AGENDA

- IPv6 Protocol
  - Who
  - What
  - Why
  - When
  - Where
  - How
  - How Much
  - References
IP Has NO Who

IP addresses do not designate people

IP addresses are logical addresses assigned to a computer’s physical interfaces

Sorry Horton
WHAT

- IP stands for “Internet Protocol”
- IPv6 is the new global addressing scheme for the Internet
- Internet Protocol version 6 (IPv6) is the most recent version of IP, that provides an identification and location system for computers on networks and routes traffic across the Internet.
- IPv6 is intended to replace IPv4 over time.
IPV6 ENHANCEMENTS

- Expanded address space
  - IPv6 increases the IP address size from 32 bits to 128 bits
    - Support more levels of addressing hierarchy
    - Has a much greater number of addressable nodes
    - Simpler auto-configuration of addresses.
  - Improves scalability of multicast routing by adding a "scope" field to multicast addresses.
  - Defines an "anycast address" that sends a packet to any one of a group of nodes.

- Address autoconfiguration
  - Dynamic assignment of IPv6 addresses

- Header Format Simplification
  - Some IPv4 header fields have been dropped or made optional
    - to reduce the common-case processing cost of packet handling
    - to limit the bandwidth cost of the IPv6 header.
IPV6 ENHANCEMENTS

- Improved Support for Extensions and Options
  - Separate optional headers between IPv6 header and transport layer header
  - Most are not examined by intermediate routes
  - Improved speed and simplified router processing
  - Easier to extend options

- Flow Labeling Capability
  - IPv6 labels packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.

- Authentication and Privacy Capabilities
  - IPv6 specifies extensions for authentication, data integrity, and (optional) data confidentiality
WHY

★ The Internet Engineering Task Force (IETF) developed IPv6 to deal with IPv4 address space exhaustion.
★ Continuing demand for unique IP addresses
★ IPv4 has 32 bit addresses – 4.2 billion unique addresses
  ★ All of these have been allocated and assigned
★ IPv6 has 128 bit addresses – 3.4e38 unique addresses
  ★ Abundance of unallocated and unassigned addresses
IPV4 ADDRESSING PROBLEMS

- The current addressing used in the Internet relies on separate IPv4 addresses being assigned to ISPs in contiguously numbered blocks for routing efficiency
  - Insufficient number of IPv4 addresses
  - Fragmentation in the IPv4 address space
  - Sites cannot easily renumber
  - Many more separate routes than absolutely necessary
  - Route computation complexity
    - too many routes,
    - too many dynamic changes
    - too much computation in routers
WHEN

- The Internet started in 1969 and used NCP protocol till 1982. A flash cut then replaced NCP with IPv4.
- IPv6 started as NextGen IP during the 1990s when the incredible success of the Internet forced network scientists to realize that 32 bit addresses would be insufficient to accommodate anticipated growth.
- Government mandates for IPv6 accelerated deployment.
IPV6 ADOPTION RATE

Native: 15.99% 6to4/Teredo: 0.01% Total IPv6: 16.00% | Jan 29, 2017
WHERE

- Used in devices intended to communicate over the global Internet
  - For example: PCs, Smartphones, IoT, Robots, Cloud
- IPv6 corresponds to Layer 3 of the OSI Network Protocol Reference Model
- Current global deployment status
INTERNET LAYERED ARCHITECTURE

- Application Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer
Most of the rest of this presentation describes how IPv6 works
MANDATORY IP PACKET HEADERS

IPv4 Header

- Version
- IHL
- Type of Service
- Total Length
- Identification
- Flags
- Fragment Offset
- Time to Live
- Protocol
- Header Checksum
- Source Address
- Destination Address

IPv6 Header

- Version
- Traffic Class
- Flow Label
- Payload Length
- Next Header
- Hop Limit
- Source Address
- Destination Address
IPV6 STRUCTURE
IPV6 HEADER FIELDS

