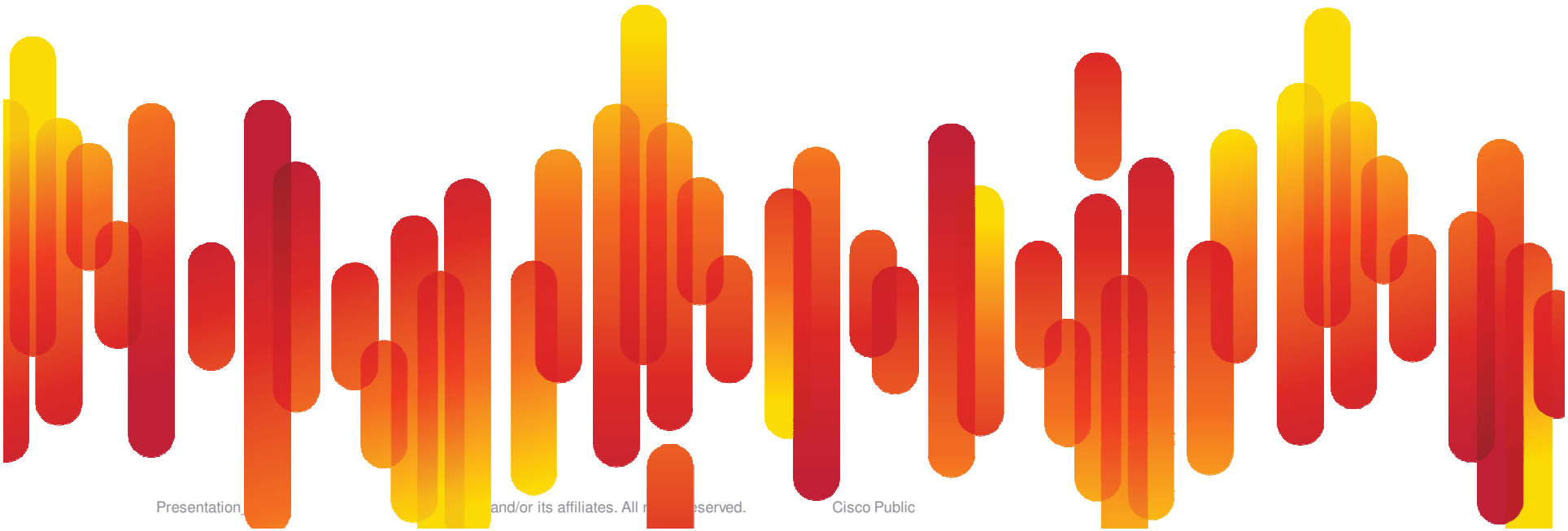
IPv6 in MPLS Environments



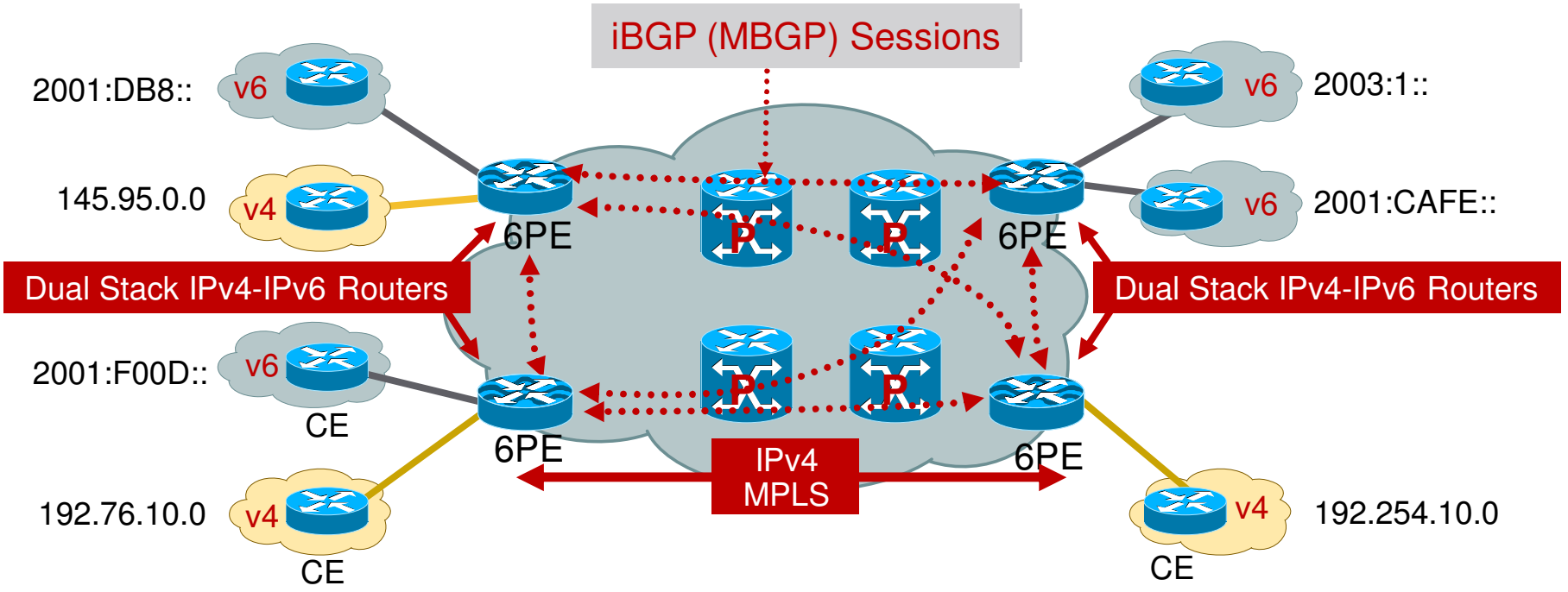
IPv6 over MPLS

- Many ways to deliver IPv6 services to end users
  - Most important is end-to-end IPv6 traffic forwarding
- Many service providers have already deployed MPLS in their IPv4 backbone for various reasons
- MPLS can be used to facilitate IPv6 integration
- Multiple approaches for IPv6 over MPLS:
  - IPv6 over L2TPv3
  - IPv6 over EoMPLS/AToM
  - IPv6 CE-to-CE IPv6 over IPv4 tunnels
  - IPv6 Provider Edge Router (6PE) over MPLS
  - IPv6 VPN Provider Edge (6VPE) over MPLS
  - Native IPv6 MPLS

6PE Overview



IPv6 Provider Edge Router (6PE) over MPLS

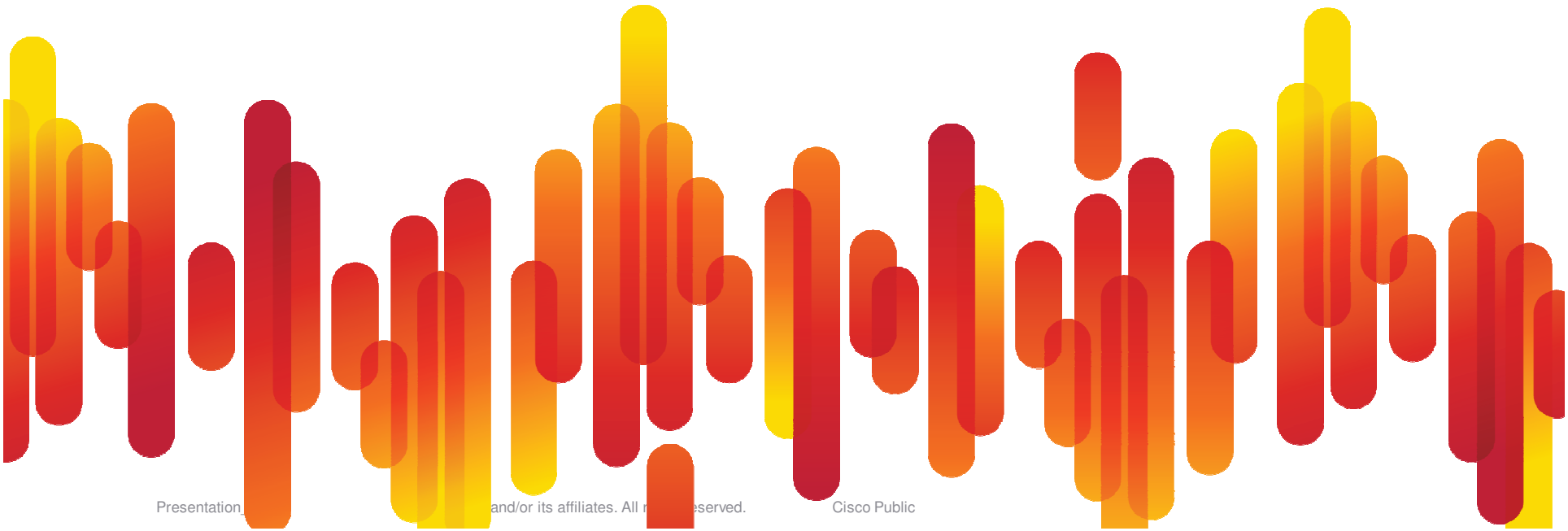


- IPv6 global connectivity over and IPv4-MPLS core
- Transitioning mechanism for providing unicast IP
- PEs are updated to support dual stack/6PE
- IPv6 reachability exchanged among 6PEs via iBGP (MBGP)
- IPv6 packets transported from 6PE to 6PE inside MPLS

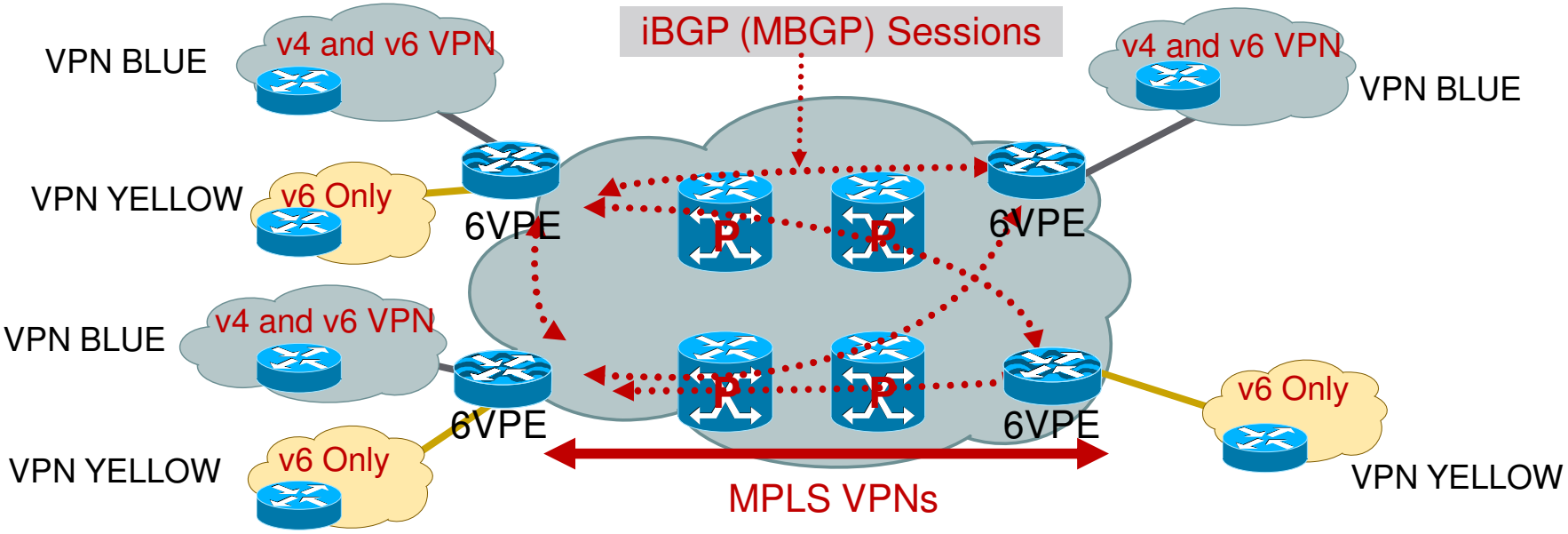
6PE Benefits/Drawbacks

- Core network (Ps) untouched
- IPv6 traffic inherits MPLS benefits (fast re-route, TE, etc.)
- Incremental deployment possible (i.e., only upgrade the PE routers which have to provide IPv6 connectivity)
- Each site can be v4-only, v4VPN-only, v4+v6, v4VPN+v6
- P routers won't be able to send ICMPv6 messages (TTL expired, trace route)
- Scalability issues arise as a separate RIB and FIB is required for each connected customer
- Good solution only for SPs with limited devices in PE role
- Cisco 6PE Documentation/Presentations:
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_data_sheet09186a008052edd3.html

