IPv6 applications

Benoit Lourdelet
Cisco Systems
Technical Marketing Engineer
blourdel@cisco.com
Agenda

- IPv6 Business Case
- IPv6 Protocols & Standards
- IPv6 Routing
- Integration and Transition
- IPv6 Deployment scenarios
A need for IPv6?

- IETF IPv6 WG began in early 90s, to solve addressing growth issues, but
  - CIDR, NAT,... were developed

- IPv4 32 bit address = 4 billion hosts
  - ~40% of the IPv4 address space is still unused
  - BUT

- IP is everywhere
  - Data, Voice, Audio and Video integration is a Reality
  - Regional Registries apply a strict allocation control

- So, Only compelling reason: more IP addresses!
IP Address Allocation History

1981 - IPv4 protocol published
1985 ~ 1/16 of total space
1990 ~ 1/8 of total space
1995 ~ 1/4 of total space
2000 ~ 1/2 of total space

• This despite increasingly intense conservation efforts
  PPP / DHCP address sharing
  CIDR (classless inter-domain routing)
  NAT (network address translation)
  plus some address reclamation

• Theoretical limit of 32-bit space: ~4 billion devices
  Practical limit of 32-bit space: ~250 million devices
  (see RFC 3194)
Do We Really Need a Larger Address Space?

- Overall Internet population is still growing
  ~420 million users in Q1 CY2001, ~620 million by 2005, less than 10% worldwide population
- Emerging population/geopolitical and Address space
  Africa, China, India, Japan, Korea need/want global IP addresses
  How to move to e-Economy without Global Internet access?
- 405 million mobile phones sold in 2000, over 1 billion by 2005
  UMTS Release 5 is Internet Mobility, eg. 1/3 of 1B should get connected
- ~1 Billion cars in 2010, 15% should get GPS and Yellow Page services
Explosion of New Internet Appliances
Coming Back to an End-to-End Architecture

New Technologies/Applications for Home Users
‘Always-on’—Cable, DSL, Ethernet-to-the-home, Wireless,…

- Internet started with end-to-end connectivity for any applications
- Today, NAT and Application-Layer Gateways connecting disparate networks
- **Always-on Devices Need an Address When You Call Them**
  - Mobile Phones
  - Gaming
  - Residential Voice over IP gateway
  - IP Fax

Global Addressing Realm
IPv6 Markets

• Academic NRN
  Internet-II (Abilene, vBNS+), Canarie*3, Renater-II, Surfnet, DFN, CERNET, Nordunet,… 6REN/6TAP

• Geographies & Politics
  IPv6 promotion council in Japan, Korea IPv6 Forum
  EEC e-Europe & IPv6 Task Force -> 6NET and Euro6IX projects

• Wireless (PDA, 3G Mobile Phone networks, Car,...)
  Multiple phases before deployment
  RFP -> Integration -> trial -> commercial
  Requires ‘client devices’, eg. IPv6 handset?
IPv6 Markets

• Home Networking
  Set-top box/Cable/xDSL/Ethernet-to-the-home
  E.g. Japan Home Information Services initiative

• Gaming
  Sony, (Sega), Nintendo, Microsoft

• Consumer Devices

• Enterprise
  Requires IPv6 support by O.S. & Applications
  SUN Solaris 8, BSD 4.x, Linux, Microsoft Windows XP Pro, etc.

• Service Providers
  Regional ISP, Carriers, Mobile ISP, IPv6 IX, and Greenfield ISP’s
How to get an IPv6 Address?

• How to get address space?
  Real IPv6 address space now allocated by APNIC, ARIN and RIPE NCC to ISP
  
  - APNIC 2001:0200::/23
  - ARIN 2001:0400::/23
  - RIPE NCC 2001:0600::/23

• 6Bone 3FFE::/16

• 6to4 tunnels 2002::/16

• Enterprises will get their IPv6 address space from their ISP.
<table>
<thead>
<tr>
<th>Prefix</th>
<th>Date</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONNECT-AU-19990916</td>
<td>2001:210::/35</td>
<td></td>
</tr>
<tr>
<td>NUS-SG-19990827</td>
<td>2001:208::/35</td>
<td></td>
</tr>
<tr>
<td>HINET-TW-20000208</td>
<td>2001:238::/35</td>
<td></td>
</tr>
<tr>
<td>CERNET-CN-20000426</td>
<td>2001:250::/35</td>
<td></td>
</tr>
<tr>
<td>DACOM-BORANET-20000908</td>
<td>2001:270::/35</td>
<td></td>
</tr>
<tr>
<td>TANET-TWNIC-TW-20001006</td>
<td>2001:288::/35</td>
<td></td>
</tr>
<tr>
<td>KORNET-KRNIC-KR-20010102</td>
<td>2001:02B0::/35</td>
<td></td>
</tr>
<tr>
<td>NGINET-KRNIC-KR-20010115</td>
<td>2001:02B8::/35</td>
<td></td>
</tr>
<tr>
<td>OMP-JPNIC-JP-20010208</td>
<td>2001:02C8::/35</td>
<td></td>
</tr>
<tr>
<td>INFOSPHERE-JPNIC-JP-20010207</td>
<td>2001:02C0::/35</td>
<td></td>
</tr>
<tr>
<td>ZAMA-AP-20010320</td>
<td>2001:02D0::/35</td>
<td></td>
</tr>
<tr>
<td>SKTELECOMNET-KRNIC-KR-20010406</td>
<td>2001:02D8::/35</td>
<td></td>
</tr>
<tr>
<td>HKenet-HK-20010420</td>
<td>2001:02E0::/35</td>
<td></td>
</tr>
<tr>
<td>CONNECT-AU-19990916</td>
<td>2001:0210::/35</td>
<td></td>
</tr>
<tr>
<td>MEX-JPNIC-JP-20010801</td>
<td>2001:02F0::/35</td>
<td></td>
</tr>
<tr>
<td>SINET-JPNIC-JP-20010809</td>
<td>2001:02F8::/35</td>
<td></td>
</tr>
<tr>
<td>MANIS-MY-20010824</td>
<td>2001:0328::/35</td>
<td></td>
</tr>
<tr>
<td>V6TELSTRAINTERNET-AU-20011211</td>
<td>2001:0360::/35</td>
<td></td>
</tr>
<tr>
<td>GCTRJP-NET-20011212</td>
<td>2001:0370::/35</td>
<td></td>
</tr>
</tbody>
</table>
IPv6 Prefix Allocations: ARIN
(whois.arin.net) – January 2002

