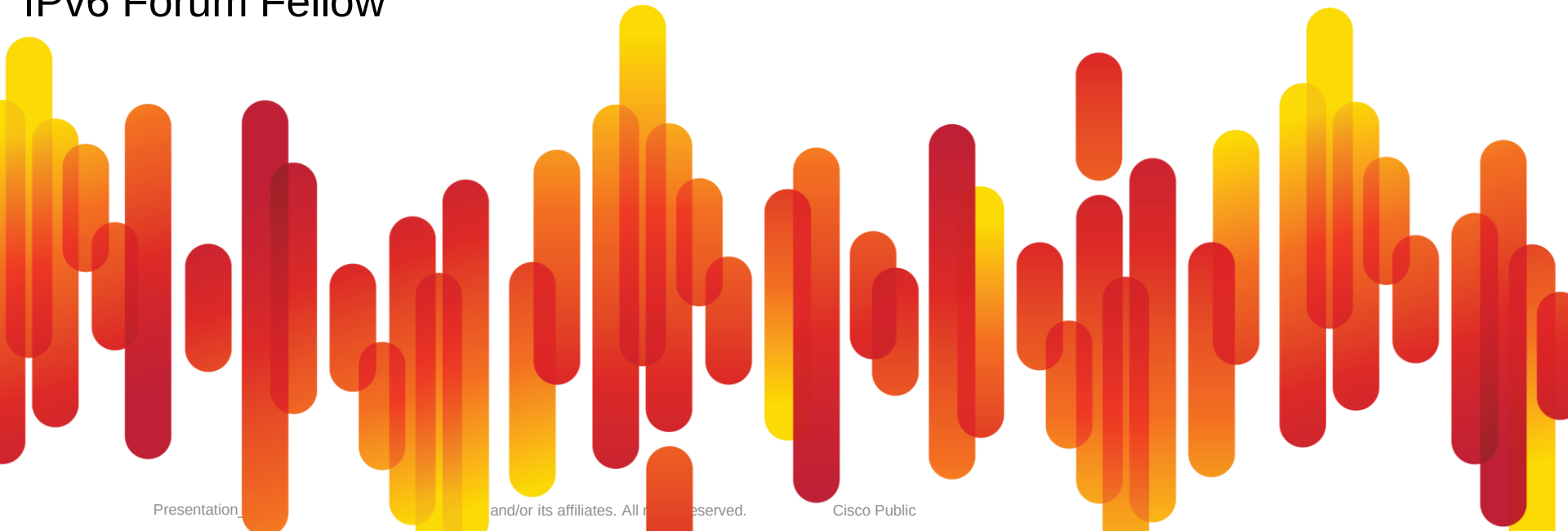
Adding IPv6 Support to Core Network gogoNET LIVE! 2

1-3 November, 2011

Salman Asadullah
Cisco Distinguished Engineer
IPv6 Forum Fellow

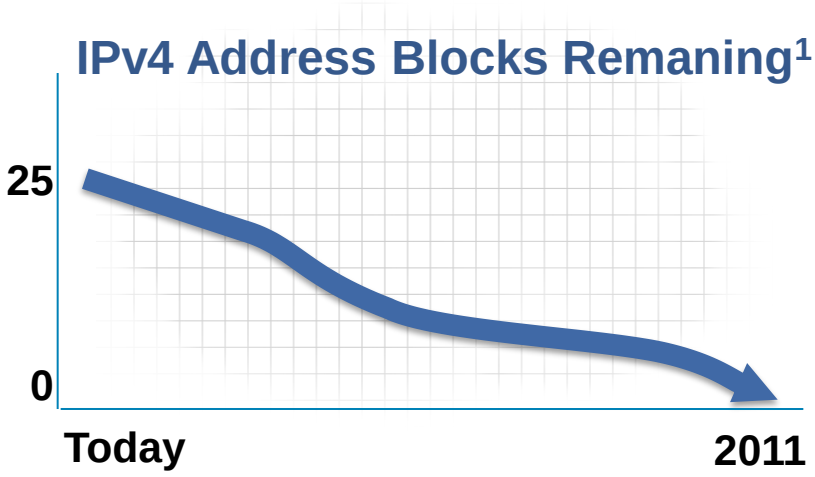


Agenda

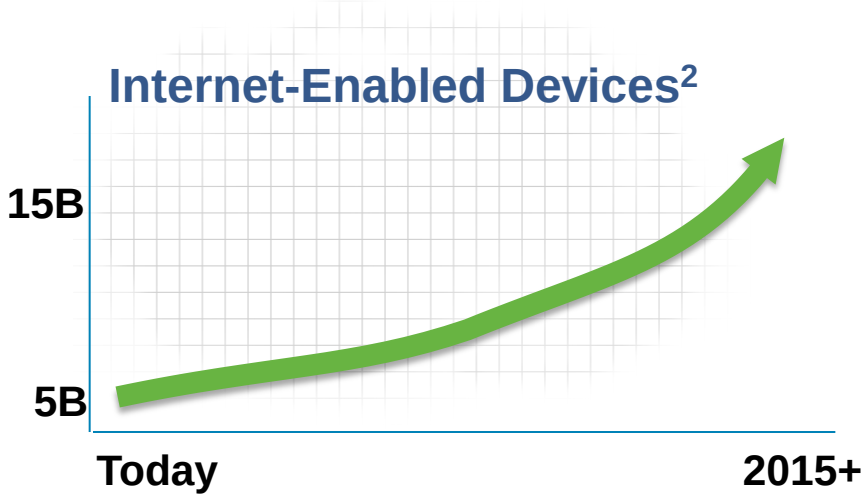
- IPv6 Integration Strategy
- IPv6 in SP Core Networks
  - Native IPv4 Environments
  - MPLS Environments
- IPv6 in Enterprise Core Networks
  - Dual-Stack
  - Hybrid
  - IPv6 Service Block
- Conclusion