6VPE Overview



6VPE over MPLS



- 6VPE ~ IPv6 + BGP-MPLS IPv4VPN + 6PE
- Cisco 6VPE is an implementation of RFC4659
- VPNv6 address:

  Address including the 64 bits route distinguisher and the 128 bits IPv6 address

- MP-BGP VPNv6 address-family:

  AFI “IPv6” (2), SAFI “VPN” (128)

- VPN IPv6 MP_REACH_NLRI

  With VPNv6 next-hop (192bits) and NLRI in the form of <length, IPv6-prefix, label>

- Encoding of the BGP next-hop

6VPE Summary

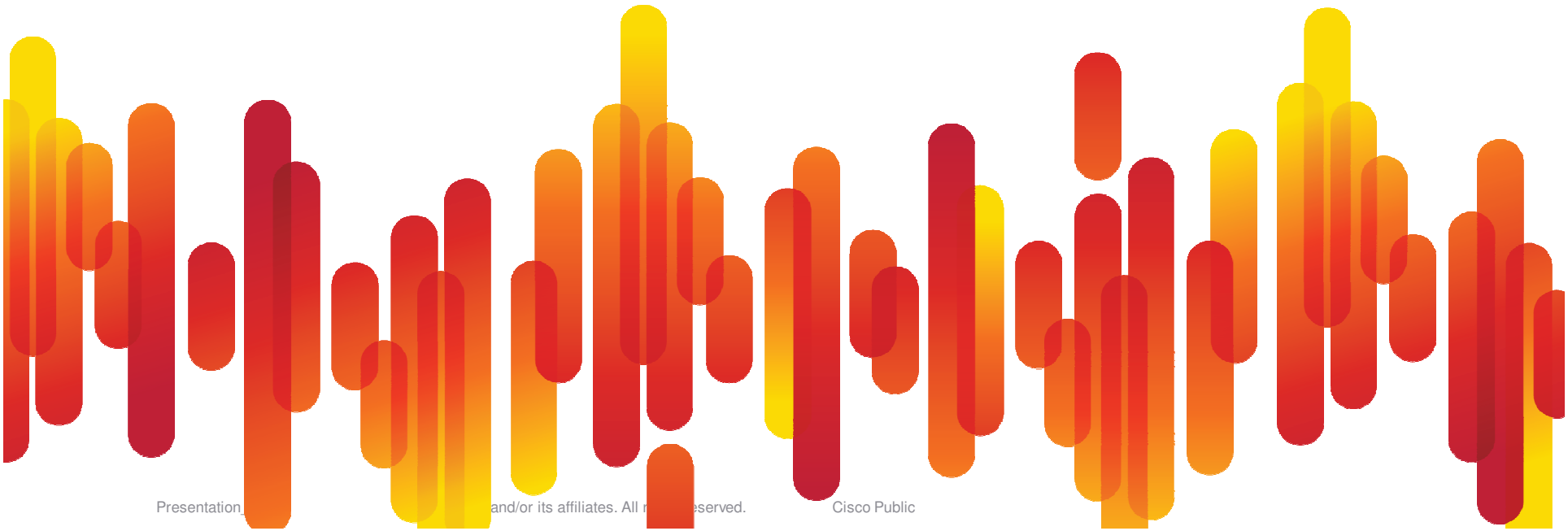
- RFC4659: BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
- 6VPE simply adds IPv6 support to current IPv4 MPLS VPN offering
- For end-users: v6-VPN is same as v4-VPN services (QoS, hub and spoke, internet access, etc.)
- For operators:

  Same configuration operation for v4 and v6 VPN

  No upgrade of IPv4/MPLS core (IPv6 unaware)
- Cisco 6VPE Documentation:

  http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/mpls_vpn/user/guide/ipv6.html

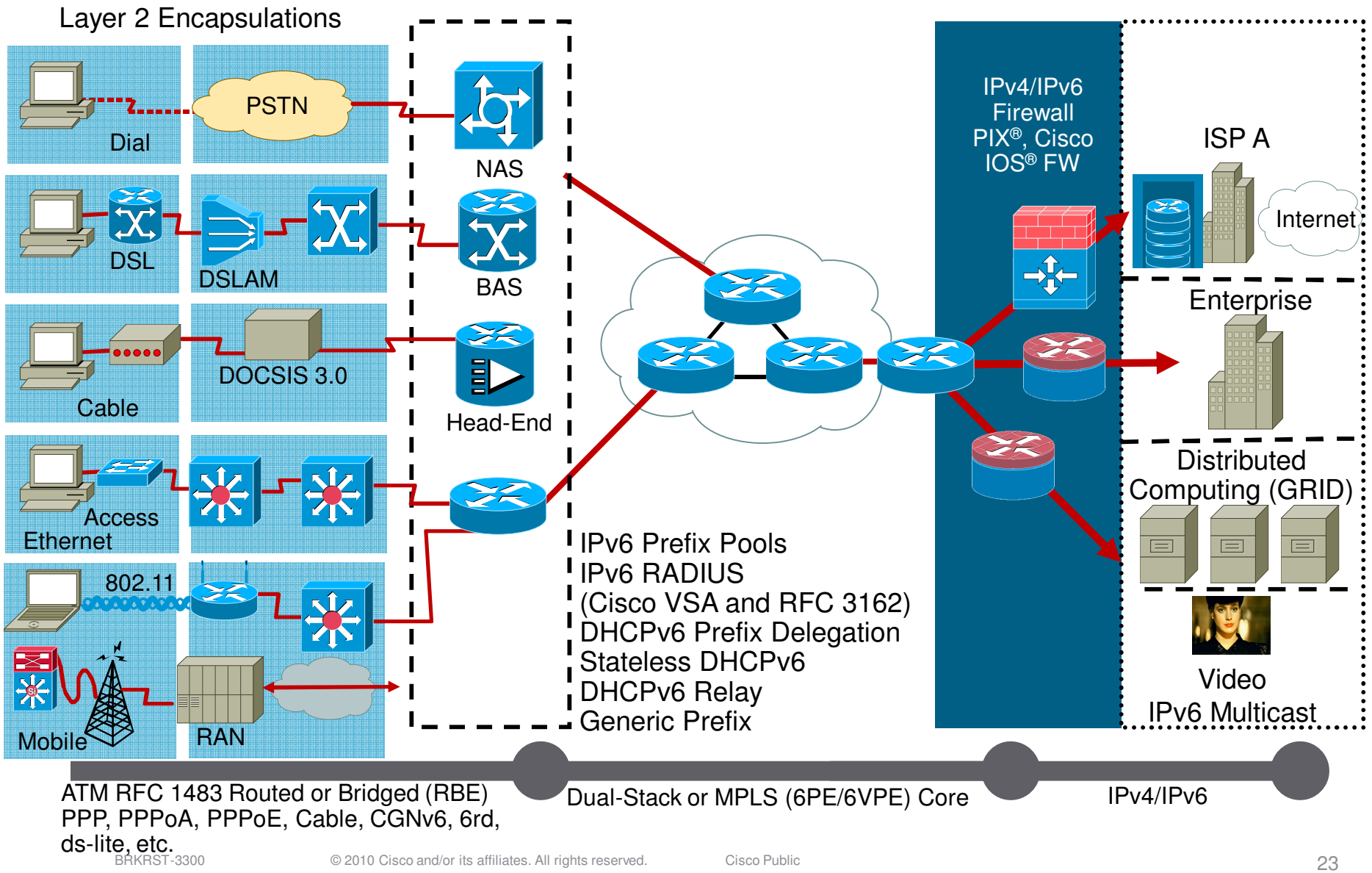
Service Provider: Access



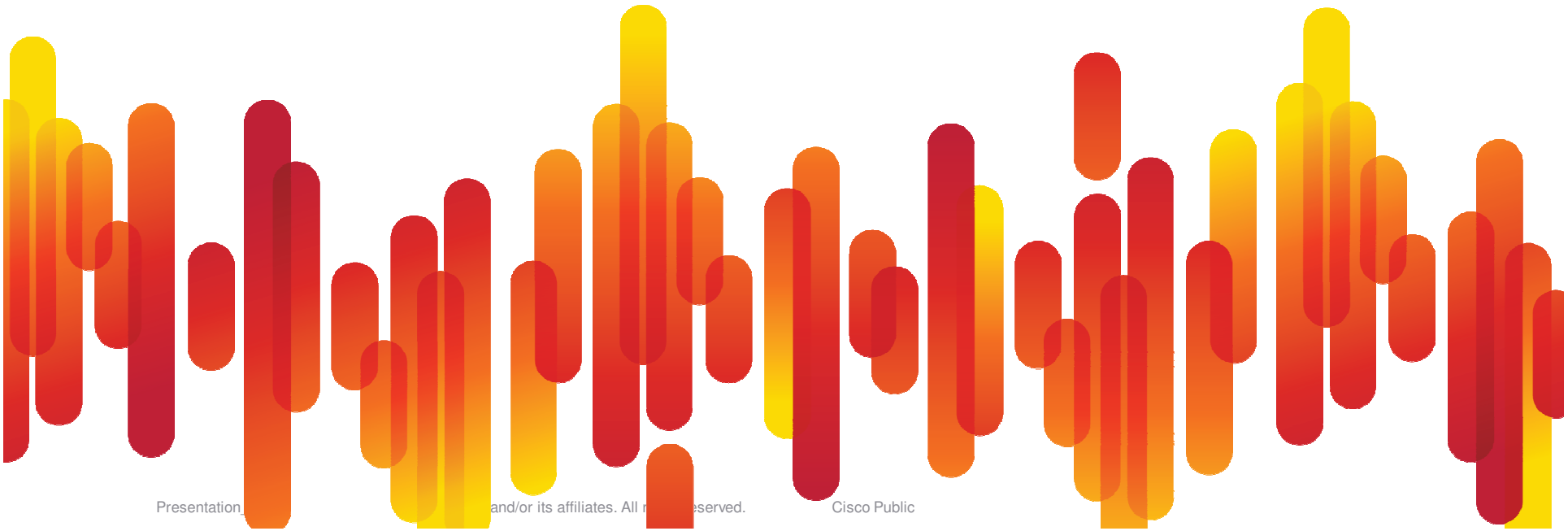
IPv6 Deployment Options – ACCESS

- IPv6 in IPv4 Access Environments
  - IPv4 Translation (NAT444)
  - IPv6 Integration
    - Dual-Stack IPv4 and IPv6
    - Dual-Stack with Tunneling
    - IPv6-Only to IPv4-Only Translation
  - IPv6 Provisioning
  - DOCSIS 3.0 IPv6 Reference Architecture