ESNET-V6 2001:0400::/35
ARIN-001 2001:0400::/23
VBNS-IPV6 2001:0408::/35
CANET3-IPV6 2001:0410::/35
VRIO-IPV6-0 2001:0418::/35
CISCO-IPV6-1 2001:0420::/35
QWEST-IPV6-1 2001:0428::/35
DEFENSENET 2001:0430::/35
ABOVENET-IPV6 2001:0438::/35
SPRINT-V6 2001:0440::/35
UNAM-IPV6 2001:0448::/35
GBLX-V6 2001:0450::/35
STEALTH-IPV6-1 2001:0458::/35
NET-CW-10BLK 2001:0460::/35
ABILENE-IPV6 2001:0468::/35
HURRICANE 2001:0470::/35
DREN-V6 2001:0480::/35
AVANTEL-IPV6-1 2001:0488::/35
NOKIA-1 2001:0490::/35
ITESM-IPV6 2001:0498::/35
# IPv6 Prefix Allocations: RIPE-NCC

(whois.ripe.net) – January 2002

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK-BT-19990903 2001:0618::/35</td>
<td></td>
</tr>
<tr>
<td>CH-SWITCH-19990903 2001:0620::/35</td>
<td></td>
</tr>
<tr>
<td>AT-ACONET-19990920 2001:0628::/35</td>
<td></td>
</tr>
<tr>
<td>UK-JANET-19991019 2001:0630::/35</td>
<td></td>
</tr>
<tr>
<td>DE-DFN-19991102 2001:0638::/35</td>
<td></td>
</tr>
<tr>
<td>NL-SURFNET-19990819 2001:0610::/35</td>
<td></td>
</tr>
<tr>
<td>RU-FREENET-19991115 2001:0640::/35</td>
<td></td>
</tr>
<tr>
<td>GR-GRNET-19991208 2001:0648::/35</td>
<td></td>
</tr>
<tr>
<td>EU-UUNET-19990810 2001:0600::/35</td>
<td></td>
</tr>
<tr>
<td>DE-TRMD-20000317 2001:0658::/35</td>
<td></td>
</tr>
<tr>
<td>FR-RENATER-20000321 2001:0660::/35</td>
<td></td>
</tr>
<tr>
<td>EU-EUNET-20000403 2001:0670::/35</td>
<td></td>
</tr>
<tr>
<td>DE-IPF-20000426 2001:0678::/35</td>
<td></td>
</tr>
<tr>
<td>DE-NACAMAR-20000403 2001:0668::/35</td>
<td></td>
</tr>
<tr>
<td>DE-XLINK-20000510 2001:0680::/35</td>
<td></td>
</tr>
<tr>
<td>DE-ECRC-19991223 2001:0650::/35</td>
<td></td>
</tr>
<tr>
<td>FR-TELECOM-20000623 2001:0688::/35</td>
<td></td>
</tr>
<tr>
<td>PT-RCCN-20000623 2001:0690::/35</td>
<td></td>
</tr>
<tr>
<td>SE-SWIPNET-20000828 2001:0698::/35</td>
<td></td>
</tr>
<tr>
<td>PL-ICM-20000905 2001:06A0::/35</td>
<td></td>
</tr>
<tr>
<td>DE-SPACE-19990812 2001:0608::/35</td>
<td></td>
</tr>
<tr>
<td>BE-BELNET-20001101 2001:06A8::/35</td>
<td></td>
</tr>
<tr>
<td>SE-SUNET-20001218 2001:06B0::/35</td>
<td></td>
</tr>
<tr>
<td>IT-CSELT-20001221 2001:06B8::/35</td>
<td></td>
</tr>
<tr>
<td>SE-TELIANET-20010102 2001:06C0::/35</td>
<td></td>
</tr>
<tr>
<td>DE-JIPPII-20000426 2001:0678::/35</td>
<td></td>
</tr>
<tr>
<td>DK-TELEDANMARK-20010131 2001:06C8::/35</td>
<td></td>
</tr>
<tr>
<td>RU-ROSNIROS-20010219 2001:06D0::/35</td>
<td></td>
</tr>
<tr>
<td>PL-CYFRONET-20010221 2001:06D8::/35</td>
<td></td>
</tr>
<tr>
<td>SE-SUNET-20001218 2001:06B0::/35</td>
<td></td>
</tr>
<tr>
<td>NL-INTOUCH-20010307 2001:06E0::/35</td>
<td></td>
</tr>
<tr>
<td>FI-TELIVO-20010321 2001:06E8::/35</td>
<td></td>
</tr>
<tr>
<td>SE-DIGITAL-20010321 2001:06F0::/35</td>
<td></td>
</tr>
<tr>
<td>UK-EASYNET-20010322 2001:06F8::/35</td>
<td></td>
</tr>
<tr>
<td>UNINETT 2001:0700::/35</td>
<td></td>
</tr>
<tr>
<td>FI-FUNET-20010503 2001:0708::/35</td>
<td></td>
</tr>
<tr>
<td>UK-INS-20010518 2001:0710::/35</td>
<td></td>
</tr>
<tr>
<td>CZ-TEN-34-20010521 2001:0718::/35</td>
<td></td>
</tr>
<tr>
<td>ES-REDIRIS-20010521 2001:0720::/35</td>
<td></td>
</tr>
<tr>
<td>UK-VERIO-20010717 2001:0728::/35</td>
<td></td>
</tr>
<tr>
<td>AT-TELEKABEL-20010717 2001:0730::/35</td>
<td></td>
</tr>
<tr>
<td>HU-HUNGARNET-20010717 2001:0738::/35</td>
<td></td>
</tr>
<tr>
<td>DE-VIAG-20010717 2001:0740::/35</td>
<td></td>
</tr>
<tr>
<td>DE-ROKA-20010817 2001:0748::/35</td>
<td></td>
</tr>
<tr>
<td>IT-EDISONTEL-20010906 2001:0750::/35</td>
<td></td>
</tr>
<tr>
<td>UK-NETKONECT-20010918 2001:0758::/35</td>
<td></td>
</tr>
<tr>
<td>IT-GARR-20011004 2001:0760::/35</td>
<td></td>
</tr>
<tr>
<td>DE-CYBERNET-20011008 2001:0768::/35</td>
<td></td>
</tr>
<tr>
<td>IE-HEANET-20011008 2001:0770::/35</td>
<td></td>
</tr>
<tr>
<td>LT-LITNET-20011115 2001:0778::/35</td>
<td></td>
</tr>
<tr>
<td>DE-NORIS-20011203 2001:0780::/35</td>
<td></td>
</tr>
<tr>
<td>FI-SONERA-20011231 2001:0788::/35</td>
<td></td>
</tr>
<tr>
<td>EU-CARRIERI-20020102 2001:0790::/35</td>
<td></td>
</tr>
<tr>
<td>EU-ZZ-2001-07F8 2001:07F8::/29</td>
<td></td>
</tr>
</tbody>
</table>
Agenda

- IPv6 Business Case
- IPv6 Protocols & Standards
- IPv6 routing
- Integration and Transition
- IPv6 Deployment scenarios
IPv6 - So what’s really changed ?!

