IPv6 Planning (Session 9267)

Cisco Systems Inc.

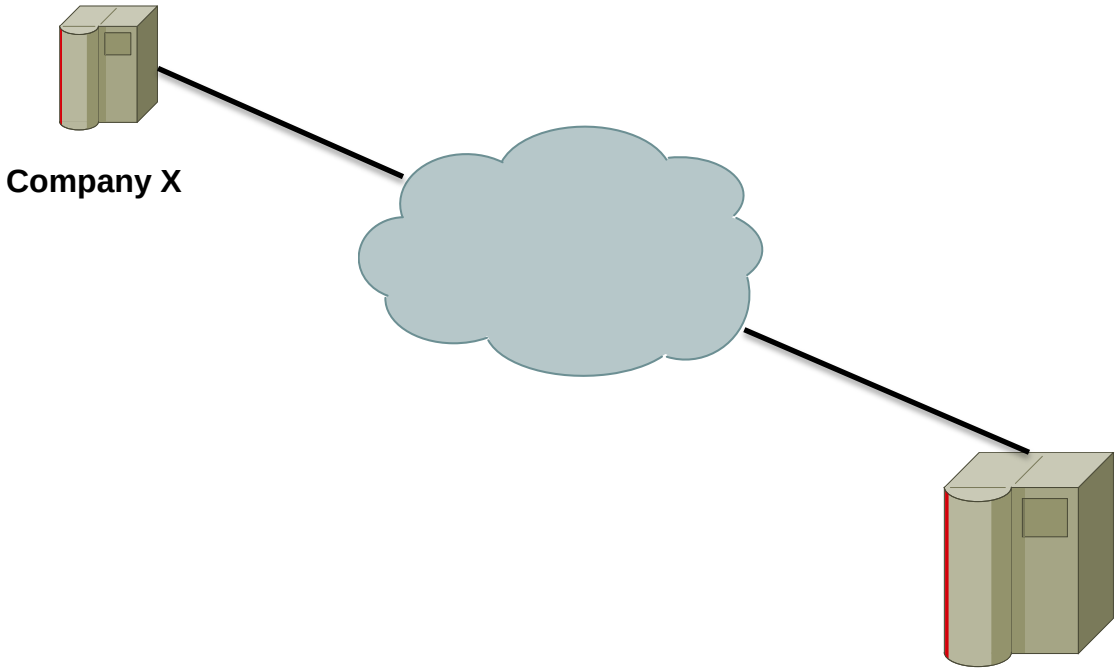
Kevin Manweiler, CCIE 5269
kmanweil@cisco.com

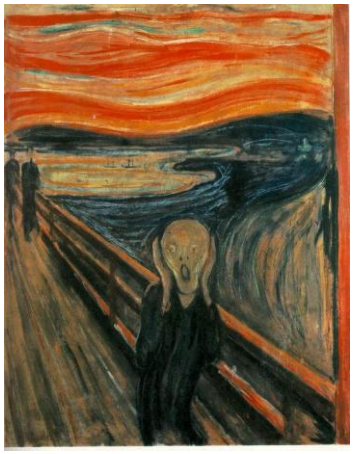
Junnie Sadler, CCIE 7028
jrsadler@cisco.com

Date of Presentation (Wednesday, August 10)
Session Number (9267)

Motivation

- Your boss has just let you know that a customer mandates IPv6 connectivity for future mainframe EE in 6 months.
- Also, you recently read that the last IPv4 address block was allocated





Advice from the Hitchhikers' Guide to Networking

- Just because the last IPv4 address has been allocated doesn't mean "The Internet" is coming to a screeching halt
- No one is going to take your existing IPv4 addresses away
- Your whole network doesn't have to be configured with IPv6 immediately
- Other people have made the transition… successfully
- You've already been through this drill with the SNA to IP migration.

Agenda

- High Level Migration Steps
- Infrastructure Assessment
- Address Considerations
- Infrastructure Deployment
- Security Considerations
- Network Management Considerations
- SNAv6
- Q&A
- References

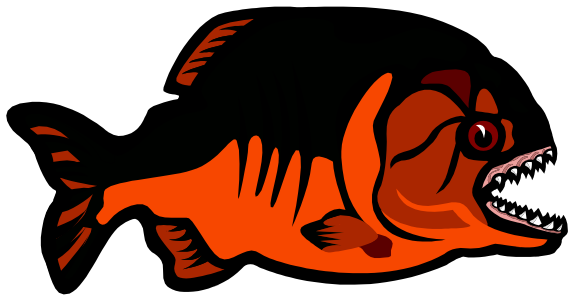
IPv6 Planning Steps

Business Case Identified/Justified

1. Evaluate effect on business model
2. Establish IPv6 project management team
3. Assess network hardware and software
4. IPv6 Training strategy
5. Obtain IPv6 prefix(es)
6. Decide IPv6 architectural solution
7. Test application software and services
8. Develop security policy
9. Develop procurement plan
10. Develop IPv6 exception strategy

Public Service Announcement

- It’s not required but advised to enlist outside aid
- How do you know what you don’t know?
- Workshops
- Consultants
- Labs
- Training (in-side and out-side)



Major Design Decisions

Addressing	Subnetting Scheme	Address Distribution	Co-existence Methodology	Migration Strategy	Tunneling methods
Provider Assigned (PA)	/64 subnet everywhere	Statically assigned	Dual Stack	Internet facing	ISATAP
Provider Independent (PI)	/64 with /127 infrastructure	Stateless Autoconfiguration (SLAC)	Tunneling	Core outwards	Toredo
/48 block (/44 if you can)	/64 with link local infrastructure	DHCP	Translation	Edge inward	6to4
Multiple /48 blocks (per region)			Separate Infrastructure	Forklift / Everywhere at once	
Unique-local addressing			Combinations/ permutations		

IPv6 Readiness Assessment

- Gives a high level view of IPv6 capability in the network
- Some device may just need a software upgrade – others may never be capable of supporting IPv6