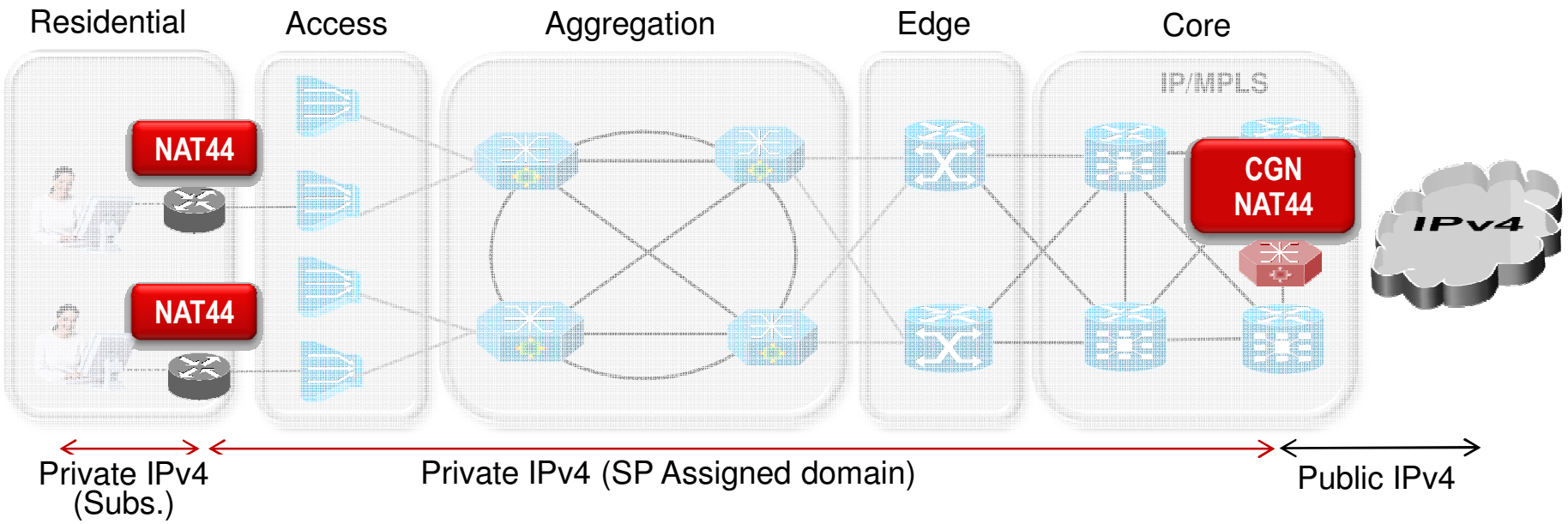
Cisco IOS IPv6 Broadband Access Solutions



IPv4 Translation (NAT444)

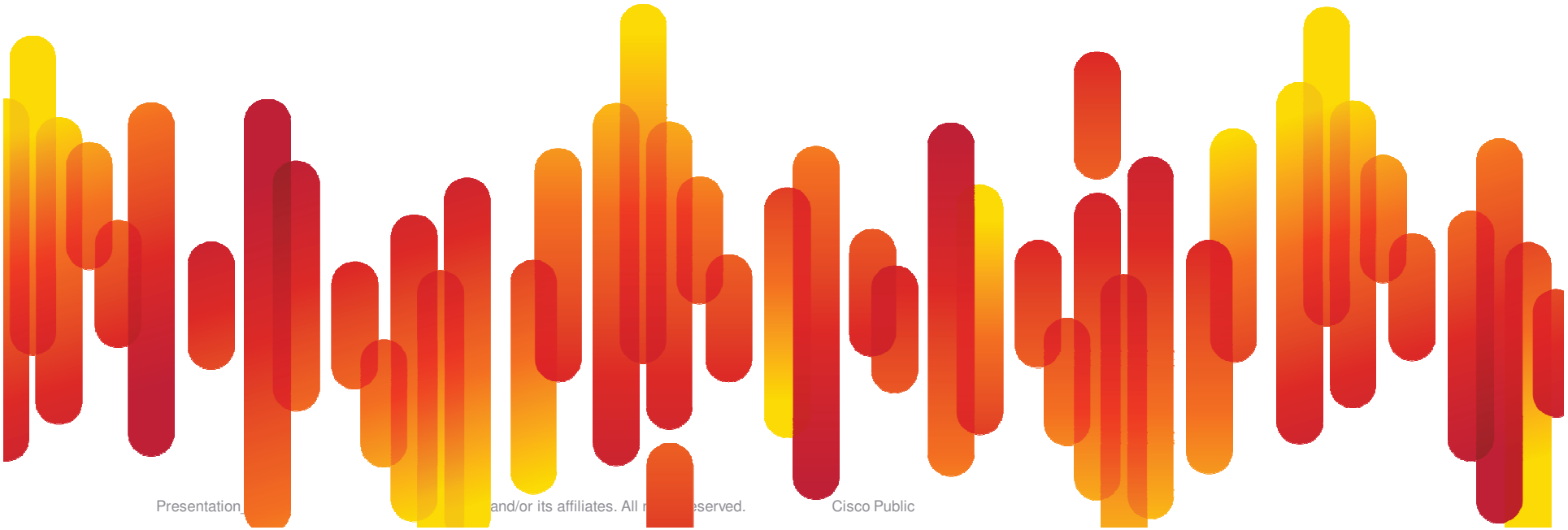


Public IPv4 Exhaustion with NAT444 Solution



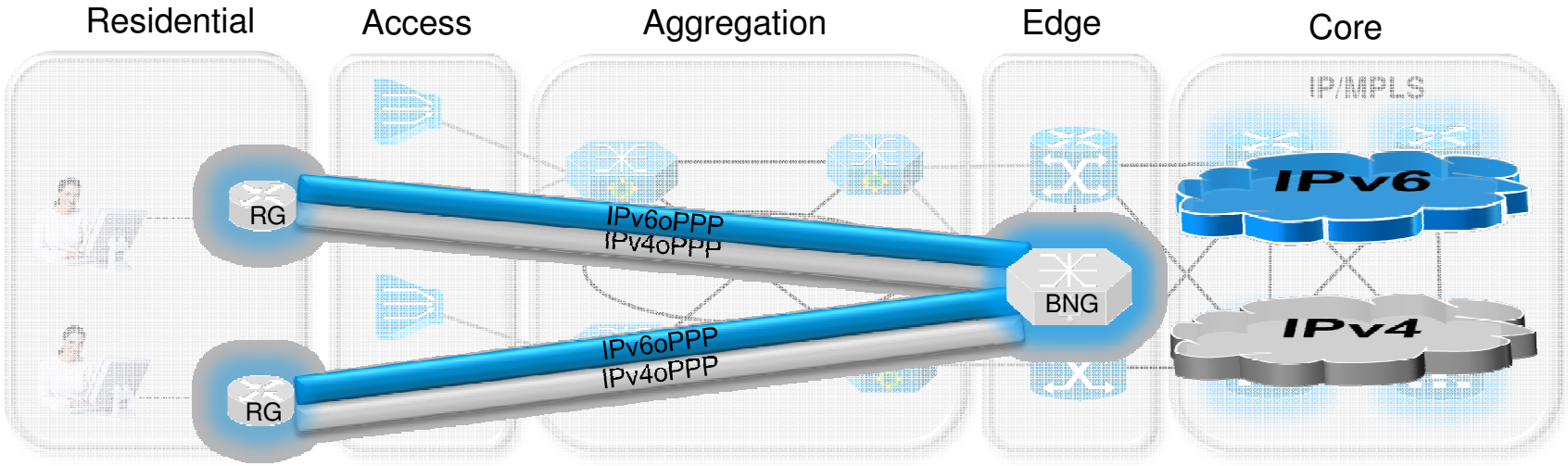
- Short-term solution to public IPv4 exhaustion issues without any changes on RG and SP Access/Aggregation/Edge infrastructure
- Subscriber uses NAT44 (i.e. IPv4 NAT) in addition to the SP using CGN with NAT44 within its network
- CGN NAT44 multiplexes several customers onto the same public IPv4 address
- CGN performance and capabilities should be analyzed in planning phase
- Long-term solution is to have IPv6 deployed

Dual-Stack IPv4 and IPv6



PPP Model (BBF TR-187*)

Dual PPP Session with Dual-stack IPv4/IPv6

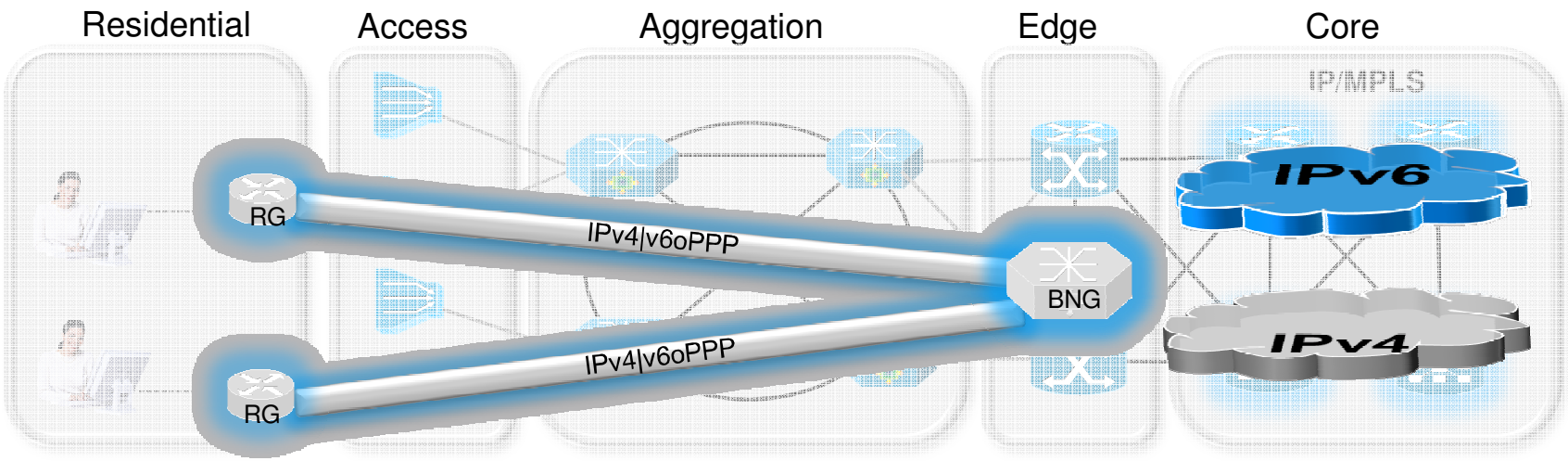


- Native Dual-Stack IPv4/IPv6 service on Residential Gateway (RG) LAN side
- NO changes in existing Access/Aggregation Infrastructure
- One PPP session per Address Family (IPv4 or IPv6) terminated on BNG*
  - As an option IPv6 PPP session from Host and bridged (PPPoE) on RG
  - Double amount of selected BNG resources (states, Subscriber plane, memory)
- IPCPv6 for Link-Local address
- SLAAC or DHCPv6 for Global address

*Broadband Forum TR-187: IPv6 for PPP Broadband Access
*Broadband Forum TR-101: BNG capabilities and definitions

PPP Model (BBF TR-187*)

