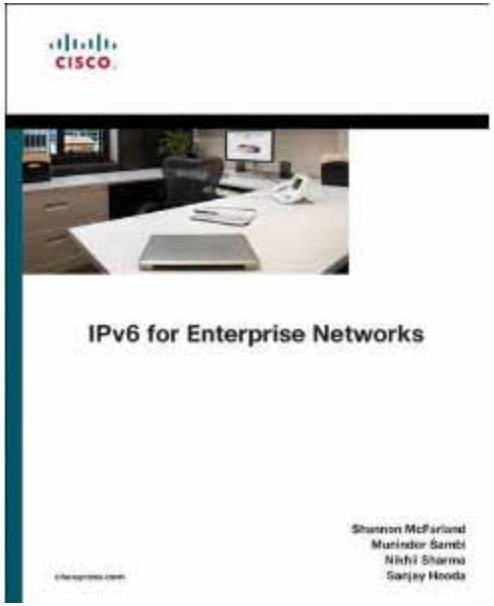
Enterprise IPv6 Deployment

Presented by Harold Ritter

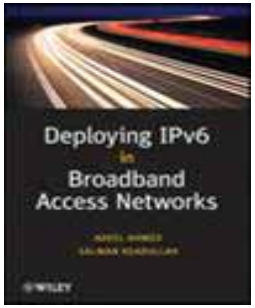
Reference Materials

- New/Updated IPv6 Cisco Sites:
  http://www.cisco.com/go/ipv6
  http://www.cisco.gom/go/entipv6
- 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

Recommended Reading



Deploying IPv6 in Broadband Networks - Adeel Ahmed, Salman Asadullah ISBN0470193387, John Wiley & Sons Publications®



Now available!!

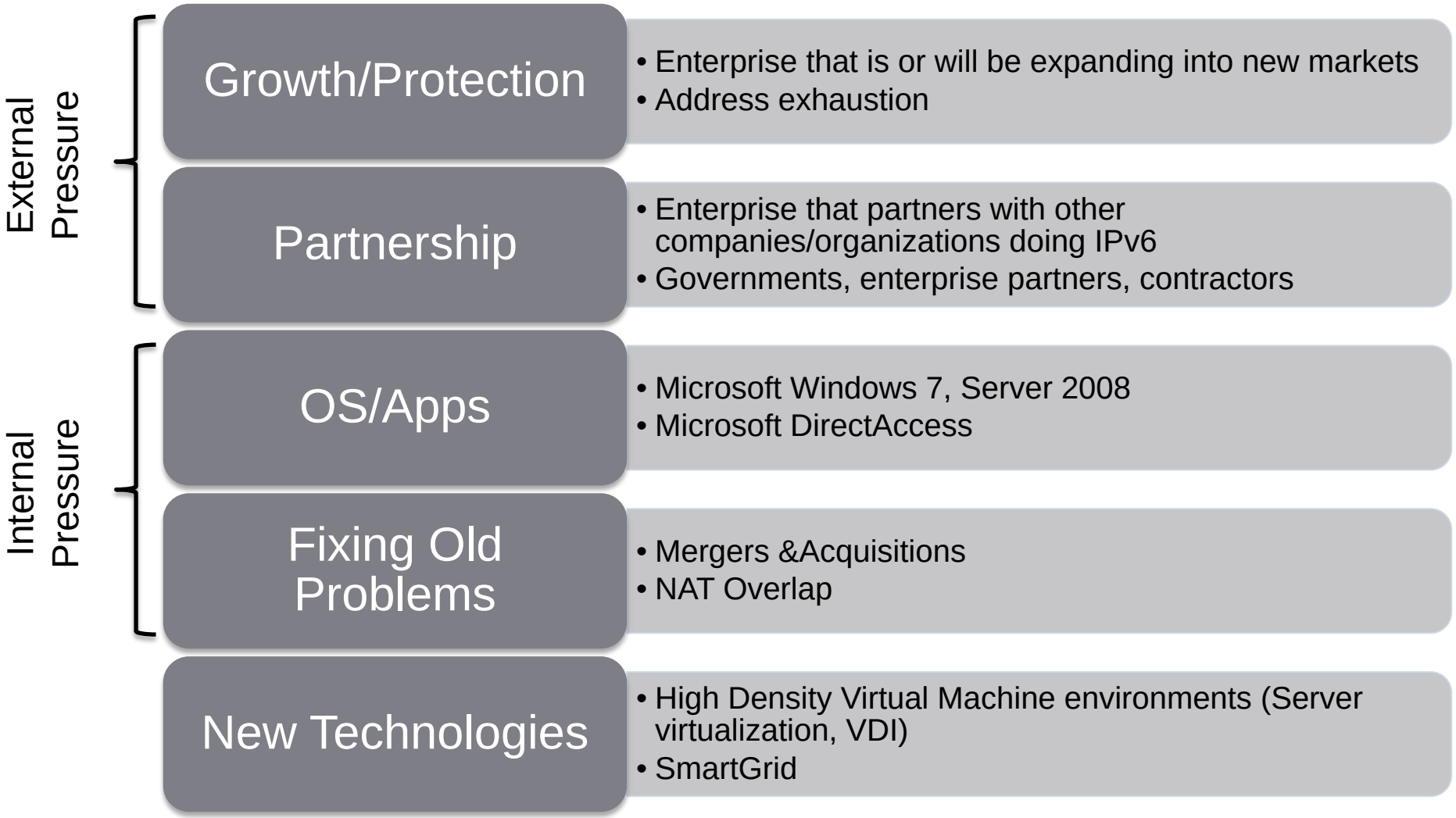
Agenda

- The Need for IPv6
- Planning and Deployment Summary
- Address Considerations
- General Concepts
- Infrastructure Deployment
  - Campus/Data Center
  - WAN/Branch
  - Remote Access
- Communicating with the Service Providers

The Need for IPv6

Dramatic Increase in Enterprise Activity

Why?



Innocent W2K3 -to- W2K8 Upgrade

Windows 2003

```
C:\>ping svr-01

Pinging svr-01.example.com [10.121.12.25] with 32 bytes of data:
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
Reply from 10.121.12.25: bytes=32 time<1ms TTL=128
```

Upgraded Host to Windows 2008

```
C:\>ping svr-01

Pinging svr-01 [fe80::c4e2:f21d:d2b3:8463%15] with 32 bytes of data:
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
Reply from fe80::c4e2:f21d:d2b3:8463%15: time<1ms
```

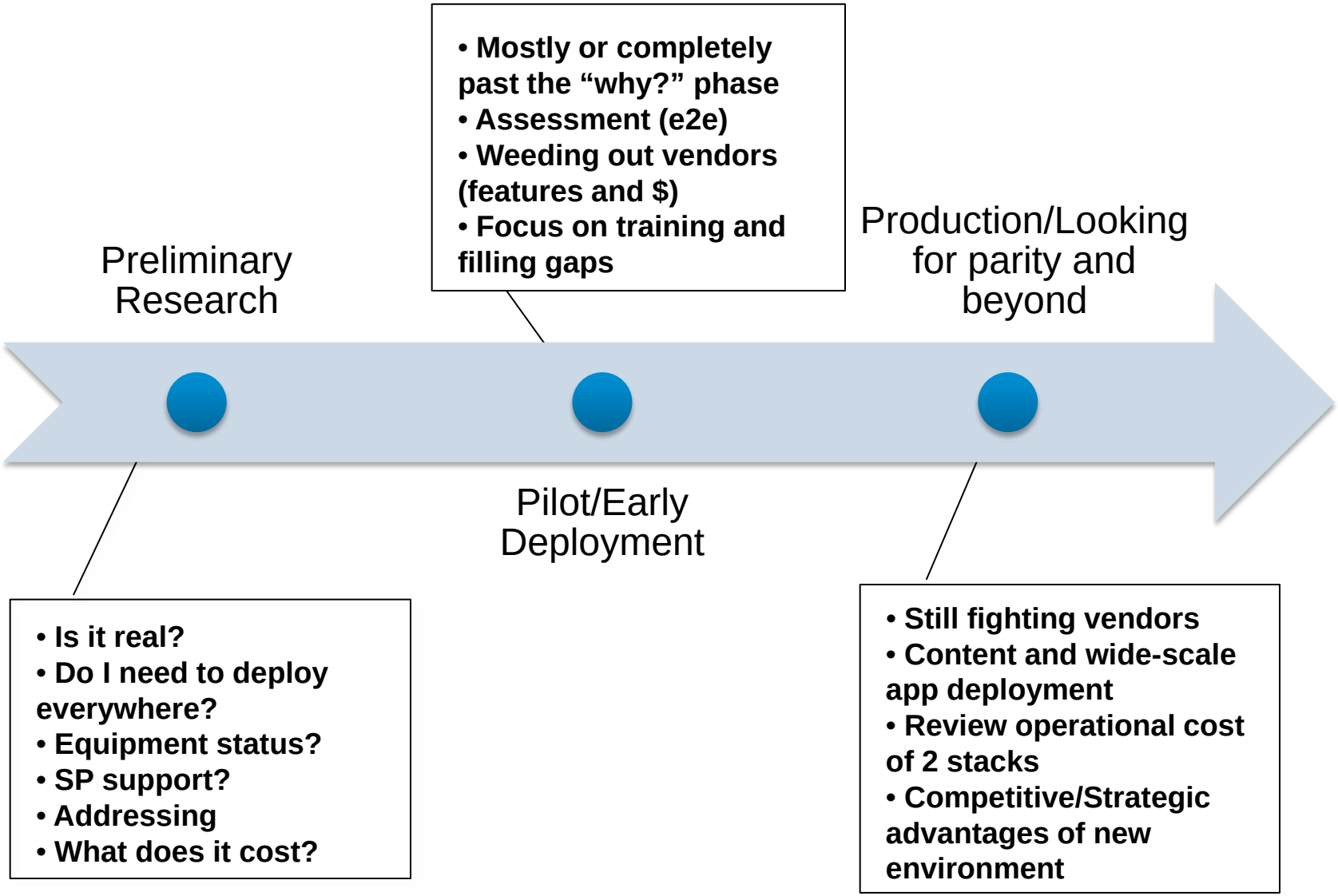
No.	Time	Source	Destination	Protocol	Info
3969	244.938775	fe80::c4e2:f21d:d2b3:8463	ff02::1:3	UDP	Source port: 63828 Destination port: llmnr
3970	244.938958	10.121.12.25	224.0.0.252	UDP	Source port: 53753 Destination port: llmnr

.....**svr-01**……..

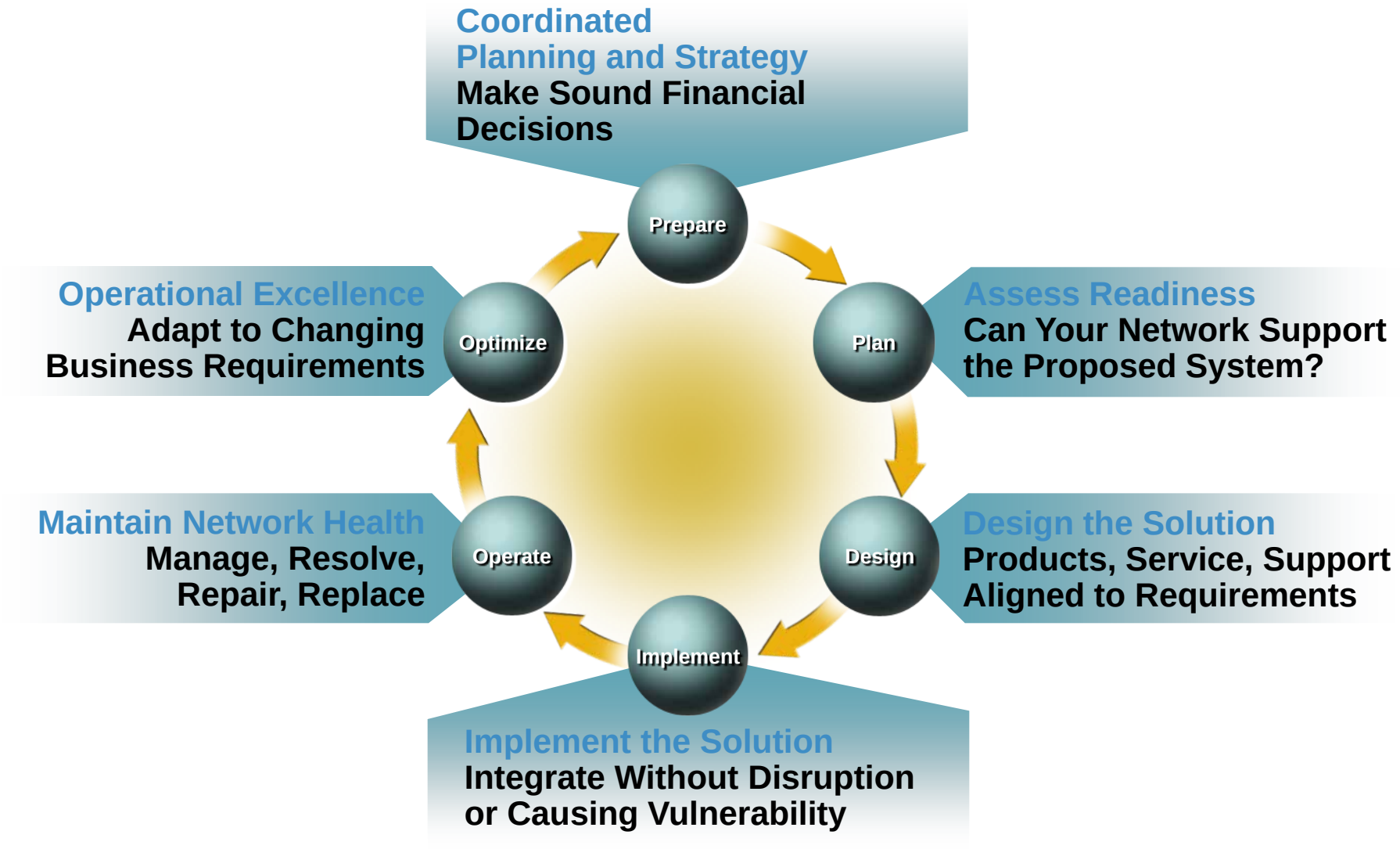
- Can happen if the circumstances are right
- http://technet.microsoft.com/en-us/library/bb878128.aspx

