



IPv6: An Overview



Karen Alderson, Cisco
Mark Ganser, Alaska Vocational Technical Center
Dallas Shiroma, Honolulu Community College

Cisco | Networking Academy®
Mind Wide Open™

Historical Overview

- In 1992:
 - Concern raised of IP address exhaustion and routing table size explosion
- 1993:
 - IETF study—IPv4 address lifetime expectancy is one year!
 - Studies began on possible IPng (next generation)
 - IPv6 has been evolving over last decade or more
- IPv4 is still in use today
 - New technologies extend life of IPv4:
 - CIDR, NAT, and private addresses
 - This delayed IPv6 implementation did not solve the problem



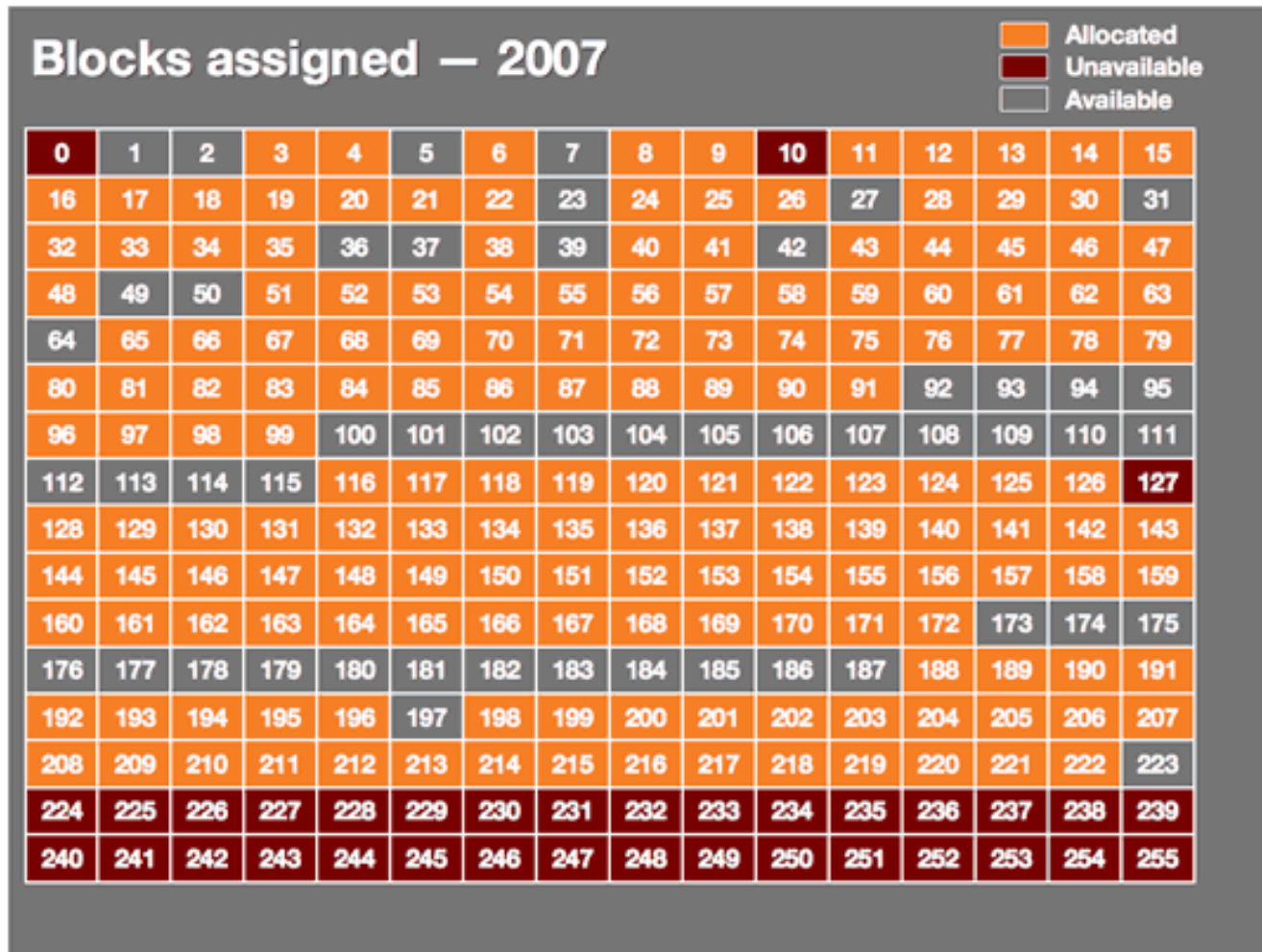
IPv4 Address Allocations (1)

Blocks assigned – 1993

Allocated
 Unavailable
 Available

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

IPv4 Address Allocations (2)





How Long Will IPv4 Addresses Last?

Estimates Remain a Moving Target

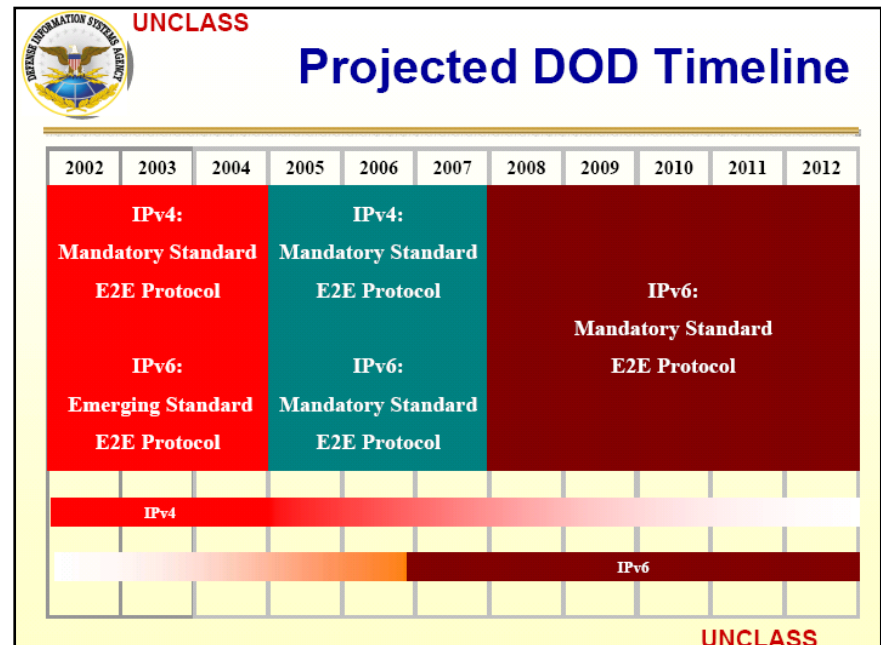
- In 2003, available IPv4 addresses would last until 2023
- In Sept 2005, a Cisco Systems study reported that IPv4 available addresses would be exhausted in four to five years
- In Nov 2007, daily updated reports projected that unallocated addresses would be exhausted in May 2010

If assigned but unused addresses were reclaimed and used, allocation of IPv4 addresses could continue until 2017

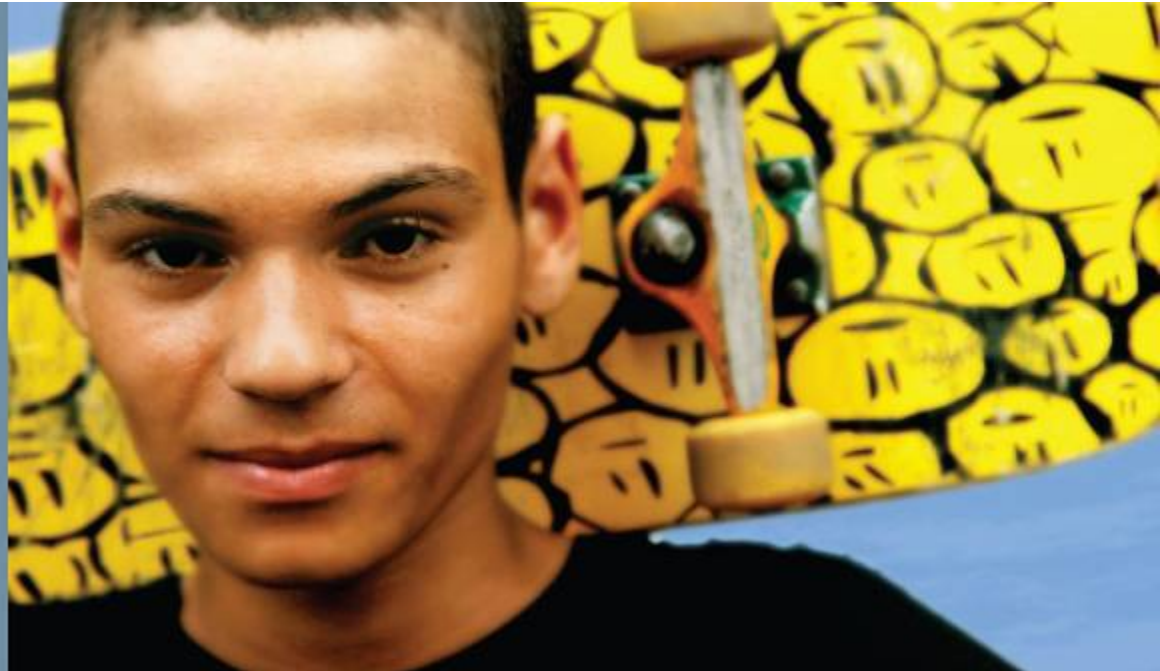
<http://www.potaroo.net/tools/ipv4/>

Migration to IPv6

- It is expected that in the US, migration from IPv4 to IPv6 will be a slow, gradual process
 - To address this, IPv6 provides several transition mechanisms
- Main impetus is DoD
 - Mandate to be IPv6 backbone capable by 2008
 - Fully IPv6 capable by 2012



