TOMORROW
starts here.
CISCO
Cisco live!

IPv6 Planning, Deployment and Operation Considerations

BRKRST-2311

Alvaro Retana (aretana@cisco.com)

Distinguished Engineer, Cisco Services

#clmel

Cisco live!

Agenda

- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- Transition Mechanisms
- IPv6 Co-existence Considerations
- Management and Operations
  - IPv6 DNS
  - IPv6 Security
  - Summary

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Market Trends

Cisco live!

IPv4 Address Exhaustion

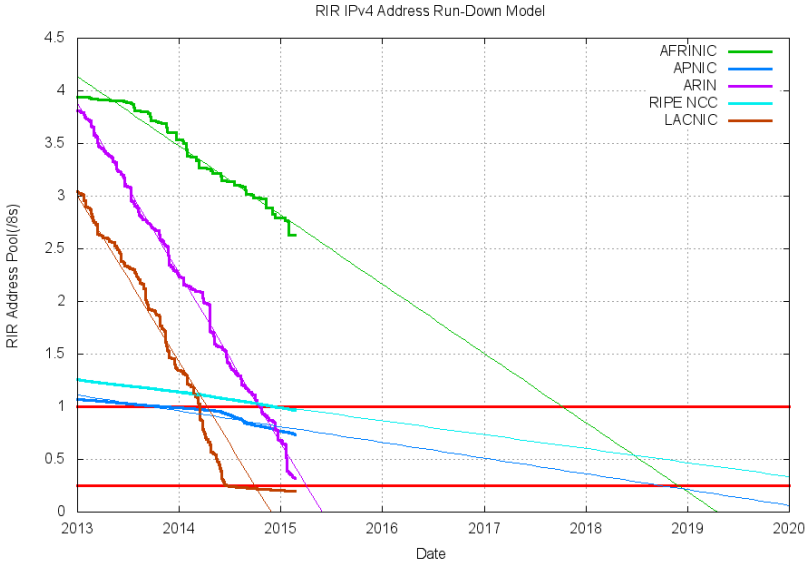
This report generated at 21-Feb-2015 08:07 UTC.

IANA Unallocated Address Pool Exhaustion:
03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date	Remaining Addresses in RIR Pool (/8s)
APNIC:	**19-Apr-2011** (actual)	0.7365
RIPE NCC:	**14-Sep-2012** (actual)	0.9643
LACNIC:	**10-Jun-2014** (actual)	0.1960
ARIN:	**15-May-2015**	0.3215
AFRINIC:	**19-Jan-2019**	2.6286

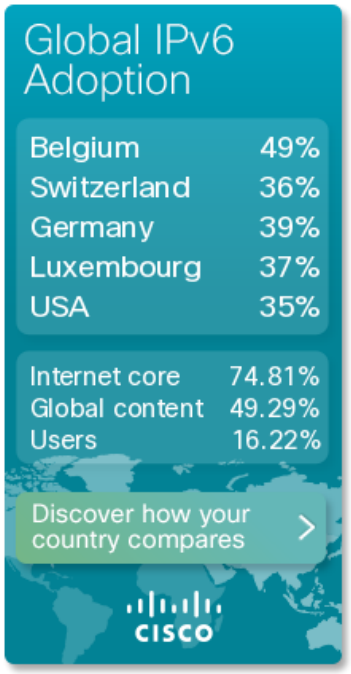
Open market: USD $10-$20 per IPv4 address

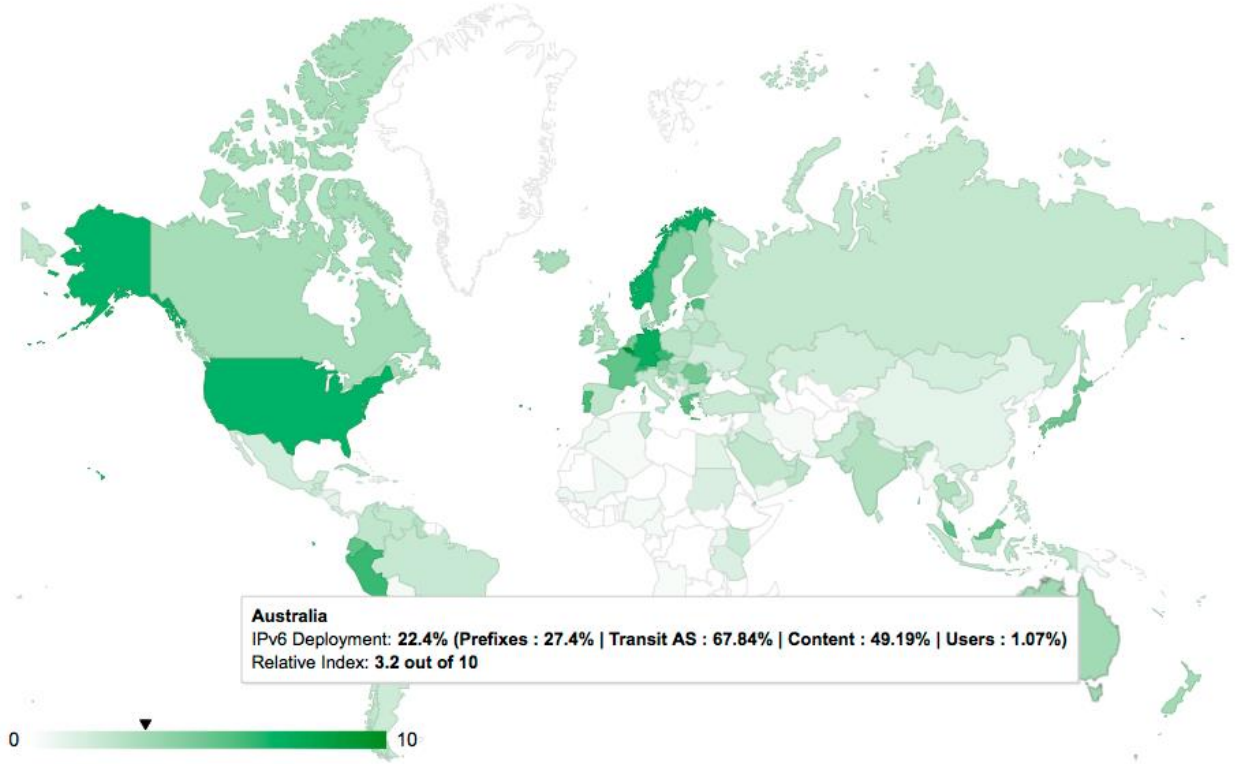


http://www.potaroo.net/tools/ipv4/

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPv6 Market Adoption





http://6lab.cisco.com/

© 2015 Cisco and/or its affiliates. All rights reserved.

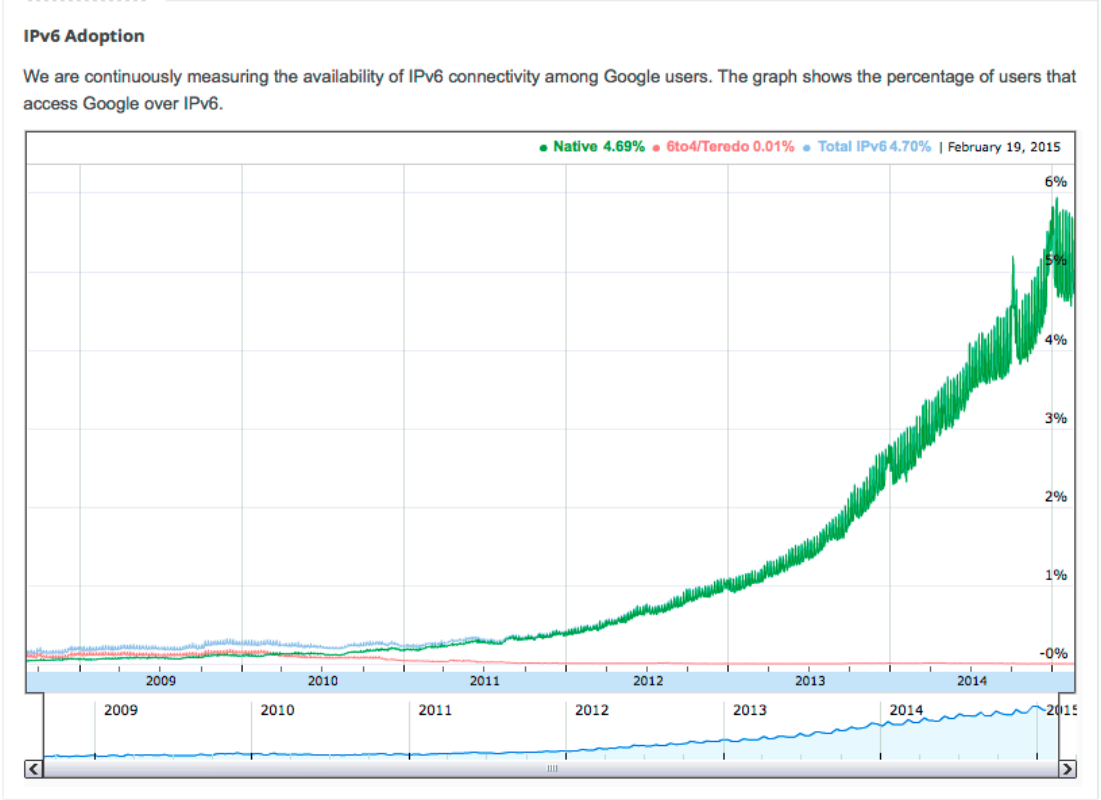
Cisco live!

IPv6 Global Deployment to Users

10+ Years for Preparation and Trial..

Now Doubling every 9 months!

Government Mandates have played a significant role in deployment.



https://www.google.com/intl/en/ipv6/statistics.html

© 2015 Cisco and/or its affiliates. All rights reserved.

Evolving Internet……

Connecting Things

- Devices – Phones, TV/Entertainment
- ATA's, Set-tops
- Systems, Game Consoles, Cars, Power Meters
- Sensors - Oil Rigs, Smart Grid, Bio Sensors

Communicating

- Machine to Machine
- Vehicle to Vehicle
- Vehicle to Infrastructure

Impacting Business

- Healthcare
- Manufacturing
- Retail
- Energy
- Financial Service

Changing User Experience

- Safety
- Convenience
- Health
- Productivity

http://www.rita.dot.gov/

International Civil Aviation Organisation

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Things Philosophy

Drivers

Ubiquitous computing
Intelligence in things at the edge (Fog)

Ubiquitous use of IP
Convergence of proprietary protocols

Ubiquitous connectivity
Radio, Cellular, Fixed

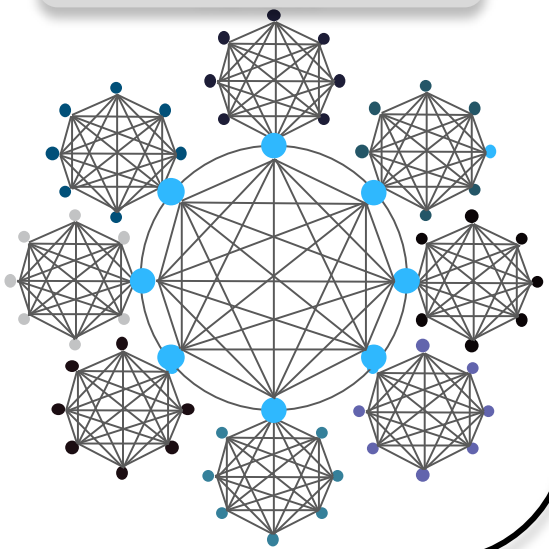
Architectural Philosophy

From

Interaction with capable devices via proprietary/closed systems

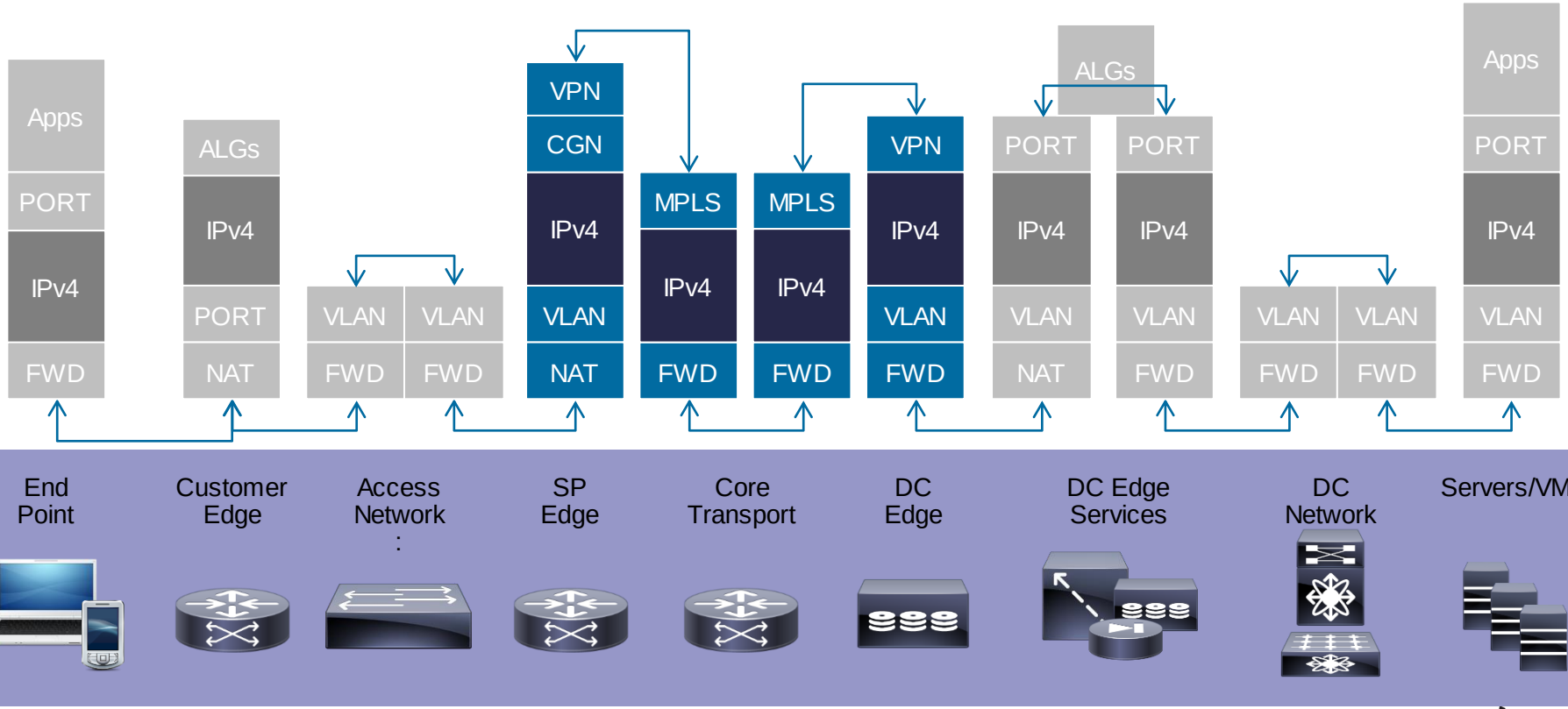
To

Distributed intelligence & actions across standardised networks & interfaces



© 2015 Cisco and/or its affiliates. All rights reserved.

IPv4: Limited End-to-End

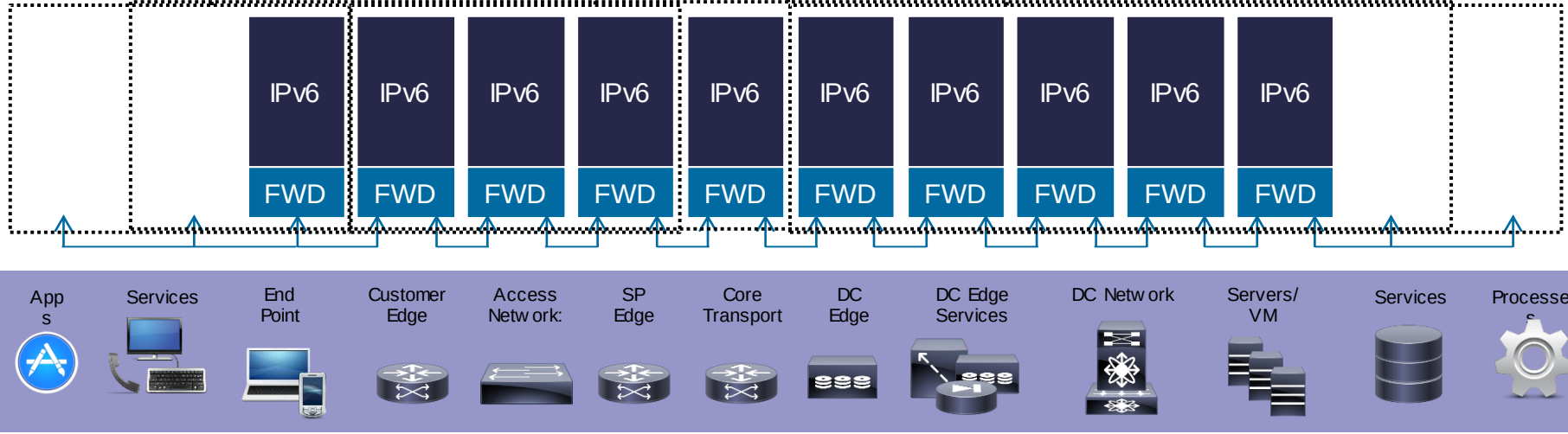


This slide from Mark Townsley's IPv6 World Congress 2014 talk

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPv6: Redefining End-to-End

Flow treatments can be influenced by several methods, including segment routing and prefix colouring (in addition to the legacy methods)



This slide modified from Mark Townsley's IPv6 World Congress 2014 talk

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPv6 in SP Networks: Drivers

- External Drivers
  - Business continuity
  - 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.)
  - SP customers that need access to IPv6 resources (for development or experimentation purposes) competing for RFP's
  - 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
  - Public IPv4 address exhaustion
  - Private IPv4 address exhaustion
- Strategic Drivers
  - Long term expansion plans and service offering strategies
  - Preparing for new services and gaining competitive advantage

© 2015 Cisco and/or its affiliates. All rights reserved.

