



IPv6 for Content Providers

Joe Wang, jiwang@cisco.com

CSE, APAC

The text "IPv6" is rendered in a large, 3D, green, glossy font. A bright white starburst effect emanates from the top right corner of the '6', with multiple lines radiating outwards.

Agenda

- IPv6 Adoptions Status
- IPv6 Transition Architecture
- IPv6 Deployment in DC

IPv6 Adoption Accelerating Worldwide

IPv4 Address Exhaustion

Most regions out by 2013



IPv6-Capable Devices

8 billion by 2016



80%
of largest
core networks
are
IPv6-ready

IPv6 Users

Steady growth
around the globe*



*3 million+ in US
as of August, 2012

IPv6 Content

40% of
Internet content*



*US and Europe
as of August, 2012

<http://6lab.cisco.com/stats>

IPv4 Milestones



IPv4 Address Exhaustion – IANA –
3 Feb 2011



IPv4 Address Exhaustion – Asia –
15 April 2011

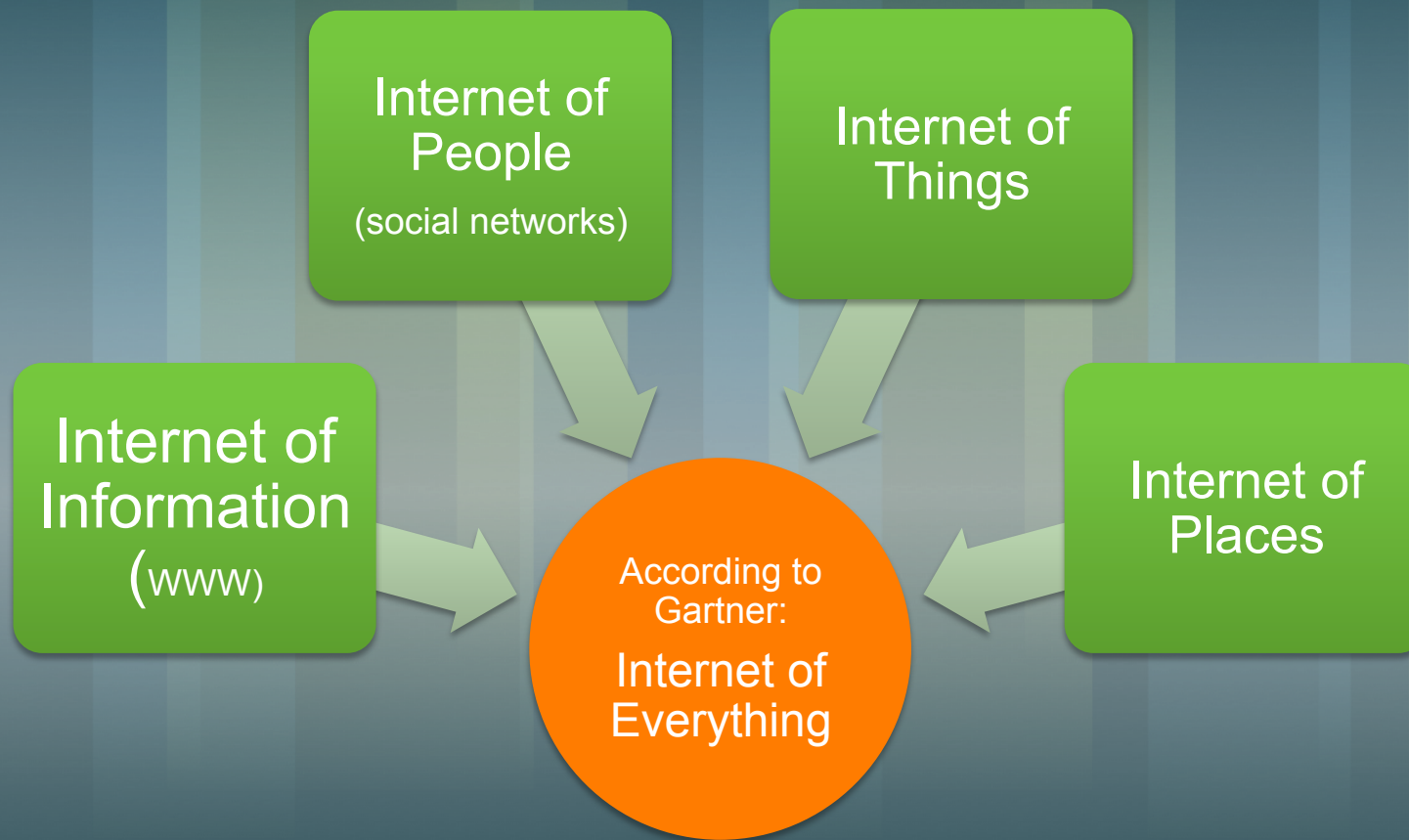


IPv4 Address Exhaustion – EMEA –
1 Sept 2012



RIR IPv4 Address Exhaustion -
Global – 2014

Internet of Things or Internet of Everything?



With trillions of connections, the IoT makes the network more important than ever.

World IPv6 Launch, June 6th 2012

<http://www.worldipv6launch.org/>



THIS TIME IT IS FOR REAL

Major Internet service providers (ISPs), home networking equipment manufacturers, and web companies around the world are [coming together to permanently enable IPv6 for their products and services](#) by 6 June 2012.

**AKAMAI
COMCAST
FREE TELECOM
KDDI
TIME WARNER CABLE**

**AT&T
D-LINK
GOOGLE
LIMELIGHT
XS4ALL**

**CISCO
FACEBOOK
INTERNODE
MICROSOFT BING
YAHOO!**

**DO YOUR PART
JOIN THE LAUNCH!**

We welcome web companies, ISPs, and home router vendors to [join the cause](#) and [spread the word](#) and [follow along](#).

Organisations need an IPv6 Strategy if...

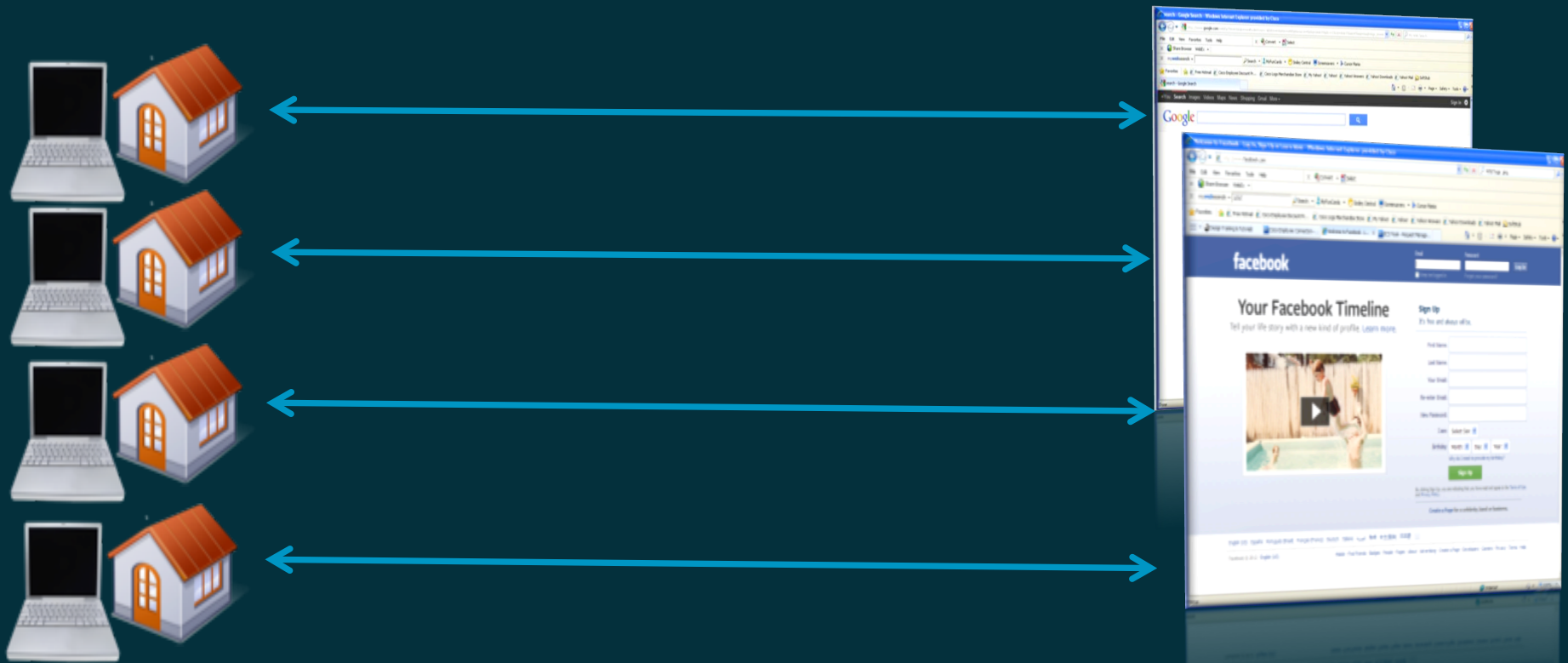
- They serve **content** to the internet
- Their end customers **fill out their tax forms/pay their bills** on the internet
- They offer **consumer banking** and financial services over the Internet
- They provide **VPN** access for home working for their employees
- They use links **internet links as a backup** strategy for “main” links
- They want to communicate with areas where IPv4 addresses are limited – China/India/Japan etc



