Communication Networks

Spring 2017/2018

Dr. Mohammad HAWA

By: Mohammad
Abu Hashya.

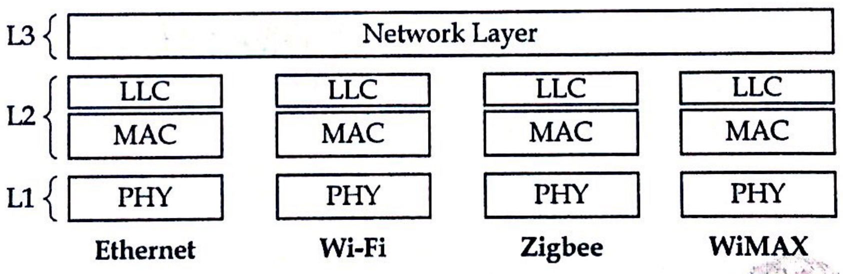
* * *

Scanned by CamScanner

Lecture 11: Internetworking and the Internet Protocol (IP)

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

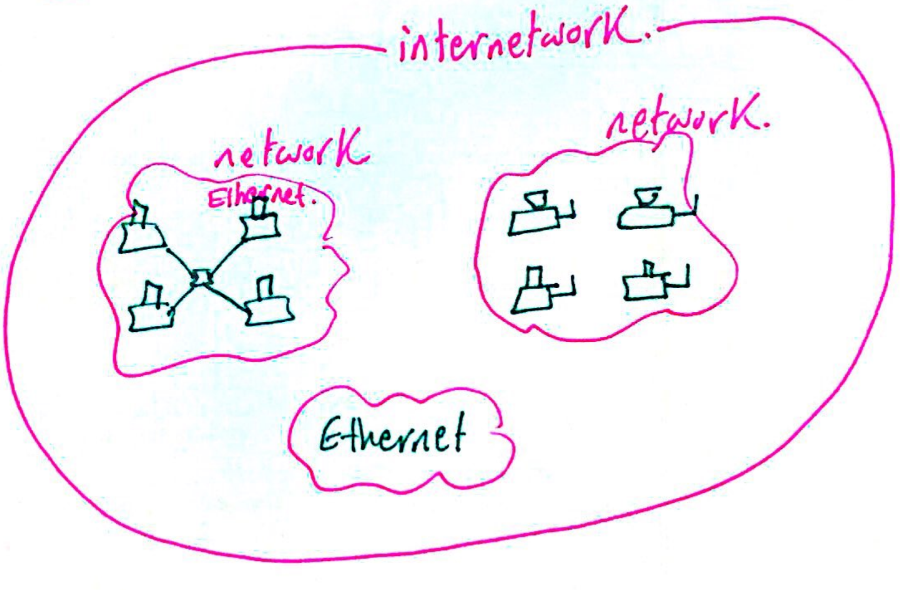
The Internetworking Concept: The Network Layer



Scanned by CamScanner

Network vs. Internetwork.

- interconnected hosts running the same data link Layer protocol represent one physical network.
- Aphysical 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 need of all users.
- An internetwork connects the different networks instead of being isolated islands, which allows info. exchange.
- The internet is a global internetwork (not network).



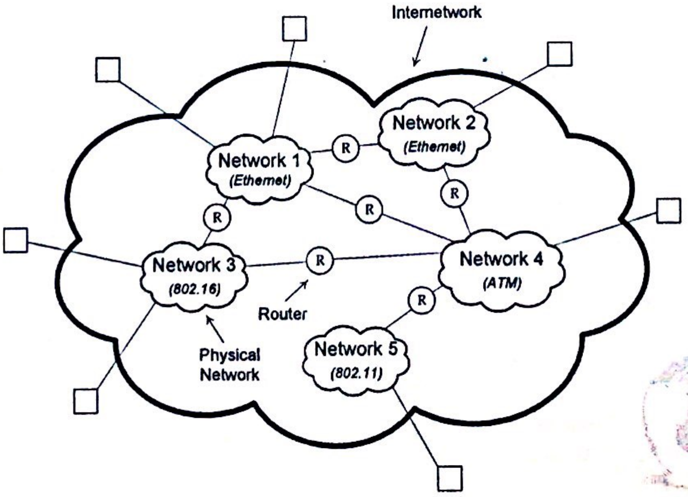
* L3 is the Common Language.

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 resoucres.

Copyright © Dr. Mohammed Hawa

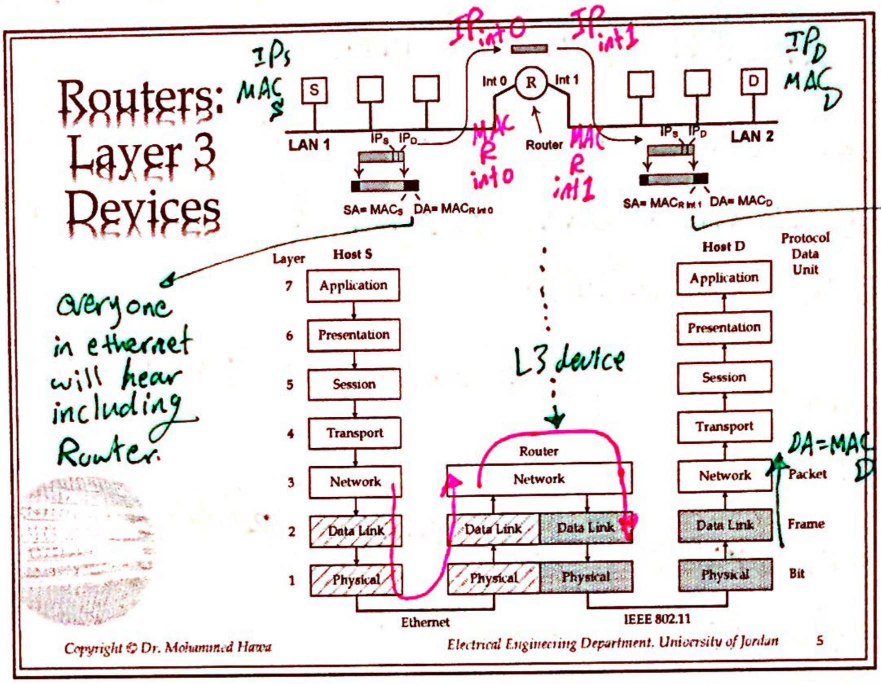
Internetworking: Routers



Copyright © Dr. Mohammed Hawa

Scanned by CamScanner

Ex. LAN1 Ethernet   LAN2 Wifi

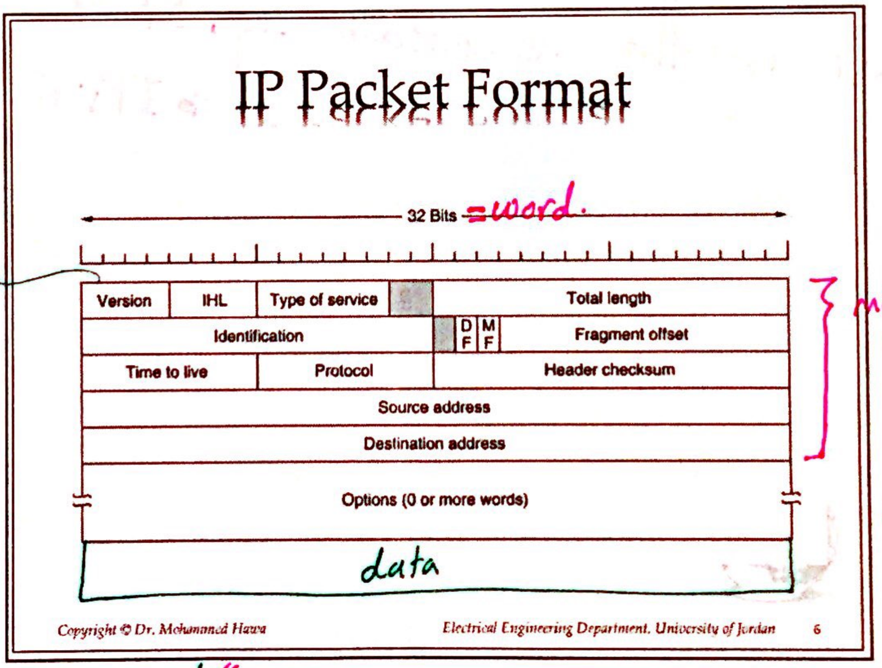


Routers: Layer 3 Devices

everyone in ethernet will hear including Router.