General Observations – Enterprises and IPv6

- They have an application requirement to drive it
- Their presence on the Internet is compromised by lack of IPv6 access
- The price of an IPv4 address exceeds the hardware cost to route it
- Sniffer traces in the network show IPv6 traffic floating around.
- Application dependency mapping for service movement misses flows.
  - Some local communication is happening over IPv6.
- Enterprise InfoSec team realises that IPv6 Security policies are not in place.

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

IPv6 Planning

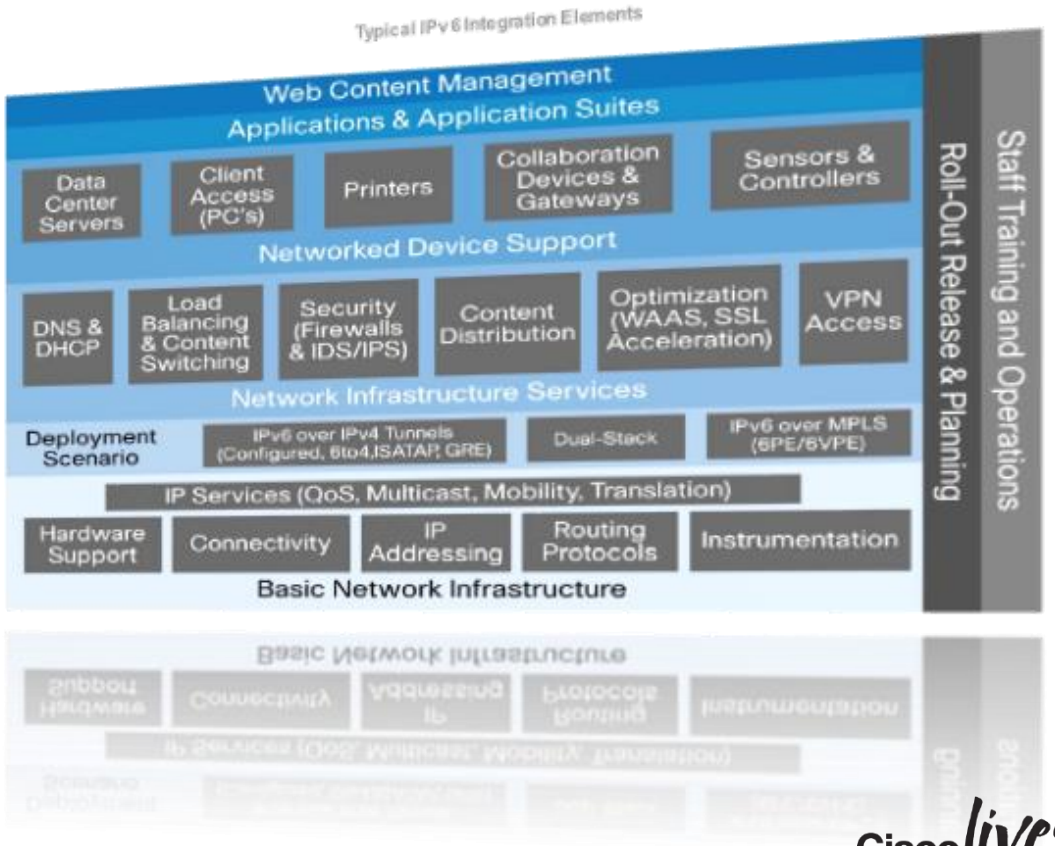
Cisco live!

The Scope of IPv6 Deployment

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

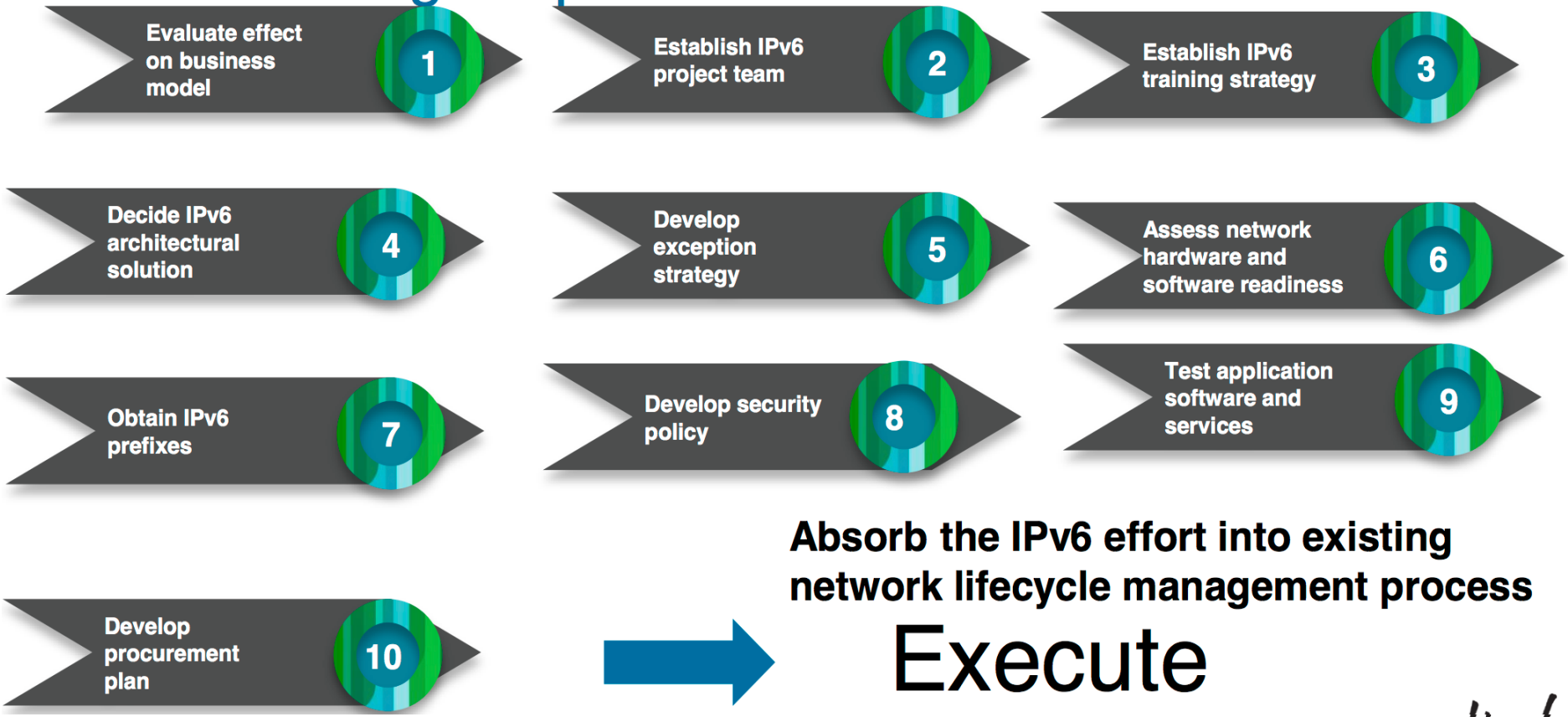
- ✓**Network engineers & operators**
- ✓**Security engineers**
- ✓**Application developers**
- ✓**Desktop / Server engineers**
- ✓**Web hosting / content developers**
- ✓**Business development managers**
- ✓**…**

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



© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Planning Steps



Absorb the IPv6 effort into existing network lifecycle management process

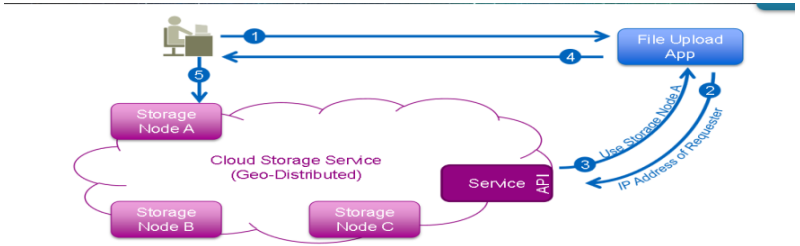
Execute

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Cisco IT Lessons Learnt

- Consider the effect of IPv6 addresses on external parties
  - including Internet service providers, CDN providers, and third-party application providers
- Security
  - Firewalls, IDS/IPS, security event management and forensics logging
- Application visibility
  - Netflow V9 not supported on all platforms including collectors
  - Had to shift Netflow collection into DMZ
  - Use of Netflow reflectors can bring some relief
- Geo-Location and Web analytics
  Client_IpAddress:= X-forwarded-for address first address;



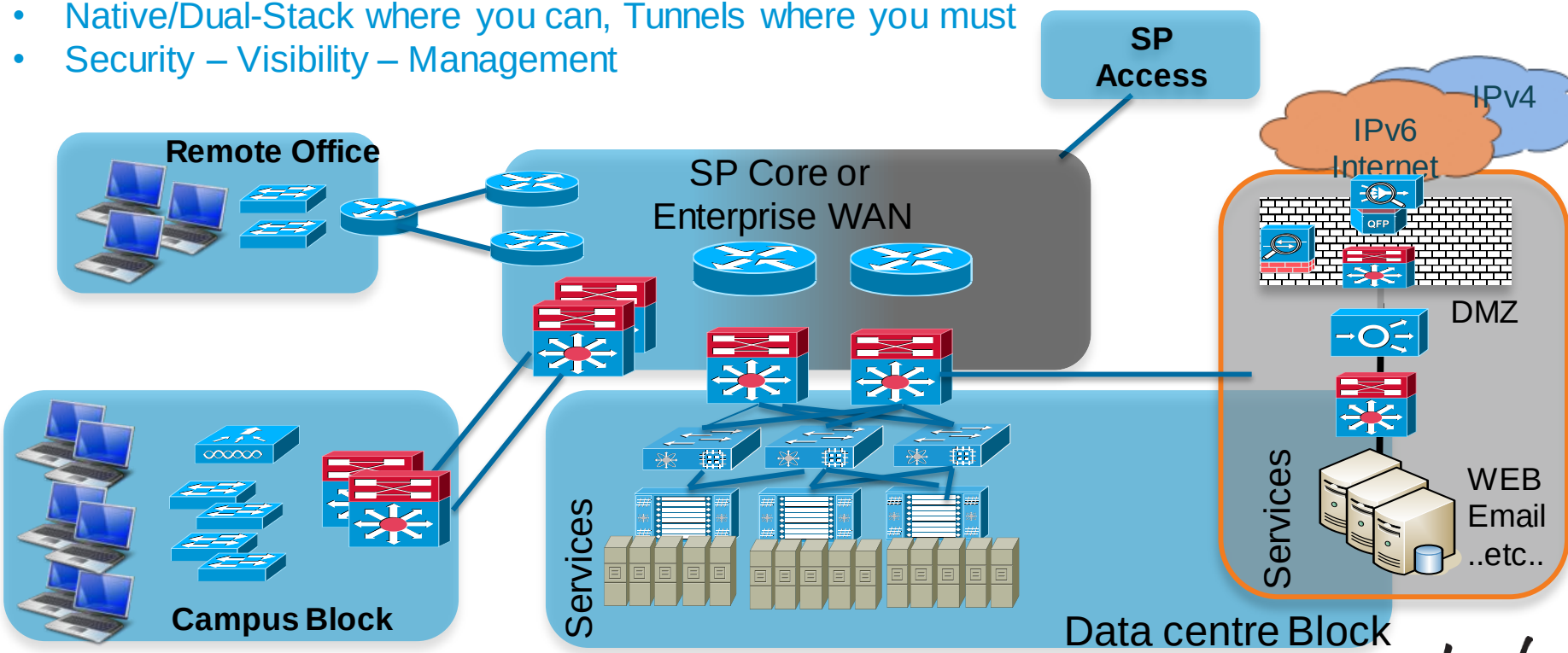
- Take advantage of prescheduled release windows when possible.

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Internal Network: Where do I start?

- Life-Cycle management, depends on Timing and Use case
- Native/Dual-Stack where you can, Tunnels where you must
- Security – Visibility – Management

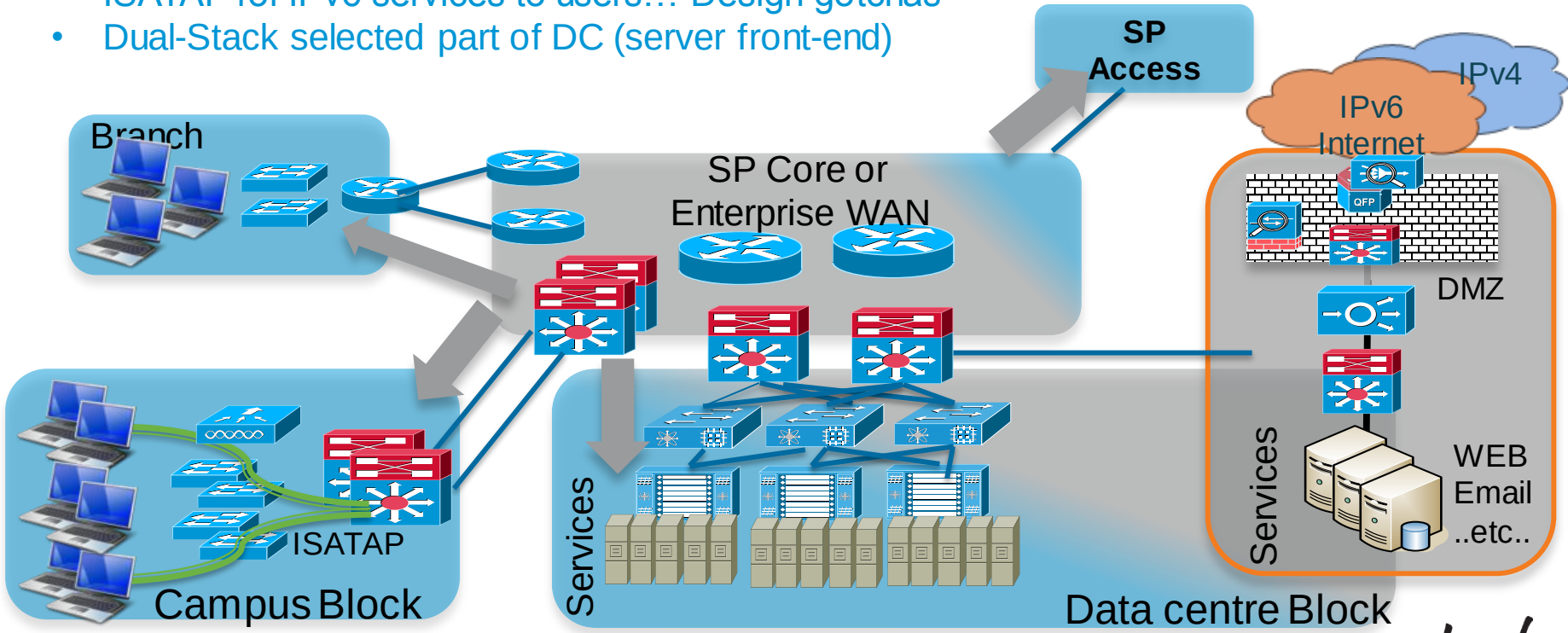


© 2015 Cisco and/or its affiliates. All rights reserved.

Core to Edge !