IPv6 Features



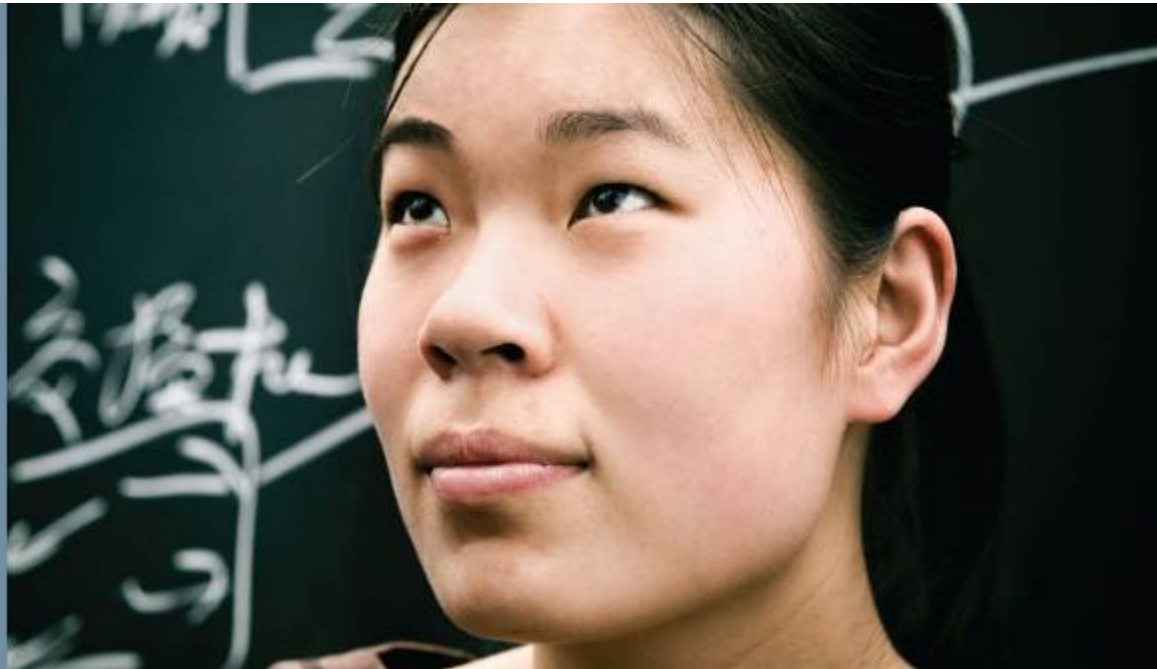
Why IPv6?

Major areas of benefits offered by IPv6:

- Greater addressing space
 - Aggregatable for efficient routing
- Simplified header
 - Better routing performance and services
- Security
- Mobility
- Transition richness

IPv6 Features	
<ul style="list-style-type: none"> • Larger Address Space: <ul style="list-style-type: none"> ■ Global reachability and flexibility ■ Aggregation ■ Multihoming ■ Autoconfiguration ■ Plug and play ■ End-to-end w/o NAT ■ Renumbering • Mobility and Security: <ul style="list-style-type: none"> ■ Mobile IP RFC-compliant ■ IPsec mandatory (or native) 	<ul style="list-style-type: none"> • Simple Header: <ul style="list-style-type: none"> ■ Routing efficiency ■ No broadcasts ■ No checksums ■ Extension headers ■ Flow labels • Transition Richness: <ul style="list-style-type: none"> ■ Dual stack ■ 6to4 tunnels ■ NAT-PT

IPv6 Addressing



IPv6 Larger Address Space

- Main driving force in converting to IPv6 is the depletion of IPv4 addresses
- 128-bit (16-byte) source and destination IP addresses
 - 2^{128} or 3.4×10^{38} possible combinations
 - About 4.3×10^{20} (430 quintillion) addresses per square inch of the earth's surface
 - IPv4's 32-bit address space allows only 2^{32} or **4,294,967,296** possible addresses
- Allows for multiple levels of subnetting and address allocation

What IPv6 Addresses Look Like

- 128 bits are separated into blocks of 16 bits
- Each 16-bit block is represented in hex and delimited with colons:

2001:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

- In each 16-bit block, leading zeros may be removed

2001:D3:0:2F3B:2AA:FF:FE28:9C5A

IPv6 Address Format—Compressing 0s

- Any consecutive 16-bit blocks of zeroes can be replaced with a double-colon (::)

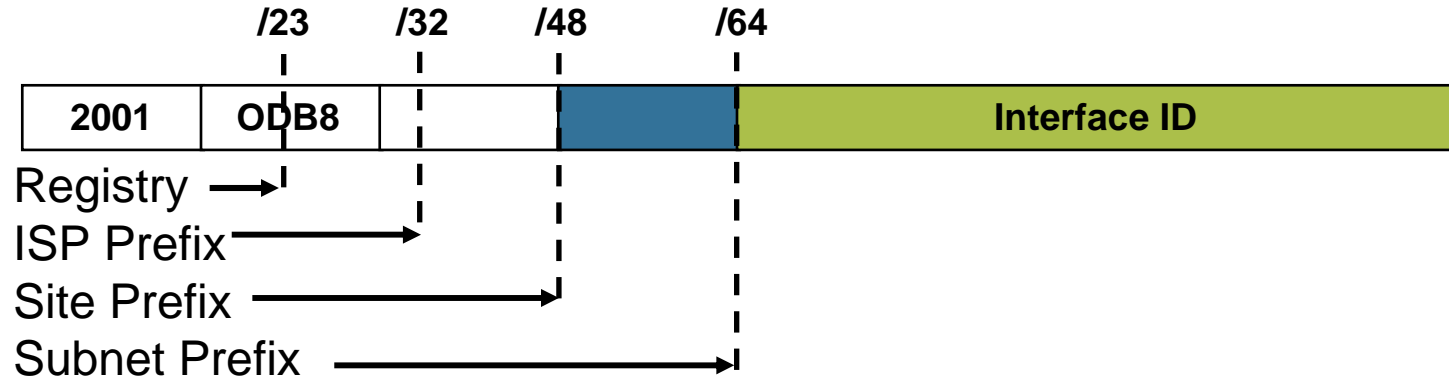
`FE80:0:0:0:2AA:FF:FE9A:4CA2` can be compressed to `FE80::2AA:FF:FE9A:4CA2`

The multicast address `FF02:0:0:0:0:0:0:2` can be compressed to `FF02::2`

- Zero compression can only be used once in a given address

Otherwise, you could not determine the number of 0 bits represented by each double-colon instance

Address Format



Represented as:

x:x:x:x:x:x:x:x where x is a 16-bit hexadecimal field

- 2001:0DB8:C003:0001:0000:0000:0000:BEEF
- 2001:DB8:C003:1:0:0:0:BEEF
- 2001:DB8:C003:1::BEEF

Address Format—IPv6 Prefixes

- Prefixes for IPv6 subnets, routes, and address ranges are expressed in the same way as Classless Inter-Domain Routing (CIDR) notation for IPv4

In **address/prefix-length** notation

For example:

2001:D3::/48 is a route prefix and

2001:D3:0:2F3B::/64 is a subnet prefix

- No use of subnet masks such as 255.255.255.192 as in IPv4!

Address Allocation

IANA allocates 2001::

- Registries allocate /32 to ISPs
- ISPs allocate /48 to each customer or site
- At each site, each LAN can be allocated a /64
 - So site can have a maximum of 65,535 LANs

2001:0200:: 23 and<br/ 2001:0C00:: 23</td <td>Asia Pacific Network Information Centre (APNIC) for Use in Asia</td>	Asia Pacific Network Information Centre (APNIC) for Use in Asia
2001:0400:: 23</td <td>American Registry for Internet Numbers (ARIN) for Use in the Americas</td>	American Registry for Internet Numbers (ARIN) for Use in the Americas
2001:0600:: 23 and<br/ 2001:0800:: 23</td <td>Réseaux IP Européens—Network Coordination Center (RIPE NCC) for Use in Europe and the Middle East</td>	Réseaux IP Européens—Network Coordination Center (RIPE NCC) for Use in Europe and the Middle East

IPv6 Aggregatable Addresses

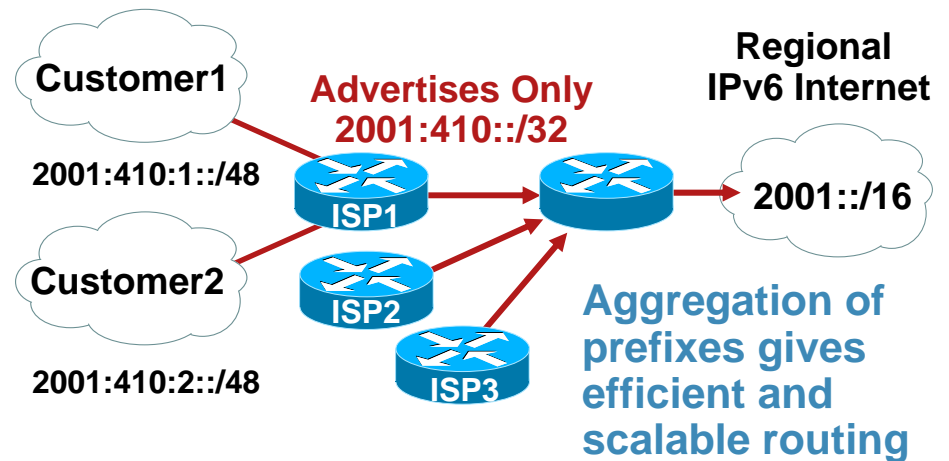
Hierarchical structure gives efficient aggregation and routing

- An ISP can aggregate all its prefixes into a single prefix!