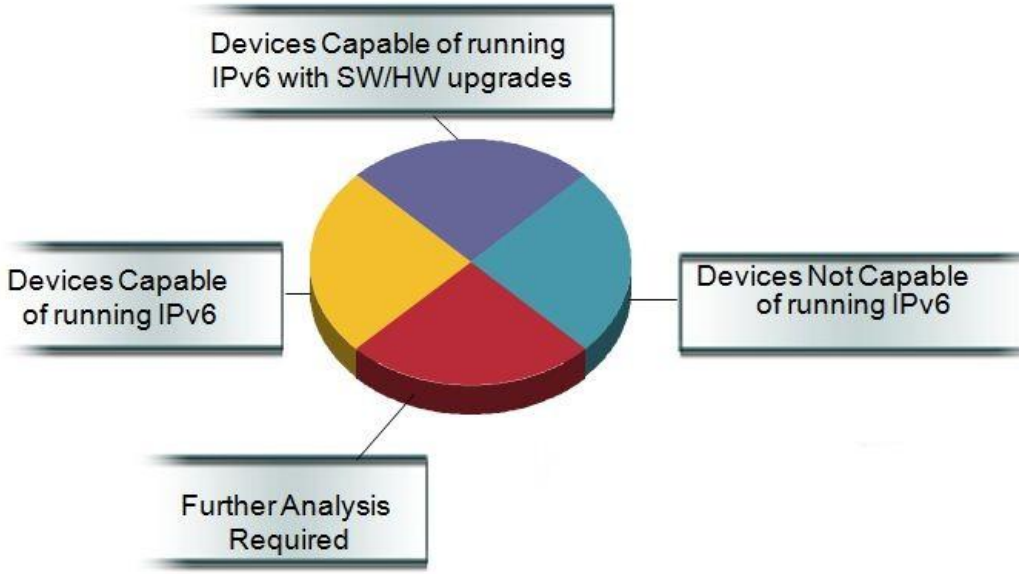


Table 2. IPv6 Summary - entire all groups

Status	Number of Devices	% of Total Devices
The device is currently capable of supporting IPv6 features; hardware and software upgrades are not required	31	15.05
The device require an upgrade, either Hardware, Software or an OS upgrade	109	52.91
The device is not capable of supporting IPv6 services	46	22.33
The analysis was unable to determine the device's capability to support IPv6; further analysis is required	20	9.71

Infrastructure Assessment

Cisco's IPv6 Network Readiness Assessment

The assessment examines Cisco IOS based routers and Catalyst Operating System (CatOS) and IOS based switches.

This assessment provides a capability assessment from a 3 point view.
Hardware – Can it support IPv6.
Software -- Does it support IPv6.
Feature – Does it support what you are looking to use in your network.

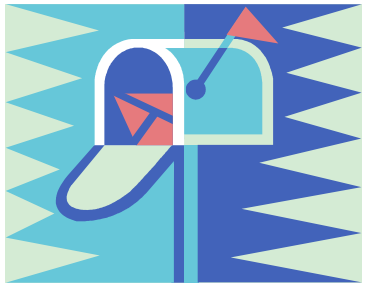
- Devices Currently IPv6 Capable
- Devices Requiring Only Software Upgrade
- Hardware IPv6 Capable, requires IOS and FLASH Upgrade
- Hardware IPv6 Capable, requires IOS and DRAM Upgrade
- Hardware IPv6 Capable, requires IOS, DRAM and FLASH Upgrade
- Not IPv6 Capable
- Devices Requiring Further Analysis

Platform Considerations

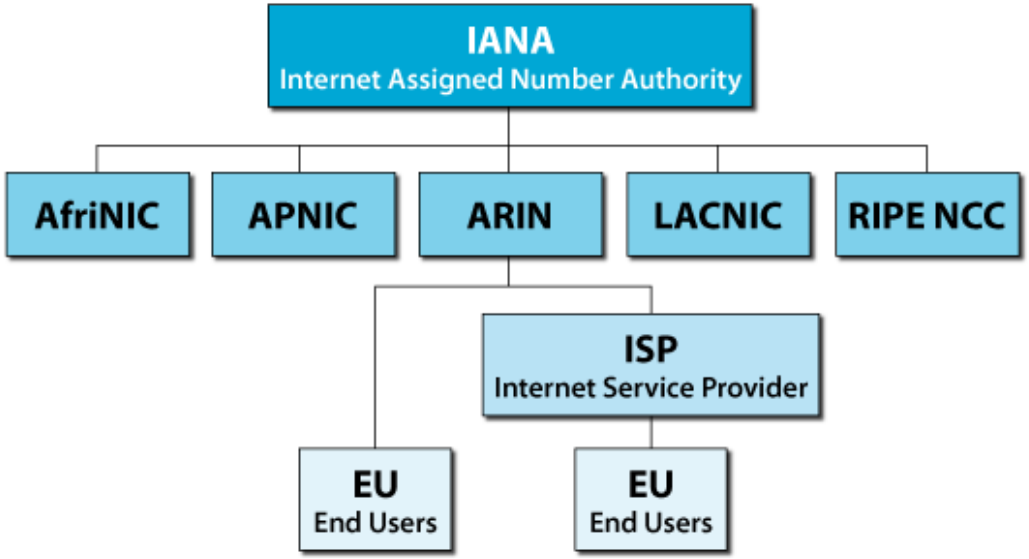
- Scalability can play a big role in IPv6 deployments
  - Dual stack can have 2x route table size, ARP cache, etc.
- Some platforms perform ASIC-based hardware packet forwarding. If traffic can't be forwarded in hardware it is punted to the Route Processor (RP). The RP has at least an order of magnitude less forwarding capability and induces delay.
- Feature Parity - basic IPv6 forwarding may exist but security and high availability features may not exist or be at that level of software.