Orderly Transition – Slow to dual-Stack all the way to user

- Dual-Stack Core – Network based Tunnel to connect island
- ISATAP for IPv6 services to users… Design gotchas
- Dual-Stack selected part of DC (server front-end)

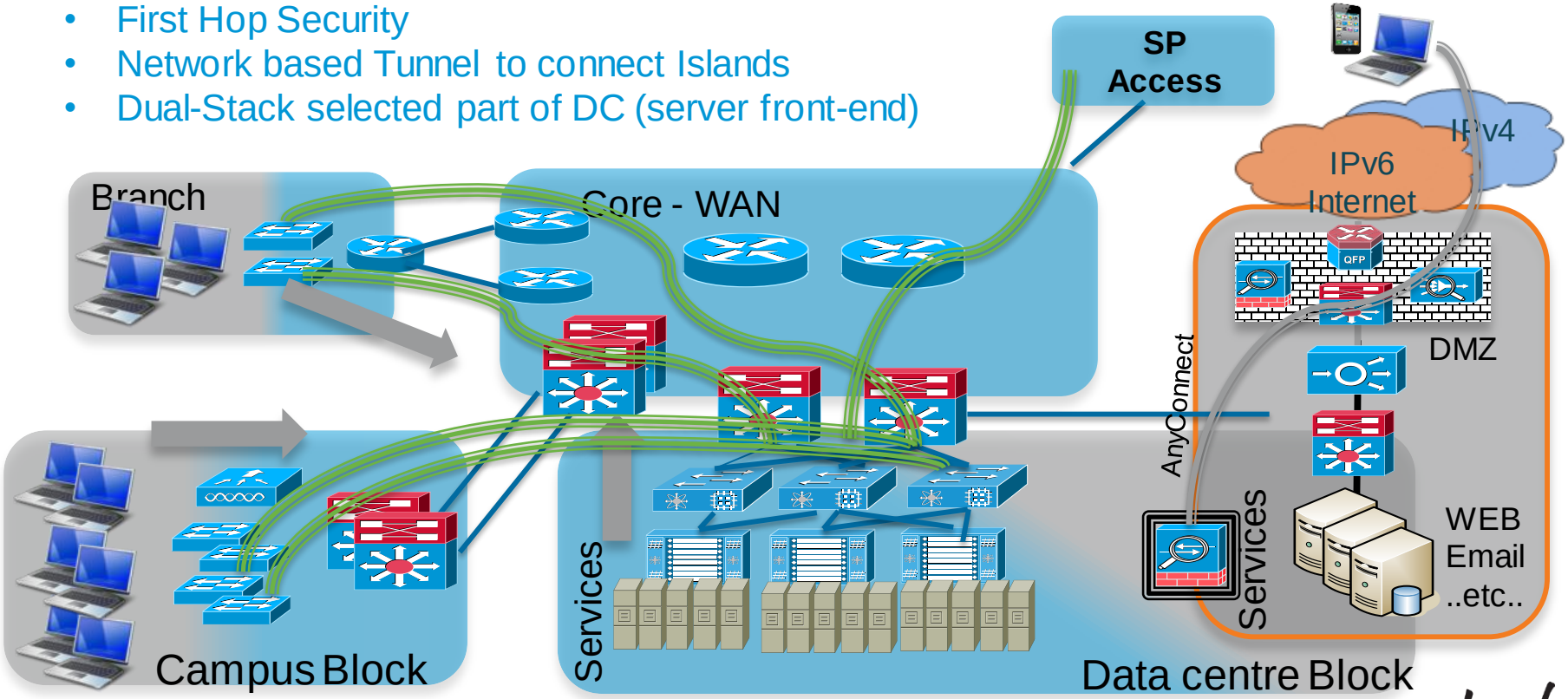


© 2015 Cisco and/or its affiliates. All rights reserved.

Edge to Core!

End User and Service first - Challenging but Doable

- First Hop Security
- Network based Tunnel to connect Islands
- Dual-Stack selected part of DC (server front-end)

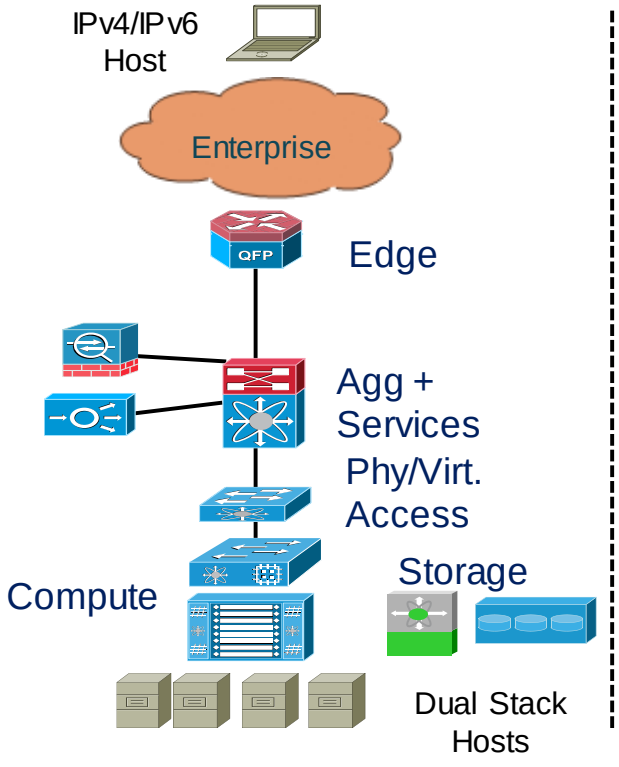


© 2015 Cisco and/or its affiliates. All rights reserved.

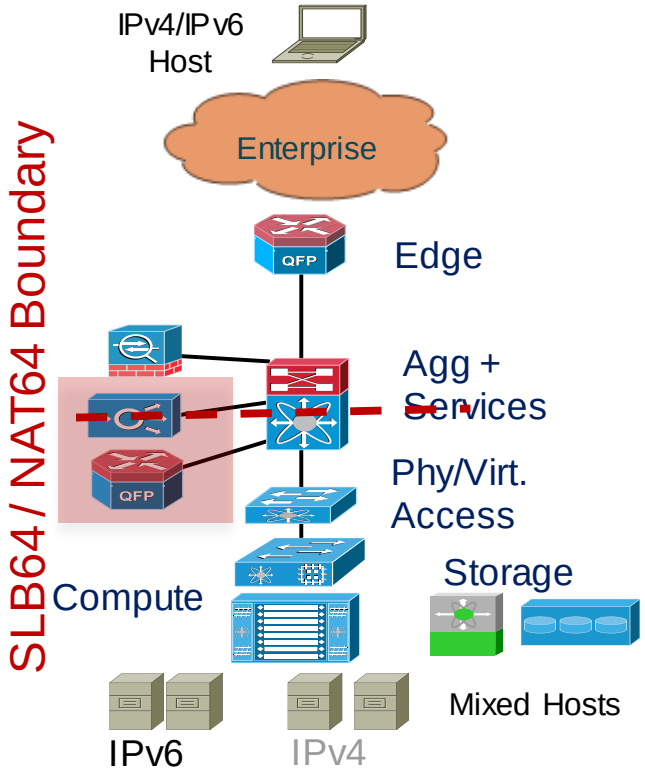
Common Deployment Models for Internet Edge

Internet, Partner, Branch

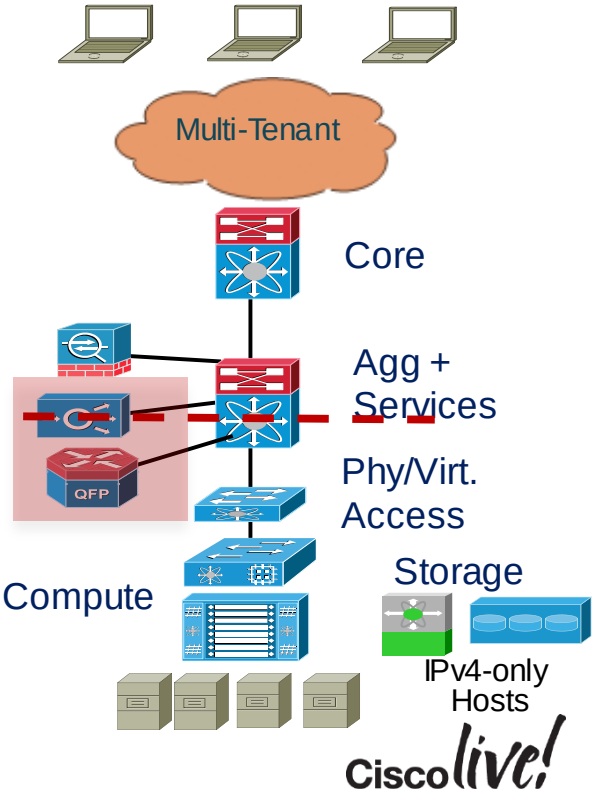
Pure Dual Stack



Conditional Dual Stack



Translation as a Service



© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Assessment

Cisco live!

Readiness Assessment

- A key and mandatory step to evaluate the impact of IPv6 integration
- Should be split in several phases
  - Infrastructure – networking devices and back end systems (OSS, BSS)
  - Hosts, Servers and applications
- Must be as complete as possible to allow upgrade costs evaluation and planning
  - Hardware type, memory size, TCAM size and dependencies, interfaces, CPU load,…
  - Software version, features enabled, license type, forwarding path, known limitations, best practices, etc.
- Difficult to complete if a set of features is not defined per device's category for a specific environment
  - IPv6-capable definition, knowledge of the environment and applications, design goals
  - Because I have it today does not mean I need it tomorrow
- Break Network into Places in the network for a more accurate assessment
  - Should Map directly into your IPv6 Network Architecture strategy, Cost analysis and time lines

© 2015 Cisco and/or its affiliates. All rights reserved.

Assessment Example

- Break the project down into phases – Avoids false positives and cuts back on upgrade costs
- Determine place in the network (PIN), platforms, features that are needed in each phase
- Work with your vendor to address the gaps

	ISR G1/G2	ASR 1000	6500 (Sup 720)	3750
Phase I (Initial Deployment - Infrastructure Only)				
IPv6 Neighbor Discovery	12.2(2)T	12.2(33)XNA	12.2(17a)SX1	12.2(25)SEA
IPv6 Address Types— Unicast	12.2(2)T	12.2(33)XNA	12.2(17a)SX1	12.2(25)SEA
ICMPv6	12.2(2)T	12.2(33)XNA	12.2(17a)SX1	12.2(25)SEA
EIGRPv6	12.4(6)T	12.2(33)XNA	12.2(33)SXI	12.2(40)SE
SSH	12.2(8)T	12.2(33)XNA	12.2(17a)SX1	12.2(25)SEE
Phase II (Internet Edge Enablement)				
Multiprotocol BGP Extensions for IPv6	12.2(2)T	12.2(33)XNA	12.2(17a)SX1	-
NetFlow for IPv6 Unicast Traffic	12.3(7)T	12.2(33)XNC	12.2(33)SXH	-
RFC 4293 IP-MIB and RFC 4292 IP-FORWARD-MIB (IPv6 Only)*	15.1(3)T	12.2(33)XNA	12.2(50)SY	12.2(58)SE
IPv6 over IPv4 GRE Tunnels	12.2(4)T	12.2(33)XNA	12.2(17a)SX1	-
NAT64 - Stateful	-	15.1(3)S	-	-
Phase III (Access Edge Enablement)				
IPv6 RA Guard	-	-	12.2(33)SXI4	-**
HSRP for IPv6 (HSRPv2)	12.4(4)T	15.1(3)S	12.2(33)SXI	12.2(46)SE
HSRP Global IPv6 Address	-	-	12.2(33)SXI4	-
DHCPv6 Relay Agent	12.3(11)T	-	12.2(33)SXI	12.2(46)SE
* Must include HW switched packets				
** 12.2(46)SE does support PACL				

© 2015 Cisco and/or its affiliates. All rights reserved.

Commonly Deployed IPv6-enabled OS/Apps

Operating Systems

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

Virtualisation & 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 that are difficult

© 2015 Cisco and/or its affiliates. All rights reserved.

Coexistence Strategy

Don’t Forget the Applications

While infrastructure is everyone’s initial focus, nothing happens until the applications use the new API. IPv4-only apps will remain IPv4-only, and these legacy apps will fail when presented with an IPv6-only infrastructure.

Line Number : 39 *Type :STRUCTURE*
Name: sockaddr
Migration Tip: 1. If you are using struct sockaddr to allocate storage, you need to change sockaddr to sockaddr_in6

© 2015 Cisco and/or its affiliates. All rights reserved.

What Defines an Application?

What about these

HTTP	→	80
FTP	→	20/21
POP3	→	110
IMAP	→	143
HTTPS	→	443
SMTP	→	25

Are these applications?

Or just ports?

IPv4/IPv6 transport

Are These Applications

Cisco live!

Questions to Ask Your Service Provider

- http://docwiki.cisco.com/wiki/What_To_Ask_From_Your_Service_Provider_About_IPv6

- **SP Deployment Type**
  - Dual Stack, Native or Overlay (if so what kind of overlay) ?
  - What kind of SLA are provided for the services ? Do you post metrics online ?
- **What kind of services are offered**
  - Internet Services
  - Layer 2 or Layer 3 VPN's
  - IPv6 Multicast support or plans ?
  - DNS Services over v4 or V6 ?
- **Visibility and footprint to the IPv6 Internet**
  - Peering arrangements
- **Service availability on nodes**
- **Acceptance Policy**
  - Prefix length acceptance?
  - Provider Independent or Provider Assigned acceptance
  - Do your Peering partners have similar policy to yours?
  - What prefix length do your upstream providers accept ?
- **Provisioning**
  - Is there a self service portal ?
  - Routing add and deletes
  - When do you plan on providing v6 services as a default offering ?
- **Charging model**

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv4 Address Assessment

- Assess how the existing IPv4 address space is used
- Useful information for
  - IPv6 integration
  - IPv4 address consolidation
  - Reclaiming unused address space
- Use existing tools
  - IPAM
  - ARP tables
  - Routing tables
  - DHCP logs

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Addressing

Cisco live!

IPv6 Address Considerations

- Many ways of building an IPv6 Address Plan
  - Regional Breakdown, Purpose built or Generic buckets, Separate per business function
  - Hierarchy is key
  - Don't worry too much about potential inefficiencies

- Prefix length selection
  - Network Infrastructure links, Host/End System LAN

- Addressing hosts
  - SLAAC, DHCP (stateful), DHCP (stateless), Manually assigned

- Building the IPv6 Address Plan
  - Cisco IPv6 Addressing White Paper

    http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_IPv6AddressingGuide-Feb2013.pdf

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Address Space - PI vs PA

- Do I Get PI or PA?
  - PI space is great for organisations who want to multihome to different SPs
  - PA if you are single homed or you plan to NAT/Proxy everything with IPv6 (not likely)

- Possible Options for PI
  - Get one large global block from local RIR and subnet out per region
  - Get a separate block from each of the RIR you have presence in

- Which route to go ?
  - Depends on specific business case
  - Enterprise that have a heavy consumer interaction using a block from each RIR will help avoid DNS and routing hacks to lead clients to regional Data Centres

- Most organisations are going down the PI path
  - Getting assignments across regional registries provides “insurance” against changing policies
  - Traffic Engineering

© 2015 Cisco and/or its affiliates. All rights reserved.

PI Space Concerns

- Concerns around prefix announcement from other regions
  - Will providers accept prefixes from other regions?
- Concerns around prefix lengths
  - What length prefix will providers accept?
  - How do I do traffic engineering?
  - What about providers upstream peers?
- Bottom line is to have a detailed conversation w/ your provider or peering partner about what their policies are
  - http://www.us.ntt.net/support/policy/routing.cfm#v6PeerFilter

© 2015 Cisco and/or its affiliates. All rights reserved.

Infrastructure - Type of Address

- Global Unicast vs. Unique Local Address for Infrastructure

Global Unicast Address	Unique Local Address (ULA)
Use of Global address space – requiring a registered address block	Free – you could use FC00::/8 or FD00::/8
No need for Address translation or Proxy for host trying to reach to Internet	Requires translation from Private to public address – there is no scalable translation solution giving V4 type NAT/PAT
Operationally Simplistic because managing only one type of space	Management becomes complicated – have to manage private and public spaces
Could gain the same security as using ULA, if filtering is done correctly at the edge	No Security benefit of using Private space – the infrastructure could still get under attack if optimal security not in place at the Edge
Global Reachability means even connectivity to islands spread out connected via Internet	No Global reach meaning islands connected over Internet have to be administered in isolation

Recommendation: Use Global Unicast Addresses

© 2015 Cisco and/or its affiliates. All rights reserved.

P2P Links IPv6 Address Selection

/64	/126	/127
Ping Pong could occur if a packet sent to an un-specified address	Theoretically Optimal but still could result in a ping pong loop	Old RFC 3627 and 5375 recommends using against /127 due to Subnet-Router anycast but newer RFC 6164 Recommends using /127
Common use with overall consistency to other LAN blocks – IOS devices have a fix for Ping pong loops	Common use keeping IPv4 type of conservation mentality – IOS devices have a fix for Ping pong loops	Cisco devices disables Subnet-Router Anycast upon configuration of a /127 address
Also, mandated by RFC 4443 to send a Code 3 Destination Unreachable message to the neighbour router	Also, mandated by RFC 4443 to send a Code 3 Destination Unreachable message to the neighbour router	Most vendor equipment does not use subnet-router anycast
Use this style, if operational focus to keep the same length across the board	Use this style, if operational focus to keep the v4 /30 type addressing semantics	Use this style, if operational focus to keep the v4 /31 type addressing semantics

Recommendation: Use what makes sense within the context of your organisation

© 2015 Cisco and/or its affiliates. All rights reserved.

Host Address Assignment

	Manual	Stateless	DHCPv6
Pros	Address is stable Controlled assignment Well understood process	Scales well Time to deploy Widely implemented	Well understood process Controlled assignment Time to deploy
Cons	Does not scale Time to deploy	No control on assignment process Not well understood Lack of management Privacy concerns	Implementation in OS Must design for HA

- The choice of assignment depends on the existing processes and the adaptability of that process
- Remember that the methods are not mutually exclusive - all three can be used
- Regardless of choice must still control the stateless address assignment of addresses

© 2015 Cisco and/or its affiliates. All rights reserved.