A prefix also indicates a global area (as allocated by RIRs)

- Organizations can define a single prefix for entire network!

Aggregation results in efficient and scalable routing tables





IPv6 Address Types

Three types of IPv6 addresses, RFC 4291

- Unicast

 - Identifies single device or interface

 - Link-local (FE80::/16); unique-local (FD00:/8); global; anycast

- Multicast (FFxy::/16)

 - One to members of a group

- Anycast

 - One-to-nearest one of designated group

No broadcasts!

Unicast IPv6 Addresses

Differentiated by their scope

- Global unicast addresses—globally routable
- Link-local addresses—only on single link, not routed
- Unique-local addresses—routed only within private network

Replaced site-local

- Special addresses

Unspecified address ::

Loopback ::1

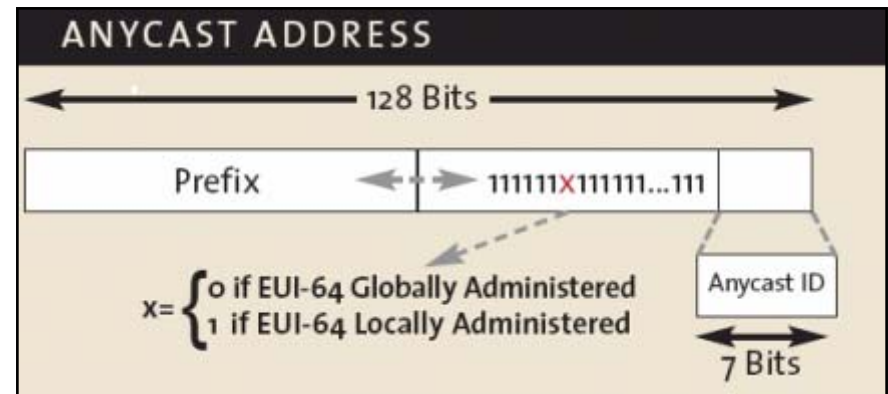
Anycast Address

Addressing where one IPv6 address represents multiple interfaces

- Packets are sent to the single best/nearest destination
- Allows a packet to be routed to one of a number of different nodes all responding to the same address

Uses of anycast addresses include:

- Load balancing of servers providing a well-known service
e.g., DNS
- Connection to closest router to an ISP





Stateless Autoconfiguration

- An IPv6-enabled host device will automatically configure its own link-local address (FE80:: address)

With link-local address, a host can discover connected routers to obtain a global prefix

A host then builds its own unicast global address

- No need for any servers (e.g., DHCP) to assign addresses

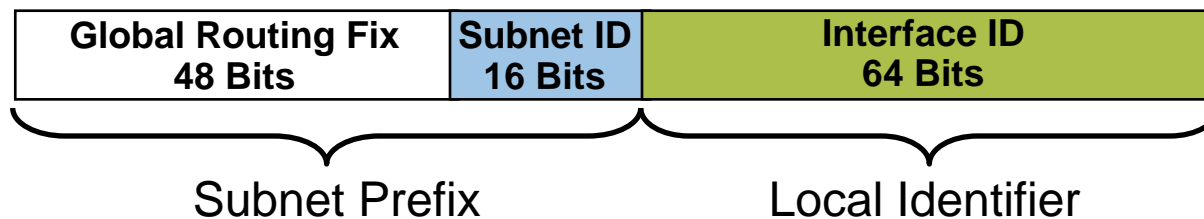


Interface ID (1)

- Autoconfiguration determines unique host or interface ID
64 bits; dynamically created from MAC address

Ethernet: 0xFFFE inserted into middle of MAC address

Universal/local bit: 1 for global scope; 0 for local scope



Interface ID (Ethernet):

For MAC addr 00-0C-29-C2-52-FF (using EUI-64 standards), interface ID is 00-0C-29-FF-FE-C2-52-FF for local scope.

IPv6 notation is 000C:29FF:FEC2:52FF

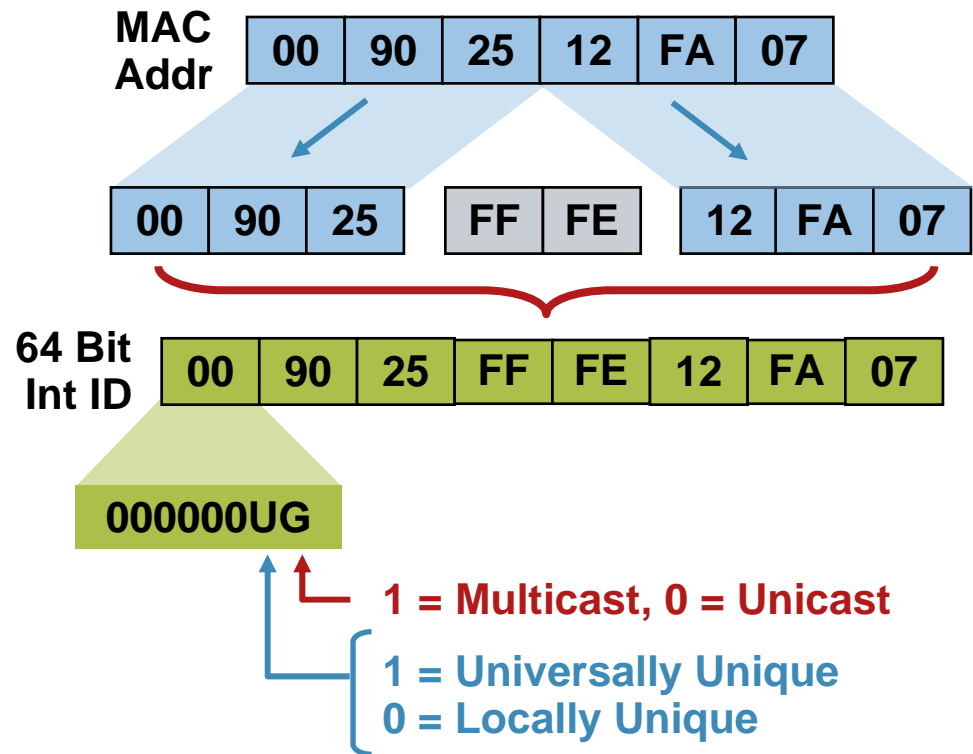
For global scope, universal bit is set to 1, and IPv6 notation is 020C:29FF:FEC2:52FF

Interface ID (2)

- 64-bit interface ID is obtained by inserting 0xFFFE into the MAC address
- 7th and 8th bits of first octet:

Indicates universally or locally unique, and multicast or unicast

Ethernet is assumed to be universally unique



IPv6 Header



IPv6 Simplified Header

- IPv6 offers a simpler packet header than IPv4:
 - Fixed-length header - more efficient memory allocations strategies and algorithm implementations
 - No packet fragmentation, or checksum fields

IPv4 Header

Ver	HL	Tos	Total Length	
Identification		Flags	Offset	
TTL		Protocol	Checksum	
Source Address				
Destination Address				

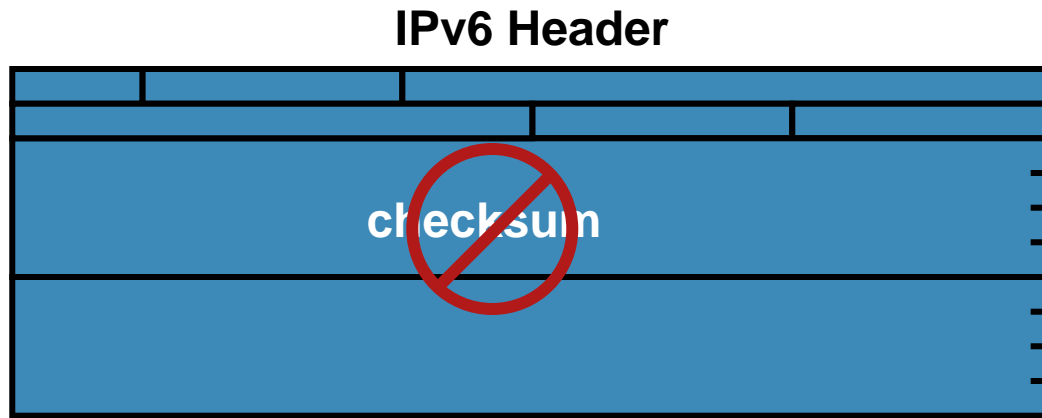
IPv6 Header

Ver	Class	Flow Label		
Payload Length		Next Hdr	Hop Limit	
Source Address				
Destination Address				

Extension Header

Next Hdr	Ext HLen			
Extension Header Information				

No Checksum



Simpler and more efficient header:

- No checksum at the IP layer, no recalculation by the routers
- Improved routing efficiency, performance, and forwarding-rate scalability
- Error detection performed by data-link layer and transport layer