Address Considerations

- Provider Independent or Provider Assigned
- Global, ULA, ULA + Global
- Prefix-length allocation
- Subnet length
- Address allocation method
- IP Address Management (IPAM)

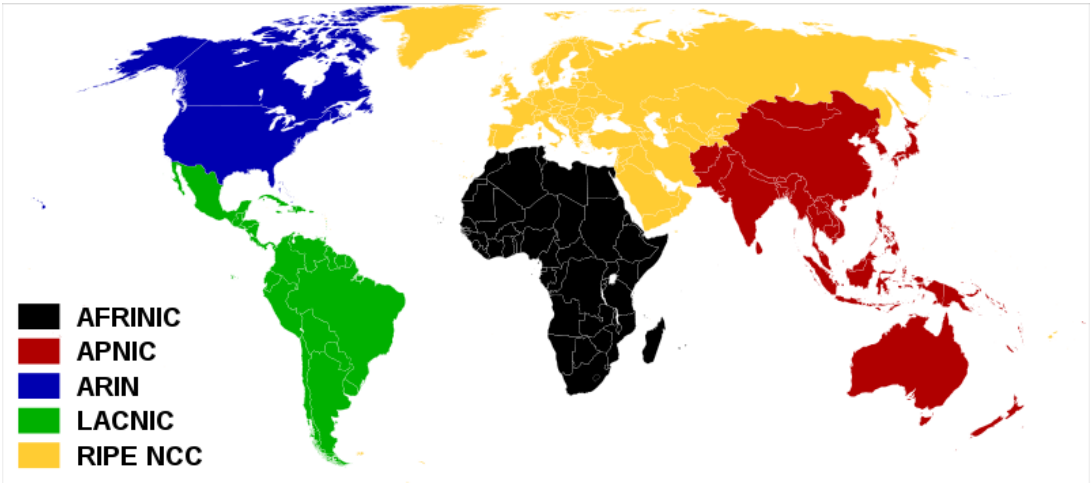


RIRs – Regional Internet Registries

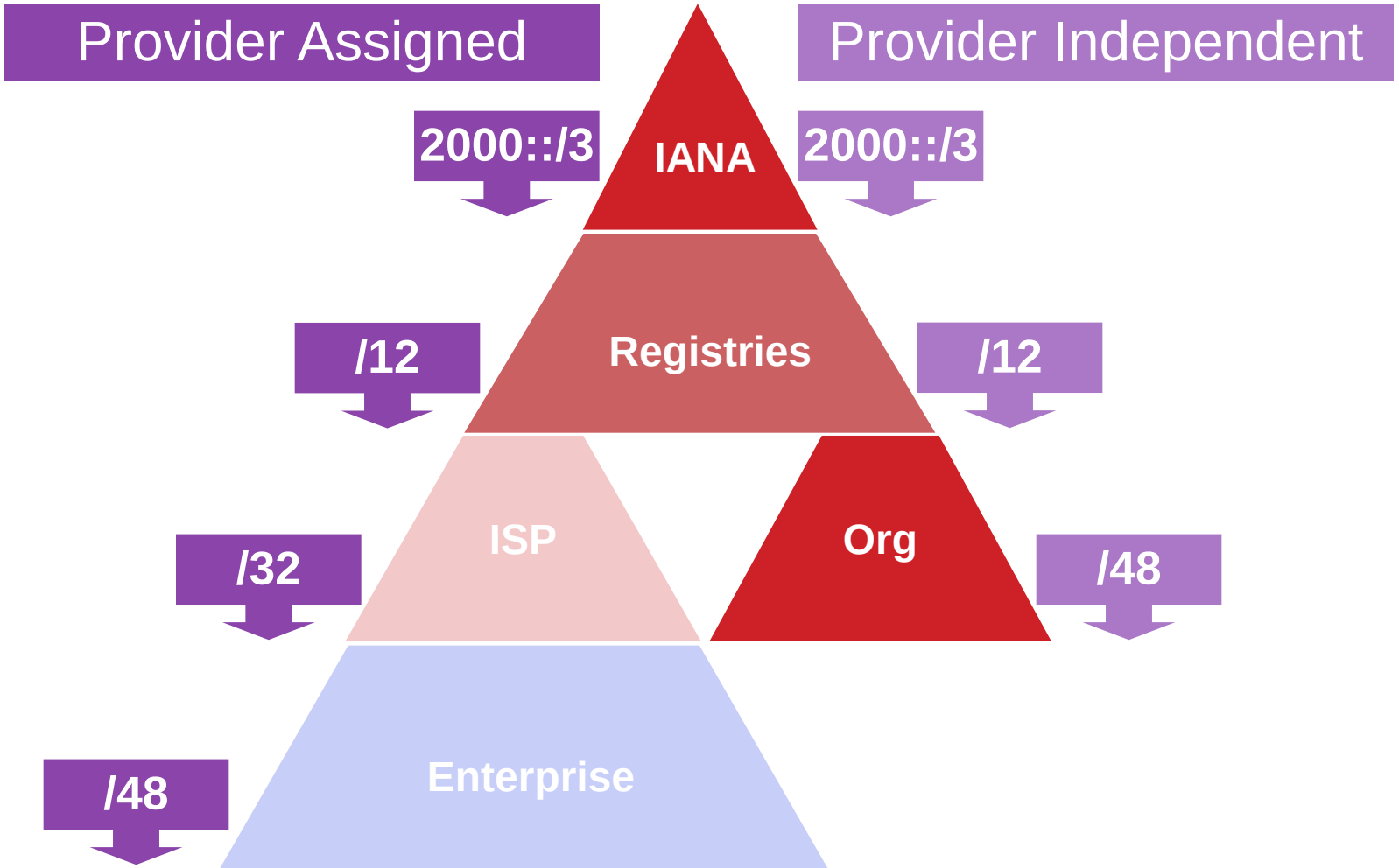


- Apply for Provider Independent address space from appropriate RIR

- www.afrinic.net
- www.arin.net
- www.apnic.net
- www.lacnic.net
- www.ripe.net

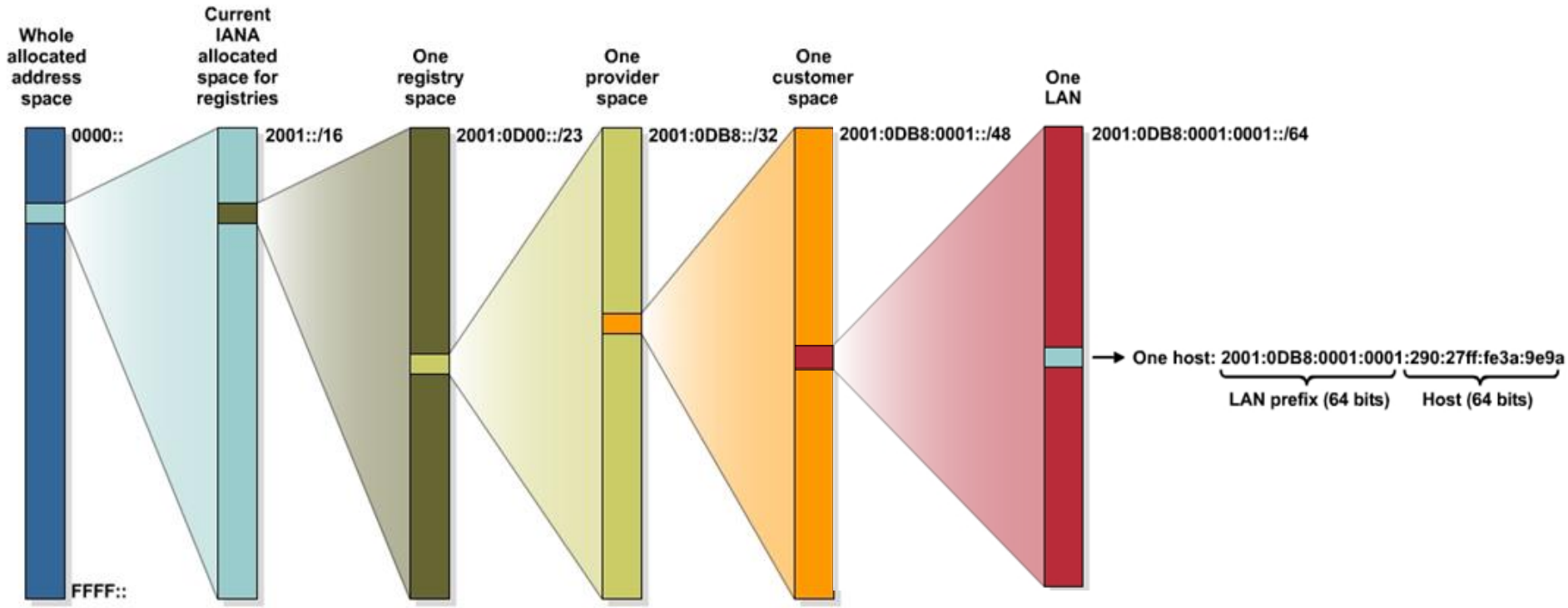


Address Allocation Process

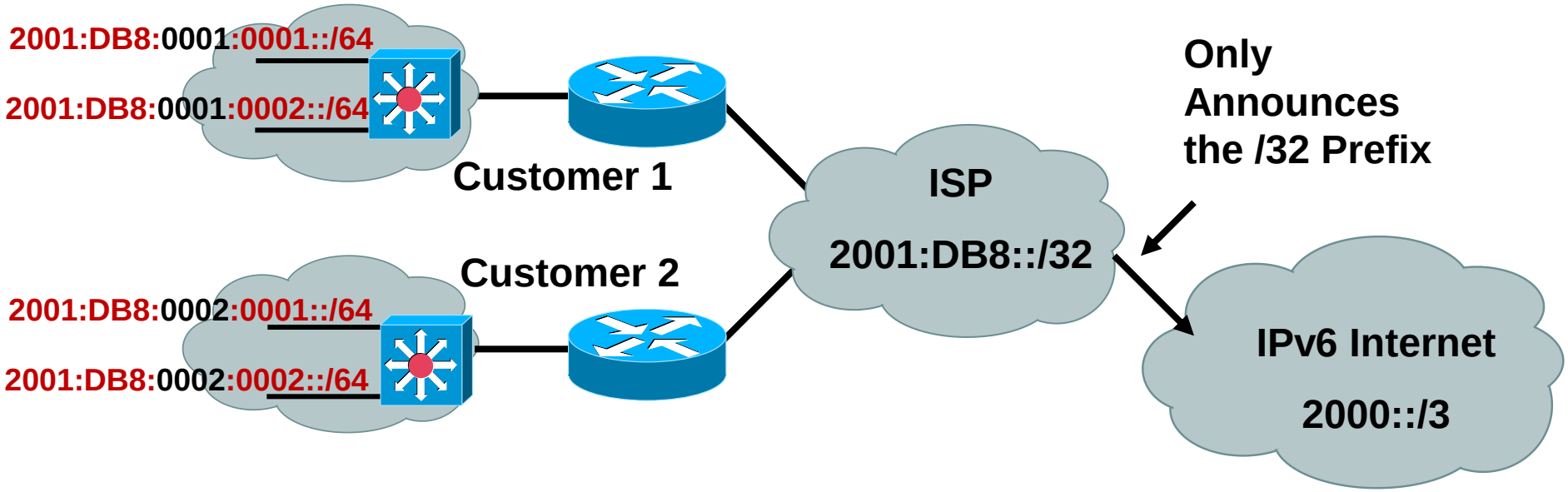


IPv6 Address Allocation Process

Partition of Allocated IPv6 Address Space (example)



Hierarchical Addressing and Aggregation



- Default is /48 – can be larger – “End-user Additional Assignment”
- https://www.arin.net/resources/request/ipv6_add_assign.html
- Provider independent – See Number Resource Policy Manual (NRPM) –
- https://www.arin.net/policy/nrpm.html

Network Level Considerations

- Global Unique Addresses
  - Commonly referred to as Global IPv6 addresses
  - Assigned by upstream provider
  - A multi-homed site may have one or more available IPv6 address ranges
  - The IPv6 address selection algorithm is key for good operation (RFC3484)

Unique-Local Addressing (RFC4193)