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**

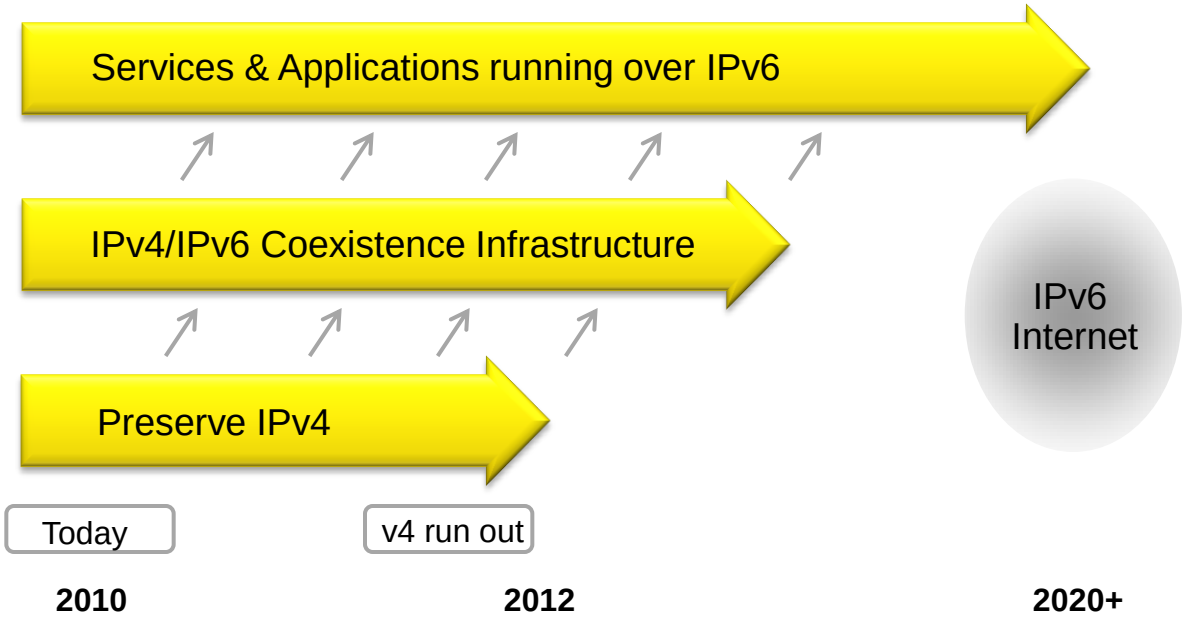


While the number of new Internet devices is **exploding**

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

... and Internet Evolution

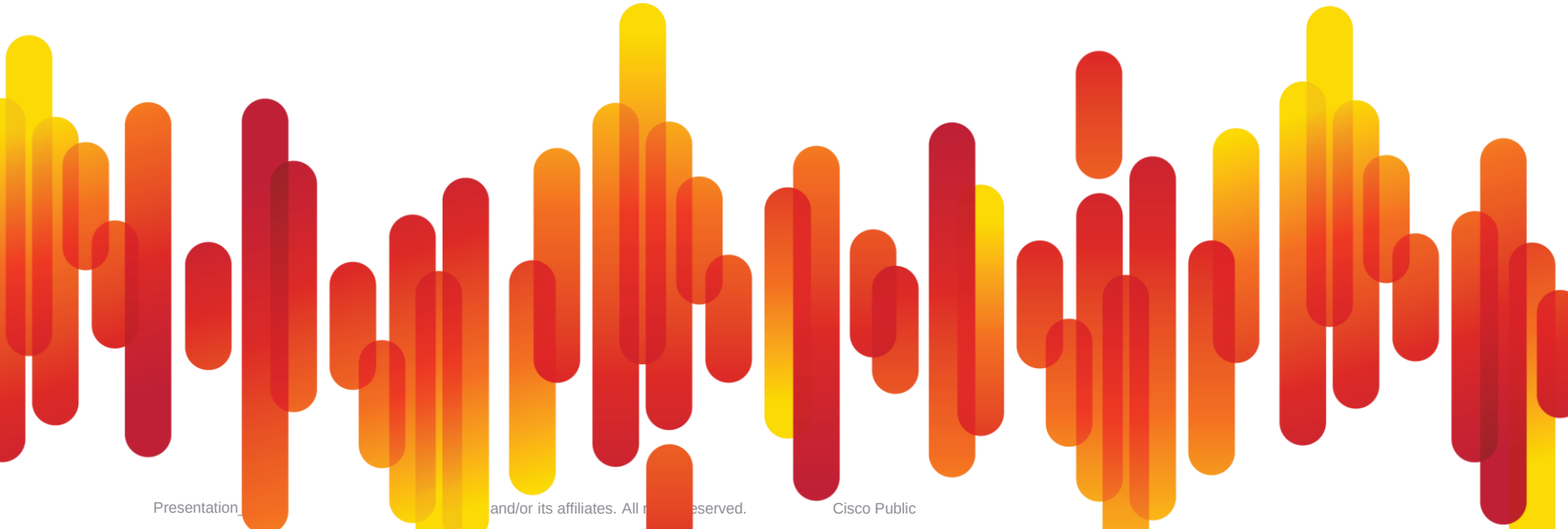
Moving to 3 IP Address Families: Public IPv4, Private IPv4, IPv6



IPv6 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
- SP/Enterprise 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

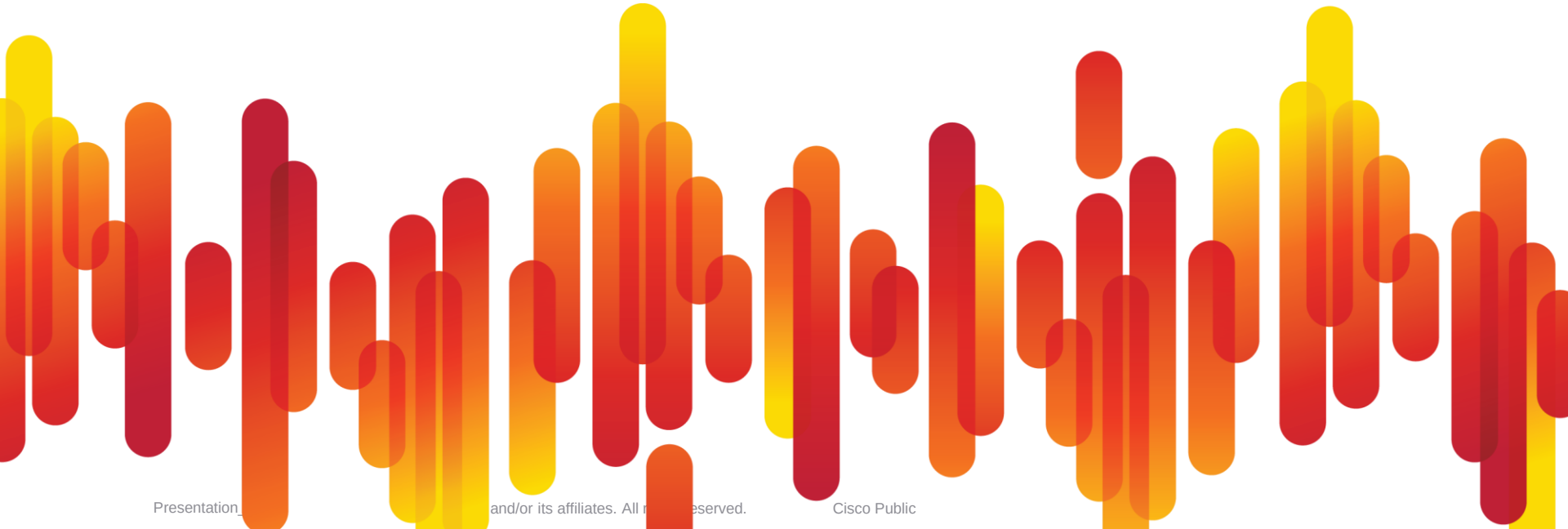
IPv6 in SP Core Networks and Deployment Models