Managing the Host Address Space

- Multiple address per host
  - Does your address identify you?
- Stateless vs Stateful
  - SLAAC
  - Privacy extensions
  - DHCP
  - Manual
- ND cache management
  - Scaling
  - Security
  - Host address selection

```
Wireless LAN adapter Wireless Network Connection:
   Connection-specific DNS Suffix  .
   Link-local IPv6 Address . . . . . : fe80::417d:2cea:988d:8324%11
   IPv4 Address. . . . . . . . . . . : 10.150.45.54
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : fe80::5:73ff:fea0:3e9%11
                                       10.150.44.1
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . : cisco.com
   IPv6 Address. . . . . . . . . . . : 2001:420:XXXX:1340:d5cd:e500:46ab:4
   Link-local IPv6 Address . . . . . : fe80::75bc:440a:7aa0:6741%10
   IPv4 Address. . . . . . . . . . . : X.X.X.X
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::208:e3ff:feff:fd90%10
                                       64.X.X.X
Tunnel adapter Teredo Tunneling Pseudo-Interface:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Tunnel adapter isatap.{DFF94FEB-3836-409C-A354-917C0251536E}:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Tunnel adapter isatap.cisco.com:
   Connection-specific DNS Suffix  . : cisco.com
   Link-local IPv6 Address . . . . . : fe80::5efe:10.x.x.x%23
   Link-local IPv6 Address . . . . . : fe80::200:5efe:x.x.x.x%23
   Default Gateway . . . . . . . . . :
```


© 2015 Cisco and/or its affiliates. All rights reserved.

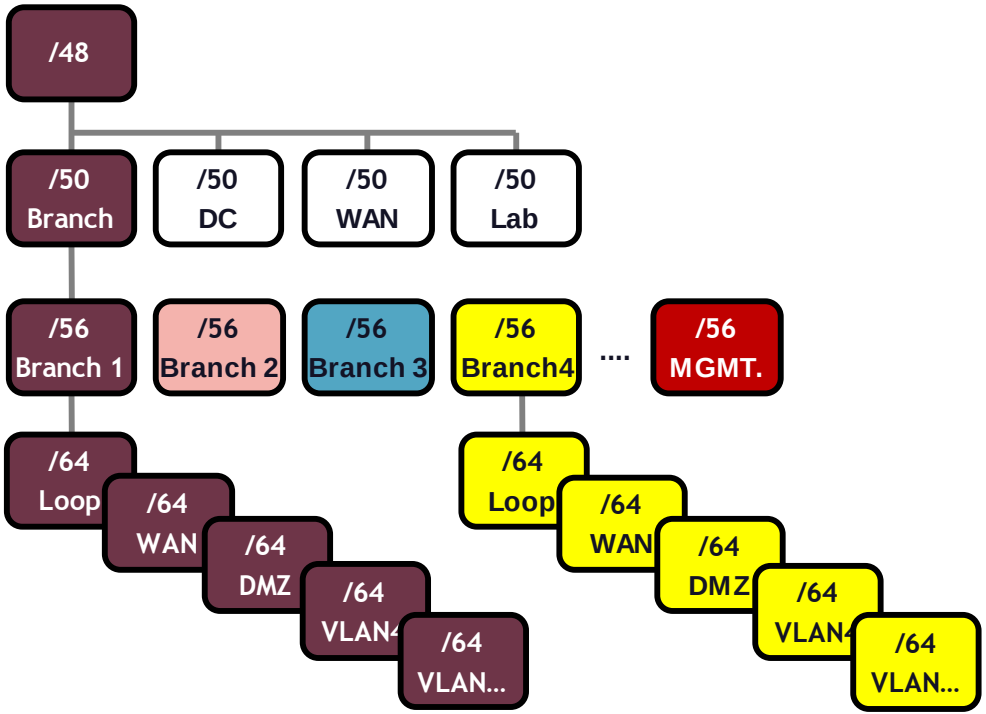
What about NAT?

- A couple of versions of address translation related to IPv6
  - NAT-PT
    Original specification
    Deprecated
  - NPTv6
    Stateless translation method
    Only manipulate the prefix
  - NAT66
    Stateful translation
    Not specified in RFC
  - NAT64
    Translation between IPv6 and IPv4 address families
    Stateless and stateful methods available

- Where should NAT be applied?
  - NAT66
    Address hiding ???
    That's the way we do IPv4???
    It provides security???
    Stateful tracking???
    Multi-homing
  - NAT64
    Boundaries between IPv4 only and IPv6
    Highly successful in getting quick IPv6 access
    Cannot be the final state
    Must move towards full IPv6 integration

© 2015 Cisco and/or its affiliates. All rights reserved.

/48 Prefix Breakdown Example



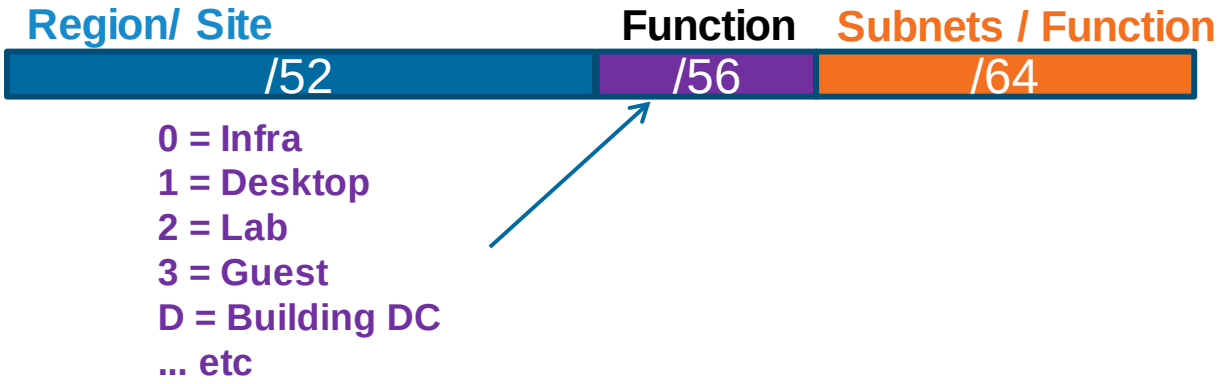
- High Level addressing plan. Indicative only. Can be modified to suit needs
- /48 = 65536 x /64 prefixes
- Break up into functional blocks (4 x /50 in this case)
- Each functional block simplifies security policy
- Assumes up to 64 Branch networks
- Each Branch has access to 256 /64 prefixes for WAN, DMZ, & VLAN use

© 2015 Cisco and/or its affiliates. All rights reserved.

Address Plan Example

2001:db8:1000::/40 ARIN assigned block
~16 million /64 subnets
2001:db8:1000::/64 -> 2001:db8:10ff:ffff::/64
2001:db8:10X0::/44 Regional assigned block
16 Regions
2001:db8:1010::/44 -> 2001:db8:10f0::/44

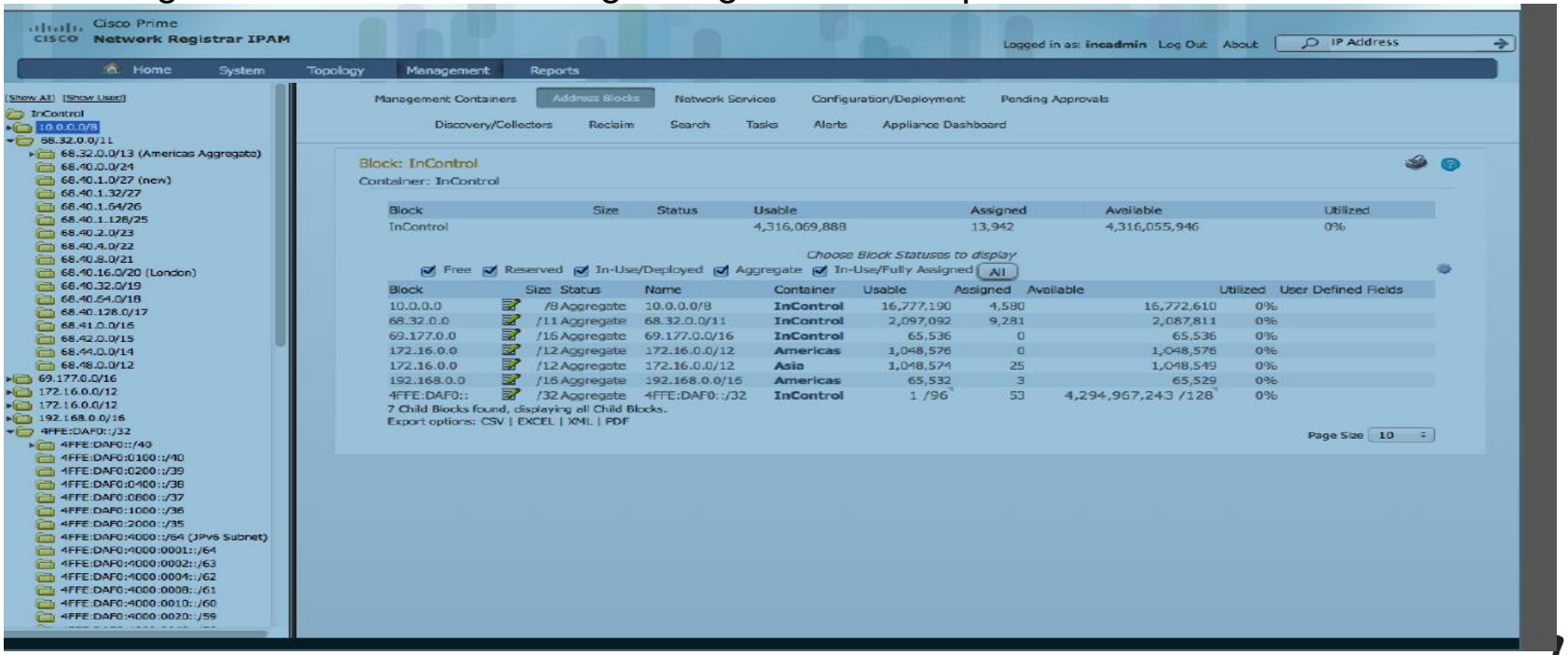
2001:db8:101Y:Y000::/52 - Site assigned block
256 Sites in a region
2001:db8:1010:0000::/52 -> 2001:db8:101f:f000::/52
2001:db8:1011:01Z0::/56 - Site functional blocks
256 subnets per site
2001:db8:1011:1111::/64 Desktop VLAN x
2001:db8:1011:1112::/64 Desktop VLAN y



© 2015 Cisco and/or its affiliates. All rights reserved.

Importance of IP Address Management Tools

- Spreadsheets do not scale and are not auditable
- Tools should allow customers to manage IP address space consistent with their management methods. Having a single source helps.

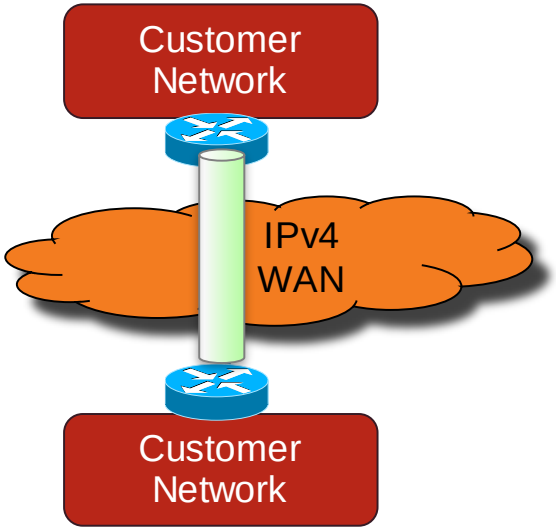


© 2015 Cisco and/or its affiliates. All rights reserved.

Transition Mechanisms

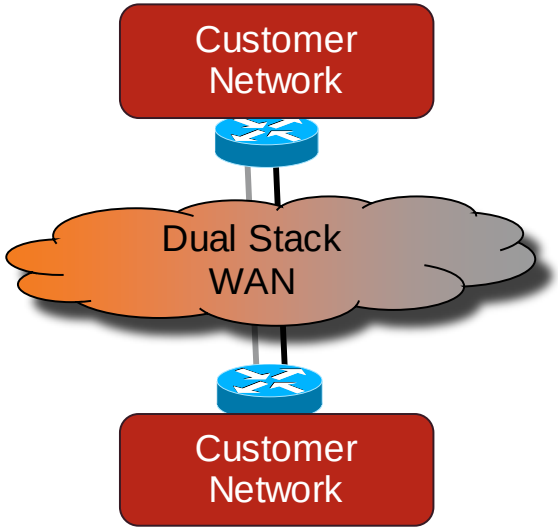
Cisco live!

Connecting IPv6 Sites Together



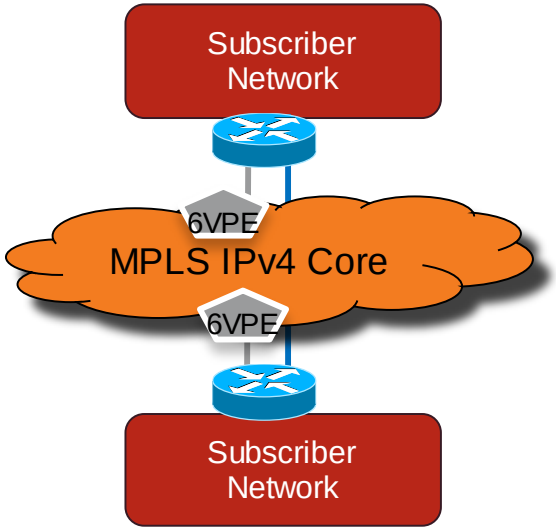
Using Tunnels

- Manually configured tunnels
- IPv6 over GRE
- LISP
- IPSec Tunnels
- Dynamic Multipoint VPN (DMVPN)