- **Expanded Address Space**
  Address length quadrupled to 16 bytes

- **Header Format Simplification**
  Fixed length, optional headers are daisy-chained
  IPv6 header is twice as long (40 bytes) as IPv4 header without options (20 bytes)

- **No checksumming at the IP network layer**

- **No hop-by-hop segmentation**
  Path MTU discovery

- **64 bit aligned**

- **Authentication and Privacy Capabilities**
  IPsec is mandated

- **No more broadcast**
IPv4 & IPv6 Header Comparison

Legend:
- field’s name kept from IPv4 to IPv6
- fields not kept in IPv6
- Name & position changed in IPv6
- New field in IPv6
How Was IPv6 Address Size Chosen?

- Some wanted fixed-length, 64-bit addresses
  
  Easily good for $10^{12}$ sites, $10^{15}$ nodes, at .0001 allocation efficiency (3 orders of magnitude more than IPv6 requirement)

  Minimizes growth of per-packet header overhead

  Efficient for software processing

- Some wanted variable-length, up to 160 bits
  
  Compatible with OSI NSAP addressing plans

  Big enough for auto-configuration using IEEE 802 addresses

  Could start with addresses shorter than 64 bits & grow later

- Settled on fixed-length, 128-bit addresses
  
  $340,282,366,920,938,463,463,374,607,431,768,211,456$ in all!
IPv6 Addressing

- IPv6 Addressing rules are covered by multiples RFC’s
  Architecture defined by RFC 2373

- Address Types are:
  - Unicast: One to One (Global, Link local, Site local, Compatible)
  - Anycast: One to Nearest (Allocated from Unicast)
  - Multicast: One to Many
  - Reserved

- A single interface may be assigned multiple IPv6 addresses of any type (unicast, anycast, multicast)
  - No Broadcast Address -> Use Multicast
IPv6 Address Representation

- 16-bit fields in case insensitive colon hexadecimal representation
  - 2031:0000:130F:0000:0000:09C0:876A:130B
- Leading zeros in a field are optional:
  - 2031:0:130F:0:0:9C0:876A:130B
- Successive fields of 0 represented as ::, but only once in an address:
  - 2031:0:130F::9C0:876A:130B
  - 2031::130F::9C0:876A:130B
  - 0:0:0:0:0:0:1 => ::1
  - 0:0:0:0:0:0:0:0 => ::
- IPv4-compatible address representation
  - 0:0:0:0:0:192.168.30.1 = ::192.168.30.1 = ::C0A8:1E01
IPv6 Addressing

- **Prefix Format (PF) Allocation**
  - PF = 0000 0000 : Reserved
  - PF = 001 : Aggregatable Global Unicast Address
  - PF = 1111 1110 10 : Link Local Use Addresses
  - PF = 1111 1110 11 : Site Local Use Addresses
  - PF = 1111 1111 : Multicast Addresses
  - Other values are currently Unassigned (approx. 7/8th of total)
- **All Prefix Formats have to have EUI-64 bits Interface ID**
  - But Multicast
Aggregatable Global Unicast Addresses

Aggregatable Global Unicast addresses are:
Addresses for generic use of IPv6
Structured as a hierarchy to keep the aggregation

See draft-ietf-ipngwg-addr-arch-v3-07
Address Allocation

• The allocation process is:
  IANA allocates 2001::/16 to registries
  Each registry gets a /23 prefix from IANA
  Registry allocates a /32 prefix to an IPv6 ISP
  Policy is that an ISP allocates a /48 prefix to each end customer

Hierarchical Addressing & Aggregation

- Larger address space enables:
  - Aggregation of prefixes announced in the global routing table.
  - Efficient and scalable routing.
- But current Multi-Homing schemes break the model
Link-Local & Site-Local Unicast Addresses

• Link-local addresses for use during auto-configuration and when no routers are present:

  \[
  \begin{array}{c|c|c}
  \hline
  1111111010 & 0 & \text{interface ID} \\
  \hline
  \end{array}
  \]

• Site-local addresses for independence from changes of TLA / NLA*:

  \[
  \begin{array}{c|c|c}
  \hline
  1111111011 & 0 & \text{SLA*} & \text{interface ID} \\
  \hline
  \end{array}
  \]
Multicast Addresses (RFC 2375)

- low-order flag indicates permanent / transient group; three other flags reserved
- scope field:  
  1 - node local  
  2 - link-local  
  5 - site-local  
  8 - organization-local  
  B - community-local  
  E - global  

(all other values reserved)
more on IPv6 Addressing

<table>
<thead>
<tr>
<th>80 bits</th>
<th>16 bits</th>
<th>32 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000..................0000</td>
<td>0000</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**IPv6 Addresses with Embedded IPv4 Addresses**

<table>
<thead>
<tr>
<th>80 bits</th>
<th>16 bits</th>
<th>32 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000..................0000</td>
<td>FFFF</td>
<td>IPv4 Address</td>
</tr>
</tbody>
</table>

**IPv4 mapped IPv6 address**
IPv6 Addressing Examples

- **Ethernet0**
  - **MAC address:** 0060.3e47.1530
  - **IPv6 address:** 2001:410:213:1::/64 eui-64

```
router# show ipv6 interface Ethernet0
Ethetnet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
  Global unicast address(es):
    2001:410:213:1::/64, subnet is 2001:410:213:1::/64
  Joined group address(es):
    FF02::1:FF47:1530
    FF02::1
    FF02::2
  MTU is 1500 bytes
```
6BONE

• The 6bone is an IPv6 testbed setup to assist in the evolution and deployment of IPv6 in the Internet.

   The 6bone is a virtual network layered on top of portions of the physical IPv4-based Internet to support routing of IPv6 packets, as that function has not yet been integrated into many production routers. The network is composed of islands that can directly support IPv6 packets, linked by virtual point-to-point links called "tunnels". The tunnel endpoints are typically workstation-class machines having operating system support for IPv6.

