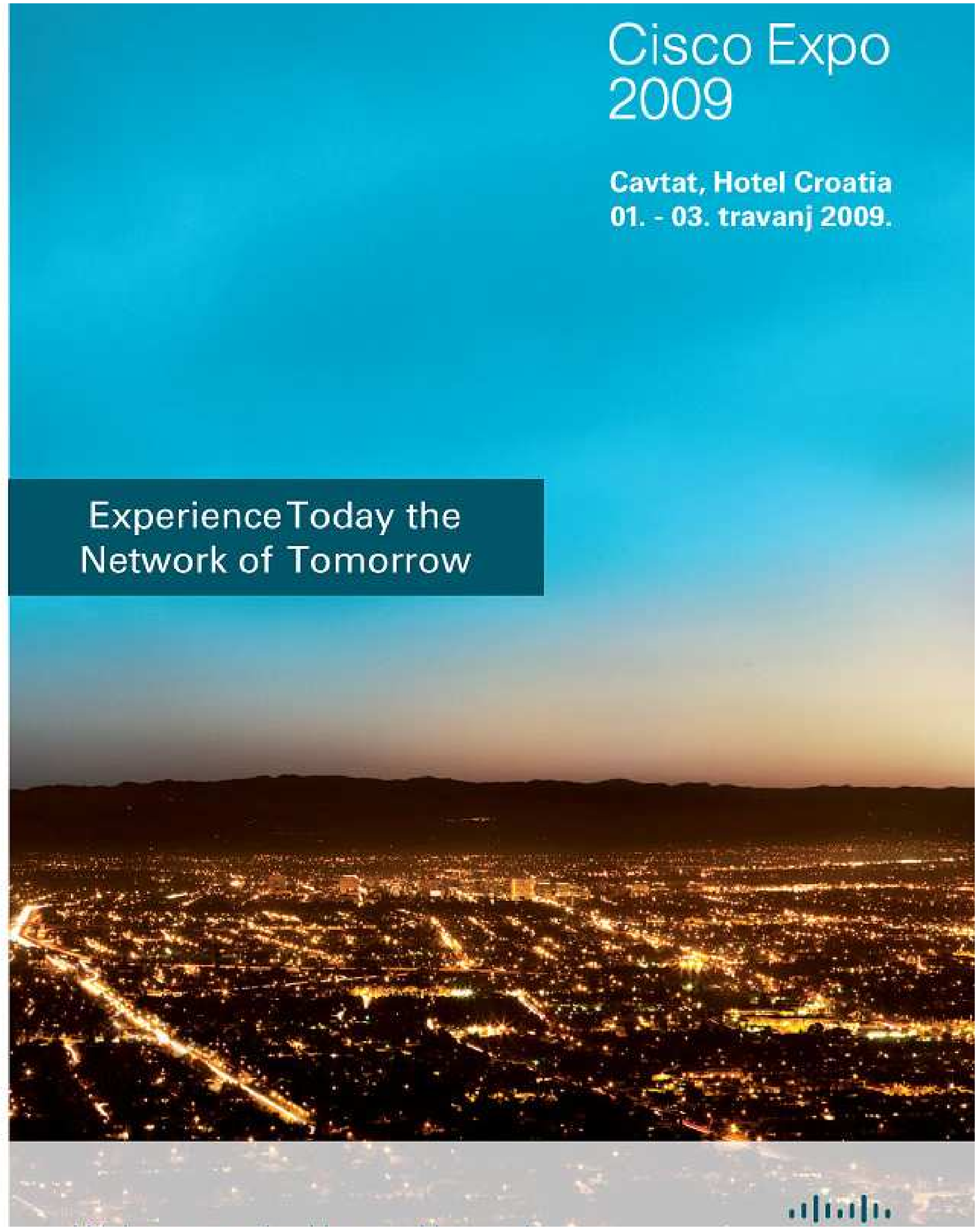
Transition to IPv6

Dejan Jaksic

Systems Engineer SP

djaksic@cisco.com



Sponzor konferencije

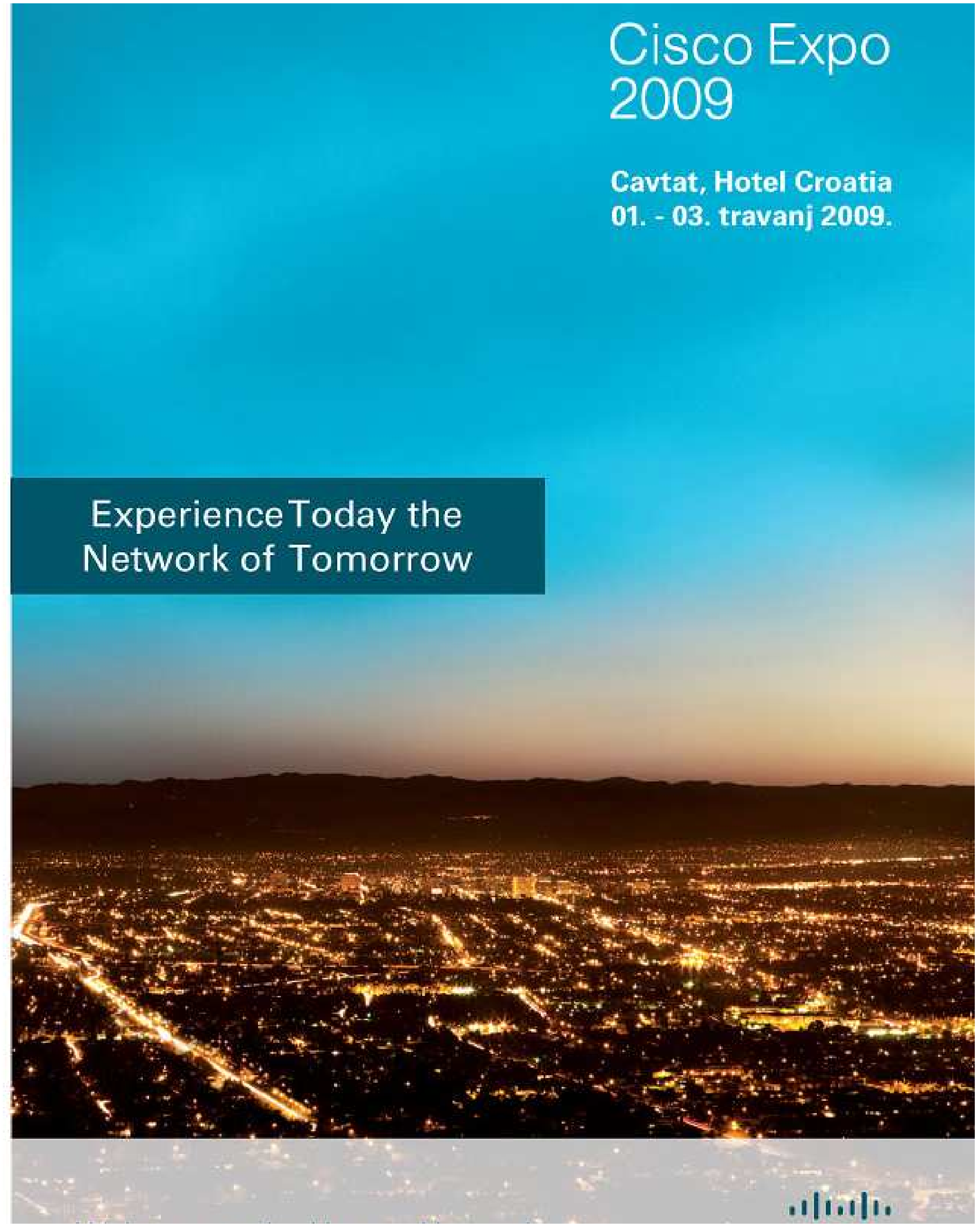
Partner digitalnog oglašavanja

Partneri konferencije

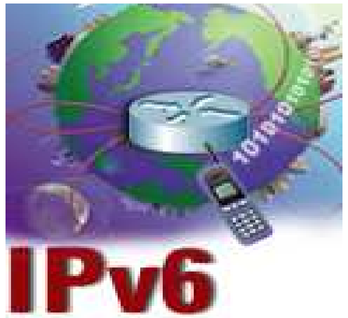
Pokrovitelji konferencije

Tehnološki sponzori

Medijski sponzori



Agenda



- IPv6 short overview
- Why deploy IPv6?
- Transition mechanisms
- IPv6 for Service Providers
- Use cases
- Conclusions

IPv6 short overview

The one thing to remember

IPv6 is not a Revolution, it is an Evolution!

but

IPv6 does not interoperate with IPv4!!!

IPv6 Technology Scope

Protocol Aspect	*IPv4*	*IPv6*
Address Range	32-bit, Network Address Translation	128-bit, Multiple Scopes
ICMP	ICMP	ICMPv6, “ARP”, SLAAC
Autoconfiguration	DHCP	Serverless, Reconfiguration, DHCP-PD, DHCP
Routing	RIPv2, EIGRP, OSPFv2, ISIS, MP-BGP	RIPng, EIGRPv6, OSPFv3, ISIS-ST/MT, MP-BGP

IPv6 Technology Scope (cont.)

Protocol Aspect	*IPv4*	*IPv6*
IP Multicast	IGMP/PIM/Multicast BGP	MLD/PIM/Multicast BGP, Scope Identifier
Quality-of-Service	Differentiated Service, Integrated Service	Differentiated Service, Integrated Service
Security	IPSec	IPSec Mandated, targets End-to-End
Mobility	Mobile IP	Mobile IP with Direct Routing

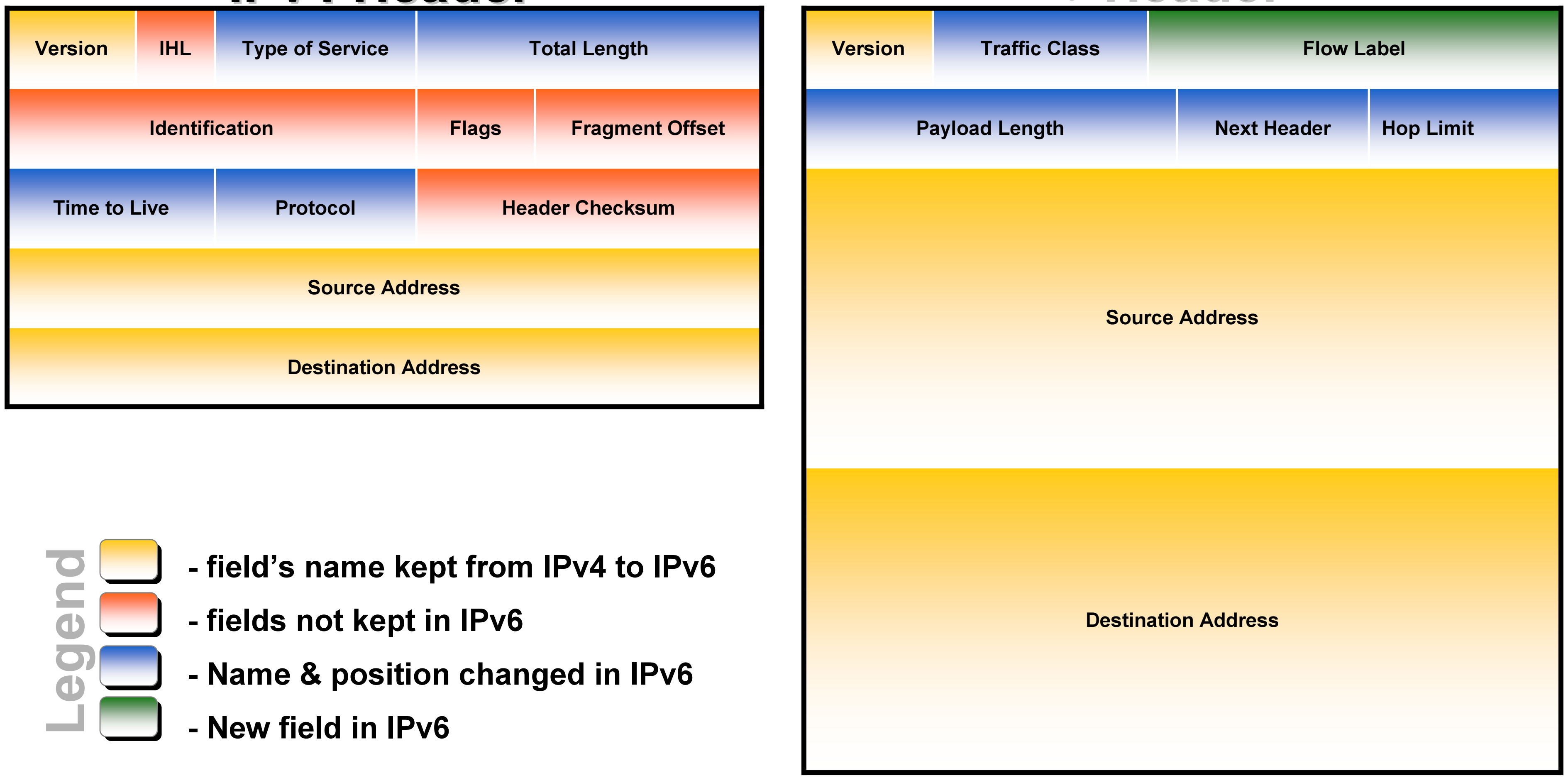
IPv6 Related Myths and Realities

Claim	*Myth or Reality*
IPv6 protocol has problems with multihoming	Not true, the protocol itself has no problems, the allocation policy creates difficulties
IPv6 has improved Quality-of-Service	Not true, the flow label could provide added capabilities but it is not used
IPv6 Multicast services are easier to deploy	True, primarily due to large address space and scopping
IPv6 is more Secure than IPv4	Not true, the claim is based on IPsec requirement
IPv6 mobility services are easier to deploy	True, primarily due to cleaner implementation
Lack of NAT in IPv6 is a security challenge	Not true, all perceived benefits of NAT can be implemented in IPv6