Planning and Deployment Summary

Enterprise Adoption Spectrum



Cisco IPv6 Deployment - A Lifecycle Approach

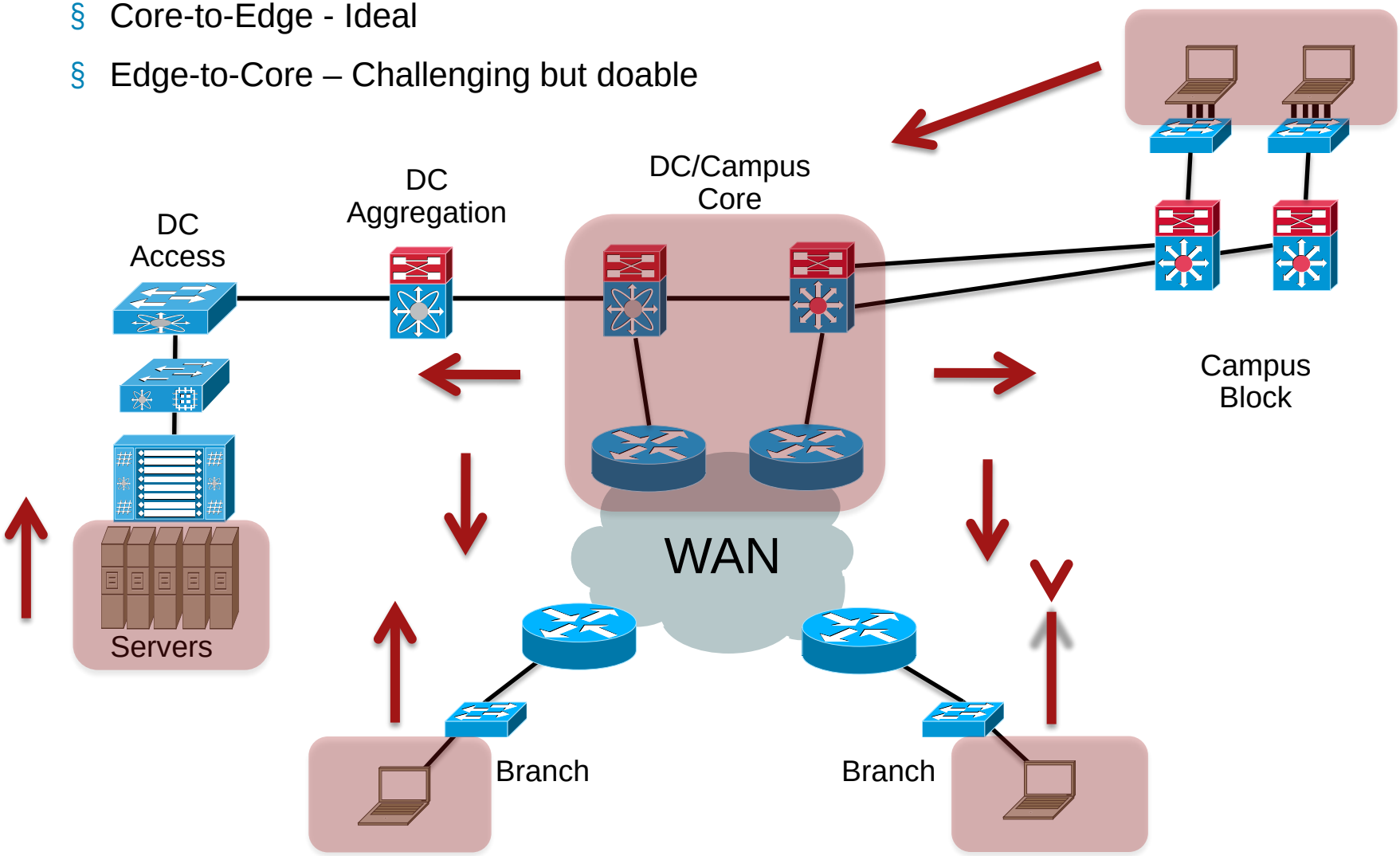


IPv6 Integration Outline

Pre-Deployment Phases	Deployment Phases
• Establish the network starting point • Importance of a network assessment and available tools • Defining early IPv6 security guidelines and requirements • Additional IPv6 “pre-deployment” tasks needing consideration	• Transport considerations for integration • Campus IPv6 integration options • WAN IPv6 integration options • Advanced IPv6 services options

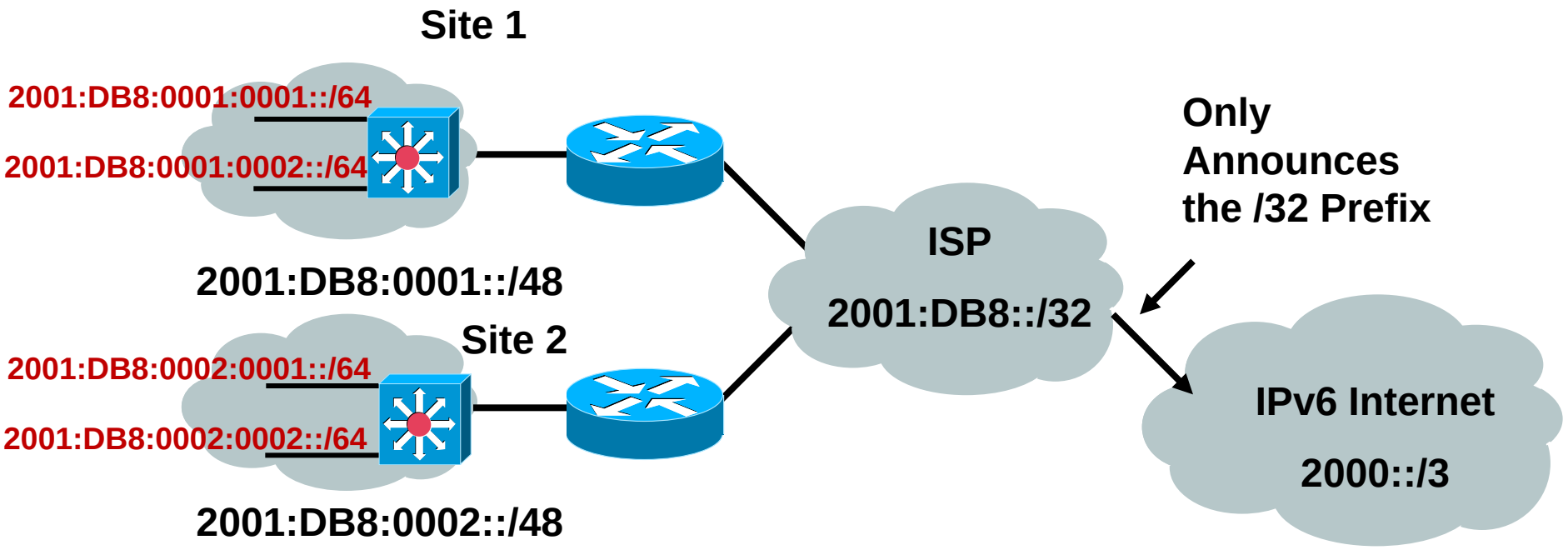
Where do I start?

- Based on Timeframe/Use case
- Core-to-Edge - Ideal
- Edge-to-Core – Challenging but doable



Address Considerations

Hierarchical Addressing and Aggregation



- Default is /48 – can be larger: http://www.ripe.net/ripe/docs/ipv6policy.html
- Provider independent - http://www.ripe.net/rs/ipv6/

Unique-Local Addressing (RFC4193)

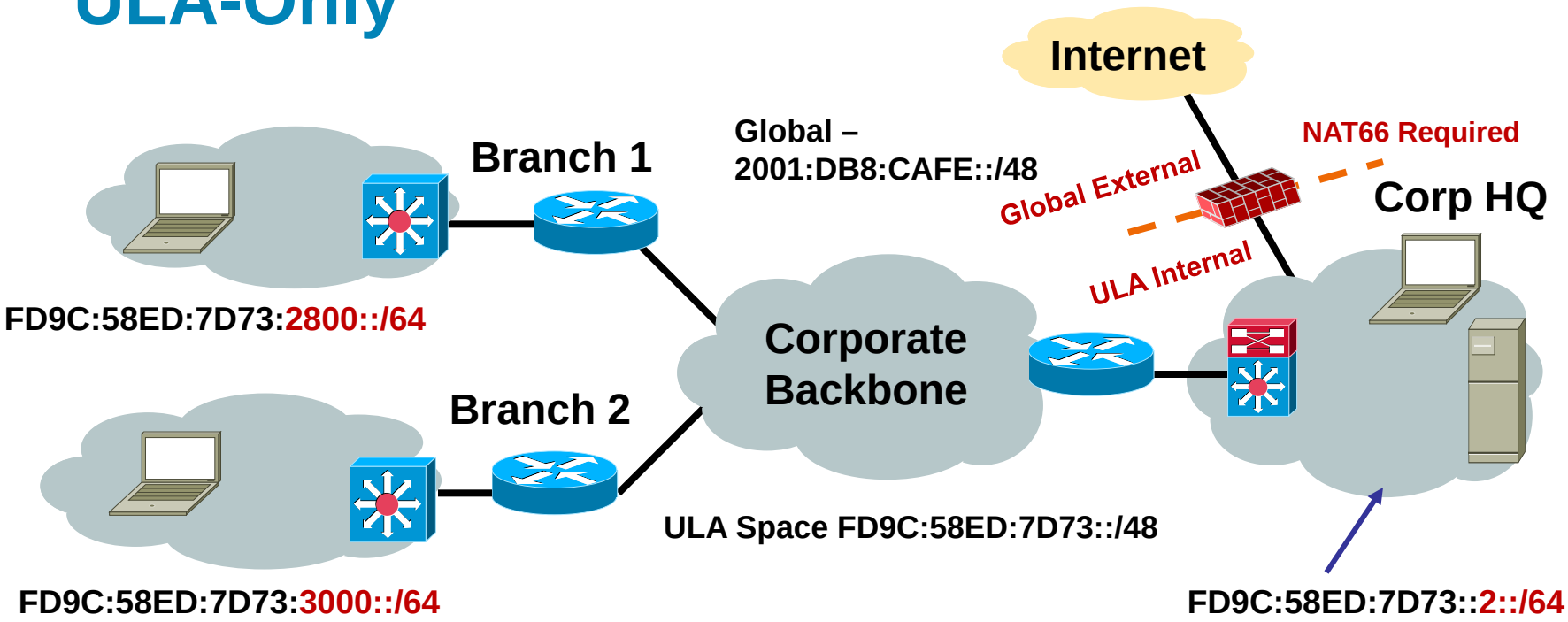
- Used for internal communications, inter-site VPNs
  - Not routable on the internet—basically RFC1918 for IPv6 only better—less likelihood of collisions
- Default prefix is /48
  - /48 limits use in large organizations that will need more space
  - Semi-random generator prohibits generating sequentially ‘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: http://www.sixxs.net/tools/grh/ula/

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

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

Not Recommended Today

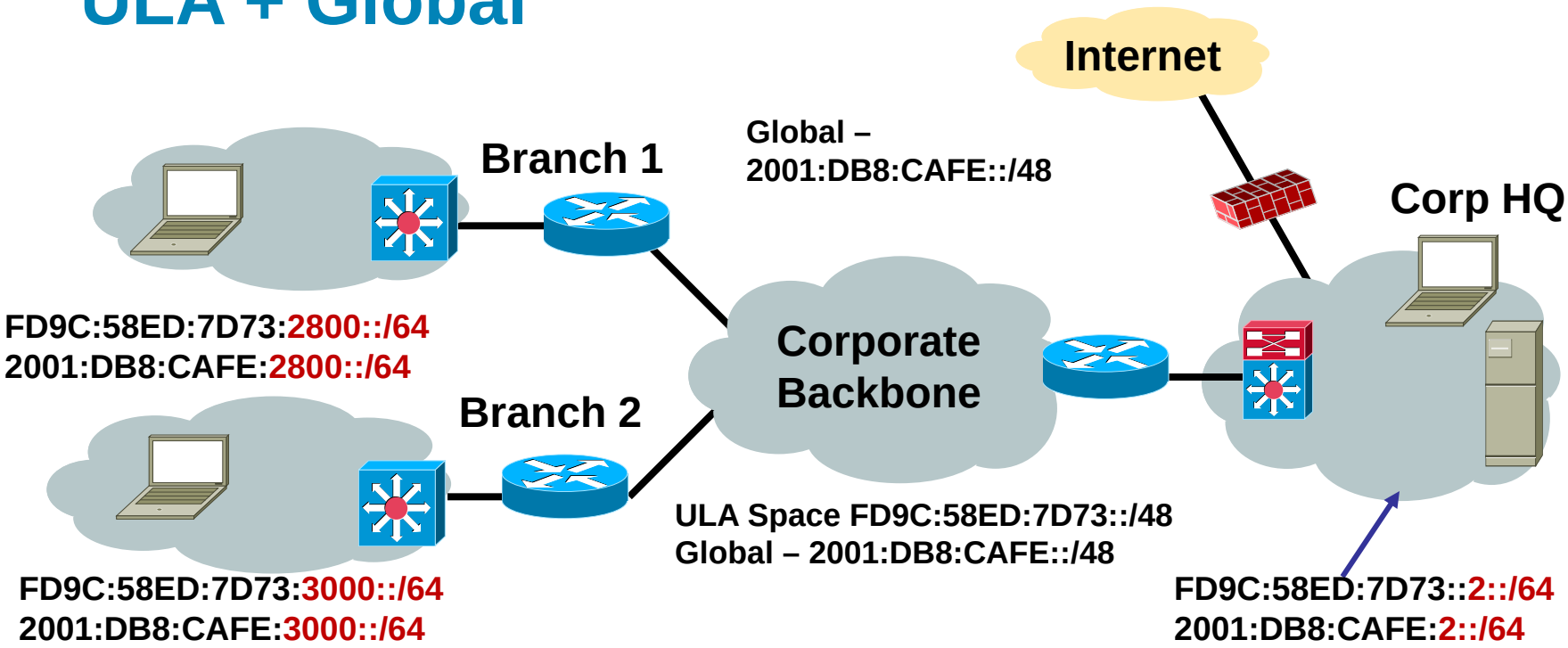
ULA-Only



- Everything internal runs the ULA space
- A NAT supporting IPv6 or a proxy is required to access IPv6 hosts on the internet — must run filters to prevent any SA/DA in ULA range from being forwarded
- Works as it does today with IPv4 except that NAT66 products/solutions do not yet scale like NAT44 and are not widely available…yet
- Removes the advantages of not having a NAT (i.e. application interoperability, global multicast, end-to-end connectivity)

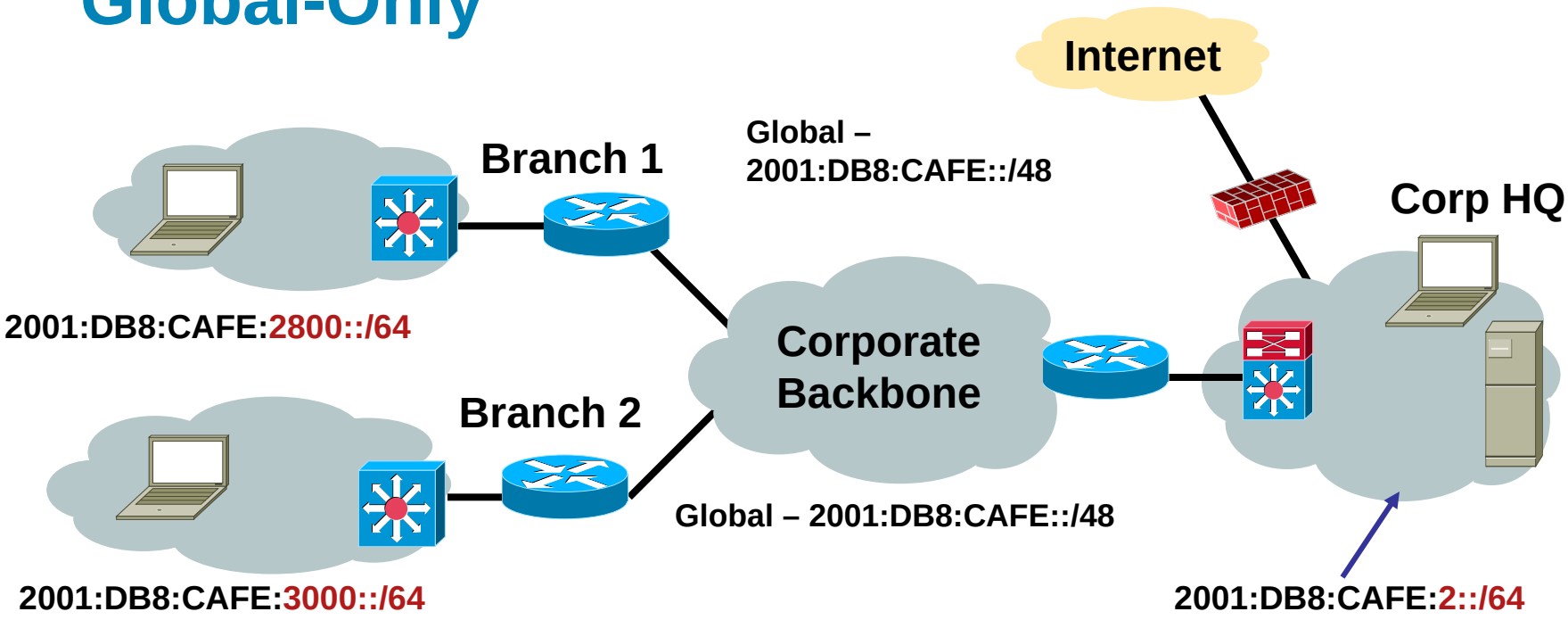
Not Recommended

ULA + Global



- Both ULA and Global are used internally except for internal-only hosts
- Source Address Selection (SAS) is used to determine which address to use when communicating with other nodes internally or externally
- In theory, ULA talks to ULA and Global talks to Global—SAS ‘should’ work this out
- ULA-only and Global-only hosts can talk to one another internal to the network
- Define a filter/policy that ensures your ULA prefix does not ‘leak’ out onto the Internet and ensure that no traffic can come in or out that has a ULA prefix in the SA/DA fields
- Management NIGHTMARE for DHCP, DNS, routing, security, etc…