“We use NAT...”

- Assumes you NAT to a Global Address. *What global address?*
- NAT complicates network architecture. Troubleshooting, downtime, expense
- NAT has slowed down growth of transparent applications (need ALG's)
 - INHIBITS GROWTH - scalability issues with TURN, ICE and STUN
 - ADDS TO COST - Problem typically ends up with the applications team
- No easy way to maintain states of NAT in case of node failures
- NAT breaks security (IPSec/Authentication Header etc)
- NAT complicates mergers, double NAT-ing is needed for devices to communicate with each other
- Large scale NAT at the Carrier level (e.g. NAT64/NAT464/NAT444) is NEVER going to be a permanent solution – speed/complexity/cost

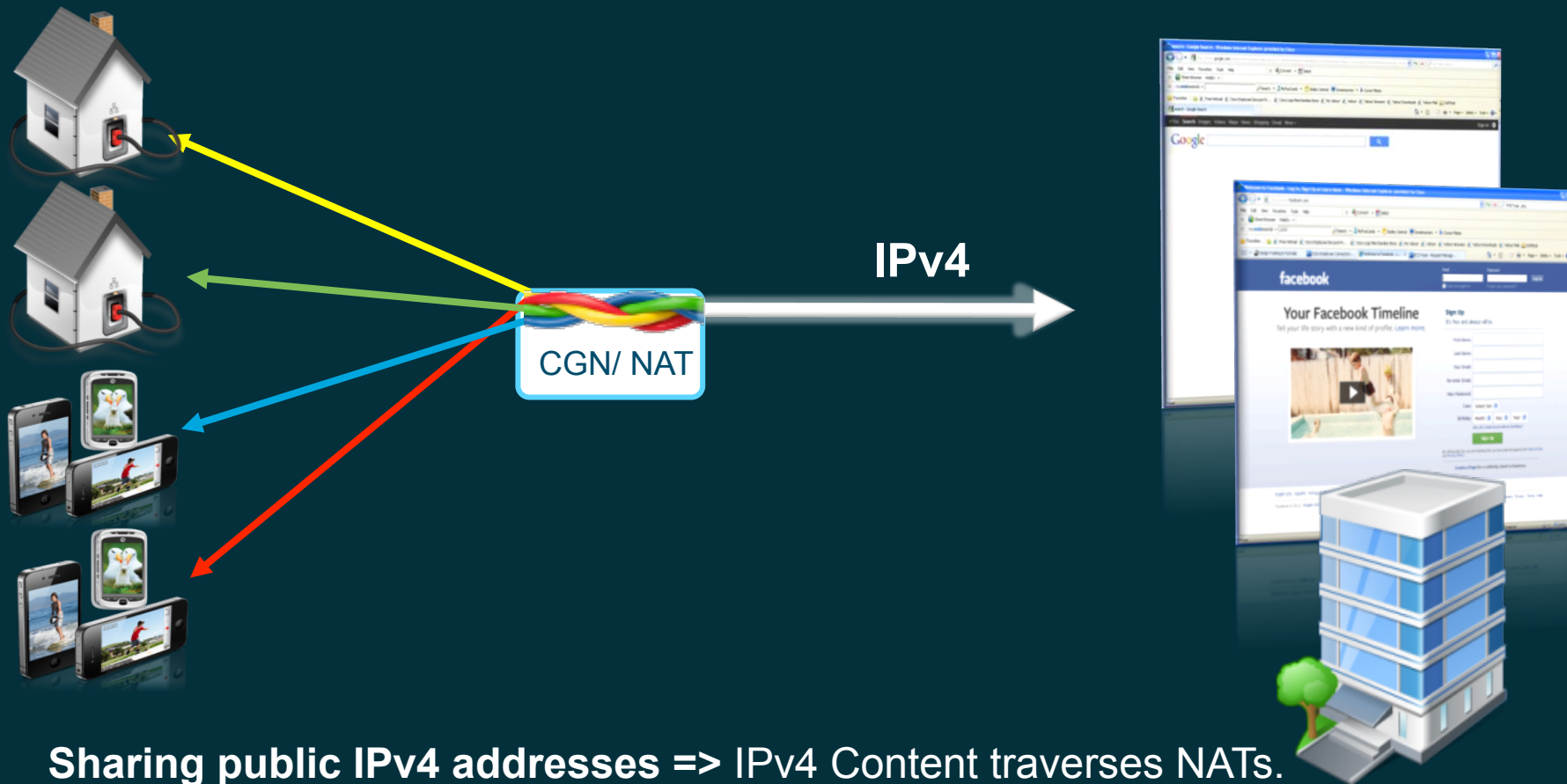
Internet evolution: IPv4 end to end model



Public addresses
End-to-end – transparent TCP session



Internet evolution: sharing IP address



Sharing public IPv4 addresses => IPv4 Content traverses NATs.

Challenges: Transparency to applications, location, security
CGN creates State (and logging) for every session

IPv6 – “Full Spectrum” Internet



Lower cost and complexity



Enable faster downloads



Improve user experience



Streamline security



IPv4 will deteriorate over time



Monetize with IPv6

Capture revenue with innovative IPv6-based services



Connections won't be limited to human-interface devices; everyday things will have IP addresses.

Managing an Orderly IPv6 Transition

IPv6 Is Not a Rip-and-Replace Proposition

Preserve

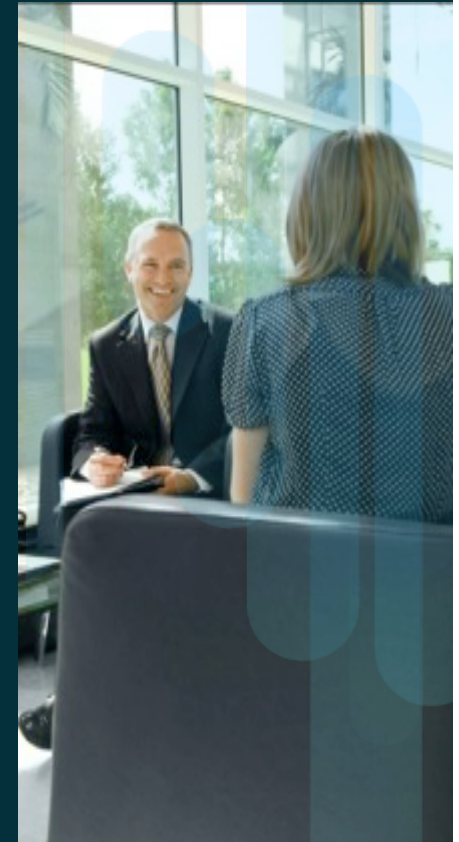
- Preserve the customer's existing investment*
- Audit and leverage existing IPv6 capabilities