Dual Stack IPv4/IPv6

- Dual Stack CPEs
- Dual Stack Headquarters
- Dual Stack WAN



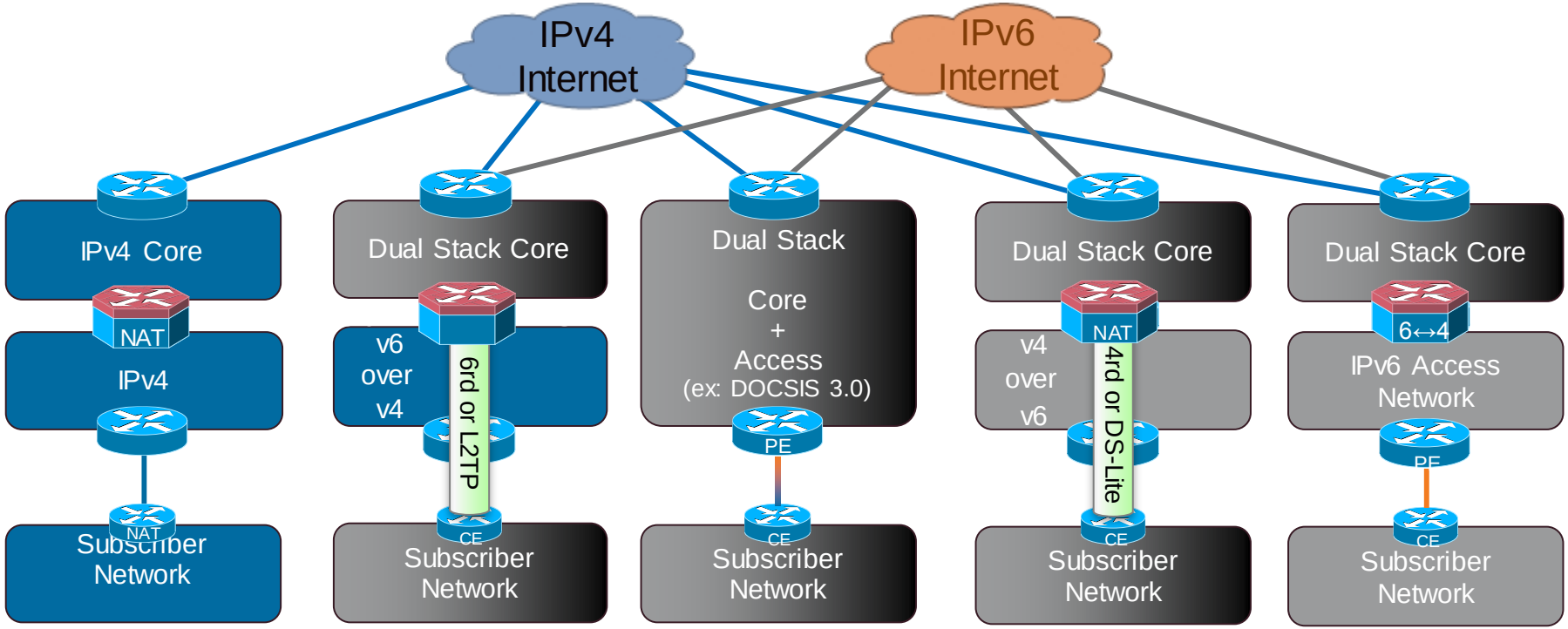
6VPE Service

- Dual Stack IPv4 / IPv6
- 6VPE VPN Service

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

SP IP Network Transition Options



NAT444

6 Rapid Deployment (6rd
L2TP
Softwires

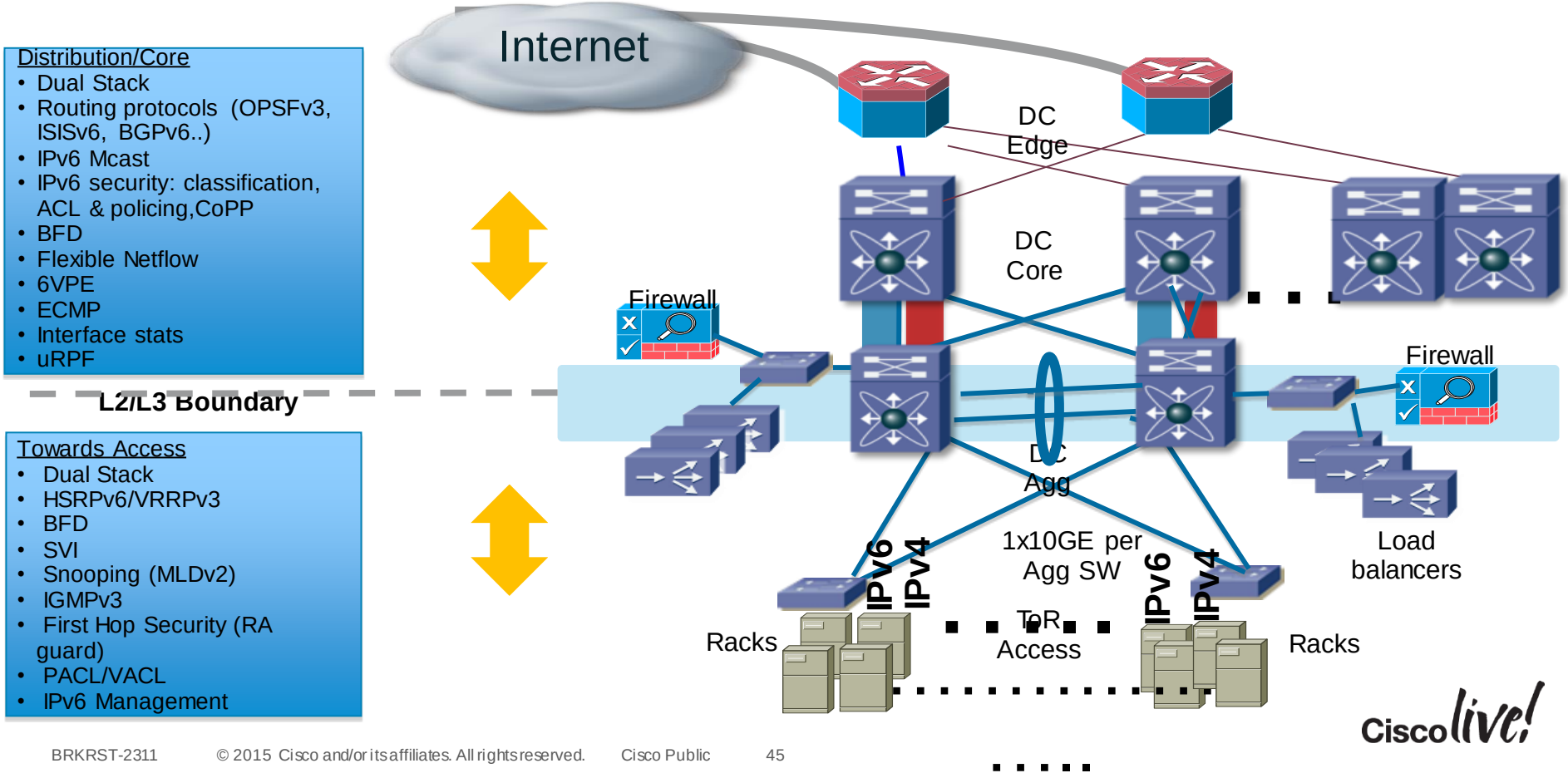
Broad Band Connectivity
Dual Stack Core
DOCSIS Access

IPv4 via IPv6
Using DS-Lite (w/NAT44)
MAP-E – Encap All
MAP-T - L3 and L4 in header
Lw4over6
4rd
464Xlat

AFT64

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Data Centre Network Architecture

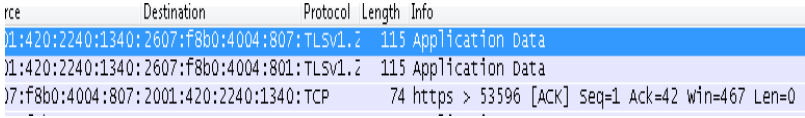


© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 and Cloud Adoption Consideration

- Contiguous large blocks of IPv4 not available
  - **Impact traffic engineering**
  - **Introduces complexities of NAT once again**
  - **Impacts end to end authentication**
- **Platform and Designs typically built around IPv4 including Scale, network management, visibility ..**
- **Most Cloud Consumption offers, tools are typically looking at IPv4**
  - **Traffic, Risk, Content - What is being missed especially from a Risk perspective ?**
- **A very large percentage of DNS queries are also handing out A and AAAA records**
  - **What is being consumed,**
  - **What happens when I need to move a work load and have missed my IPv6 communication between two devices**

- **Incorporate IPv6 into your cloud strategy –**
  - **Better scalability, address aggregation**
  - **Portolio for NFV and Service Chaining should include IPv6**
  - **Keep an eye out for Open Stack functions and IPv6 support.**
    - **Typically supported however caveats with the various implementations**



© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 in the Cloud

- Private, Hybrid or Public: they all need IPv6 to reveal the full potential of the resources
- What has been the hold up?
  - LARGE number of moving parts
  - Proprietary software systems have lagged behind on full IPv6 support slowly catching up depending on release (VMware vSphere prior to 5.x, etc..)
  - Open Source Cloud solutions have not prioritised IPv6
    - OpenStack is still lacking robust IPv6 support as of the Juno (Nov. 2014) release
    - Large effort to close gaps in Kilo (April/May 2015)
  - Provider may Support IPv6
    - What about Native API Integration ?
    - Address block allocation ? Yours or their ?
    - Native ? ULA ? Prefix Translation ?

© 2015 Cisco and/or its affiliates. All rights reserved.

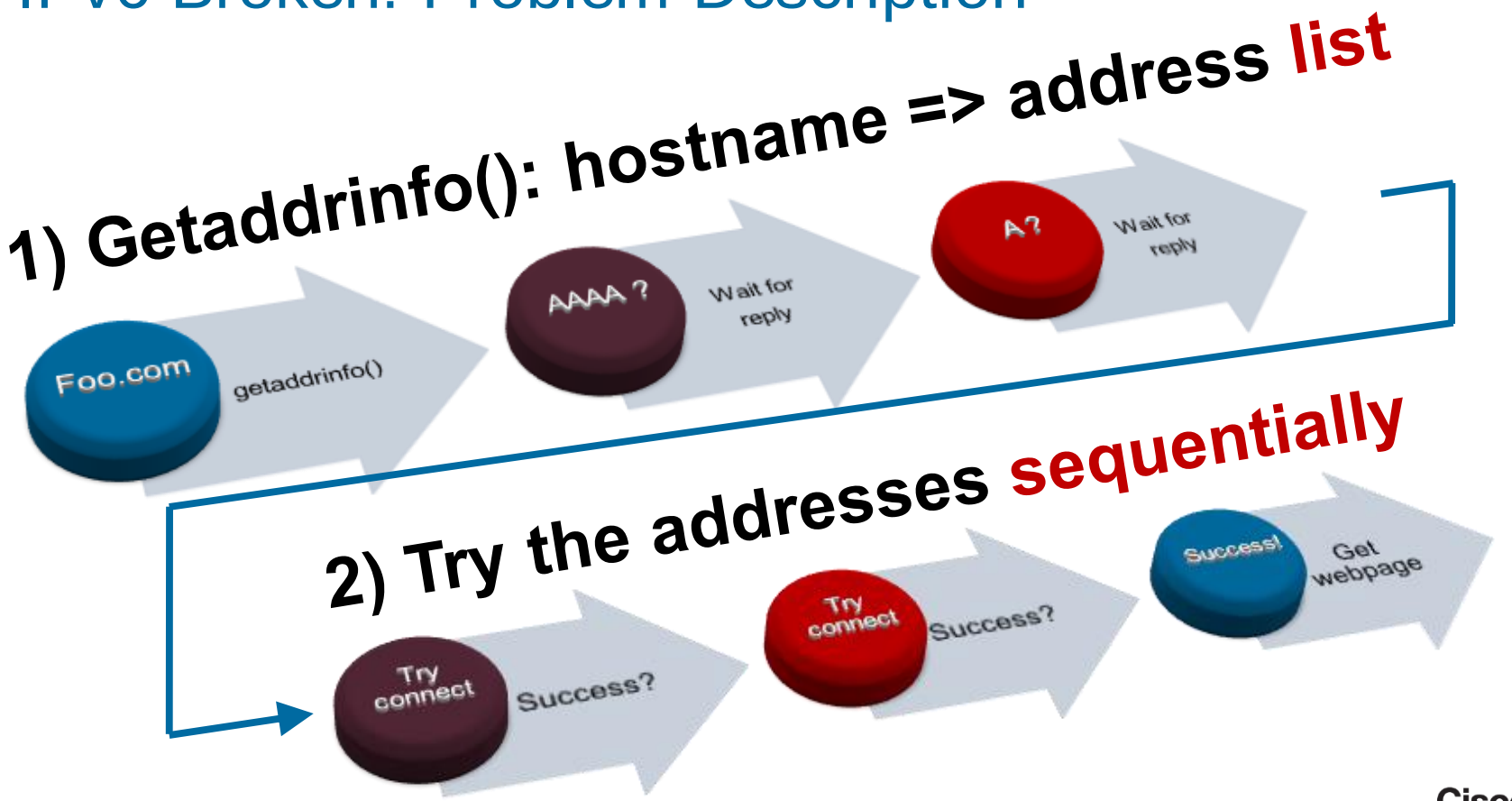
Cisco live!

Dual Stack Affecting IPv4 Applications

- Slowness because of IPv6 Path brokenness
  - Need registry fix to override the default behaviour to chose IPv6 stack
  - Happy Eyeballs
- Embedded IPv4 addresses
- Path MTU
  - Fragmentation and Reassembly… adds latency.
- Address representation and logging
  - Scripts that match on address
  - IP Address Logging - Database Structure: Is the database is structured to accommodate the IPv6 addresses?

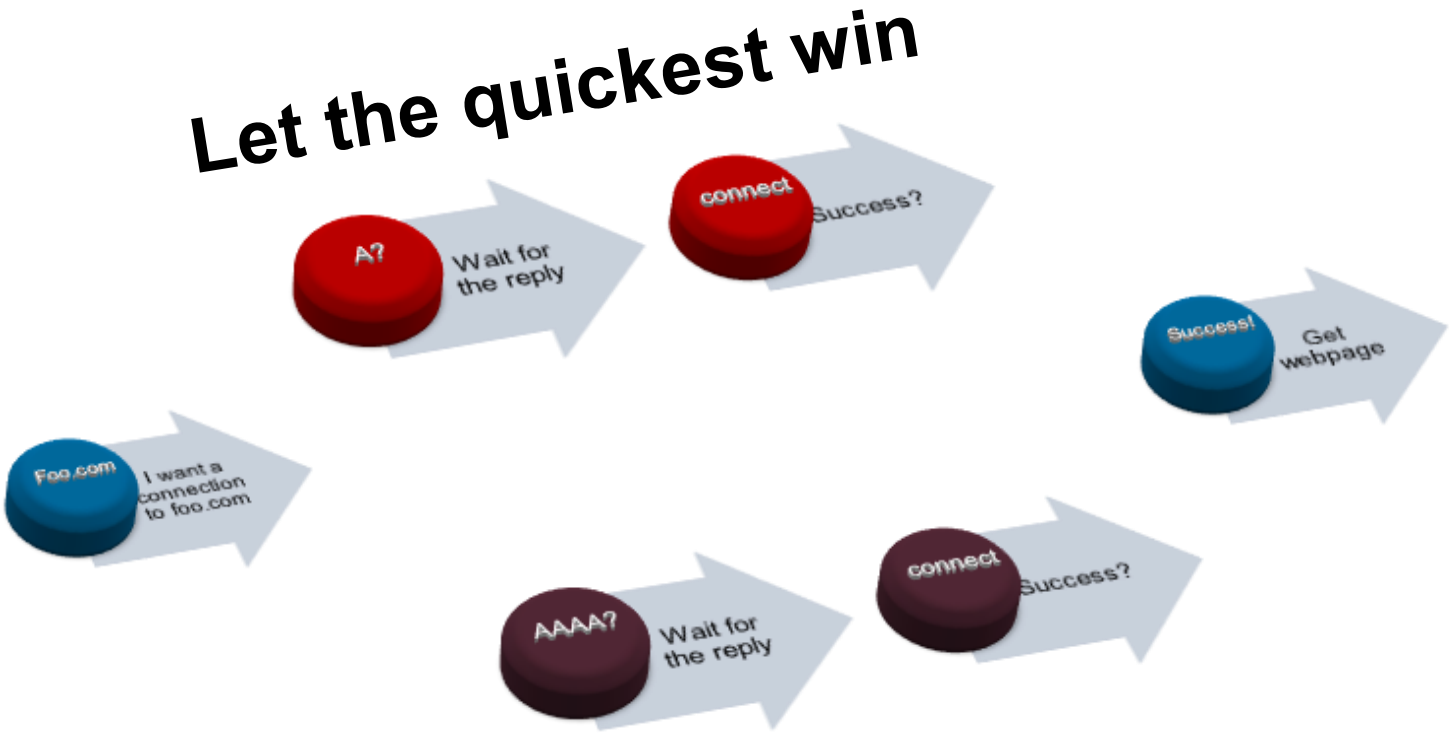
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPv6 Broken: Problem Description



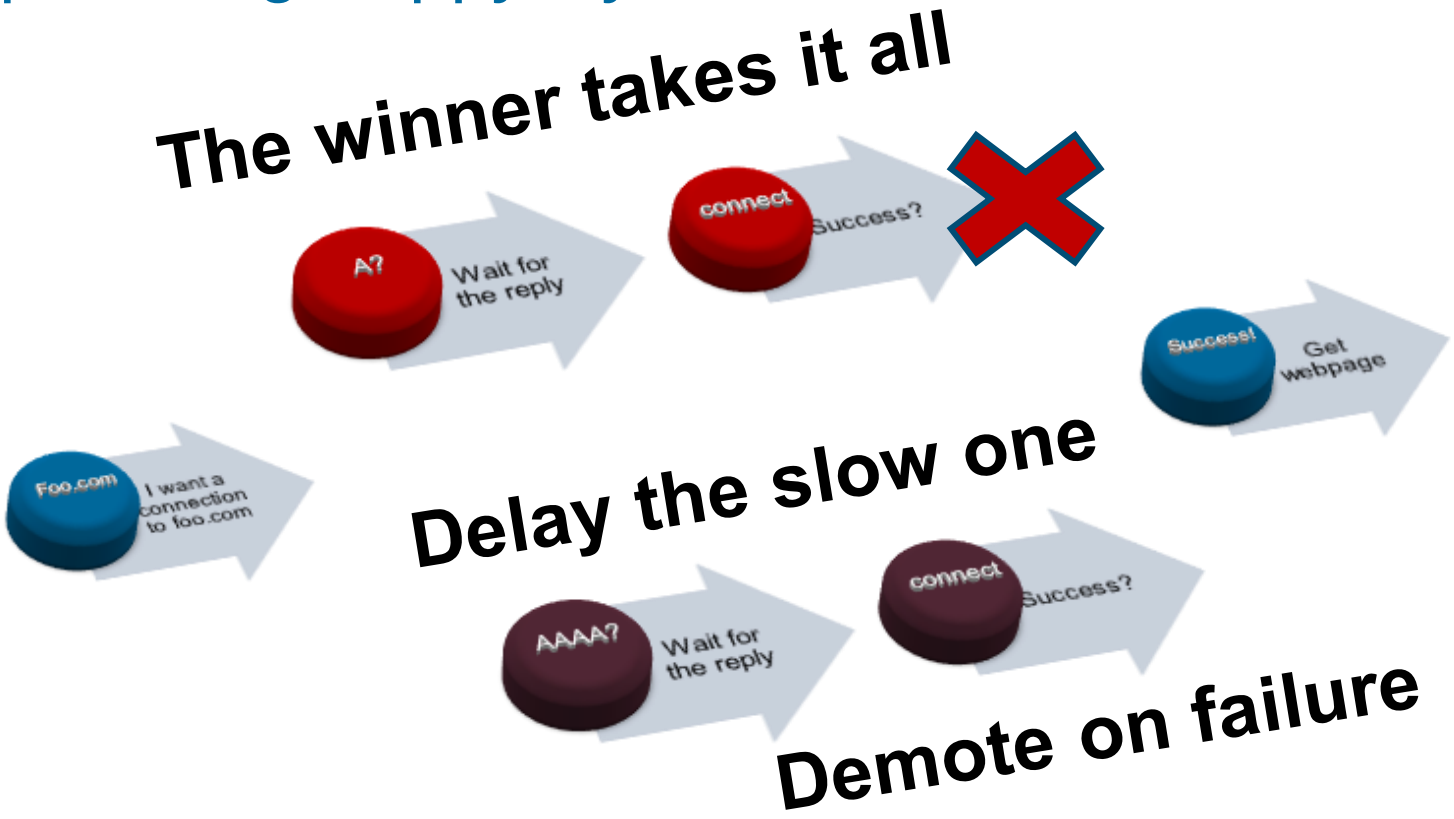
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Happy Eyeballs Solution



