Internet Layer

Josh Wilcox (jw14g24@soton.ac.uk)

February 4, 2025

Contents

1 Internet Layer

- The internet layer is the layer above the Link layer in TCP/IP
- Sends packets via the link layer
- Passes a received packet's payload to the (correct) transport layer
- Provides *unique addressing*
- Handles *next-hop routing*
- Hides the complexity of the physical network

1.1 Functions

- Internetworking
  - Hides routing from the transport layer
- Transmitted packets
  - Packets data into *datagrams*
  - Processes and Routes these datagrams
  - Executes fragmentation
- Receiving Packets
  - Handles error checking
  - Fragment reassembly

1.2 Internet Protocol Properties

- Connectionless
  - Packet is sent into the network and is seemlessly switched to where it needs to go
- Somewhat *unreliable*
  - No guarantee given datagrams will arrive at all or in the right order
  - Packets are sent and routed on a *best effort* basis
- Routed
  - Usually destination routed
  - Routers have routing tables to facilitate routing

1.3 Unreliabaility

- Routers act on a best effort basis
- IP packets may get dropped or delays
  - Could be due to congestion control
- Quality of Service methods can help
  - Prioritizes certain traffic
  - If a big campus network, quality of service could prioritize things like video calls, and things like video streaming could be unPrioritized

2 IPv4

2.1 Fragmentation

- Physical connections have a **Maximum Transmission Unit**
  - Ethernet typically has a 1,500 byte MTU

  y
- If data units are larger than the MTU, they are split into multiple smaller packets to be sent and *reassembled*

2.2 RFC 791

- 32-Bit Addresses
- The physical structure of an IPv4 Address
- Written as 'dotted quads'
- Variable sized header with a minimum of 20-bytes

2.2.1 Header Structure

Octet	0								1								2								3							
\Bit Byte Offset\	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
0	Version				IHL				DSCP						ECN		Total Length															
4	Identification																Flags			Fragment Offset												
8	Time To Live								Protocol								Header Checksum															
12	Source IP Address																															
16	Destination IP Address																															
20	Options (optional, if IHL > 5)																															

3 IPv6

3.1 RFC 2460, 8200

- 128-bit addresses
- Written as 'colon-hex'
- You can replace single sets of repeated 0 blocks with "::"
- You can also omit leading 0s within each block:
  - `2001:0630:00d0:f500:0000:0000:0000:0064` → `2001:630:d0:f500::64`

3.1.1 Header Structure

Octet												1								2								3				
\Bit Offset\	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
0	Version				Traffic Class								Flow Label																			
4	Payload Length																Next Header								Hop Limit							
8, 12, 16, 20	Souce IP Address																															
24, 28, 32, 36	Destination IP Address																															

3.2 Address Scopes

- **Link-Local Address**
  - Every IPv6 device has a link-local address for each network adapter.
  - These addresses are used for communication within the same local network and are never routed to other networks.
  - They are useful for local service discovery and communication between devices on the same network.
- **Global Unicast Address**
  - These are unique addresses assigned to devices for communication over the internet.
  - A device can have multiple global unicast addresses.
- **Unique Local Address (ULA)**
  - These addresses are similar to private IPv4 addresses and are used for local communication within a site or organization.
  - They are not routable on the global internet.
- **Multicast Address**
  - These addresses are used to send a single packet to multiple destinations.
  - IPv6 devices listen for specific multicast addresses to receive certain types of network traffic.

3.3 Main Benefits of IPv6

- Remove the needs for **Network Address Translation**
  - NAT is Bad in a lot of ways
- Restores end-to-end psychology of the internet
- More plug-and-play than IPv4
- Much more streamlined header
- Fragmentation only occurs at sender

3.4 Barriers to IPv6 Deployment

- Time and Money
- Hardware support
- Have to learn something new

3.4.1 Address Accountability

- Tracking who's got what address can be harder because people can choose their own addresses
-

4 Comparison: IPv4 vs IPv6

Feature	**IPv4**	**IPv6**
Addressing	32-bit addressing	128-bit addressing
Header	20-byte, 13-field header	40-byte, 8-field header
Host Addresses	Hosts usually have one address per adapter	Hosts typically have multiple addresses
Routing	Fragmented routing	Simplified routing
NAT Usage	Prolific use of NAT	End-to-end paradigm restored
Global Adoption	99%+ global adoption	45% global adoption

Table 1: Comparison of IPv4 and IPv6

5 Netmasks

- Determines what is local to you and what isn't
- Specifies how many bits identify the network prefix
- Always all of the first n bits are common - can't just have a random outlier

5.1 Subnets

- Networks are made up of lots of subnetworks
- Limits the propogation of Ethernet broadcast traffic limits
- Logically divides the network
  - Campus would typically have a subnet on a per-building or per-department basis
- Size of a subnet should be based on the number of devices that would use them

6 Routing

- Describes how packets move between subnets
- Occurs on *change of IP address space*
- Each host has a *routing table*

6.1 Netmasks

- Specify how many bits identify the network prefix
- 153.242.152.0/x
- The first x bits are common and identify the network
- Addresses outside this address space need to go through a router
  - Devices in the same netmask group can talk directly to each other and will never need to go through a router

7 ICMP

- Internet Control Message Protocol
- Encapsulated in a standard IP packet
  - Essentially part of IP
- Usually used for information and error messages in IPv4
- In IPv6, it is used for *router advertisement* and *neighbour discovery*

8 Multicast

- On-to-many communications
- Broadcasts packets to many hosts - **but only to hosts that are interested**
- Done through *multicast groups*