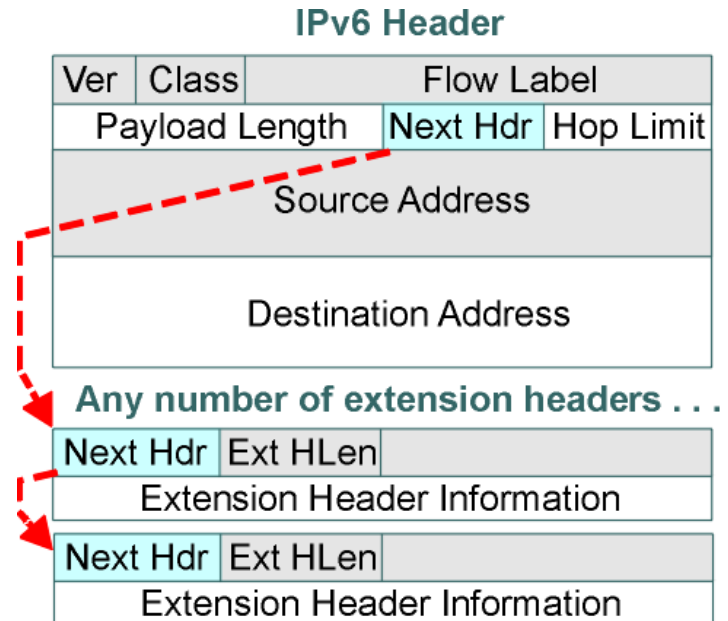
IPv6 Extension Header (1)

- Uses extension headers for additional information

Several can be chained together, identified by next header field

- Provides a flexible architecture

New headers may be defined, without changing the IPv6 header



IPv6 Extension Header (2)

Six defined extension headers

- RFC 2460

IPv6 options

- Placed in extension headers to facilitate routing and to provide framework for future options
- Designed to be processed only by destination node
 - exception being hop-by-hop options header

Extension Headers

- Hop-by-hop options
- Routing header
- Fragment header
- Destination options
- Authentication header
- ESP header

Security



Security

- IPv4 was not developed with security in mind

Assumed trusted networks

Security was an add-on (as needs arose, application level security was added)

- IPv6: security functionality as part of the protocol

All implementation of IPv6 must include IPSec

- Provides for security at network layer (instead of added on at application layer)

This does not mean IPv6 is “more secure” than IPv4

- Similar safeguards used in IPv4 must also be implemented in IPv6

IPSec must be implemented fully and consistently across the network

IPv6 Security (1)

- IPv6 address space is so large; randomly scanning for vulnerabilities is not practical

“Security by obscurity”

- So many addresses, would take years to scan a network!
- At 40 Gbps (much faster than Fast Ethernet or DSL/cable access), would take over 5000 yrs to scan /64 network

IPv6 Security (2)

Designers of IPv6 addressed known vulnerabilities of IPv4:

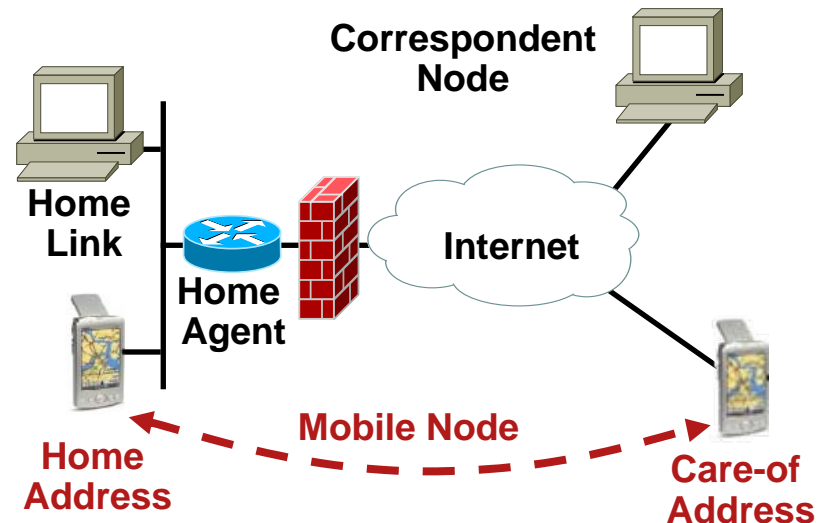
- **Broadcast storms**
 - No broadcasts in IPv6
 - No ICMPv6 responses to IPv6 multicasts
- **Fragmentation attacks**
 - Fragmentation can be specified only by the source, not intermediary devices
 - No overlapping fragments allowed
 - Reassembled packets <1280 bytes are dropped
- **IPv6** provides security services, i.e., authentication, integrity, and confidentiality with native IPSec support

Mobility



Mobile IPv6 (1)

- For mobile nodes, two addresses are used:
 - Home address** - global, unicast address of mobile device on its home network
 - Care-of-address** - global, unicast address of mobile device when it is away from its home network
- Home agent** - router that intercepts packets destined for the home address, and forwards those packets to the care-of-address



Mobile IPv6 (2)

Two Modes of Operation

- **Bidirectional tunneling**

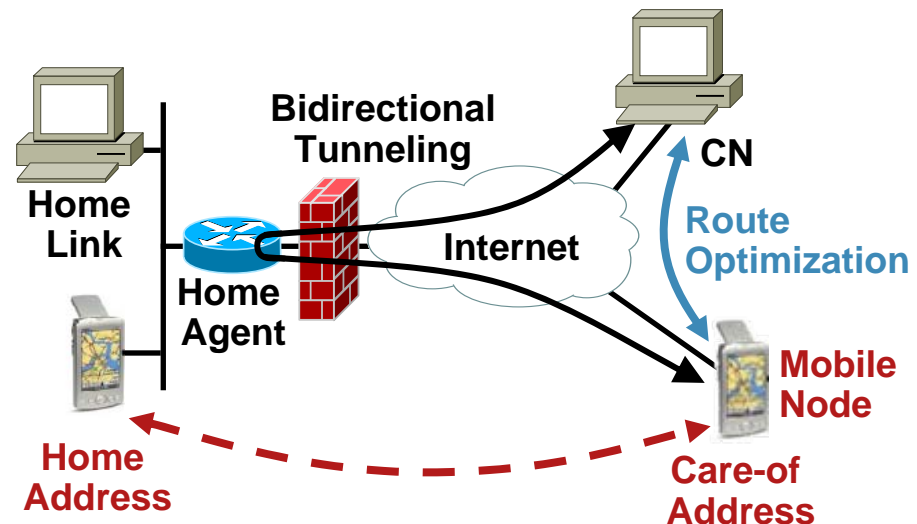
Packet sent to home address is intercepted by home agent and tunneled to care-of address

- **Route optimization**

Packets send directly between correspondent node (CN) and mobile node w/out going through home agent

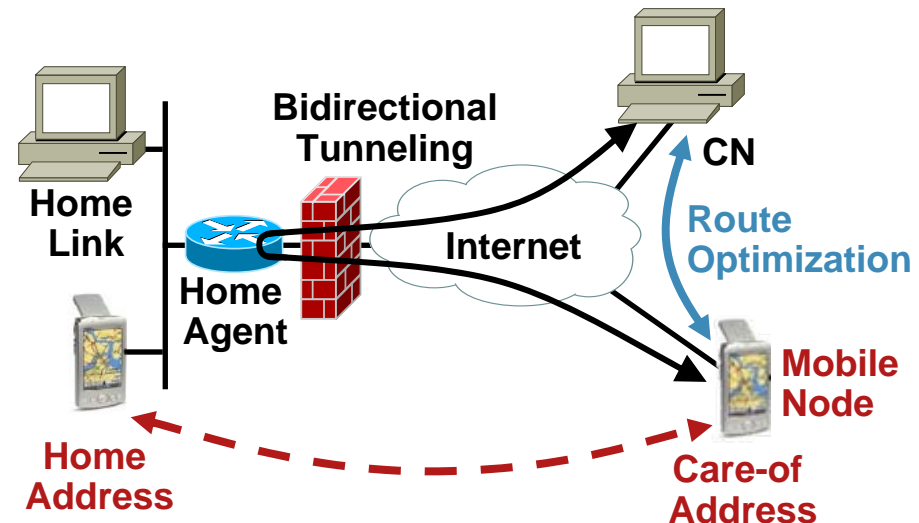
CN maintains binding update list

Binds home address and care-of-address of mobile node



Mobile IPv6 (3)

- Mobility will be a key reason to deploy IPv6
 - To provide full range of mobility services, devices need to move to IPv6
 - This may take some time as it is a core investment



Transition Richness



IPv4 to IPv6 Transition Mechanism

- Transition from IPv4 to IPv6 will take years
 - Migration is a long-term goal
- Major techniques to transition from IPv4 to IPv6:
 - Dual stack
 - Tunneling
- Most-likely transition technique is a combination of dual-stack and tunneling
 - “Dual stack where you can; tunnel where you must.”