Global-Only



- Global is used everywhere
- No issues with SAS
- 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 J

Link Level—Prefix Length Considerations

64 bits	> 64 bits
§ Recommended by RFC5375 and IAB/IESG § Consistency makes management easy § MUST for SLAAC (a few other technologies) § Significant address space loss	§ Address space conservation § Special cases: /126—valid for p2p (RFC3627) /127—(RFC6164) /128—loopback § Complicates management § Must avoid overlap with specific addresses: Router Anycast (RFC3513) Embedded RP (RFC3956) ISATAP addresses

SLAAC & Stateful/Stateless DHCPv6

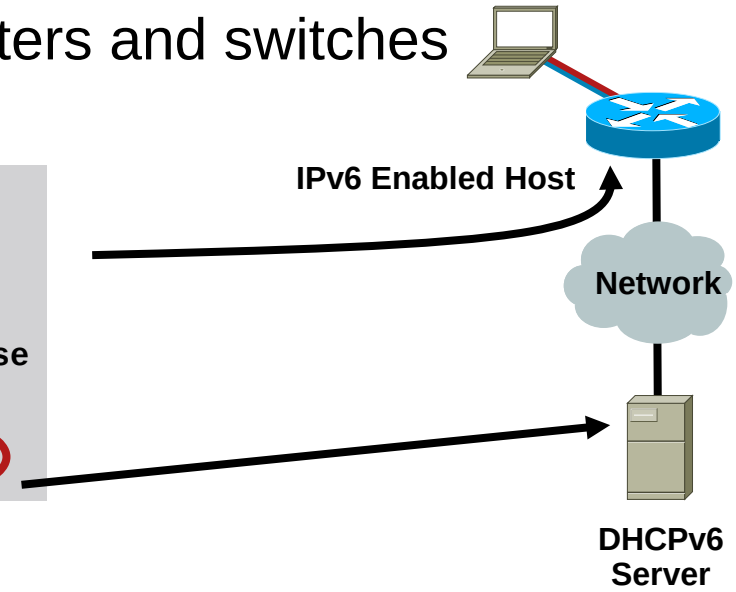
- StateLess Address AutoConfiguration (SLAAC)
- Stateful and stateless DHCPv6 server

  Cisco Network Registrar:
  http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/

  Microsoft Windows Server 2008:
  http://technet2.microsoft.com/windowsserver2008/en/library/bab0f1a1-54aa-4cef-9164-139e8bcc44751033.mspx?mfr=true

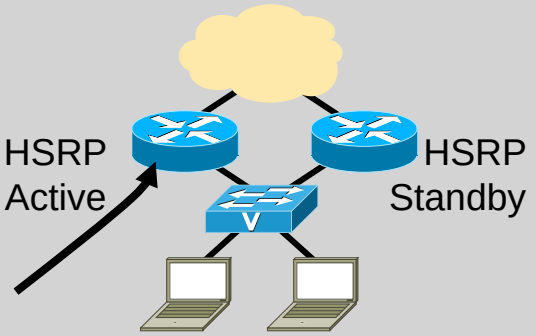
- DHCPv6 Relay—supported on routers and switches

```
interface FastEthernet0/1
 description CLIENT LINK
 ipv6 address 2001:DB8:CAFE:11::1/64
 ipv6 nd prefix 2001:DB8:CAFE:11::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
```



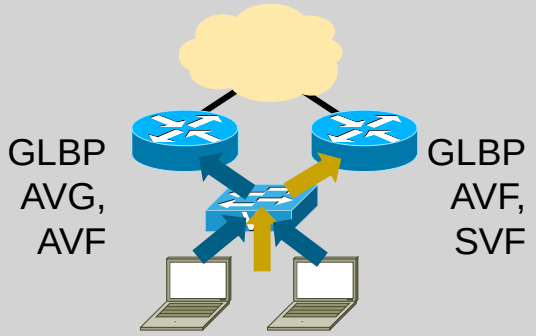
General Concepts FHRP and QOS

First Hop Router Redundancy



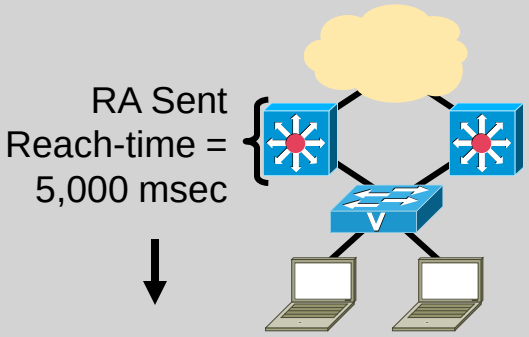
HSRP for v6

- Modification to Neighbor Advertisement, router Advertisement, and ICMPv6 redirects
- Virtual MAC derived from HSRP group number and virtual IPv6 link-local address



GLBP for v6

- Modification to Neighbor Advertisement, Router Advertisement—GW is announced via RAs
- Virtual MAC derived from GLBP group number and virtual IPv6 link-local address



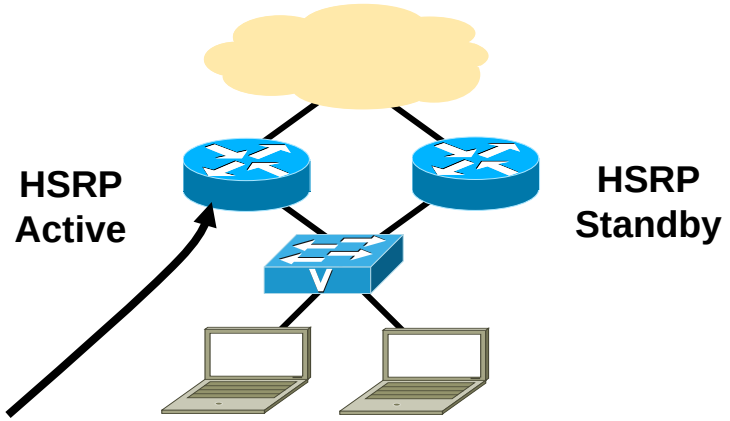
Neighbor **U**nreachability **D**etection

- For rudimentary HA at the first HOP
- Hosts use NUD “reachable time” to cycle to next known default gateway (30s by default)

No longer needed

HSRP for IPv6

- Many similarities with HSRP for IPv4
- Changes occur in Neighbor Advertisement, Router Advertisement, and ICMPv6 redirects
- No need to configure GW on hosts (RAs are sent from HSRP active router)
- Virtual MAC derived from HSRP group number and virtual IPv6 link-local address
- IPv6 Virtual MAC range:
  0005.73A0.0000 - 0005.73A0.0FFF (4096 addresses)
- HSRP IPv6 UDP Port Number 2029 (IANA Assigned)
- No HSRP IPv6 secondary address
- No HSRP IPv6 specific debug




```
interface FastEthernet0/1
 ipv6 address 2001:DB8:66:67::2/64
 ipv6 cef
 standby version 2
 standby 1 ipv6 autoconfig
 standby 1 timers msec 250 msec 800
 standby 1 preempt
 standby 1 preempt delay minimum 180
 standby 1 authentication md5 key-string cisco
 standby 1 track FastEthernet0/0
```

Host with GW of Virtual IP

```
#route -A inet6 | grep ::/0 | grep eth2
::/0      fe80::5:73ff:fea0:1                    UGDA  1024   0        0 eth2
```

IPv6 QoS Policy & Syntax

- Unified QoS Policy (v4/v6 in same policy) or separate?
- IPv4 syntax has used “ip” following match/set statements

  Example: `match ip dscp, set ip dscp`
- Modification in QoS syntax to support IPv6 and IPv4

  New `match` criteria

  `match dscp` – Match DSCP in v4/v6

  `match precedence` – Match Precedence in v4/v6

  New `set` criteria

  `set dscp` – Set DSCP in v4/v6

  `set precedence` – Set Precedence in v4/v6
- Additional support for IPv6 does not always require new Command Line Interface (CLI)

  Example—WRED

Scalability and Performance

- IPv6 Neighbor Cache = ARP for IPv4

  In dual-stack networks the first hop routers/switches will now have more memory consumption due to IPv6 neighbor 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
```

- Full internet route tables—ensure to account for TCAM/memory requirements for both IPv4/IPv6—not all vendors can properly support both
- Multiple routing protocols—IPv4 and IPv6 will have separate routing protocols. Ensure enough CPU/Memory is present
- Control plane impact when using tunnels—terminate ISATAP/configured tunnels in HW platforms when attempting large scale deployments (hundreds/thousands of tunnels)

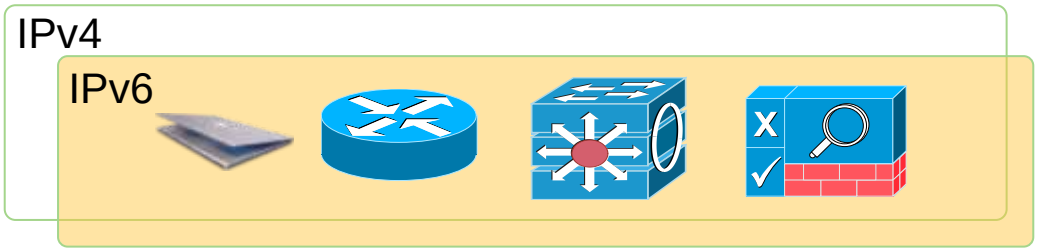
Infrastructure Deployment

Start Here: Cisco IOS Software Release Specifics for IPv6 Features

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html

IPv6 Co-existence Solutions

Dual Stack

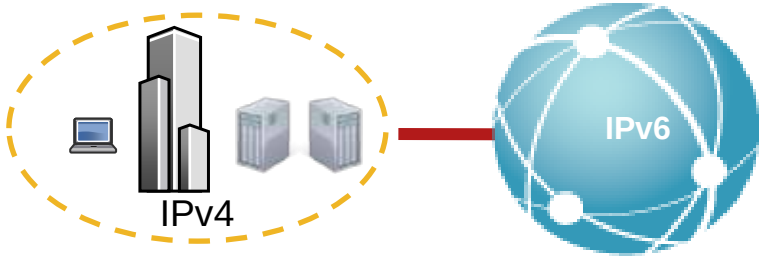


Recommended Enterprise Co-existence strategy

Tunneling Services

Connect Islands of IPv6 or IPv4

Translation Services



Connect to the IPv6 community

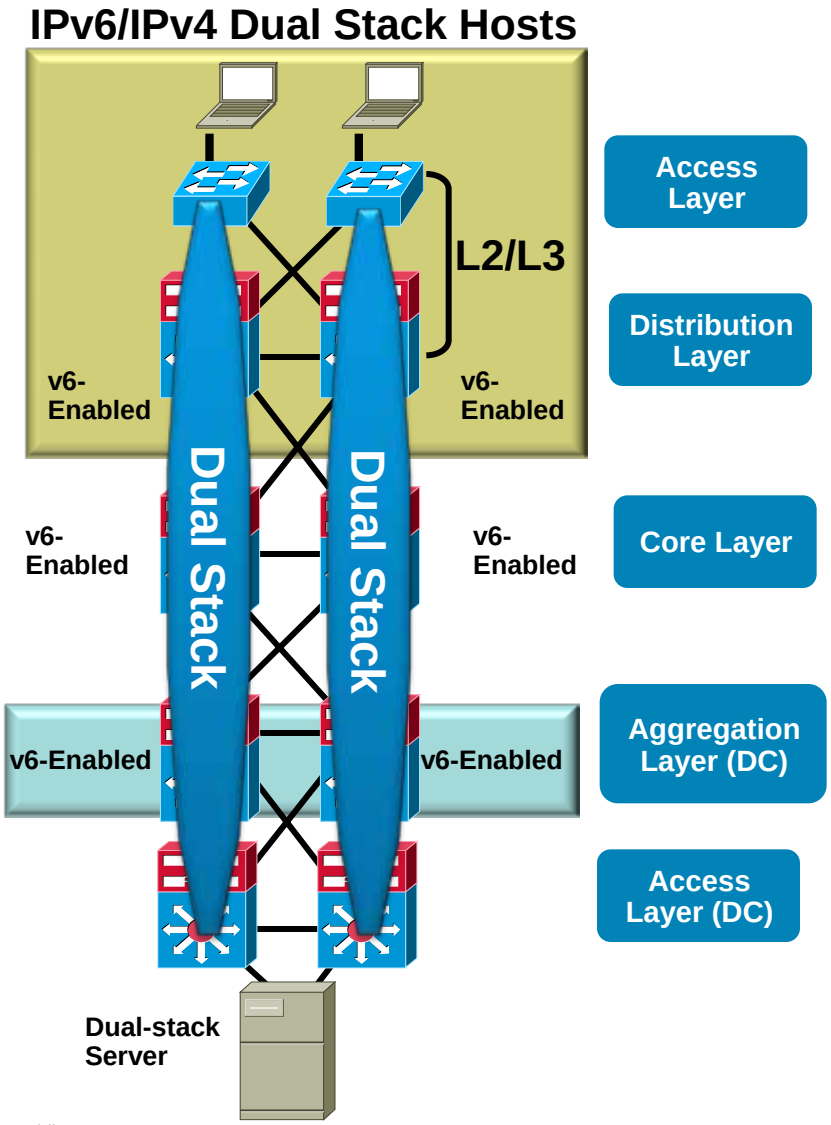
Campus/Data Center

Deploying IPv6 in Campus Networks:
http://www.cisco.com/univercd/cc/td/doc/solution/campipv6.pdf

Campus 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
- VSS supports IPv6



Distribution Layer: HSRP, EIGRP and DHCPv6-relay (Layer 2 Access)

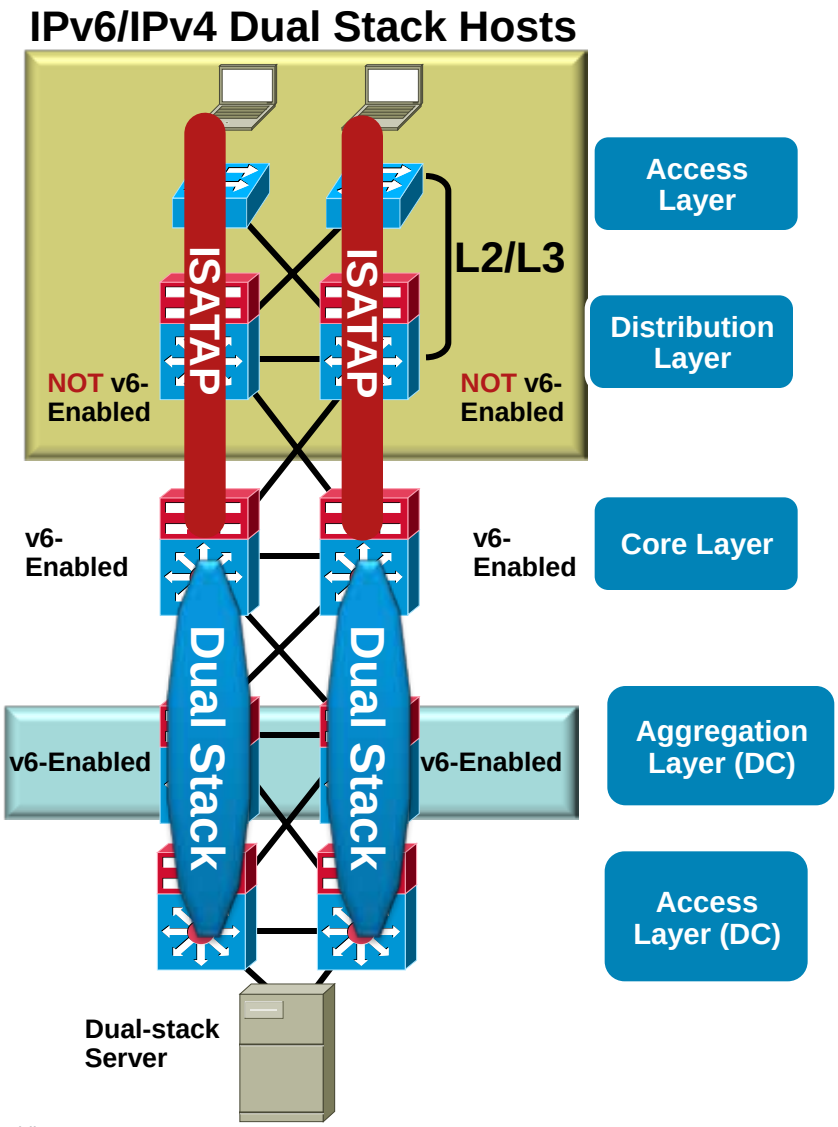
```
ipv6 unicast-routing
!
interface GigabitEthernet1/0/1
 description To 6k-core-right
 ipv6 address 2001:DB8:CAFE:1105::A001:1010/64
 ipv6 eigrp 10
 ipv6 hello-interval eigrp 10 1
 ipv6 hold-time eigrp 10 3
 ipv6 authentication mode eigrp 10 md5
 ipv6 authentication key-chain eigrp 10 eigrp
!
interface GigabitEthernet1/0/2
 description To 6k-core-left
 ipv6 address 2001:DB8:CAFE:1106::A001:1010/64
 ipv6 eigrp 10
 ipv6 hello-interval eigrp 10 1
 ipv6 hold-time eigrp 10 3
 ipv6 authentication mode eigrp 10 md5
 ipv6 authentication key-chain eigrp 10 eigrp
```