Prepare

- Prepare a migration and deployment plan*
- Identify and enable critical IPv6 functional areas
 - Enable Dual-Stack capabilities

Prosper

- Prosper through the transition to IPv6 Internet*
- Pervasive dual-stack capabilities
 - Grow seamlessly as customers transition to IPv6



IPv6 is the foundation of a lifecycle management discussion

IPv6 Integration Outline

Pre-Deployment Phases

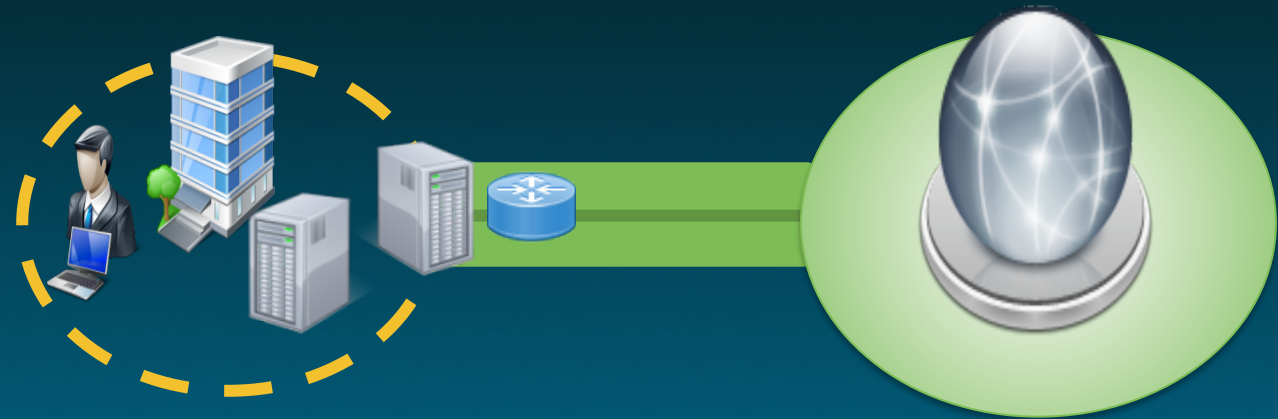
- Establish the network starting point
- Importance of a network assessment and available tools
- Build a pilot or lab environment
- Obtain addressing or use ULA or documentation prefix (in lab)
- Learn the basics (DNS, routing changes, address assignment)

Deployment Phases

- Transport considerations for integration
- Internet Edge (ISP, Apps)
- Campus IPv6 integration options
- Data Center integration options
- WAN IPv6 integration options
- Execute on gaps found in assessment

Enterprise Deployment Options (High Level)

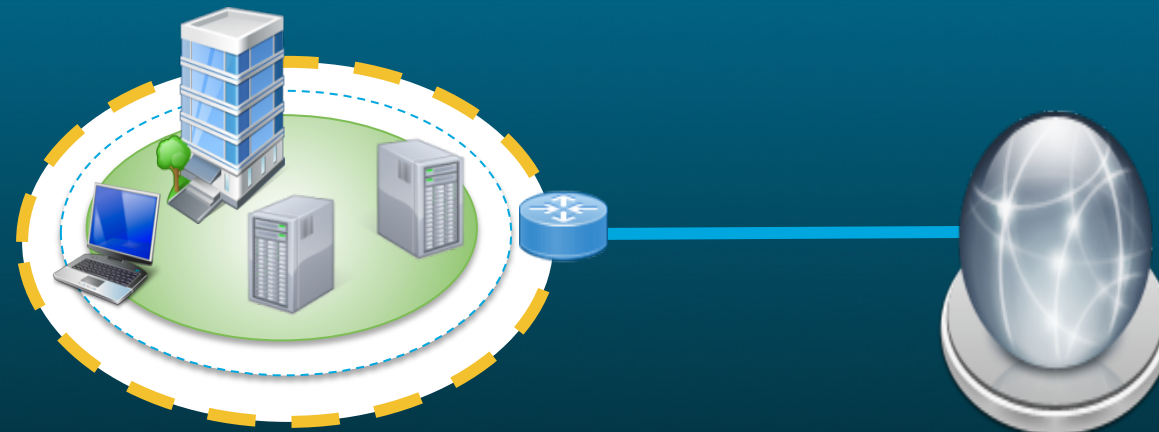
Outside - In



IPv4 Enterprise

IPv6 Internet

Inside - Out



Dual-Stack Enterprise

IPv4 Internet

Enterprise Use Cases

Use Case

IPv6 Technology

Relevant Products

IPv6 Internet Presence

- Get started on the IPv6 Internet Edge for “Outside-In” deployment

Statefull NAT64 HTTP Proxy

- Allows IPv6 or dual-stack Internet users to access content/application (and vice versa)

- Stateful NAT / ASR1000
- ACE30 IPv6 SLB/Proxy,GSS
- Internet Edge Security ASA, IDS,
- Internet Edge Routing ISR, ASR1K, ASR9K..FNF
- Catalyst 6k,4k,3k, NAM

Internal Network

- Set up devices to run IPv4 and IPv6 in parallel
- Link hosts and islands of IPv6 devices together
- Expand toward the edge