→ everyone will hear in Wifi including Router.

Copyright © Dr. Mohammed Hawa   *Electrical Engineering Department, University of Jordan*   5



IP Packet Format

Version	IHL	Type of service				Total length
Identification				D F	M F	Fragment offset
Time to live		Protocol				Header checksum
Source address						
Destination address						
Options (0 or more words)						
data						

memorize the length for each one.

min value is 5 word.

No trailer in the IP PKt Format.

Copyright © Dr. Mohammed Hawa   *Electrical Engineering Department, University of Jordan*   6

HW: "IP is end to end."

Scanned by CamScanner

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 RFC791 (published 1981).

- The next version is 6, called IPv6.
- This specification was obsoleted again & replaced by

⇒ RFC8200 (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.

* What is the percentage → IPv4 80%

↳ IPv6 20%

Scanned by CamScanner

max. header size 60 Bytes = 15 words.

max options size 40 Bytes = 10 words.

IP Packet Fields

- **Version:** A 4 bit field. The current version is 4 (0100b). The future 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.

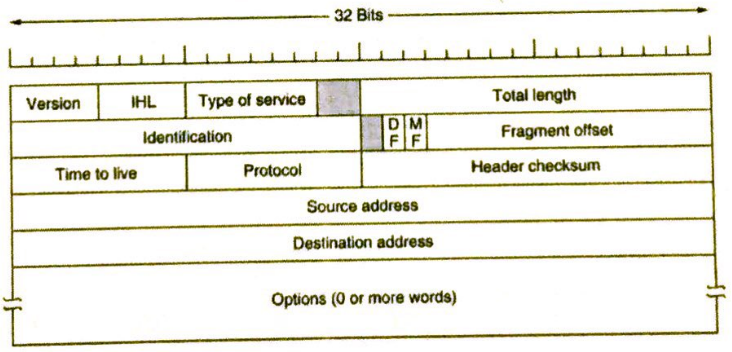
No use for version 5.

15 x 4 = 60 Bytes.

for voice, data

⇒ Voice X (Keep data).

IP Packet Format



32 Bits

Version	IHL	Type of service	▨	Total length		
Identification			▨	DF	MF	Fragment offset
Time to live	Protocol	Header checksum				
Source address						
Destination address						
Options (0 or more words)						

4/9/2018

* Fragmentation.
* reassembly is Done only @ final destination By L3.
* if source peform MTU discovery then fragmentation will NOT happen.

- **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.

once the router decrements from TTL=1 → TTL=0 it immediatly discards the PKt & send ICMP.

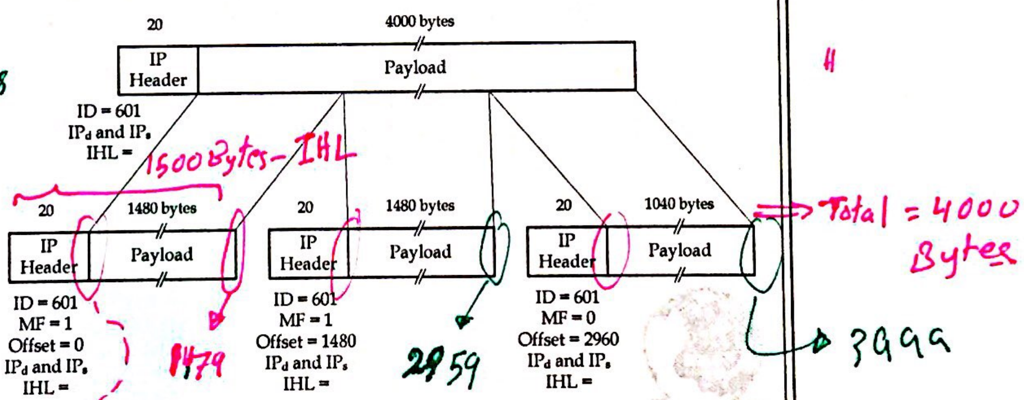
• Microsoft windows TTL=128

• linux TTL=255

Fragmentation of an IP Packet

(MTU = 1500)

Total Length = 4020 Bytes



offset is the first Byte of the fragment

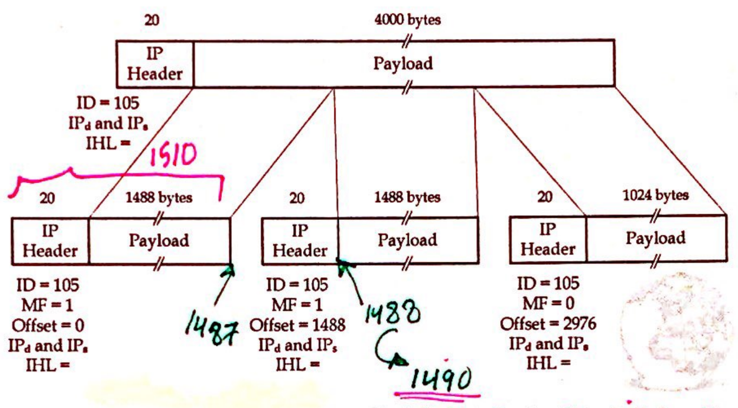
* if you lose one or more fragments, discard all the other fragments.

Scanned by CamScanner

1488 d = 0000010111 010 000

IP Fragmentation Homework

(MTU = 1510)



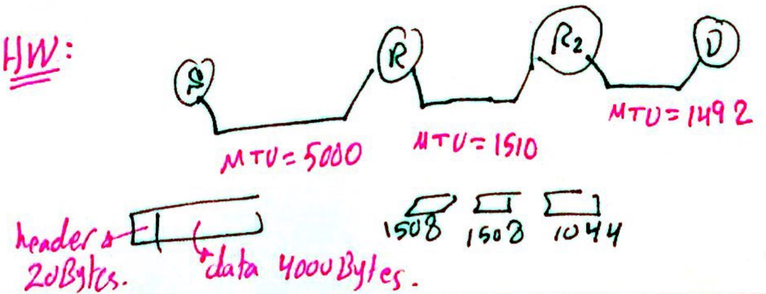
1488 is multiple of 8

IP Packet Fields

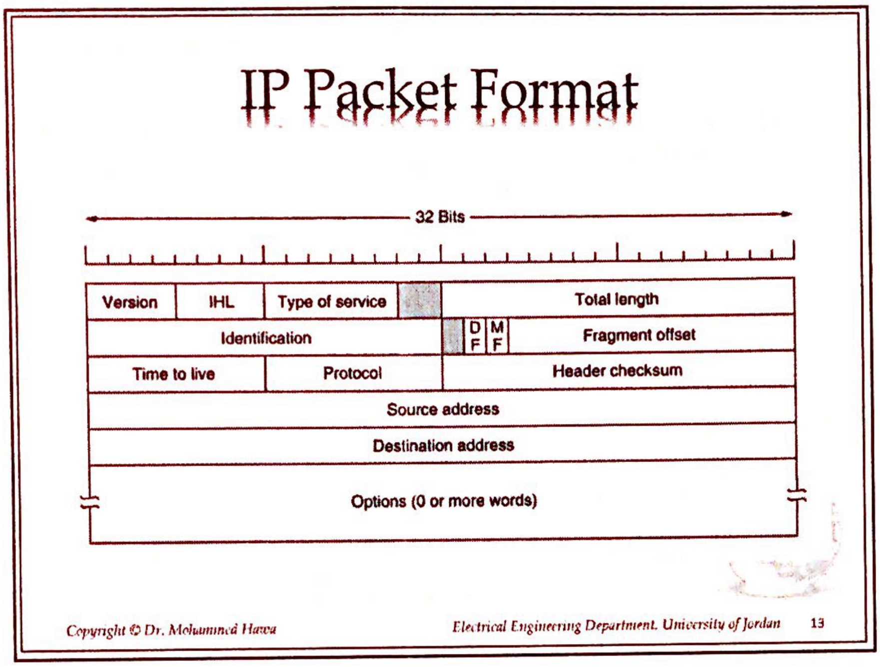
- **Protocol:** A number that tells the receiver to which Layer 4 process to deliver data. Possibilities include TCP = 6, UDP = 17, ICMP = 1, etc. memorize.
- **Header Checksum:** used to detect errors in the header only. Note that the header checksum must be recomputed at each hop because at least one field always changes (the TTL field), but special tricks can be used to speed up the computation. including options.
- **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: source address come before Dest. address.