Dual Stack (1)

- Both IPv4 and IPv6 are configured on the router

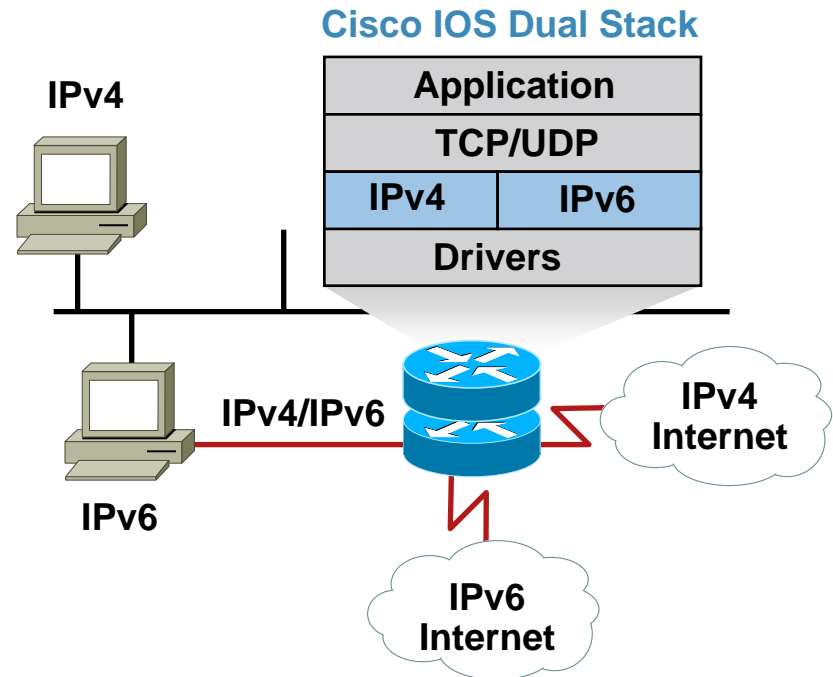
Dual-stack node has both IPv4 and IPv6 connectivity

Hosts decides which connection to use based on the availability of IPv6 connectivity and DNS records

Simple; common transition mechanism

- IPv4 and IPv6 stacks are independent

Need IPv4 and IPv6 addresses on dual-stacked devices





Dual Stack (2)

- Issue of DNS records:

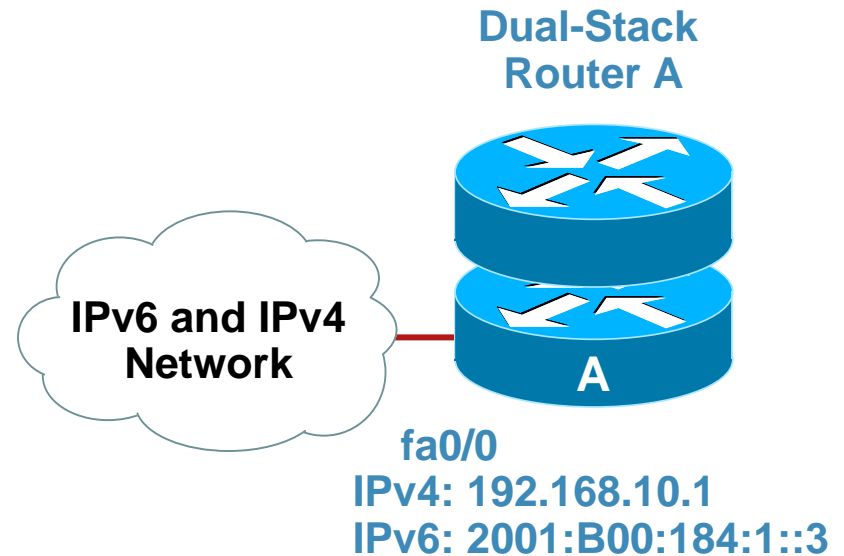
Require DNS resolver to resolve both IPv4 (A) and IPv6 (AAAA) DNS records

Application must have options to specify order of use of addresses (i.e. which is preferred protocol)

- Advantages:

Simple

Can provide connectivity between IPv4 and IPv6 networks



Dual Stack (3)

Disadvantages of Dual-Stack:

- Need to maintain separate protocol stacks
 - Separate tables (routing table, topology tables, etc.) for each protocol
 - More difficult to maintain security
- Different commands (e.g., ping for IPv4, ping6 for IPv6)
- More memory and CPU power for devices

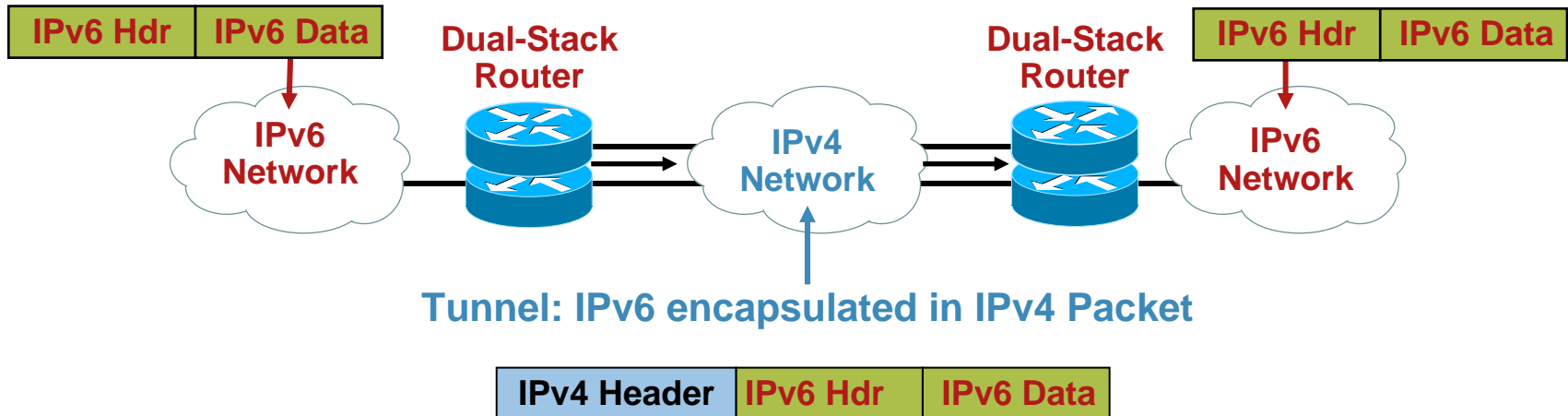
Tunneling

- Tunneling:

Encapsulating IPv6 into IPv4 packets for transport

Prefixing IPv6 packet with IPv4 header

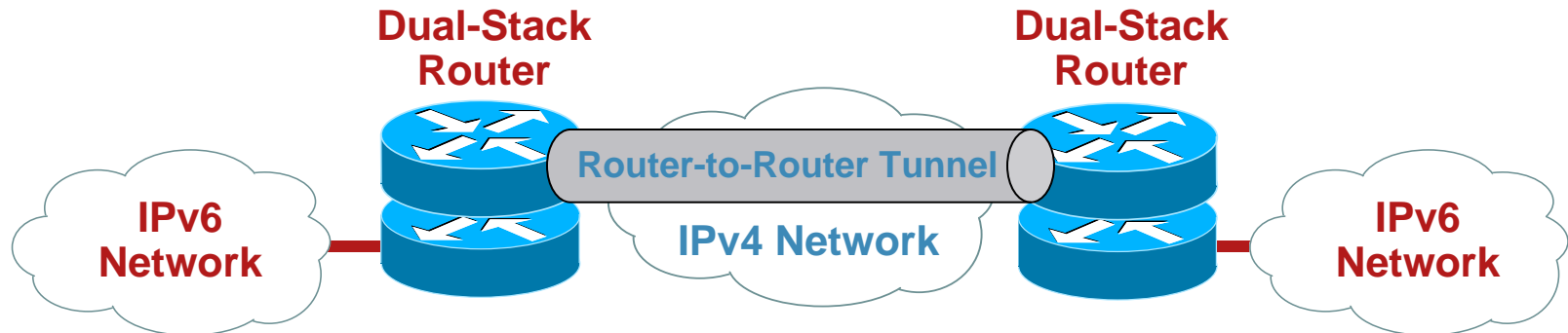
- As you deploy IPv6 islands, tunnels can provide connectivity thru an existing IPv4 network





Tunnels (1)

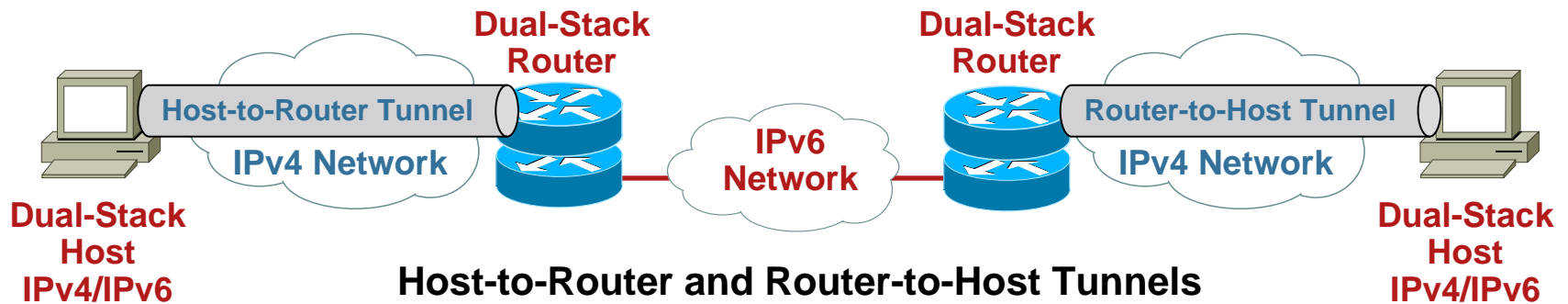
- Form a virtual point-to-point link between two devices
- Can be manually configured or automatic
- Types of tunnels:
 - Router-to-router, router-to-host, host-to-router, or host-to-host