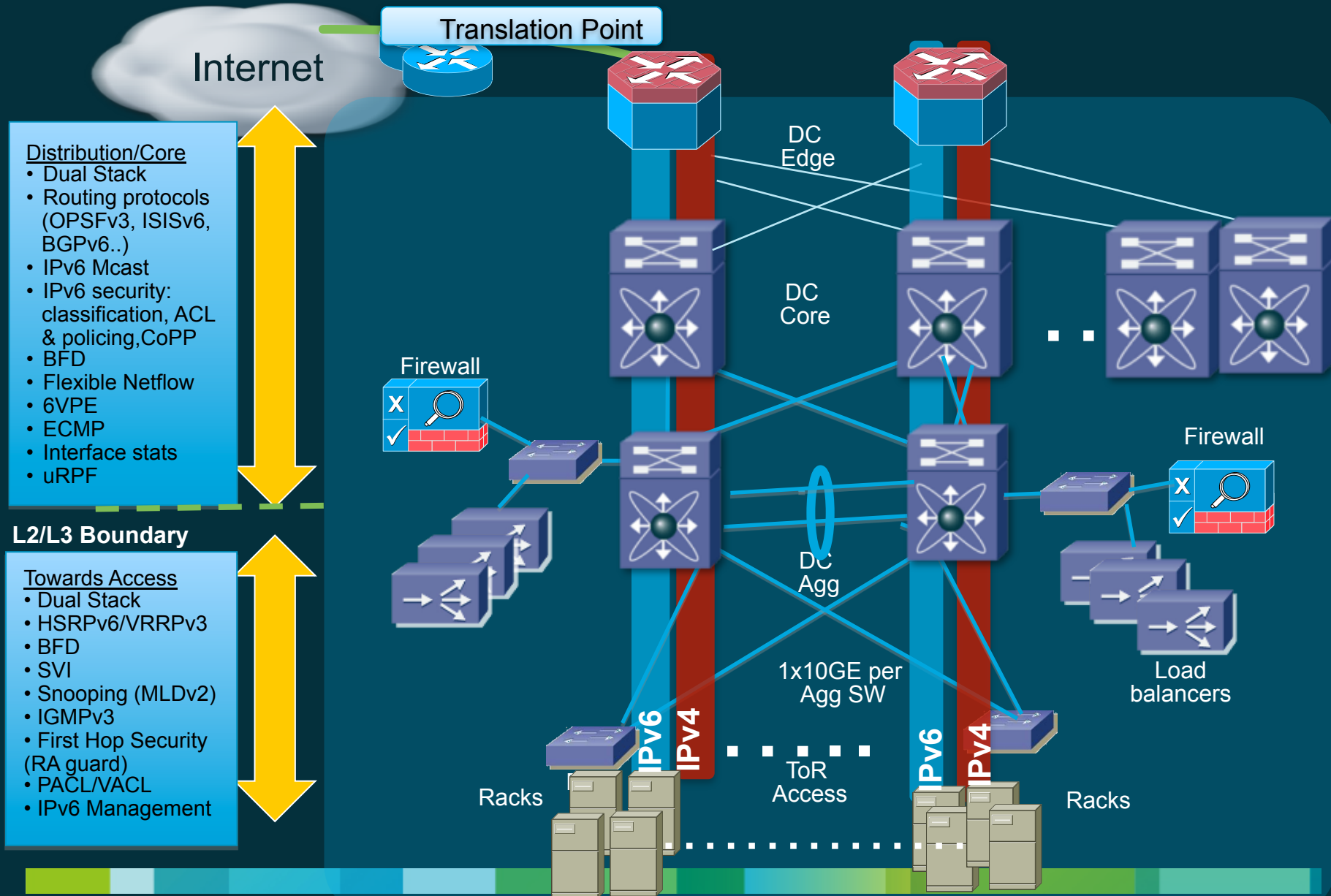
IPv6 and IPv4

- IPv6 switching and routing
- IPv6 over IPv4 tunneling
- First Hop Security
- Monitoring

- Catalyst 6K, 4K, 3K, 2K
- Nexus 7K, Security appl.
- AnyConnect VPN client
- ASR 1000
- ISR G2
- NAM

Cisco Advanced Services

IPv6 Data Center Network Architecture



- Distribution/Core
- Dual Stack
 - Routing protocols (OPSFv3, ISISv6, BGPv6..)
 - IPv6 Mcast
 - IPv6 security: classification, ACL & policing, CoPP
 - BFD
 - Flexible Netflow
 - 6VPE
 - ECMP
 - Interface stats
 - uRPF

- Towards Access
- Dual Stack
 - HSRPv6/VRRPv3
 - BFD
 - SVI
 - Snooping (MLDv2)
 - IGMPv3
 - First Hop Security (RA guard)
 - PACL/VACL
 - IPv6 Management

IPv6 in the Enterprise Data Center

Biggest Challenges Today

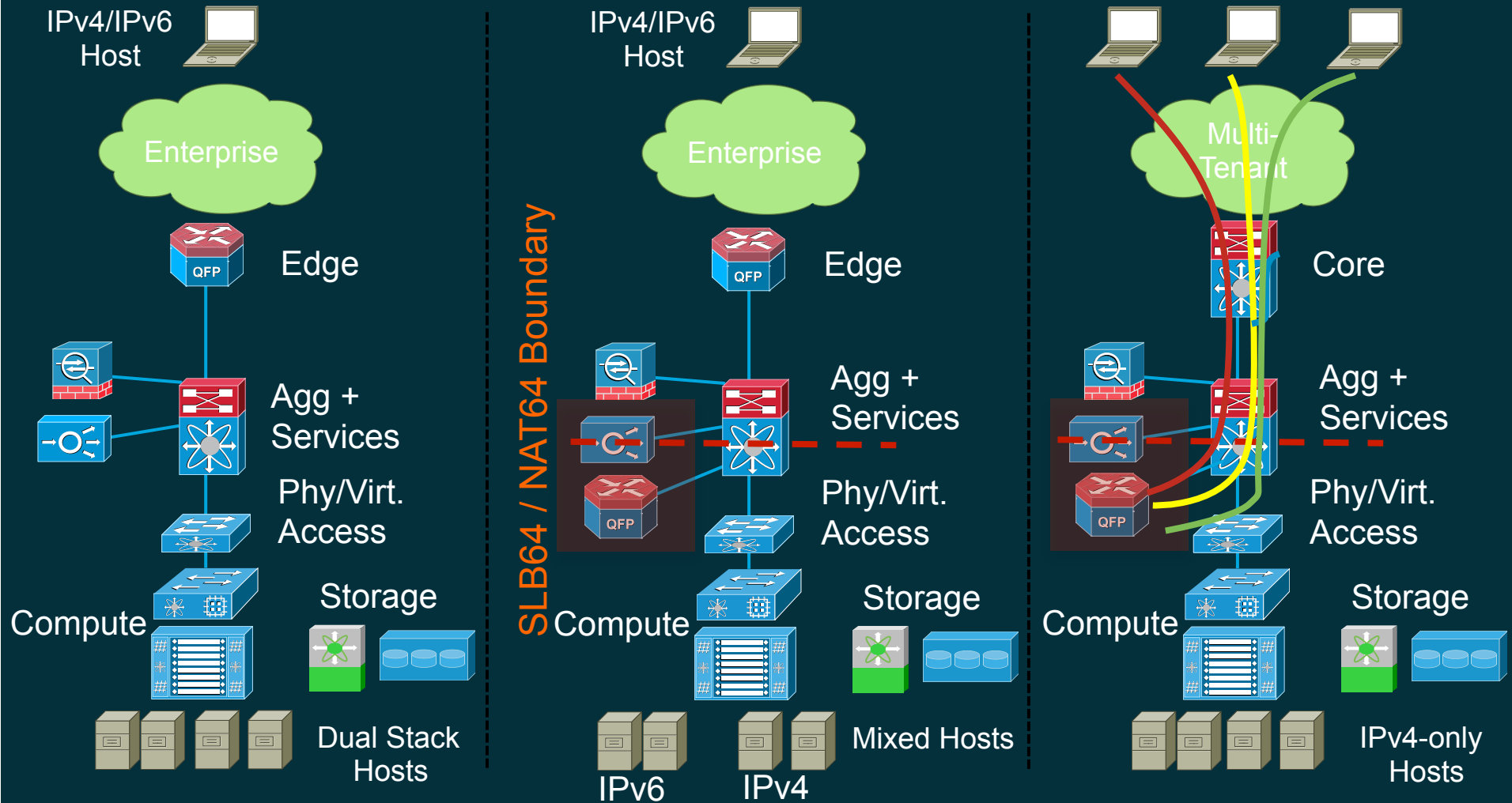
- Application support for IPv6 – Know what you don't know
 - If an application is protocol centric (IPv4):
 - Needs to be rewritten
 - Needs to be translated until it is replaced
 - Wait and pressure vendors to move to protocol agnostic framework
- Deployment of translation
 - NAT64 (Stateful for most enterprises)
 - Apache Reverse Proxy
 - Windows Port Proxy
 - 3rd party proxy solutions
- Network services above L3 (A short-term challenge)
 - SLB, SSL-Offload, application monitoring (probes)
 - Application Optimization
 - High-speed security inspection/perimeter protection