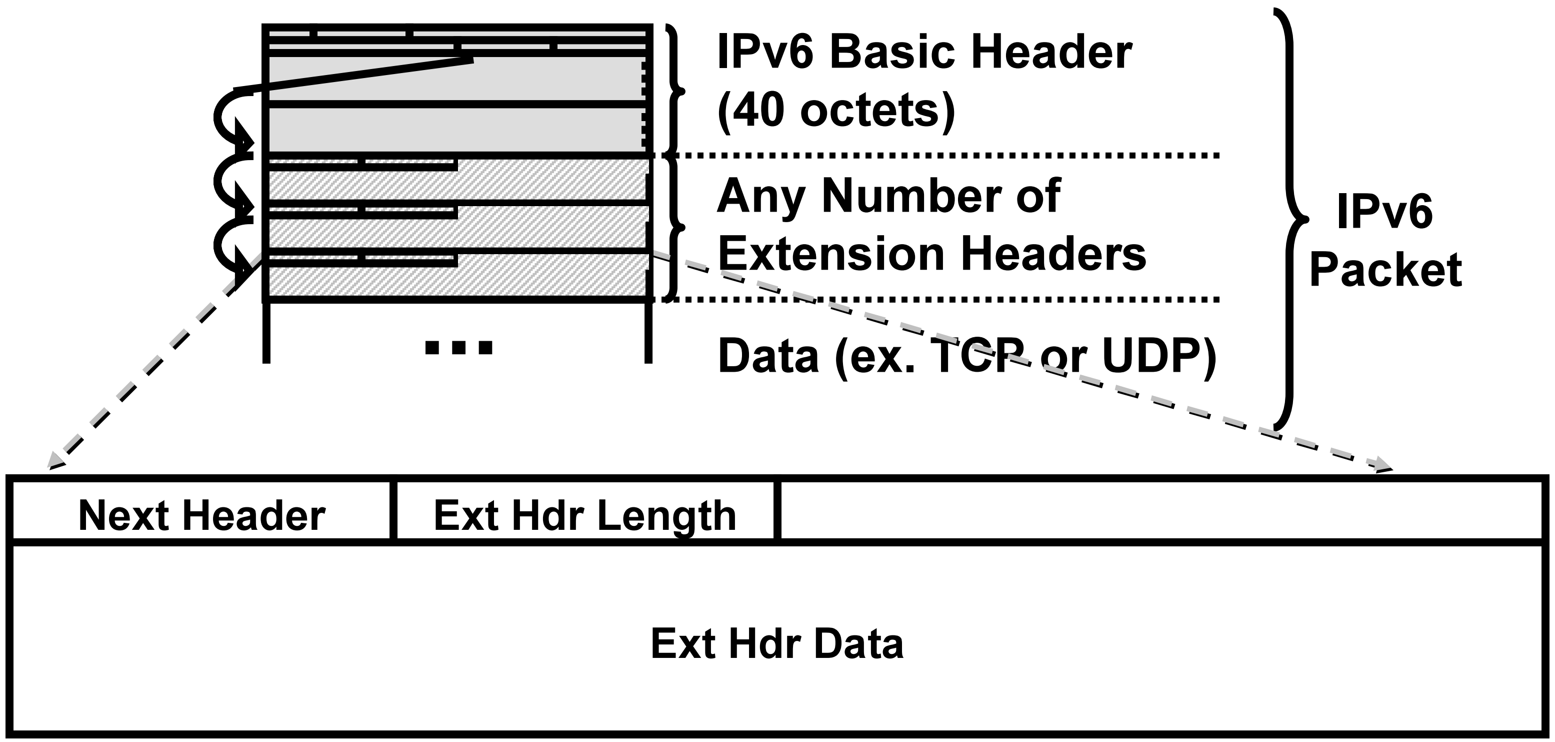
IPv4 & IPv6 Header Comparison

IPv4 Header

IPv6 Header



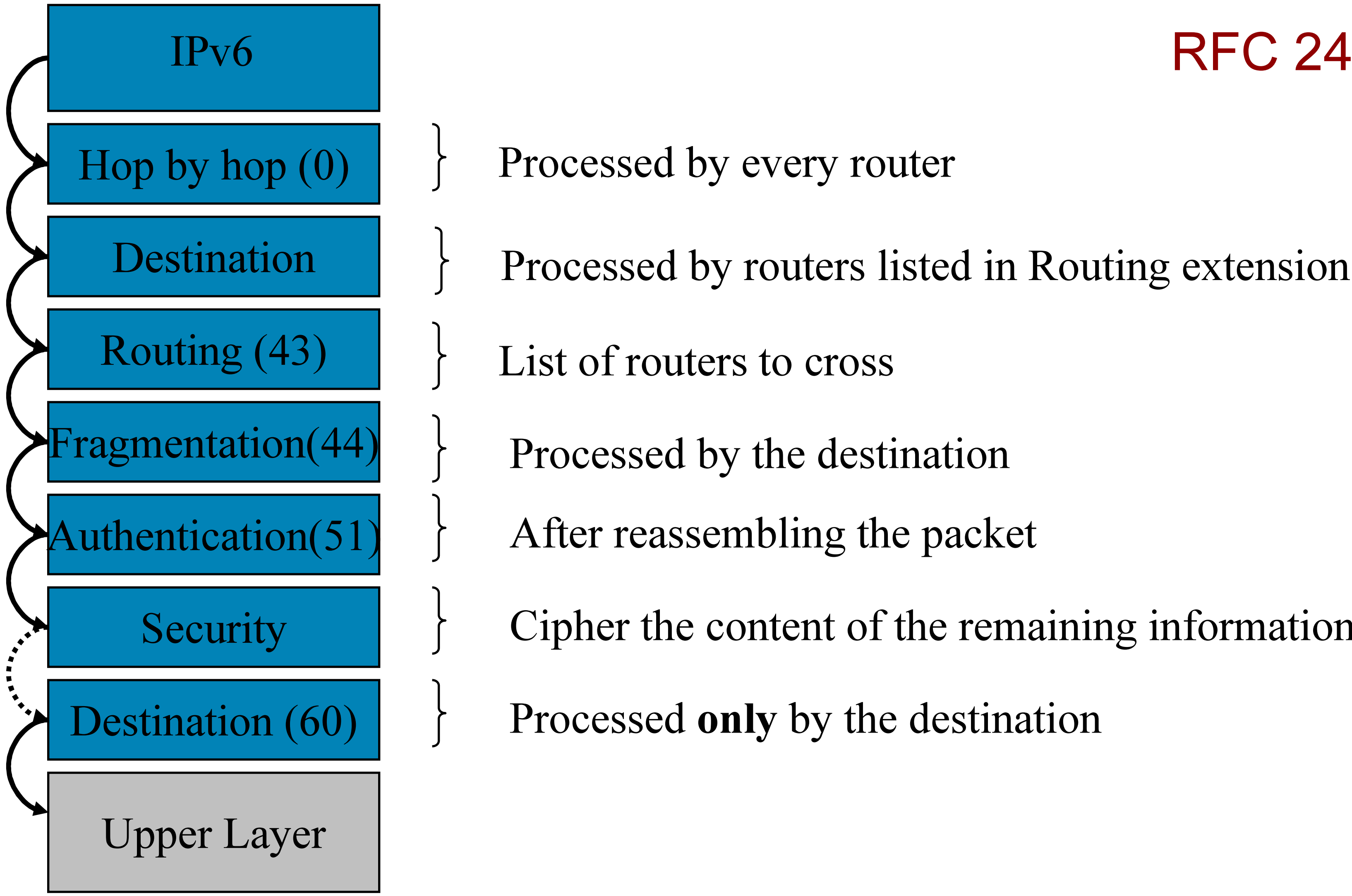
Header Format Simplification
IPv6 Extension Headers



- The value of Next Header field determines the type of information following the basic IPv6 header; it can be a transport layer packet, such as TCP/UDP or can be an extension header
- Extension headers are optional following the IPv6 basic header
- Each extension header is 8 octets(64 bits) aligned
- Together all extension headers form a chained list of headers

IPv6 extension headers: order is important

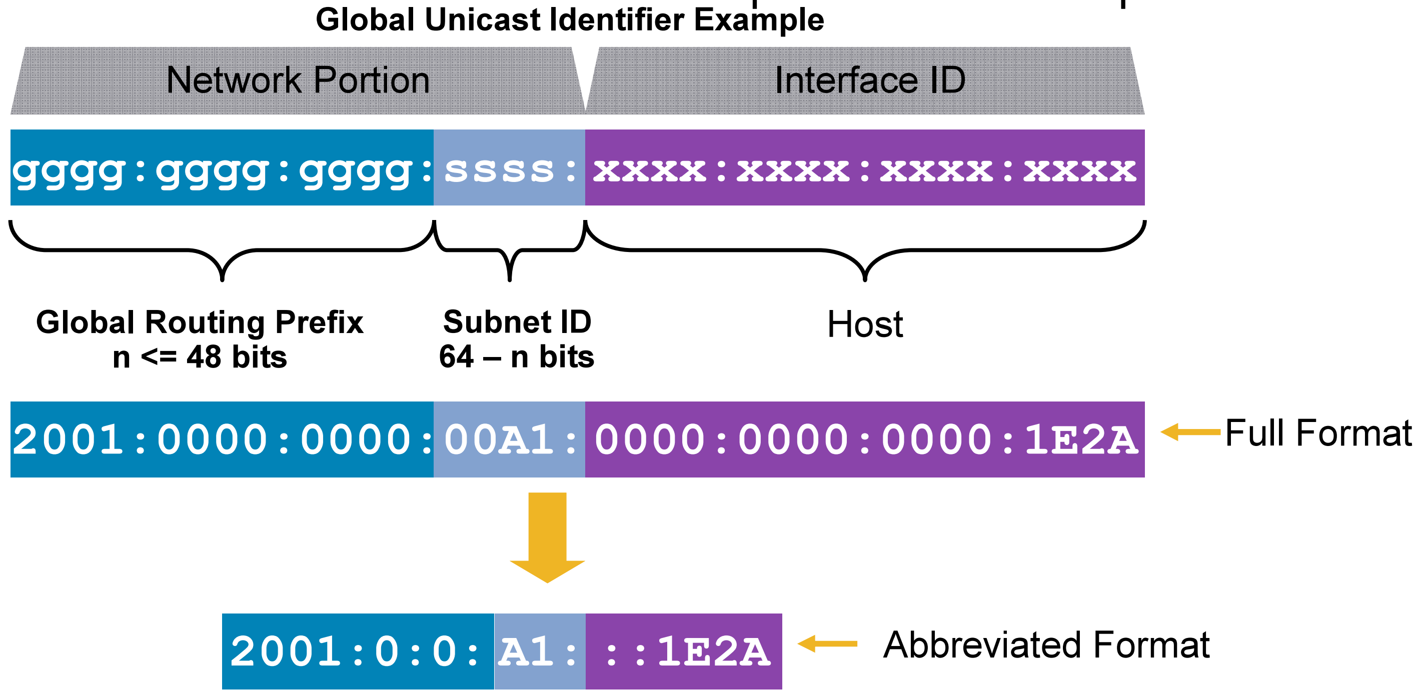
RFC 2460



IPv6 Addresses – RFC 2460

IPv6 addresses are 128 bits long

- Segmented into 8 groups of four HEX characters
- Separated by a colon (:)
- 50% for network ID, 50% for interface ID
- Network portion is allocated by Internet registries 2^64 (1.8×10^{19})
- Still leaves us with ~ 3 billion network prefixes for each person on earth



IPv6 Address Types - RFC 2460

- Three types of unicast address scopes

  Link-Local – Non routable exists on single layer 2 domain (FE80::/64)

  `FE80:0000:0000:0000:xxxx:xxxx:xxxx:xxxx`

  Site/Unique-Local – Routable with an administrative domain (FC00::/7)

  `FC00:gggg:gggg:ssss:xxxx:xxxx:xxxx:xxxx`

  Global Aggregatable Unicast – Routable across the Internet (2000::/3)

  `2000:GGGG:GGGG:ssss:xxxx:xxxx:xxxx:xxxx`

- Multicast addresses begin with FF00::/8

  `FFfs:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`

  Flags (f) carried in 3rd nibble (4 bits)

  Scope (s) incorporated into 4th nibble (4 bits)

PI versus PA space

- IPv6 addresses can be allocated in two ways
- Provider Assigned (PA)

  Addresses and prefixes assigned to subscribers from prefix pool assigned to service provider

  PA provides prefix and route aggregation

  This is good because Internet routing table size minimised
- Provider Independent (PI)