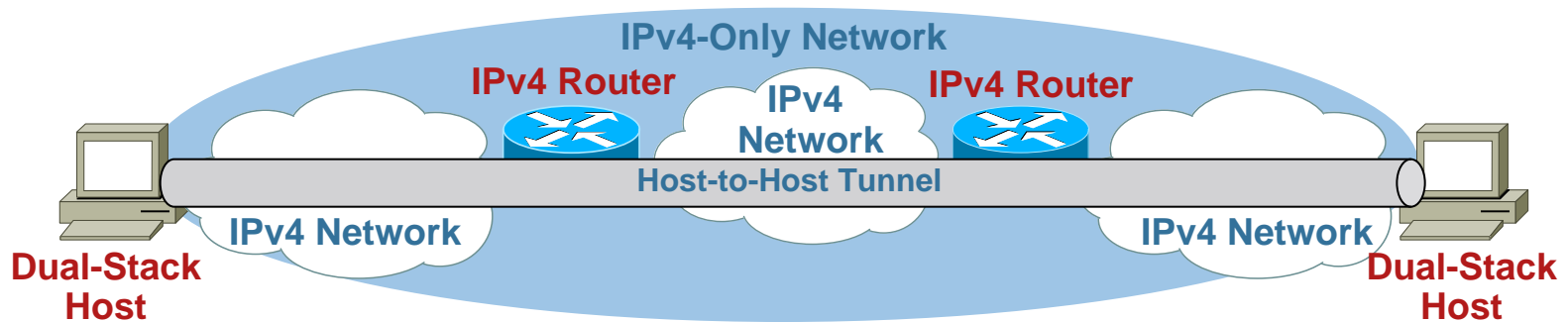
Router-to-Router Tunnel to Connect to IPv6 Islands

Tunnels (2)

- Tunnels: host-to-router and router-to-host



- Host-to-host tunnel





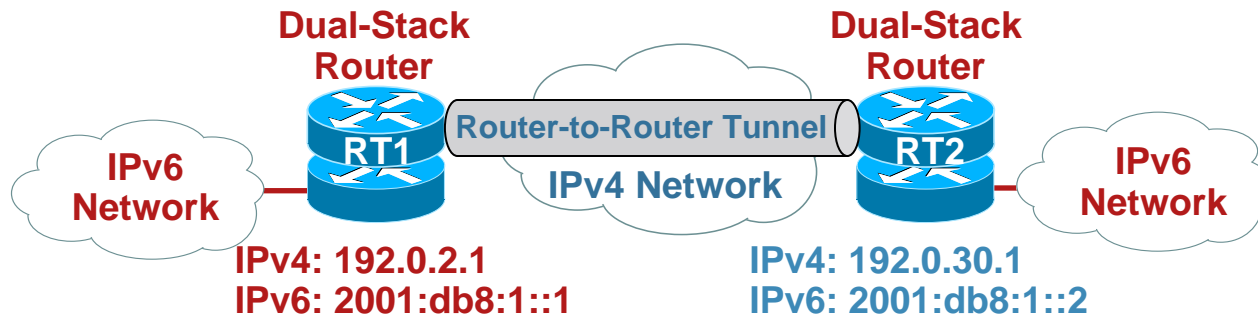
Configured Tunnels (1)

Have manually configured tunnel end-points

Tunnel routers are dual-stacked, with both IPv4 and IPv6 addresses

Note: IPv6 addresses are next hops (IPv4 need not be)

Cisco IOS® example configuration of IPv6-over-IPv4 tunnel



```
RT1#  
int Tunnel0  
  ipv6 address 2001:db8:1::1/64  
  tunnel source 192.0.2.1  
  tunnel destination 192.0.30.1  
  tunnel mode ipv6ip
```

```
RT2#  
int Tunnel0  
  ipv6 address 2001:db8:1::2/64  
  tunnel source 192.0.30.1  
  tunnel destination 192.0.2.1  
  tunnel mode ipv6ip
```



Configured Tunnels (2)

- Manually configured tunnels provide more control over forwarding path than automatic tunnels

May be desirable for security reasons

A good security practice:

Tunnel routers should accept encapsulated packets only from the other end of the tunnel

But manually configured tunnels require more administrative overhead



Automatic Tunnels

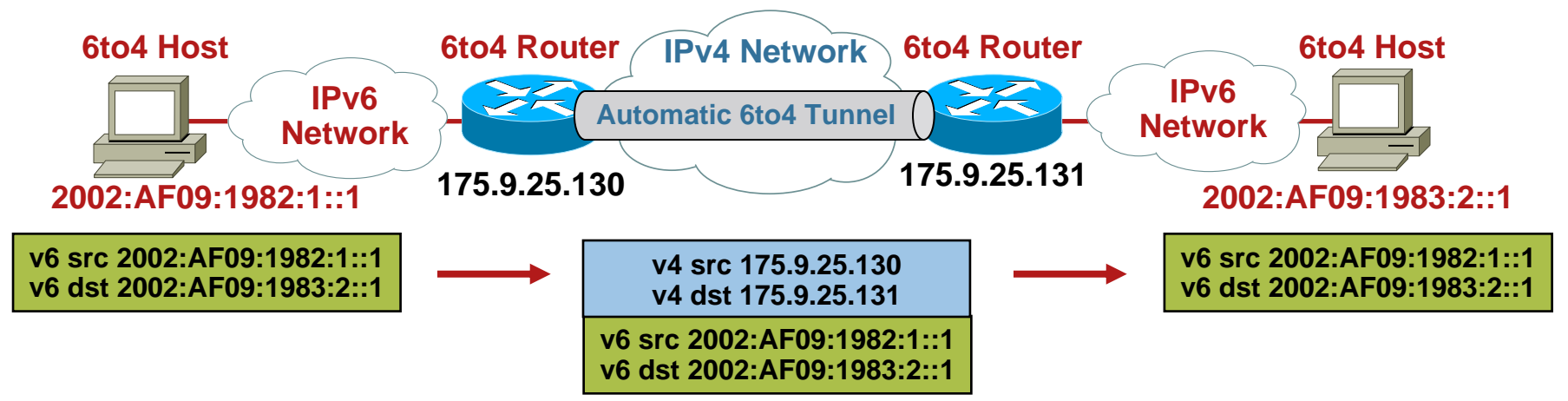
- No configuration of tunnel destination required
 - Less administrative work
 - More susceptible to misuse, because at receiving end, packets are accepted from any source!
- Automatic tunnels are created based on info in IPv6 packet
 - Most use an IPv6 address with embedded IPv4 address
- Automatic tunneling techniques include:
 - 6to4** (router to router)
 - Tunneling to/from host:
 - ISATAP** (Intra-Site Automatic Tunnel Addressing Protocol)
 - Teredo** (can tunnel thru NAT device)



Automatic 6to4 Tunnel

6to4 (Router-to-Router)

- Uses global prefix 2002:WWXX:YYZZ::/48
Where IPv4 address of host is w.x.y.z
- 6to4 routers extracts IPv4 address for routing through IPv4 network

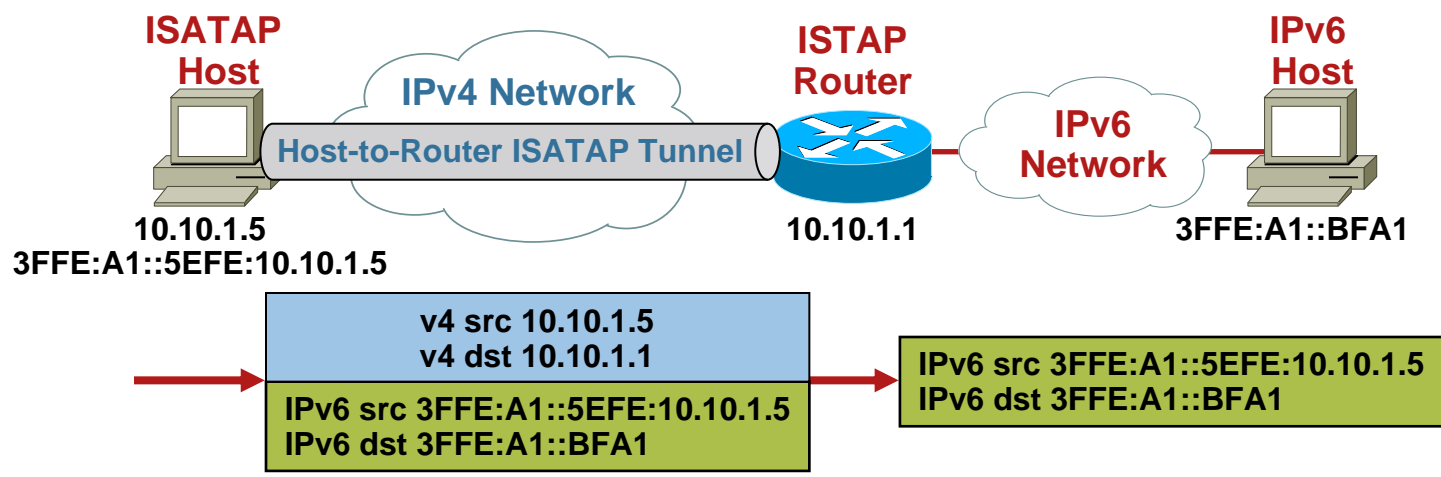


Note: 175.9.25.130 = AF09:1982 and 175.9.25.131 = AF09:1983



ISATAP Tunnel

- **ISATAP** (Intra-Site Automatic Tunneling Addressing Protocol)
 - Uses IPv6 address with embedded IPv4 address in interface ID
 - For host-to-router, router-to-host, and host-to-host tunnels
 - Encapsulates IPv6 with IPv4 header
- For host with IPv4 address of w.x.y.z
 - ISATAP address has interface ID of 0:5EFE:w.x.y.z
 - e.g., link-local address: FE80::5EFE:192.168.4.1 where the IPv4 address is 192.168.4.1