Common Deployment Models for DC

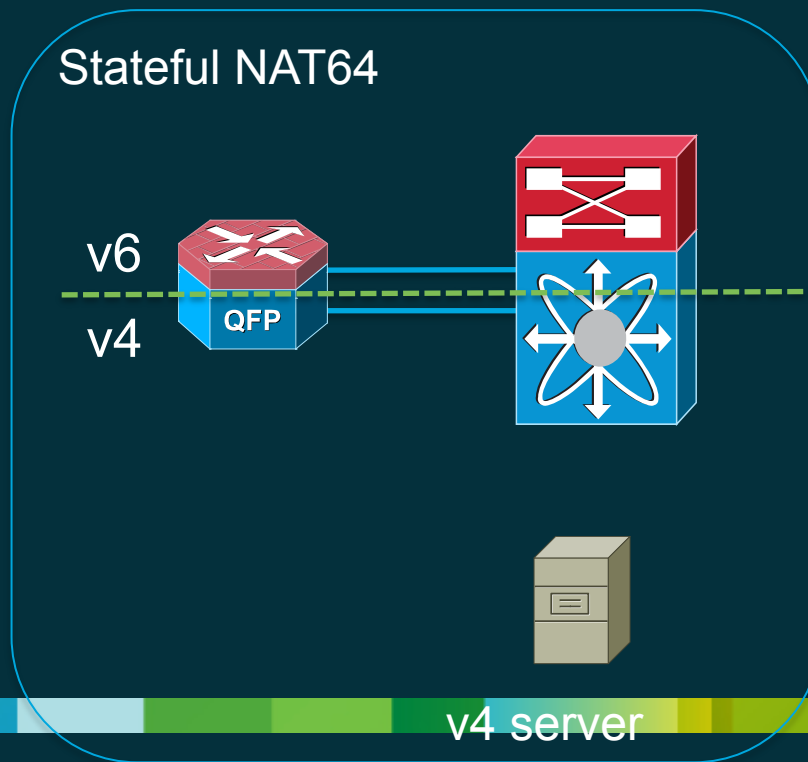
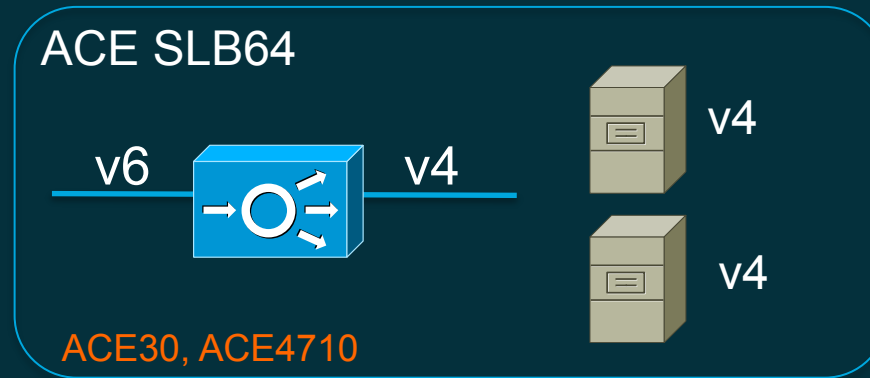
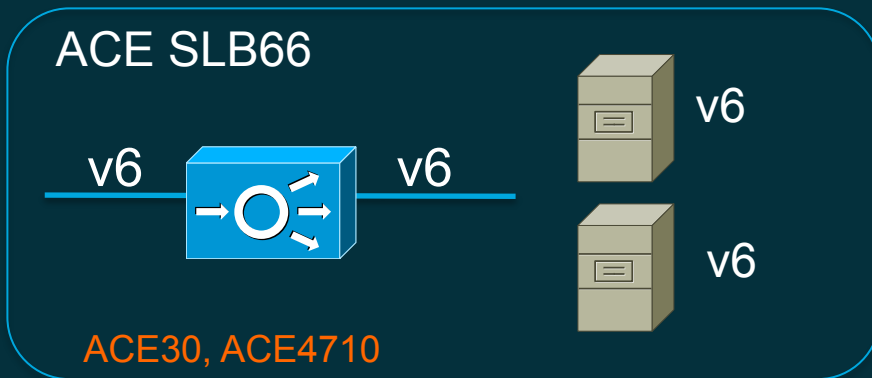
Pure Dual Stack

Conditional Dual Stack

Translation as a Service



ACE + IPv6 / ASR + NAT64



Commonly Deployed IPv6-enabled OS/Apps

Operating Systems

- Windows 7
- Windows Server 2008/R2
- SUSE
- Red Hat
- Ubuntu
- FreeBSD
- The list goes on

Virtualization & Applications

- VMware vSphere 4.1
- Microsoft Hyper-V
- Microsoft Exchange 2007 SP1/2010
- Apache/IIS Web Services
- Windows Media Services
- Multiple Line of Business apps

**Most commercial applications won't be your problem
– it will be the custom/home-grown apps**

Application/OS Support Drives DC Options

Exchange 2003/2007/W2K3

Exchange 2007 SP1/W2K8

Exchange 2010/W2K8

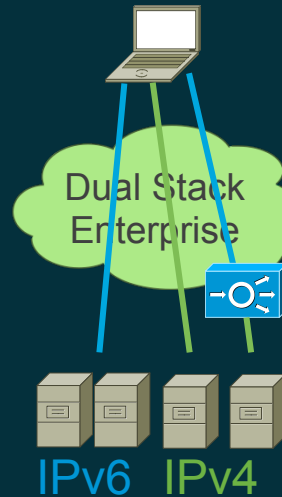
No App IPv6 Support / Limited OS Support

- Leave on IPv4
- Translation won't work – no ALG support for MAPI/RPC, etc...



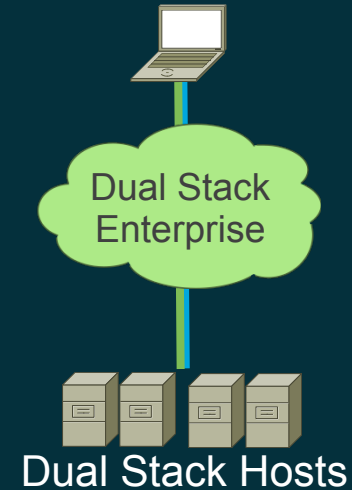
Most of App Supports IPv6 / Full OS Support

- Dual stack what you can
- IPv4 legacy components (i.e. MSFT UC)
- Lazy man's method – Translate HTTP/S components



Full App Support / Full OS Support

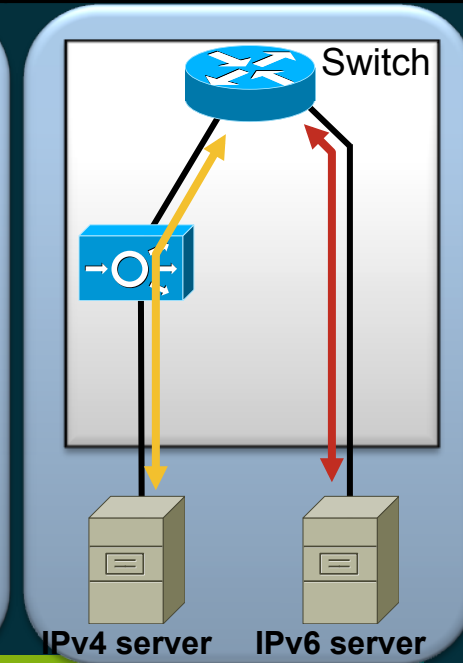
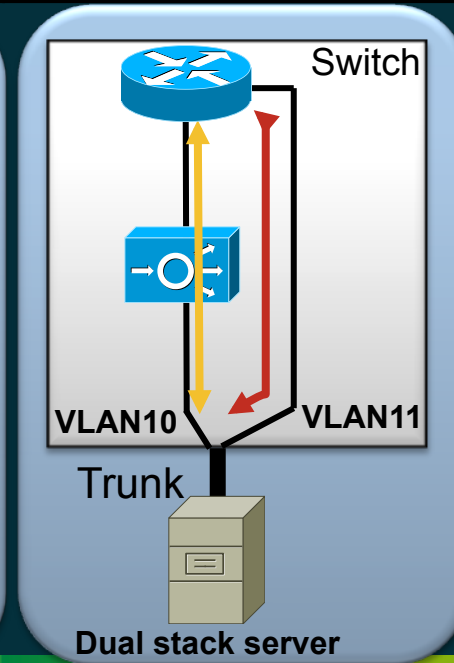
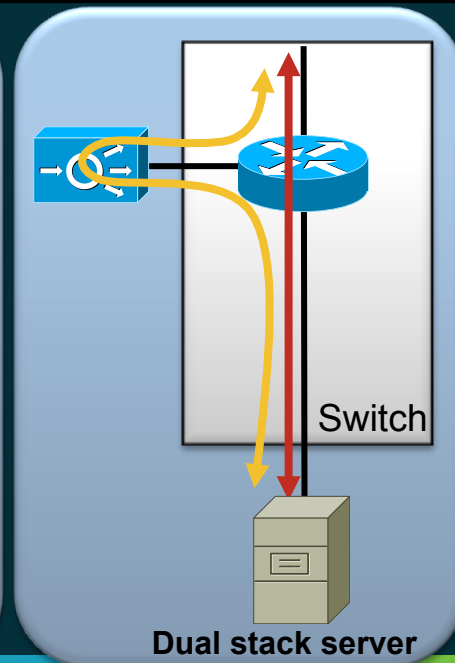
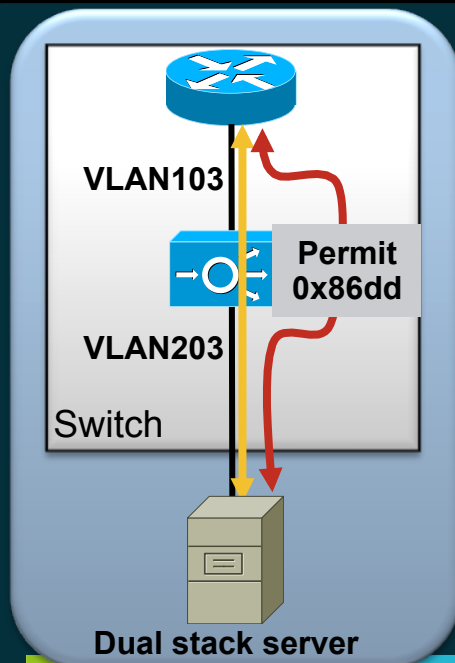
- Dual stack everything
- Lazy man's method – Translate HTTP/S components