• Over 50 countries are currently involved

• Registry, maps and other information may be found on http://www.6bone.net/
6Bone Addressing

- 6Bone address space defined in RFC2471 uses 3FFE::/16
  - A pTLA receives a /28 prefix
  - A site receives a /48 prefix
  - A LAN receives a /64 prefix
- Guidelines for routing on 6bone - RFC2772
6Bone Topology

- 6Bone is a test bed network with hundreds of sites from 50 countries.
- The 6Bone topology is a hierarchy of providers.
- First-level nodes are backbone nodes called pseudo Top-Level Aggregator (pTLA).
IPv6 Header Options (RFC 2460)

- Processed only by node identified in IPv6 Destination Address field lower overhead than IPv4 options
  - exception: Hop-by-Hop Options header
- Eliminated IPv4’s 40-octet limit on options
  - in IPv6, limit is total packet size, or Path MTU in some cases
IPv6 Header Options (RFC2460)

- Currently defined Headers should appear in the following order
  - IPv6 header
  - Hop-by-Hop Options header
  - Destination Options header
  - Routing header
  - Fragment header
  - Authentication header (RFC 1826)
  - Encapsulating Security Payload header (RFC 1827)
  - Destination Options header
  - upper-layer header
MTU Issues

- minimum link MTU for IPv6 is 1280 octets (versus 68 octets for IPv4)
  => on links with MTU < 1280, link-specific fragmentation and reassembly must be used
- implementations are expected to perform path MTU discovery to send packets bigger than 1280
- minimal implementation can omit PMTU discovery as long as all packets kept = 1280 octets
- a Hop-by-Hop Option supports transmission of “jumbograms” with up to $2^{32}$ octets of payload
Neighbour Discovery (RFC 2461)

- Protocol built on top of ICMPv6 (RFC 2463)
  - combination of IPv4 protocols (ARP, ICMP, IGMP, ...)
- Fully dynamic, interactive between Hosts & Routers
  - defines 5 ICMPv6 packet types
    - Router Solicitation / Router Advertisements
    - Neighbor Solicitation / Neighbor Advertisements
    - Redirect
Neighbour Discovery (RFC 2461)

• defined mechanisms between nodes attached on the same link
  • Router discovery
  • Prefix discovery
  • Parameters discovery, i.e.: link MTU, hop limit,…
  • Address auto-configuration
  • Address Resolution (same function as ARP)
  • Next-hop determination
  • Neighbor Unreachability Detection (useful for default routers)
  • Duplicate Address Detection
  • Redirect
IPv6 Auto-Configuration

• **Stateless (RFC2462)**
  
  Host autonomously configures its own Link-Local address

  Router solicitation are sent by booting nodes to request RAs for configuring the interfaces.

• **Stateful**
  
  DHCPv6 (under definition at IETF)

• **Renumbering**
  
  Hosts renumbering is done by modifying the RA to announce the old prefix with a short lifetime and the new prefix.

  Router renumbering protocol (RFC 2894), to allow domain-interior routers to learn of prefix introduction / withdrawal

At boot time, an IPv6 host builds a Link-Local address, then its global IPv6 address(es) from RA
IP Mobility

- Mobility means:
  Mobile devices are fully supported while moving
  Built-in on IPv6
  Any node can use it
  Efficient routing means performance for end-users

![Diagram of IP Mobility with Home Agent, Mobile Node, and Destination Node with IPv6 addresses 3ffe:0b00:c18::1 and 2001:2:a010::5, indicating that it is not possible in IPv4]
Overview of Mobile IPv6 Functionality

1. MN obtains IP address using stateless or stateful autoconfiguration
2. MN registers with HA
3. HA tunnels packets from CN to MN
4. MN sends packets from CN directly or via tunnel to HA
# IPv6 Technology Scope

<table>
<thead>
<tr>
<th>IP Service</th>
<th>IPv4 Solution</th>
<th>IPv6 Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing Range</td>
<td>32-bit, Network Address Translation</td>
<td>128-bit, Multiple Scopes</td>
</tr>
<tr>
<td>Autoconfiguration</td>
<td>DHCP</td>
<td>Serverless, Reconfiguration, DHCP</td>
</tr>
<tr>
<td>Security</td>
<td>IPSec</td>
<td>IPSec Mandated, works End-to-End</td>
</tr>
<tr>
<td>Mobility</td>
<td>Mobile IP</td>
<td>Mobile IP with Direct Routing</td>
</tr>
<tr>
<td>IP Multicast</td>
<td>IGMP/PIM/Multicast BGP</td>
<td>MLD/PIM/Multicast BGP, Scope Identifier</td>
</tr>
</tbody>
</table>
IPv6 Standards

• Core IPv6 specifications are IETF Draft Standards
  => well-tested & stable
  IPv6 base spec, ICMPv6, Neighbor Discovery, PMTU Discovery,...

• Other important specs are further behind on the standards track, but in good shape
  mobile IPv6, header compression,...
  for up-to-date status: playground.sun.com/ipv6

• 3GPP UMTS Rel. 5 cellular wireless standards mandate IPv6; also being considered by 3GPP2
IPv6 Current Status - Standardisation

- Several key components now on Standards Track:
  - Specification (RFC2460)
  - Neighbour Discovery (RFC2461)
  - ICMPv6 (RFC2463)
  - IPv6 Addresses (RFC2373/4/5)
  - RIP (RFC2080)
  - BGP (RFC2545)
  - IGMPv6 (RFC2710)
  - OSPF (RFC2740)
  - Router Alert (RFC2711)
  - Jumbograms (RFC2675)
  - Autoconfiguration (RFC2462)

IPv6 over:
- PPP (RFC2023)
- Ethernet (RFC2464)
- FDDI (RFC2467)
- Token Ring (RFC2470)
- NBMA (RFC2491)
- ATM (RFC2492)
- Frame Relay (RFC2590)
- ARCnet (RFC2549)
Recent IPv6 “Hot Topics” in the IETF

- Multi-homing
- Address selection
- Address allocation
- DNS discovery
- 3GPP usage of IPv6
- Anycast addressing
- Scoped address architecture
- Flow-label semantics
- API issues
  (flow label, traffic class, PMTU discovery, scoping,...)
- Enhanced router-to-host info
- Site renumbering procedures
- Inter-domain multicast routing
- Address propagation and AAA issues of different access scenarios
- End-to-end security vs. firewalls
- And, of course, transition / co-existence / interoperability with IPv4
  (a bewildering array of transition tools and techniques)

