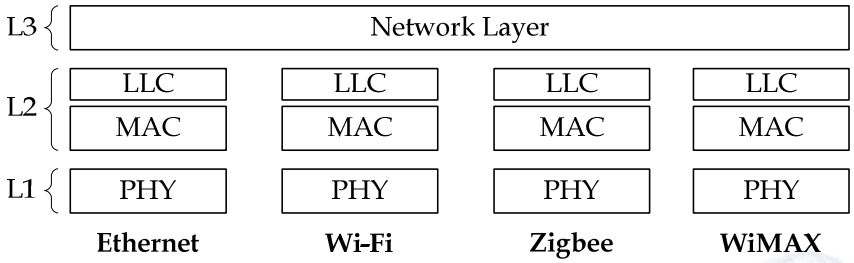
Lecture 11: Internetworking and the Internet Protocol (IP)

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

Network vs. Internetwork

- Interconnected hosts running the same data link layer protocol represent one *physical network*.
- A physical network is usually controlled by a single administrative entity.
- Different physical networks exist to fit different set of needs (e.g., wired vs. wireless). No single networking technology fits the needs of all users.
- An *internetwork* connects the different networks instead of being isolated islands, which allow information exchange.
- The Internet is a *global* internetwork (*not* network).

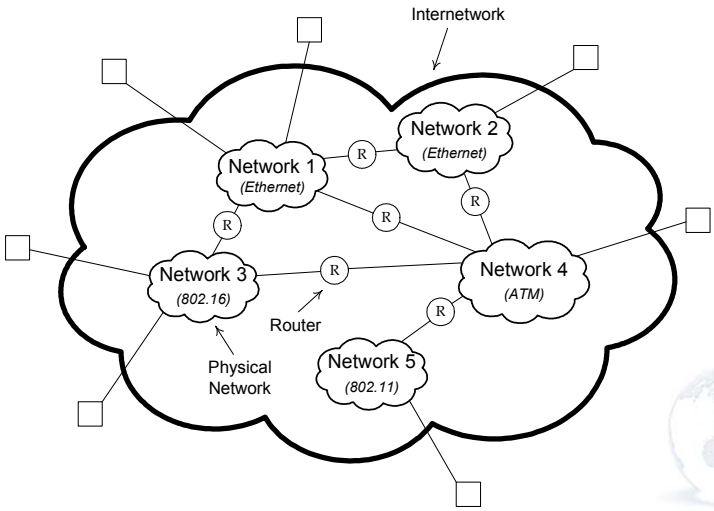
The Internetworking Concept: The Network Layer



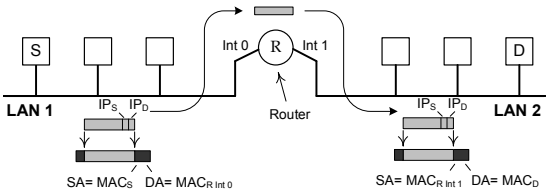
Network Layer solves 3 issues:

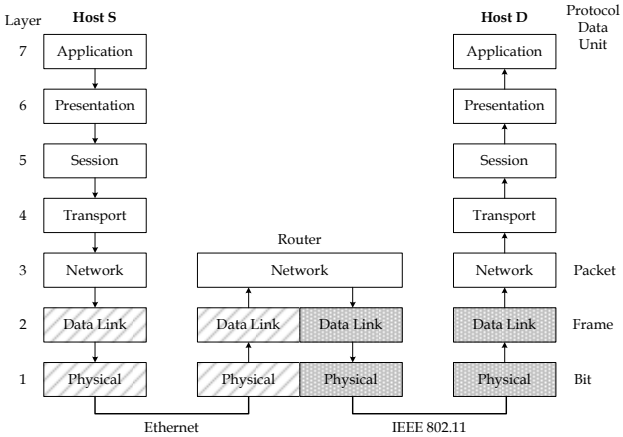
1. Provides a *homogeneous* addressing scheme that is *globally unique*: Different L2 protocols might use different sizes (number of bits) for their MAC addresses. LAA addresses might be re-used on different networks (no guarantees).
2. Provides a *uniform* packet format. Different L2 protocols might use different sizes for their frames, and might include different fields in the header depending on the protocol design.
3. Defines *end-to-end* routing across multiple physical networks (through routers): A huge self-learning table in each switch for the *whole* world is not feasible, plus flooding to all machines in the world from one PC consumes excessive resources.