IPv6 Deployment in the Data Center

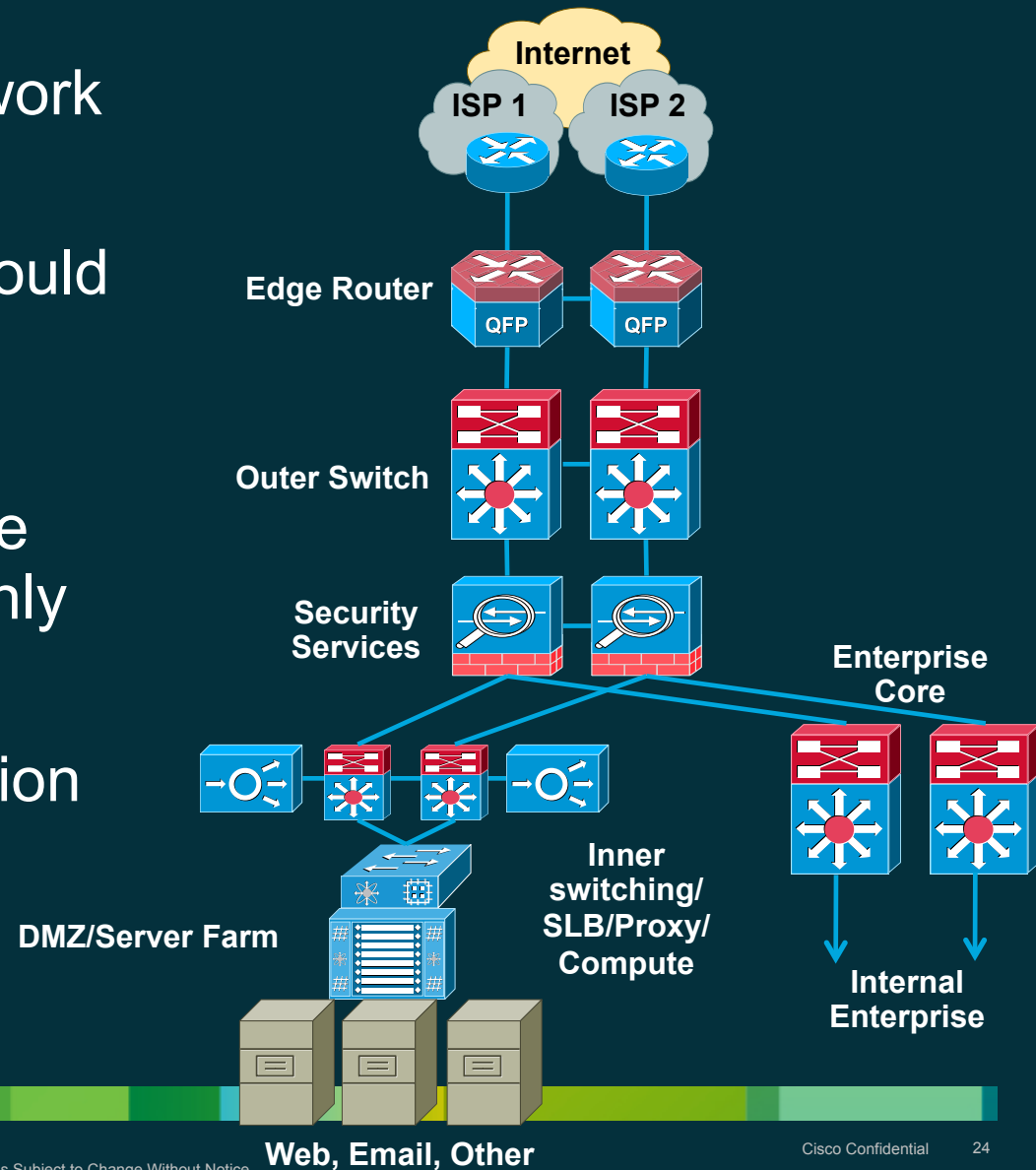
Services/Appliances Do Not Support IPv6

Transparent	One-Armed	Routed	Dedicated Server Farm
<ul style="list-style-type: none"> IPv6 traffic is bridged between VLANs Permit Ethertype 0x86dd (IPv6) 	<ul style="list-style-type: none"> IPv6 traffic bypasses services IPv4 traffic is sent to one-arm attached module/appliance 	<ul style="list-style-type: none"> Create trunk between switch and server IPv4 has default gateway on service module IPv6 on separate VLAN to MSFC 	<ul style="list-style-type: none"> New IPv6 only servers can be connected to existing access/agg pair on different VLANs New access/agg switches just for IPv6 servers



Dual Stack the Internet Edge

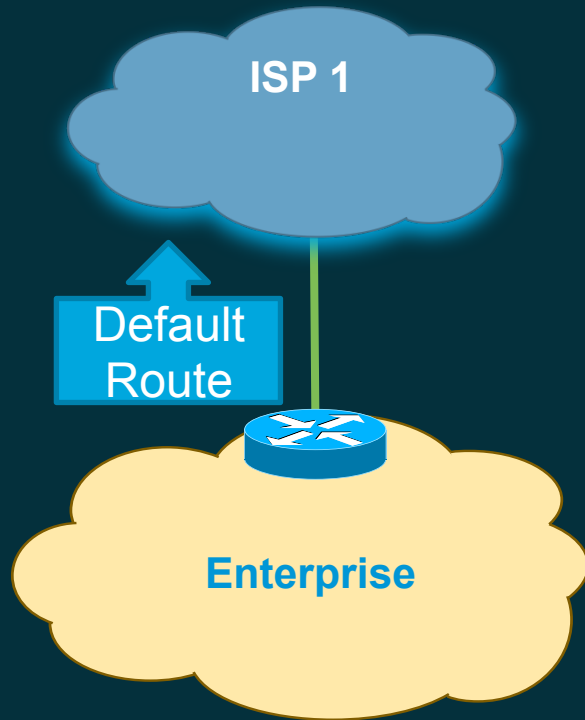
- Dual stack the same network you have
- Most design elements should be the same as with IPv4 (minus pure NAT/PAT)
- You may have to embrace SLB64/NAT64 for IPv4-only apps
- LISP (Locator/ID Separation Protocol)