Note: this indicates vitality, not incompleteness, of IPv6!
Agenda

- IPv6 Business Case
- IPv6 Protocols & Standards
- IPv6 Routing
- Integration and Transition
- IPv6 Deployment scenarios
Routing in IPv6

- As in IPv4, IPv6 supports IGP and EGP routing protocols:
  - IGP for within an autonomous system are
    - RIPng (RFC 2080)
    - OSPFv3 (RFC 2740)
    - Integrated IS-ISv6 (draft-ietf-isis-ipv6-02.txt)
    - EIGRP for IPv6 (Cisco)
  - EGP for peering between autonomous systems
    - MP-BGP4 (RFC 2858 and RFC 2545)
- IPv6 still uses the longest-prefix match routing algorithm
IPv6 IGP LSP Option

- i/IS-ISv6
  Shared IGP for IPv4 & IPv6
  Route from A to B same for IPv4 & IPv6
  Separate SPFs may provide SIN routing

- OSPFv3
  "Ships in the Night" routing
  Need to run another IGP for IPv4
  Route from A to B may differ for IPv4 & IPv6
Integrated IS-IS for IPv6

- ISO 10589 specifies OSI IS-IS routing protocol for CLNS traffic
  - Tag/Length/Value (TLV) options to enhance the protocol
  - A Link State protocol with a 2 level hierarchical architecture.

- IETF RFC 1195 added IP support, also known as Integrated IS-IS (I/IS-IS)
  - I/IS-IS runs on top of the Data Link Layer
  - Requires CLNP to be configured

- IETF Draft RFC defines how to support IPv6 on I/IS-IS
draft-ietf-isis-ipv6-02.txt
New Tag/Length/Values for IPv6 routing

- IPv6 Reachability TLV (0xEC)
  - External bit
  - Equivalent to IP Internal/External Reachability TLV’s
- IPv6 Interface Address TLV (0xE8)
  - For Hello PDUs, must contain the Link-Local address
  - For LSP, must only contain the non-Link Local address
- IPv6 NLPID (0x8E) is advertised by IPv6 enabled routers
Single SPF rules

- If IS-IS is used for both IPv4 and IPv6 in an area, both protocols must support the same topology within this area.

- All interfaces configured with IS-ISv6 must support IPv6
  Can’t be configured on MPLS/TE since IS-ISv6 extensions for TE are not yet defined

- All interfaces configured with IS-IS for both protocols must support both of them
  IPv6 configured tunnel won’t work, GRE should be used in this configuration
IS-IS Hierarchy & IPv6 example

IPv4-IPv6 enable router
IPv4-only enable router
OSPFv3 overview

- OSPFv3 is OSPF for IPv6
- Based on OSPFv2, with enhancements
- Distributes IPv6 prefixes
- Runs directly over IPv6
- Ships-in-the-night with OSPFv2
Similarities to OSPFv2

• Same basic packet types
  Hello, DBD, LSR, LSU, LSA

• Same mechanisms for neighbor discovery and adjacency formation

• Same interface types
  P2P, P2MP, Broadcast, NBMA, Virtual

• Same LSA flooding and ageing

• Almost same LSA type
Differences from OSPFv2

- Runs over a link, not a subnet
  - Multiple instances per link
- Topology not IPv6-specific
  - Router ID
  - Link ID
- Standard authentication mechanisms
- Uses link local addresses
- Generalized flooding scope
- Two new LSA types
# LSA Type Review

<table>
<thead>
<tr>
<th>LSA function code</th>
<th>LSA type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router-LSA</td>
<td>0x2001</td>
</tr>
<tr>
<td>Network-LSA</td>
<td>0x2002</td>
</tr>
<tr>
<td>Inter-Area-Prefix-LSA</td>
<td>0x2003</td>
</tr>
<tr>
<td>Inter-Area-Router-LSA</td>
<td>0x2004</td>
</tr>
<tr>
<td>AS-External-LSA</td>
<td>0x4005</td>
</tr>
<tr>
<td>Group-membership-LSA</td>
<td>0x2006</td>
</tr>
<tr>
<td>Type-7-LSA</td>
<td>0x2007</td>
</tr>
<tr>
<td>Link-LSA</td>
<td>0x0008</td>
</tr>
<tr>
<td>Intra-Area-Prefix-LSA</td>
<td>0x2009</td>
</tr>
</tbody>
</table>

© 2003, Cisco Systems, Inc. All rights reserved.
Link LSA

- A link LSA per link
- link local scope flooding on the link they are associated with
- Provide router link local address
- List all IPv6 prefixes attached to the link
Intra-area prefix LSA

- Multiple LSA with the different Link State ID
- Area flooding scope
- 1- associate prefix with transit network referencing a Network-LSA
- 2- associate prefix with a router or a stub referencing a Router-LSA
Multi-Protocol BGP - RFC2283

- Extension to the BGP protocol in order to carry routing information about other protocols

  - Multicast
  - MPLS VPN
  - IPv6
  - IPv6+label
  - CLNS

- Exchange of Multi-Protocol NLRI must be negotiated at session set up
Two new attributes

- New non-transitive and optional BGP attributes
  - **MP_REACH_NLRI**
    
    “Carry the set of reachable destinations together with the next-hop information to be used for forwarding to these destinations”

  - **MP_UNREACH_NLRI**
    
    Carry the set of unreachable destinations
MP_REACH_NRLI structure

- Attribute contains one or more Triples
  - Address Family Information (AFI) and Sub-AFI
    - AFI = 1 (IPv4)
    - AFI = 2 (IPv6)
  - Next-hop information
  - NLRI (Network Layer Reachability Info)
IPv6 specific extensions:

Scoped addresses: Next-hop contains a global IPv6 address and/or potentially a link-local address

NEXT_HOP and NLRI are expressed as IPv6 addresses and prefix.