- Used for internal communications, inter-site VPNs
  - Not routable on the internet—basically RFC1918 for IPv6 only better—less likelihood of collisions
- Default prefix is /48
  - /48 limits use in large organizations that will need more space
  - Semi-random generator prohibits generating sequentially ‘useable’ prefixes—no easy way to have aggregation when using multiple /48s
  - Why not hack the generator to produce something larger than a /48 or even sequential /48s?
  - Is it ‘legal’ to use something other than a /48? Perhaps the entire space? Forget legal, is it practical? Probably, but with dangers—remember the idea for ULA; internal addressing with a slim likelihood of address collisions with M&A. By consuming a larger space or the entire ULA space you will significantly increase the chances of pain in the future with M&A
- Routing/security control
  - You must always implement filters/ACLs to block any packets going in or out of your network (at the Internet perimeter) that contain a SA/DA that is in the ULA range—today this is the **only** way the ULA scope can be enforced
- Generate your own ULA: https://www.arin.net/policy/nrpm.html

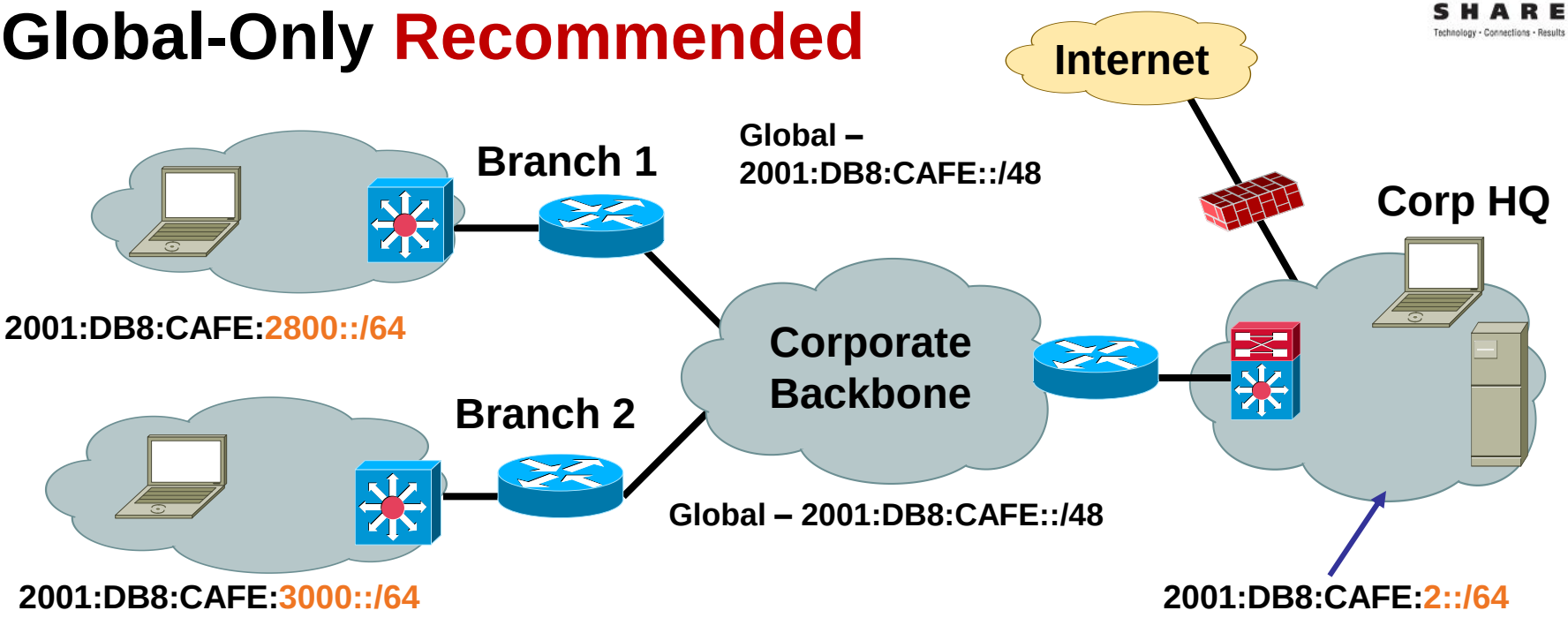
```
Generated ULA= fd9c:58ed:7d73::/48

    * MAC address=00:0D:9D:93:A0:C3 (Hewlett Packard)
    * EUI64 address=020D9Dfffe93A0C3
    * NTP date=cc5ff71943807789 cc5ff71976b28d86
```

ULA, ULA + Global or Global

- What type of addressing should I deploy internal to my network? It depends:
  - ULA-only—Today, no IPv6 NAT is useable in production so using ULA-only will not work externally to your network
  - ULA + Global allows for the best of both worlds **but** at a price— much more address management with DHCP, DNS, routing and security
  - Global-only—Recommended approach but the old-school security folks that believe topology hiding is essential in security will bark at this option