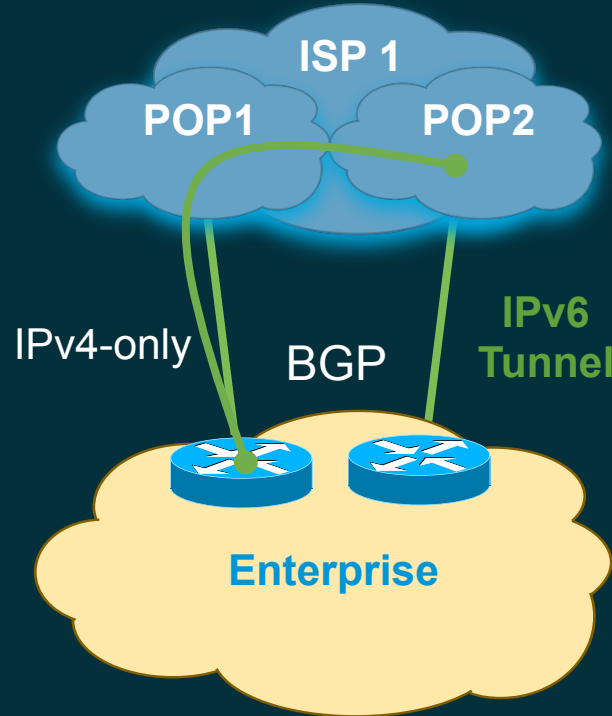
Internet Edge - to - ISP

Boatloads of options

Single Link
Single ISP

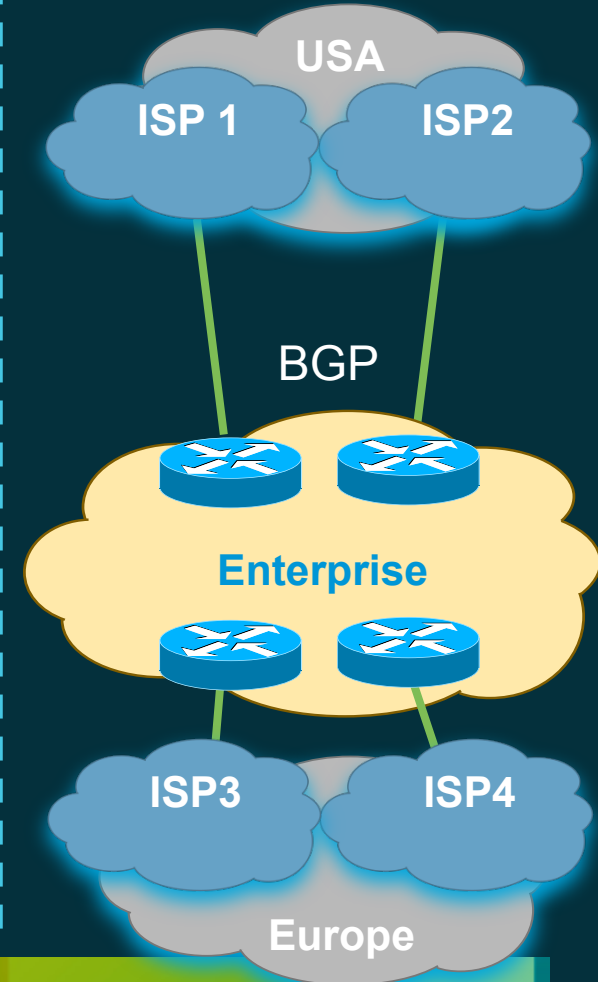


Dual Links
Single ISP



Your ISP may not have IPv6 at the local POP

Multi-Homed
Multi-Region



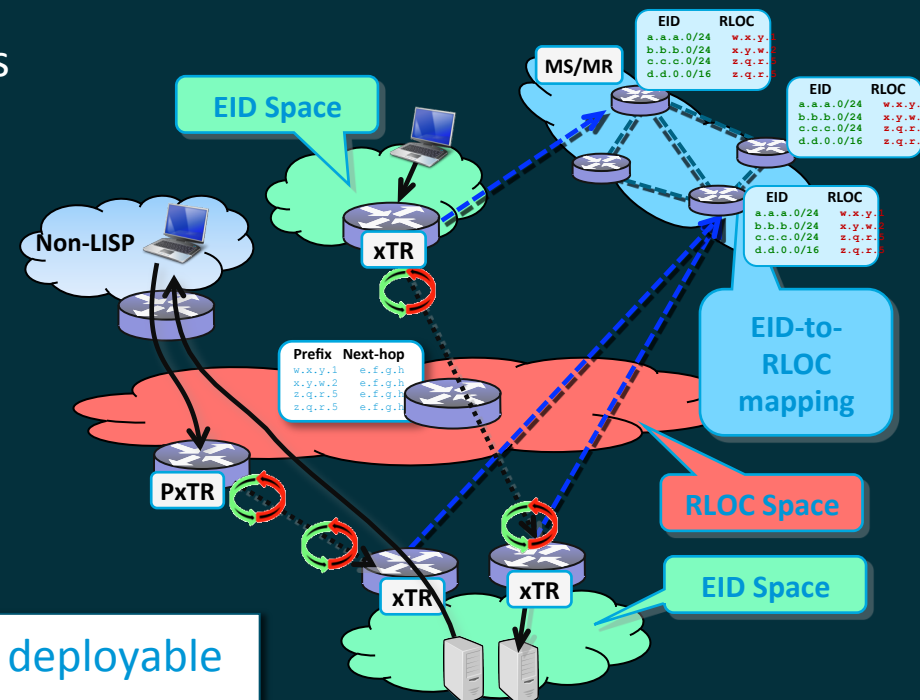
LISP Overview

Location/ID Separation Protocol

LISP creates a “Level of indirection” with two namespaces: **EID** and **RLOC**

- **EID (Endpoint Identifier)** is the IP address of a host – just as it is today
- **RLOC (Routing Locator)** is the IP address of the LISP router for the host
- **EID-to-RLOC mapping** is the distributed architecture that maps **EIDs** to **RLOCs**

- Network-based solution
- No host changes
- Minimal configuration
- Incrementally deployable
- Support for mobility
- Address Family agnostic



LISP for IPv6 Migration

Needs:

- Rapid IPv6 Deployment
- Minimal Infrastructure disruption

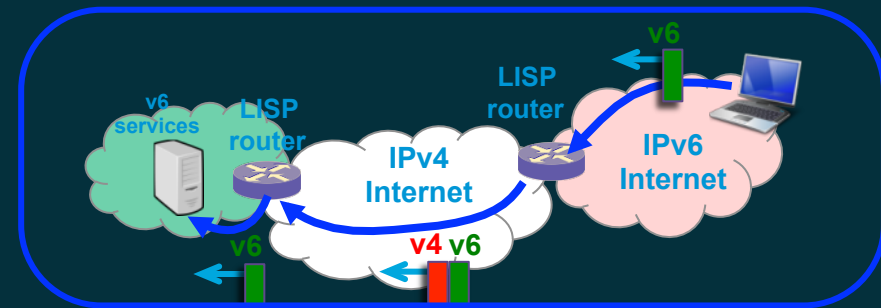
LISP Solution:

- LISP encapsulation is Address Family agnostic
 - IPv6 interconnected over IPv4 core
 - IPv4 interconnected over IPv6 core

Benefits:

- Accelerated IPv6 adoption
- Minimal added configurations
- No core network changes
- Can be used as a transitional or permanent solution

IPv6 Transition Support



- v6-over-v4, v6-over-v6
- v4-over-v6, v4-over-v4

IPv6 Services and Applications Tested

- SLB66 on Cisco ACE – One arm mode
- Cisco ASA in A/A or A/S – Failover over IPv4 OR IPv6
- Cisco IPS/IDS – any model
- Baremetal servers on Catalyst or Nexus and UCS C-Series
- Virtualized on Nexus 5000, Nexus 1000v and UCS C-Series or other combo

Application Networking Manager 5.1

- Full Monitoring
- Configure all elements of policies
- Configure by context, filter by multiple conditions, etc..