Address Family Information (AFI) = 2 (IPv6)

Sub-AFI = 1 (NLRI is used for unicast)

Sub-AFI = 2 (NLRI is used for multicast RPF check)

Sub-AFI = 3 (NLRI is used for both unicast and multicast RPF check)
Multi-Protocol BGP – Packet format

• The BGP UPDATE Message

- Unfeasible Routes Length (2 Octets)
- Withdrawn Routes (Variable)
- Total path Attribute Length (2 Octets)
- Path Attributes (Variable)
- Network Layer Reachability Information (Variable)

- Each update message contains attributes, like origin, AS-Path, Next-Hop, ....... MP_REACH_NLRI
MBGP – Packet format for IPv6

- **MP_REACH_NLRI Attribute**

  - Address Family Identifier (2)
  - Subsequent Address Family Identifier (1)
  - Length of the Next-Hop Address (16 or 32)
  - Network Address of Next-Hop (global and/or Link local)
  - Network Layer Reachability Information (Variable)
BGP Capabilities Negotiation

- BGP routers establish BGP sessions through the OPEN message
- OPEN message contains optional parameters
- BGP session is terminated if OPEN parameters are not recognised
- A new optional parameter: CAPABILITIES
BGP Capabilities Negotiation

- A BGP router sends an OPEN message with CAPABILITIES parameter containing its capabilities:
  - Multiprotocol extension (AFI/SAFI)
  - Route Refresh
  - Outbound Route Filtering
MBGP—Capability Negotiation

AS 123

BGP Session for IPv6 Unicast

NLRI

AS 321

BGP: 3FFE:B00:C18:2:1::1 sending OPEN, version 4, my as: 123
BGP: 3FFE:B00:C18:2:1::1 rcv OPEN, version 4
BGP: 3FFE:B00:C18:2:1::1 rcv OPEN w/ OPTION parameter len: 16
BGP: 3FFE:B00:C18:2:1::1 rcvd OPEN w/ optional parameter type 2 (Capability) len 6
BGP: 3FFE:B00:C18:2:1::1 OPEN has CAPABILITY code: 1, length 4
BGP: 3FFE:B00:C18:2:1::1 OPEN has MP_EXT CAP for afi/safi: 2/1
BGP: 3FFE:B00:C18:2:1::1 went from OpenSent to OpenConfirm
BGP: 3FFE:B00:C18:2:1::1 went from OpenConfirm to Established
%BGP-5-ADJCHANGE: neighbor 3FFE:B00:C18:2:1::1 Up
Agenda

- IPv6 Business Case
- IPv6 Protocols & Standards
- IPv6 Routing
- Integration and Transition
- IPv6 Deployment scenarios
IETF NGTrans Working Group

- Define the processes by which networks can be transitioned from IPv4 to IPv6
- Define & specify the mandatory and optional mechanism that vendors are to implement in Hosts, Routers and other components of the Internet in order for the Transition.
IPv4-IPv6 Transition / Co-Existence

A wide range of techniques have been identified and implemented, basically falling into three categories:

1. **Dual-stack** techniques, to allow IPv4 and IPv6 to co-exist in the same devices and networks
2. **Tunneling** techniques, to avoid order dependencies when upgrading hosts, routers, or regions
3. **Translation** techniques, to allow IPv6-only devices to communicate with IPv4-only devices

Expect all of these to be used, in combination
Dual Stack Approach

- Dual stack node means:
  - Both IPv4 and IPv6 stacks enabled
  - Applications can talk to both
  - Choice of the IP version is based on name lookup and application preference

Preferred method on Application’s servers

Frame Protocol ID
In a dual stack case, an application that:

- Is IPv4 and IPv6-enabled
- Asks the DNS for all types of addresses
- Chooses one address and, for example, connects to the IPv6 address
A Dual Stack Configuration

IPv6-enable router

If IPv4 and IPv6 are configured on one interface, the router is dual-stacked

Telnet, Ping, Traceroute, SSH, DNS client, TFTP,...

IPv4: 192.168.99.1
IPv6: 2001:410:213:1::1/64

router#
ipv6 unicast-routing

interface Ethernet0
ip address 192.168.99.1 255.255.255.0
ipv6 address 2001:410:213:1::1/64
Using Tunnels for IPv6 Deployment

- Many techniques are available to establish a tunnel:
  - Manually configured
    - Manual Tunnel (RFC 2893)
    - GRE (RFC 2473)
  - Semi-automated
    - Tunnel broker
  - Automatic
    - Compatible IPv4 (RFC 2893)
    - 6to4 (RFC 3056)
    - 6over4 (RFC 2529)
    - ISATAP
**IPv6 over IPv4 Tunnels**

- Tunneling is encapsulating the IPv6 packet in the IPv4 packet
- Tunneling can be used by routers and hosts
Manually Configured Tunnel (RFC 2893)

- Manually Configured tunnels require:
  - Dual stack end points
  - Both IPv4 and IPv6 addresses configured at each end

```
routerA#
interface Tunnel0
  ipv6 address 3ffe:b00:c18:1::3/64
  tunnel source 192.168.99.1
  tunnel destination 192.168.30.1
  tunnel mode ipv6ip
```
```
routerB#
interface Tunnel0
  ipv6 address 3ffe:b00:c18:1::2/64
  tunnel source 192.168.30.1
  tunnel destination 192.168.99.1
  tunnel mode ipv6ip
```
IPv4 Compatible Tunnel (RFC 2893)

- IPv4-compatible addresses are easy way to auto-tunnel
6to4 Tunnel (RFC 3056)

- **6to4 Tunnel:**
  
  Is an automatic tunnel method
  Gives a prefix to the attached IPv6 network
  2002::/16 assigned to 6to4
  Requires one global IPv4 address on each Ingress/Egress site

```
routerB#
interface Loopback0
  ip address 192.168.30.1 255.255.255.0
  ipv6 address 2002:c0a8:1e01::/64 eui-64
interface Tunnel0
  no ip address
  ipv6 unnumbered Ethernet0
  tunnel source Loopback0
  tunnel mode ipv6ip 6to4
ipv6 route 2002::/16 Tunnel0
```
**6to4 Relay**

6to4 Router A

IPv6 Network

Network prefix: 2002:c0a8:6301::/48

IPv6 address: 2002:c0a8:6301:1::/64 eui-64

interface Loopback0
  ip address 192.168.99.1 255.255.255.0
  ipv6 address 2002:c0a8:6301:1::/64 eui-64

interface Tunnel0
  no ip address
  ipv6 unnumbered Ethernet0
tunnel source Loopback0
tunnel mode ipv6ip 6to4

ipv6 route 2002::/16 Tunnel0
ipv6 route ::/0 2002:c0a8:1e01::1

6to4 Relay

IPv6 Internet

IPv6 Network

IPv6 address: 2002:c0a8:1e01::1

- **6to4 relay:**
  - Is a gateway to the rest of the IPv6 Internet
  - Default router
  - Anycast address (RFC 3068) for multiple 6to4 Relay
Tunnel Broker

3. Tunnel Broker configures the tunnel on the tunnel server or router.
4. Client establishes the tunnel with the tunnel server or router.