Internetworking: Routers



Routers: Layer 3 Devices

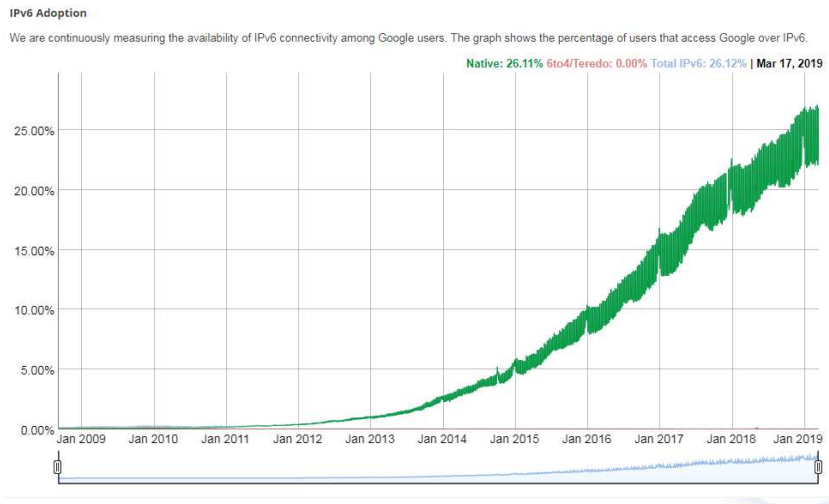




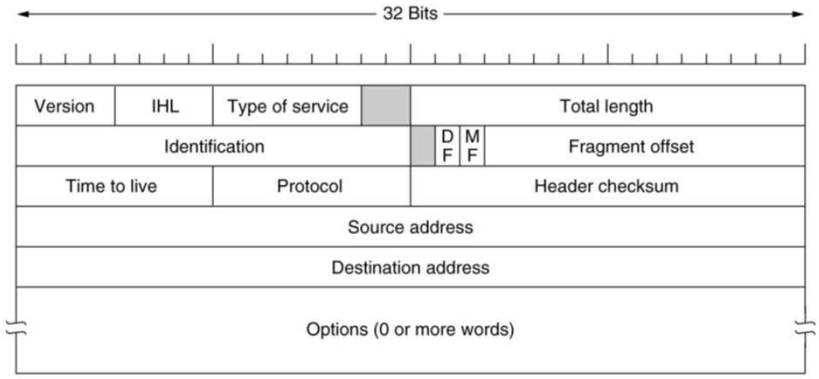
Internet Protocol (IP)

- The IP protocol is the *de facto* L3 protocol nowadays.
- IP is currently in its version 4, called IPv4, described in IETF RFC 791 (published 1981).
- The next version is 6, called IPv6.
- IPv6 was first formally described in RFC 1883 (published 1995). That RFC was obsoleted and replaced by RFC 2460 (published 1998).
- This specification was obsoleted again and replaced by RFC 8200 (July 2017).
- Deployment of IPv6 was slow, but is picking up in recent years.
- Routers forward based on IP address (e.g., 128.2.1.1) not the MAC address.