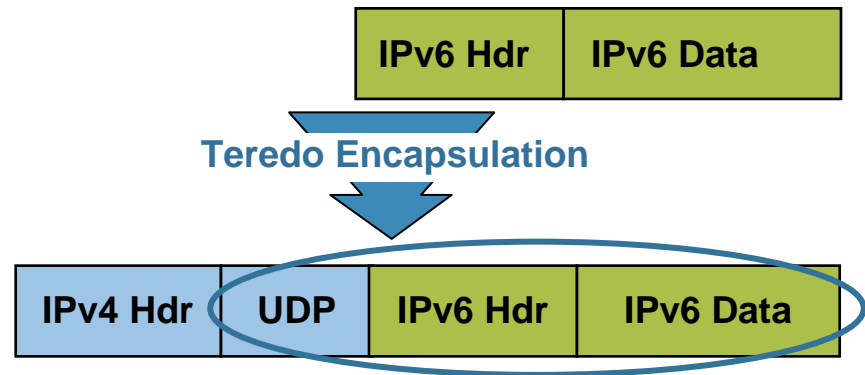




Teredo Automatic Tunnel (1)

Teredo

- For host-to-host tunneling through NAT devices
 - IPv6 datagrams embedded within IPv4 UDP
 - Basically “hides” tunnel (protocol 41) with additional UDP header, to traverse NAT devices
- Will be phased out as 6to4-enabled or IPv6-aware firewall routers come into use
- RFC 4380

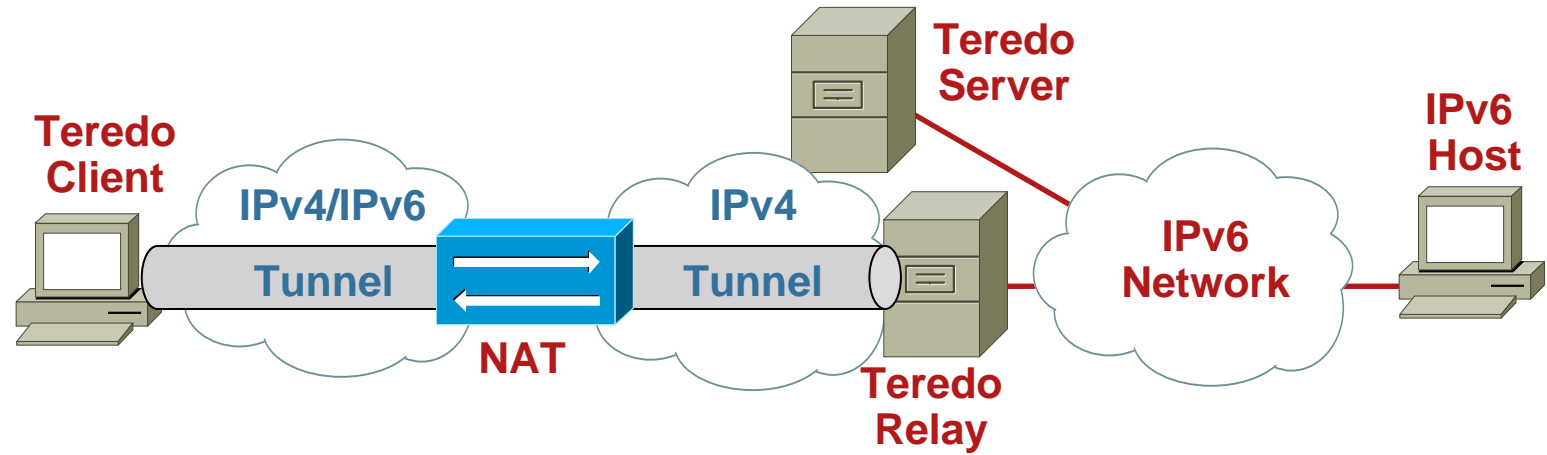




Teredo Automatic Tunnel (2)

- Teredo prefix is 2001::/32
- Requires Teredo client, Teredo server, and Teredo relay

High overhead



Comparison: IPv6 vs IPv4

Characteristic	IPv6	IPv4
Address Length	128 Bits	32 Bits
Address Representation	Hexadecimal	Dotted-Decimal
Header Length	Fixed (40 Bytes)	Variable
Address Configuration	Stateless Autoconfig or Stateful DHCP	Stateful DHCP
DNS	AAAA Records	A Records

Comparison: IPv6 vs IPv4

Characteristic	IPv6	IPv4
Interior Routing Protocols	OSPFv3, RIPng, IS-IS for IPv6	OSPFv2, RIPv2, IS-IS
Private Addresses	Site-Local Addresses	RFC 1918 Private Address Space
Fragmentation	Sending Host Only	Sending Host and Intermediate Routers
Loopback Address	0:0:0:0:0:0:0:1	127.0.0.1
Address Types	Unicast, anycast, multicast	Unicast, multicast, broadcast

IPv6 Deployment



IPv6 deployment (1)

- Deployment of IPv6 networks has taken off since 2005

Governments in US, China, Japan, Korea, Singapore, and Germany are committing millions of dollars in building IPv6 networks

- **China** launches pure IPv6 network
September 25, 2006

China has built the first pure IPv6 network in the world and has linked telecom operators China Telecom, China Unicom, China Mobile, etc.

China has more people (1.3 billion) than available IPv4 addresses

IPv6 deployment (2)

- **Japan** - technology-driven demand for more devices

Everything from pocket videophones to airport kiosks to building heat sensors and plain-old desktop PCs will be linked together in a vast broadband network

Service providers, notably market leader NTT East and NTT West provide native IPv6 Internet access for both business and consumer and video-on-demand IPv6 multicast services

- **USA**

Department of Defense (DoD) plans to establish IPv6 in all Internet and intranet systems department-wide by 2008

Domestic IPv6 Networks

- There are two large IPv6 networks of note in the US
- Abilene Network Indiana University
<http://abilene.internet2.edu/>
- Open Contributors Corporation for Advanced Internet Development (OCCAID)
<http://www.occaid.org/occaidv6.pdf>

Internet2 (Abilene Network)

- **UCAID (University Corporation for Advanced Internet Development)**

Non-profit consortium which develops and deploys advanced network applications and technologies, for education and high-speed data transfer purposes