Monitor > Devices > Load Balancing > Real Servers ace-4710-1:IE-WEB

Real Servers (Last Polled: 27-Oct-2011 17:42:22)

<input type="checkbox"/> Real Server	IP Address	Port	Server Farm	Admin Status	Operational Status	VM	Weight	Locality	Current Conns	Conns/Sec	Dropped Conns/Sec
<input type="checkbox"/> WEB_V6_1	2001:db8:cafe:115::10	80	WEB_V6_SF	<input checked="" type="checkbox"/> Inservice	<input checked="" type="checkbox"/> Inservice	-	8	Not Supported	0	0	0
<input type="checkbox"/> WEB_V6_2	2001:db8:cafe:115::11	80	WEB_V6_SF	<input checked="" type="checkbox"/> Inservice	<input checked="" type="checkbox"/> Probe failed	-	8	Not Supported	0	0	0

Config > Devices > Network > NAT Pools ace-4710-1:IE-WEB

NAT Pools

<input type="radio"/> VLAN ID	NAT Pool ID	Start IP Address	End IP Address	Netmask Or Prefix Length	PAT Enabled
<input checked="" type="radio"/> 19	1	2001:db8:cafe:115::ace	2001:db8:cafe:115::ace	128	<input checked="" type="checkbox"/>
<input type="radio"/> 19	2	10.140.19.250	10.140.19.250	255.255.255.0	<input checked="" type="checkbox"/>

Config > Devices > Load Balancing > Real Servers ace-4710-1:IE-WEB

Real Servers

<input checked="" type="radio"/> Name	Type	State	Operational Status	Last Polled	Description	IP Address	Min. Connections	Max. Connections
<input checked="" type="radio"/> WEB_V4_1	Host	In Service	InService	2011-10-27 17:47:22		10.140.19.80		
<input type="radio"/> WEB_V4_2	Host	Out Of Service	OutOfService	2011-10-27 17:47:22		10.140.19.81		
<input type="radio"/> WEB_V6_1	Host	In Service	InService	2011-10-27 17:47:22		2001:db8:cafe:115::10		
<input type="radio"/> WEB_V6_2	Host	In Service	InService	2011-10-27 17:47:22		2001:db8:cafe:115::11		

ASA Firewall IPv6 Support

- Since version 7.0 (April 2005)
- Dual-stack, IPv6 only, IPv4 only
- Extended IP ACL with stateful inspection
- Application awareness
 - HTTP, FTP, telnet, SMTP, TCP, SSH, UDP
- uRPF and v6 Frag guard
- IPv6 header security checks
 - Always block routing-header (type 0 and 2)
- Management access via IPv6
 - Telnet, SSH, HTTPS
- ASDM support (ASA 8.2)
- Routed & transparent mode (ASA 8.2)
- Fail-over support (ASA 8.2.2)

Dual-Stack IPS Engines

Service HTTP

The screenshot shows the Cisco IPS Manager Express 7.0.1 interface. The 'Event Monitoring' tab is active, displaying 'View Settings' for a 'Basic Filter'. The settings include Packet Parameters (Attacker IP, Victim IP, Signature Name/ID, Victim Port) and Rating and Action Parameters (Severity, Risk Rating, Threat Rating, Action(s) Taken). The 'Other Parameters' section includes Sensor Name(s), Virtual Sensor, Status (set to 'New'), and Vict. Locality.

Below the settings is a table of detected events:

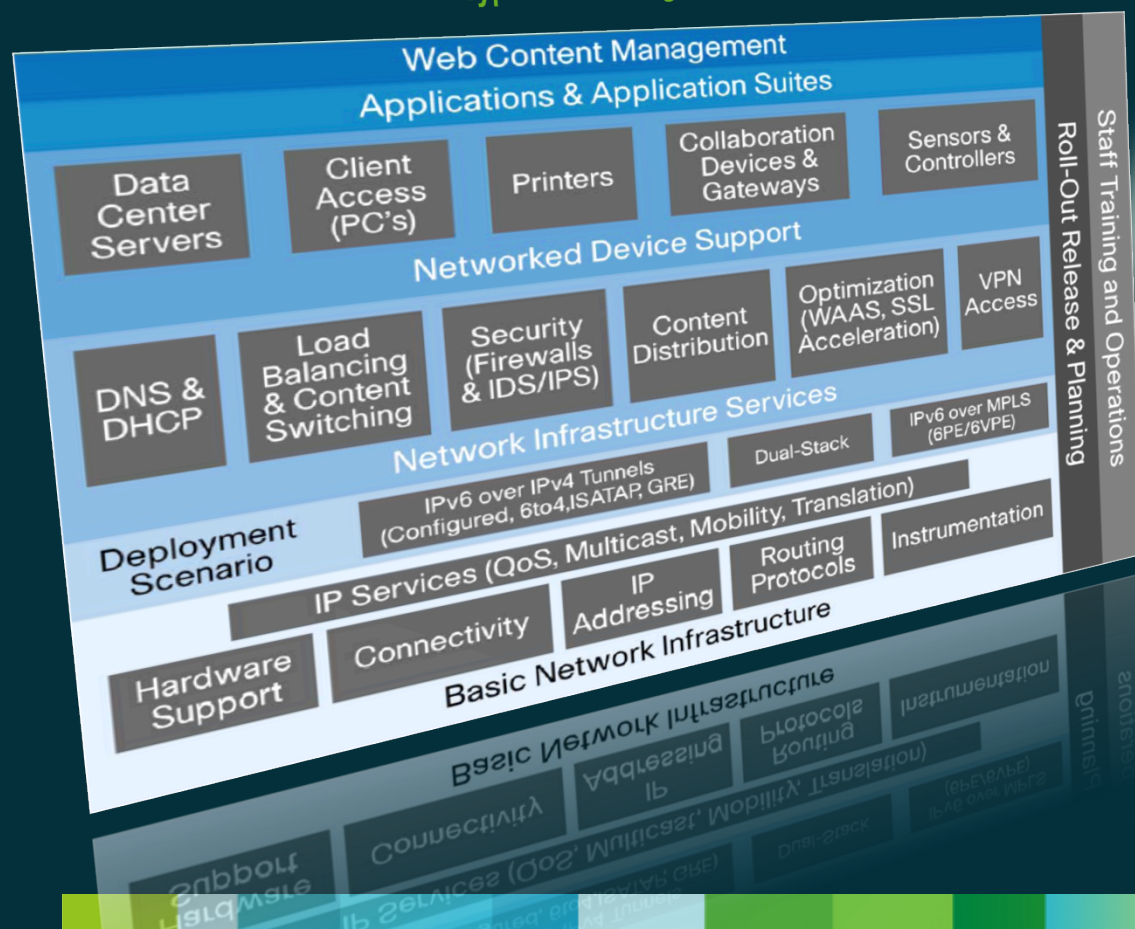
Severity	Date	Time	Device	Sig. Name	Sig. ID	Attacker IP	Victim IP	Victim Port	Threat Rating
low	06/11/2009	17:06:56	4240-munsec	Dot Dot Slash in URI	5256/0	192.168.200.46	192.168.200.38	80	52
low	06/11/2009	17:07:14	4240-munsec	Dot Dot Slash in URI	5256/0	2001:db8:0:0:0:0:0:46	2001:db8:0:0:0:0:0:38	80	42

	Sig. Name	Sig. ID	Attacker IP	Victim IP	Victim Port	Threat Rating
c	Dot Dot Slash in URI	5256/0	192.168.200.46	192.168.200.38	80	
c	Dot Dot Slash in URI	5256/0	2001:db8:0:0:0:0:0:46	2001:db8:0:0:0:0:0:38	80	

IPv6 integration architecture (systems-wide)

IPv6 integration is not 'just a network upgrade' but complex endeavour, involving many elements and capabilities which evolve over time, rather than changing all at once.

Typical IPv6 Integration Elements



Planning and coordination is required from many across the organisation, including ...

- ✓ Network engineers & operators
- ✓ Security engineers
- ✓ Application developers
- ✓ Desktop (Office Automation) / Server engineers
- ✓ Web hosting / content developers
- ✓ Business development managers
- ✓ ...

Moreover, training will be required for all involved in supporting the various IPv6 based network services

Thank you.