```
interface Vlan4
 description Data VLAN for Access
 ipv6 address 2001:DB8:CAFE:4::2/64
 ipv6 nd prefix 2001:DB8:CAFE:4::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2001:DB8:CAFE:10::2
 ipv6 eigrp 10
 standby version 2
 standby 2 ipv6 autoconfig
 standby 2 timers msec 250 msec 750
 standby 2 priority 110
 standby 2 preempt delay minimum 180
 standby 2 authentication ese
!
ipv6 router eigrp 10
 no shutdown
 router-id 10.122.10.10
 passive-interface Vlan4
 passive-interface Loopback0
```

Some OS/patches may need “no-autoconfig”

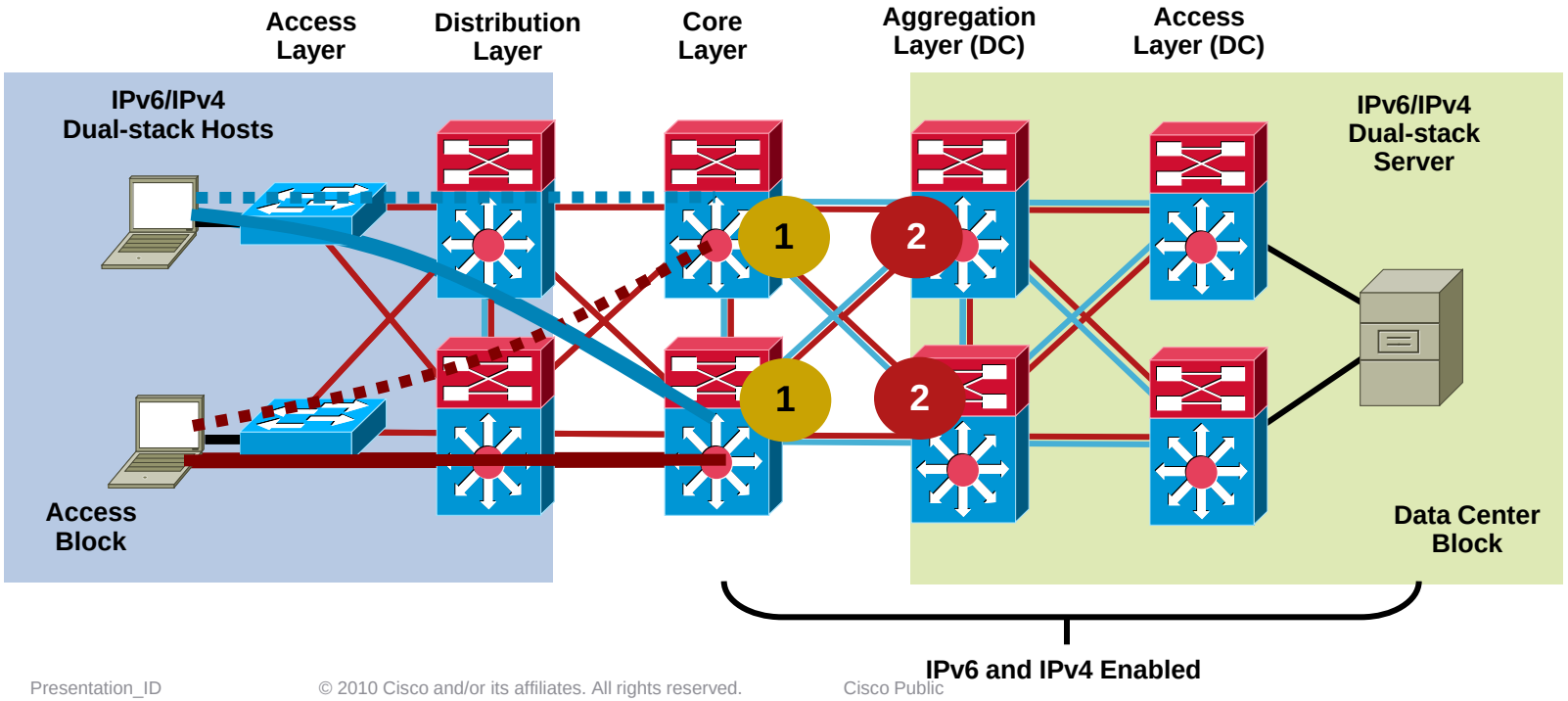
Campus IPv6 Deployment Options
Hybrid Model

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



Campus Hybrid Model 1
QoS

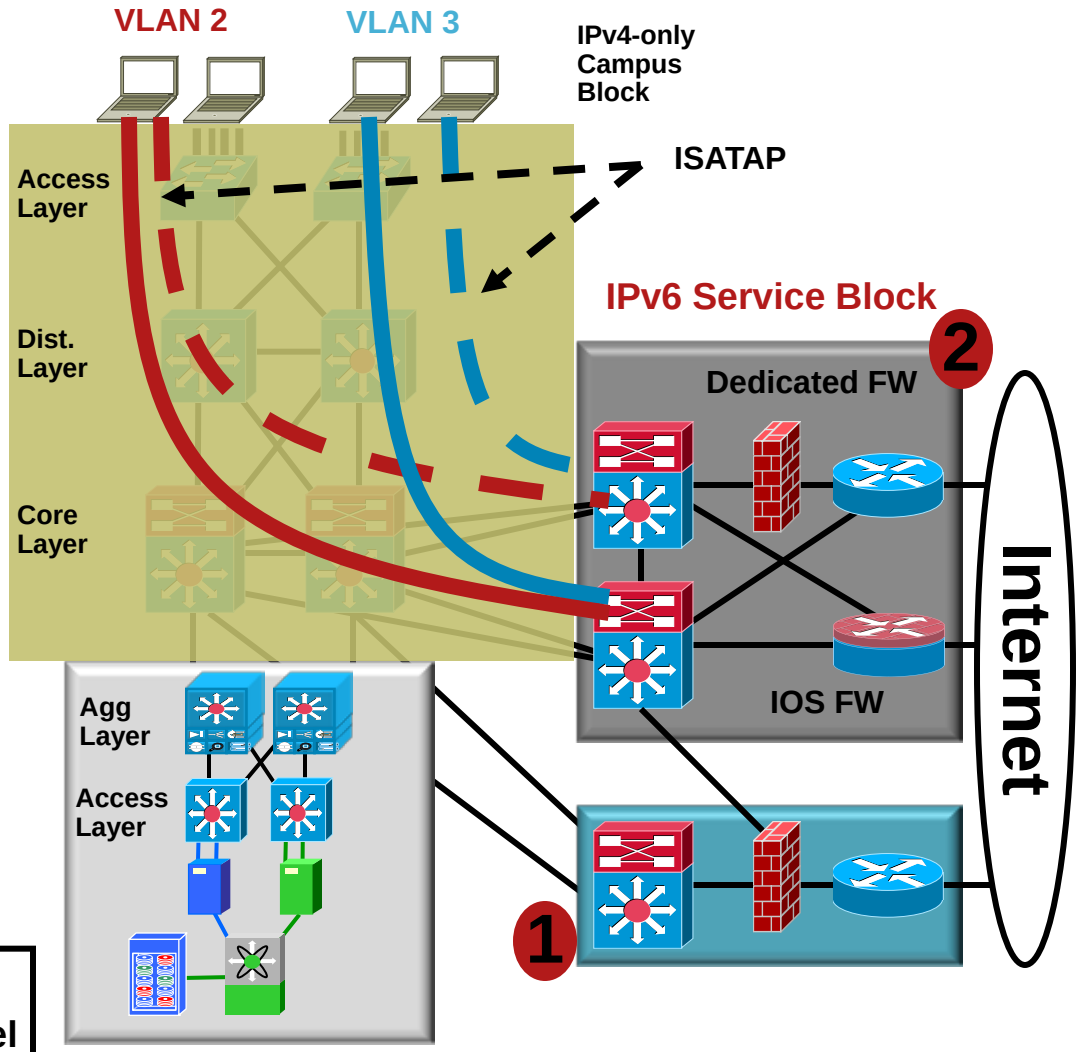
1. Classification and marking of IPv6 is done on the egress interfaces on the core layer switches because packets have been tunneled until this point—QoS policies for classification and marking cannot be applied to the ISATAP tunnels on ingress
2. The classified and marked IPv6 packets can now be examined by upstream switches (e.g. aggregation layer switches) and the appropriate QoS policies can be applied on ingress. These polices may include trust (ingress), policing (ingress) and queuing (egress)



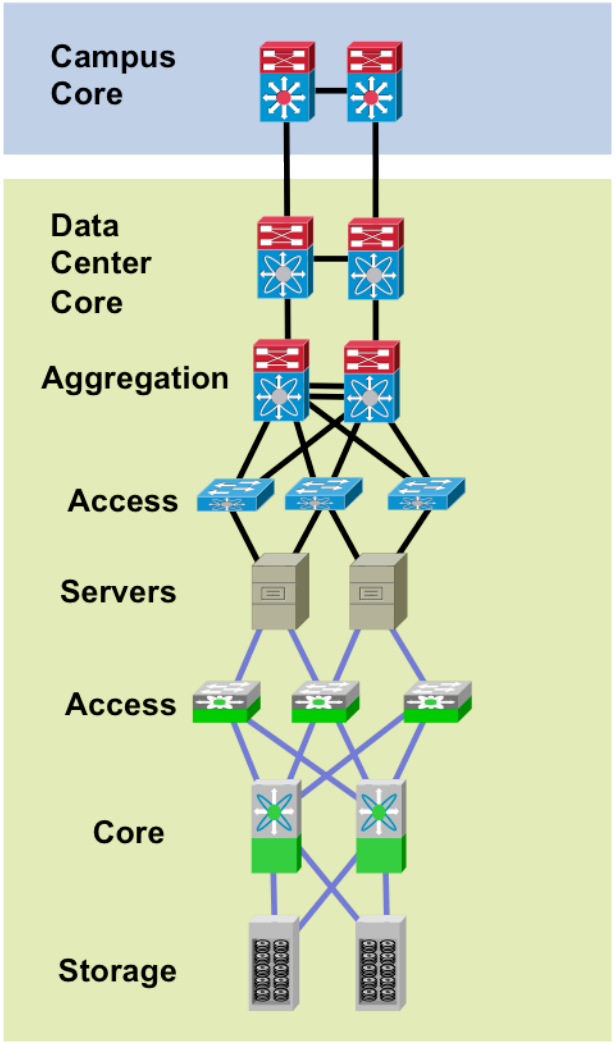
Campus IPv6 Deployment Options

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

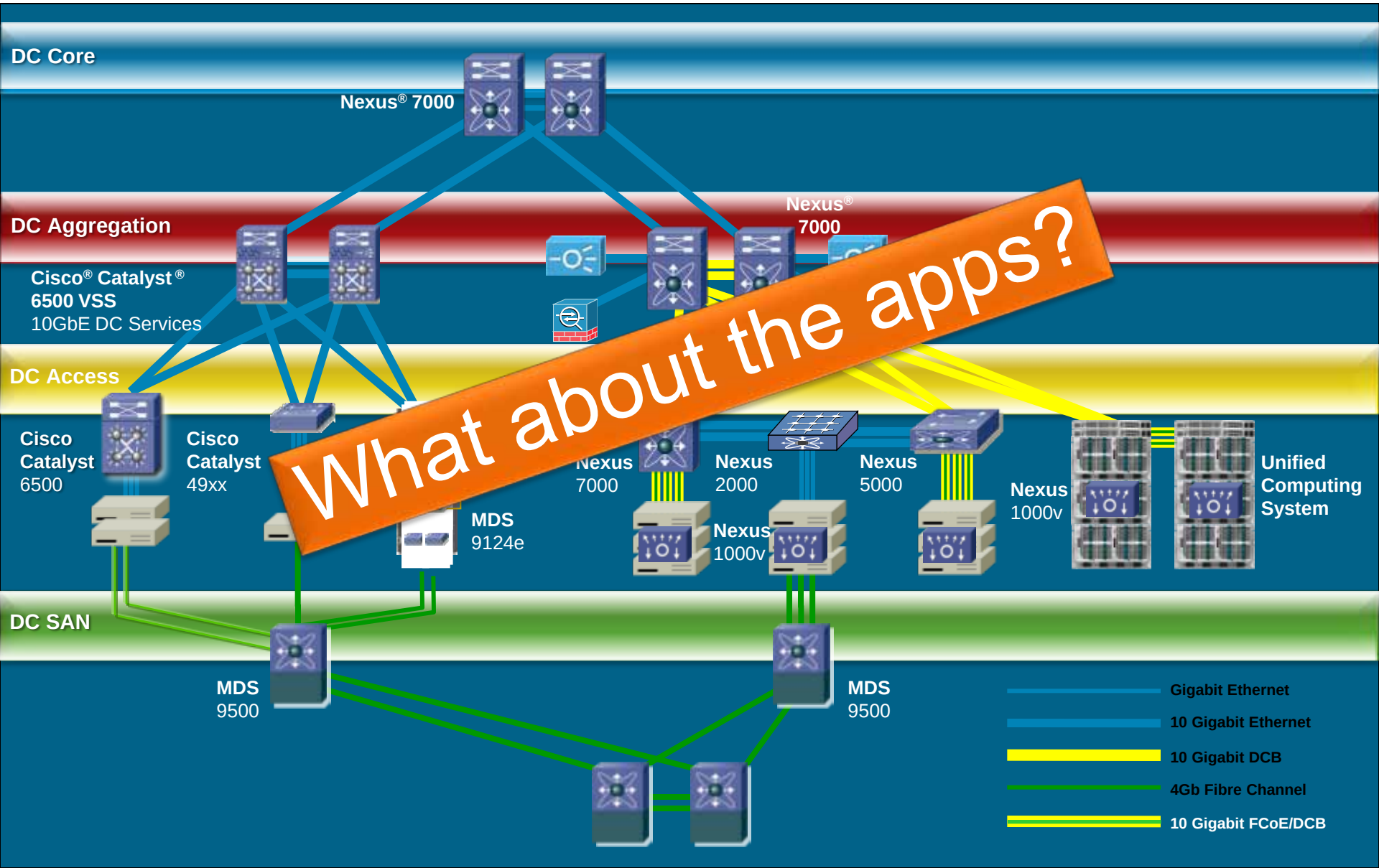


IPv6 Data Center Integration



- The single most overlooked and potentially complicated area of IPv6 deployment
- Route/Switch design will be similar to campus based on feature, platform and connectivity similarities – Nexus, 6500 4900M
- IPv6 for SAN is supported in SAN-OS 3.0
- Stuff people don't think about:
  - NIC Teaming, iLO, DRAC, IP KVM, Clusters
  - Innocent looking Server OS upgrades – Windows Server 2008 - Impact on clusters – Microsoft Server 2008 Failover clusters full support IPv6 (and L3)
- Build an IPv6-only server farm?

Virtualized DC Solutions



IPv6 in the Enterprise Data Center
Biggest Challenges Today

- Network services above L3
  - SLB, SSL-Offload, application monitoring (probes) – ACE and GSS
  - Application Optimization – WAAS and ACE
  - High-speed security inspection/perimeter protection – ASA/IPS/IDS/IronPort
- Application support for IPv6 – Know what you don't know
  - If an application is protocol centric (IPv4):
    - Leave as-is
    - Needs to be rewritten
    - Needs to be translated until it is replaced
    - Wait and pressure vendors to move to protocol agnostic framework
- Virtualized and Consolidated Data Centers
  - Virtualization '*should*' make DCs simpler and more flexible
  - Lack of robust DC/Application management is often the root cause of all evil
  - Ensure management systems support IPv6 as well as the devices being managed

Commonly Deployed IPv6-enabled OS/Apps

Operating Systems

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

Virtualization & Applications

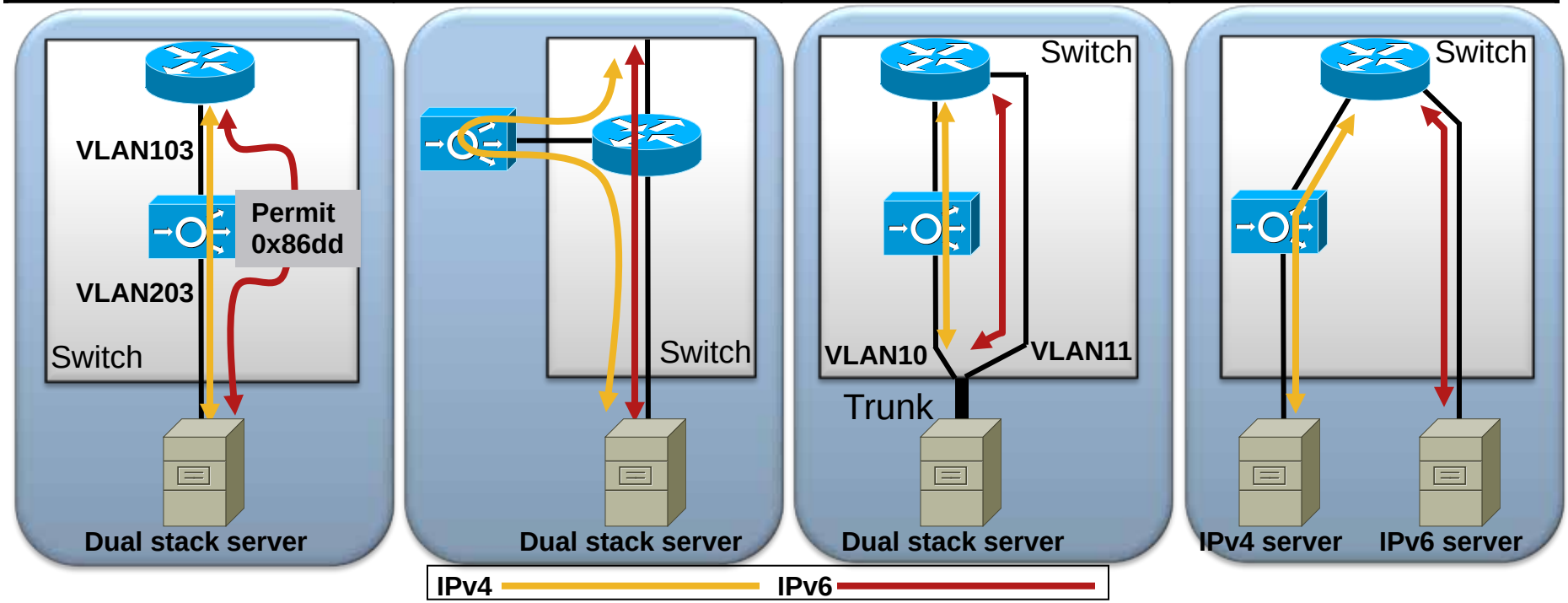
- VMware vSphere 4.1
- Microsoft Hyper-V
- Microsoft Exchange 2007 SP1/2010
- Apache/IIS Web Services
- Windows Media Services
- Multiple Line of Business apps

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

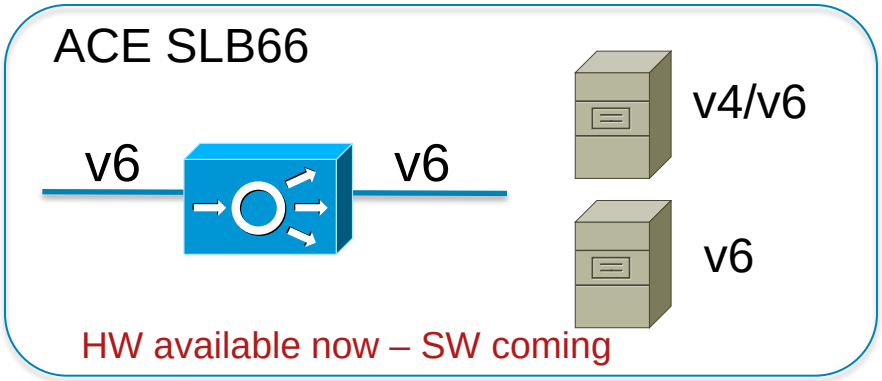
IPv6 Deployment in the Data Center

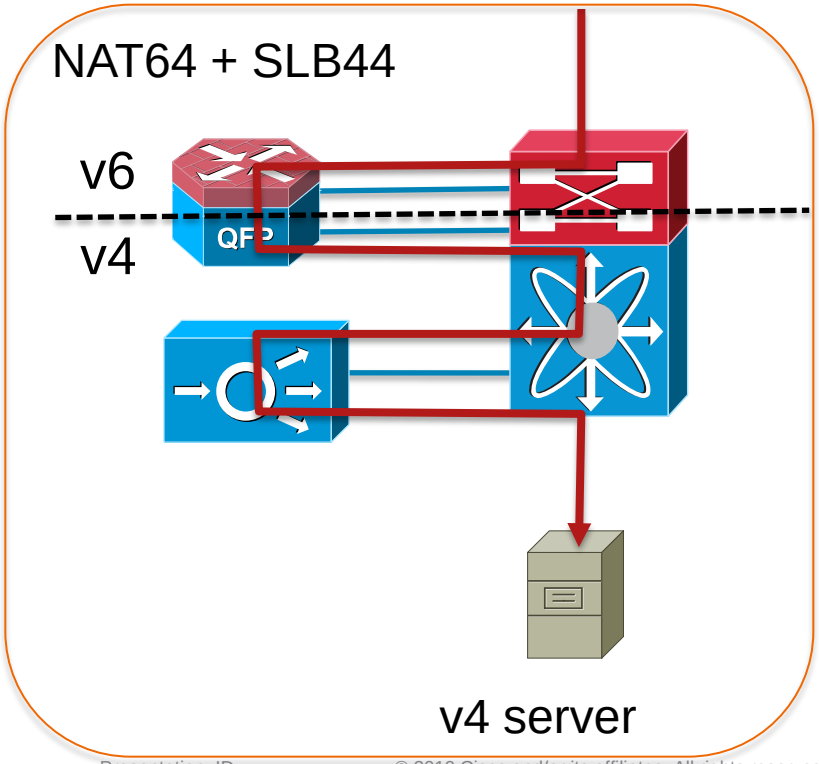
Services/Appliances Do Not Support IPv6

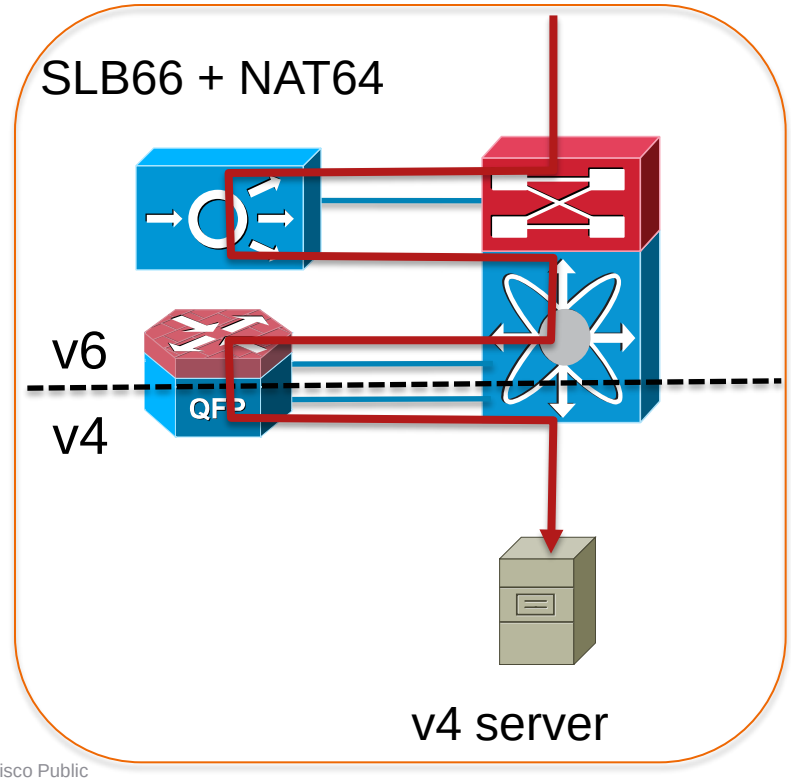
Transparent	One-Armed	Routed	Dedicated Server Farm
§ IPv6 traffic is bridged between VLANs § Permit Ethertype 0x86dd (IPv6)	§ IPv6 traffic bypasses services § IPv4 traffic is sent to one-arm attached module/appliance	§ Create trunk between switch and server § IPv4 has default gateway on service module § IPv6 on separate VLAN to MSFC	§ New IPv6 only servers can be connected to existing access/agg pair on different VLANs § New access/agg switches just for IPv6 servers



ACE + IPv6 / ACE + ASR + NAT64





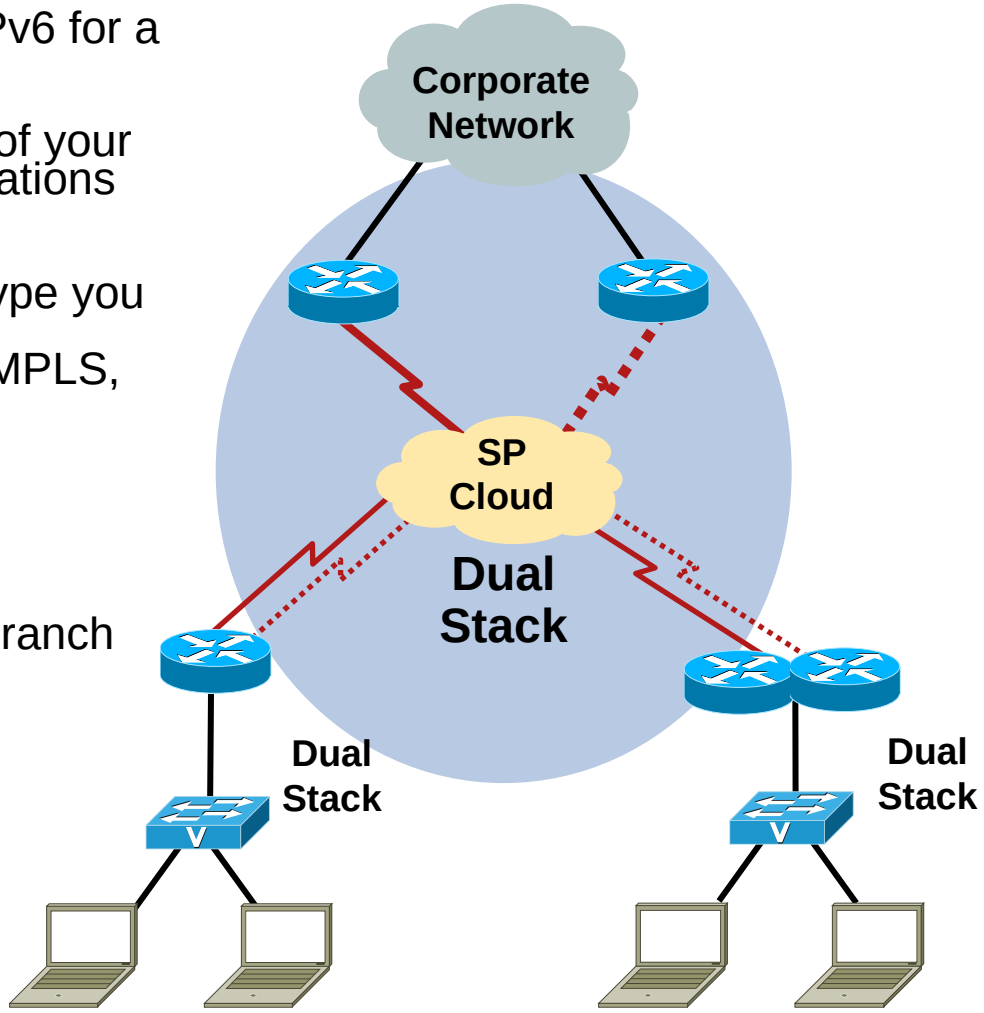


WAN/Branch

Deploying IPv6 in Branch Networks:
http://www.cisco.com/univercd/cc/td/doc/solution/brchipv6.pdf

WAN/Branch Deployment

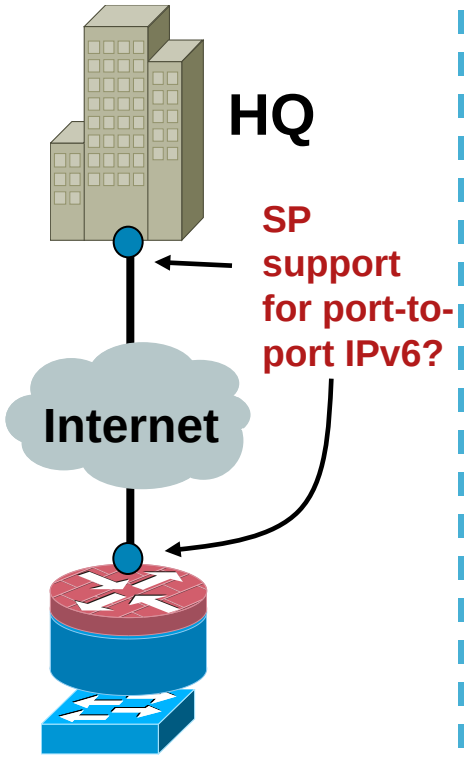
- Cisco routers have supported IPv6 for a long time
- Dual-stack should be the focus of your implementation—but, some situations still call for tunneling
- Support for every media/WAN type you want to use (Frame Relay, leased-line, broadband, MPLS, etc.)
- Don’t assume all features for every technology are IPv6-enabled
- Better feature support in WAN/branch than in campus/DC



IPv6 Enabled Branch

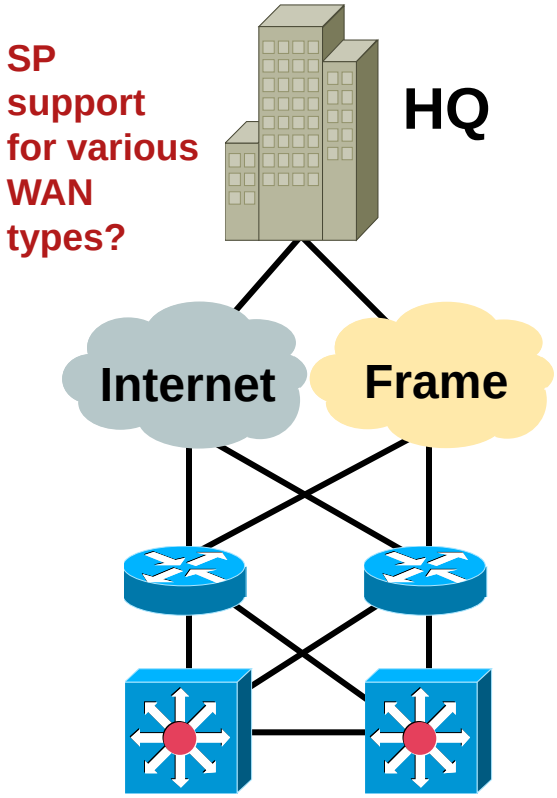
Focus more on the provider and less on the gear

Branch Single Tier



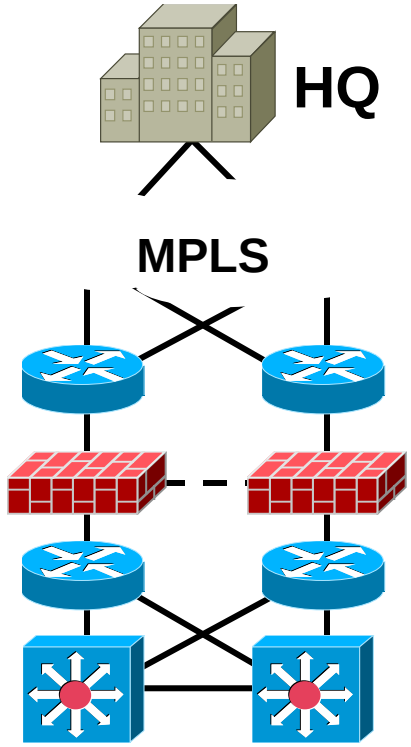
Dual-Stack
IPSec VPN (IPv4/IPv6)
Firewall (IPv4/IPv6)
Integrated Switch (MLD-snooping)

Branch Dual Tier



Dual-Stack
IPSec VPN or Frame Relay
Firewall (IPv4/IPv6)
Switches (MLD-snooping)

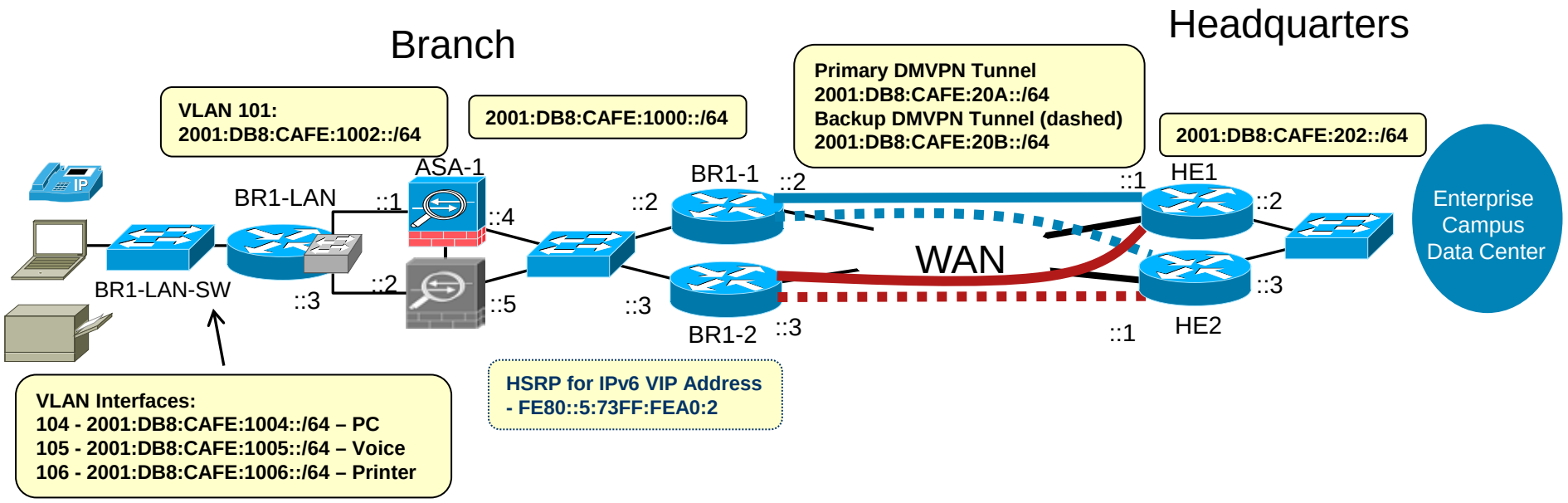
Branch Multi-Tier



Dual-Stack
IPSec VPN or
MPLS (6PE/6VPE)
Firewall (IPv4/IPv6)
Switches (MLD-snooping)

Hybrid Branch Example

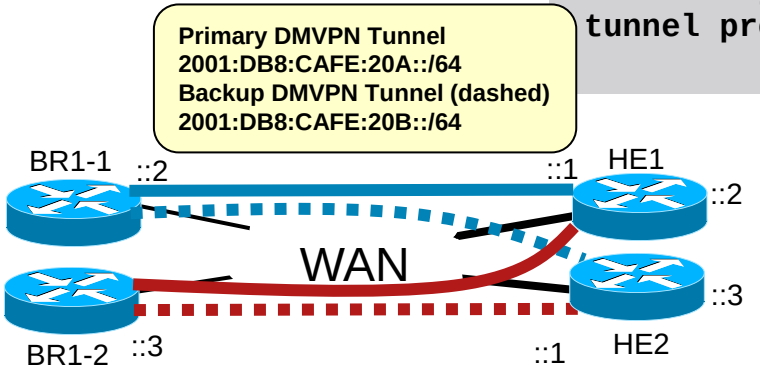
- Mixture of attributes from each profile
- An example to show configuration for different tiers
- Basic HA in critical roles is the goal



DMVPN with IPv6
Hub Configuration Example

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
crypto isakmp key CISCO address ipv6 ::/0
!
crypto ipsec transform-set HUB esp-aes 256 esp-sha-hmac
!
crypto ipsec profile HUB
 set transform-set HUB
```