- Version Number - 6
- Traffic Class
  - Classes or priorities of this packet (typically diffserv)
- Flow Label (RFC 3697)
  - Used by hosts requesting special handling
  - Routers cannot parse this field
- Payload length
  - Excludes 40 Byte IP header, includes all extension headers plus user data, 1280 Byte MTU (min)
- Next Header
  - Identifies type of header following the IPv6 header, uses the same values as the IPv4 Protocol field
- Hop Limit
  - Decremented by 1 by each node that forwards the packet.
  - The packet is discarded if Hop Limit is decremented to zero.
- Source Address
- Destination address
IPV6 QOS AND FLOWS

- Traffic Class Field
  - Functionally equivalent to DiffServ in IPv4, as defined by RFC2474, 2475, etc.
- Flow Label Field – 20 bits that enable classification of packets belonging to a specific flow as defined in RFC3697
  - A flow is a sequence of packets that should receive specific non-default handling from the network
  - Designated by a 3-tuple of the Flow Label and the Source and Destination Address fields
  - IPv6 source nodes supporting the flow labeling MUST be able to label known flows
  - Flow state expires 120 seconds after last packet in flow processed
  - A Flow Label of 0 is used to indicate packets not part of any flow
  - Network routers have no definitions of flow labels, they are only processed by end nodes
  - Without the flow label, a classifier must use transport next header value and port numbers
    - Less efficient – needs to parse the option headers
    - Not possible under all conditions (fragmentation or IPSec ESP)
OBTAINING IPV6 ADDRESSES

- Make up your own (But won’t be globally routed)
- From your ISP
- From your Regional Internet Registry (as per IANA.org)

<table>
<thead>
<tr>
<th>Registry</th>
<th>Area Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFRINIC</td>
<td>Africa Region</td>
</tr>
<tr>
<td>APNIC</td>
<td>Asia/Pacific Region</td>
</tr>
<tr>
<td>ARIN</td>
<td>Canada, USA, and some Caribbean Islands</td>
</tr>
<tr>
<td>LACNIC</td>
<td>Latin America and some Caribbean Islands</td>
</tr>
<tr>
<td>RIPE NCC</td>
<td>Europe, the Middle East, and Central Asia</td>
</tr>
</tbody>
</table>
IPV6 ADDRESS NOTATION

- IPv6 uses hex numbers (base 16, 0-F) that compresses the resulting address by allowing the removal of some zeros. So a typical address appears as:
  - DEAD:BEEF:0000:0000:0000:0073:FEED:F00D
  - Each address contains 8 groups of four hex digits (16 bit groups)
  - Notice that the separators are now colons rather than periods

- This address can be shown in a shorthand version which is:
  - DEAD:BEEF::73:FEED:F00D
  - Leading zeros within the four digit groups can be dropped, so 0073 becomes 73
  - Consecutive 16-bit numbers with a zero value may be replaced with a double colon
  - Only one null string can be replaced with the double colon since if more then a single null string were compressed, it would not be possible to determine the length of each

- The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. Notated as ::0

- The unicast address 0:0:0:0:0:0:1 is called the loopback address. It must never be assigned to any physical interface. Notated as ::1
IPV6 ADDRESSES

- 128 bits in length
- IPv6 addresses are assigned to interfaces, not nodes.
- Multiple IP addresses may be assigned to a single interface
- All interfaces are required to have at least one link-local unicast address
- Three types of address
  - Unicast
    - Single interface
  - Anycast
    - Set of interfaces (typically different nodes)
    - Delivered to any one interface
    - the “nearest”
  - Multicast
    - Set of interfaces, single sender, multiple receivers
    - Delivered to all interfaces identified
IPV6 PREFIXES

- Also called subnet mask or subnet prefix
- Same concept as IPv4 CIDR
- IPv6 uses /nn after the address to indicate the number of bits in the prefix
  - nn is left aligned with address
  - Ones in nn bits indicate network
  - Zeros indicate host
## ADDRESS TYPE IDENTIFICATION