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Optimising Happy Eyeballs



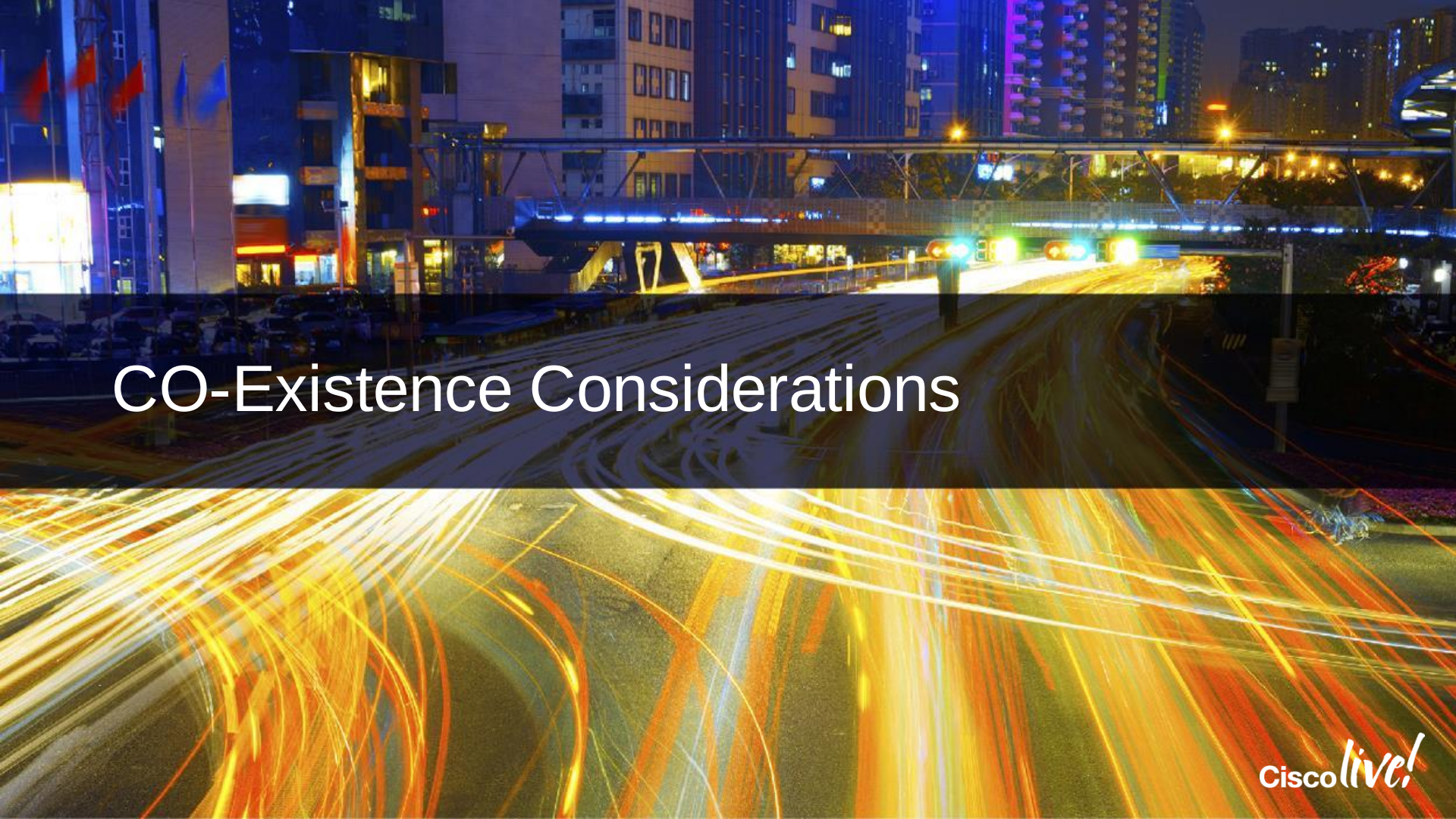
© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Happy Eyeballs

- Aimed initially at web browsing
  - Web browsing is *the* most common application
- Users are happy – fast response even if IPv6 (or IPv4) path is down
- Network administrators are happy
  - Users no longer trying to disable IPv6
  - Reduces IPv4 usage (reduces load on CGN)
- Content providers are happy
  - Improved geolocation and DoS visibility with IPv6

- RFC6555 (formerly draft-ietf-v6ops-happy-eyeballs)
  - By Dan Wing and Andrew Yourtchenko

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public



CO-Existence Considerations

Cisco live!

IPv4 and IPv6 Co-existence

	Single Process / Single Topology	Single Process / Multi Topology	Multi Process / Multi Topology
Protocols	IS-IS ST	IS-IS MT	OSPFv2 + OSPFv3 EIGRP + EIGRPv6
IP topologies	Single (IPv4+IPv6) Congruent	Multiple Non-congruent	Multiple Non-congruent
Flooding + router/network resources	Common	Common	Multiple protocol instances on given link
SPF	Single	Multiple	Multiple (OSPF)
LS databases / topology tables	Single Large	Single Large	Multiple
Control plane	- Common - Less resource intensive - More deterministic IPv4/IPv6 co-existence	- More separation - Protocol-specific optimisation possible - More resource intensive	- Clear separation - Protocol-specific optimisation possible - More resource intensive

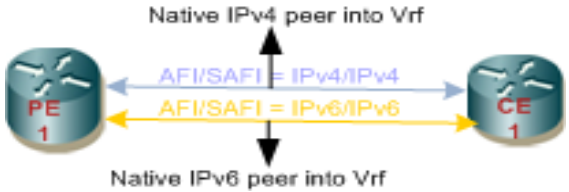
For Your Reference

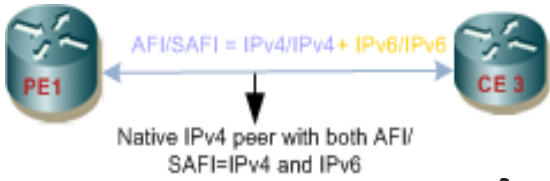
© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

IPv6 PE to CE E-BGP Peering Options

- Separate BGP peering whenever possible
  - Keep V4 and V6 Prefix exchange independent
  - Ships in the night easier for troubleshooting and resolution
- If required both IPv4/IPV6 Address-families can be established over IPv4 peer.
- Depending on implementation and next hop – I.E. peering with link local address may require in and outbound route-maps to manually set next hops





© 2015 Cisco and/or its affiliates. All rights reserved.

Scalability and Performance

- IPv6 Neighbour Cache = ARP for IPv4
  - In dual-stack networks the first hop routers/switches will now have more memory consumption due to IPv6 neighbour entries (can be multiple per host) + ARP entries

ARP entry for host in the campus distribution layer:

```
Internet  10.120.2.200                  2       000d.6084.2c7a  ARPA  Vlan2
```

IPv6 Neighbor Cache entry:

```
2001:DB8:CAFE:2:2891:1C0C:F52A:9DF1   4       000d.6084.2c7a  STALE Vl2
2001:DB8:CAFE:2:7DE5:E2B0:D4DF:97EC   16      000d.6084.2c7a  STALE Vl2
FE80::7DE5:E2B0:D4DF:97EC             16      000d.6084.2c7a  STALE Vl2
```

- There are some implications to managing the IPv6 neighbour cache when concentrating large numbers of end systems

© 2015 Cisco and/or its affiliates. All rights reserved.

Co-existence

Co-Existence

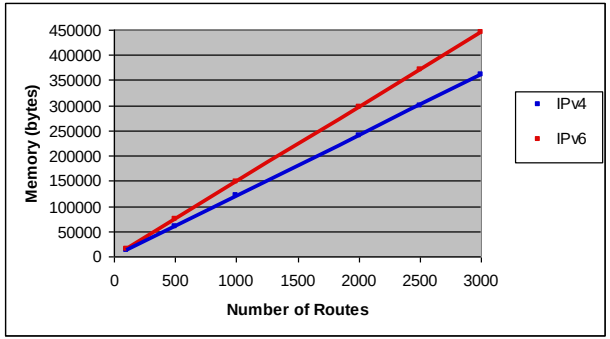
- IPv6 Router Advertisement
  - Disable when not needed
  - Router Advertisement can be risky – i.e. if you do not want to auto configure existing servers without control or knowledge
  - Recommend RA Guard whenever possible
- Over time as new operating systems come on line it will be harder to identify "IPv6" issues. Most folks do not know Ipv6 is running in their network specifically in the same LAN segment
- Management of SLA or Network Management of a device. Yes it is reachable over IPv4 for both stacks. However, still need to ensure IPv6 connectivity
- Understand host behaviour when multiple addresses are present. Saves time during testing and implementation at time expected address is not being used.
  - http://tools.ietf.org/html/rfc6724 is the authoritative source for implementations
  -

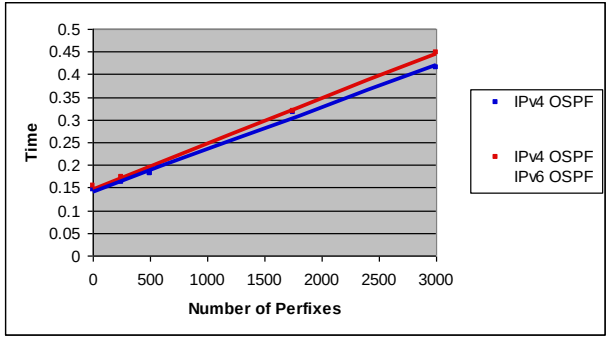
© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Understanding Co-Existence Implications

- **Resources considerations**
  - **Memory (storing the same amount of IPv6 routes requires less memory than might be expected)**
  - **CPU (insignificant increase in the case of HW platforms, additive in the case of SW platforms)**
- **Control plane considerations**
  - **Balance between IPv4/IPv6 control plane separation and scalability of the number of sessions**
- **Performance considerations**
  - **Forwarding in the presence of advanced features**
  - **Convergence of IPv4 routing protocols when IPv6 is enabled**

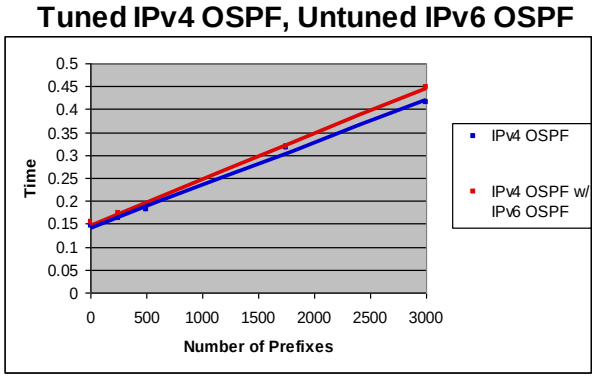


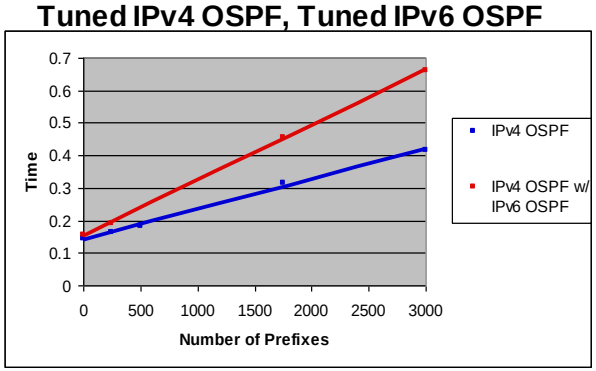


© 2015 Cisco and/or its affiliates. All rights reserved.

The Coexistence Twist

- IPv6 IGP impact on the IPv4 IGP convergence
- Aggressive timers on both IGPs will highlight competition for resources
- Is parity necessary from day 1?

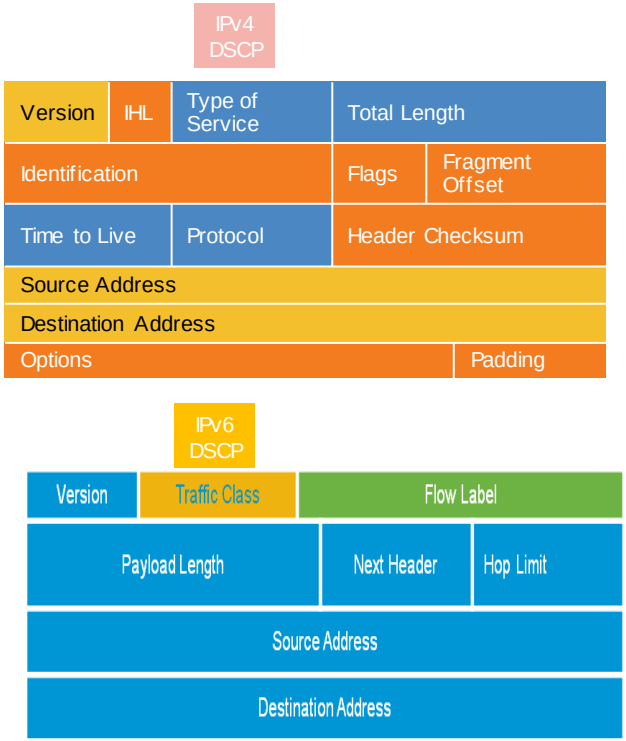




© 2015 Cisco and/or its affiliates. All rights reserved.

QoS Considerations

- IPv4 and IPv6 QoS features are mostly compatible (RFC 2460/3697)
- Both Transport uses DSCP (aka Traffic Class)
- Control plane Queues need to now take into account IPv6 Overhead too
- IPv6 classification can follow the same IP Precedence, Service Class, DSCP and EXP QOS Taxonomy values already defined for IPv4.
- CE devices will need additional configuration to set appropriate values on the IPv6 traffic class field.
- IPv6 will utilise the same Network Control, Voice,, Gold, Bronze, Silver, Best Effort classes



© 2015 Cisco and/or its affiliates. All rights reserved.

Management and Operations

Cisco live!

Don’t Forget About Network Management

Introduction of IPv6 creates new network management challenges

- Management and design strategies for IPv6 addressing model, policies and operation
- Introduction of extended IP services: DHCPv6, DNSv6, IPAM
- Managing security infrastructures: Firewall, IDS, AAA
- Tool visibility, insight and analysis of IPv6 traffic Netflowv9, IPv6 SLA
- Troubleshooting
  - IPv4-IPv6 interaction
- Requires support in
  - Instrumentation (MIB , Netflow records, etc.)
  - NMS tools and systems
- Dual Stack Interfaces will result in tools i.e. MRTG reporting combined v4 and V6 traffic statistics.

© 2015 Cisco and/or its affiliates. All rights reserved.

NetFlow for IPv6

- Application Performance monitoring is a great differentiator for IPv6
- IPv6 support added as part of Flexible NetFlow (metering) and NetFlow v9 (exporting) Monitors the IPv6 traffic.
- Export is over an IPv4 Transport
- Exporting: NetFlow version 9
  - Advantages: extensibility
    - Integrate new technologies/data types quicker (MPLS, IPv6, BGP next hop, etc.)
    - Integrate new aggregations quicker
  - Note: for now, the template definitions are fixed
- Metering: Flexible NetFlow
  - Advantages: cache and export content flexibility
    - User selection of flow keys
    - User definition of the records

© 2015 Cisco and/or its affiliates. All rights reserved.

Flexible NetFlow

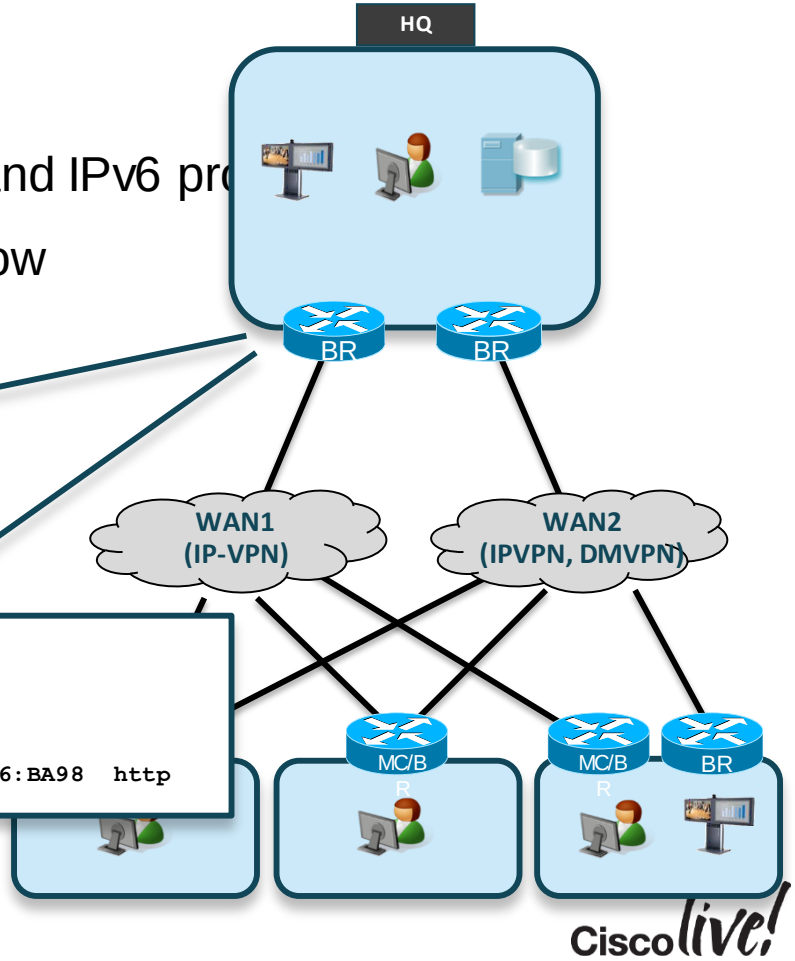
IPv6 Application Monitoring

- Configure traffic statistics collection for IPv4 and IPv6 pr
- IPv6 application reporting with Flexible NetFlow

```
flow record RECORD-FNF-v6
  match ipv6 source address
  match ipv6 destination address
  match application name
```

```
# sh flow monitor MONITOR-FNF-v6  cache format table

IPV6 SOURCE ADDRESS                          IPV6 DESTINATION ADDRESS
APPL NAME
2A01:E35:8ABF:9510:FA1E:DFFF:FEE1:E789   2A01:E35:8ABF:9510:222:55FF:FEE6:BA98  http
```



© 2015 Cisco and/or its affiliates. All rights reserved.