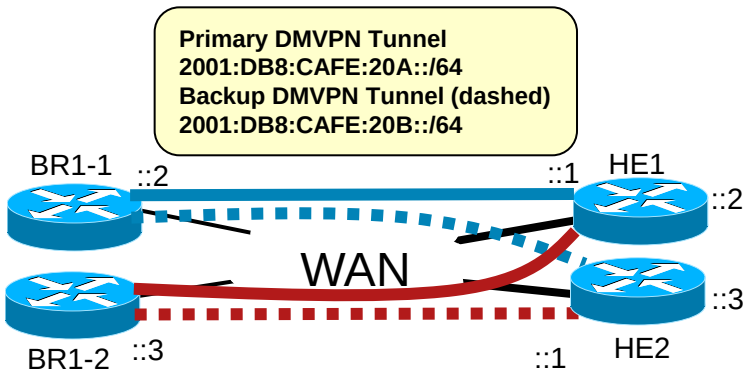
```
interface Tunnel0
 description DMVPN Tunnel 1
 ip address 10.126.1.1 255.255.255.0
 ipv6 address 2001:DB8:CAFE:20A::1/64
 ipv6 mtu 1416
 ipv6 eigrp 10
 ipv6 hold-time eigrp 10 35
 no ipv6 next-hop-self eigrp 10
 no ipv6 split-horizon eigrp 10
 ipv6 nhrp authentication CISCO
 ipv6 nhrp map multicast dynamic
 ipv6 nhrp network-id 10
 ipv6 nhrp holdtime 600
 ipv6 nhrp redirect
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 10
 tunnel protection ipsec profile HUB
```