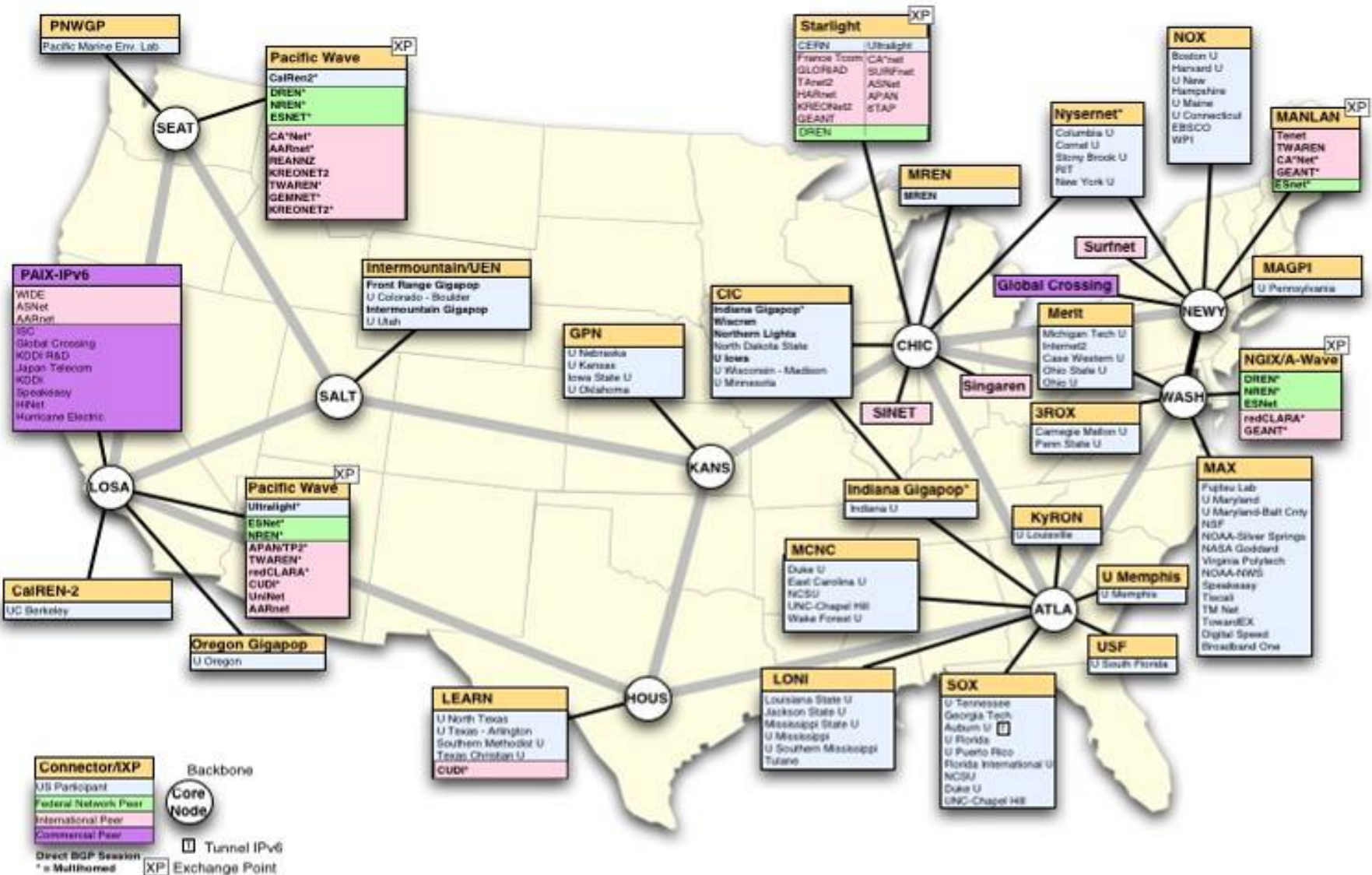
<http://www.abilene.iu.edu>

- UCAID created the Abilene network

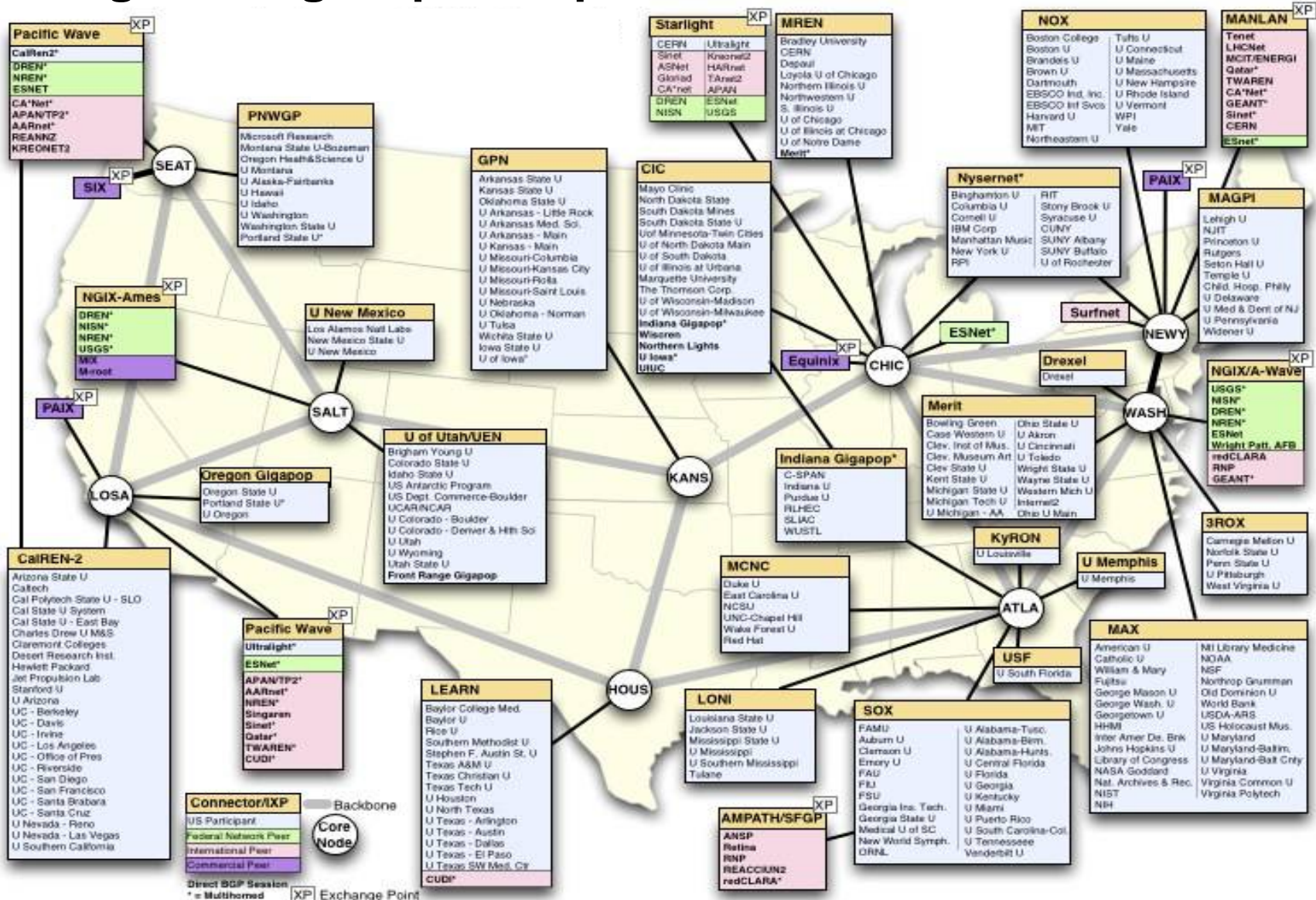
Now called Internet2 Network

Internet2 Network

IPv6 Deployment, 16 April 2008



Internet2 Network Engineering Map, 15 April 2008



OCCAID

- Open Contributors Corporation for Advanced Internet Development

Non-profit consortium that operates one of the largest IPv6 research networks in the world

<http://www.occaid.org>

Has become center of North American interest in IPv6



OCCAID R&D Backbone Network North America



Legend:

- OCCAID2 Segments:** 1-2.4 Gbps Backbone Capacity Upgrade
- 100Mbps Connection:** MPLS, SD-WAN or tunneled over same upstream
- Tunnel Connection:**
- DS-3 (45Mbps):**
- Pending Connection:**
- OCCAID Core Node:**
- Pending OCCAID Core Node:**
- Layer2 Facility:** Upstream/transport provider's POP
- Operations Center:**
 - C: Command/Administrative Center, 24x7 Staffed
 - F: Field Engineering Depot, Business Hours
 - E: Local Command/Administrative Center, Business Hours
- Exchange Point:**
- SixXS Access Node:**

© OCCAID September 2007

NORTH AMERICAN INFRASTRUCTURE PARTNERS

Partners include: Citrinet, UnitedLayer, HotNIC, thinktel, KC X NAP, midPhase, LAYER, equinix, choopa, nap of the Americas, and TADA MEDIA.

IPv6 in Academy Curriculum





IPv6 in Academy Curriculum

CCNA Discovery: Designing and Supporting Computer Networks (Discovery 4)

- Chapter 6: Using IP Addressing in the Network Design
 - 6.3 Describing IPv4 and IPv6

CCNA Exploration: Accessing the WAN (Exploration 4)

- Chapter 7: IP Addressing Services
 - 7.3 IPv6

CCNP: Building Scalable Internetworks (CCNP BSI v5.0)

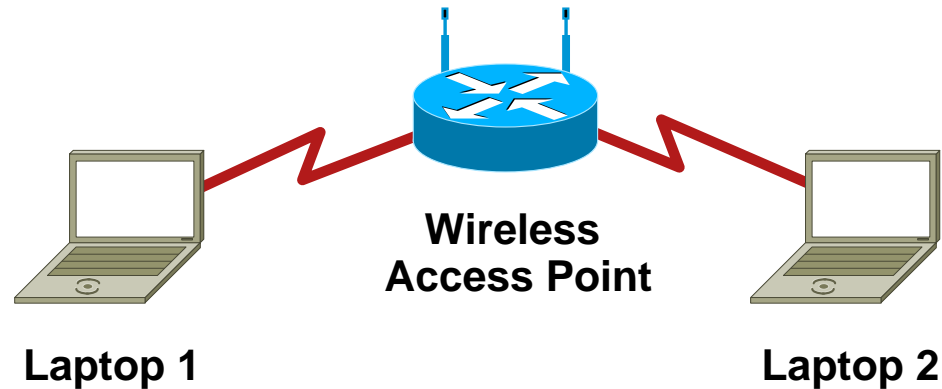
- Module 8: IPv6

Activity





IPv6: An Overview, Demonstration Activity



- Demonstrate configuring Microsoft Windows or Mac OS X for IPv6
- Demonstrate how to display IPv6 addresses in Windows or OS X
- Demonstrate the ping command in an IPv6 environment



Link-local IPv6 Address

```
ca. Administrator: Command Prompt
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : avtec.ak
    Link-local IPv6 Address . . . . . : fe80::486a:aff5:ed80:4595%8
    IPv4 Address. . . . . : 10.10.20.161
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.20.1

Tunnel adapter Local Area Connection* 6:

    Connection-specific DNS Suffix . : avtec.ak
    Link-local IPv6 Address . . . . . : fe80::5efe:10.10.20.161%10
    Default Gateway . . . . . :

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

C:\Users\Administrator>
```



Zone ID (Interface Index)

```
ca. Administrator: Command Prompt
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : avtec.ak
    Link-local IPv6 Address . . . . . : fe80::486a:aff5:ed80:4595%8
    IPv4 Address. . . . . : 10.10.20.161
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.20.1

Tunnel adapter Local Area Connection* 6:

    Connection-specific DNS Suffix  . : avtec.ak
    Link-local IPv6 Address . . . . . : fe80::5efe:10.10.20.161%10
    Default Gateway . . . . . :

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\Administrator>
```



Ping6

Command

Destination Address

Source Zone ID

```
C:\> CMD.EXE
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS> ping6 fe80::214:22ff:fed4:6624%4

Pinging fe80::214:22ff:fed4:6624%4
from fe80::212:3fff:fef4:21ea%4 with 32 bytes of data:

Reply from fe80::214:22ff:fed4:6624%4: bytes=32 time<1ms
Reply from fe80::214:22ff:fed4:6624%4: bytes=32 time<1ms
Reply from fe80::214:22ff:fed4:6624%4: bytes=32 time<1ms
Reply from fe80::214:22ff:fed4:6624%4: bytes=32 time<1ms

Ping statistics for fe80::214:22ff:fed4:6624%4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS> _
```

Questions?



Cisco | Networking Academy[®]

Mind Wide Open[™]



CISCO