HW:



Scanned by CamScanner



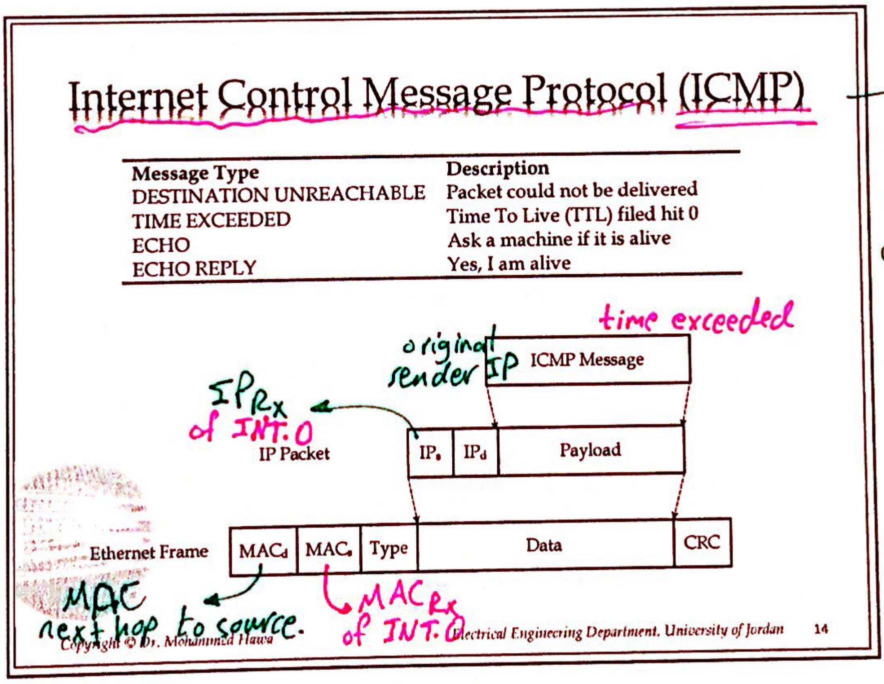
IP Packet Format

32 Bits

<table>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="4">Total length</td></tr>
<tr><td colspan="3">Identification</td><td></td><td>D
F</td><td>M
F</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="4">Header checksum</td></tr>
<tr><td colspan="7">Source address</td></tr>
<tr><td colspan="7">Destination address</td></tr>
<tr><td colspan="7">Options (0 or more words)</td></tr>
</table>

Copyright © Dr. Mohammed Hawa

Electrical Engineering Department, University of Jordan



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

time exceeded

original sender IP

IP_{Rx} of INT.0

MAC next hop to source.

MAC_{Rx} of INT.0

Copyright © Dr. Mohammed Hawa

Electrical Engineering Department, University of Jordan

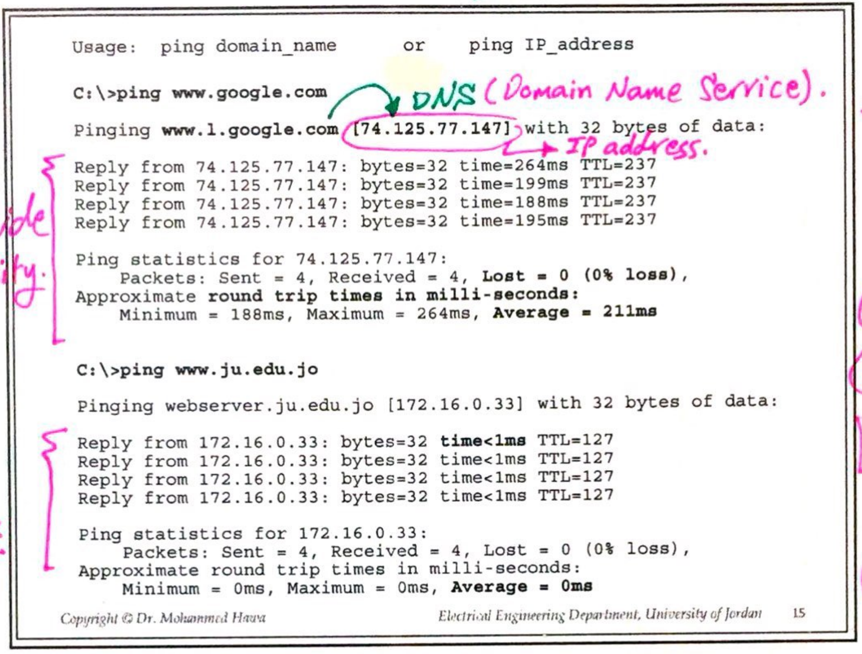
it is between L4 & L3 we might call it L3.5 & it almost work like L4.

Scanned by CamScanner

*HW: windows → CMD prompt

*HW: calculate #of routers between google & your Machine.

DNS Translate (alias = URL). → www.google.com



```
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
```

Copyright © Dr. Mohammed Hawa — Electrical Engineering Department, University of Jordan 15

→ DNS (Domain Name Service).

→ IP address.

outside university.

inside university.

* We Can get:

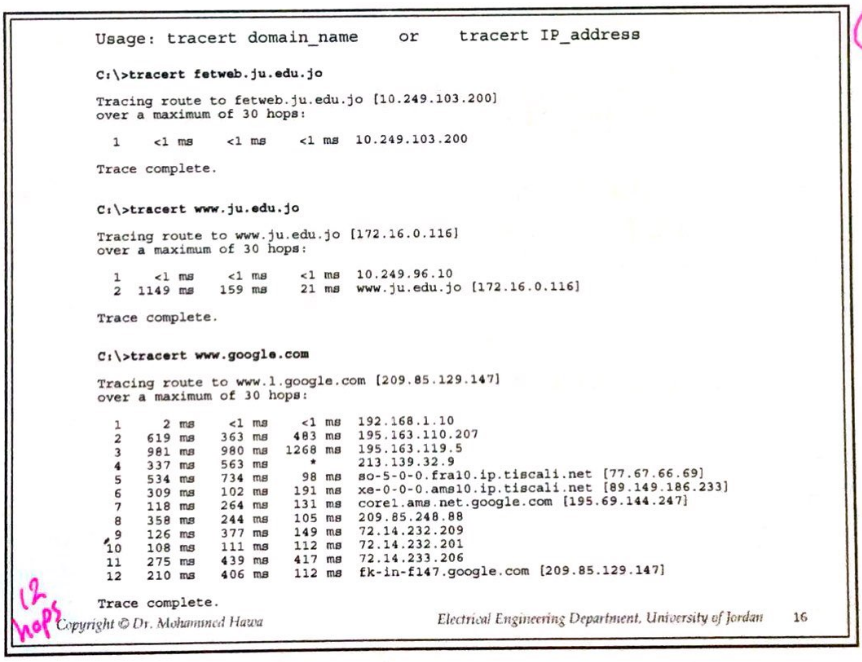
① fully Qualified domain name.