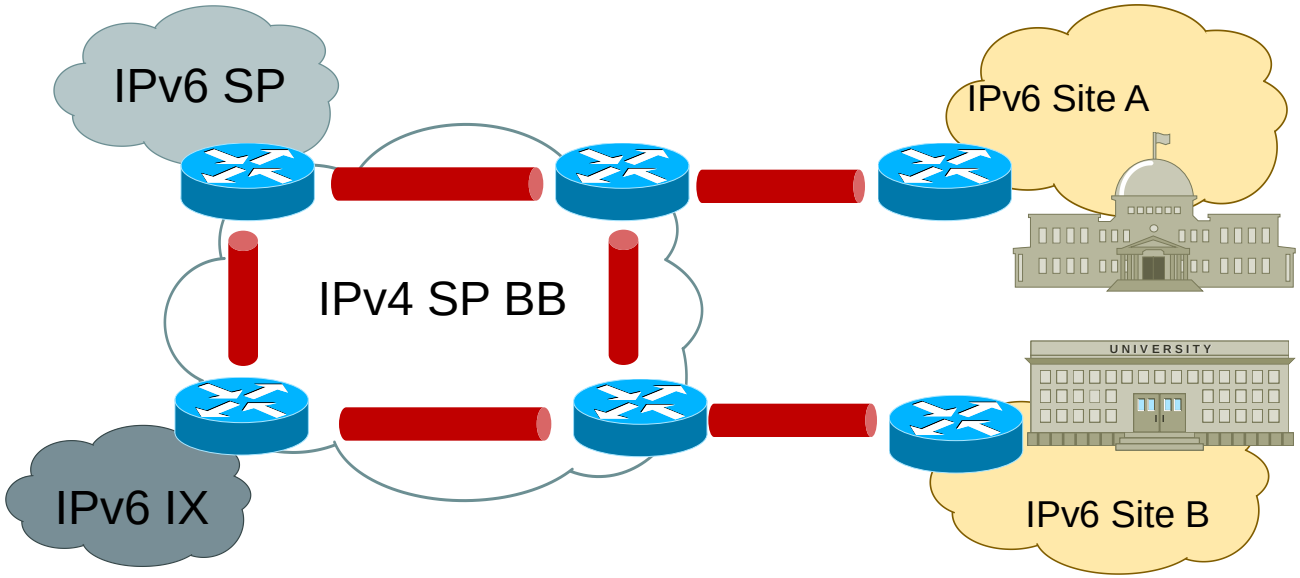
IPv6 Deployment Options — CORE

- 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

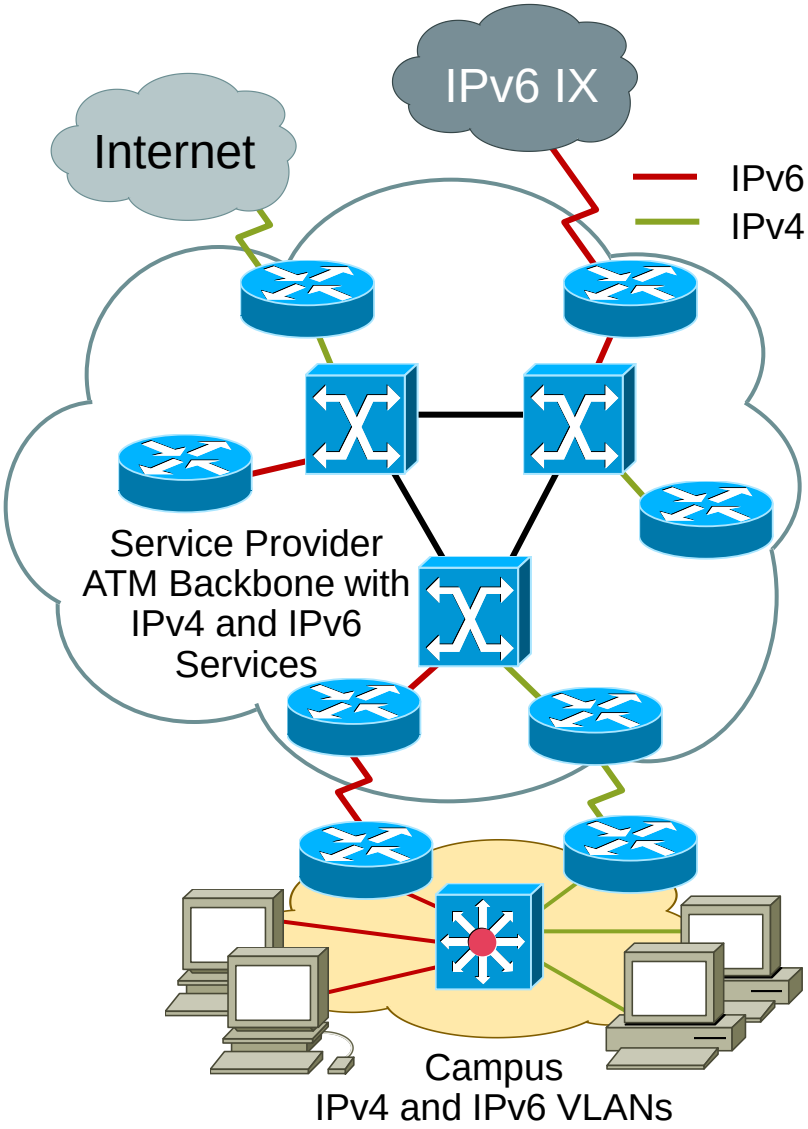


Tunnelling IPv6 in IPv4



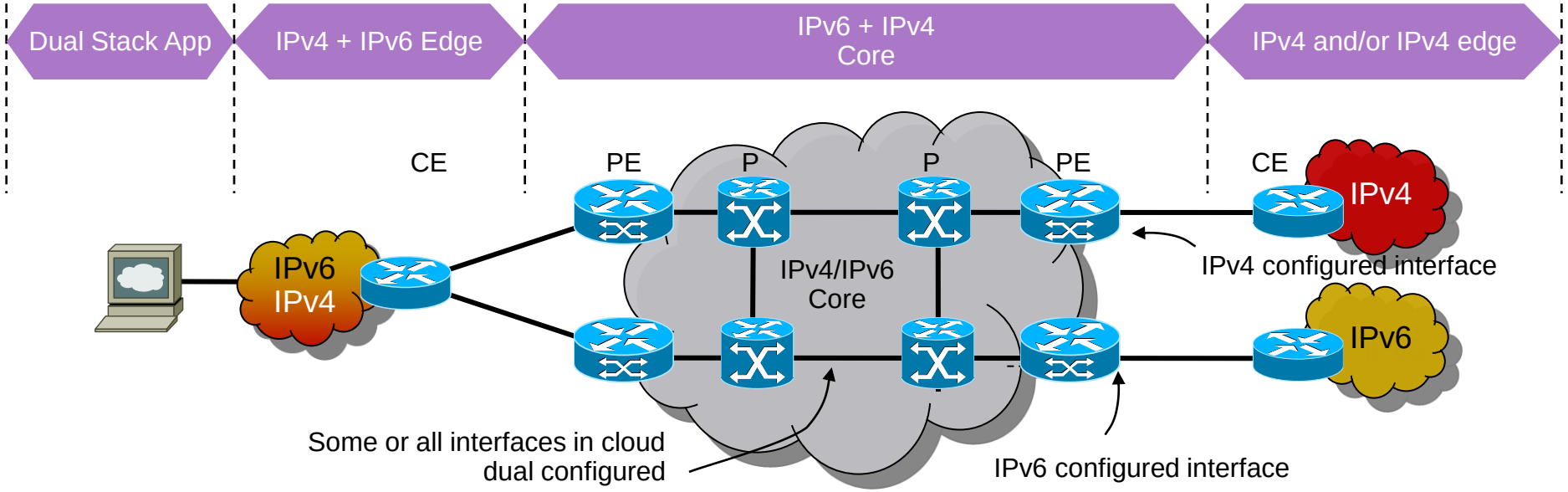
- Tunnelling Options
  - Manual Tunnels (RFC 2893), GRE Tunnels (RFC 2473), L2TPv3, …
- SP Scenarios
  - Configured Tunnels in Core
  - Configured Tunnels or Native IPv6 to IPv6 Enterprise's Customers
  - MP-BGP4 Peering with other IPv6 users
  - Connection to an IPv6 IX

Native IPv6 over Dedicated Data Link



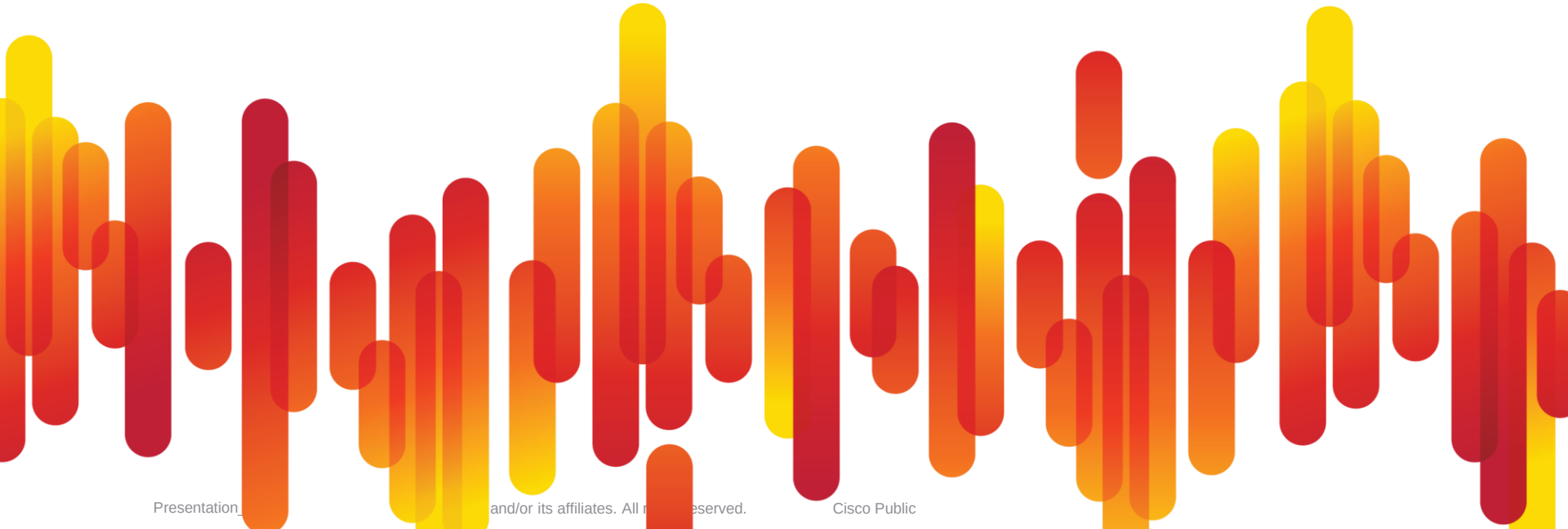
- ISP Scenario
  - Dedicated Data Links between Core routers
  - Dedicated Data Links to IPv6 Customers
  - Connection to an IPv6 IX