- **Tunnel broker:**
  Tunnel information is sent via http-ipv4
IPv6-IPv4 Communication Mechanisms

- Translation
  - NAT-PT (RFC 2766)
  - TCP-UDP Relay (RFC 3142)
- DSTM (Dual Stack Transition Mechanism)
- API
  - BIS (Bump-In-the-Stack) (RFC 2767)
  - BIA (Bump-In-the-API)
- ALG
  - SOCKS-based Gateway (RFC 3089)
  - NAT-PT (RFC 2766)
ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

- Tunnelling of IPv6 in IPv4
- In a single administrative domain
- Creates a virtual IPv6 link over the full IPv4 network
- Automatic tunnelling is done by a specially formatted ISATAP address which includes
  - An ISATAP special identifier
  - The IPv4 address of the node
- ISATAP nodes are dual-stack
ISATAP address format

- An ISATAP address of a node is defined as:
- A /64 prefix dedicated to the ISATAP overlay link
- Interface identifier:
  - Leftmost 32 bits = 0000:5EFE:
    - Identify an ISATAP address
  - Rightmost 32 bits = <ipv4 address>
    - The IPv4 address of the node

| ISATAP dedicated prefix | 0000:5EFE | IPv4 address |
ISATAP prefix advertisement

1. Potential router list (PRL): 192.168.4.1
   - 192.168.2.1
   - fe80::5efe:c0a8:0201
   - 192.168.4.1
   - fe80::5efe:c0a8:0401
   - 3ffe:b00:ffff:5efe:c0a8:0401

2. IPv6 over IPv4 tunnel
   - Dest Addr: fe80::5efe:c0a8:0201
   - Src Addr: fe80::5efe:c0a8:0401

3. IPv6 over IPv4 tunnel
   - Dest Addr: fe80::5efe:c0a8:0401
   - Src Addr: fe80::5efe:c0a8:0201
   - Prefix = 3ffe:b00:ffff::/64
   - Lifetime, options

4. Host A configures global IPv6 address using ISATAP prefix 3ffe:b00:ffff::/64
ISATAP configuration example

IPv6 Network        IPv4 Network

192.168.4.1
fe80::5efe:c0a8:0401
3ffe:b00:ffff:5efe:c0a8:0401

192.168.2.1
fe80::5efe:c0a8:0201
3ffe:b00:ffff:5efe:c0a8:0201

192.168.3.1
fe80::5efe:c0a8:0301
3ffe:b00:ffff:5efe:c0a8:0301

interface FastEthernet0/0
ipv6 address3FFE:ffff:123:1999::1/64
!
int tu0
Tunnel mode isatap
!
int fa0/0
NAT-PT for IPv6

- NAT-PT (Network Address Translation - Protocol Translation) - RFC 2766
- NAT-PT allows native IPv6 hosts and applications to communicate with native IPv4 hosts and applications, and vice versa.
- Easy-to-use transition and co-existence solution
NAT-PT Concept

• PREFIX is a 96-bit field that allows routing back to the NAT-PT device

IPv4 Host

172.16.1.1

IPv6 Host

NAT-PT packet flow

IPv4 Host 172.16.1.1


   Dst: PREFIX::1

2. Src: 172.17.1.1
   Dst: 172.16.1.1

3. Src: 172.16.1.1
   Dst: 172.17.1.1

4. Src: PREFIX::1
# Stateless IP ICMP Translation

<table>
<thead>
<tr>
<th>IPv6 field</th>
<th>IPv4 field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version = 6</td>
<td>Version = 4</td>
<td>Overwrite</td>
</tr>
<tr>
<td>Traffic class</td>
<td>DSCP</td>
<td>Copy</td>
</tr>
<tr>
<td>Flow label</td>
<td>N/A</td>
<td>Set to 0</td>
</tr>
<tr>
<td>Payload length</td>
<td>Total length</td>
<td>Adjust</td>
</tr>
<tr>
<td>Next header</td>
<td>Protocol</td>
<td>Copy</td>
</tr>
<tr>
<td>Hop limit</td>
<td>TTL</td>
<td>Copy</td>
</tr>
</tbody>
</table>
DNS Application Layer Gateway

IPv4 DNS

1. Type=AAAA Q="host.nat-pt.com"

2. Type=A Q="host.nat-pt.com"

3. Type=A R="172.16.1.5"

IPv6 Host

4. Type=AAAA R="2010::45"

5. Type=PTR Q="5.1.16.172.in-addr-arpa"

6. Type=PTR R="host.nat-pt.com"

7. Type=PTR Q="5.4.0...0.1.0.2.IP6.INT"

NAT-PT

8. Type=PTR R="host.nat-pt.com"
NAT-PT points of attention

- ALG per application carrying IP address
- No End to End security
  - no DNSsec
  - no IPsec because different address realms
Agenda

- IPv6 Business Case
- IPv6 Protocols & Standards
- IPv6 routing
- Integration and Transition
- IPv6 Deployment scenarios
IPv6 Timeline

- **Early adopter**
- Application porting <= Duration 3+ years =>
- ISP adoption <= Duration 3+ years =>
- Consumer adoption <= Duration 5+ years =>
- Enterprise adoption <= Duration 3+ years =>

Distributed Gaming on Sony PS2?

Windows .NET server availability
How long do you need for each phase of an IPv6 deployment project?
IPv6 Deployment Scenarios

- Many ways to deliver IPv6 services to End Users
  - End-to-end IPv6 traffic forwarding is the Key feature
  - Minimize operational upgrade costs
- Service Providers and Enterprises may have different deployment needs
  - Incremental Upgrade/Deployment
  - ISPs differentiate Core and Edge infrastructures upgrade
  - Enterprise Campus and WAN may have separate upgrade paths
- IPv6 over IPv4 tunnels
- Dedicated Data Link layers for native IPv6
- Dual stack Networks
  - IPv6 over MPLS or IPv4-IPv6 Dual Stack Routers
IPv6 over IPv4 Tunnels

- Several Tunnelling mechanisms defined by IETF
  - Apply to ISP and Enterprise WAN networks
    - GRE, Configured Tunnels, Automatic Tunnels using IPv4 compatible IPv6 Address, 6to4
  - Apply to Campus
    - ISATAP
- Leverages 6Bone experience
- No impact on Core infrastructure
  - Either IPv4 or MPLS
Native IPv6 over Dedicated Data Links

- Native IPv6 links over dedicated infrastructures
  - ATM PVC, dWDM Lambda, Frame Relay PVC, Serial, Sonet/SDH, Ethernet
- No impact on existing IPv4 infrastructures
  - Only upgrade the appropriate network paths
  - IPv4 traffic (and revenues) can be separated from IPv6
- Network Management done through IPv4
IPv6 Tunnels & Native Case Study