DMVPN with IPv6

Spoke Configuration Example

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
crypto isakmp key CISCO address ipv6 ::/0
!
crypto ipsec transform-set SPOKE esp-aes 256 esp-sha-hmac
!
crypto ipsec profile SPOKE
 set transform-set SPOKE
```




```
interface Tunnel0
 description to HUB
 ip address 10.126.1.2 255.255.255.0
 ipv6 address 2001:DB8:CAFE:20A::2/64
 ipv6 mtu 1416
 ipv6 eigrp 10
 ipv6 hold-time eigrp 10 35
 no ipv6 next-hop-self eigrp 10
 no ipv6 split-horizon eigrp 10
 ipv6 nhrp authentication CISCO
 ipv6 nhrp map 2001:DB8:CAFE:20A::1/64 172.16.1.1
 ipv6 nhrp map multicast 172.16.1.1
 ipv6 nhrp network-id 10
 ipv6 nhrp holdtime 600
 ipv6 nhrp nhs 2001:DB8:CAFE:20A::1
 ipv6 nhrp shortcut
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 10
 tunnel protection ipsec profile SPOKE
```

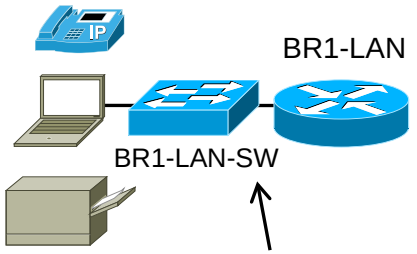
ASA with IPv6

Snippet of full config – examples of IPv6 usage

```
name 2001:db8:cafe:1003:: BR1-LAN description VLAN on EtherSwitch
name 2001:db8:cafe:1004:9db8:3df1:814c:d3bc Br1-v6-Server
!
interface GigabitEthernet0/0
 description TO WAN
 nameif outside
 security-level 0
 ip address 10.124.1.4 255.255.255.0 standby 10.124.1.5
 ipv6 address 2001:db8:cafe:1000::4/64 standby 2001:db8:cafe:1000::5
!
interface GigabitEthernet0/1
 description TO BRANCH LAN
 nameif inside
 security-level 100
 ip address 10.124.3.1 255.255.255.0 standby 10.124.3.2
 ipv6 address 2001:db8:cafe:1002::1/64 standby 2001:db8:cafe:1002::2
!
ipv6 route inside BR1-LAN/64 2001:db8:cafe:1002::3
ipv6 route outside ::/0 fe80::5:73ff:fea0:2
!
ipv6 access-list v6-ALLOW permit icmp6 any any
ipv6 access-list v6-ALLOW permit tcp 2001:db8:cafe::/48 host Br1-v6-Server object-group RDP
!
failover
failover lan unit primary
failover lan interface FO-LINK GigabitEthernet0/3
failover interface ip FO-LINK 2001:db8:cafe:1001::1/64 standby 2001:db8:cafe:1001::2
access-group v6-ALLOW in interface outside
```

Branch LAN
Connecting Hosts

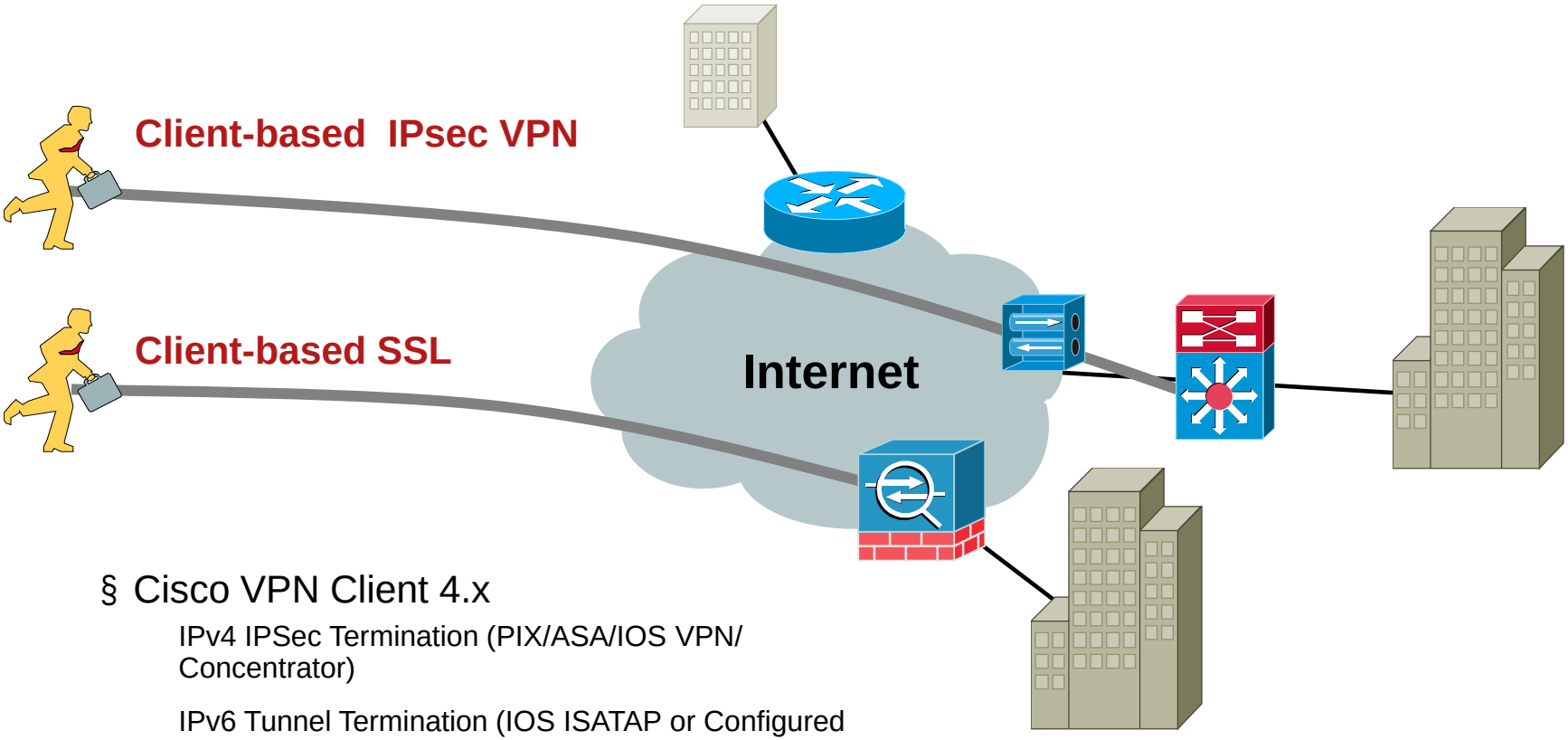
```
ipv6 dhcp pool DATA_W7
 dns-server 2001:DB8:CAFE:102::8
 domain-name cisco.com
!
interface GigabitEthernet0/0
 description to BR1-LAN-SW
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.104
 description VLAN-PC
 encapsulation dot1Q 104
 ip address 10.124.104.1 255.255.255.0
 ipv6 address 2001:DB8:CAFE:1004::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server DATA_W7
 ipv6 eigrp 10
!
interface GigabitEthernet0/0.105
 description VLAN-PHONE
 encapsulation dot1Q 105
 ip address 10.124.105.1 255.255.255.0
 ipv6 address 2001:DB8:CAFE:1005::1/64
 ipv6 nd prefix 2001:DB8:CAFE:1005::/64 0 0 no-autoconfig
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2001:DB8:CAFE:102::9
 ipv6 eigrp 10
```



VLAN Interfaces:
104 - 2001:DB8:CAFE:1004::/64 – PC
105 - 2001:DB8:CAFE:1005::/64 – Voice
106 - 2001:DB8:CAFE:1006::/64 – Printer

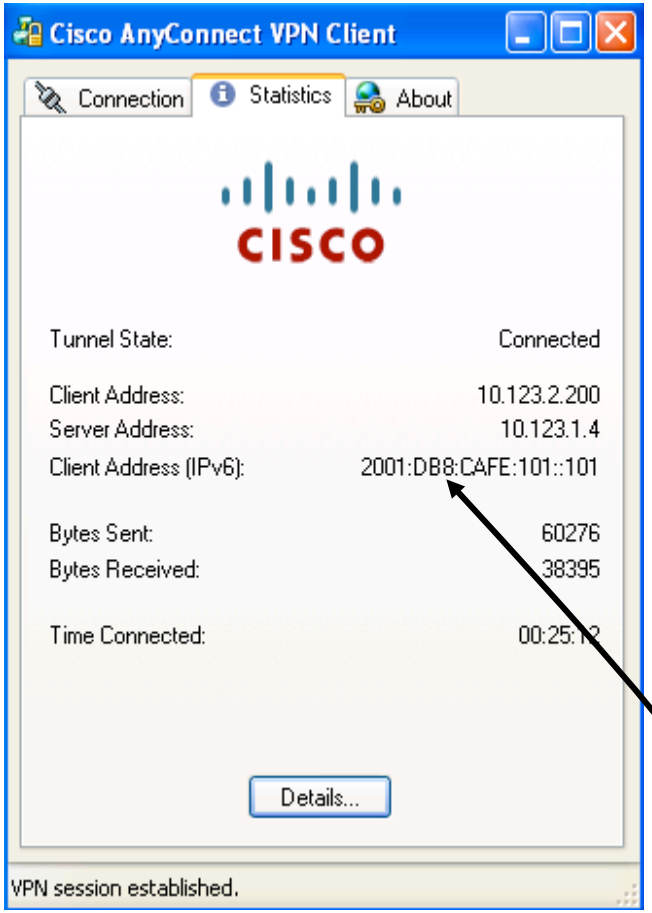
Remote Access

Cisco Remote VPN – IPv6

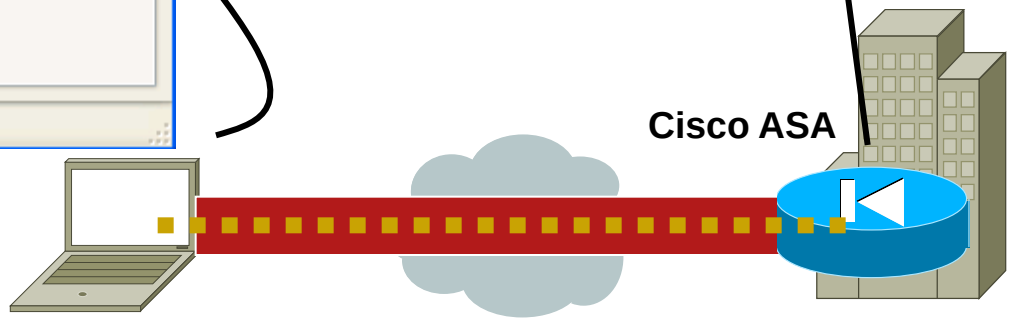


- Cisco VPN Client 4.x
  - IPv4 IPSec Termination (PIX/ASA/IOS VPN/ Concentrator)
  - IPv6 Tunnel Termination (IOS ISATAP or Configured Tunnels)
- AnyConnect Client 2.x
  - SSL/TLS or DTLS (datagram TLS = TLS over UDP)
  - Tunnel transports both IPv4 and IPv6 and the packets exit the tunnel at the hub ASA as native IPv4 and IPv6.

AnyConnect 2.x—SSL VPN



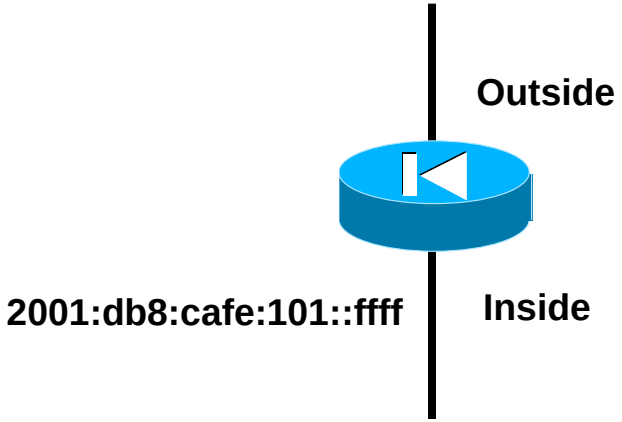

