**CSCI 367 - Computer Networks I**

IP – Internet Protocol (Layer 3/Network Layer)

References:

<http://www.cs.newpaltz.edu/~easwaran/CCN/Week10/IPHeader.pdf>

<https://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm>

<https://en.wikipedia.org/wiki/IPv4>

1. The Internet Protocol (IP) is the most common Layer-3 Network protocol.
2. An IP packet is often termed a datagram.
3. An IP packet is encapsulated in an Ethernet frame’s payload section.
4. An IP packet consists of a header section and a payload section.

Table

Description automatically generated

1. The following are the various components/fields of IP packet header:

* **Version:** The first IP header field is a 4-bit version indicator. In IPv4, the value of its four bits is set to 0100, which indicates 4 in binary. However, if the router does not support the specified version, this packet will be dropped.
* **Internet Header Length:** Internet header length, shortly known as IHL, is 4 bits in size. It is also called HELEN (Header Length). This IP component is used to show how many 32-bit words are present in the header.
* **Type of Service:** Type of Service is also called Differentiated Services Code Point or DSCP. This field is provided features related to the quality of service for data streaming or VoIP calls. The first 3 bits are the priority bits. It is also used for specifying how you can handle Datagram.
* **Total length:** The total length is measured in bytes. The minimum size of an IP datagram is 20 bytes and the maximum, it can be 65535 bytes . HELEN and Total length can be used to calculate the dimension of the payload.All hosts are required to be able to read 576-byte datagrams. However, if a datagram is too large for the hosts in the network, the fragmentation method is widely used.
* **Identification:** Identification is a packet that is used to identify fragments of an IP datagram uniquely. Some have recommended using this field for other things like adding information for packet tracing, etc.
* **IP Flags:** Flag is a three-bit field that helps you to control and identify fragments. The following can be their possible configuration:

Bit 0: is reserved and has to be set to zero

Bit 1: means do not fragment

Bit 2: means more fragments.

* **Fragment Offset:** Fragment Offset represents the number of Data Bytes ahead of the particular fragment in the specific Datagram. It is specified in terms of the number of 8 bytes, which has a maximum value of 65,528 bytes.
* **Time to live:** It is an 8-bit field that indicates the maximum time the Datagram will be live in the internet system. The time duration is measured in seconds, and when the value of TTL is zero, the Datagram will be erased. Every time a datagram is processed its TTL value is decreased by one second. TTL are used so that datagrams are not delivered and discarded automatically. The value of TTL can be 0 to 255.
* **Protocol:** This IPv4 header is reserved to denote that internet protocol is used in the latter portion of the Datagram. For Example, 6 number digit is mostly used to indicate TCP, and 17 is used to denote the UDP protocol.
* **Header Checksum:** The next component is a 16 bits header checksum field, which is used to check the header for any errors. The IP header is compared to the value of its checksum. When the header checksum is not matching, then the packet will be discarded.
* **Source Address:** The source address is a 32-bit address of the source used for the IPv4 packet.
* **Destination address:** The destination address is also 32 bit in size stores the address of the receiver.
* **IP Options:** It is an optional field of IPv4 header used when the value of IHL (Internet Header Length) is set to greater than 5. It contains values and settings related with security, record route and time stamp, etc. You can see that list of options component ends with an End of Options or EOL in most cases.
* **Data:** This field stores the data from the protocol layer, which has handed over the data to the IP layer.

1. If the destination IP address is on a separate network, routers route (forward) the packet to the destination computer.
2. An IP address consists of a dotted decimal value, such as 216.155.1.41.
3. Every device connected to a network has an IP address.
4. The length of a Layer-3 Network IP header is a minimum of 20 bytes.
5. The length of a Layer-3 Network IP packet is limited by the maximum value of the 16-bit Total Length field in the IP header. For IPv4, this results in a maximum payload size of 65515 (= (2^16-1) - 20 bytes minimum header length).
6. Because IPv6 has a 40-byte header, it allows for payloads up to 65495.
7. Using the Jumbo Payload header extension, IPv6 could allow packets up to 4 GB.
8. A MAC address is a physical address that’s burned-in to every NIC. Every computer or device that’s connected to a network must have a NIC, and every NIC has a MAC address. On the other hand, an IP address is a logical address. The IP address of a device attached to a network doesn’t have to be permanent. It can change, and often does, over time.
9. A network usually consists of multiple network segments, often referred to as Local Area Networks (LANs). Two networks are connected by a device called a router. If two communicating devices are on the same network, then the MAC addresses of the communicating devices are all that’s needed to send and receive packets. On the other hand, if the two communicating devices are on separate networks, the router uses the IP address of the destination device to forward the packet to the destination network. Once the packet is forwarded to the destination network, the router forwards the packet to the destination device using the destination device’s MAC address.
10. Rather than using an IP address to locate a remote computer, a uniform resource locator (URL), such as www.google.com, can be used instead. If a URL is used instead of the device’s IP address, a domain name server (DNS) computer located on each network is used to lookup the IP address associated with the URL. Once the IP address is obtained, the packet is sent to the appropriate network.
11. DNS software resolves/maps a URL to its associated IP address. To resolve a URL to its associated IP address, the DNS application maintains a file that contains records. Each record consists of two fields that are key/value pairs: The key field is the URL, and the value field is the associated IP address. The DNS software uses this file when resolving URLs.

**Computer Networks**

Router



2A-B3-54-EF-4B-5C



Networks

2A-B3-54-EF-4B-5D

2A-B3-54-EF-4B-5E

AA-2D-FA-EF-4B-E1

AA-2D-FA-EF-4B-E2

AA-2D-FA-EF-4B-E3

216.155.1.41

216.155.1.42

164.67.235.91

164.67.235.92

164.67.235.93

216.155.1.43

Switch

Switch

B1-1B-54-E2-45-22

B1-1B-54-E2-45-23

216.155.1.1

164.67.235.1