② IP Address.

③ Round Trip Time.
→ distance & congestion.

④ TTL.
→ Tells you the number of routers.

⑤ Lost packets.
→ which tells that: machine is down or congestion occur or some other things.



```
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.
```

12 hops

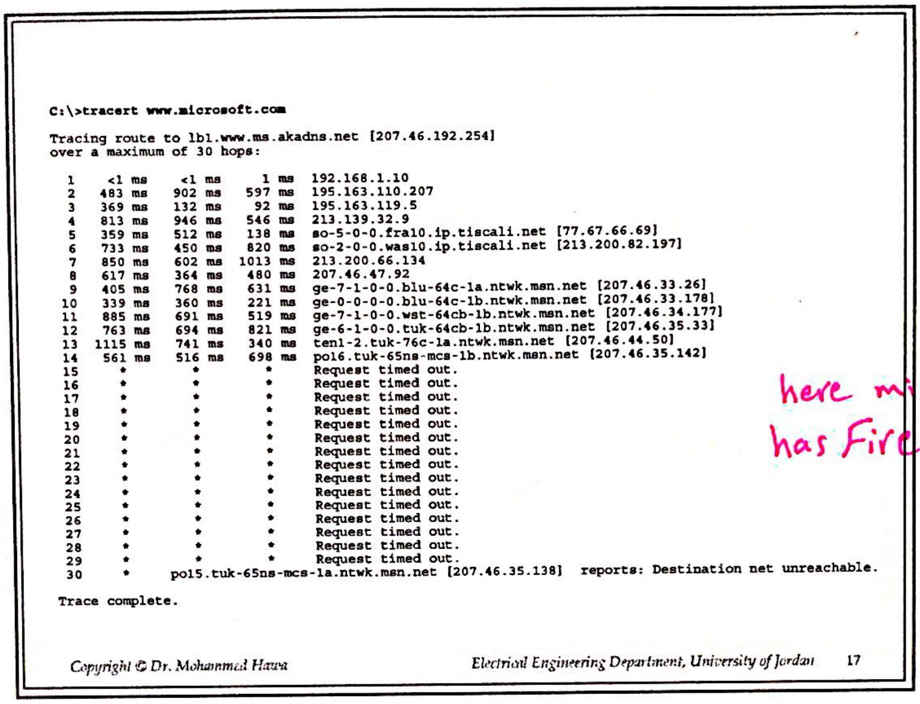
Copyright © Dr. Mohammed Hawa — Electrical Engineering Department, University of Jordan 16

*
send IP PKt & we put TTL = 1

send IP PKt. TTL = 2

send IP PKt TTL = 3

Scanned by CamScanner



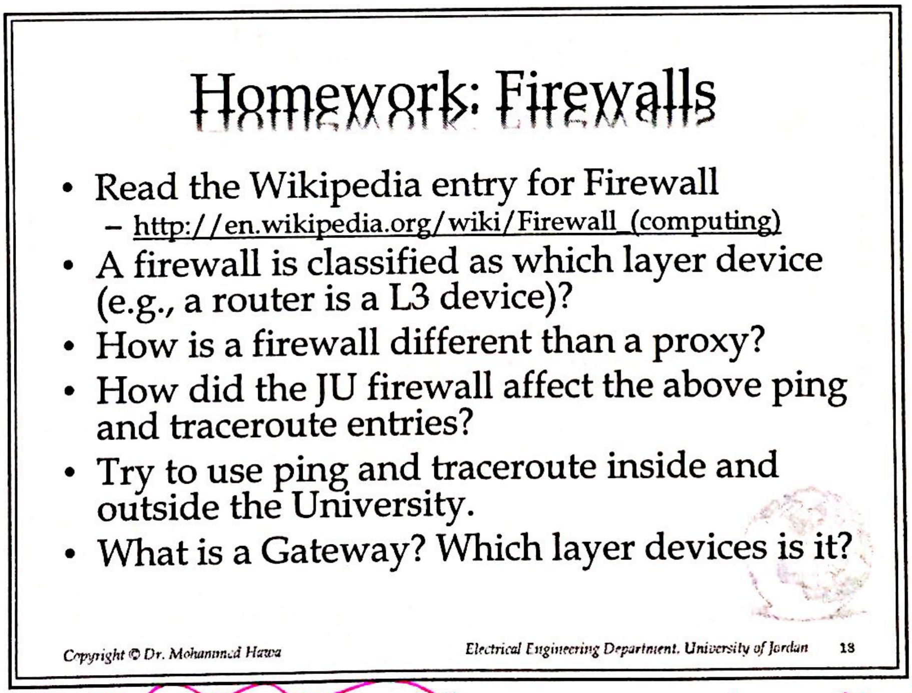
```
C:\>tracert www.microsoft.com

Tracing route to lbl.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.
```

here microsoft has Firewall.



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 devices is it?

Firewall ⇒ L7 , proxy , Gateway ⇒ L7

router ⇒ L3

switch = Bridge ⇒ L2

hub ≡ Repeater ⇒ L1

Scanned by CamScanner

Communication Networks

Spring 2017/2018

Dr. Mohammad HAWA

By: Mohammad
Abu Hashya.

* * *

Scanned by CamScanner

Lecture 12: IP Addressing and Datagram Forwarding

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

IPv4 ⇒ 32 bits (4 Bytes)   IPv6 ⇒ 128 bits (16 Bytes).

The IPv4 Address

Each host is assigned a unique **32-bit IP address**, which is typically expressed in <u>dotted decimal notation</u>:

(8 bits).(8 bits).(8 bits).(8 bits)

Examples:

10.2.0.37	00001010.00000010.00000000.00100101
128.10.2.3	
128.128.255.1	10000000.10000000.11111111.00000001
129.52.6.2	
182.24.31.144	10110110. 00011000.00011111.10010000
192.5.48.3	

Range:

$00000000_b . 00000000_b . 00000000_b . 00000000_b - 11111111_b . 11111111_b . 11111111_b . 11111111_b$

$0_d . 0_d . 0_d . 0_d - 255_d . 255_d . 255_d . 255_d$

Total of 2^{32} = 4,294,967,296 addresses.

.remember:
in MAC
48bits
& we use
Hexadecimal.

→ Max. # of addresses for IPv4.

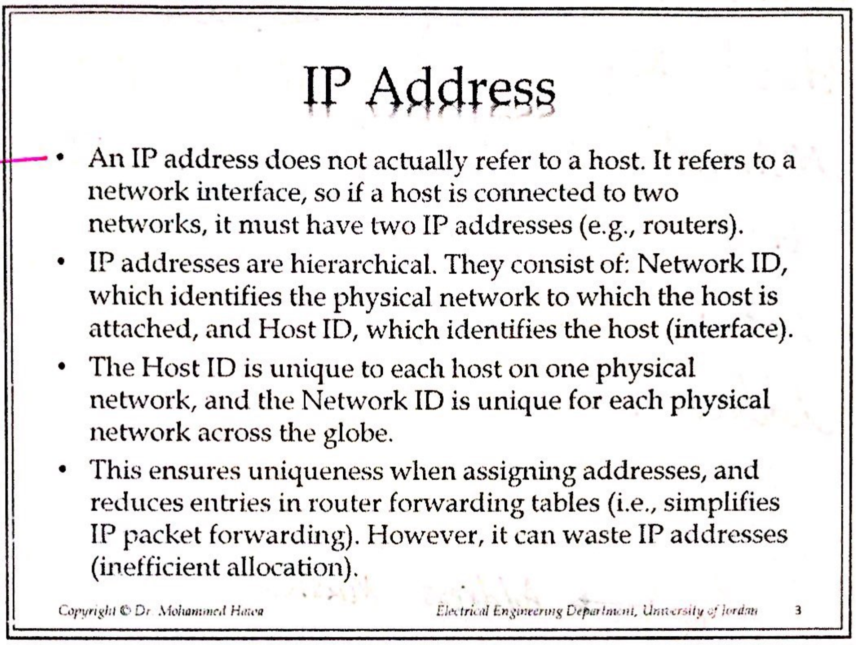
* Decimal to Binary:

128	64	32	16	8	4	2	1
0	0	0	0	1	0	1	0

8 + 2 = 10.