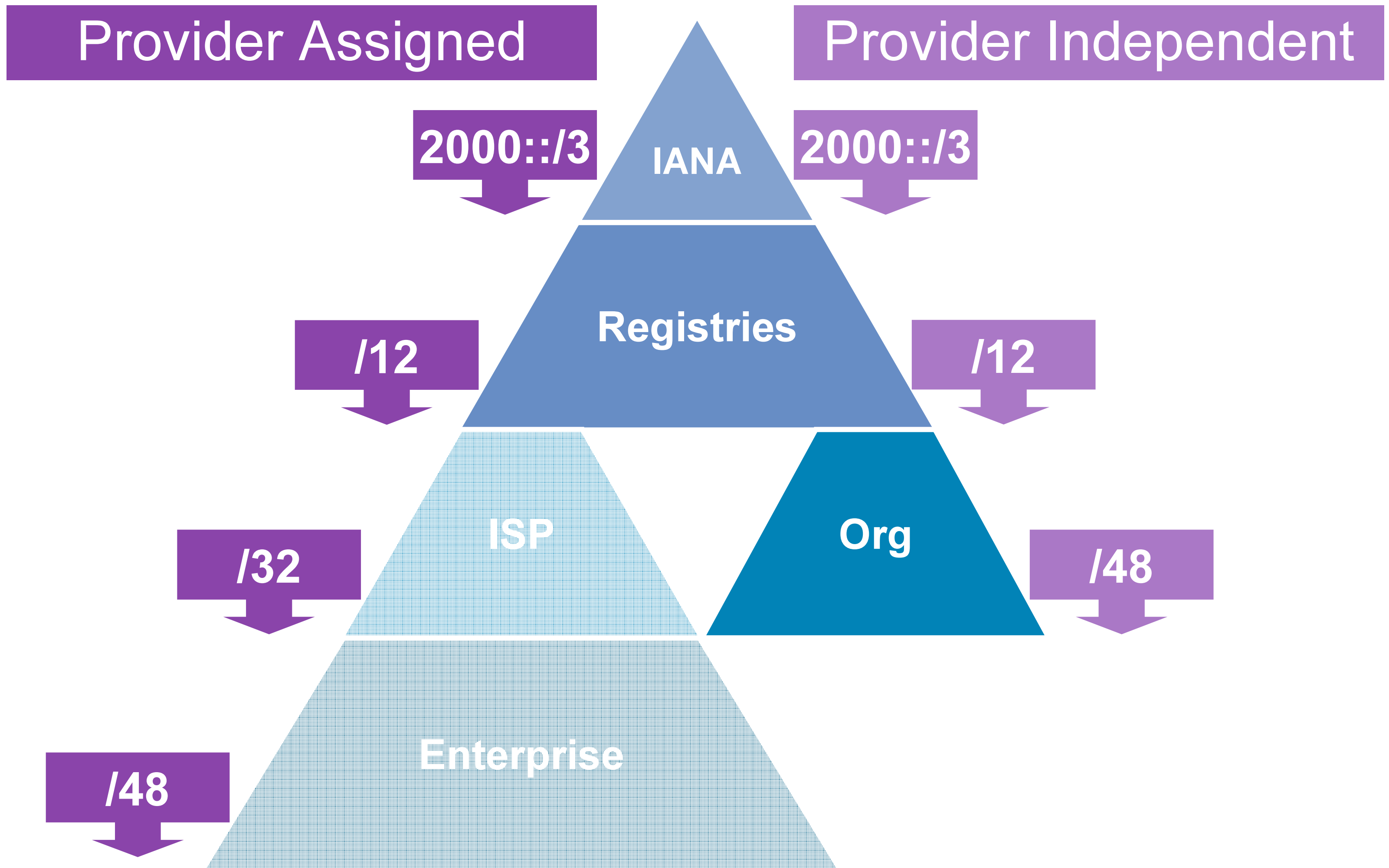
  Addresses and prefixes assigned to subscribers independent of provider pool

  PI allows subscriber to change between service providers; PA requires renumbering of subscriber network

  Allows multi-homing with same address space

  This is not so good – eventually we have same problem as IPv4

PI and PA Allocation Process



http://www.ripe.net/ripe/policies/proposals/2006-01.html
http://www.ripe.net/ripe/policies/proposals/2006-05.html

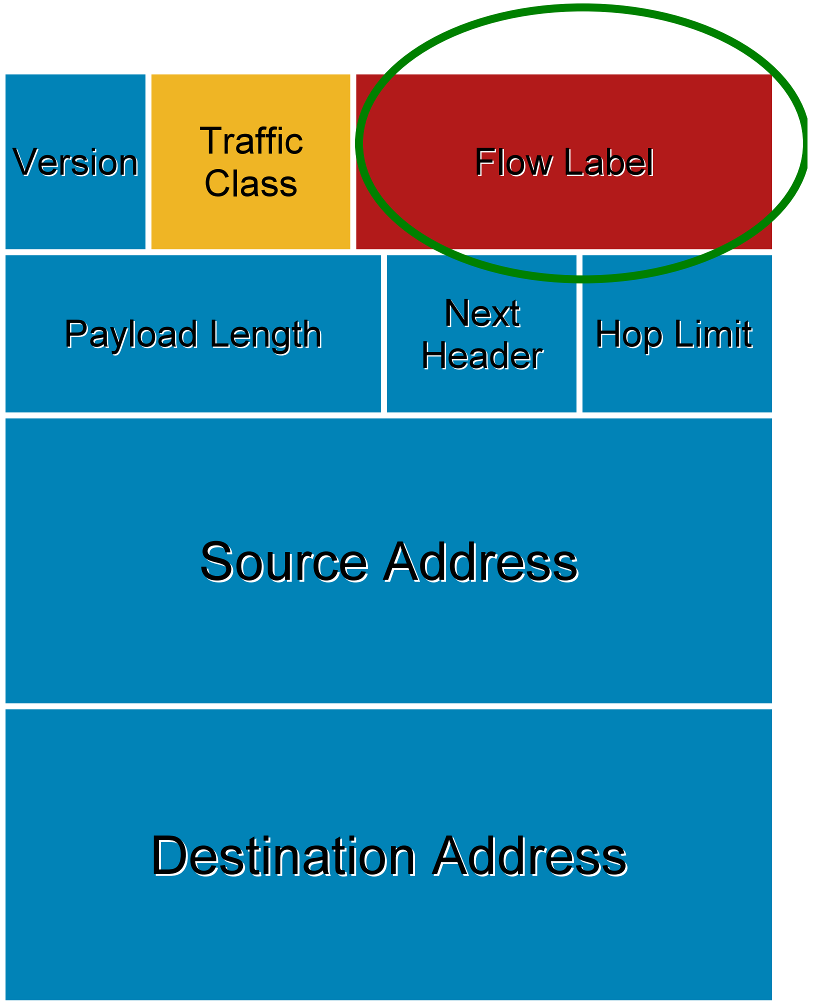
Routing: The IPv4 – IPv6 Parallel

RIP	RIPv2 for IPv4 RIPng for IPv6 Distinct but similar protocols with RIPng taking advantage of IPv6 specificities
OSPF	OSPFv2 for IPv4 OSPFv3 for IPv6 Distinct but similar protocols with OSPFv3 being a cleaner implementation that takes advantage of IPv6 specificities
IS-IS	Extended to support IPv6 Natural fit to some of the IPv6 foundational concepts Supports Single and Multi Topology operation
EIGRP	Extended to support IPv6 (IPv6_REQUEST_TYPE, IPv6_METRIC_TYPE, IPv6_EXTERIOR_TYPE) Some changes reflecting IPv6 characteristics
BGP	New MP_REACH_NLRI, MP_UNREACH_NLRI, AFI=2 with SAFI for Unicast/Multicast/Label/VPN Peering over IPv6 or IPv4 (route maps)

- For all intents and purposes, IPv6 IGPs are similar to their IPv4 counterparts
- IPv6 IGPs have additional features that could lead to new designs

Quality of Service

- IPv6 QoS
  - Same architectural models as IPv4
  - *Differentiated Services (Traffic Class field)*
  - *Integrated Services (RSVP)*
- IPv6 traffic class
  - Value defined per applications, same DSCP for applications over both IPv4 and IPv6 – decision to differentiate per protocol is an operational one
- RSVP for IPv6
  - Major RSVP RFC's do support IPv6
  - Use Hop-by-Hop option header for Router Alert
- IPv6 flow label (RFC 3697)
  - A new 20-bit field in the IPv6 basic header
  - Its value cannot be changed by intermediate devices
  - **No RFC regarding flow label usage yet**
- Transition
  - Mapping between IPv6 DSCP & IPv4 ToS or MPLS EXP



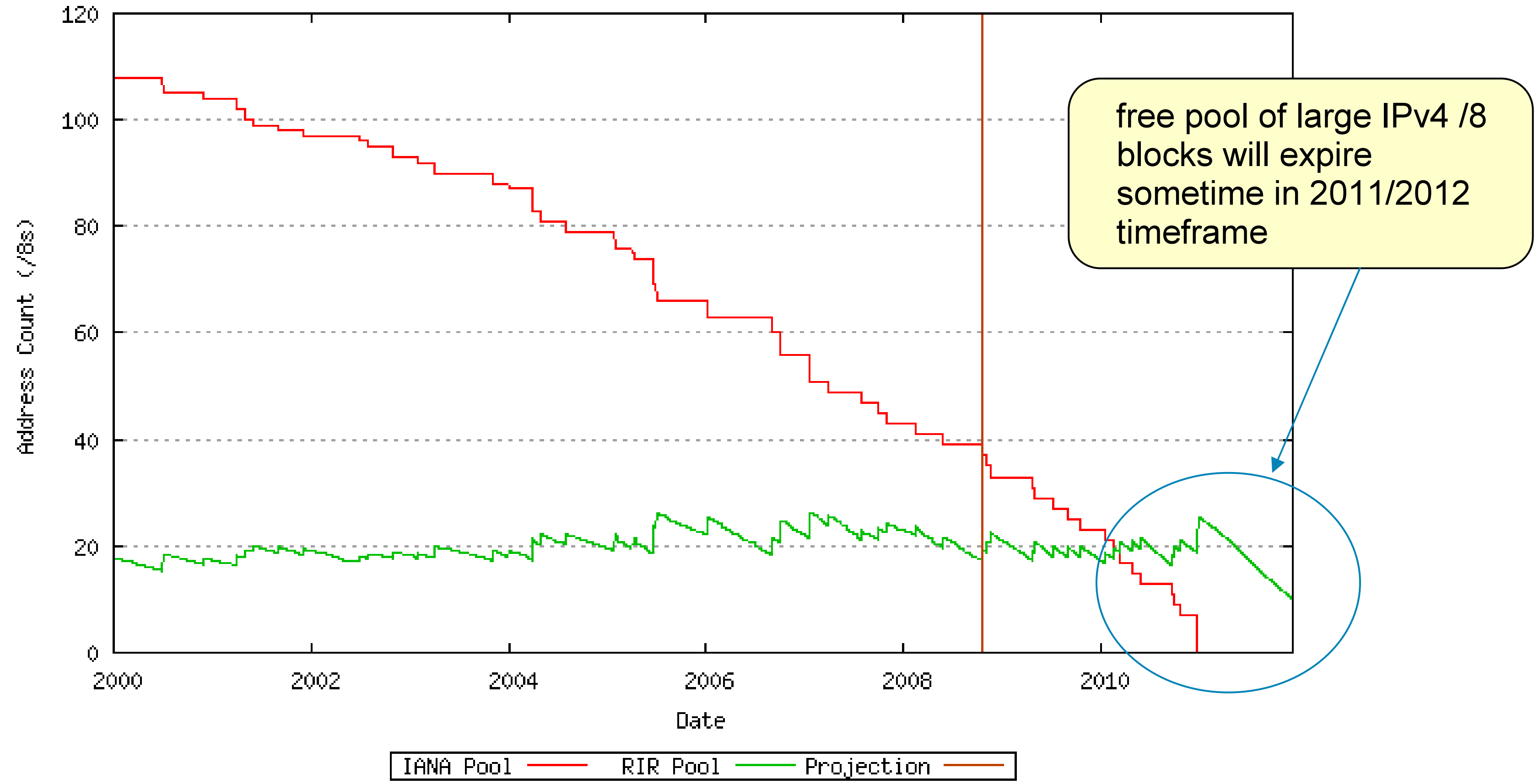
IPv4 and IPv6 Multicast Comparison

Service	IPv4 Solution	IPv6 Solution
Addressing Range	32-bit, Class D	128-bit (112-bit Group)
Routing	Protocol Independent, All IGPs and MBGP	Protocol Independent, All IGPs and MBGP with v6 mcast SAFI
Forwarding	PIM-DM, PIM-SM, PIM-SSM, PIM-bidir, PIM-BSR	PIM-SM, PIM-SSM, PIM-bidir, PIM-BSR
Group Management	IGMPv1, v2, v3	MLDv1, v2
Domain Control	Boundary, Border	Scope Identifier
Interdomain Solutions	MSDP across Independent PIM Domains	Single RP within Globally Shared Domains

- Static RP, BSR, No Auto-RP
- **Embedded RP**

Why deploy IPv6?

IPv4 Address Completion (Run-Out)



- see http://www.potaroo.net/tools/ipv4/index.html for more details

Drivers

- Internal/External Drivers
- Tactical/Strategic Drivers
- No Killer Apps but plenty other less glamorous reasons
- Business case
- Upgrade for IPv6 and for its deployment usually occurs in the context of and coordination with other major efforts (BW upgrades, NGNs, etc)
- All in all … a great opportunity to win or lose business for less obvious reasons!

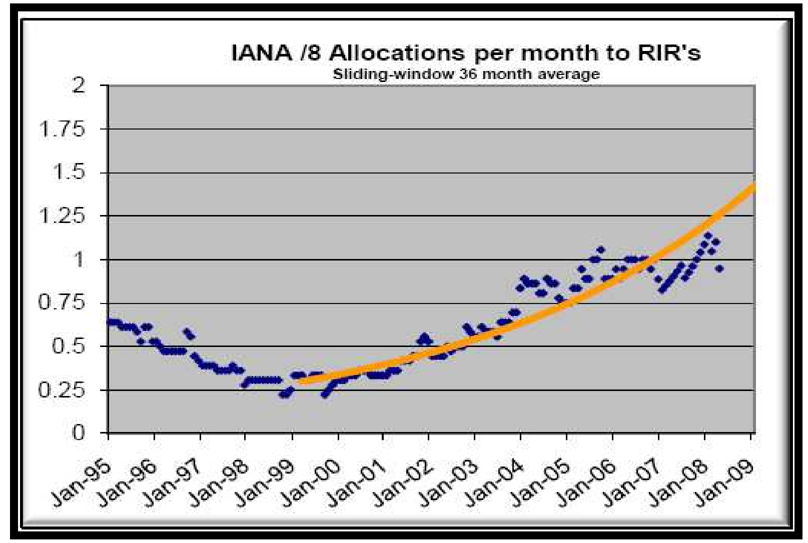
''It's an infrastructure issue, not an application issue.''