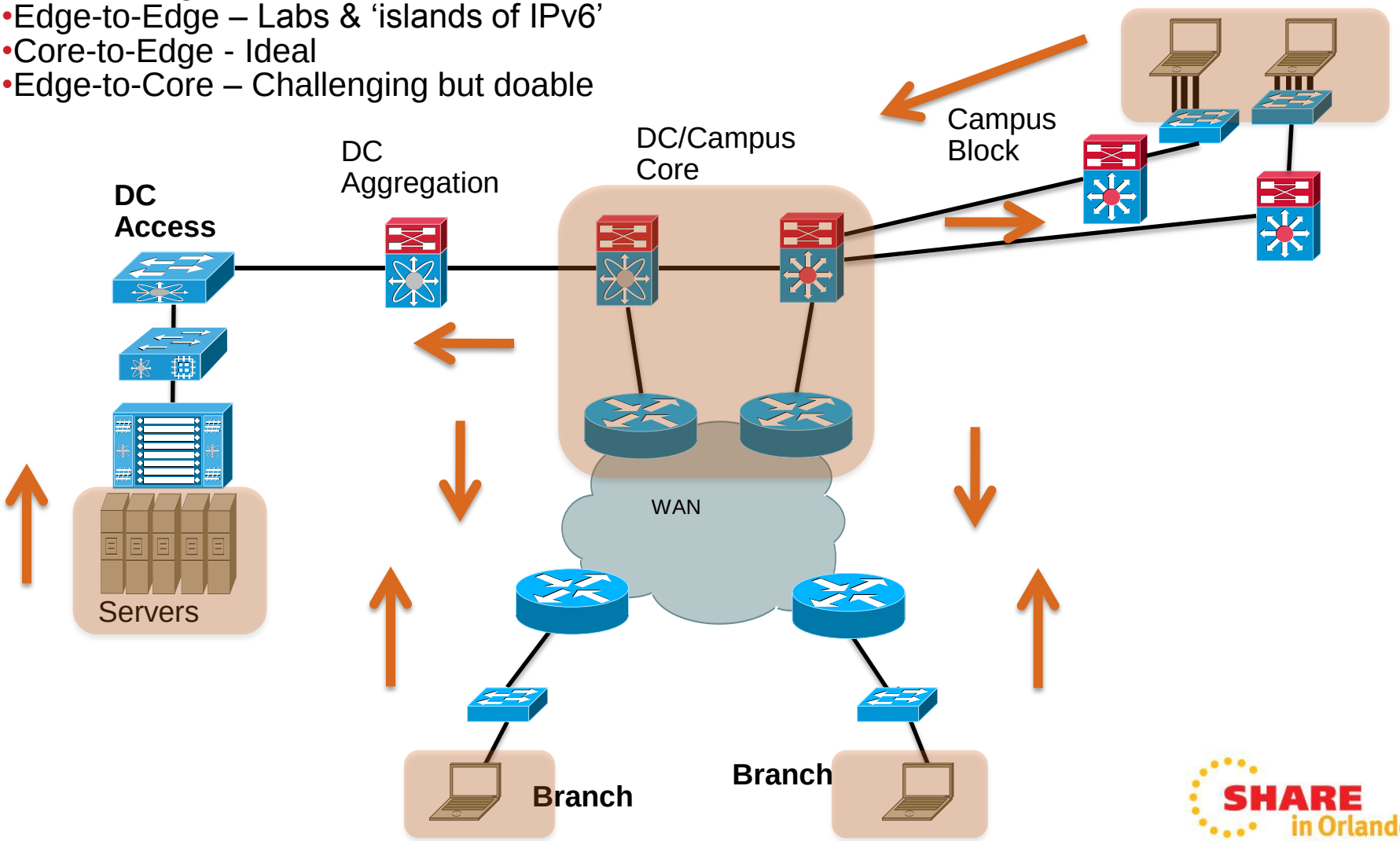
Global-Only Recommended



- Global is used everywhere
- No requirements to have NAT for ULA-to-Global translation—but, NAT may be used for other purposes
- Easier management of DHCP, DNS, security, etc.
- Only downside is breaking the habit of believing that topology hiding is a good security method

Where do I start?

- Based on Timeframe/Use case
- Mainframe
- Internet Edge/DMZ
- Edge-to-Edge – Labs & 'islands of IPv6'
- Core-to-Edge - Ideal
- Edge-to-Core – Challenging but doable