The type of an IPv6 address is identified by the high-order bits of the address, as follows:

<table>
<thead>
<tr>
<th>Address type</th>
<th>Binary prefix</th>
<th>IPv6 notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecified</td>
<td>00...0 (128 bits)</td>
<td>::/128</td>
</tr>
<tr>
<td>Loopback</td>
<td>00...1 (128 bits)</td>
<td>::1/128</td>
</tr>
<tr>
<td>Multicast</td>
<td>11111111</td>
<td>FF00::/8</td>
</tr>
<tr>
<td>Link-local unicast</td>
<td>1111111010</td>
<td>FE80::/10</td>
</tr>
<tr>
<td>Site-local unicast</td>
<td>1111111011</td>
<td>FEC0::/10</td>
</tr>
<tr>
<td>Global unicast</td>
<td>(everything else)</td>
<td></td>
</tr>
<tr>
<td>Anycast addresses</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Anycast addresses are not syntactically distinguishable from unicast addresses.

*Site local addresses deprecated by IETF*
UNICAST ADDRESSES

- At a minimum unicast addresses have no internal structure

- A host may be aware of subnet prefix(es) for its link(s) where different addresses may have different values for n:

- The general format for IPv6 global unicast addresses is:

- Interfaces are usually assigned 64 bits
The Link-Local is for use on a single link

Link-Local addresses are used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

Routers must not forward any packets with link-local source or destination addresses to other links.
GLOBAL UNICAST ADDRESSES

- The global routing prefix is a (typically hierarchically-structured) value assigned to a site (a cluster of subnets/links).
- The subnet ID is an identifier of a link within the site.
- Interface ID
  - All global unicast addresses other than those that start with binary 000 have a 64-bit interface ID field (i.e., n + m = 64),
  - Global unicast addresses that start with binary 000 have no such constraint on the size or structure of the interface ID field.
The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure.

"IPv4-mapped IPv6 address" represents the addresses of IPv4 nodes as IPv6 addresses.
ANYCAST ADDRESS

- Address assigned to more than one interface
- Same format as unicast address and comes from the same address space
- Anycast syntax not distinguishable from unicast addresses
- Anycast packets are delivered to the nearest interface
- Anycast packets may not be the source address of an IPv6 packet
MULTICAST ADDRESSES

Identifies a group of interfaces
Usually belonging to more than one node
Interfaces may join more than one group
Replaces broadcasts
May not ever be used as a source address

Flag bits: 0 R P T

T = 0 permanent addresses (managed by IANA)
T = 1 transient multicast addresses

P = 1 derived from unicast prefix (RFC3306)
R = 1 embedded RP addresses (I-D)

Scope
0 : Reserved
1 : Interface-local
2 : Link-local
3 : Subnet-local
4 : Admin-local
5 : Site-local
8 : Organization-local
E : Global
F : Reserved
**INTERFACE IDENTIFIERS**

- An interface identifier (IID) specifies the interface’s local logical address.
- Invert the global/local bit to form manually assigned addresses with only leading zeros.
- 48-bit MAC address is turned into 64 bits by a filler field inserted in the middle.
- This enlarged Interface ID will allow newer technologies to have unique interface identifiers assigned to them from a global address space.
- The use of a media-level address for a network-level Interface ID allows the IPv6 Stateless Address Autoconfiguration Protocol to work.
STATELESS ADDRESS AUTOCONFIGURATION

- The Media Access Control (MAC) address is used to form the host’s interface ID. For example, if a host has an Ethernet interface that it is trying to configure for use with IPv6, the 48-bit Ethernet MAC address is formed into a 64-bit interface ID, which is the right-most 64 bits of the IPv6 address. RFC 3041

- Then, using the Neighbor Discovery (ND) protocol, RFC 2461, this formed interface ID is checked to see that it does not have a duplicate on this subnet. If it does, a randomly generated token may be used (though a rare occurrence, it is a necessary protection against illegal Ethernet address usage and situations where the same address may be used on multiple interfaces for legitimate reasons).