Jeff Doyle, CCIE No. 1919

External Drivers

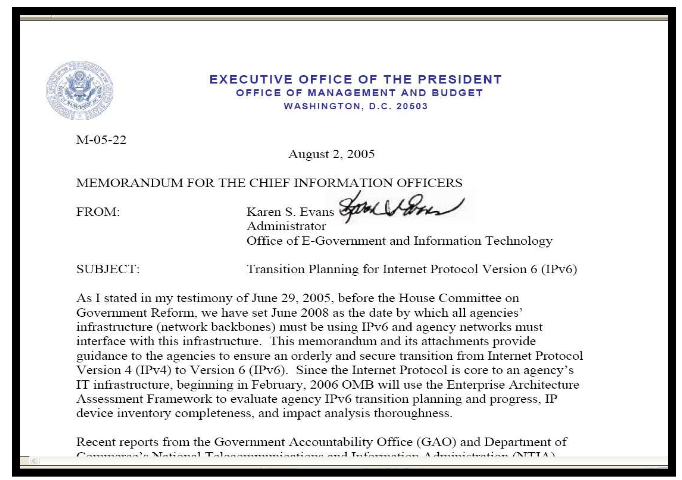
IPv4 address space exhaustion

- Growth constraints
- Scalability constraints
- Increased Opex



Customer demand:

- Federal mandate
- Early adopters



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, beginning in February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Recent reports from the Government Accountability Office (GAO) and Department of

Internal Drivers

Operational costs

- Managing devices
- Simplifying designs

Services:

- Content delivery
- Connected home
- Managed services
- Fixed-Mobile Convergence
- LTE and Evolved Packet Core

IPv6 @ Comcast Managing 100+ Million IP Addresses

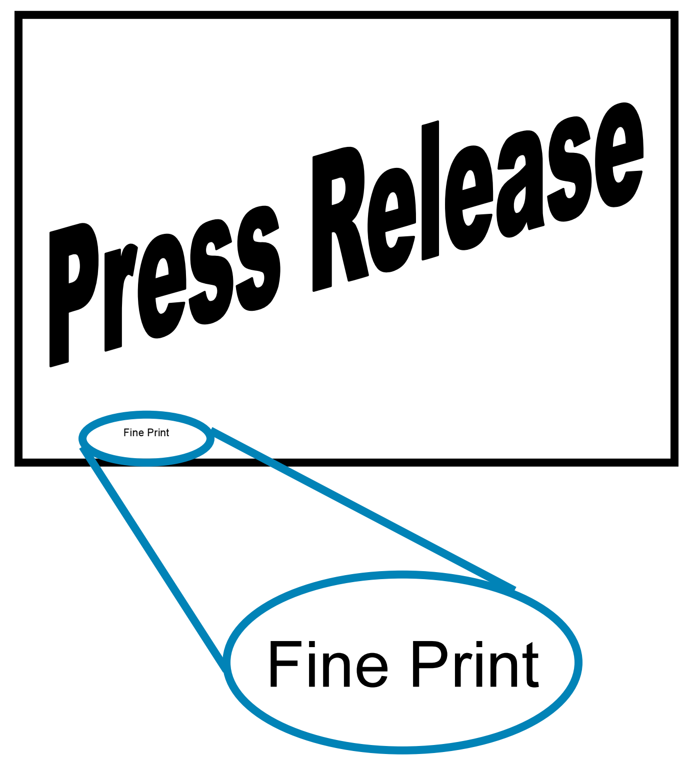
2006-02-06

Alain Durand
Advanced Engineering
Director – IPv6 Architect

Strategic Perspectives

Leadership:

- Innovative services
- Competitiveness
- Marketing



Transition mechanisms

Co-existence between IPv6 and IPv4

- **Three main categories:**
  - **Dual stack – IPv4 and IPv6 coexist in the same device**
  - **Tunelling – configured or automatic tunnels – IPv6 as IPv4 packet payload and vice versa**
  - **Protocol Translation – enables IPv6-only device to communicate with an IPv4-only device**

Dual stacks for IPv6 deployment

- IP capable device supporting simultaneously both IPv4 and IPv6
- Dual-stack routers and application servers
- **IPv4 - IPv6 transition:**

  1. **Replace all IPv4-only devices with dual stack devices**
  2. **Once all devices support both protocols – introduce IPv6-only devices – BUT…..dual stack device still require IPv4 address**

Tunnels for IPv6 Deployment

- Tunneling is encapsulating the IPv6 packet into an IPv4 packet and vice versa

  Host to Router, Router to Router
  Router to Host, Host to Host

- Manually configured tunnels – endpoints are static

  Manual Tunnel (RFC 2893)

  IPv6 over GRE (RFC 2473)

- Semi-automated tunnels

  Tunnel broker (RFC 3053)dedicated server for tunnel config

- Automatic tunnels

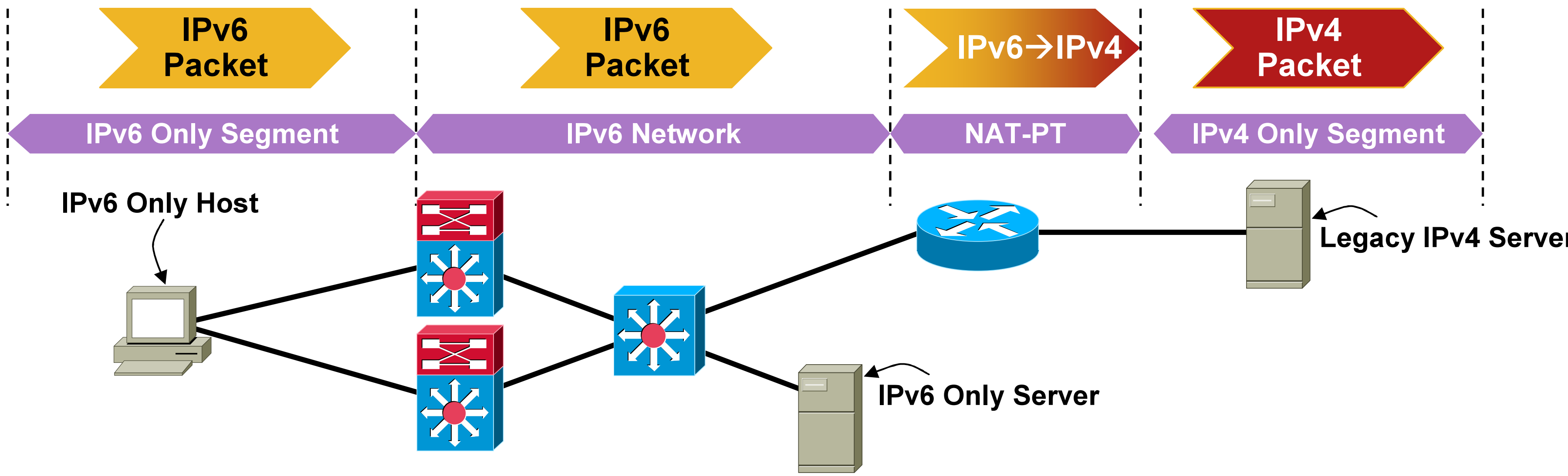
  6to4 (RFC 3056), DSTM (IPv4overIPv6)

  ISATAP (Intra-site Automatic Tunnel Addressing Protocol)

Protocol Translation – NAT PT

- Translation one IP version to another IP version
- NAT PT is NOT transparent – problems with SIP, IPSec
- NAT PT obstructs - ability to perform global addressing, always-on systems (SIP based), p2p networks, push services
- NAT PT - **Deprecated in RFC4966** due to multiple issues
- Security issues – NAT PT does not hide internal network
- For web browsing – **IPv6-to-IPv4 HTTP proxy** – dual-stack Proxy GW is making translation between IPv6 host and IPv4 web server acceseed via IPv4 Internet – HTTP port 80 (scalability issue)

NAT-PT

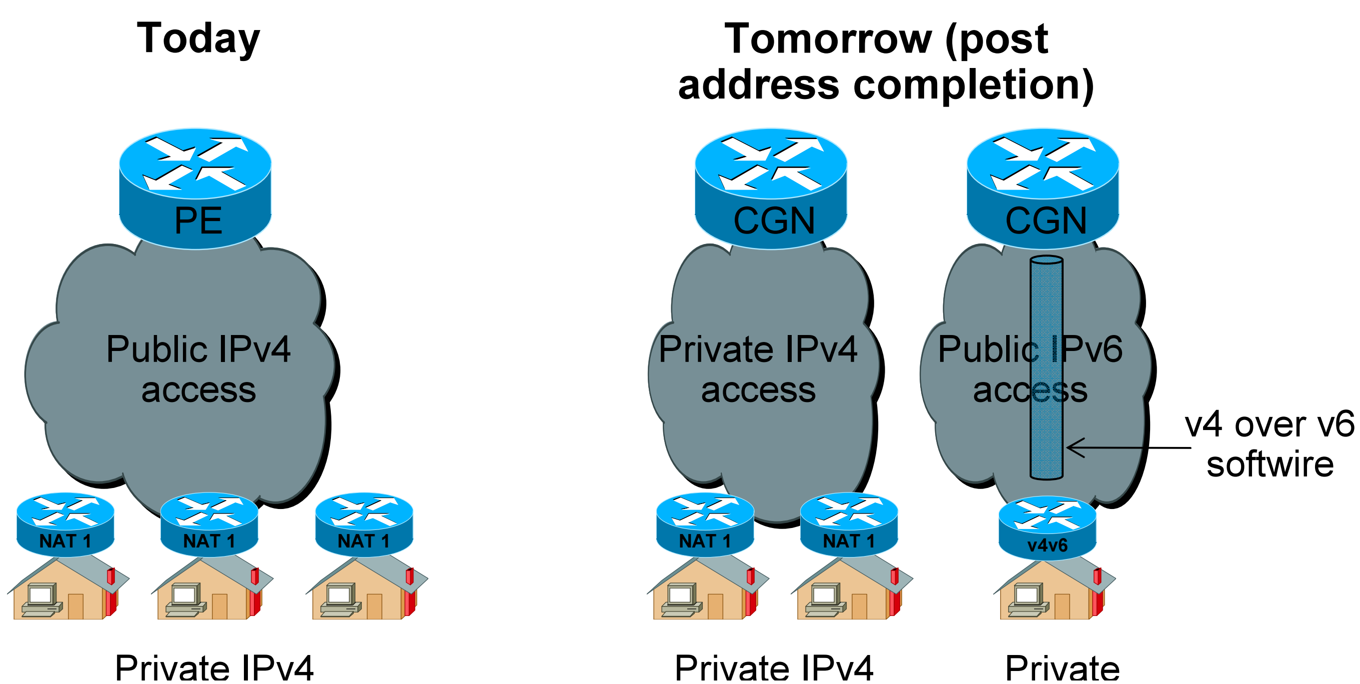


- Network Address Translation – Protocol Translation
  - RFC 2766
  - RFC 4966 obsoletes RFC 2766 – outlines NAT-PT problems
  - NAT-PT is being moved to experimental
- Allows native IPv6 ←→ IPv4 communication
  - Host to Host, Application to Application
  - NAT-PT front ends IPv4 only server
- Place NAT-PT box as close to IPv4 only server as possible
- Be very aware of performance and manageability issues

Delaying or assisting the IPv6 transition

Carrier Grade NAT (CGN)

- What is CGN? **Gigantic NAT** needing O(10G) performance, 20M sessions, 200K IP addresses - runs on CRS-1 Service PLIMs
- NAT private-to-public translation function previously performed at the HGW for O(# of subscribers in home) is pushed upstream, at SP edge, for O(# of total subscribers in the access network)



Softwires

- Standardization of discovery, control and encapsulation methods for connecting IPv4 networks across IPv6 networks and IPv6 networks across IPv4 networks
- Softwire: A "tunnel" that is created on the basis of a control protocol setup between endpoints with a shared point-to-point or multipoint-to-point state

  Softwire Concentrator (SC) - The node terminating the softwire in the service provider network

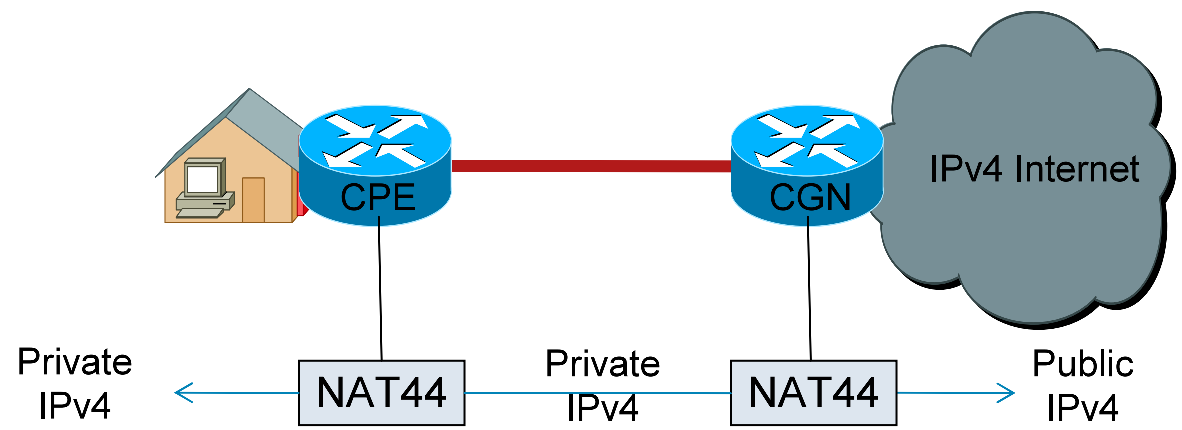
  Softwire Initiator (SI) - The node initiating the softwire within the customer network

  Address Family Border Router (AFBR) - The router that interconnects two networks that use different address families