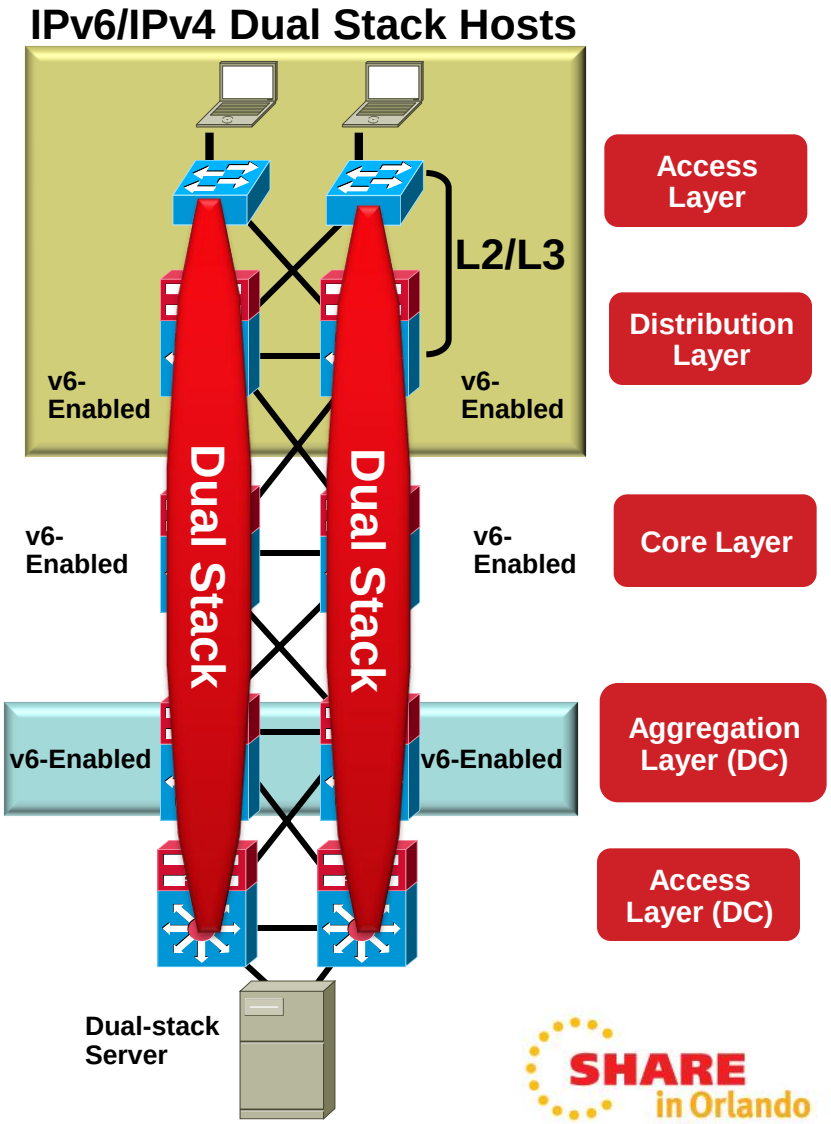


IPv6 Deployment
Three Major Options

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

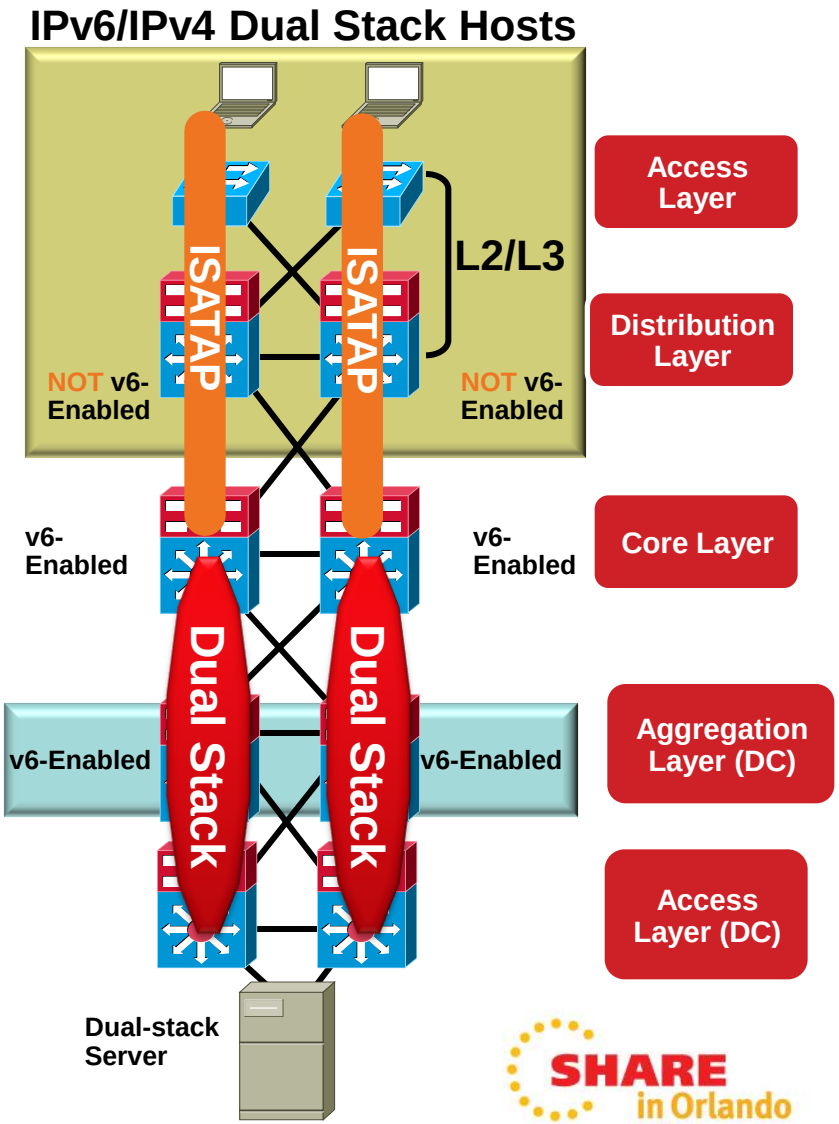
IPv6 Deployment Options
Dual-Stack IPv4/IPv6

- #1 requirement—switching/ routing platforms must support hardware based forwarding for IPv6
- IPv6 is transparent on L2 switches but—
  - L2 multicast—MLD snooping
  - IPv6 management—Telnet/SSH/HTTP/SNMP
  - Intelligent IP services on WLAN
- Expect to run the same IGPs as with IPv4



IPv6 Deployment Options
Hybrid Model

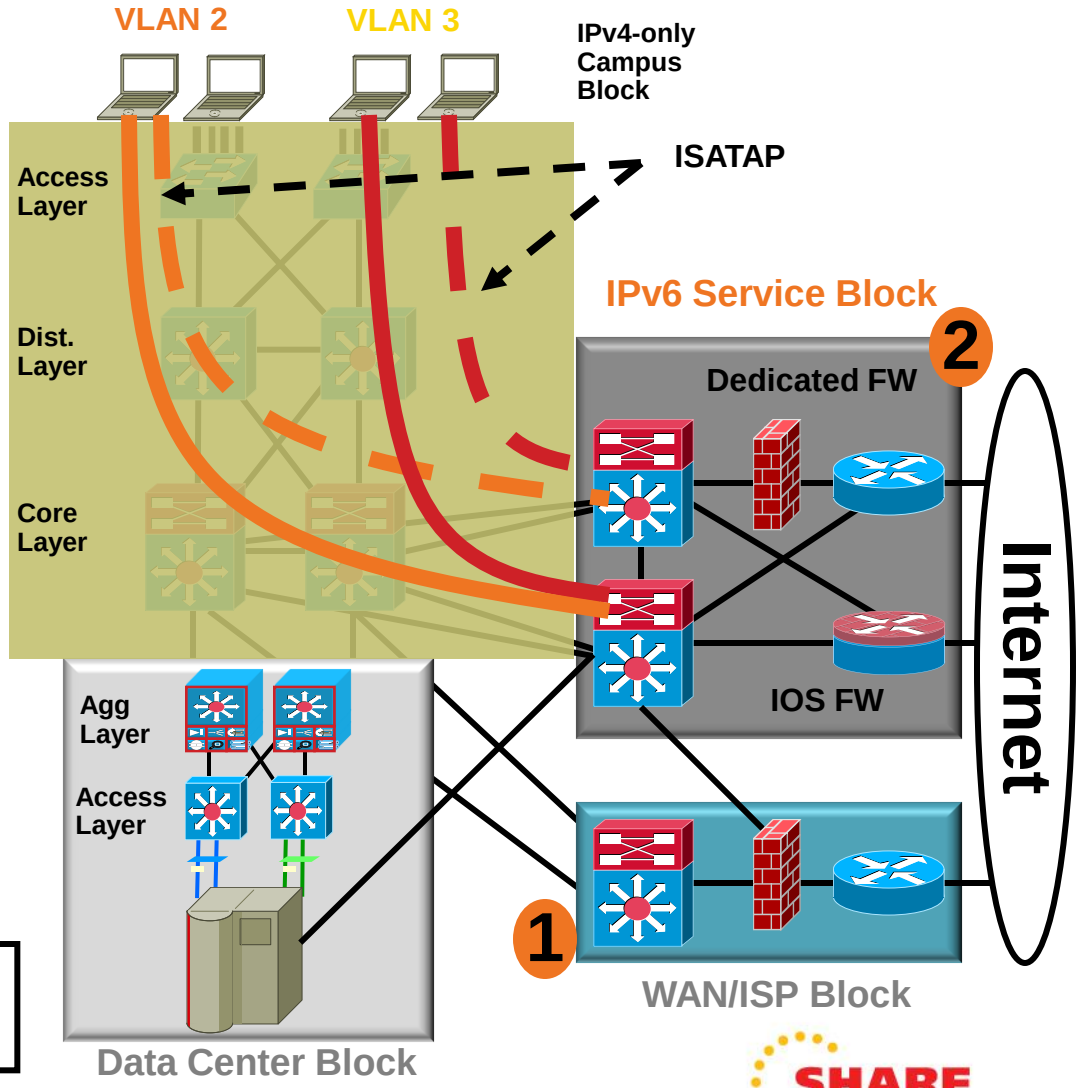
- Offers IPv6 connectivity via multiple options
  - Dual-stack
  - Configured tunnels—L3-to-L3
  - ISATAP—Host-to-L3
- Leverages existing network
- Offers natural progression to full dual-stack design
- May require tunneling to less-than-optimal layers (i.e. core layer)
- ISATAP creates a flat network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