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)

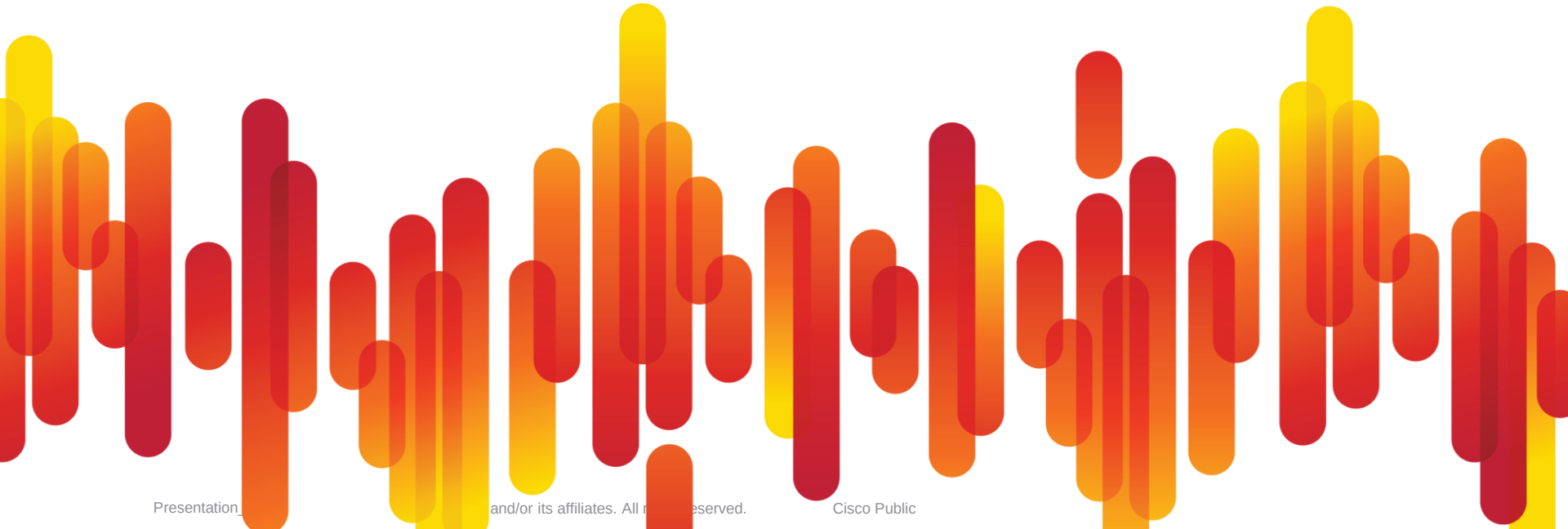
IPv6 in MPLS Environments



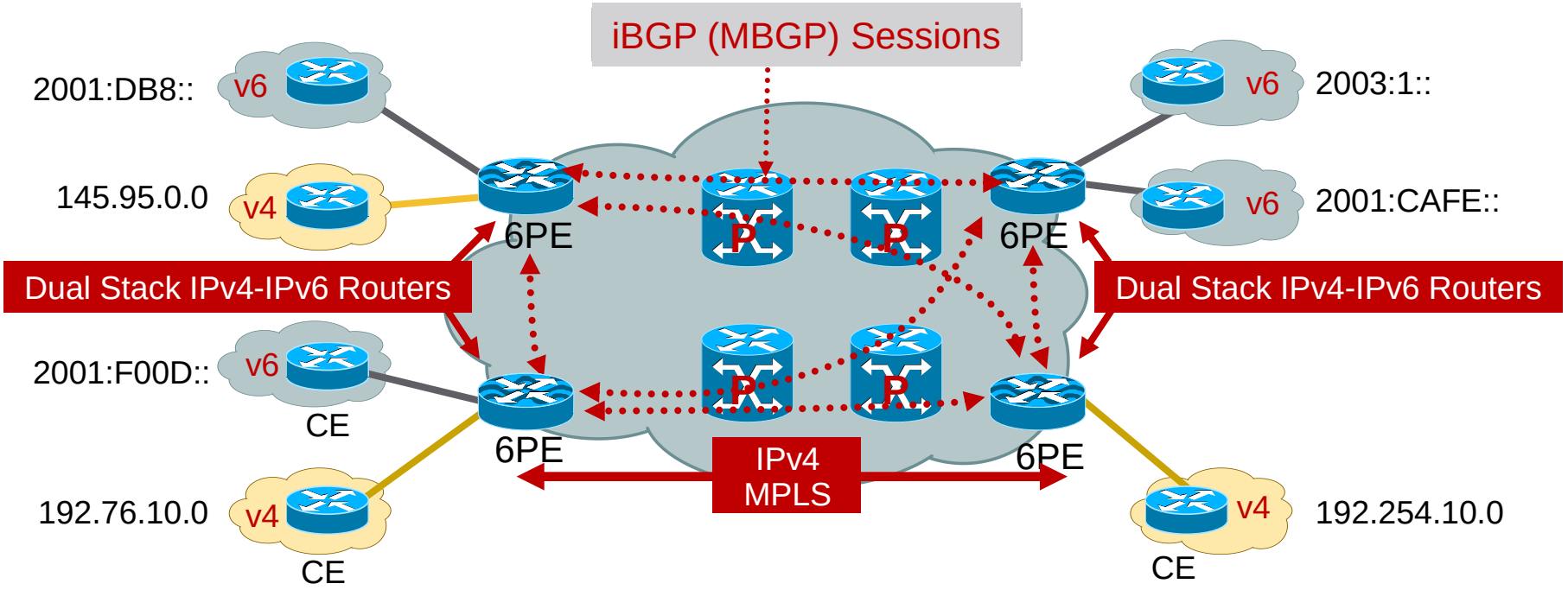
IPv6 over MPLS

- 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

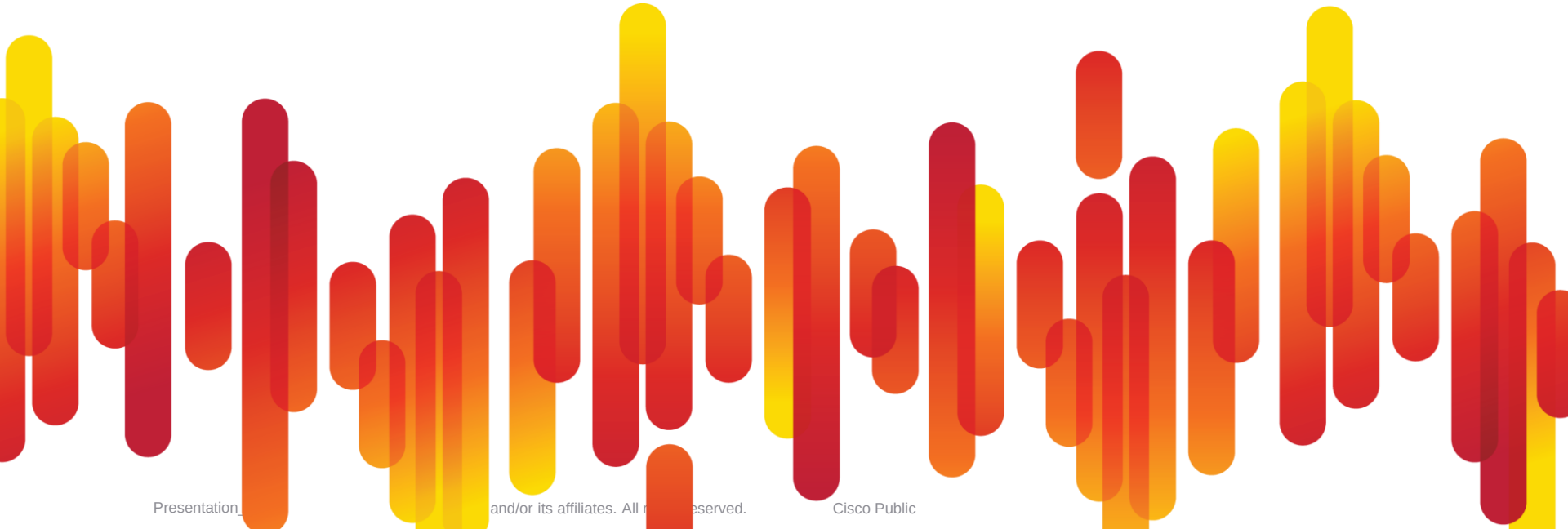


- IPv6 global connectivity over and IPv4-MPLS core
- Transitioning mechanism for providing unicast IP
- PEs are updated to support dual stack/6PE
- IPv6 reachability exchanged among 6PEs via iBGP (MBGP)
- IPv6 packets transported from 6PE to 6PE inside MPLS