Single PPP Session with Dual-Stack IPv4/IPv6

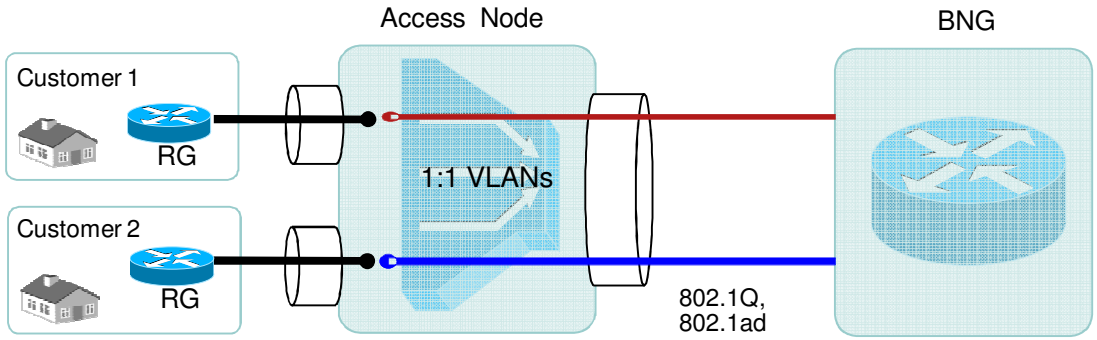


- Native Dual-Stack IPv4/IPv6 service on Residential Gateway (RG) LAN side
- NO changes in existing Access/Aggregation Infrastructure
- Dual-stack IPv6 and IPv4 supported over a shared PPP session with IPv4 and IPv6 NCPs running as ships in the night terminated on Broadband Network Gateway (BNG*)
  - Limited impact on PPP control plane
  - Limited impact on BNG data plane
- IPCPv6 for Link-Local address
- SLAAC or DHCPv6 for Global address

*Broadband Forum TR-187: IPv6 for PPP Broadband Access
*Broadband Forum TR-101: BNG capabilities and definitions

IPv6oE Model (BBF WT-177*)

IPv6 over Ethernet with 1:1 VLAN

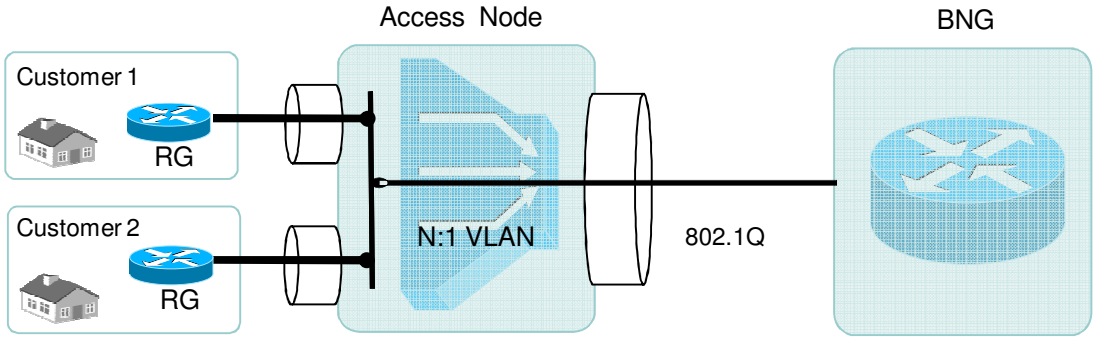


- IPv6oE with 1:1 VLANs vs PPPoE - What's different?
- Subscriber Line-identifier used for 1:1 VLAN mapping = (S-TAG, C-TAG)
- At L2 IPv6oE with 1:1 VLANs does resemble PPPoE
  - Effectively point-point broadcast domain does not require any special L2 forwarding constraints on Access Node – NO change to Access Node
  - SLAAC and Router Discovery are required
- However 1:1 VLANs and IPoE *do* require some extra BNG functionality
  - Neighbour Discovery needs to be run (along with some security limits)

***Broadband Forum WT-177 (draft): IPv6 in the Context of TR-101**

IPv6oE Model (BBF WT-177*)

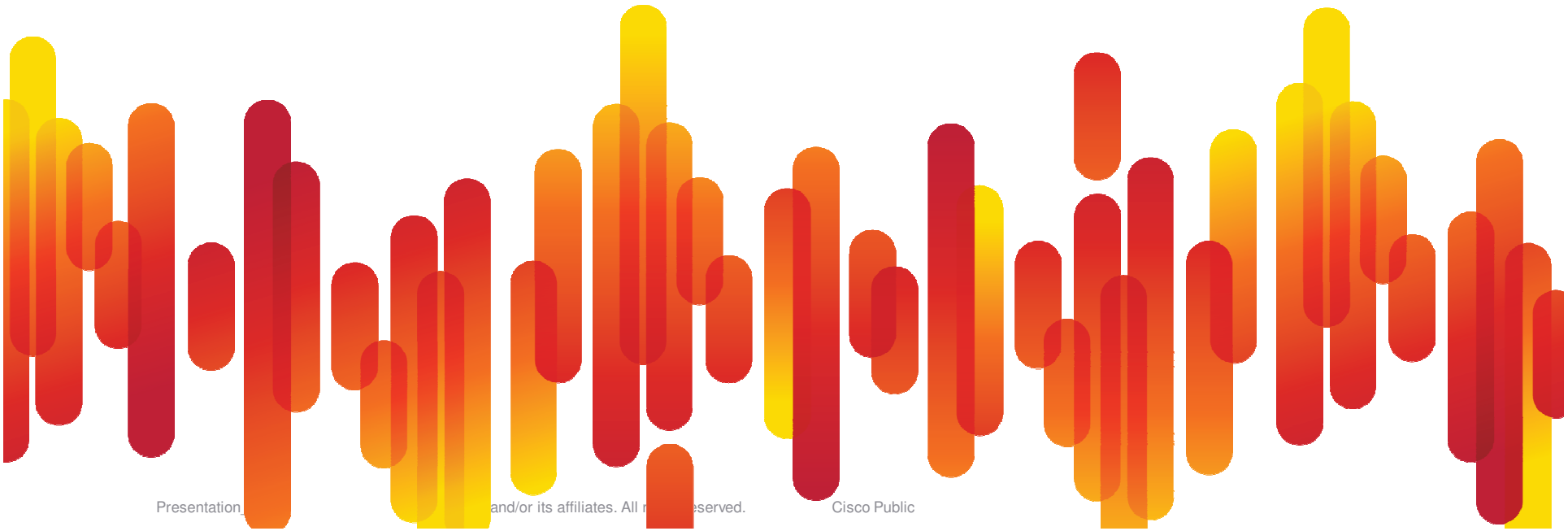
IPv6 over Ethernet with N:1 VLAN



- Requires changes in existing Access Node
  - Security requirements: IPv6 anti-spoofing, RA snooping, DHCPv6 snooping (etc.)
  - Multicast requirements: MLDv2, MLDv2 snooping
- Subscriber line identification
  - VLAN no longer provides a unique subscriber line identifier
  - Lightweight DHCP Relay Agent on the Access Node to convey subscriber line-identifier
- N:1 challenges due to non broadcast multiple access (NBMA) nature of split horizon forwarding
  - Risk of duplicate LL address if shared IPv6 subnet between RGW and BNG (proxy DAD)

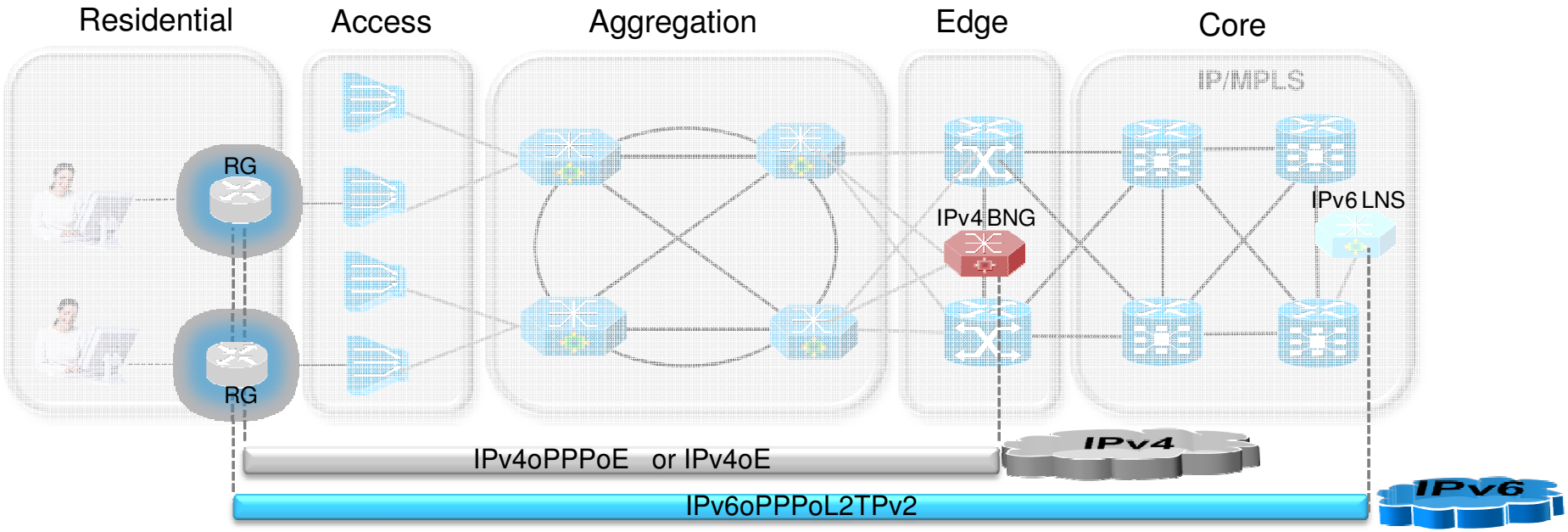
***Broadband Forum WT-177 (draft): IPv6 in the Context of TR-101**

Dual Stack with Tunneling



IPv6 over Tunnel

IPv6 over L2TP softwire

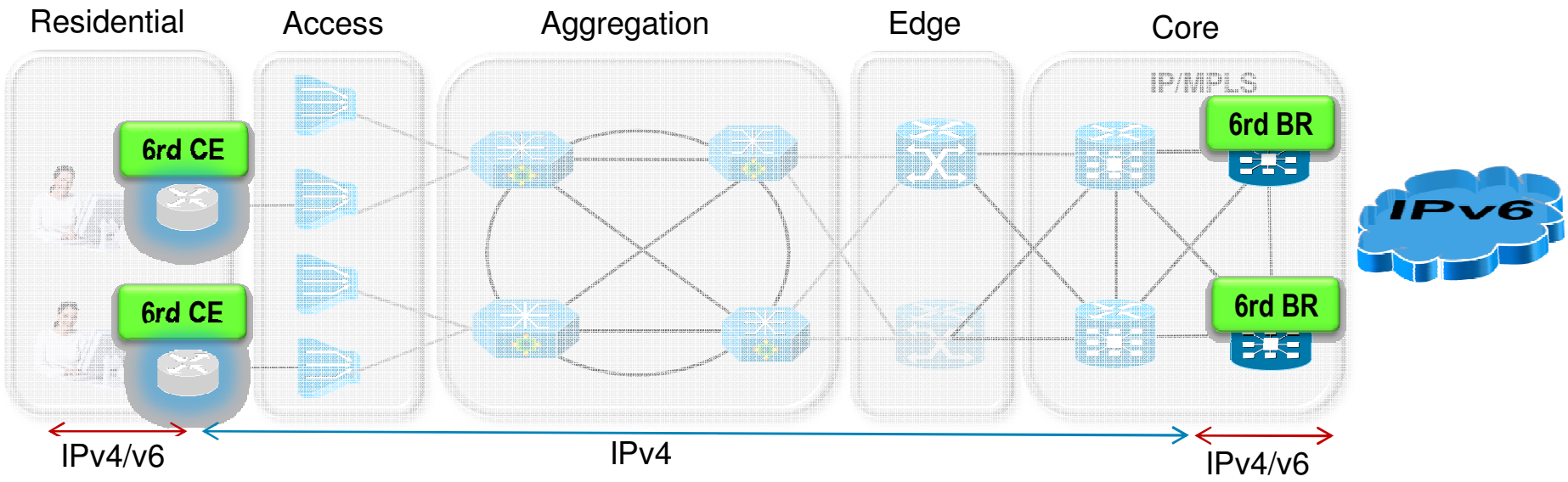


- Dual-Stack IPv4/IPv6 service on RG LAN side
- PPPoE or IPv4oE Termination on IPv4-only BNG
- L2TPv2 softwire between RG and IPv6-dedicated L2TP Network Server (LNS)
- Stateful architecture on LNS, offers dynamic control and granular accounting of IPv6 traffic
- Limited investment & impact on existing infrastructure