8.1 Uses

- Local service discovery
  - Allows name resolution in a local network through Multicast DNS
- One-to-many multimedia (such as live-streaming)
- Used for router advertisement, neighbour discovery, and duplicate address detection
  - IPv6 needs multicast to work in order for it to function

9 Address Resolution Protocol - ARP

- Technically a link layer thing - but is heavily related to IP addresses
- Within a subnet, it maps an IPv4 address to the MAC address on a particular device
- The host looking for a MAC address *broadcasts* an ARP "who has" request
  - The device with the matching IP address responds with its MAC address

10 DHCP (IPv4)

- Dynamic Host Configuration Protocol automates the process of configuring IP addresses and other network settings on devices within a subnet.
  - When a host connects to a network, it broadcasts a **DHCP Discover** message to locate available DHCP servers.
  - A DHCP server responds with a **DHCP Offer** message, providing an available IP address and other configuration details.
  - The client then sends a **DHCP Request** message to the server, indicating its acceptance of the offered IP address.
  - Finally, the server sends a **DHCP Acknowledgment (DHCP ACK)** message, confirming the lease of the IP address and providing additional configuration information such as the lease duration, subnet mask, default gateway, and DNS servers.
- DHCP simplifies network administration by dynamically assigning IP addresses, reducing the need for manual configuration.
- DHCP leases can be renewed or released by the client, allowing efficient reuse of IP addresses within the network.
- DHCP also supports options for providing additional configuration parameters, such as NTP servers, domain names, and more.

11 Neighbour Discovery Protocol (NDP)

Neighbour Discovery Protocol (NDP) is a crucial protocol in IPv6 that is responsible for various functions related to the interaction between IPv6 nodes on the same link. It replaces several IPv4 protocols, including ARP (Address Resolution Protocol), ICMP Router Discovery, and ICMP Redirect. Here are the key components and functions of NDP:

- **Address Resolution:** NDP is used for mapping IP addresses on the local subnet to MAC addresses, similar to how ARP works in IPv4. This is essential for devices to communicate within the same local network.
- **Router Discovery:** NDP allows hosts to discover the presence of routers on the local link. Routers periodically send out **Router Advertisements (RA)** to announce their presence and provide information such as the network prefix and default gateway.
- **Prefix Discovery:** Hosts use NDP to discover the network prefixes that are available on the local link. This information is included in the Router Advertisements.

NDP uses ICMPv6 (Internet Control Message Protocol for IPv6) messages for its operations. The key ICMPv6 messages used by NDP include:

- **Neighbour Solicitation (NS):** Sent by a node to determine the link-layer address of a neighbour or to verify the reachability of a neighbour.
- **Neighbour Advertisement (NA):** Sent in response to a Neighbour Solicitation message or to announce a change in the link-layer address.
- **Router Solicitation (RS):** Sent by a host to request Router Advertisements from routers on the local link.
- **Router Advertisement (RA):** Sent by routers to announce their presence and provide network information to hosts.
- **Redirect Message:** Sent by routers to inform hosts of a better next-hop address for a destination.

NDP relies heavily on multicast addresses for its operations:

- **Solicited-Node Multicast Address:** Used for Neighbour Solicitation messages. This address is derived from the target IPv6 address and ensures that only the relevant node processes the solicitation.
- **All-Nodes Multicast Address:** Used for Router Advertisements and other messages that need to be received by all nodes on the link.

Understanding NDP is essential for managing and troubleshooting IPv6 networks, as it plays a critical role in the basic operation and configuration of IPv6 devices.

12 Router Advertisments

- When a host connects to an IPv6 network, it sits and listens for router advertisments - or does a solicitation for a router
- If it solicits, a router advertisement will be generated
- These advertisements are multicast - all hosts will see them
- In a typical network, these carry the IPv6 network prefix (/64) to use
- The Router Advertisements's source address implies the default router address - will not generally be in the same subnet
  - Link local address of router knows how to deal with this
- Flags indicate how addresses are allocated
- DNS server information can be included in the advertisement

13 SLAAC - Stateless Address Autoconfigurations

- Allows a host to autoconfigure basic network settings without a DHCPv6 server.
- The Router Advertisement specifies whether SLAAC should be used or not
- The host using SLAAC builds its address from:

13.1 RFC4862 Method

- Host part of the address is based on the host's MAC address
- Suppose a host has a MAC address of `00:1A:2B:3C:4D:5E`.
- The MAC address is split into two 24-bit halves: `00:1A:2B` and `3C:4D:5E`.
- The 7th bit of the first byte is inverted to form the modified EUI-64 identifier: `02:1A:2B:FF:FE:3C:4D:5E`.
- The host part of the IPv6 address is then `021A:2BFF:FE3C:4D5E`.
- For network prefix `2001:0db8:85a3::/64`, the resulting address is `2001:0db8:85a3:021A:2BFF:FE3C:4D5E`.

13.2 RFC7217 Method

- Embedding the MAC address in a global address is a privacy nightmare
  - You could track a host across subnets, ISPs, etc etc.
- However, there is a need for a stable IPv6 Address for each subet
- RFC7217 uses a pseudo-random function that takes multiple physical characteristics are arguments and a secret key.
  - The result is a unique but stable address for each subnet that does not embed the MAC address

14 DHCPv6

- Required Router Advertisements
- Uses DHCP Unique Identifier to devices instead of a MAC Address
- Can have SLAAC and DHCPv6 Addresses at the same time
- Can be used *just* to give extra information