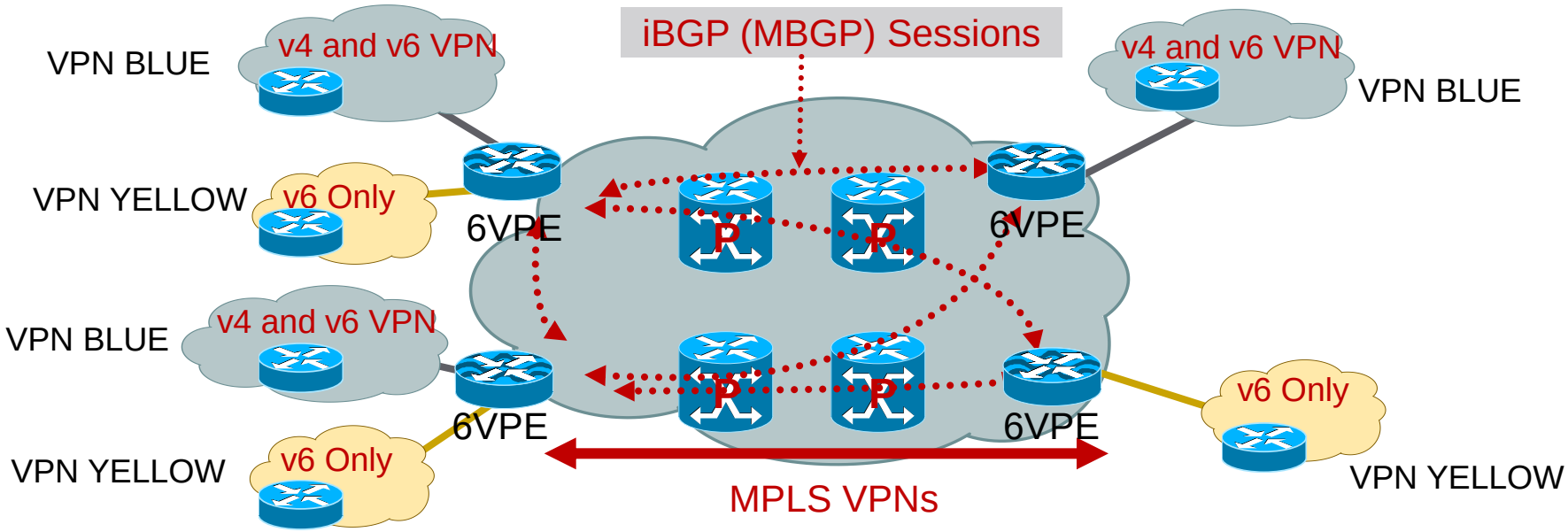
6PE Benefits/Drawbacks

- 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

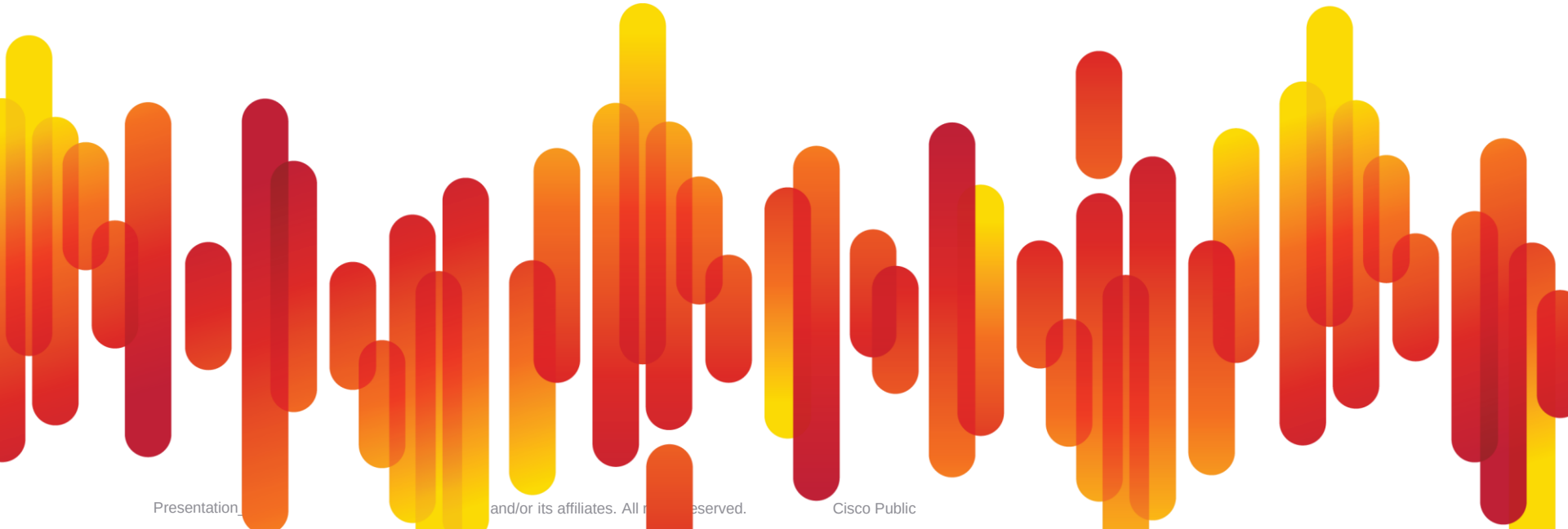
- RFC4659: BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
- 6VPE simply adds IPv6 support to current IPv4 MPLS VPN offering
- For end-users: v6-VPN is same as v4-VPN services (QoS, hub and spoke, internet access, etc.)
- For operators:

  Same configuration operation for v4 and v6 VPN

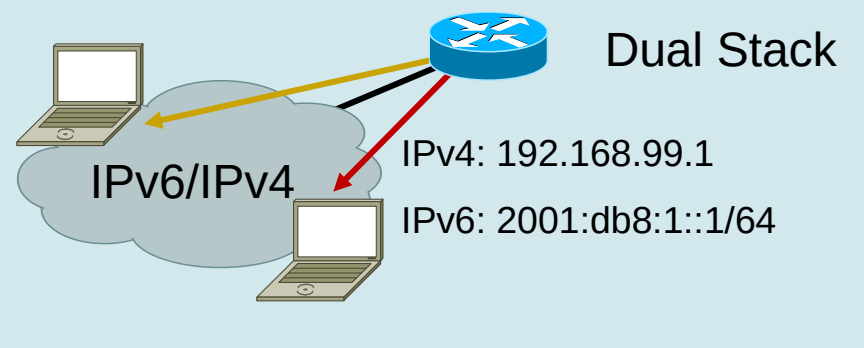
  No upgrade of IPv4/MPLS core (IPv6 unaware)
- Cisco 6VPE Documentation:

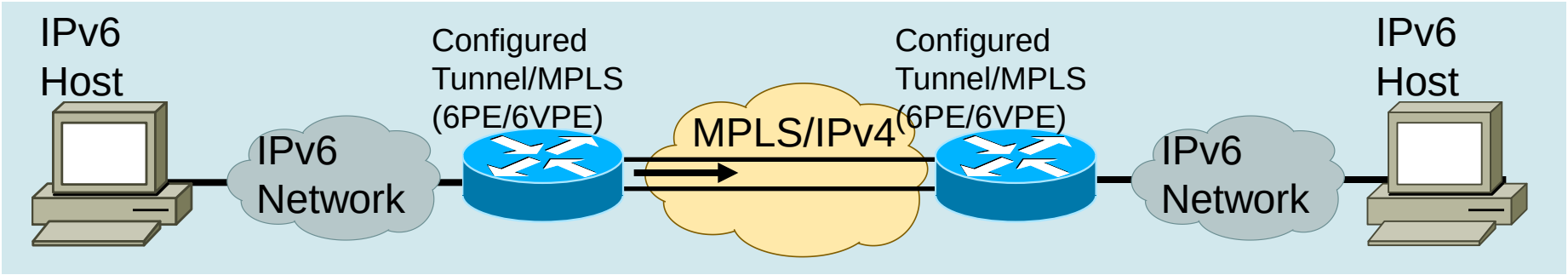
  http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/mpls_vpn/user/guide/ipv6.html