Broadband Forum WT-242: Getting to Dual Stack

IPv6 over Tunnel

IPv6 over IPv4 via 6rd (RFC 5569)

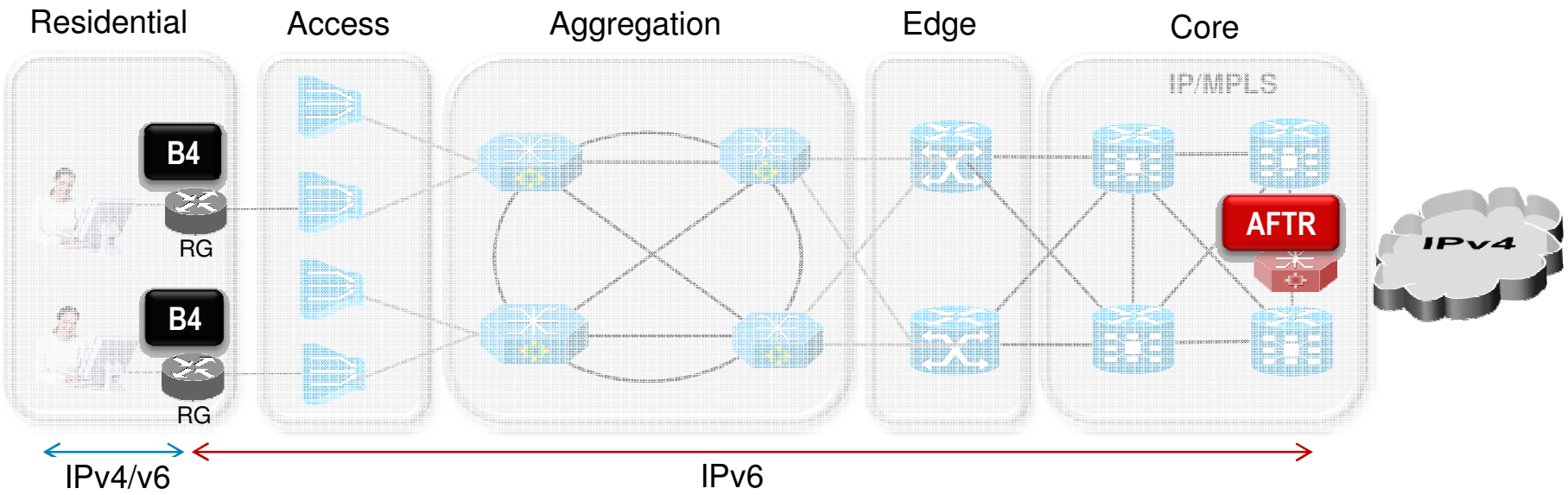


- Introduction of two Components: 6rd CE (Customer Edge) and 6rd BR (Border Relay)
- Automatic Prefix Delegation on 6rd CE
- Simple, stateless, automatic IPv6-in-IPv4 encap and decap functions on 6rd (CE & BR)
- IPv6 traffic automatically follows IPv4 Routing
- 6rd BRs addressed with IPv4 anycast for load-balancing and resiliency
- Limited investment & impact on existing infrastructure

3 Key Components of 6rd

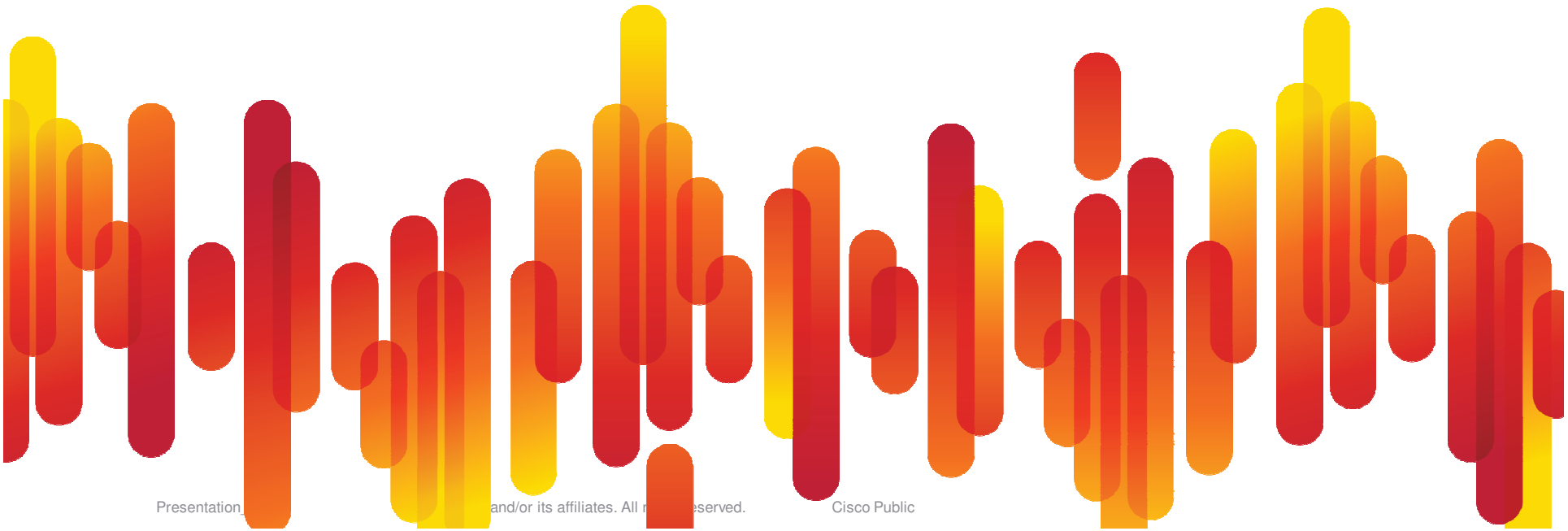
- IPv6 Prefix Delegation Derived from IPv4
  - No need for DHCPv6 on 6rd CE WAN interface
  - No need for DHCPv6 server in the network
  - Supports Global IPv4 or NATed IPv4 in same deployment
- Stateless Mapping and Encapsulation of IPv6 over IPv4 (RFC4213)
  - IPv4 encapsulation automatically determined from each packet's IPv6 destination
  - No per-subscriber tunnel state or provisioning, hence single dimension scaling (data-plane) on 6rd BR
- IPv4 Anycast to Reach BR
  - Simplify network 6rd BR placement, load-balancing and/or redundancy across multiple 6rd BRs

IPv4 via IPv6 using DS-Lite (w/NAT44)

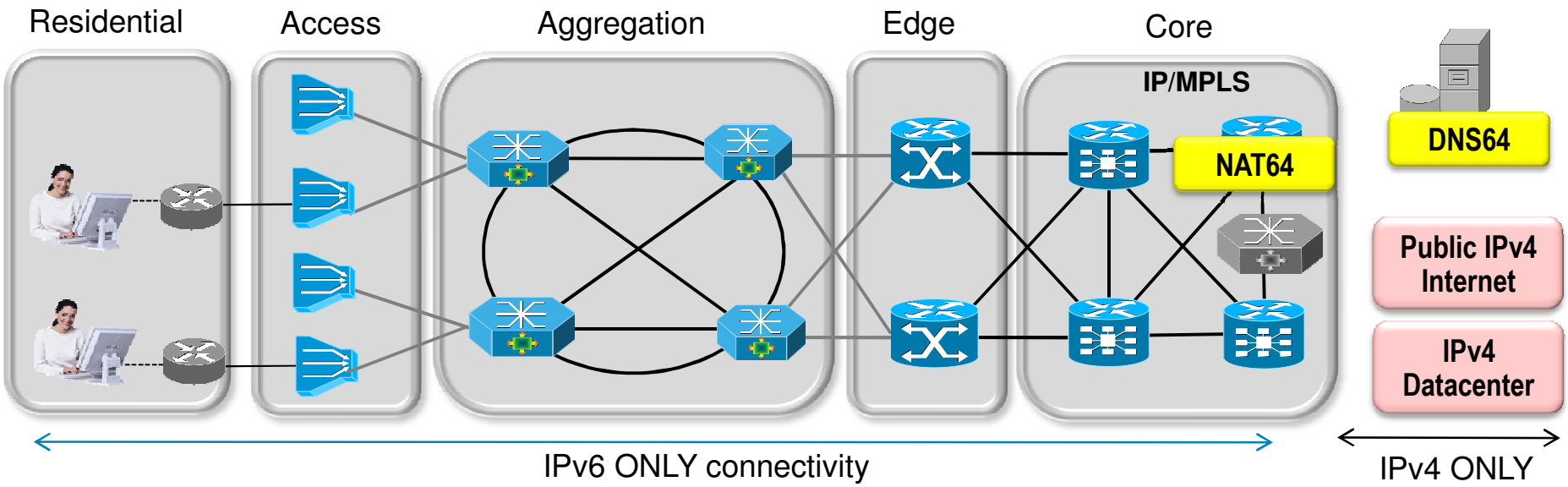


- Access, Aggregation, Edge and Core migrated to IPv6. NMS/OSS and network services migrated to IPv6 as well (DNS, DHCP)
- IPv4 Internet service still available and overlaid on top of IPv6-only network.
- Introduction of two Components: B4 (Basic Bridging Broadband Element) and AFTR (Address Family Transition Router)
  - B4 typically sits in the RG
  - AFTR is located in the Core infrastructure
- Assumption: IPv4 has been phased out, IPv6 only Access/aggregation network

IPv6-Only to IPv4-Only Translation

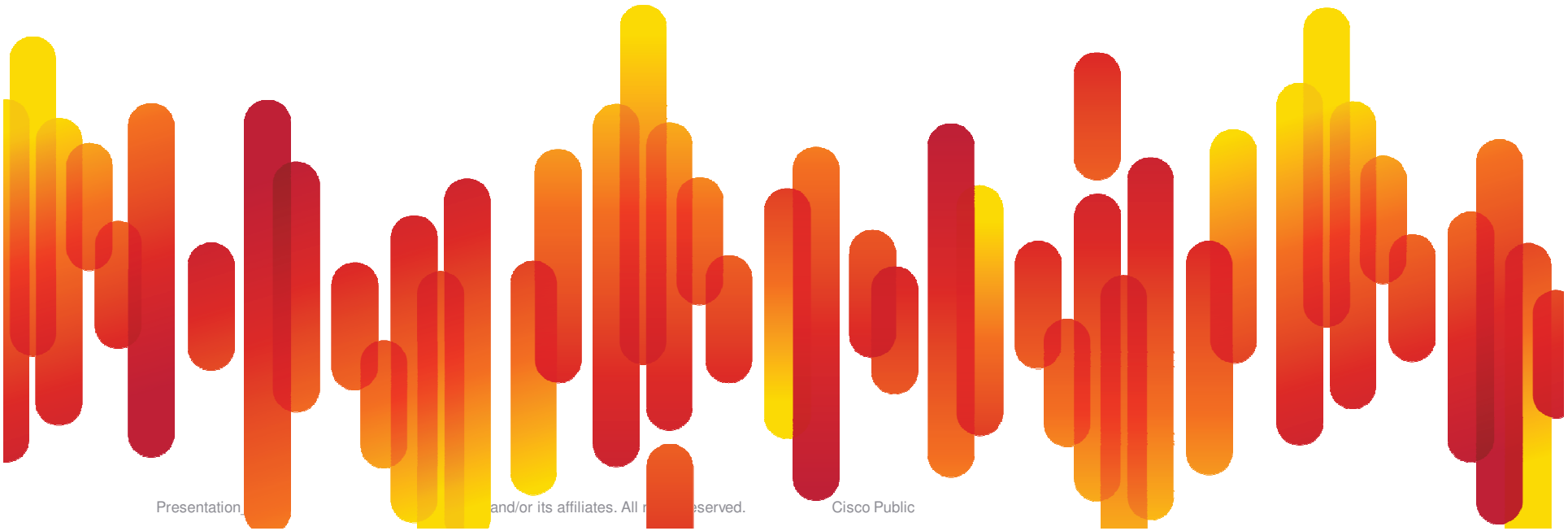


Connecting IPv6-only with IPv4-only: AFT64



- AFT64 technology is only applicable in case where there are IPv6 only end-points that need to talk to IPv4 only end-points (AFT64 for going from IPv6 to IPv4)
- AFT64:= “stateful v6 to v4 translation” or “stateless translation”, ALG still required
- Key components includes NAT64 and DNS64
- Assumption: Network infrastructure and services have fully transitioned to IPv6 and IPv4 has been phased out