* Max. # of addresses for IPv6

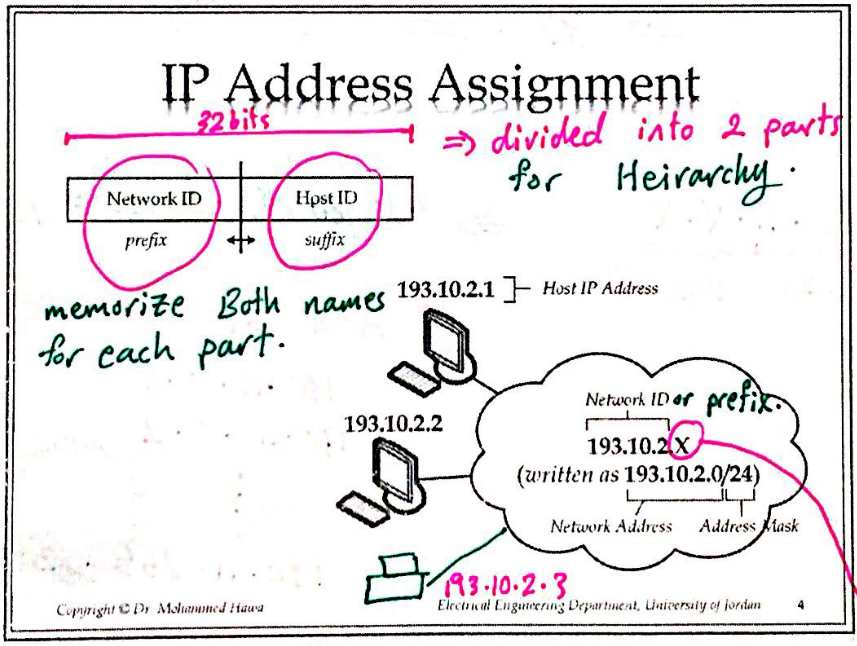
$\boxed{2^{128}}$



IP Address

- An IP address does not actually refer to a host. It refers to a network interface, so if a host is connected to two networks, it must have two IP addresses (e.g., routers).
- IP addresses are hierarchical. They consist of: Network ID, which identifies the physical network to which the host is attached, and Host ID, which identifies the host (interface).
- The Host ID is unique to each host on one physical network, and the Network ID is unique for each physical network across the globe.
- This ensures uniqueness when assigning addresses, and reduces entries in router forwarding tables (i.e., simplifies IP packet forwarding). However, it can waste IP addresses (inefficient allocation).

Copyright © Dr. Mohammed Hawa — Electrical Engineering Department, University of Jordan — 3



IP Address Assignment

⇒ divided into 2 parts for Heirarchy.

memorize Both names for each part.

always the address will start with 193.10.2

→ Host ID (suffix).

Copyright © Dr. Mohammed Hawa — Electrical Engineering Department, University of Jordan — 4

- if we have 0 at the top of right it is NOT Host ID.

193.10.2.0 ⇒ will be called [Network Address.]

⇒ the same for 255.

otherwise we call it [Host IP Address.]

Host ID (8 bits)
could be 1,2,...,254
0 & 255 are reserved.

Scanned by CamScanner

* Note: (carful for each name) memorize

Network ID
Host ID } < 32 Bits.

Network Address
Host Address. } = 32 Bits.

Subnetwork= Mask = Network Mask ≡ Address Mask.

Address Range

193.10.2.0 /(24) → Address Mask.

⇒ 24 Bits.

⇒ 32 - 24 = 8 Bits. for Host ID.

* for: $\underbrace{130 \cdot 11}_{\text{Net. ID}} \cdot \underbrace{X \cdot X}_{\text{Host ID}}$ ⇒ *Network address ≡ 130.11.0.0

* Host IP addresses:

130.11.0.1
130.11.0.2
⋮
130.11.255.254.

* 193.10.2.X
* How to know that the limit is 254?

$2^8 - \underset{\downarrow}{2} = 254.$

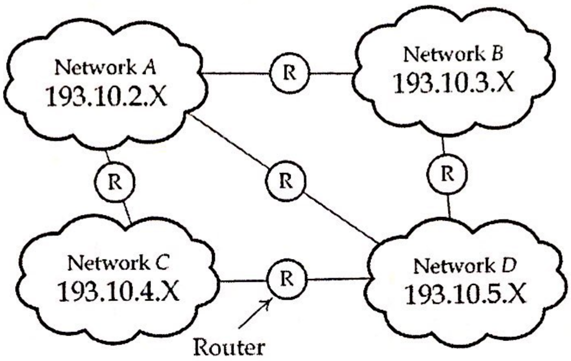
2 are reserved.

* What is the possible host IP addresses for 130.11.X.X ?

$2^{16} - 2 = 65,534$

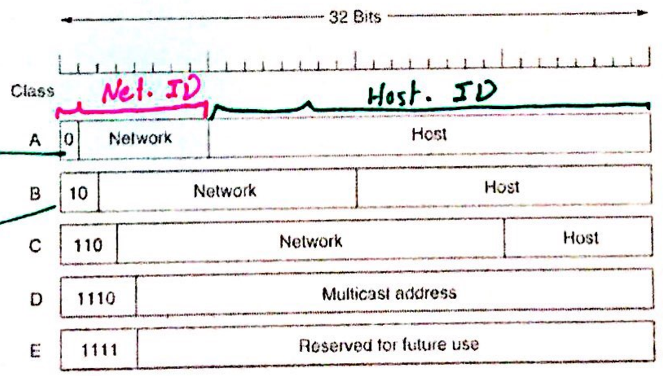
Scanned by CamScanner

Network IDs are Unique Globally
Host IDs are Unique Locally



Copyright © Dr. Mohammed Hawa

Classful IP Addresses:
Classes A, B and C



if the address start with 0 then class A.

if the address start with 10 then class B

⋮

Host ID

/8 → class A

/16 → class B

/24 → class C

Copyright © Dr. Mohammed Hawa

193.10.2.0/24 is a class "C".

Scanned by CamScanner

what is the class for 1.1.1.1 ?

this is decimal
NOT Binary.

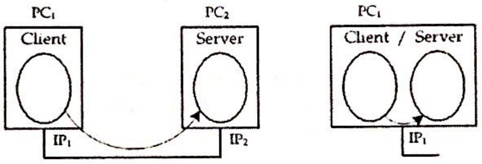
1.1.1.1
00000001
⟹ class A.

Class A
00000000
00000001
00000010
⋮
01111111

class B 128.0.X.X
10 000000
⋮
10 ~~11~~11111
191.255.X.X

Ranges: Classes A, B and C

Class	Possible Network IDs	No. of Networks	Max Hosts per Network
A	1.X.X.X to 127.X.X.X	$2^7 - 1 = 127$	$2^{24} - 2 = 16{,}777{,}214$
B	128.0.X.X to 191.255.X.X	$2^{14} = 16{,}384$	$2^{16} - 2 = 65{,}534$
C	192.0.0.X to 223.255.225.X	$2^{21} = 2{,}097{,}152$	$2^8 - 2 = 254$
D	224.0.0.0 to 239.255.255.255		
E	240.0.0.0 to 255.255.255.254		
Broadcast	255.255.255.255		



Copyright © Dr. Mohammed Hawa

Examples

- MIT (Massachusetts Institute of Technology), USA, network, was assigned the IP class A address range 18.0.0.0/8 (18.0.0.1 – 18.255.255.254). Gave some back.
- University of Kansas, USA, network, is assigned the IP class B address range 129.237.0.0/16 (129.237.0.1 – 129.237.255.254).
- University of Jordan, was assigned the class C network address 193.188.81.0/24 when it was first connected to the Internet through NIC (National Information Center, Jordan),
- But since JU switched to Orange, they gave up this address range for the smaller range of 213.139.45.192/27 (213.139.45.193 – 213.139.45.222).
- Try whois utility or https://www.whois.com/whois.