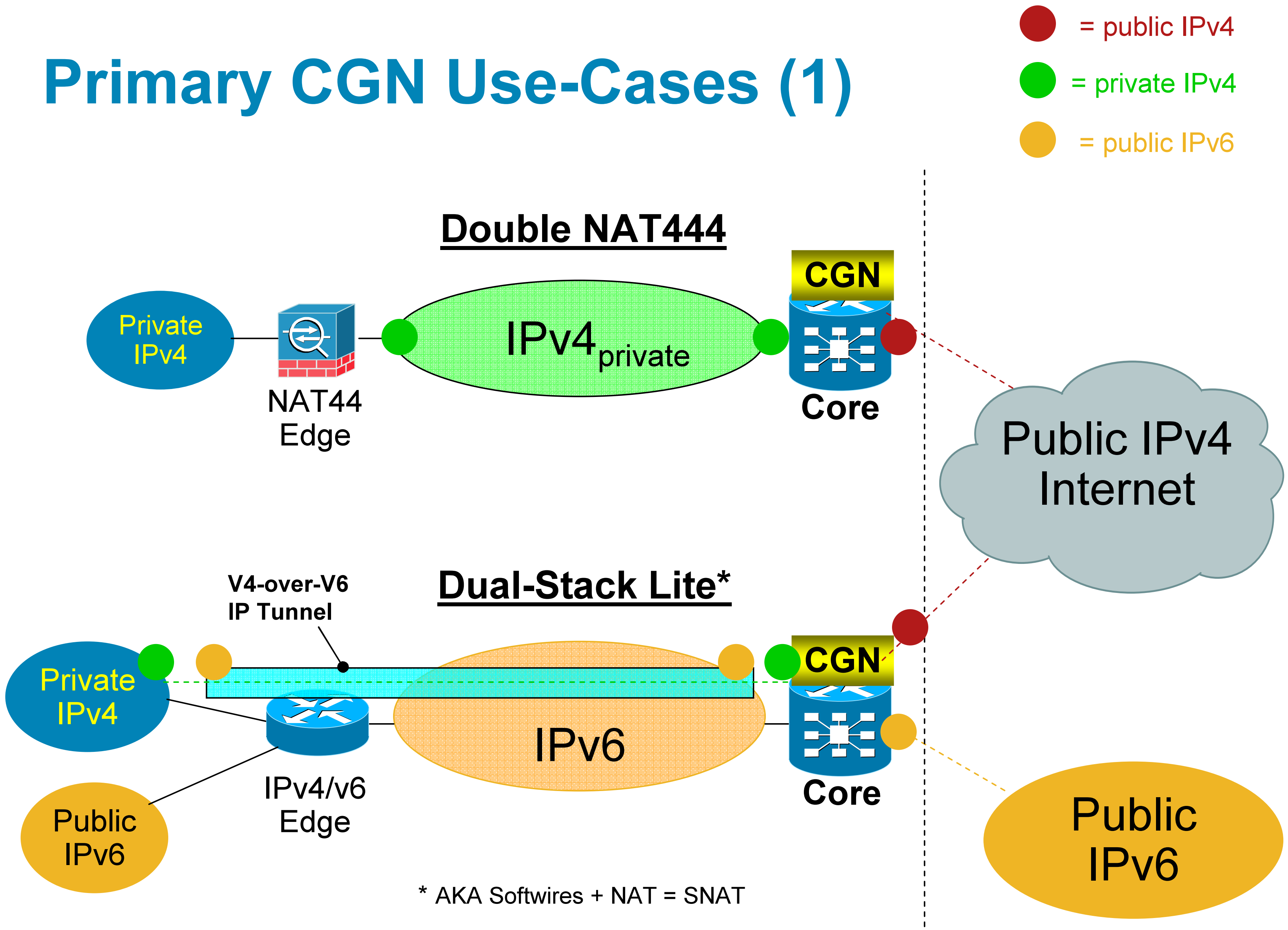
CGN Solution example

- CGN is located on the PE & performing private IPv4-to-public IPv4 translation
- The access network is using a private IPv4 address space & that the CPE is required to perform a private-to-private IPv4 NAT translation

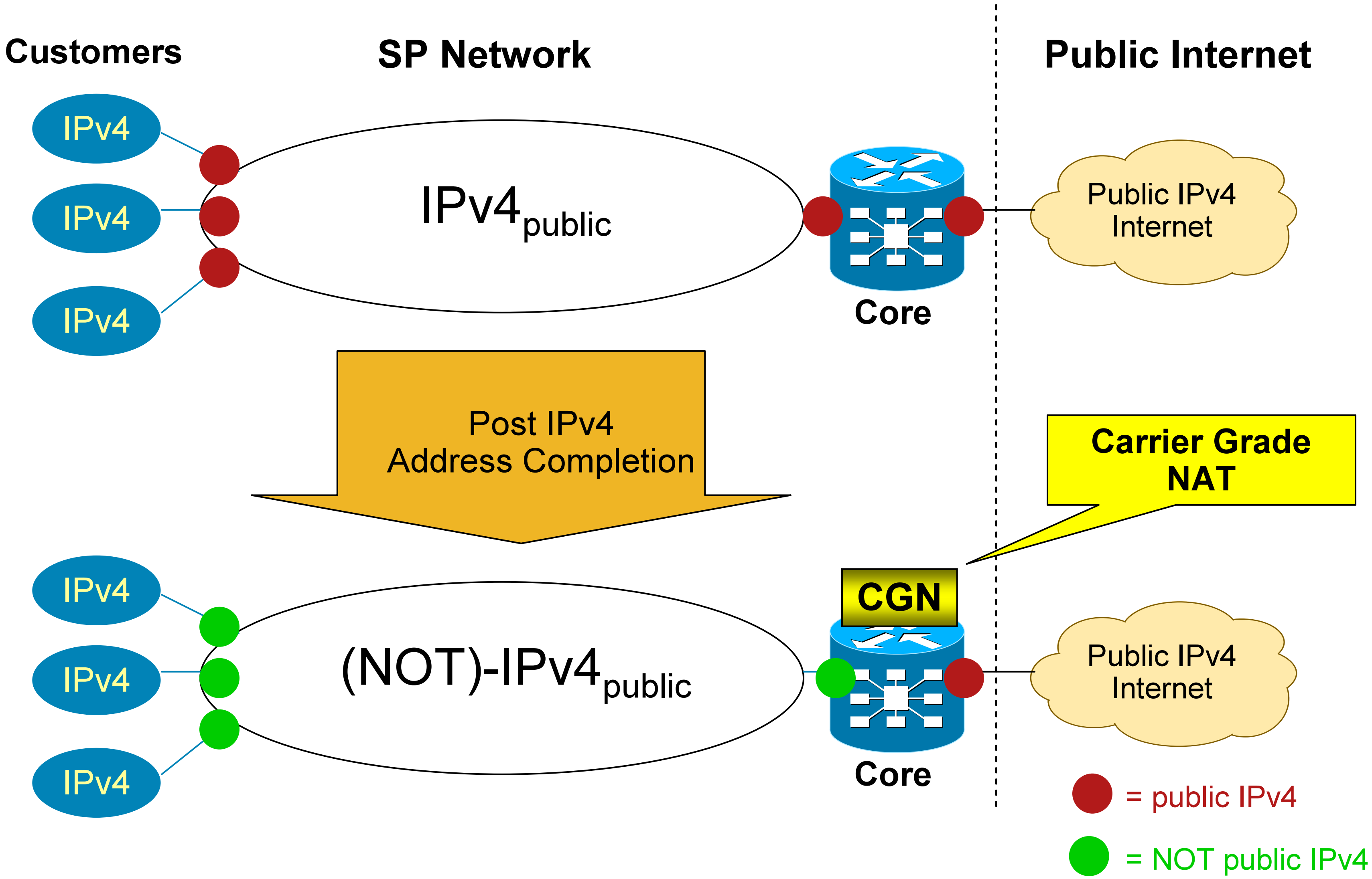
It is also possible for a device upstream from the CPE (such as an access router or switch) to perform the NAT44 function.



Primary CGN Use-Cases (1)



A Strategy for Dealing with the IPv4 Address Completion Problem



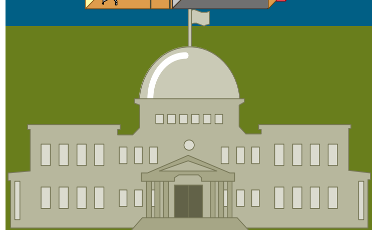
Common Deployment Scenarios

	Environment	Scenario	Cisco IOS support
Core	Native IP – Core is IPv6 aware	Dual Stack	Yes
	MPLS – Core is IPv6 unaware	6PE/6VPE	Yes
WAN	IPv6 services on L3 Managed Services	Dual Stack	Yes
	IPv6 over L2 services	Dual Stack	Yes
Campus	L3 infrastructure – IPv6 capable	Dual Stack	Yes
	L3 infrastructure – not IPv6 capable, or sparse IPv6 hosts population	ISATAP	Yes
Less optimum	IPv6 over IPv4 tunnels	Scalability & Management	Yes
	Translation (NAT-PT)	Scalability, [illegible]	Yes

Who is Deploying IPv6 Today?

Service Providers

- Carrier – Transit services
http://www.sixxs.net/faq/connectivity/?faq=ipv6transit
- Internet eXchange Point (IX) – NRN & ISP
http://www.bgp4.as/internet-exchanges
- Broadband SP
Japan - http://www.ipv6style.jp/en/statistics/services/index.shtml
Europe - http://www.sixxs.net/faq/connectivity/?faq=native
- Mobile SP – R&D and Trials for 3G/4G services



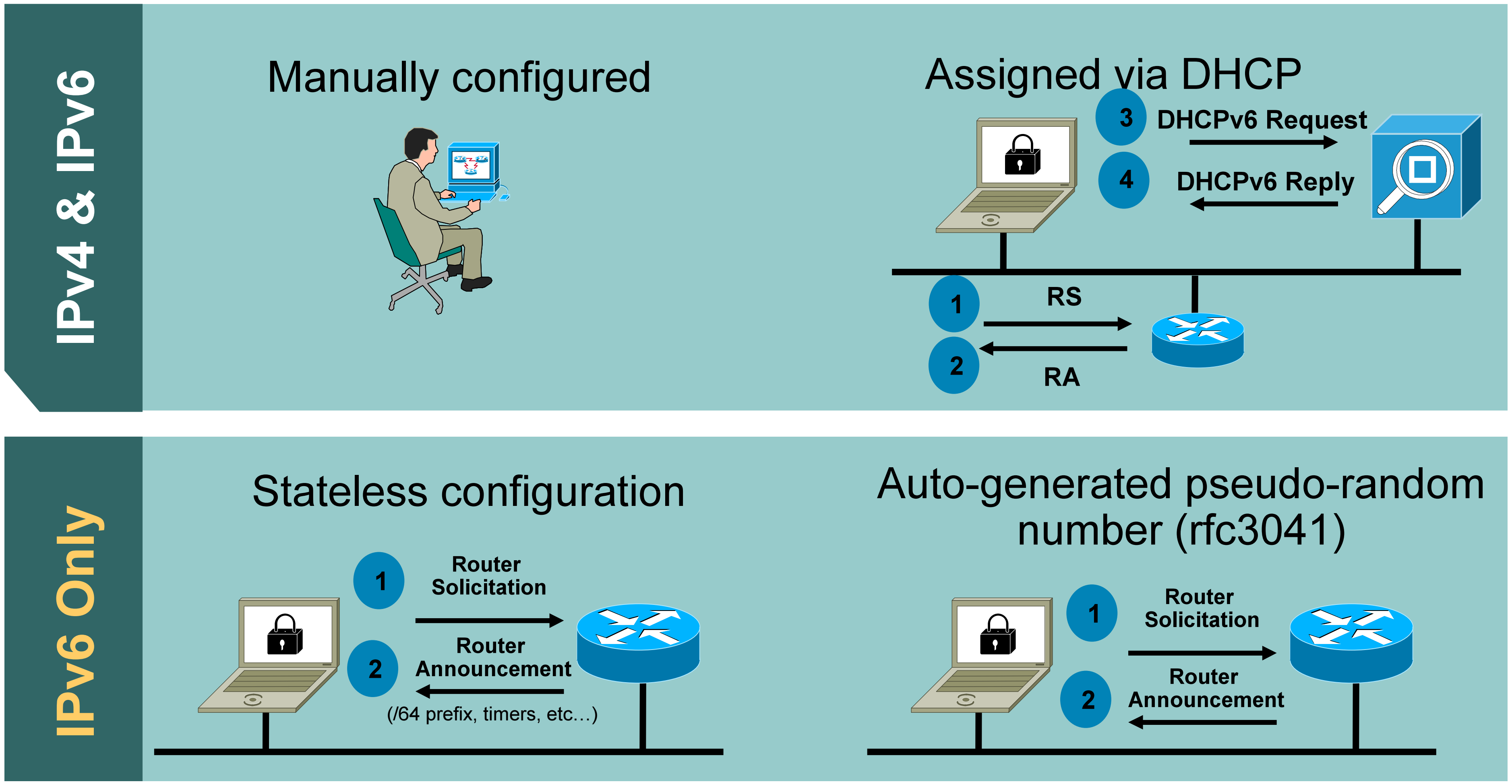
Enterprises

- NRN, Universities, Schools, Research Labs
- Government agencies, eg. US Federal mandate, Eurocontrol, Military,…
- IT Vendors and System Integrators, eg. Cisco, Bechtel, Microsoft, Command Information,…
- IT department deploying Vista and Server 2008

IPv6 for Service Providers

IPv6 Address Assignment

- **Lowest-order 64-bit field of unicast addresses may be assigned in several different ways**