DOCSIS 3.0 IPv6 Reference Architecture



Drivers for IPv6 in Cable

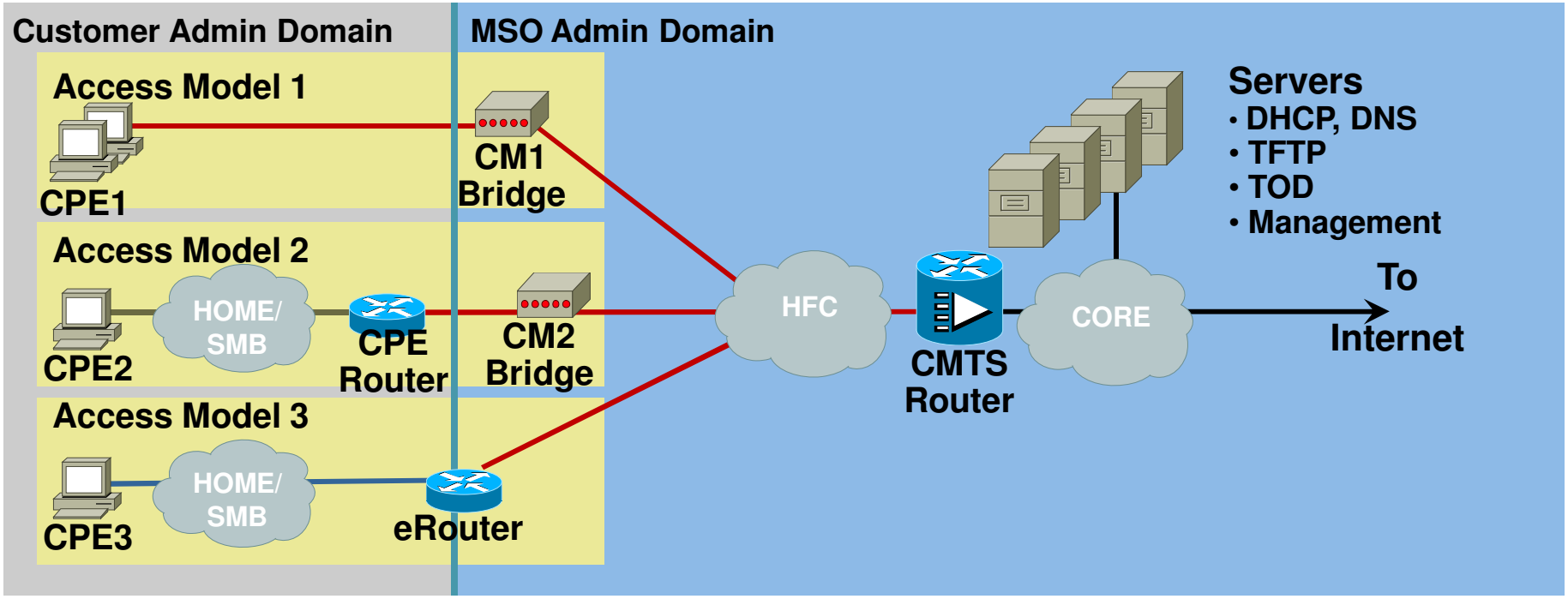
- Use IPv6 for managing large number of devices
  - Exponential growth in number of IP devices connected to CMTS
  - Cable MSOs in the US would like to use IPv6 to manage CM/MTA
  - Currently RFC1918 addresses assigned to CM for management
- RFC 1918 provides 16 million 10.net addresses, plus:
  - 1M addresses under 172.16.0.0/12
  - 65K addresses under 192.168/16
- Moreover, address utilization efficiency for large numbers decreases with topology hierarchies*
  - 6.5M addresses for 4M CMs
  - Only 61.5% efficient use
  - Density of only 9.8M CMs exhausts all 16M RFC1918 addresses

***See HD Ratio, RFC1715 and RFC3194**

CableLabs IPv6 Decision and Approach

- CableLabs put IPv6 in consideration for DOCSIS 3.0
  - Cisco responded with proposal for IPv6 architecture and features
  - IPv6 identified as one of top three ranked order priorities by MSOs
- Decision: DOCSIS 3.x MUST fully support IPv6
  - Cisco primary author for DOCSIS 3.0 IPv6 and enhanced IPv4/v6 Multicast specifications
- Rationale
  - Increased address space for CM management
  - New CPE services
- Proposed phases
  - Phase 1—CM hardware impacting features, CM provisioning and management over IPv6, embedded IPv6 router in CM
  - Phase 2—remaining IPv6 features for CPE services, for example IPv6 CPE provisioning and IPv6 service support

IPv6 Deployment Models for DOCSIS 3.0

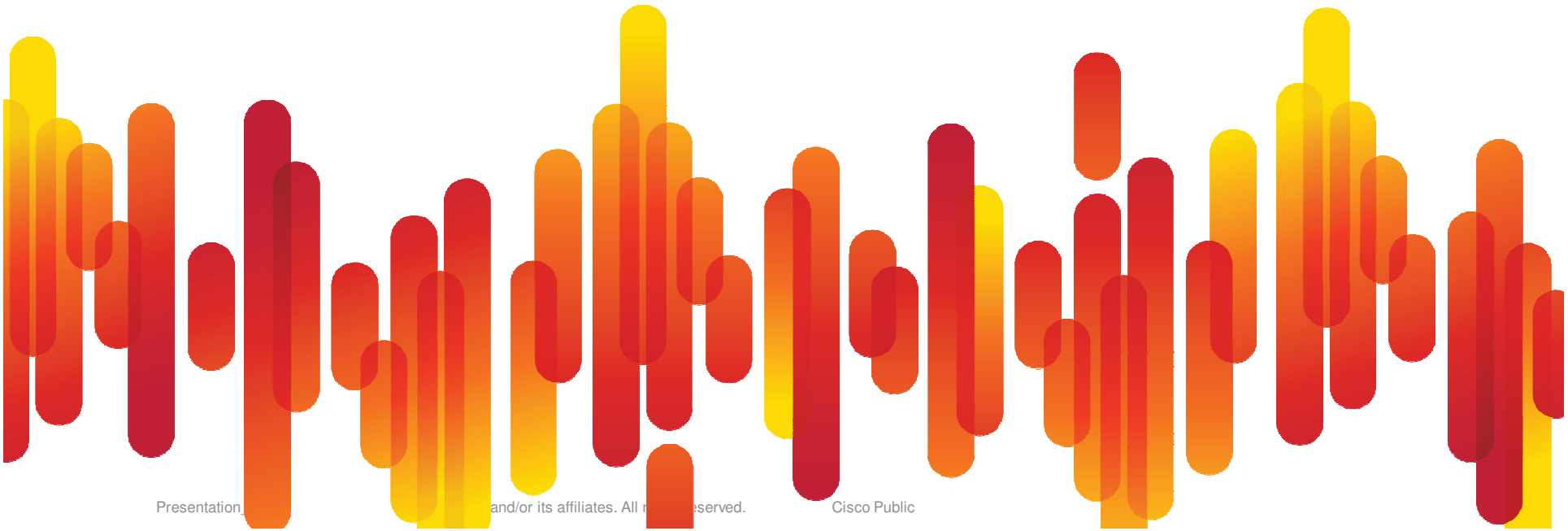


Management Prefix: 2001:DB8:FFFF:0::/64
Service Prefix: 2001:DB8:FFFE:0::/64
Customer 2 Prefix: 2001:DB8:2::/48
Customer 3 Prefix: 2001:DB8:3::/48

HFC Link; Assigned 2001:DB8:FFFF:0::/64 (Mgmt) and 2001:DB8:FFFE:0::/64 (Serv)
Customer 2 Premises Link; Assigned 2001:DB8:2:0::/64
Customer 3 Premises Link; Assigned 2001:DB8:3:0::/64

Routers Span Customer and MSO Administrative Domains

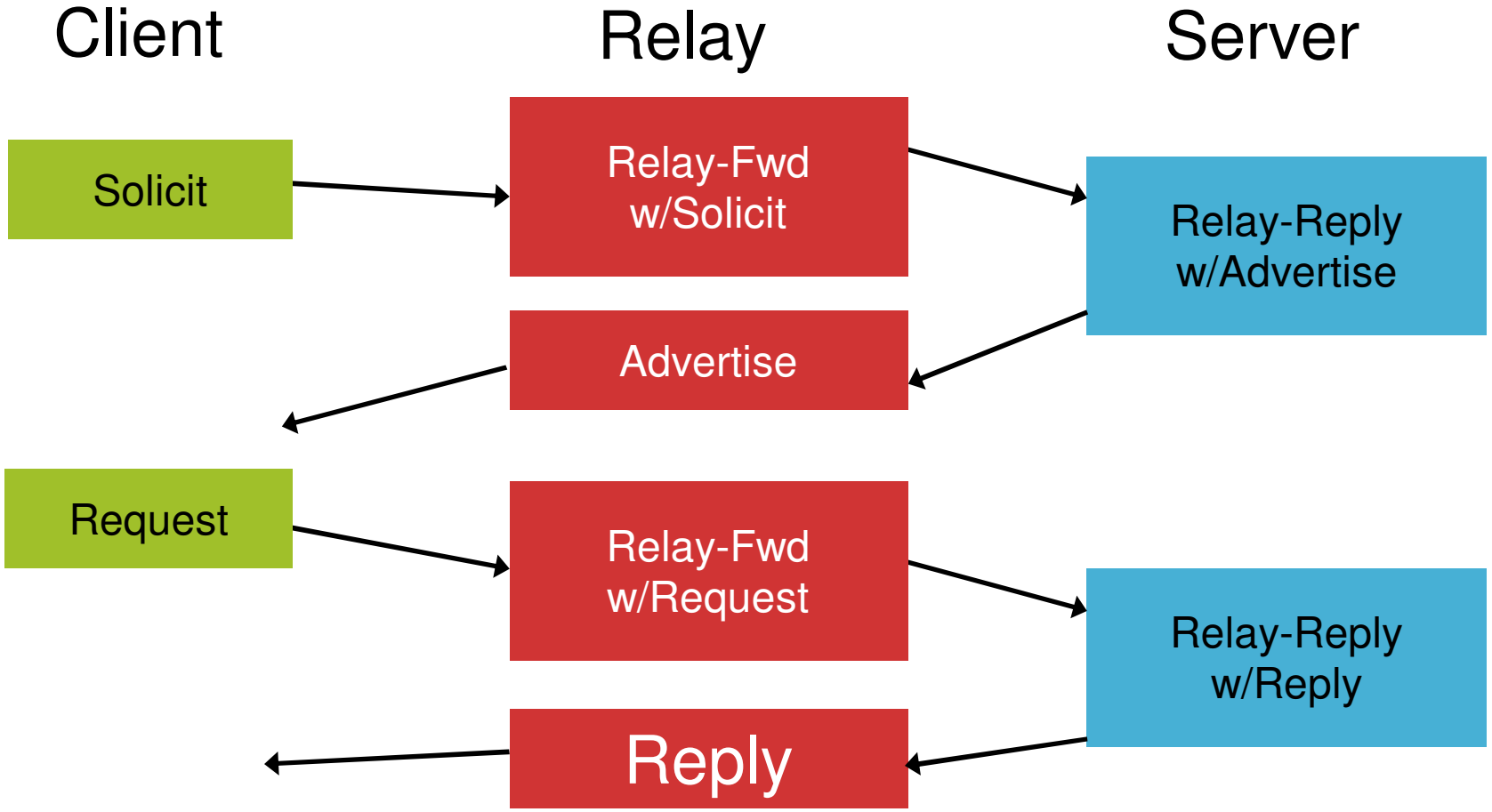
Provisioning in IPv6 Access Environments