27 Bit + 5 bit
Net.ID Host ID
= 32 Bits.

$2^5 - 2 = 30$ hosts.

Copyright © Dr. Mohammed Hawa

Scanned by CamScanner

Global Address Assignment

- Internet Assigned Numbers Authority (IANA) oversees global IP address allocation, autonomous system number allocation, root zone management in DNS, media types, and other IP-related symbols and numbers.
- IANA is a department operated by the Internet Corporation for Assigned Names and Numbers (ICANN).
- IANA hands out /8 address blocks to Regional Internet Registries (RIR):
  - RIPE NCC (Europe, Middle East, Russia, Central Asia)
  - APNIC (Asia Pacific)
  - ARIN (North America)
  - LACNIC (Latin America)
  - AfriNIC (African Region)
- (see http://www.iana.org/assignments/)
- ISPs obtain their network addresses from RIRs.
- End users and companies obtain their IP addresses form ISPs

DONOT Memorize.

Memorize

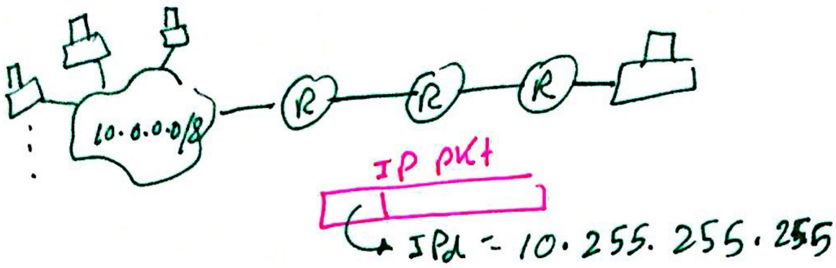
Special IP Addresses

Network ID	0000000 0000000	Network Address
Network ID	1111111 1111111	Directed (Distant) Broadcast Address
0.0.0.0 00000000000000000000000000000000		This Host Address
255.255.255.255 11111111111111111111111111111111		Limited (Local) Broadcast Address
000...000	Host ID	Hosts on This Network
127	Anything	Loopback Addresses

class A.
10.0.0.0/8

$10\underbrace{.0.0.0}_{\text{Host. ID.}}$

Scanned by CamScanner



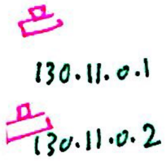
/8
10.0.0.0

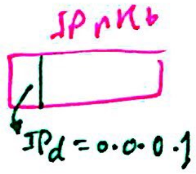
0.1.2.3 ⇒ 10.1.2.3

0.5.5.3 ⇒ 10.5.5.3

Special IP Addresses

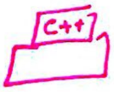
- **Network Address**: Refers to the network itself. For example 128.211.0.0 denotes the network that has been assigned the Network ID 128.211.X.X (or 128.211.0.0/16). The network address is not assigned to any of the hosts in the network, which means it should never appear as the source or destination addresses in an IP packet. However, it is useful for routing (see later).
- **Directed (Distant) Broadcast Address**: When an IP packet is sent to a network's directed broadcast address, a single copy of the packet travels across the Internet until it reaches the specified network, and the packet is then delivered to all hosts on the network. This address is not assigned to any single host, so it can appear as destination address, but not as source address.
- **This Host Address**: When the computer is not assigned an IP address beforehand (e.g., when the computer boots up), it is allowed to use the address 0.0.0.0 as the source IP address to mean "This Computer" or "This Host". This is useful when executing certain protocols at startup such as DHCP.





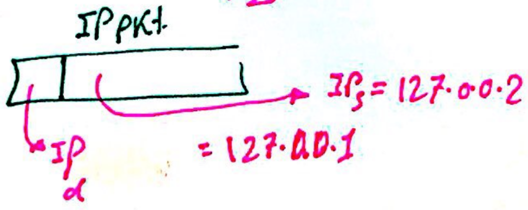
Special IP Addresses

- **Limited (Local) Broadcast Address**: Using 255.255.255.255 as the destination address, the IP packet will be broadcast across the local network (i.e., all the hosts on the physical network will read the packet). Typically sent in L2 frame with FF:FF:FF:FF:FF:FF destination MAC address. Useful when a computer starts up, as it does not yet know the Network ID.
- **Hosts on This Network**: Such addresses allow machines to refer to their own network without knowing its network ID (but they have to know its class to know how many 0's to include).
- **Loopback Addresses**: Used to test network applications (i.e., for debugging). All IP addresses in the range 127.0.0.0/8 are loopback. The host address you choose within 127.0.0.0/8 is irrelevant since packets sent to any one of these IP addresses are not put onto the wire; instead they are recycled locally. The most popular loopback IP address is 127.0.0.1.



127.0.0.1
127.0.0.2
⋮
127.255.255.254

127.0.0.0/8



Scanned by CamScanner

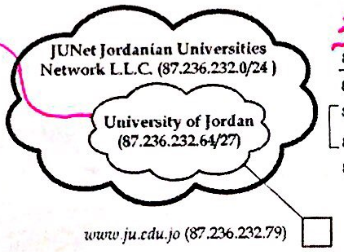
↱ described in RFC 1519.

4/23/2018

CIDR ≡ Classless Inter-Domain Routing.

Classless IP Addresses (CIDR Addresses)

The original **class A** network address 11.0.0.0 **becomes** 11.0.0.0/8
The original **class B** network address 128.5.0.0 **becomes** 128.5.0.0/16
The original **class C** network address 192.6.1.0 **becomes** 192.6.1.0/24



host ID . net. address ⇒ all 0's.

01 | 000000

24 bit

87 . 236 . 232 .	64	/27	Allocation
87 . 236 . 232 . 010	00000		Network Address
87 . 236 . 232 . 010	00001		87.236.232.65 Host Address
	. . .		
87 . 236 . 232 . 010	11110		87.236.232.94 Host Address
87 . 236 . 232 . 010	11111		87.236.232.95 Directed Broadcast

11111 → 87.236.232.95

Copyright © Dr. Mohammed Hawa — Electrical Engineering Department, University of Jordan — 13

net. ID host ID
27Bit. 5bit.

max host $= 2^5 - 2$
= 30 hosts.

11.0.0.0/8
net. ID host ID
8. 24.

12.0.0.0/9
net. ID host ID
9bit 23bit
max host $= 2^{23} - 2$

128.5.0.0/16
net ID host ID
16 16

192.6.1.0/24
net ID host ID
24 8.

87.236.232.0/24 ⇒ This is Class C.
Net. ID host ID

Network Address:
87.236.232.0

distant broadcast:
87.236.232.255

Possible host IP addresses:
87.236.232.1
↓
87.236.232.254.

Example

- If a network contains a maximum of 60 computers, only 6 bits of Host ID are needed ($2^6 - 2 = 62$).
- The remaining 26 bits are used for the Network ID, and the network address would be written with **/26** (e.g., **130.5.1.128/26**). Possible IP addresses within this network are 130.5.1.129 to 130.5.1.190.

⇒ $2^n \geq 60+2$
proper n is:
$\boxed{n = 6 \text{ bits}}$

host ID

128+1

10000010. 00000101. 00000001. 10	000001	130.5.1.129
	. . .	
	111110	130.5.1.190

↳ 62

↳ 128+62

130.5.1.192/26
↳ 1100 0000

111111 → 130.5.1.191 ⇒ This distant Broadcast.