- At this point, a ND Router Solicitation multicast message is sent out to discover if there is a local IPv6 capable router, what the local site’s topology ID for the host’s subnet is, and what the site’s public topology routing prefix is.

- Neighbor Discovery may also be used to control whether the site then wishes to continue with further configuration using Stateful Autoconfiguration with DHCPv6.

- IPv6 Autoconfiguration (RFC 2462) provides for standalone operation of two or more hosts on a local LAN link with no router present, provides for operation within a site with no outside Internet connectivity present, and allows a site’s public topology routing prefix to change, either when external connectivity comes on line, or when the external connectivity is changed, such as when a different ISP is chosen.
IPV6 NEIGHBOR DISCOVERY

- Router Advertisement Message
- Provides prefix to link-local nodes for autoconfiguration
- Prefixes have associated valid and preferred lifetimes
- Includes “router lifetime” to specify default route
- May include “uses stateful configuration process” flag
ROUTER RENUMBERING PROTOCOL

- Because IPv6 addressing is based on the PRT prefix assigned by its ISP, it is essential that it be easy for a site to renumber itself when its choice of ISP changes. To aid in this, a new Router Renumbering (RR) protocol, in conjunction with Autoconfiguration, Neighbor Discovery and the new Aggregatable Unicast addressing PRT prefix are used.

- RR allows a site’s network administrator to set new PRT prefixes into the site’s routers, as well as lower the lifetime of existing ISP PRT prefixes to specify an overlap interval, after which the old ISP’s service is discontinued.

- Hosts learn their new routing prefixes either when they restart, and thus are automatically configured with Autoconfiguration, or when they are informed by their local router that a new prefix is to be used during periodic router notification updates using ND.

- For example, a new ISP service is readied for service while the old ISP is notified that it will provide service for just 60 more days. After the new PRT prefix is announced to the site’s routers by RR, hosts will use the new prefix (that is, new ISP) for all new connections, while existing connections continue to work until the old prefix is withdrawn (that is, after 60 days in this example).

- The easy renumbering of an IPv6 site will make easy a task that is currently very painful for an IPv4 site because hosts are often manually configured in many networks.
IP EXTENSION HEADERS

Each extension header is an integral multiple of 8 octets.

- IPv6 Mandatory Header
- Processed by every router
- Processed by routers listed in Routing extension
- List of routers to cross
- Processed by the destination
- After reassembling the packet
- Cipher the content of the remaining information
- Processed only by the destination
IPV6 EXTENSION HEADERS

(a) Hop-by-hop options header; destination options header

(b) Fragment header

(c) Generic routing header

(d) Type 0 routing header
## IPV6 NEXT HEADER FIELD VALUES

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Hop x hop option header following</td>
<td>50</td>
<td>Encrypted security payload</td>
</tr>
<tr>
<td>1</td>
<td>ICMPv4   IPv4 support</td>
<td>51</td>
<td>Authentication header</td>
</tr>
<tr>
<td>2</td>
<td>IGMPv4   IPv4 support</td>
<td>58</td>
<td>ICMPv6</td>
</tr>
<tr>
<td>4</td>
<td>IP in IP encapsulation</td>
<td>59</td>
<td>No next header</td>
</tr>
<tr>
<td>6</td>
<td>TCP</td>
<td>60</td>
<td>Destination options</td>
</tr>
<tr>
<td>8</td>
<td>EGP</td>
<td>88</td>
<td>EIGRP</td>
</tr>
<tr>
<td>9</td>
<td>IGP</td>
<td>89</td>
<td>OSPF</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
<td>108</td>
<td>IP payload compression</td>
</tr>
<tr>
<td>41</td>
<td>IPv6</td>
<td>115</td>
<td>Layer 2 tunneling (L2TP)</td>
</tr>
<tr>
<td>43</td>
<td>Routing header</td>
<td>132</td>
<td>Stream control transmission</td>
</tr>
<tr>
<td>44</td>
<td>Fragmentation header</td>
<td>134-254</td>
<td>unassigned</td>
</tr>
<tr>
<td>45</td>
<td>Interdomain routing protocol</td>
<td>255</td>
<td>reserved</td>
</tr>
<tr>
<td>46</td>
<td>RSVP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HOP-BY-HOP OPTIONS HEADER