DHCPv6 Overview

- Operational model based on DHCPv4
- Details are different
  - Client uses link-local address for message exchanges
  - Server can assign multiple addresses per client through identity associations
  - Clients and servers identified by DUID
  - Address assignment
  - Prefix delegation
  - Message exchanges similar, but will require new protocol engine
  - Server-initiated configuration, authentication part of the base specification
  - Extensible option mechanism
  - Relay-agents
- Allows both statefull and stateless configuration
- RFC 3315 (DHCPv6)
  - Additional options:
    - DNS configuration—RFC 3646
    - Prefix delegation—RFC 3633
    - NTP servers
    - Stateless DHCP for IPv6—RFC 3736

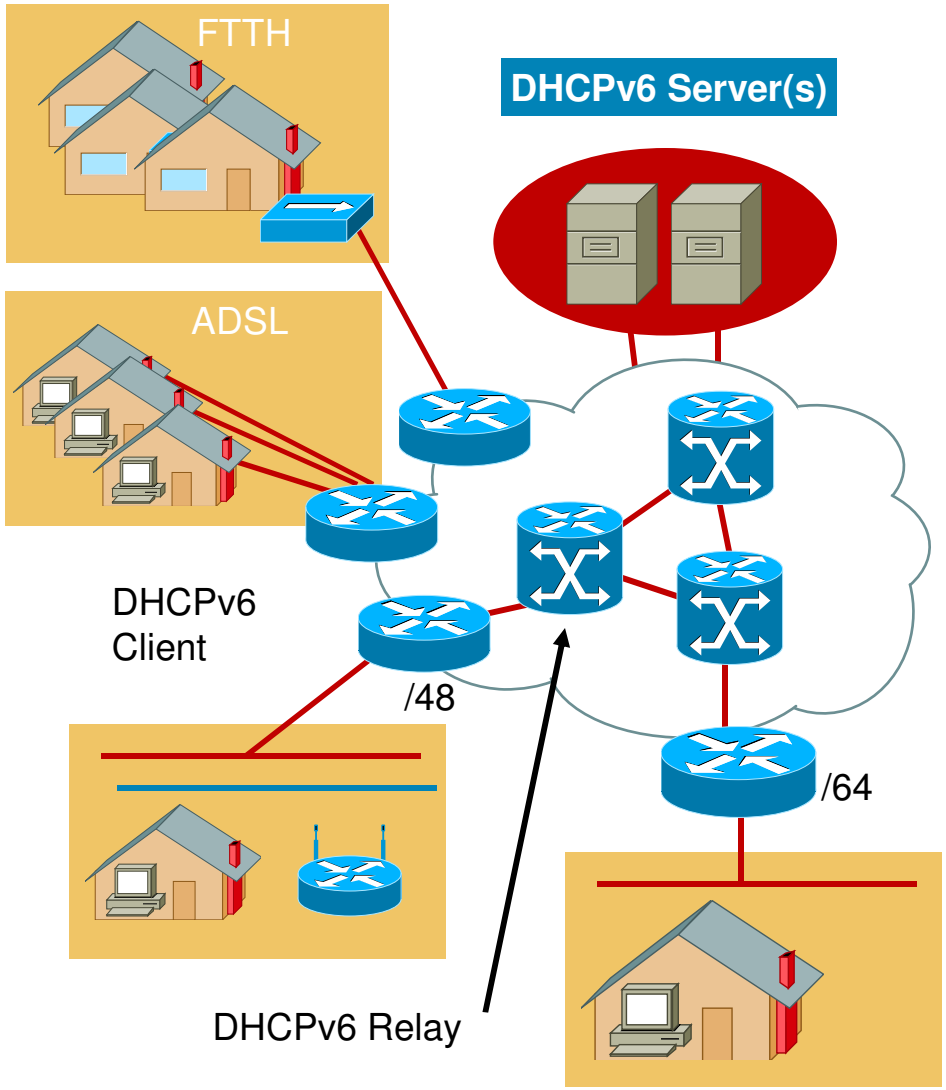
DHCPv6 Operation



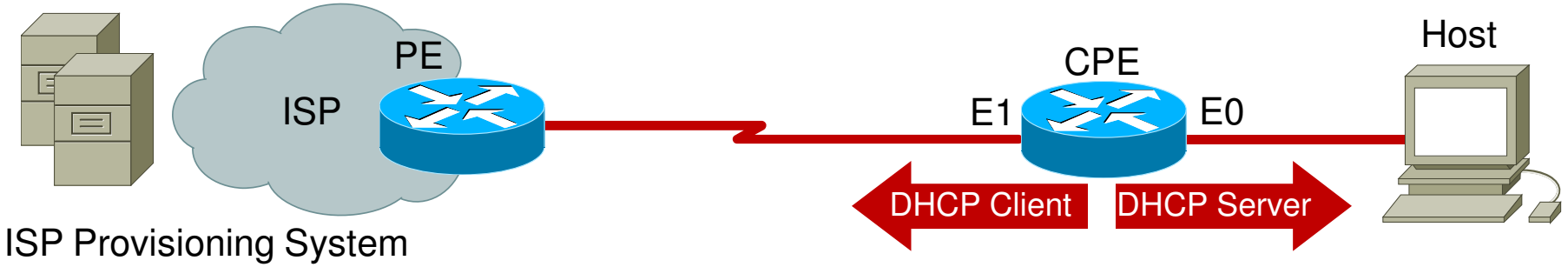
- All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
- All_DHCP_Servers (FF05::1:3)
- DHCP Messages: Clients listen UDP port 546. Servers and relay agents listen on UDP port 547

DHCPv6 PD: RFC 3633

- Media independence
  - xDSL, FTTH, …
  - Only knows identity of requesting router
- Leases for prefixes
- Flexible deployments
  - Client/relay/server model
- Requesting router includes request for prefixes in DHCP configuration request
- Delegating router assigns prefixes in response along with other DHCP configuration information



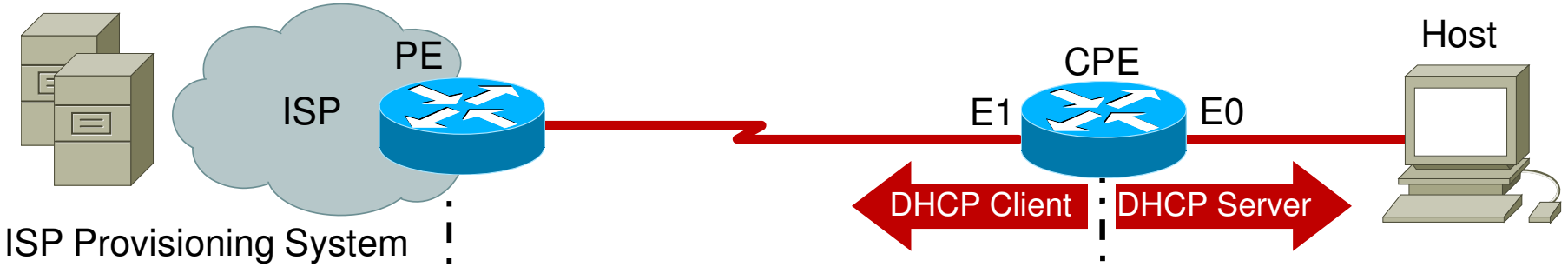
Router Advertisement



Source of RA	User of RA	A Bit		M/O Bits	
		A	Operation	M/O	Operation
PE	CPE E1	0	Don't Do Stateless Address Assignment	11	Use Dhcpv6 for Address + Other Config. (i.e., Stateful Dhcpv6)
CPE Router	Host	1	Do Stateless Address Assignment	01	Use Dhcpv6 for Other Config. (i.e., Stateless Dhcpv6)

Stateless (RFC2462)
RS Are Sent by Booting Nodes to Request RAs for Configuring the Interfaces; Host Autonomously Configures Its Own Link-Local Address

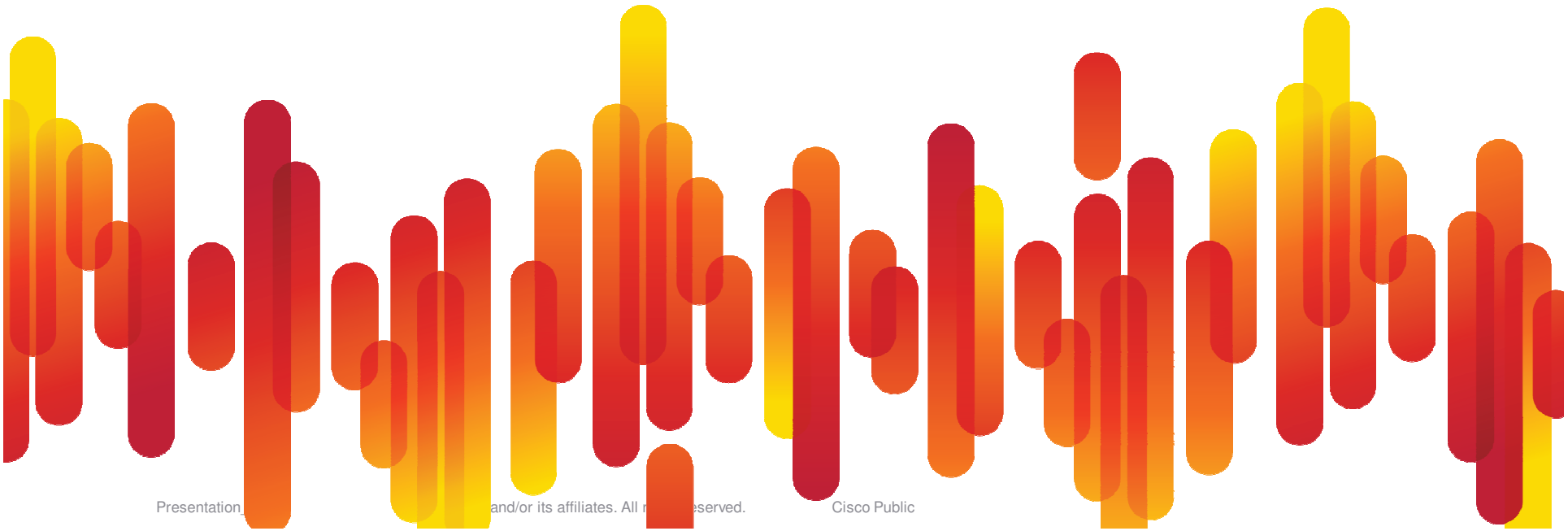
Prefix/Options Assignment



1. CPE Sends DHCP Solicit with ORO = PD
2. PE Sends RADIUS Request for the User
3. RADIUS Responds with User's Prefix(es)
4. PE Sends DHCP REPLY with Prefix Delegation Options
5. CPE Configures Addresses from The Prefix on Its Downstream Interfaces, and Sends an RA. O-bit Is Set to On
6. Host Configures Addresses Based on the Prefixes Received in the RA. As the O-bit Is on, It Sends a DHCP Information-request Message, with an ORO = DNS
7. CPE Sends a DHCP REPLY Containing Request Options