Copyright © Dr. Mohammed Hawa — Electrical Engineering Department, University of Jordan — 14

Net ID host ID.
26 Bits. 6 Bits.
——/26.

is 130.5.1.129/26 a valid address for your Network?

NO.

130.5.1.128/24 X

Network with 64 machines.
⇒ Net. ID host ID
25 7.

Scanned by CamScanner

for 130.5.1.128/26 subnet mask = address mask = network mask.
= mask = /26

1111 1111 . 1111 1111 . 1111 1111 . 11 0000 00
255 . 255 . 255 . 192.

Example (*Different Approach*)

- What is the Network Address?
- What is the Subnet Mask (Address Mask)? for 87.238.232.0/24 Subnet mask ⇒ /24. or
- What is the Distant Broadcast Address?
- What is the maximum number of hosts that can be connected to this network?
- Is the host IP address 130.5.1.131 within this network? Yes.
- Is the host IP address 130.5.1.199 within this network? NO.

another answer.

11111111.11111111.11111111.0000 0000
255.255.255.0

Example (*Cont.*)

- The host with IP address 130.5.1.131 is part of the network 130.5.1.128/26 because:
- (130.5.1.131) AND (/26) =
(130.5.1.131) AND (255.255.255.192) = 130.5.1.128

	10000010. 00000101. 00000001. 10000011 128+ 2+1	130.5.1.131
AND	11111111. 11111111. 11111111. 11000000	255.255.255.192
	10000010. 00000101. 00000001. 10000000	130.5.1.128 → Network address.

Yes it is within the network.

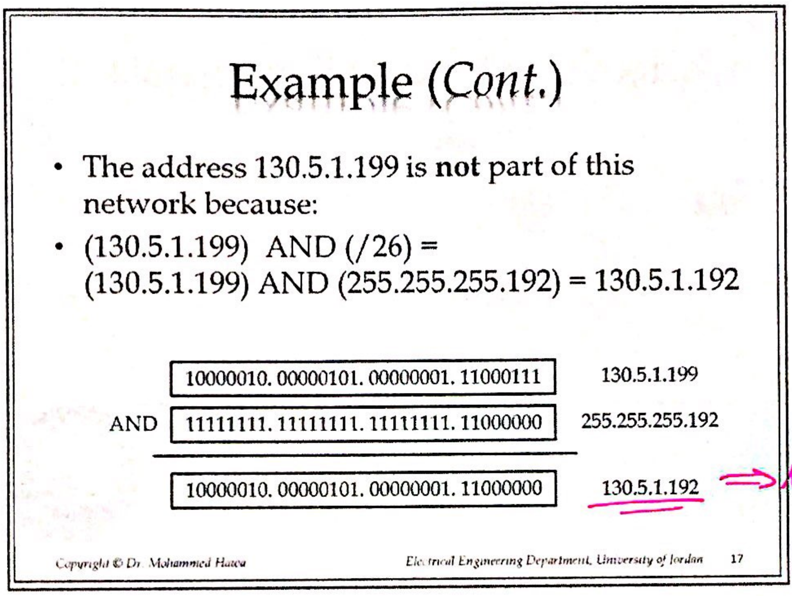
This is how the router work. through AND process.

IP$_d$ = 130.5.1.191 ⇒ 10111111
AND 255.255.255.192 11000000
130.5.1.128 ← 10000000

⇒ Deliver YES to Whom ALL on 130.5.1.128/26.

* in IP PKts : only the address is sent.
* inside router table & host tables: Both network address & Subnet mask.

11.0.0.0/16 (classless) ⇒ Class B.
11.0.0.1 ⇒ Class A.
↳ 0000 1011



Example (Cont.)

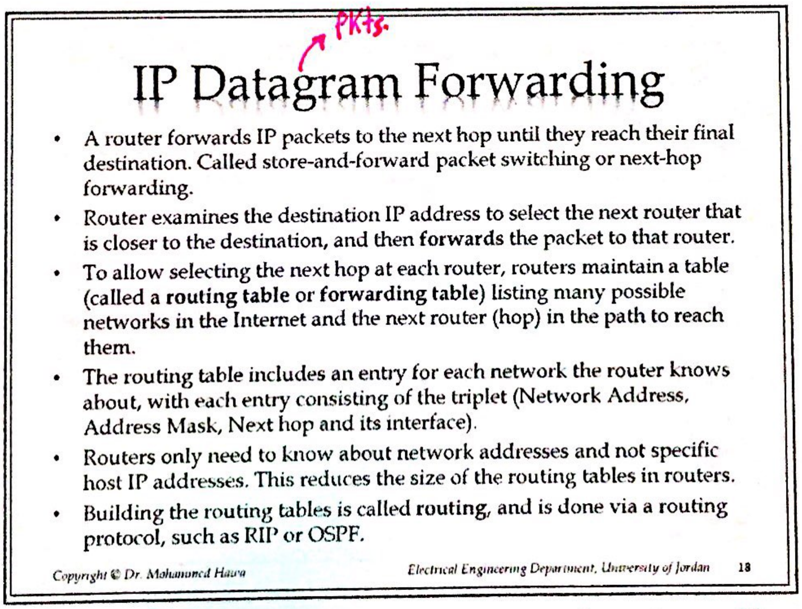
- The address 130.5.1.199 is **not** part of this network because:
- (130.5.1.199) AND (/26) = (130.5.1.199) AND (255.255.255.192) = 130.5.1.192

	10000010. 00000101. 00000001. 11000111	130.5.1.199
AND	11111111. 11111111. 11111111. 11000000	255.255.255.192
	10000010. 00000101. 00000001. 11000000	130.5.1.192 ⇒ Network address

No it is NOT within the network.

Copyright © Dr. Mohammed Hawa

Electrical Engineering Department, University of Jordan 17



IP Datagram Forwarding

PKts.

- A router forwards IP packets to the next hop until they reach their final destination. Called store-and-forward packet switching or next-hop forwarding.
- Router examines the destination IP address to select the next router that is closer to the destination, and then **forwards** the packet to that router.
- To allow selecting the next hop at each router, routers maintain a table (called a **routing table** or **forwarding table**) listing many possible networks in the Internet and the next router (hop) in the path to reach them.
- The routing table includes an entry for each network the router knows about, with each entry consisting of the triplet (Network Address, Address Mask, Next hop and its interface).
- Routers only need to know about network addresses and not specific host IP addresses. This reduces the size of the routing tables in routers.
- Building the routing tables is called **routing**, and is done via a routing protocol, such as RIP or OSPF.

Copyright © Dr. Mohammed Hawa

Electrical Engineering Department, University of Jordan 18

Routers Do two different things
→ Routing (speaking with each other to build tables).
→ Forwarding (looking up table to forward PKts)

max host $2^{24}-2-2$

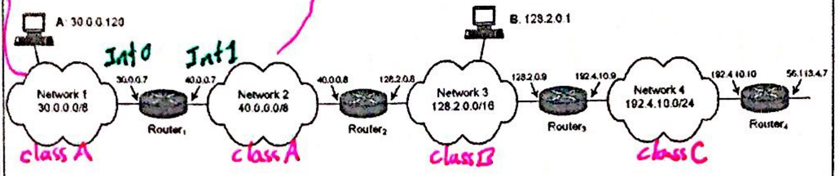
valid host $2^{24}-2$

IP Datagram Forwarding/Example

max. hosts connected to Network 1:

$2^{24}-2-1$

#of connected routers



for router2:

Net 1

30.0.0.0 /8

40.0.0.7 Int0

Route Table at Router 1

Network Destination	Netmask	Next Hop	Metric	Interface	Comments
30.0.0.0	/8	Direct	6	Int0	other hosts on LAN
40.0.0.0	/8	Direct	6	Int1	other hosts on LAN
128.2.0.0	/16	40.0.0.8	6	Int1	next hop
192.4.10.0	/24	40.0.0.8	6	Int1	next hop
0.0.0.0	/0	40.0.0.8	6	Int1	default gateway
....					other entries