IPv6 Deployment



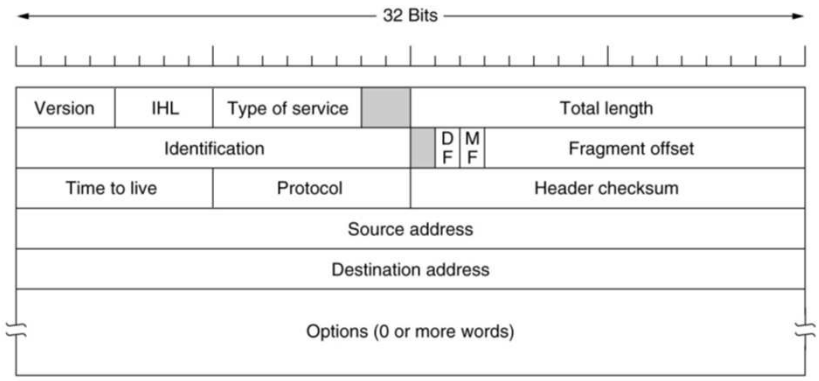
IP Packet Format



IP Packet Fields

- **Version:** A 4 bit field. The current version is 4 (0100b). The next version is 6 (0110b).
- **IP Header Length (IHL):** A 4 bit field. Specifies the length of the header, in units of 32-bit words. Used because the header length is not constant. The minimum value is 5, and the maximum value is 15, which limits the header to 60 bytes, and the Options field to 40 bytes.
- **Type of Service:** Used to distinguish quality of service desired for the packet (mainly used for the Diffserv QoS architecture). It allows the router to decide on a certain queueing priority and a discard priority for the received packet. For voice, fast delivery is preferred. For file transfer, complete transmission is more important.

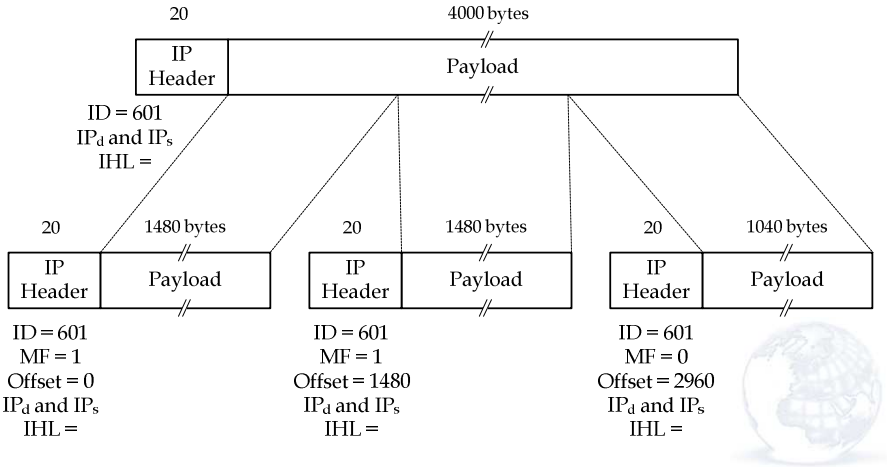
IP Packet Format



- **Total Length:** A 16-bit integer that specifies the total number of bytes in the packet (including both the header and the data). So, the maximum IP packet length is $2^{16} - 1 = 65{,}535$ bytes.
- **Identification, Flags and Fragment Offset:** used when the IP datagram is fragmented. All fragments of a single IP datagram contain the same identification.
- The MF flag stands for "More Fragments to follow". All fragments of an IP datagram except the last one have this bit set.
- The DF flag stands for "Do not Fragment". When a host does not want its IP packet to be fragmented, it sets this bit to 1.
- The Fragment Offset tells the receiver where in the current datagram the fragment belongs. All fragments in a datagram except the last one must be a multiple of 8 bytes.
- **Time to Live (TTL):** A counter used to limit packet lifetime. It is initialized to a positive integer between 1 and 255 by the sender, and is decremented by 1 for each one hop. When the counter hits zero, the router discards the IP packet and sends an ICMP packet back to the source. (*Usually*: 128 or 255).