Campus IPv6 Deployment Options

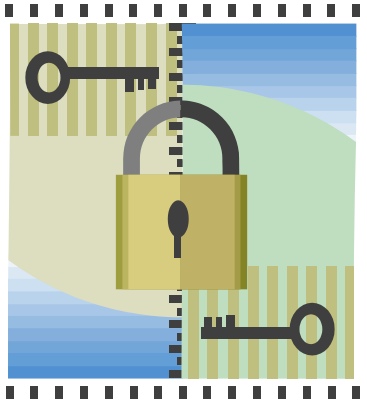
IPv6 Service Block—an Interim Approach

- Provides ability to rapidly deploy IPv6 services without touching existing network
- Provides tight control of where IPv6 is deployed and where the traffic flows (maintain separation of groups/locations)
- Offers the same advantages as Hybrid Model without the alteration to existing code/configurations
- Configurations are very similar to the Hybrid Model
  - ISATAP tunnels from PCs in access layer to service block switches (instead of core layer—Hybrid)
- 1) Leverage existing ISP block for both IPv4 and IPv6 access
- 2) Use dedicated ISP connection just for IPv6—Can use IOS FW or PIX/ASA appliance



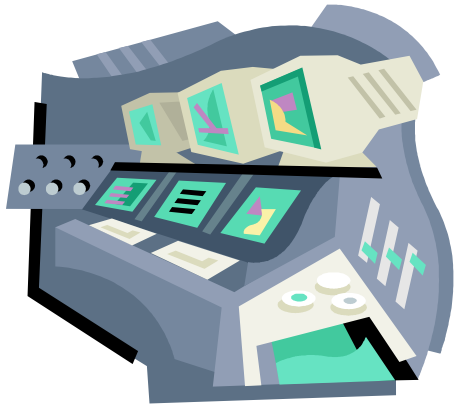
Security Considerations

- A lot of early docs touted IPv6's inherent security and IPSec use.
  This is a false sense of security
- What's old is new: old exploits re-introduced with a "v6" at the end.
- IPv6 is enabled by default on Windows Vista and 7.
- IPv6 Bogon list- http://www.cymru.com/Bogons/ipv6.txt



Network Management Considerations

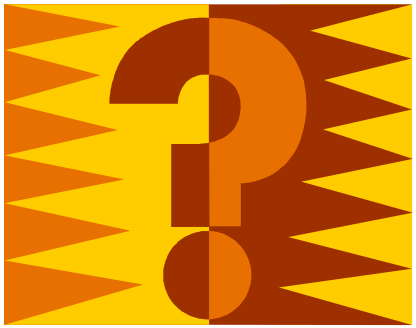
- Do your NMS tools understand IPv6 addresses?
- IPv6 specific MIBs
- Don’t necessarily have to use IPv6 transport to manage IPv6 networks - many NMS tools (and network devices) don’t support polling, etc. via IPv6 today
- Netflow version 9 for IPv6 support
- IP-SLAs support IPv6



Conclusion

- “Dual stack where you can – Tunnel where you must”
- Create a virtual team of IT representatives from every area of IT to ensure coverage for OS, Apps, Network and Operations/Management
- Microsoft Windows Vista, 7 and Server 2008 will have IPv6 enabled by default—understand what impact any OS has on the network
- Deploy it – at least in a lab – IPv6 won’t bite
- Things to consider:
  - Focus on what you must have in the near-term (lower your expectations) but pound your vendors and others to support your long-term goals
  - Don’t be too late to the party – anything done in a panic is likely going to go badly

Q&A



Reference Materials

- Deploying IPv6 in Campus Networks:
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html
- Deploying IPv6 in Branch Networks:
  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns816/landing_br_ipv6.html
- CCO IPv6 Main Page:
  http://www.cisco.com/go/ipv6
- Cisco Network Designs:
  http://www.cisco.com/go/designzone
- ARIN IPv6 Wiki:
  http://www.getipv6.info/index.php/Main_Page
- World IPv6 Day (June 8, 2011):
  http://isoc.org/wp/worldipv6day/
- IPv6 at IBM
  http://www-01.ibm.com/software/info/ipv6/index.jsp
- IBM IPv6 Compliance
  http://www-01.ibm.com/software/info/ipv6/compliance.jsp
- Security for IPv6 Routers
  www.**nsa.gov**/ia/_files/routers/I33-002R-06.pdf

End of Session