Interface Level – Address Assignment

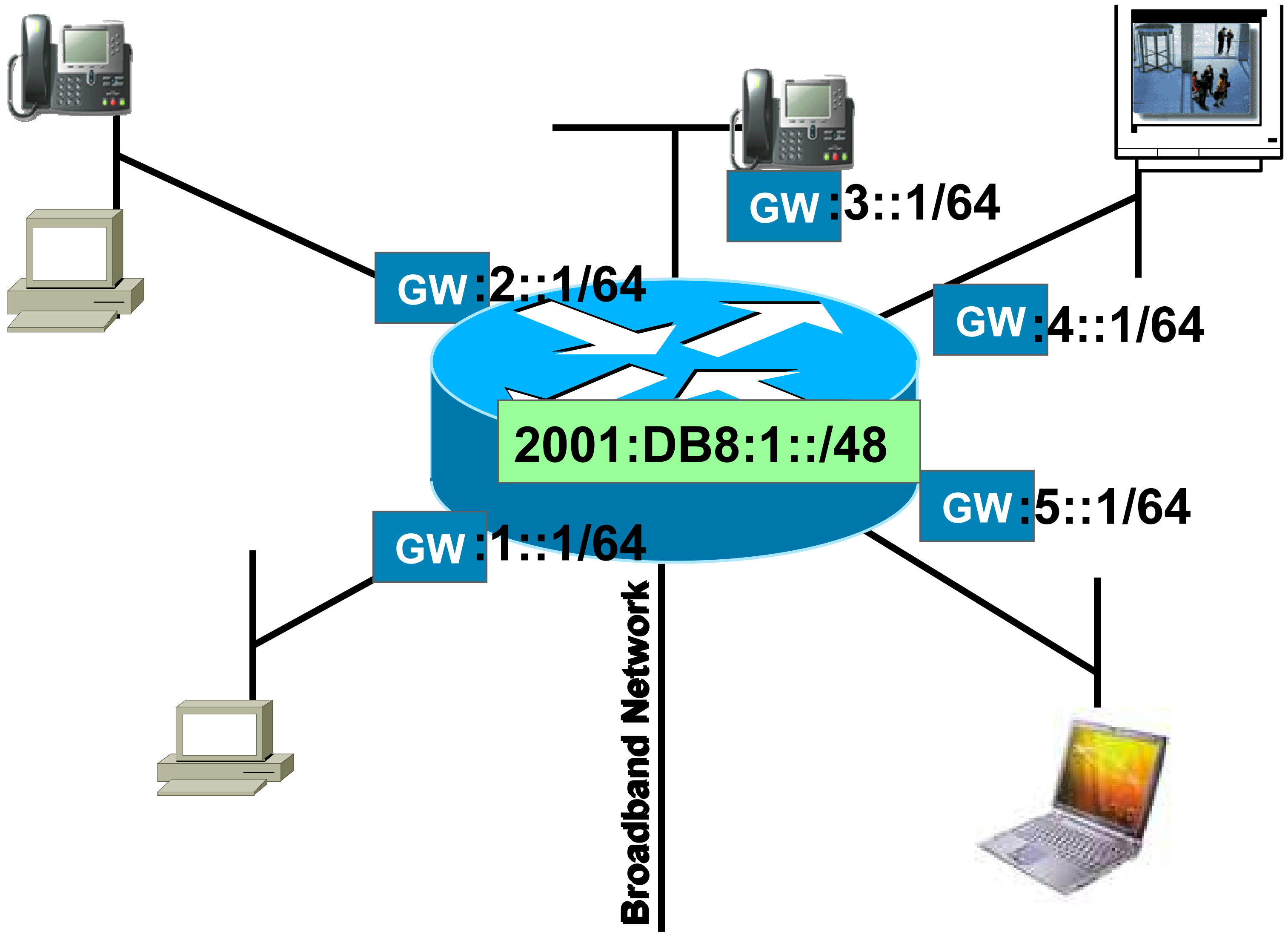
- DHCPv6
  - Same as in IPv4
- Automatic EUI-64
  - Stateless Address Autoconfiguration
- Privacy Extensions (RFC3041)
  - Challenging for network management
  - May not have reverse DNS entries
- Cryptographically Generated IPv6 Addresses
  - Regenerate CGA if host compromised
  - Needs support tools for network management
- Manual/Dynamic Assignment Option
  - Suitable and recommended for network elements and fixed resources (servers for example) but not for hosts

Provisioning Considerations

Different provisioning mechanisms and tools can be leveraged such as:

- Stateless Address Autoconfiguration (SLAAC)
- Stateless/Statefull DHCP
- General Prefix
- DHCP-PD (with gateway as server), DHCP-PD (centralized server)
- RADIUS (CISCO VSA, RFC3162)
- Manual/Static Configuration

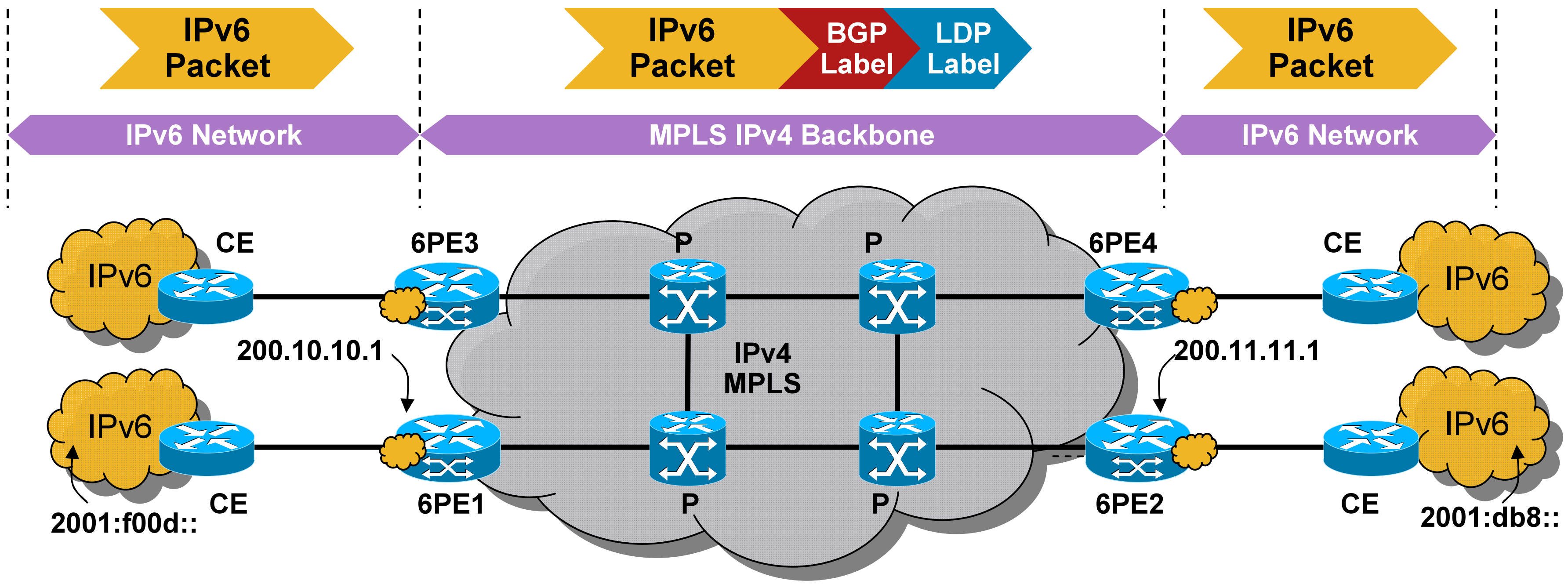
DHCP- Prefix Delegation (Quick Review)



IPv6 over MPLS

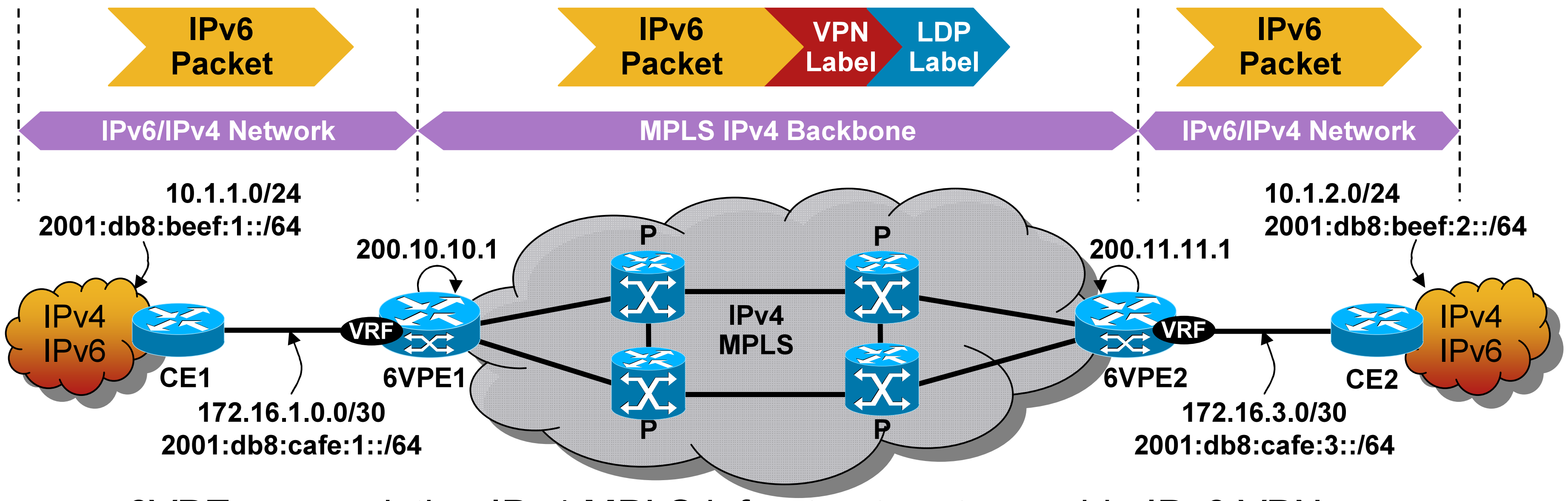
- IPv6 over MPLS Pseudowires
  - Transparent to service provider
- IPv6 over IPv4 tunnels over MPLS (Manual Tunnels)
  - PE must be IPv6 aware, core remains IPv4
- IPv6 Transit using MPLS 6PE
  - PE must be IPv6 aware, core remains IPv4
- IPv6 VPN using MPLS 6VPE
  - PE provide VPN services for IPv6, core remains IPv4
- No LDPv6 available as yet
  - Core control plane must be MPLS+LDP using IPv4 IGP
- Previous solutions discussed can also work over MPLS
  - ISATAP, Manual Tunnels, GRE, 6 to 4

IPv6 Transit using MPLS 6PE (RFC 4798)



- 6PEs must support dual stack IPv4+IPv6 (acts as normal IPv4 PE)
- IPv6 packets transported from 6PE to 6PE over Label Switch Path
- IPv6 addresses exist in global table of PE routers only – one global VPN
  - IPv6 addresses exchanged between 6PE using MP-BGP session
- Core uses IPv4 control plane (LDPv4, TEv4, IGPv4, MP-BGP)
- Benefits from MPLS features such as FRR, TE

IPv6 VPN 6VPE (RFC 4659)



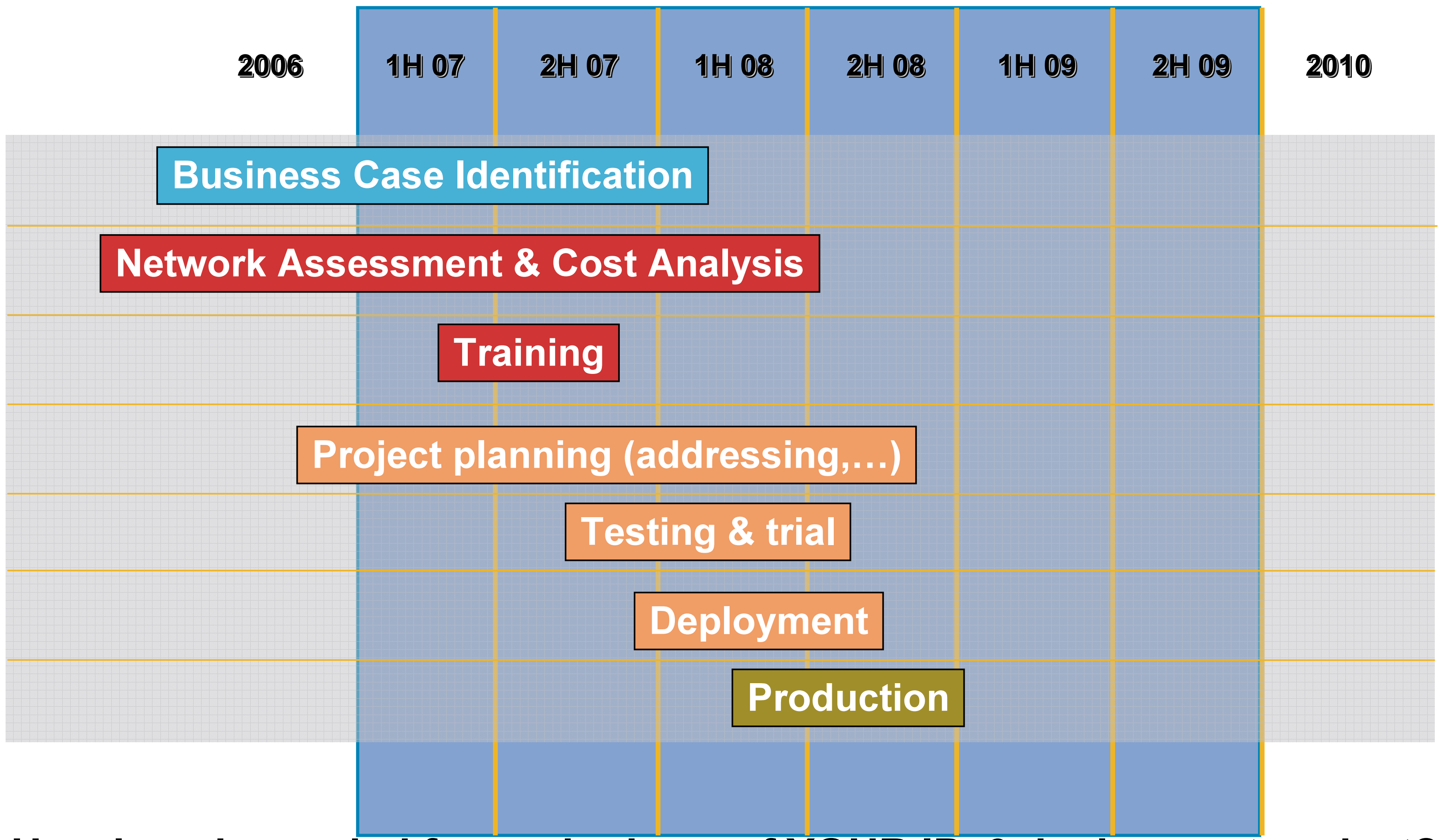
- 6VPE uses existing IPv4 MPLS infrastructure to provide IPv6 VPN
  - Core uses IPv4 control plane (LDPv4, TEv4, IGPv4)
- PEs must support dual stack IPv4+IPv6
- Offers same architectural features as MPLS-VPN for IPv4
  - RTs, VRFs, RDs are appended to IPv6 to form VPNv6 address
  - MP-BGP distributed both VPN address families
  - BGP NH uses IPv4 to IPv6 mapped address format ::ffff:A.B.C.D
- VRF can contain both VPNv4 and VPNv6 routes