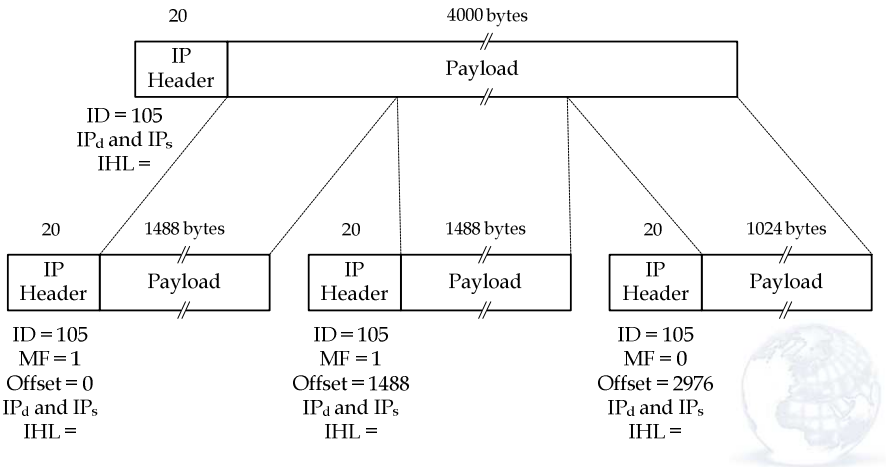
Fragmentation of an IP Packet

(MTU = 1500)



IP Fragmentation Homework

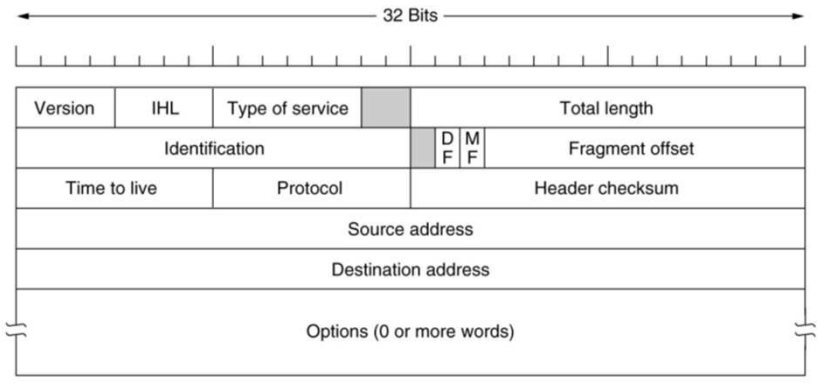
(MTU = 1510)



IP Packet Fields

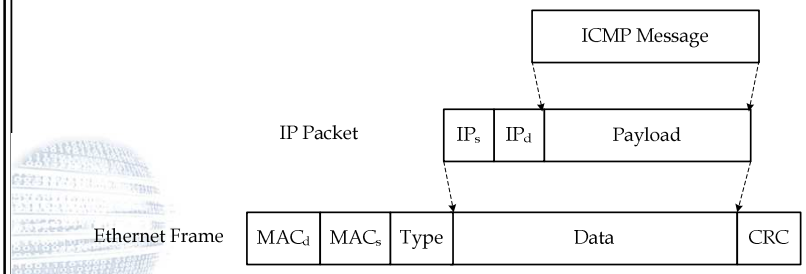
- **Protocol:** A number that tells the receiver to which Layer 4 process to deliver data. Possibilities include TCP = 6, UDP = 17, ICMP = 1, etc.
- **Header Checksum:** used to detect errors in the header only. Note that the header checksum must be recomputed at each hop because at least one field always changes (the TTL field), but special tricks can be used to speed up the computation.
- **Source Address:** the IP address of the sender (a unique 32-bit number).
- **Destination Address:** IP address of the intended recipient (a unique 32-bit number).
- **Options:** provides an escape to include information not present in the original design, to permit experimenters to try out new ideas, and to avoid allocating header bits to information that is rarely used.

IP Packet Format



Internet Control Message Protocol (ICMP)

Message Type	Description
DESTINATION UNREACHABLE	Packet could not be delivered
TIME EXCEEDED	Time To Live (TTL) filed hit 0
ECHO	Ask a machine if it is alive
ECHO REPLY	Yes, I am alive




```
Usage:  ping domain_name      or    ping IP_address

C:\>ping www.google.com

Pinging www.l.google.com [74.125.77.147] with 32 bytes of data:

Reply from 74.125.77.147: bytes=32 time=264ms TTL=237
Reply from 74.125.77.147: bytes=32 time=199ms TTL=237
Reply from 74.125.77.147: bytes=32 time=188ms TTL=237
Reply from 74.125.77.147: bytes=32 time=195ms TTL=237

Ping statistics for 74.125.77.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 188ms, Maximum = 264ms, Average = 211ms


C:\>ping www.ju.edu.jo

Pinging webserver.ju.edu.jo [172.16.0.33] with 32 bytes of data:

Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127
Reply from 172.16.0.33: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.0.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Usage: tracert domain_name or tracert IP_address

C:\>tracert fetweb.ju.edu.jo