• **ISP scenario**
  
  Configured Tunnels or Native IPv6 between IPv6 Core Routers
  
  Configured Tunnels or Native IPv6 to IPv6 Enterprise’s Customers
  
  Tunnels for specific access technologies, eg. Cable
  
  MP-BGP4 Peering with other 6Bone users
  
  Connection to an IPv6 IX
  
  6to4 relay service

• **Enterprise/Home scenario**

  6to4 tunnels between sites, use 6to4 Relay to connect to the IPv6 Internet

  Configured tunnels between sites or to 6Bone users

  ISATAP tunnels or Native IPv6 on a Campus

Use the most appropriate
Dual Stack IPv4-IPv6 Infrastructure

- It is generally a long term goal when IPv6 traffic and users will be rapidly increasing
- May be easier on network’s portion such as Campus or Access networks
- Theoretically possible but the network design phase has to be well planned
  - Memory size to handle the growth for both IPv4 & IPv6 routing tables
  - IGP options & its management: Integrated versus “Ships in the Night”
  - Full network upgrade impact
- IPv4 and IPv6 Control & Data planes should not impact each other
  - Feedback, requirements & experiments are welcome
Dual Stack IPv4-IPv6 Case Study

• **Campus scenario**
  
  Upgrade all layer 3 devices to allow IPv6 hosts deployment anywhere, similar to IPX/IP environment

• **ISP**
  
  Access technologies may have IPv4 dependencies, eg. for User’s management
  
  Transparent IPv4-IPv6 access services
  
  Core may not go dual-stack before sometimes to avoid a full network upgrade
IPv6 over MPLS Infrastructure

- Service Providers have already deployed MPLS in their IPv4 backbone for various reasons
  - MPLS/VPN, MPLS/QoS, MPLS/TE, ATM + IP switching
- Several IPv6 over MPLS scenarios
  - IPv6 Tunnels configured on CE (no impact on MPLS)
  - IPv6 over Circuit_over_MPLS (no impact on IPv6)
  - IPv6 Provider Edge Router (6PE) over MPLS (no impact on MPLS core)
  - Native IPv6 MPLS (require full network upgrade)
- Upgrading software to IPv6 Provider Edge Router (6PE)
  - Low cost and risk as only the required Edge routers are upgraded or installed
  - Allows IPv6 Prefix delegation by ISP
IPv6 Provider Edge Router (6PE) over MPLS

- IPv4 or MPLS Core Infrastructure is IPv6-unaware
- PEs are updated to support Dual Stack/6PE
- IPv6 reachability exchanged among 6PEs via iBGP
- IPv6 packets transported from 6PE to 6PE inside MPLS
Native IPv6-only Infrastructure?

- **Application’s focus**
  
  When will the IPv6 traffic be important enough?

- **Requires**
  
  Full Network upgrade (software & potentially hardware)

  Native IPv6 Network Management Solutions

  Enhanced IPv6 services availability
  
  Multicast, QoS, security,…

  Transport IPv4 through tunnels over IPv6

  IPv4 traffic requirements?
# IPv6 Deployment Phases

<table>
<thead>
<tr>
<th>Phases</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Tunnels over IPv4</td>
<td>Low cost, low risk to offer IPv6 services. No infrastructure change. Has to evolve when many IPv6 clients get connected.</td>
</tr>
<tr>
<td>Dedicated Data Link layers for Native IPv6</td>
<td>Natural evolution when connecting many IPv6 customers. Require a physical infrastructure to share between IPv4 and IPv6 but allow separate operations.</td>
</tr>
<tr>
<td>MPLS 6PE</td>
<td>Low cost, low risk , it requires MPLS and MP-BGP4. No need to upgrade the Core devices , keep all MPLS features (TE, IPv4-VPN).</td>
</tr>
<tr>
<td>Dual stack</td>
<td>Requires a major upgrade. Valid on Campus or Access networks as IPv6 hosts may be located anywhere.</td>
</tr>
<tr>
<td>IPv6-Only</td>
<td>Requires upgrading all devices. Valid when IPv6 traffic will become predominant.</td>
</tr>
</tbody>
</table>
Moving IPv6 to Production

Enterprise
WAN: 6to4, IPv6 over IPv4, Dual Stack

Aggregation
IPv6 over IPv4 tunnels or Dedicated data link layers

Dual Stack or MPLS & 6PE

Cable
IPv6 over IPv4 Tunnels

6Bone
IPv6 over IPv4 tunnels or Dedicated data link layers

ISP’s
IPv6 IX

Telecommuter
IPv6 over IPv4 tunnels or Dual stack

Residential

DSL, FTTH, Dial

Enterprise

WAN: 6to4, IPv6 over IPv4, Dual Stack

6to4 Relay

Dual Stack

ISATAP
..a lot to do still..

Though IPv6 today has all the functional capability of IPv4:

• Implementations are not as advanced (e.g., with respect to performance, multicast support, compactness, instrumentation, etc.)

• Deployment has only just begun

• Much work to be done moving application, middleware, and management software to IPv6

• Much training work to be done (application developers, network administrators, sales staff,...)

• Some of the advanced features of IPv6 still need specification, implementation, and deployment work
IPv6 Implementations

- Most of Operating Systems can deliver an IPv6 stack
- Internetworking vendors are committed on IPv6 support
  - Interoperability events, eg. TAHI, UNH, ETSI,…
- For an update status, please check on
- Applications IPv6 awareness (see www.hs247.com)
  - Net Utilities (ping, finger, ifconfig….etc), NFS, Routing Daemons
  - FTP, TELNET, WWW Server & Browser, Sendmail, SMTP
IPv6 Forum

• 138 members (March 22\textsuperscript{nd}, 2002)
  Created in 1999

• Mission is to promote IPv6 not to specify it (IETF)
  www.ipv6forum.com

• IPv6 Forum OneWorld working group
  Australian, India, Korea, Mexico, Russian, UK,…

• Held ‘IPv6 summit’ around the World
IPv6—Conclusion

IPv6 Ready for Production Deployment?

• Evaluate IPv6 products and services, as available
  Major O.S., applications and infrastructure for the IT industry
  New IP appliances, e.g…3G (NTT DoCoMo,…), gaming,…
  IPv6 services from ISP

• Upgrade your routers with IPv6 ready software

• Plan for IPv6 integration and IPv4-IPv6 co-existence
  Training, applications inventory, and IPv6 deployment planning
Questions?