IPv6 over DMVPN

- Connects private IPv6 islands across public IPv4 cloud
- **IPv6 services over IPv4 Internet**
- Public IPv4 network treated as NBMA network
  - Static hub and spoke topology
  - Dynamic spoke to spoke topology
- Supports dynamic unicast and multicast routing
- Uses several established protocols
  - Multipoint GRE (mGRE) tunnels
    - Single mGRE interface supports all spokes (many logical tunnels)
  - Next Hop Resolution Protocol (NHRP)
    - Resolves Private IPv6 address to Public IPv4 NBMA address

Use cases

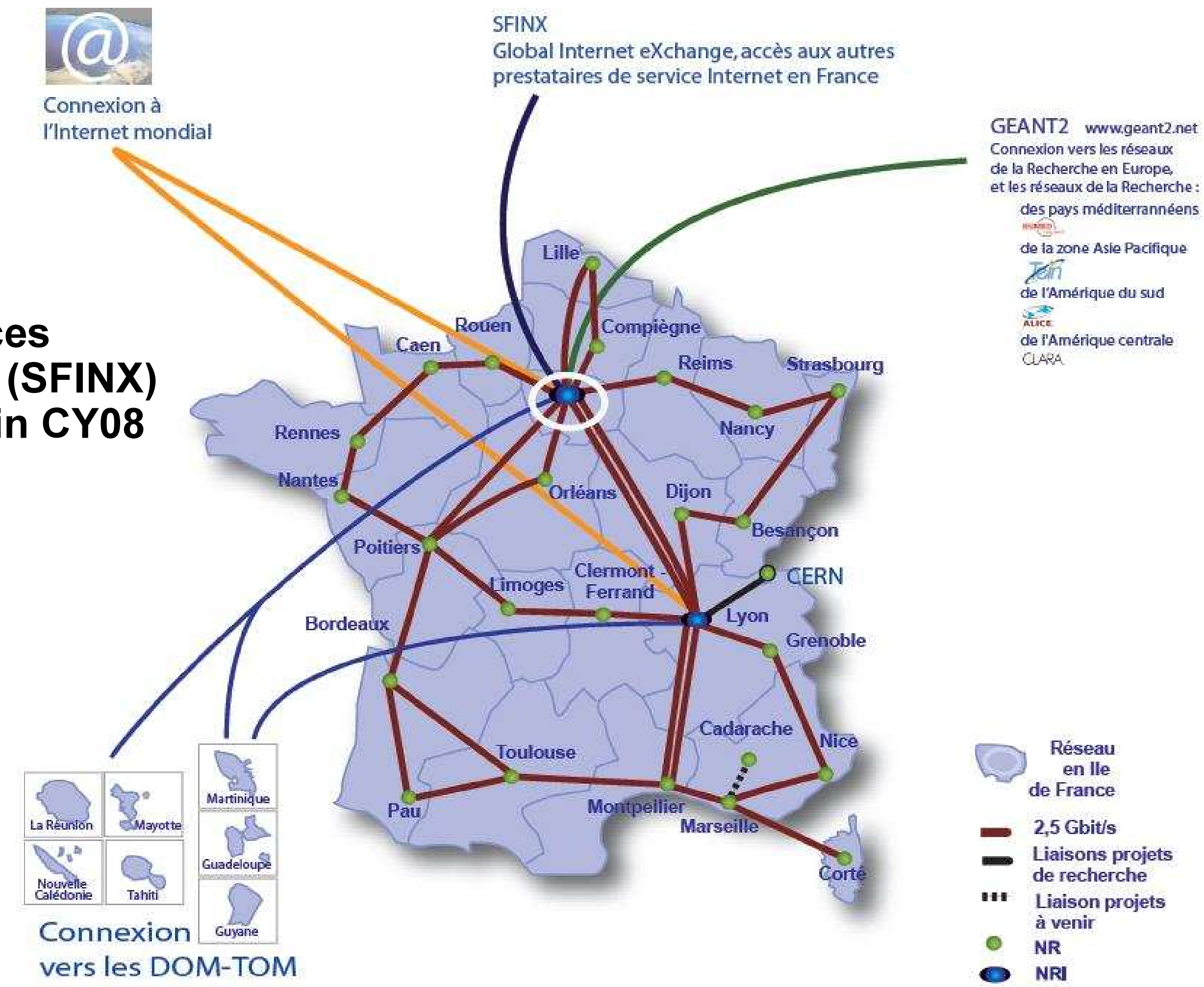
IPv6 – Planning Steps



How long is needed for each phase of YOUR IPv6 deployment project?

Dual Stack IPv4-IPv6 in production

RENATER (French NRN)
• IPv6 as production services since 5 years, including IX (SFINX)
• New phase (RENATER5) in CY08
  • CRS-1
  • Cisco 12000 series
  • Cisco 7600 series



http://supervision.ipv6.renater.fr/Portail/IPv6WP/indexWP_renater.php

Bechtel Well Positioned to Serve Customers by Using Microsoft and Cisco IPv6 Solution

> "Turning on IPv6 is just the start. The longer-term benefit will be looking at Software as a Service in conjunction with IPv6 and peer-to-peer discovery. Those capabilities will enable Bechtel to be more effective and efficient."
>
> *Fred Wettling,*
> *Bechtel Fellow and Technology Strategy Manager,*
> *Bechtel*

onsumed less
udget, and the
part of the
These costs

Software and Services	Hardware	Partners	
• Windows Vista • Microsoft Server Product Portfolio • Windows Server 2008 • Windows Server 2003 Enterprise Edition • Windows XP • Services • Microsoft Services	• Cisco Catalyst 6500 Series Switches, Cisco Catalyst 3500 XL Series Switches, Cisco Integrated Services Routers (ISRs), Cisco PIX firewalls, CiscoWorks LAN Management Solution (LMS) • Dell personal computers, portable computers, and server computers • HP personal computers, portable computers, and server computers	• Cisco	
		• Command Information	
		• Microsoft	

Simplistic View of Comcast IP problem

20 Million video customer

2.5 set-top box per customer

2 IP addresses per set-top box

Total: 100 Millions IP address

And we have not yet talked about High Speed Data
nor Comcast Digital Voice…

Comcast Specific Needs

- The extra large address space is for **managemen**t (a.k.a. control plane) of Cable Modems, eMTA and Set-Top boxes
  - This is not for customer PC-type devices (data plane). This would require a separate allocation.
- This address space is for **internal consumption only**, i.e. it is not seen from outside Comcast.
- Until recently, Comcast was using **Net 10 (RFC1918)** for managing the modems. That space has been **exhausted**.
- Comcast recently was allocated the largest part of Net 73 and is currently renumbering cable modems in that space.
- In the control plane, all devices need to be remotely managed, so NAT(v4-to-v4) isn't going to help …
- **IPv6 was the chosen solution**
  - However, even we are starting now, the move to IPv6 is not going to happen overnight

Comcast IPv6 Strategy

- Plan for IPv6 deployment ***NOW***
- Deploy IPv6 ***initially*** for the ***management*** and operation of the customer devices we manage:
  - DOCSIS CM
  - Set Top boxes, PacketCable MTA,…
- Be ready to offer v6 service to customer as soon as demand picks up.

IPv6 Migration – Guiding Principles

- The migration to IPv6 project has the following principles:
  - Deploying IPv6 must be minimally disruptive to the operations of existing networks and devices
  - IPv6 must be included in the roadmap of next generation equipment and devices
  - Comcast operations, infrastructure and systems must become ready to support IPv6-enabled devices
    - IPv6 will slowly penetrate Comcast other services

IPv6 Deployment: Principles and Approach

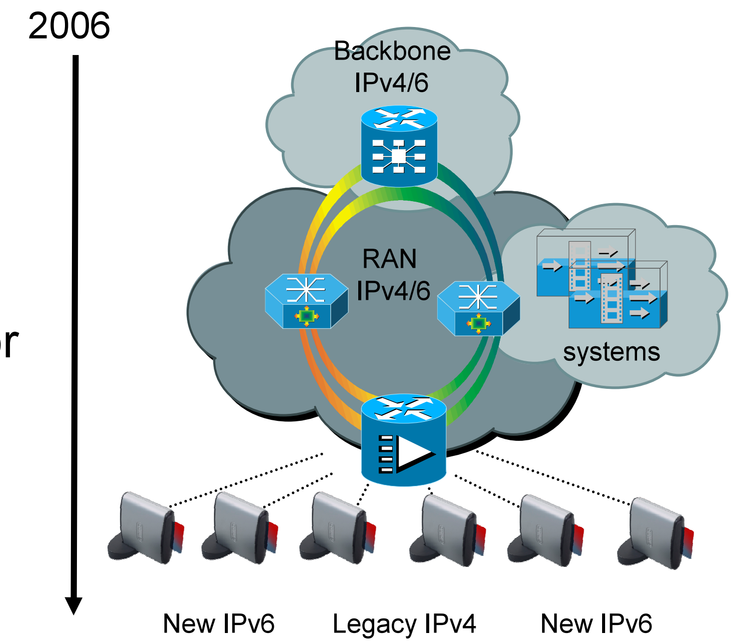
- Primary objective is to deploy IPv6 for the IP address of the CM & STB
- **Architecture**: dual-stack at the core, v6-only at the edges

  Co-existence of dual stack core network (Backbone, RAN, Back Office), and

  IPv6-only at the edge (CM, STB, MTA…) for new devices
- **Deployment approach:**

  From the core to the edges

  This is an incremental deployment
- **Follow same operational model as with IPv4**



Lots of learning & work to go

- IPv6 QoS configuration is not deployed
- Still concerns over addressing (/64 vs. /126 on point-to-points)
- Continuing concerns regarding security policies (ACL processing, etc.)
- Dual vendor CMTS strategy is delaying deployment to edge
- ISIS optimizations under consideration

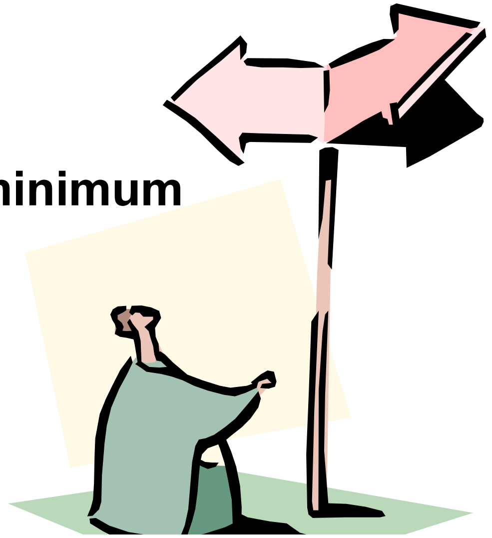
Conclusions

Provider issues as sound bites:

- San Isabel Telecom (US) 4/9/08 - 'Ideal differentiation for small providers; need complete package due to small staff'
- China Netcom (China) 4/16/08 - 'Other vendors are saying to avoid IPv6 due to lack of traffic'
- China Mobile (China) 4/17/08 - 'Case studies as examples? Push-to-talk without nat is goal. CGN for content?'
- Telenor AB (Sweden) 5/12/08 - 'Need production support for mobile devices'
- Globe Telecom (Manila) 5/23/08 - 'How do we start?'
- NTT NGN (Japan) 6/9/08 - 'CGN is an unfortunate stepping stone'
- NTT Communications (Japan) 7/28/08 - 'CGN will be painful to both the provider and customer'
- CERNET2 (China) 7/30/08 - 'Created IVI for legacy clients to access IPv6-only servers; expects IPv6-only will reduce costs'
- T-Mobile (US) 8/5/08 - 'We have to do it, but what about the content providers?'
- Telstra (Australia) 8/13/08 - 'CGN is an undesirable but unavoidable step; initially OSS issues, then hard to remove'
- Verizon Wireless (US) 8/14/08 - 'We need the entire team onboard'
- Internet NZ (New Zealand) 8/27/08 - 'Where is the case study to follow?'
- Telstra (Australia) 8/28/08 - 'Need a comprehensive plan, though CPE is not a concern ... yet'
- Chunghwa (Taiwan) 9/1/08 - 'Tunnel broker service for access network traversal. Need seamless provisioning'
- Hurricane Electric (US) 9/1/08 - 'When will Linksys support technologies for carrier access?'
- Manetic (Macau) 9/2/08 - 'Without content, what is the business case?'
- GoDaddy (US) 9/9/08 - 'Expect to deploy end-to-end by end of 08 ... but where is the ACE?'
- Verizon Wireless (US) 9/16/08 - 'LTE will be IPv6-only; need security and CGN'
- Chunghwa (Taiwan) 10/16/08 - 'Strategy for access provisioning and CPE?'
- Cogent (US) 10/16/08 - 'Can't afford ½ performance if traffic suddenly shifted, but will deploy by end of 2009'
- AT&T (US) 10/16/08 - 'Business continuity; Service continuity; Minimal customer impact'
- TANET /TWAREN (Taiwan) 10/21/08 - 'We built it, where is the traffic?'

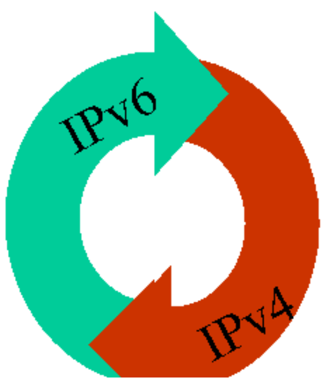
How Do we Get There from Here?