```
asa-edge-1#show vpn-sessiondb svc
Session Type: SVC
Username     : ciscoese              Index        : 14
Assigned IP  : 10.123.2.200          Public IP    : 10.124.2.18
Assigned IPv6: 2001:db8:cafe:101::101
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : SSL VPN
Encryption   : RC4 AES128            Hashing      : SHA1
Bytes Tx     : 79763                 Bytes Rx     : 176080
Group Policy : AnyGrpPolicy          Tunnel Group: ANYCONNECT
Login Time   : 14:09:25 MST Mon Dec 17 2007
Duration     : 0h:47m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```



Dual-Stack Host
AnyConnect Client

AnyConnect 2.x—Summary Configuration

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.123.1.4 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.123.2.4 255.255.255.0
 ipv6 address 2001:db8:cafe:101::ffff/64
!
ipv6 local pool ANYv6POOL 2001:db8:cafe:101::101/64 200
```

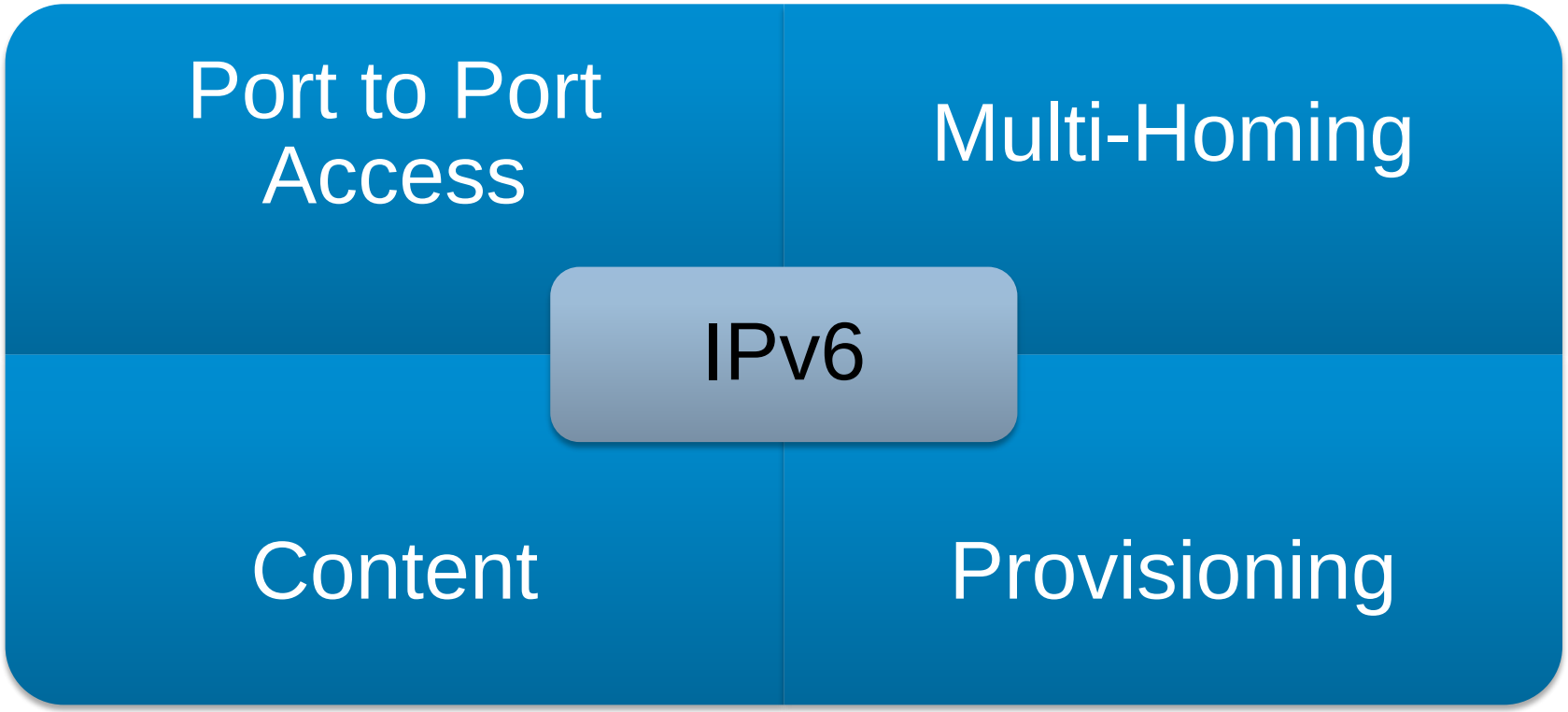