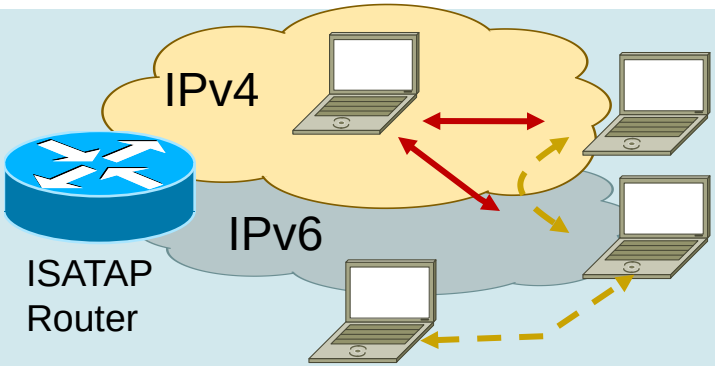
IPv6 in Enterprise Core Networks and Deployment Models



IPv6 Coexistence







ISATAP Tunneling
(Intra-Site Automatic Tunnel Addressing Protocol)

Enterprise IPv6 Deployment
Three Major Options

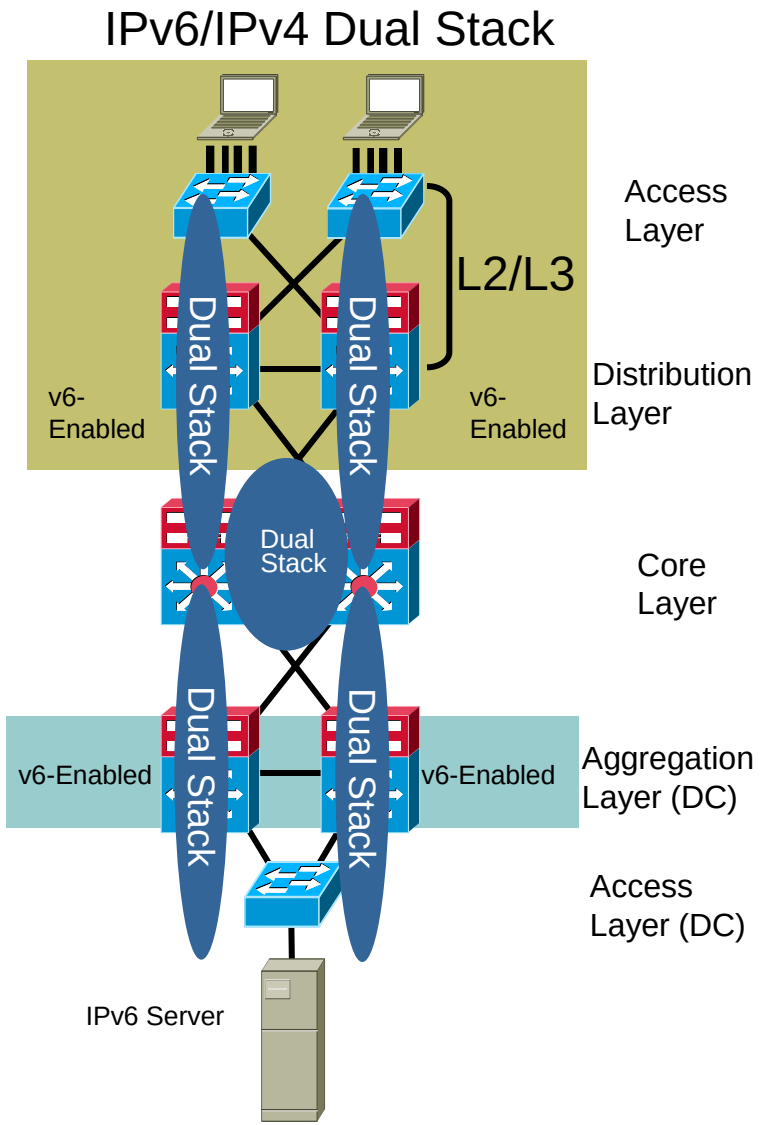
- Dual-stack – The way to go for obvious reasons: performance, security, QoS, Multicast and management
  - Layer 3 switches should support IPv6 forwarding in hardware
- Hybrid – Dual-stack where possible, tunnels for the rest, but all leveraging the existing design/gear
  - Pro – Leverage existing gear and network design (traditional L2/L3 and Routed Access)
  - Con – Tunnels (especially ISATAP) cause unnatural things to be done to infrastructure (like Core acting as Access layer) and ISATAP does not support IPv6 multicast
- IPv6 Service Block – A new network block used for interim connectivity for IPv6 overlay network
  - Pro – Separation, control and flexibility (still supports traditional L2/L3 and Routed Access)
  - Con – Cost (more gear), does not fully leverage existing design, still have to plan for a real dual-stack deployment and ISATAP does not support IPv6 multicast

Campus IPv6 Deployment Options
Dual-stack IPv4/IPv6

- Requires switching/routing platforms to support hardware based forwarding for IPv4 and IPv6
- IPv6 is transparent on L2 switches except for multicast - MLD snooping

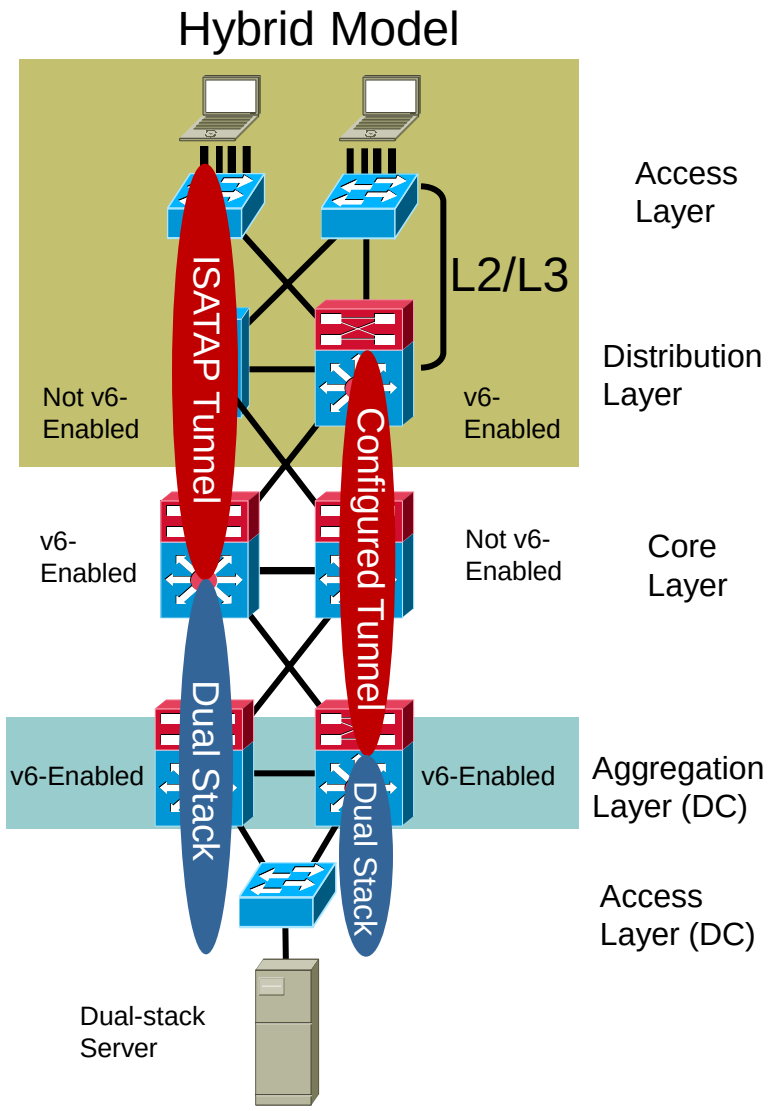
  IPv6 management—Telnet/SSH/HTTP/SNMP
- Requires robust control plane for both IPv4 and IPv6