- IPv6 integration must not affect the integrity of existing business operations on the IPv4 network
  - Education & Careful Planning are crucial
- Hardware Support – standard HW lifecycle process
- Software and services - RFI's & RFP's ask vendors for IPv6
- IP Addressing
  - IPv6 prefix subscription from a RIR (or ISP)
  - Definition of addressing scheme per geography
  - Policy for address auto-configuration
- Routing Protocols
  - Choice as on IPv4 – keeping the learning curve as minimum
- Management & Security
  - Monitoring of IPv6 traffic
- Infrastructure services
  - Still requires development work to offer IPv4 parity

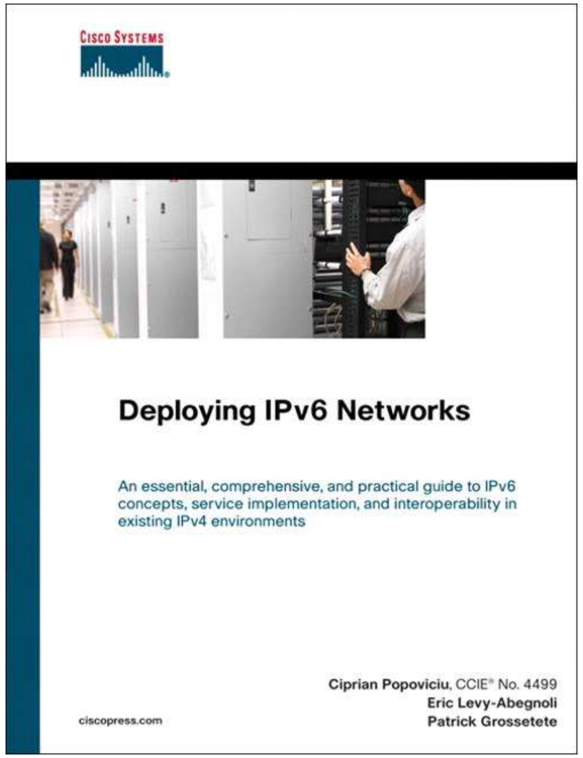


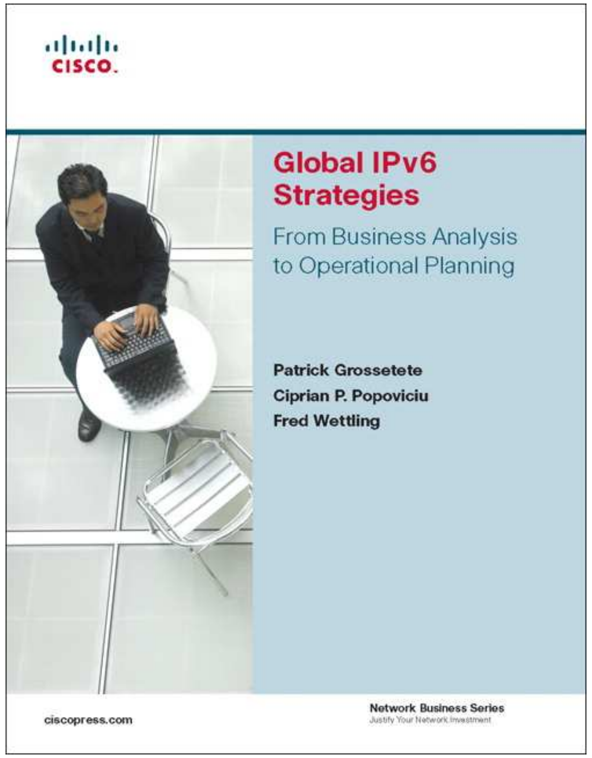
Summary

- **CRITICAL QUESTION: Transition or NOT?!**
- **Facts:**
- OPEX can be higher during IPv4-IPv6 transition period
- Risk of service interruption
- Protocol is evolving – potential issues
- IPv4 address managing becomes more complex every day
- How to make profit with IPv6
- **…**
- **The right way:**
- **Develop IPv6 transition plan** – phased approach
- **Make equipment inventory**
- **Invest in trainings**
- **IPv6 is standard part of IP**
-



References





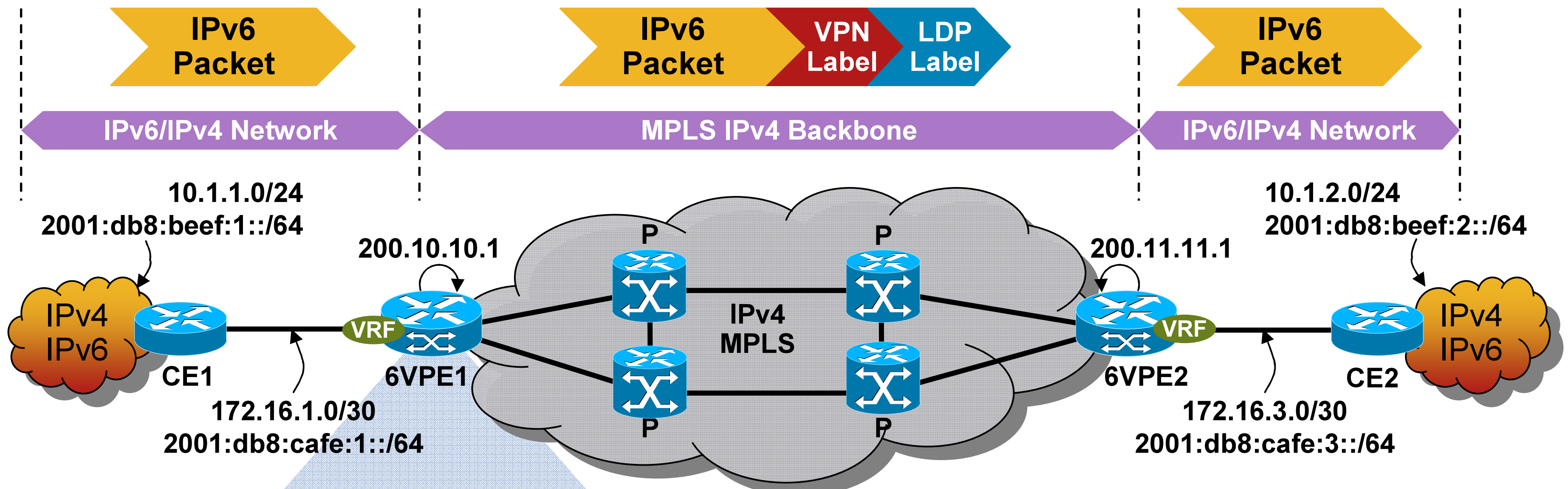
- Networkers IPv6 Sessions
- "IPv6 Transition Guidance", Federal CIO Council Architecture and Infrastructure Committee, http://www.cio.gov/documents/IPv6_Transition_Guidance.doc
- "The choice: IPv4 exhaustion or transition to IPv6", Jordi Palet, http://www.ipv6tf.org/pdf/the_choice_ipv4_exhaustion_or_transition_to_ipv6_v4.4.pdf

Q and A

CISCO

Backup Slides

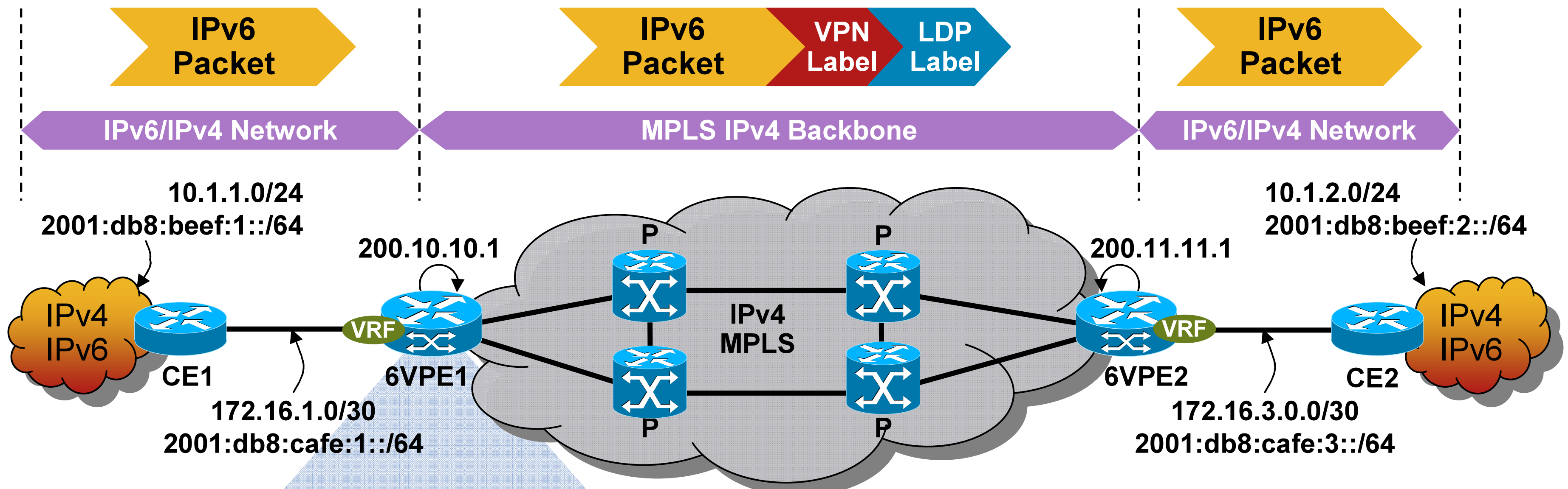
6VPE1 General Configuration




```
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
 ip address 200.10.10.1  255.255.255.255
!
interface Ethernet0/0
 Description Link to CE1
 vrf forwarding GREEN
 ip address 172.16.1.2 255.255.255.0
 ipv6 address 2001:db8:cafe:1::2/64
```

```
!
interface Ethernet2/0
 description Link to Core Network
 ip address 192.168.1.1 255.255.255.252
 mpls ip
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 passive-interface Loopback0
 network 192.168.1.0 0.0.0.255 area 0
```

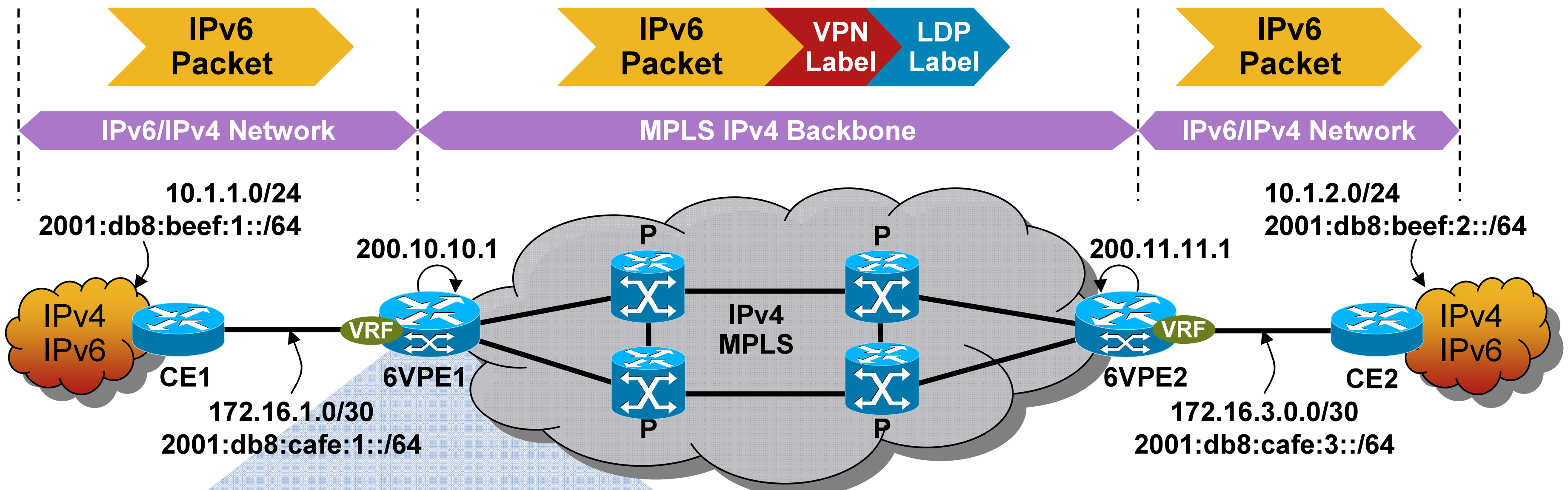
6VPE1 BGP Configuration




```
router bgp 100
 neighbor 200.11.11.1 remote-as 100
 neighbor 200.11.11.1 update-source lo0
 !
 address-family ipv4 ← Internet Routes
 neighbor 200.11.11.1 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4 ← To 6VPE2
 neighbor 200.11.11.1 activate
 neighbor 200.11.11.1 send-community ext
 exit-address-family
```

```
address-family vpnv6 ← To 6VPE2
neighbor 200.11.11.1 activate
neighbor 200.11.11.1 send-community ext
exit-address-family
!
address-family ipv4 vrf GREEN ← To CE1
redistribute connected
neighbor 172.16.1.1 remote-as 500
neighbor 172.16.1.1 activate
exit-address-family
!
address-family ipv6 vrf GREEN ← To CE1
neighbor 2001:db8:cafe:1::1 remote-as 500
neighbor 2001:db8:cafe:1::1 activate
exit-address-family
```

6VPE1 LFIB




```
6VPE1#show mpls forwarding
Local  Outgoing    Prefix            Bytes Label   Outgoing   Next Hop
Label  Label or VC or Tunnel Id      Switched      interface
16     Pop Label   192.168.1.4/30    0             Et2/0      192.168.1.2
17     16          192.168.1.8/30    0             Et2/0      192.168.1.2
18     Pop Label   200.12.12.1/32    0             Et2/0      192.168.1.2
19     18          200.13.13.1/32    0             Et2/0      192.168.1.2
20     19          200.11.11.1/32    0             Et2/0      192.168.1.2
21     No Label    10.1.1.0/24[V]    0             Et0/0      172.16.1.1
22     Aggregate   172.16.1.0/24[V]  570           GREEN
25     No Label    2001:db8:beef:1::/64[V]   \
                                     570           Et0/0      FE80::A8BB:CCFF:FE01:F400
26     Aggregate   2001:db8:cafe:1::/64[V]   \
                                     35456         GREEN
```