AAA | DHCP | ND/DHCP

IPv6 Provisioning Tools



AAA/RADIUS

- RADIUS attributes and IPv6 (RFC3162)—Cisco IOS 12.3(4)T
- RADIUS Server support requires an upgrade (supporting RFC3162) Few RADIUS solutions support RFC3162 functionality today
- Prefix pools and pool names are configurable through AAA
- The following RADIUS attributes as described in RFC 3162 are supported for IPv6: Framed-Interface-Id, Framed-IPv6-Prefix, Login-IPv6-Host, Framed-IPv6-Route, Framed-IPv6-Pool
- IPv6 AAA/RADIUS Configuration Examples on CCO

RADIUS Configuration with Permanently Assigned /64:

```
Auth-Type = Local, Password = "foo"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ipv6:prefix=2001:DB8:1:1::/64"
```

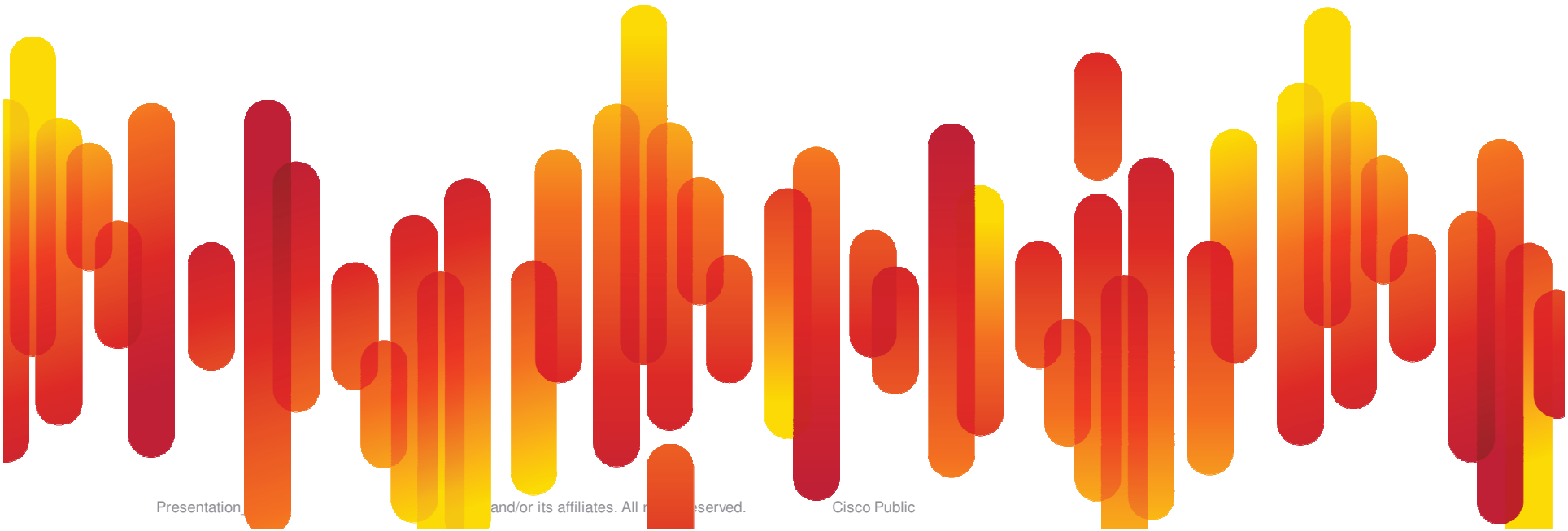
Interface Identifier Attribute (Framed-Interface-Id) Can Be Used:

```
Interface-Id = "0:0:0:1",
```

CNR 7.x Supports DHCPv6 (since 6.2 release)

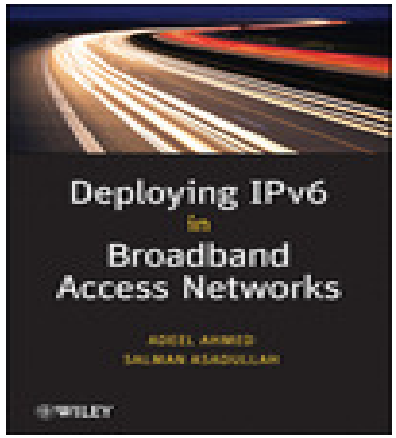
- DHCPv6 extensions: Existing extension points to be used for DHCPv4, DHCPv6, or both. New DHCPv6 only extension point to allow an extension to control lease address and delegated prefix generation
- Implements DOCSIS 3.0 options: CNR 7.0 supports DHCPv6 CableLabs Vendor-specific Information Options
- DNS Enhanced Searching: Server wide search also performs auto-translation of IPv4 and IPv6 addresses to PTR record names as part of the search.
- DHCPv6 DNS Updates: CNR 7.0 DHCP server supports DHCPv6 DNS updates (over IPv4 only) and DHCPv6 Client FQDN option
- DHCPv6 and DHCPv4 Leasequery Control: New “expert” mode DHCP server attribute ‘leasequery’ allows overall control of both DHCPv4 and DHCPv6 leasequery processing
- DHCPv6 SNMP Monitoring: DHCPv6 SNMP Monitoring, SNMP queries/traps only supported over IPv4
- http://www.cisco.com/en/US/docs/net_mgmt/network_registrar/7.0/release/notes/CNR70ReleaseNotes.html#wp56332

Conclusion



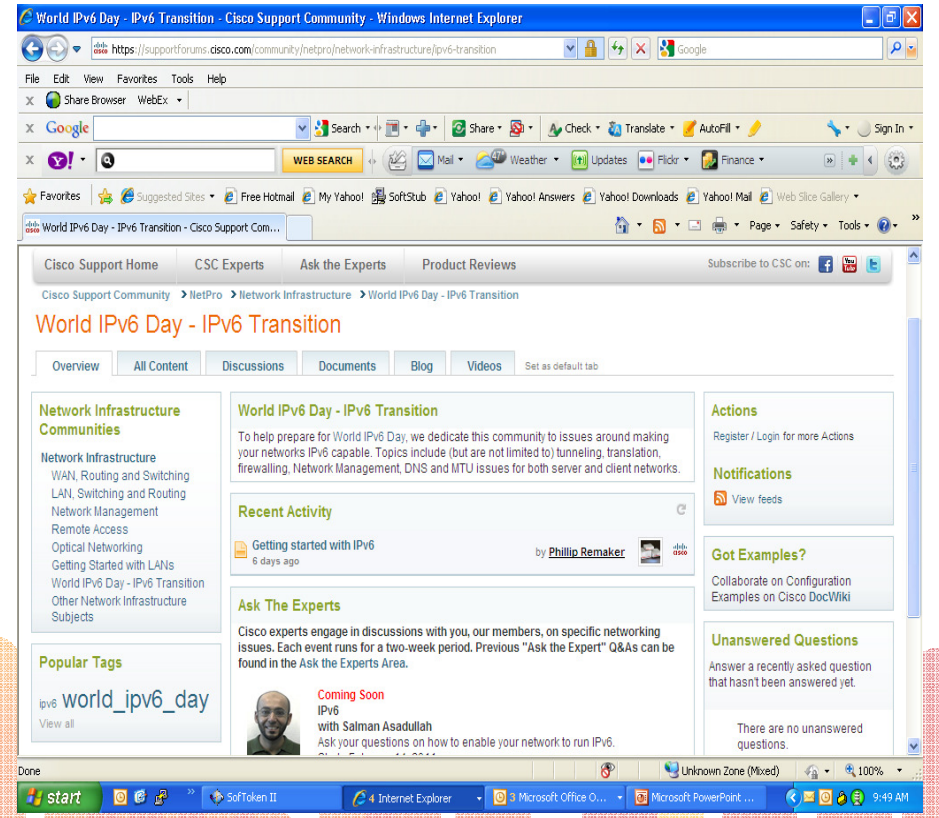
Conclusion

- Start now rather than later:
  - Multiple technology adoption scenarios available!!!
  - Purchase for the future and test, test and then test some more
  - Start moving legacy application towards IPv6 support
  - Don't assume your favorite vendor/app/gear has an IPv6 plan
  - Full parity between IPv4 and IPv6 is still a ways off
- Deploying IPv6 in Broadband Access Networks - Adeel Ahmed, Salman Asadullah, John Wiley & Sons Publications®
- Deploying IPv6 Networks - Ciprian Popoviciu, Patrick Grossetete, Eric Levy-Abegnoli, Cisco Press®
- IPv6 Security - Scott Hogg, Eric Vyncke, Cisco Press®
- IPv6 for Enterprise Networks - Shannon McFarland, Muninder Sambi, Nikhil Sharma, Sanjay Hooda, Cisco Press®
- www.cisco.com/go/ipv6 - CCO IPv6 Main Page
- www.cisco.com/go/srnd - Cisco Network Design Central
- www.ietf.org
- www.ipv6forum.org



Join Cisco IPv6 Support Community!

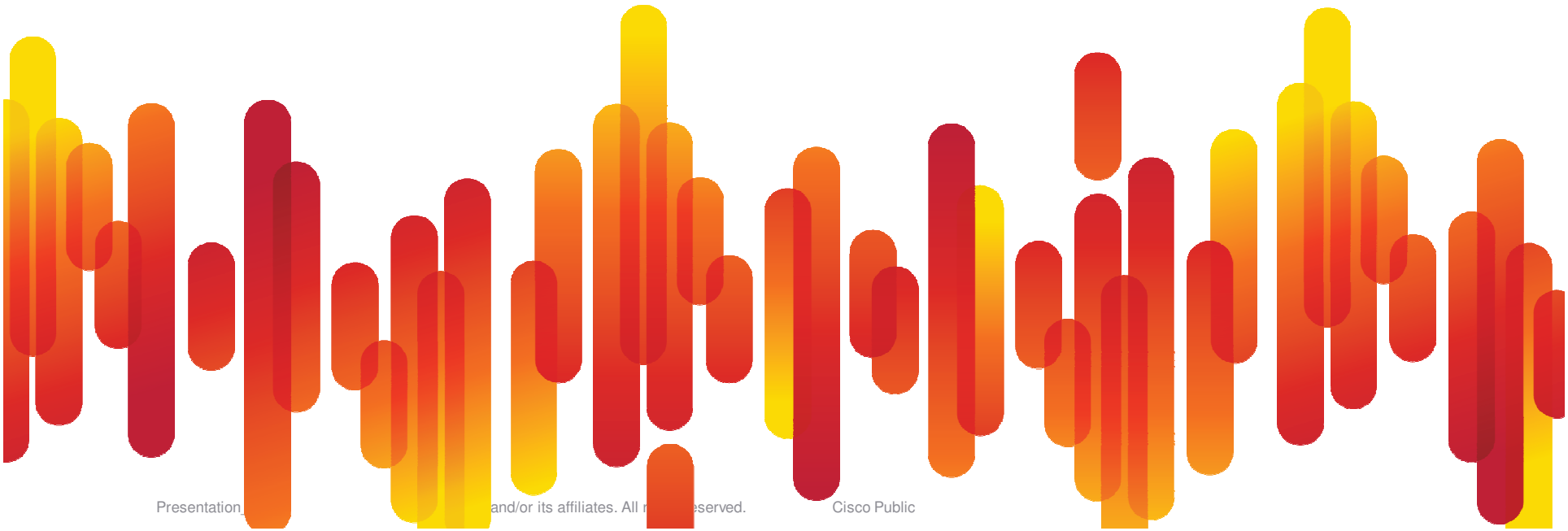
- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*
- Visit the Cisco Support Community booth in the World of Solutions for more information



supportforums.cisco.com
supportforums.cisco.mobi

The Cisco Support Community is your one-stop community destination from Cisco for sharing current, real-world technical support knowledge with peers and experts.

Q and A




CISCO