IPv4 and IPv6 Classification (Modified)

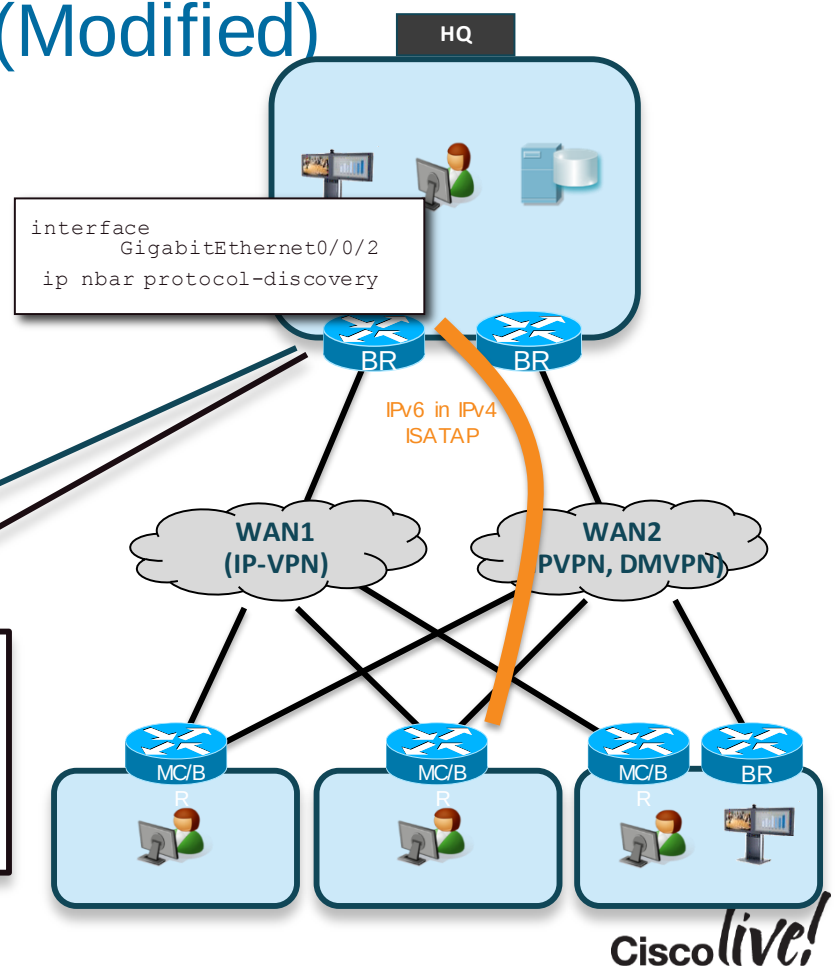
Protocol Discovery - NBAR 2

- Discover application protocols transiting an interface, and populate CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- Supports both input and output traffic
- Detection of IPv6 in IPv4 traffic (ISATAP, Teredo,6to4,..)
- Statefull application classification for IPv6 in IPv4 traffic

NBAR classifies this flow as “ISATAP” by default

With IPv6 tunnel inspection turn ON, NBAR classifies this flow as “HTTP”

```
interface Gi1/1
  ip nbar classification tunneled-traffic ?
              ipv6inip Tunnel type ISATAP, 6to4 and 6RD
              teredo   Tunnel type TEREDO
```



© 2015 Cisco and/or its affiliates. All rights reserved.

Troubleshooting Considerations

- Current process and procedures apply
  - Gather information
  - Break the problem down to isolate the issue
  - Look for what has changed
  - Is it Layer 1? Or a problem w/ the “cup holder”?
- But what about….
- Initial analysis of the problem
  - Can it be isolated to IPv4 or IPv6?
  - Is it host/server/application or network based?
  - Is everything dual stacked?
- There are differences
  - Neighbour discovery
  - Multiple addresses per device

```
Router#sh ipv6 int gig 6/2
GigabitEthernet6/2 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::208:20FF:FEF2:2C00 [UNA]
  Virtual link-local address(es):
    FE80::5:73FF:FEA0:0 [OOD]
  Global unicast address(es):
    2001:DB8::1, subnet is 2001:DB8::/64
    2001:DB8::1111, subnet is 2001:DB8::/64 [OOD/VIRT]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:1
    FF02::1:FF00:1111
    FF02::1:FFA0:0
    FF02::1:FFF2:2C00
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Output features: HW Shortcut Installation
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

IPV6 Testing Considerations

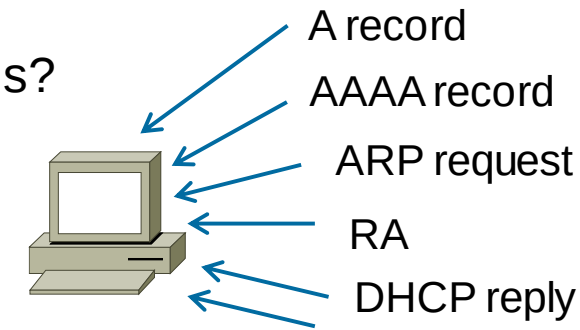
- Create base line template that should be run as part of all IPv6 solution testing.
  - Hosts/Servers/End Systems
  - Routers/Switches
  - Firewalls/IPS

- Template should consist of basic IPv6 RFC 2460 functionality.
  - IPv6 Ready Logo
  - USGv6
  - RIPE-554

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Testing Considerations

- How do hosts re-act to auto-configuration?
- Are devices taking both a static and auto-configuration ?
  - Understand so that security Policy is not affected?
- Should IPv6 RA's be disabled how do devices re-act to that?
- Does application being used implement SAS (Source address selection) algorithm correctly?
- How do devices re-act with A and AAAA DNS records?
- What happens if IPv4 is disabled?
- What happens if IPv6 is impaired?



© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Tools

- Different ways to check on what is happening
- Where's my prefix?
  - Route servers and looking glasses - http://www.bgp4.as/looking-glasses
- What's happening with traffic and adoption rates?
  - Cisco - http://6lab.cisco.com/stats/
  - Internet Society - http://www.worldipv6launch.org/measurements/
  - Google - http://www.google.com/ipv6/statistics.html
- Look at your network from the outside in
- Pings, traceroutes, SSLcert and DNS queries
  - https://atlas.ripe.net/results/

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

IPv6 DNS

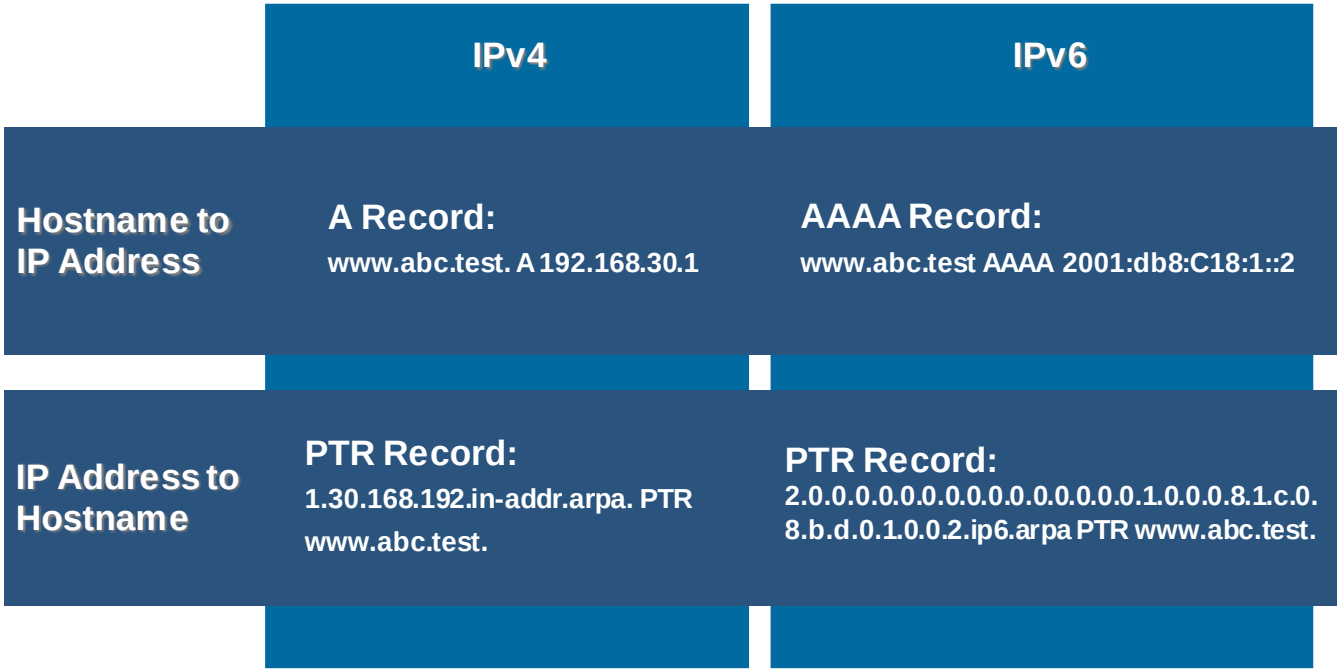
Cisco live!

Introduction to DNS and IPv6

- Introduction of IPv6, will require use both IPv4 &IPv6 addresses in your network
- Need to add mappings from names to IPv6 addresses in parallel with the existing mapping from names to IPv4 addresses
- One example of such a mapping, using the AAAA resource record type, is shown here:
  - www.ipv6.cisco.com. 86400 IN AAAA 2001:420:80:1::5
- Mapping from a name to an IPv6 address is performed using an AAAA resource record, with the IPv6 address given as a hexadecimal address (RFC 3596)

© 2015 Cisco and/or its affiliates. All rights reserved.

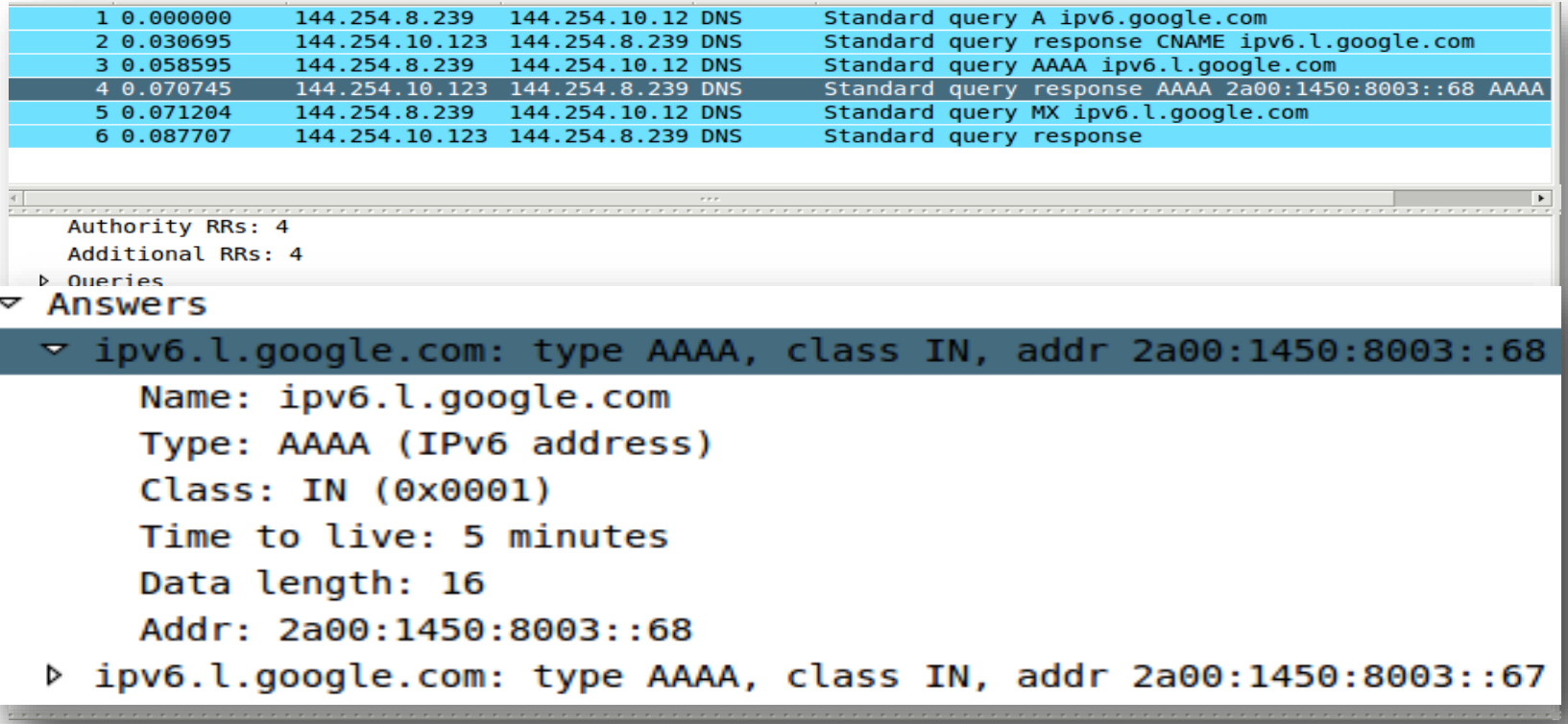
IPv6 and DNS



© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

AAAA Records on the Wire



© 2015 Cisco and/or its affiliates. All rights reserved.

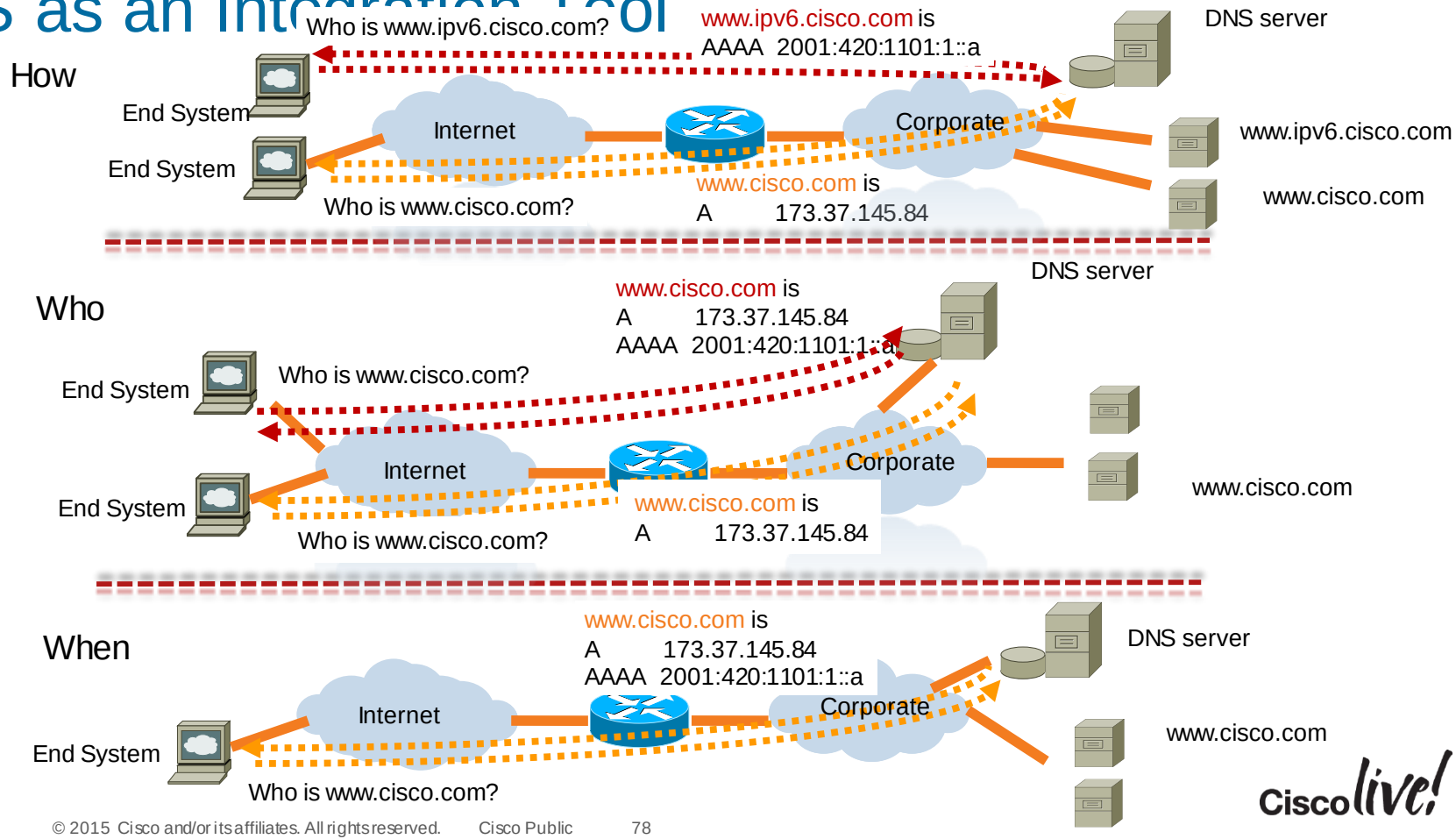
DNS as an Integration Tool

- DNS controls how people will access the application or service
  - Who wants to remember 2001:420:1101:1::a?
- Control when the service is available
  - AAAA record in DNS means service is available
- Control who receives the AAAA record
  - Whitelist who gets the AAAA response
- Control how the service is accessed
  - Separate domain

    ipv6.cisco.com vs cisco.com

© 2015 Cisco and/or its affiliates. All rights reserved.

DNS as an Integration Tool



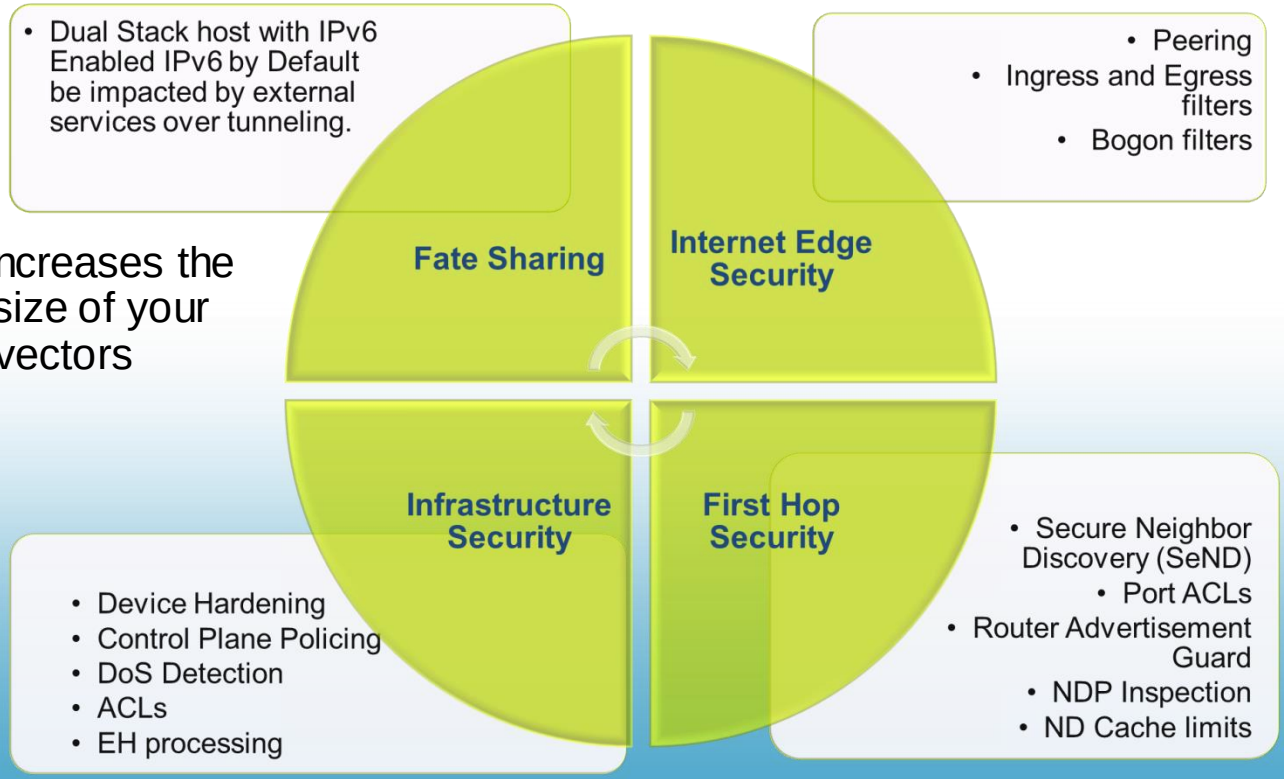
© 2015 Cisco and/or its affiliates. All rights reserved.
Cisco Public

IPv6 Security

Cisco live!

Security Considerations

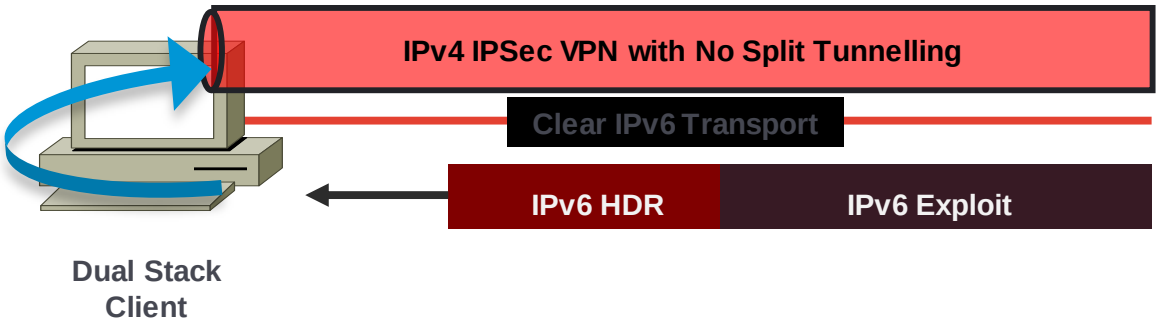
Dual Stack increases the types and size of your attack vectors



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stack Host Considerations

- Host security on a dual-stack device
  - Applications can be subject to attack on both IPv6 and IPv4
  - **Fate sharing**: as secure as the least secure stack…
- Host security controls should block and inspect traffic from both stacks
  - Host intrusion prevention, personal firewalls, VPN clients, etc.



Does the IPSec Client Stop an Inbound IPv6 Exploit?

© 2015 Cisco and/or its affiliates. All rights reserved.

Infrastructure Security - Management Plane

- SSH, syslog, SNMP, NetFlow all work over IPv6
- Dual-stack management plane
  - More resilient: works even if one stack is down
  - More exposed: can be attacked over IPv4 and IPv6
- RADIUS over IPv6 is recent but IPv6 RADIUS attributes can be transported over IPv4
- As usual, infrastructure ACL is your friend as well as out-of-band management