```
Tracing route to fetweb.ju.edu.jo [10.249.103.200]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.249.103.200

Trace complete.
```

C:\>tracert www.ju.edu.jo

```
Tracing route to www.ju.edu.jo [172.16.0.116]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.249.96.10
  2  1149 ms   159 ms    21 ms  www.ju.edu.jo [172.16.0.116]

Trace complete.
```

C:\>tracert www.google.com

```
Tracing route to www.l.google.com [209.85.129.147]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  192.168.1.10
  2   619 ms   363 ms   483 ms  195.163.110.207
  3   981 ms   980 ms  1268 ms  195.163.119.5
  4   337 ms   563 ms     *     213.139.32.9
  5   534 ms   734 ms    98 ms  so-5-0-0.fra10.ip.tiscali.net [77.67.66.69]
  6   309 ms   102 ms   191 ms  xe-0-0-0.ams10.ip.tiscali.net [89.149.186.233]
  7   118 ms   264 ms   131 ms  core1.ams.net.google.com [195.69.144.247]
  8   358 ms   244 ms   105 ms  209.85.248.88
  9   126 ms   377 ms   149 ms  72.14.232.209
 10   108 ms   111 ms   112 ms  72.14.232.201
 11   275 ms   439 ms   417 ms  72.14.233.206
 12   210 ms   406 ms   112 ms  fk-in-f147.google.com [209.85.129.147]

Trace complete.
```


C:\>tracert www.microsoft.com

```
Tracing route to lb1.www.ms.akadns.net [207.46.192.254]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     1 ms  192.168.1.10
  2   483 ms   902 ms   597 ms  195.163.110.207
  3   369 ms   132 ms    92 ms  195.163.119.5
  4   813 ms   946 ms   546 ms  213.139.32.9
  5   359 ms   512 ms   138 ms  so-5-0-0.fra10.ip.tiscali.net [77.67.66.69]
  6   733 ms   450 ms   820 ms  so-2-0-0.was10.ip.tiscali.net [213.200.82.197]
  7   850 ms   602 ms  1013 ms  213.200.66.134
  8   617 ms   364 ms   480 ms  207.46.47.92
  9   405 ms   768 ms   631 ms  ge-7-1-0-0.blu-64c-1a.ntwk.msn.net [207.46.33.26]
 10   339 ms   360 ms   221 ms  ge-0-0-0-0.blu-64c-1b.ntwk.msn.net [207.46.33.178]
 11   885 ms   691 ms   519 ms  ge-7-1-0-0.wst-64cb-1b.ntwk.msn.net [207.46.34.177]
 12   763 ms   694 ms   821 ms  ge-6-1-0-0.tuk-64cb-1b.ntwk.msn.net [207.46.35.33]
 13  1115 ms   741 ms   340 ms  ten1-2.tuk-76c-1a.ntwk.msn.net [207.46.44.50]
 14   561 ms   516 ms   698 ms  po16.tuk-65ns-mcs-1b.ntwk.msn.net [207.46.35.142]
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *     po15.tuk-65ns-mcs-1a.ntwk.msn.net [207.46.35.138]  reports: Destination net unreachable.

Trace complete.
```

Homework: Firewalls

- Read the Wikipedia entry for Firewall
  - http://en.wikipedia.org/wiki/Firewall_(computing)
- A firewall is classified as which layer device (e.g., a router is a L3 device)?
- How is a firewall different than a proxy?
- How did the JU firewall affect the above ping and traceroute entries?
- Try to use ping and traceroute inside and outside the University.
- What is a Gateway? Which layer device is it?

Networking Devices

Layer	Device
Layer 7	Firewall, Proxy, Gateway
Layer 3	Router
Layer 2	Switch, Bridge
Layer 1	Hub, Repeater