  Variety of routing protocols—The same ones in use today with IPv4
- Requires support for IPv6 multicast, QoS, infrastructure security, etc…
- IPv4 and IPv6 control planes and data planes must not impact each other



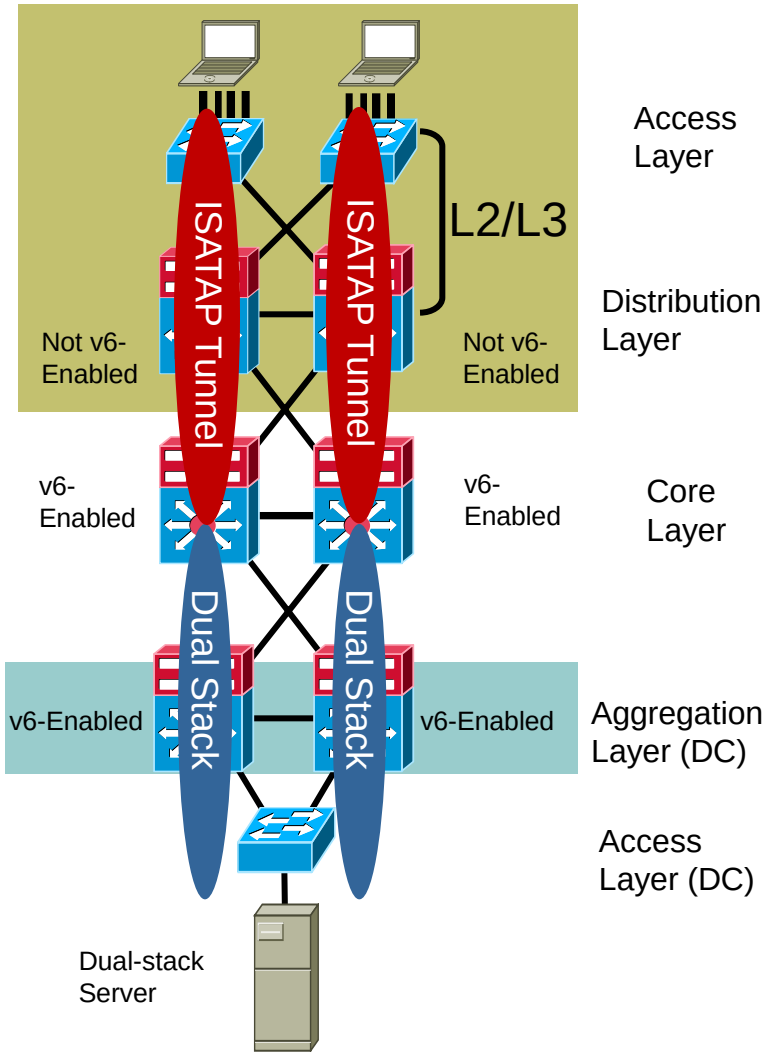
Campus IPv6 Deployment Options
Hybrid Model

- Offers IPv6 connectivity via multiple options
  - Dual-stack
  - Configured tunnels – L3-to-L3
  - ISATAP – Host-to-L3
- Leverages existing network
- Offers natural progression to full dual-stack design
- May require tunneling to less-than-optimal layers (i.e. Core layer)
- ISATAP creates a flat network (all hosts on same tunnel are peers)
  - Create tunnels per VLAN/subnet to keep same segregation as existing design (not clean today)
- Provides basic HA of ISATAP tunnels via old Anycast-RP idea
- ISATAP does not support IPv6 Multicast
- Configured tunnels do support IPv6 Multicast