It carries optional information that must be examined by every node along the path of the packet. If a Hop-by-Hop Extension header is absent, a router knows that it does not need to process router-specific information and can route the packet immediately to the final destination. If a Hop-by-Hop Extension header is present, the router only needs to examine this header and not look further into the packet.

RFC2460

Options Type Field

- Value 00: skip and continue processing.
- Value 01: discard the packet.
- Value 10: discard the packet and send ICMP Parameter Problem, Code 2 message to the packet’s source address, pointing to the unrecognized option type.
- Value 11: discard the packet and send ICMP Parameter Problem, Code 2 message to the packet’s source address only if the destination is not a multicast address.

The third bit of the Options Type field specifies whether the option information can change en route (value 01) or does not change en route (value 00).
ROUTING HEADER

- **Next Header (1 byte)**
- **Header Extension Length (1 byte)**
- **Routing Type (1 byte)**
- **Segments Left (1 byte)**
- **Type Specific Data (Variable)**

- **Identifies type of following header.**
- **Length of routing header in units of 8 bytes, not including the first 8 bytes.**
- **Identifies type of routing header. Currently type zero defined.**
- **Number of listed nodes until final destination.**
- **Depends on routing type. For type zero:**
  - **Reserved (4 bytes)**
  - **Address 1 (16 bytes)**
  - **Address 2 (16 bytes)**
  - **Address X (16 bytes)**
ROUTING HEADER FIELDS

- **Next Header (1 byte)**
  - identifies the type of header that follows the Routing header

- **Header Extension Length (1 byte)**
  - This field identifies the length of the Routing header in 8-byte units. The length calculation does not include the first 8 bytes.

- **Routing Type (1 byte)**
  - This field identifies the type of Routing header. RFC 2460 describes Routing Type zero. The first node that processes the Routing header is the node addressed by the Destination address field in the IPv6 header. This node decrements the Segments Left field by one and inserts the next address field from within the Routing header in the IPv6 header Destination address field.
  - Then the packet is forwarded to the next hop that will again process the Routing header as described until the final destination is reached.
  - The final destination is the last address in the Routing Header Data field.

- **Segments Left (1 byte)**
  - This field identifies how many nodes are left to be visited before the packet reaches its final destination.

- **Type-Specific Data (Variable-length)**
  - The length of this field depends on the Routing Type. The length must be a multiple of 8 bytes.
IPv6 uses Path MTU discovery to determine the maximum packet size that can be used on the path to that destination. If the packet to be sent is larger than the supported MTU, the source host fragments the packet. Unlike IPv4, with IPv6, a packet does not get fragmented by a router along the path. Fragmentation only occurs on the source host sending the packet. The destination host handles reassembly.
A Destination Options header carries optional information that is examined by the destination node only.

The Next Header value identifying this type of header is the value 60.