```
ipv6 access-list VTY
  permit ipv6 2001:db8:0:1::/64 any

line vty 0 4
  ipv6 access-class VTY in
```

In IOS-XR: The command is
'`access-class VTY ingress`',
And
The IPv4 and IPv6 ACL must have the same name

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Control Plane Policing

- Control Plane Policing can be applied to IPv6
- Adapt what's in place today to accommodate IPv6
  - Routing protocols
  - Management protocols
- Remember the extended functionality of ICMP
- Monitor carefully to see what shows up in the logs
- Remember the default rules at the end of all IPv6 ACLs

  permit ipv6 any any nd-na

  permit ipv6 any any nd-ns

  deny ipv6 any any

  - They apply to any CoPP policy that uses ACLs to match

```
policy-map COPPr
 class ICMP6_CLASS
   police 8000
 class OSPF_CLASS
   police 200000
 class class-default
   police 8000
!
control-plane cef-exception
 service-policy input COPPr
```


© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Routing Protocol Authentication - Control Plane

- BGP, ISIS, EIGRP no change:
  - MD5 authentication of the routing update
- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead rely on transport mode IPsec (for authentication and confidentiality)
- Or New Alternative is Authentication trailer for OSPFv3 (Refer to RFC 6506)
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPsec to secure protocols such as OSPFv3

```
interface Ethernet0/0
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5
   1234567890ABCDEF1234567890ABCDEF
```

```
interface Ethernet0/0
 ipv6 authentication mode eigrp 100 md5
 ipv6 authentication key-chain eigrp 100 MYCHAIN

key chain MYCHAIN
 key 1
key-string 1234567890ABCDEF1234567890ABCDEF
accept-lifetime local 12:00:00 Dec 31 2006 12:00:00 Jan
   1 2008
send-lifetime local 00:00:00 Jan 1 2007 23:59:59 Dec 31
   2007
```

No crypto maps, no ISAKMP: transport mode with static session keys

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public

Perimeter Security: Anti-Spoofing and Bogon Filters

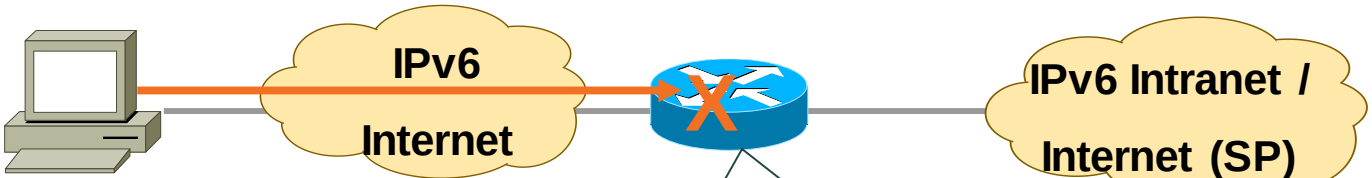
- Similar to IPv4, IPv6 has Bogons
- Anti-spoofing in IPv6 same as IPv4
  - => Same technique for single-homed edge= uRPF

```
ipv6 access-list NO_BOGONS
    remark Always permit ICMP unreachable (PMTUD)
    permit icmp any any unreachable
    remark Permit only large prefix blocks from IANA
    permit ip 2001::/16 any
    permit ip 2002::/16 any
    permit ip 2003::/18 any
    permit ip 2400::/12 any
    permit ip 2600::/10 any
    permit ip 2800::/12 any
    permit ip 2a00::/12 any
    permit ip 2c00::/12 any
    Remark implicit deny at the end
```

Inter-Networking Device with uRPF Enabled

For Full list of Bogons:

http://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt



IPv6 Unallocated Source Address

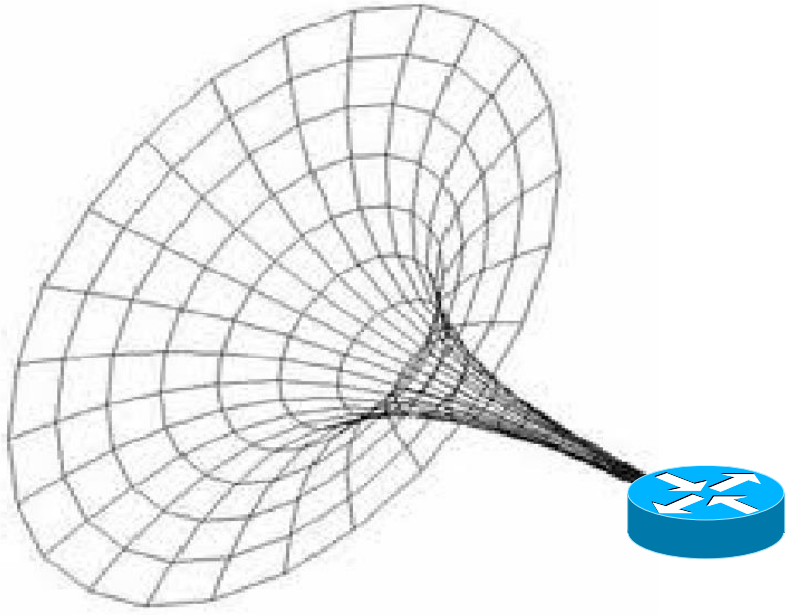
No Route to SrcAddr => Drop

© 2015 Cisco and/or its affiliates. All rights reserved.

Cisco live!

Remote Triggered Black Hole (RTBH)

- RFC 5635 RTBH is easy in IPv6 as in IPv4
- uRPF is also your friend for blackholing a source
- 100::/64
  - RFC 6666 has a specific discard ONLY prefix announced by IANA (100::/64)
  - added the prefix to the "IANA IPv6 Special Purpose Address Registry"
- Consult the following RTBH CCO Resource:
  - http://www.cisco.com/web/about/security/intelligence/ipv6_rtbh.html



© 2015 Cisco and/or its affiliates. All rights reserved.

Conclusion

- Start now and position for growth
- Next Steps:
  - Assess, Plan, Design Trial, Train, Roll out
- Map out opportunities to be IPv6 ready in planned technology refresh cycles
  - Reference IPv6 Ready Logo, USGv6 and RIPE-501
- Adapt IPv4 best practices for IPv6
- IPv6 is not identical to IPv4 so a review of the current architectures is necessary to understand the possible impact of integrating IPv6
- Education is key!
- Don't make IPv6 an all or nothing matter – It wont work and will fail

http://www.cisco.com/go/ipv6

© 2015 Cisco and/or its affiliates. All rights reserved.

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

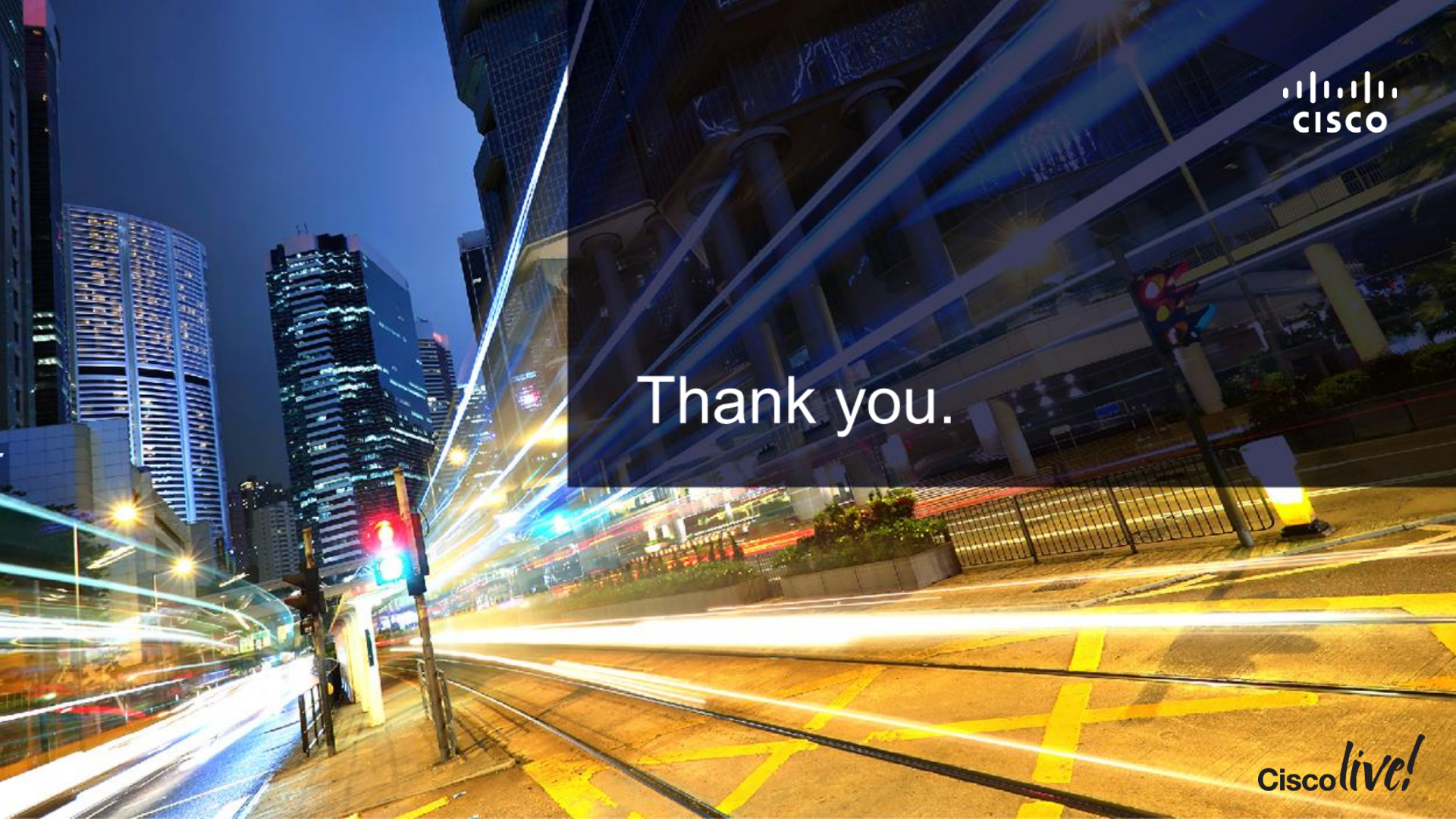
Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public


Thank you.

CISCO