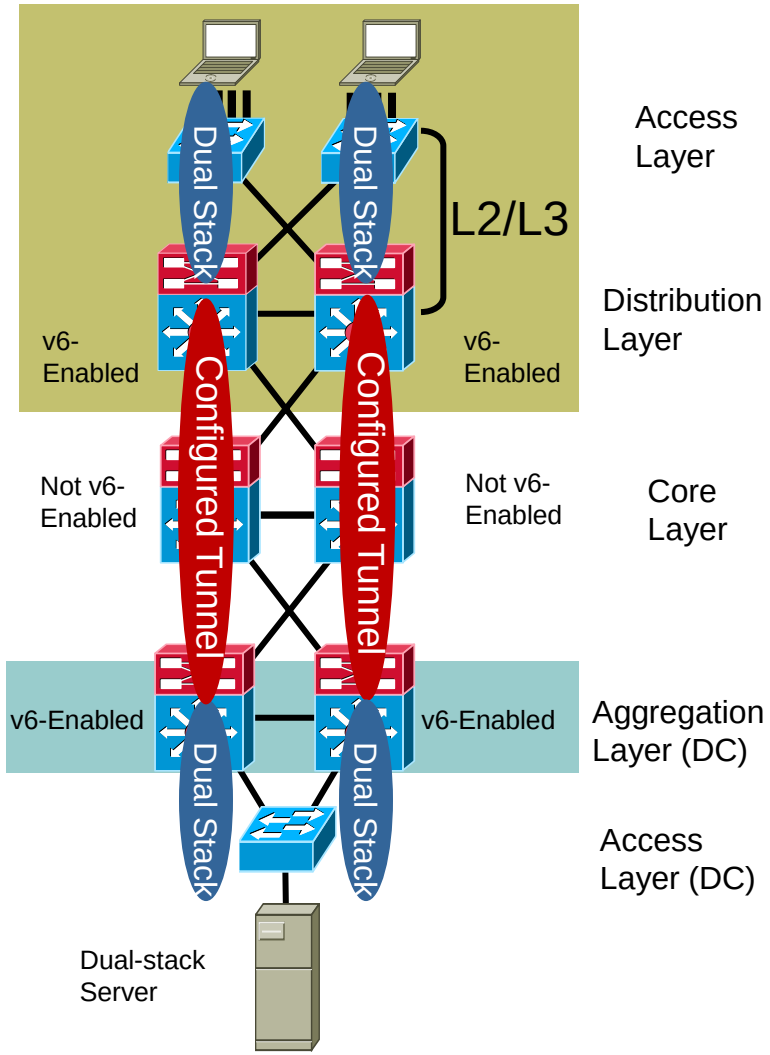


Hybrid Model Examples

Hybrid Model Example #1



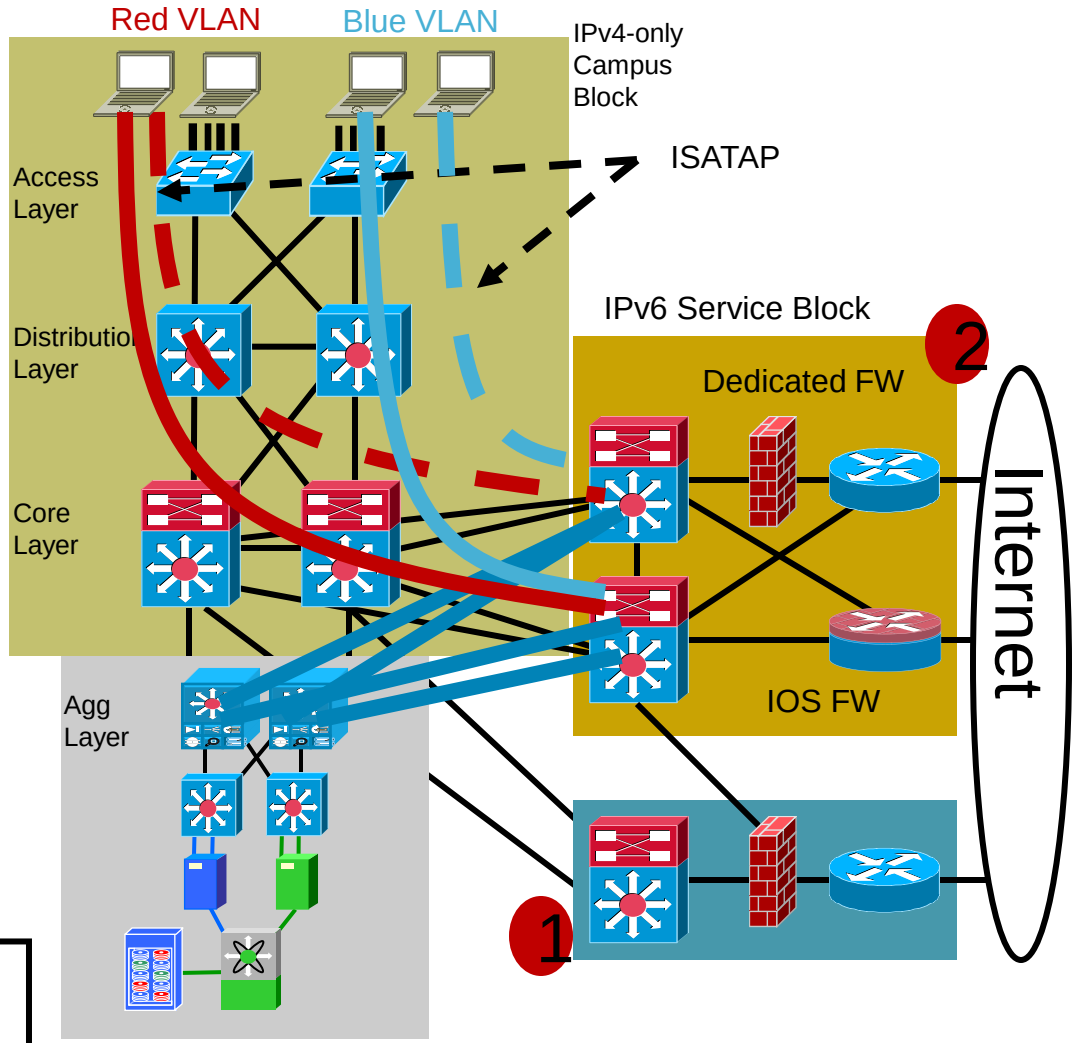
Hybrid Model Example #2



Campus IPv6 Deployment Options

IPv6 Service Block – An Interim Approach

- Provides ability to rapidly deploy IPv6 services without touching existing network
- Provides tight control of where IPv6 is deployed and where the traffic flows (maintain separation of groups/locations)
- Provides basic HA of ISATAP
- ISATAP tunnels from PCs in Access layer to service Block switches
- In this example configured tunnels are used from Data Center to Service Block
- Dependency on ISATAP alienates IPv6 multicast applications
- 1) Leverage existing ISP block for both IPv4 and IPv6 access
- 2) Use dedicated ISP connection just for IPv6 – Can use IOS FW or PIX/ASA appliance



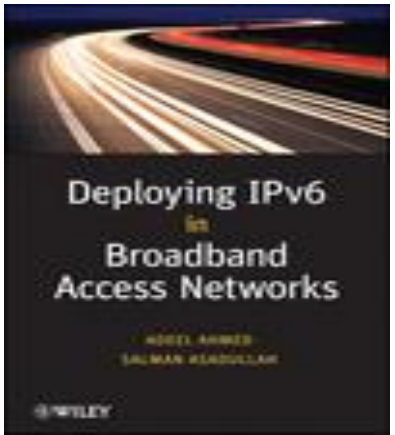
Primary ISATAP Tunnel

Secondary ISATAP Tunnel

Equal-cost Configured Tunnel (Mesh)

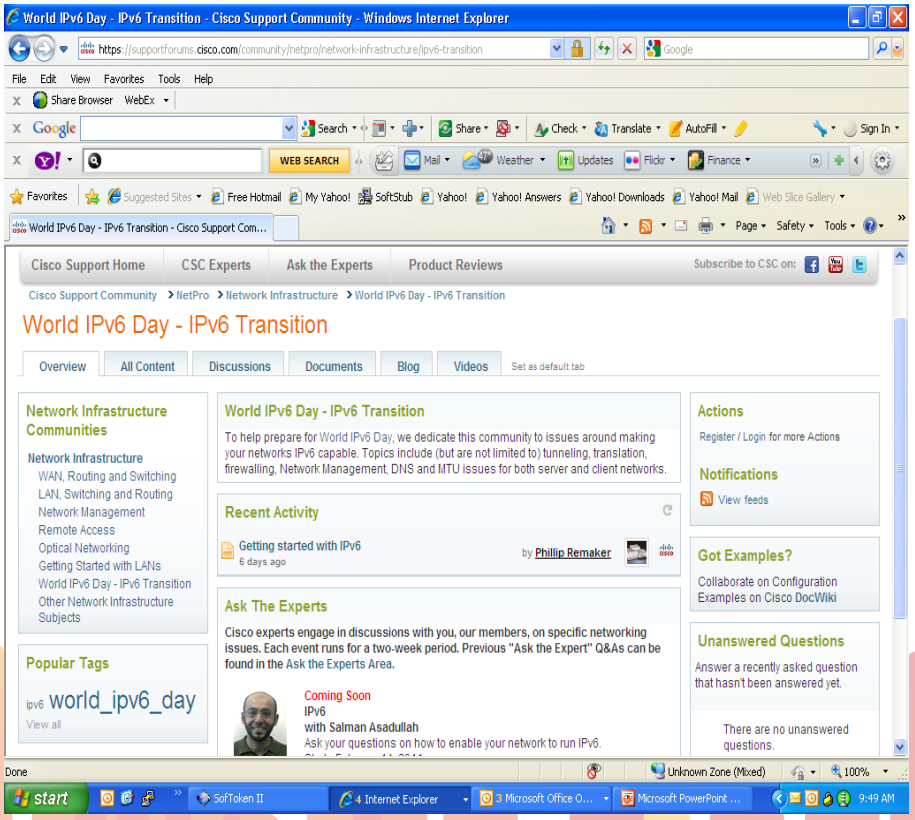
Conclusion

- 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!

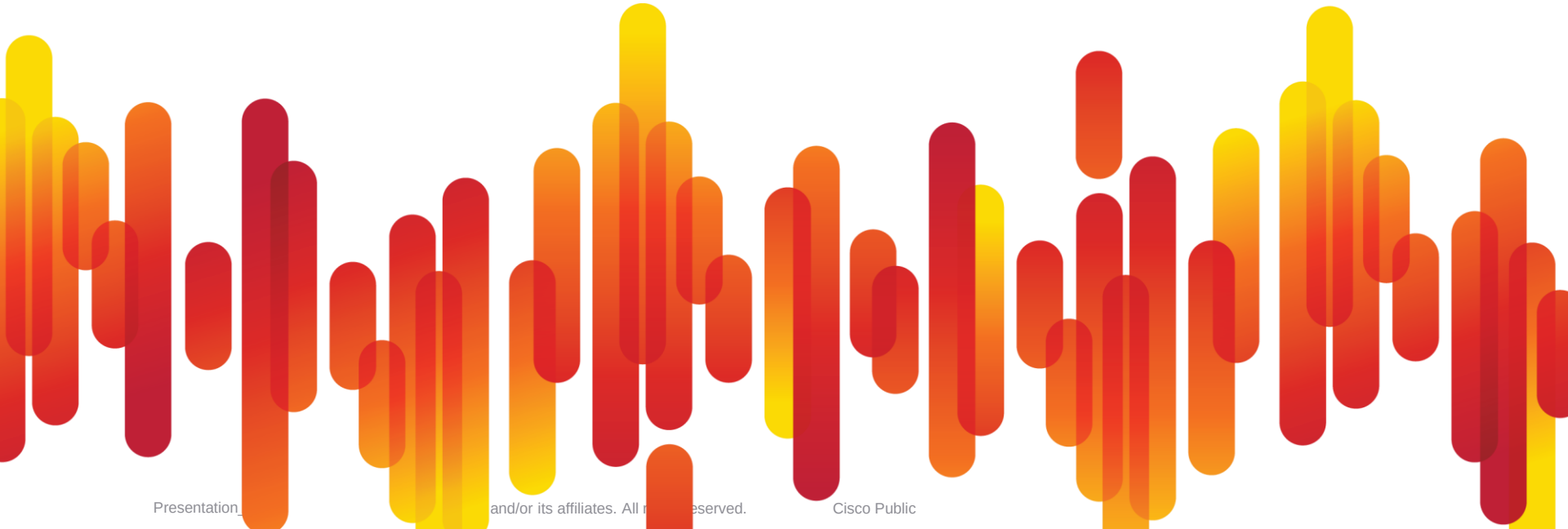
- **Free** for anyone with Cisco.com registration
- Get **timely** answers to your technical questions
- Find **relevant** technical documentation
- Engage with over 200,000 **top technical experts**
- **Seamless** transition from discussion to TAC Service Request *(Cisco customers and partners only)*
- 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