The Options field is used in the same way as the Hop-by-Hop Options header.
IPV6 EXTENSION HEADERS

- ICMPv6 (58) (RFC2463)
  - Nodes use ICMPv6 to report errors encountered in processing packets
    - Neighbor Discovery uses ICMPv6 extension header
    - Neighbor Solicitation / Neighbor Advertisement
    - Router Solicitation / Router Advertisement
    - Redirect
  - Integral component of IPv6
  - Each node MUST fully implement ICMPv6
ICMPv6 MESSAGES

- **Type 1: Destination Unreachable**
  - Code 0: no route to destination
  - Code 1: communication administratively prohibited
  - Code 2: not assigned
  - Code 3: address unreachable
  - Code 4: Port unreachable

- **Type 2: Packet too big**
  - Message contains MTU

- **Type 3: Time exceeded**
  - Code 0: hop limit exceeded
  - Code 1: fragment reassembly timeout
ICMPv6 MESSAGES

- Type 4: Parameter problem
  - Code 0: erroneous header field
  - Code 1: unrecognized “Next Header” type
  - Code 2: unrecognized IPv6 option
  - Pointer – identifies the octet offset within the invoking packet where the error was detected

- Type 128: Echo request
  - Message contains identifier and sequence numbers

- Type 129: Echo reply
  - Message contains identifier and sequence numbers
IPV6 EXTENSION HEADERS

- Encapsulating Security Payload (50) (RFC2406)
  - Provides encryption security
  - Confidentiality
  - Data origin authentication
  - Connectionless integrity

- Authentication Options (51) (RFC2402)
  - Provides connectionless integrity
  - Data origin authentication
HOW MUCH

- Difficult to pin down costs
  - Code
  - Cost of conversion
  - Managing and Maintaining
  - Security
IOT PROTOCOL RECOMMENDATION

- What do things need? IPv4 or IPv6?
  - no point waiting for a ubiquitous IPv6 substrate to support things
  - no point deploying things equipped only with IPv4
- Regardless of protocol, all devices need a way to phone “Home” reliably and trusted
  - “Home” should be able to upgrade the device fully unattended or be able to close it down into a safe state.
  - Assume it will receive hostile or malicious traffic, and be able to distinguish between friend and foe.
  - Only respond to transactions that can be authenticated, and respond in ways that cannot be perverted or warped into an attack vector on others.
- Things need to sense and adapt to their environment and fulfil their intended function using any available means
- The most pragmatic answer to the question of what IP protocol to load into a thing is: both!
  - Use a Dual Stack Approach
<table>
<thead>
<tr>
<th>Reference</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF RFCs</td>
<td><a href="http://www.rfc-editor.org">http://www.rfc-editor.org</a></td>
</tr>
<tr>
<td>NIST</td>
<td><a href="https://www.nist.gov/">https://www.nist.gov/</a></td>
</tr>
<tr>
<td>NANOG</td>
<td><a href="https://www.nanog.org/">https://www.nanog.org/</a></td>
</tr>
<tr>
<td>Internet Protocol Journal</td>
<td>ipj.dreamhosters.com/</td>
</tr>
<tr>
<td>IP Address Registries</td>
<td></td>
</tr>
<tr>
<td>ARIN</td>
<td><a href="https://www.arin.net">https://www.arin.net</a></td>
</tr>
<tr>
<td>RIPE NCC</td>
<td><a href="https://www.ripe.net/">https://www.ripe.net/</a></td>
</tr>
<tr>
<td>APNIC</td>
<td><a href="https://www.apnic.net/">https://www.apnic.net/</a></td>
</tr>
<tr>
<td>LACNIC</td>
<td><a href="http://www.lacnic.net/">www.lacnic.net/</a></td>
</tr>
<tr>
<td>AFRINIC</td>
<td><a href="http://www.afrinic.net/">www.afrinic.net/</a></td>
</tr>
<tr>
<td>Internet Assigned Numbers Authority (IANA)</td>
<td><a href="http://www.iana.org">www.iana.org</a></td>
</tr>
<tr>
<td>IPv6 &amp; IoT by Geoff Huston</td>
<td><a href="https://blog.apnic.net/2016/04/13/ipv6-internet-things/">https://blog.apnic.net/2016/04/13/ipv6-internet-things/</a></td>
</tr>
</tbody>
</table>