```
webvpn
 enable outside
 svc enable
 tunnel-group-list enable
group-policy AnyGrpPolicy internal
group-policy AnyGrpPolicy attributes
 vpn-tunnel-protocol svc
 default-domain value cisco.com
 address-pools value AnyPool
tunnel-group ANYCONNECT type remote-access
tunnel-group ANYCONNECT general-attributes
 address-pool AnyPool
 ipv6-address-pool ANYv6POOL
 default-group-policy AnyGrpPolicy
tunnel-group ANYCONNECT webvpn-attributes
 group-alias ANYCONNECT enable
```

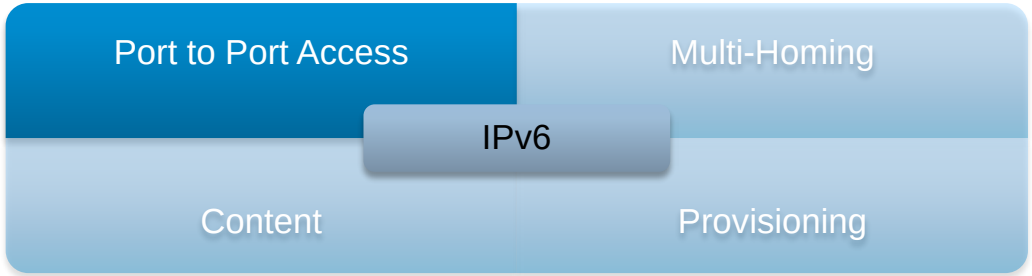
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin6.html#wp1002258

Communicating with the Service Provider

Top SP Concerns for Enterprise Accounts



Port-to-Port Access



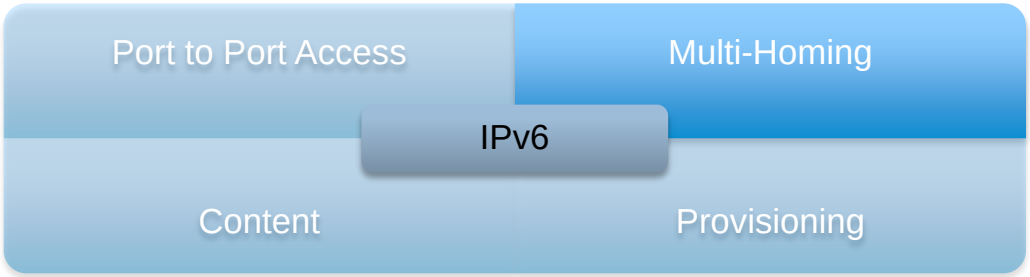
Basic Internet*
- Dual-stack or native IPv6 at each POP
- SLA driven just like IPv4 to support VPN, content access

MPLS
- 6VPE
- IPv6 Multicast
- End-to-End traceability

Hosted (see content)
- IPv6 access to hosted content
- Cloud migration (move data from Ent DC to Hosted DC)

* = most common issue

Multi-Homing



PI/PA Policy * Concerns

- PA is no good for customers with multiple providers or change them at any pace
- PI is new, constantly changing expectations and no “guarantee” an SP won’t do something stupid like not route PI space
- Customers fear that RIR will review existing IPv4 space and want it back if they get IPv6 PI

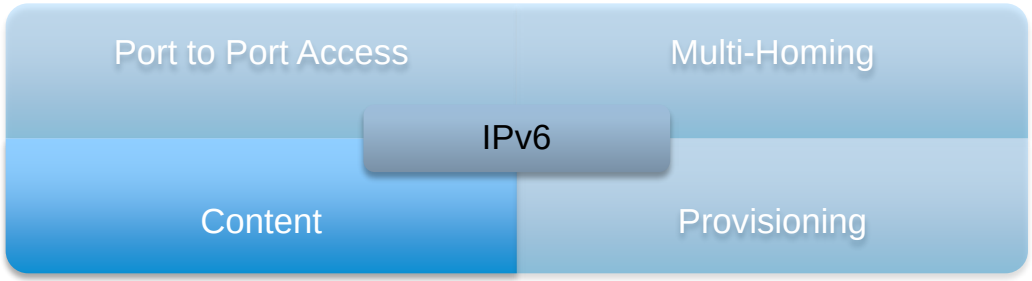
NAT

- Religious debate about the security exposure – not a multi-homing issue
- If customer uses NAT like they do today to prevent address/policy exposure, where do they get the technology from – no scalable IPv6 NAT exists today

Routing

- Is it really different from what we do today with IPv4? Is this policy stuff?
- Guidance on prefixes per peering point, per theater, per ISP, ingress/egress rules, etc.. – this is largely missing today

Content



Hosted/Cloud Apps today*

- IPv6 provisioning and access to hosted or cloud-based services today (existing agreements)
- Salesforce.com, Microsoft BPOS (Business Productivity Online Services), Amazon, Google Apps

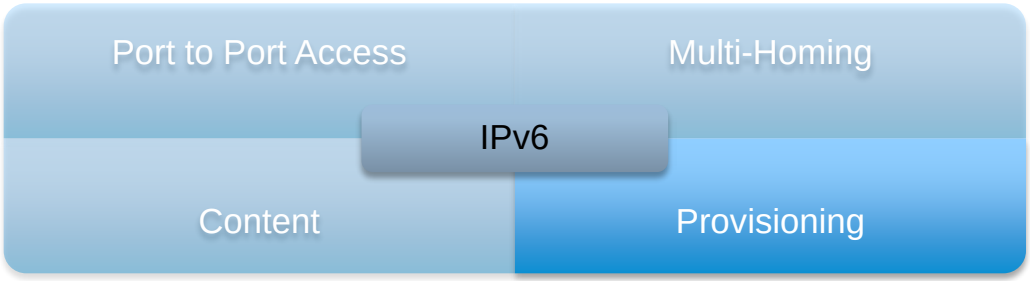
Move to Hosted/Cloud

- Movement from internal-only DC services to hosted/cloud-based DC
- Provisioning, data/network migration services, DR/HA

Contract/Managed Marketing/Portals

- Third-party marketing, business development, outsourcing
- Existing contracts – connect over IPv6

Provisioning



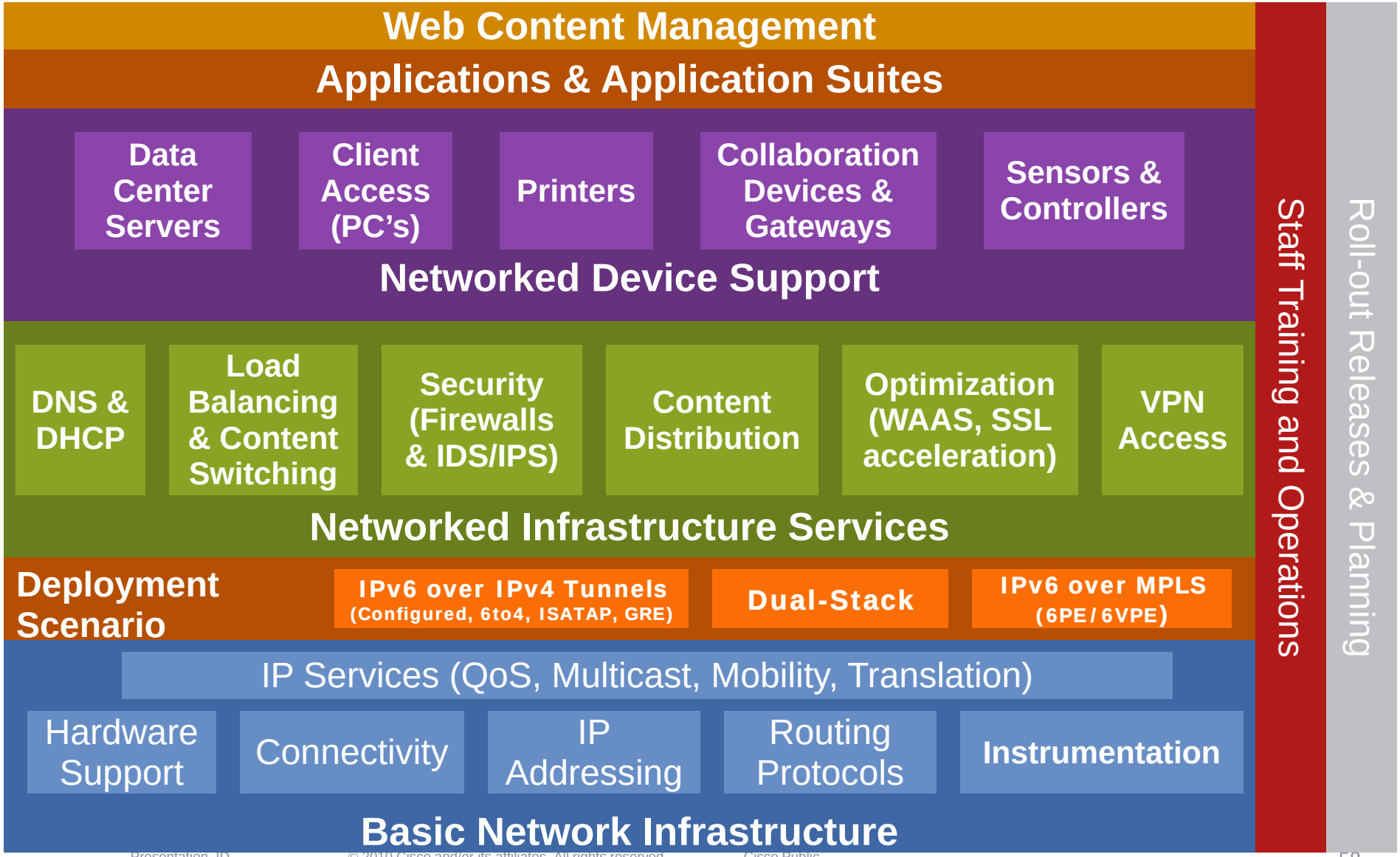
SP Self-Service Portals

- Not a lot of information from accounts on this but it does concern them
- How can they provision their own services (i.e. cloud) to include IPv6 services and do it over IPv6

SLA *

- More of a management topic but the point here is that customers want the ability to alter their services based on violations, expiration or restrictions on the SLA
- Again, how can they do this over IPv6 AND for IPv6 services

The Scope of IPv6 Deployment



IPv6 + VDI and/or High-density VM

- Movement to Virtual Desktop Infrastructure and large scale VM deployments leads customers to the question – how many VMs can I get on a single VLAN?
  - Today - Limited to broadcast domain and ARP scaling
  - IPv6 has no broadcast – what is the control plane impact of having only IPv6 multicast for neighbor/router activity? Less/Same??
  - Can I greatly increase the number of hosts/VMs per VLAN without IPv4?
- Can IPv6 solve my internal RFC1918 starvation issue – specifically inside my Data Center?
  - Most VDI deployments are ‘additive’ in host count not a direct 1:1 replacement from thick-to-thin/zero client
- Building on interest and possibilities with LISP

Conclusion

- “Dual stack where you can – Tunnel where you must – Translate only when you have a gun to your head”
- 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, Windows 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

For conference presentations visit:

www.networkerssolutionsforum.com

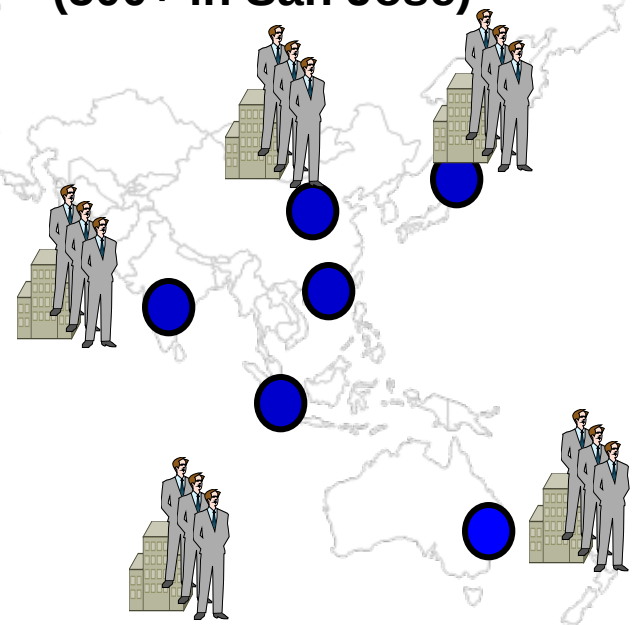
Please take a moment to complete the Networkers Conference Event Evaluation Form

Thank you.

What is Cisco doing?

Information about Cisco

- 300 locations in 90 countries
- 400 buildings
- 51 data centers and server rooms
- 1500+ labs world wide (500+ in San Jose)
- 66,000+ Employees
- 20,000 Channel Partners
- 110+ Application Service Providers
- 210+ Business and Support Development Partners



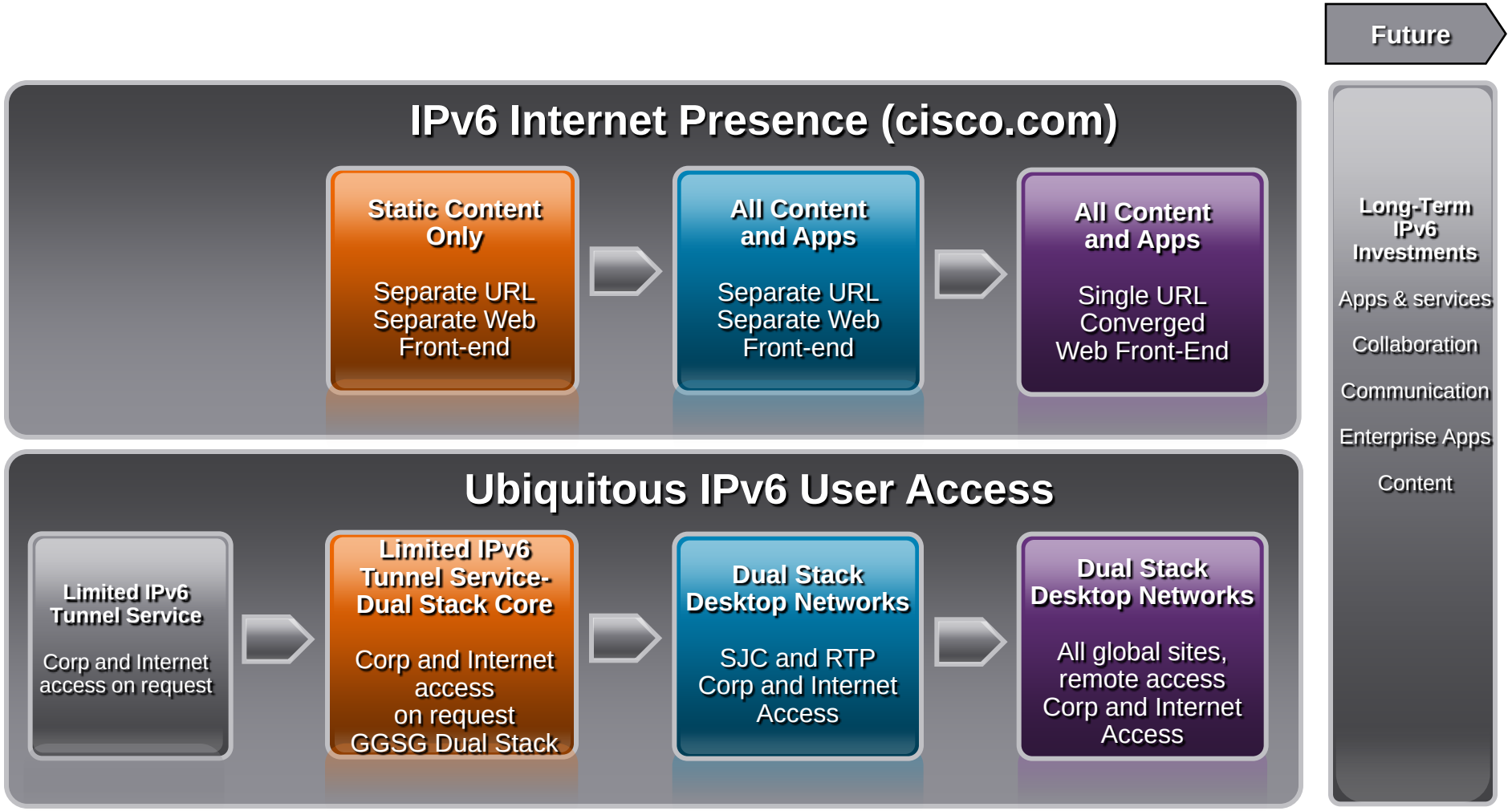
Over 180,000 people around the world in the extended Cisco family

ASIAPAC | N. America | S. America | Europe | Middle East

Drivers and Goals

- Business Drivers
  1. IPv6 leadership and mindshare
  2. IPv6 product and solution readiness
- IT Drivers
  1. Corporate Growth (IPv4 Address Depletion)
  2. Enable IPv6 Infrastructure for development and testing
  3. Cisco on Cisco
- Goals
  1. cisco.com IPv6 Internet presence
  2. Enable ubiquitous IPv6-enabled user access in the network
  3. End to end IPv6 (Dual Stack)

Cisco IT's IPv6 Strategy



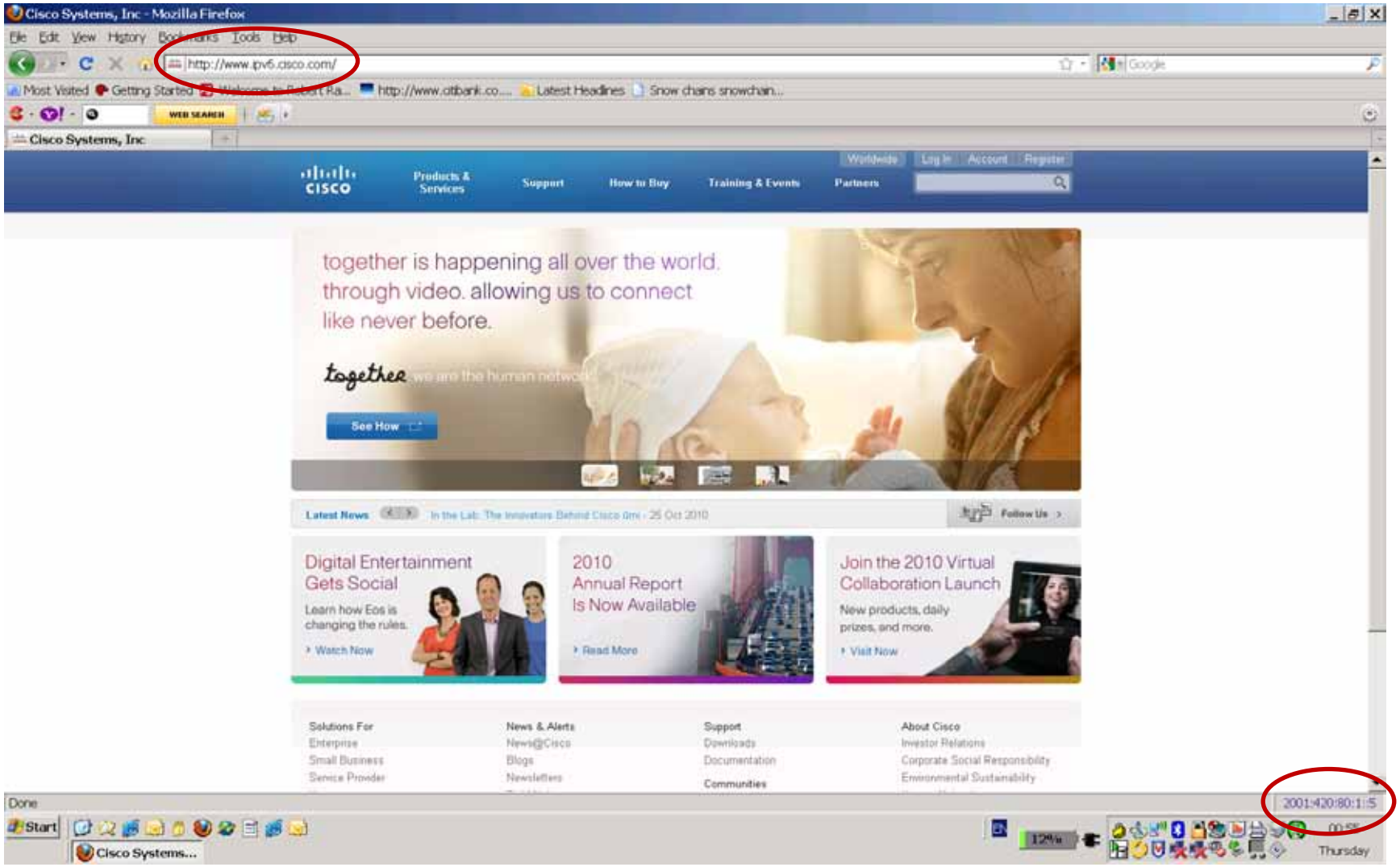
IPv6 Deployment Plan (Ubiquitous IPv6 User Access)

- Pilot Phase (Completed)
  - Ø Single Tunnel Head End with Tunnelled IPv6 Internet Connectivity
  - Ø Offers 6in4 Tunnels for Labs and ISATAP for Desktop users
- Phase 1 – Dual Stacked Core and Tunnelling Infrastructure
  - Ø Dual Stacked CAPNet and Partial Core
  - Ø Five Regional Tunnels Head Ends
  - Ø Native IPv6 in SJ with Dual stacked Alpha DMZ
  - Ø Native IPv6 in RTP with Dual Stacked Alpha DMZ
- Phase 2 – Desktop (Wired and Wireless) and DC Pilot
  - Ø Dual Stack Pilot Desktop Wired and Wireless
  - Ø Isolated Dual Stacked DC Pod (IPv6 DC Island)
- Phase 3 – DC, DMZ, RO, OOB, Lab, Remaining Core, MPLS VPNs, Multicast, QoS, Extranet (TBD)

Cisco.com Phase I Solution Overview

- Replication
  - Replicate “static content” to v6 environment
  - Directories with secure content in them will not be replicated
  - 200G of content is replicated to IPv6 environment
- Content Delivery
  - AAAA record for www.ipv6.cisco.com served from DNS
  - “Static Content” served locally
  - Dynamic Content redirected to WWW

www.ipv6.cisco.com – 2001:420:80:1::5

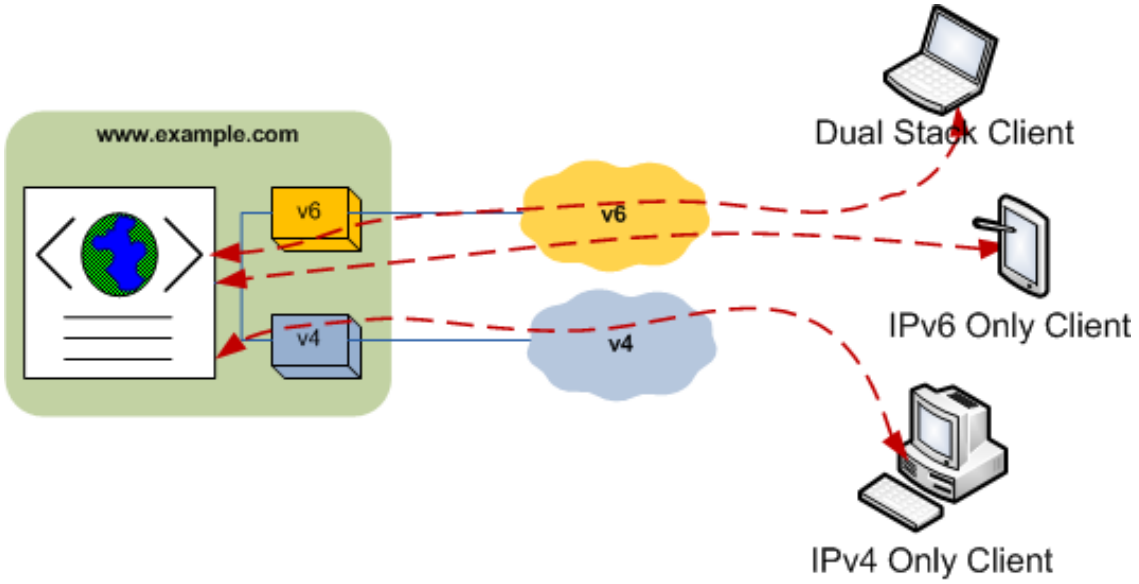


World IPv6 Day

World IPv6 Day

- June 8, 2011 from 0:00 UTC to June 9, 2011 0:00 UTC
- Coordinated, cooperative IPv6 activation by websites and CDNs
- Worldwide testbed for data gathering
- http://isoc.org/wp/worldipv6day/

Step Back: How are Clients Served?



- Dual stacked (IPv4 and IPv6 enabled hosts) as well as IPv6 only hosts use IPv6 network
- IPv4 only clients will use IPv4 network

- IPv6 data paths are independent of IPv4 paths
- IPv6 capable devices will prefer IPv6 connectivity
- IPv6 paths will see unprecedented stress on June 8
- IPv4 only sites will see no changes

Impacted Users

Website Owners

Network Operators (end users)

	IPv4 Only	Dual Stack (IPv4/IPv6)	Dual Stack with IPv6 problem
IPv4 Only			
Dual Stack (IPv4/IPv6)			
Dual Stack with IPv6 problem			

Anticipated Problems

- Estimated impacted Internet population:
  - 0.05% of all users or ~ 500,000 hosts *
- Most sites or hosts will not notice the change
- Typical impacts
  - Slow connection startup as IPv6 fails and falls back to IPv4
  - Slow performance due to congested IPv6 paths
  - Failed connectivity for misconfigured devices or networks
  - DNS lookup failures

* Source: http://www.isc.org/solutions/survey

Thank you.