Default Gateway.

```
if( (DestIPAddress & AddressMask[i]) == DestinationNetwork[i])
      Forward to NextHop[i];
```

Route Table at Router 1

Network Destination	Netmask	Next Hop	Metric	Interface	Comments
30.0.0.0	/8	Direct	6	Int0	other hosts on LAN
40.0.0.0	/8	Direct	6	Int1	other hosts on LAN
128.2.0.0	/16	40.0.0.8	6	Int1	next hop
192.4.10.0	/24	40.0.0.8	6	Int1	next hop
0.0.0.0	/0	40.0.0.8	6	Int1	default gateway
....					other entries

Route Table at Router 2

Network Destination	Netmask	Next Hop	Metric	Interface	Comments
30.0.0.0	/8	40.0.0.7	6	Int0	next hop
40.0.0.0	/8	Direct	6	Int0	other hosts on LAN
128.2.0.0	/16	Direct	6	Int1	other hosts on LAN
192.4.10.0	/24	128.2.0.9	6	Int1	next hop
0.0.0.0	/0	128.2.0.9	6	Int1	default gateway
....					other entries

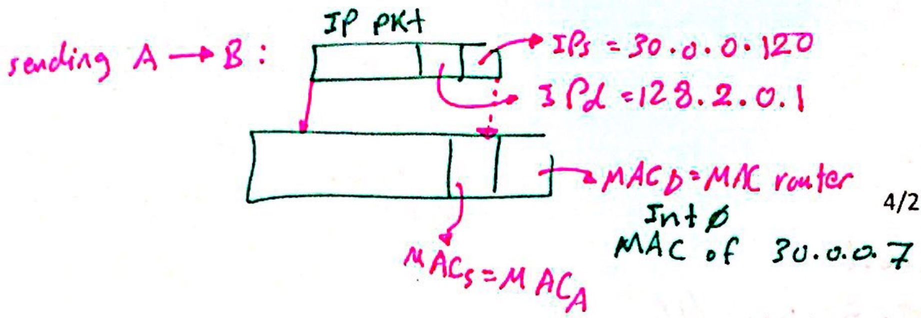
Route Table at Router 3

Network Destination	Netmask	Next Hop	Metric	Interface	Comments
30.0.0.0	/8	128.2.0.8	6	Int0	next hop
40.0.0.0	/8	128.2.0.8	6	Int0	next hop
128.2.0.0	/16	Direct	6	Int0	other hosts on LAN
192.4.10.0	/24	Direct	6	Int1	other hosts on LAN
0.0.0.0	/0	192.4.10.10	6	Int1	default gateway
....					other entries

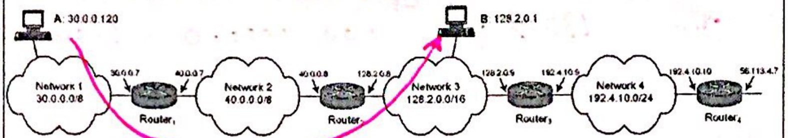
Route Table at Router 4

Network Destination	Netmask	Next Hop	Metric	Interface	Comments
30.0.0.0	/8	192.4.10.9	6	Int0	next hop
40.0.0.0	/8	192.4.10.9	6	Int0	next hop
128.2.0.0	/16	192.4.10.9	6	Int0	next hop
192.4.10.0	/24	Direct	6	Int0	other hosts on LAN
0.0.0.0	/0	56.113.4.8	6	Int1	default gateway
....					other entries

Scanned by CamScanner



IP Datagram Forwarding/Example



Route Table at Host 30.0.0 120

Network Destination	Netmask	Next Hop	Metric	Interface	Comments
127.0.0.0	/8	127.0.0.1	1	127.0.0.1	Loopback
30.0.0.120	/32	127.0.0.1	1	127.0.0.1	Host own IP address
30.0.0.0	/8	Direct	6	Int0	other hosts on LAN
30.255.255.255	/32	Direct	6	Int0	directed broadcast
255.255.255.255	/32	Direct	6	Int0	limited broadcast
224.0.0.0	/4	Direct	6	Int0	multicast
0.0.0.0	/0	30.0.0.7	6	Int0	default gateway

```
if( (DestIPAddress & AddressMask[i]) == DestinationNetwork[i])
      Forward to NextHop[i];
```

Host 30.0.0.120 wants to send an IP packet to the host 128.2.0.1.

IPd AND Net1,Network mask = result $\overset{?}{=}$ net1 address.

(128.2.0.1) AND (255.0.0.0) = 128.0.0.0 ≠ 30.0.0.0

(128.2.0.1) AND (255.0.0.0) = 128.0.0.0 ≠ 40.0.0.0

(128.2.0.1) AND (255.255.0.0) = 128.2.0.0 = 128.2.0.0 (Match, Longest) ⟹ pick Longest match. if the same Length ⟹ pick smaller metric.

/16

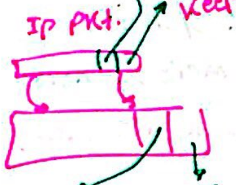
(128.2.0.1) AND (255.255.255.0) = 128.2.0.0 ≠ 192.4.10.0

(128.2.0.1) AND (0.0.0.0) = 0.0.0.0 = 0.0.0.0 (Match)

/0 has 32 host ID bits (all zeros)

IPd = 128.2.0.1

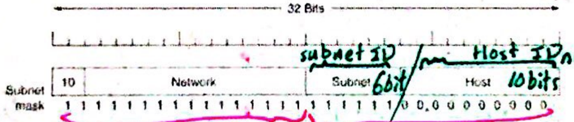
IPs = 30.0.0.120 keep.



MACs = MAC of 40.0.0.7 = R1 Int 1

MACD = MAC of 40.0.0.8

Subnets / Example



For example, the class B network address 130.50.0.0/16 can be subnetted to the following **64 subnets** using **6 bits** for the Subnet ID,

outside.

inside.

130.50.0.0/22	10000010.00110010. /	000000	/	00.00000000
130.50.4.0/22	10000010.00110010. /	000001	/	00.00000000
130.50.8.0/22	10000010.00110010. /	000010	/	00.00000000
130.50.12.0/22	10000010.00110010. /	000011	/	00.00000000
130.50.16.0/22	10000010.00110010. /	000100	/	00.00000000
...	130. 50 . 16 .0	111111		

→ how many hosts on each subnet? $2^{10}-2$.

*Subnet : net ID for inside routers.

*subnet : host ID for outside routers.

new net ID = old networkID + Subnet ID = 16+6 = 22.

2^6 = 64 subnets.

Ex. 130.50.0.0/16 divide it into 4 departments.

130.50.00/00 0000. 0 ⟹ 130.50.0.0/18 1st subnet → # of hosts = $2^{14}-2$

130.50.00 00 0000. 0

130.50.01 0 0 0000. 0 → 130.50.64.0/18 → $2^{14}-2$

130.50.10 0 0 0000. 0 → 130.50.128.0/18 → $2^{14}-2$

130.50.11 0 0 0000. 0 → 130.50.192.0/18 → $2^{14}-2$

Scanned by CamScanner

Ex.

Class B

130 . 50.0.0 /16

into 2 subnets.

#1 130.50./0 000 0000.0 = 130.50.0.0/17

subnet ID

#2 130 . 50 /1 000 0000 . 0 = 130.50.128.0/17

subnet ID

130.50.1/00/0 0000 . 0 ⇒ 130.50.128.0/19

.01 → 128+32 = 160 ⇒ 130.50.160.0/19

.10 → 128+64=192 ⇒ 130 . 50.192 . 0/19

11 → 128 + 64 + 32 = 224 ⇒ 130.50.224. 0/19

→ HW. split into 8 more subnets. (will give /22).

* for this Ex. show entries in routing table inside University of Jordan :

130. 50.0.0/17 → 2^{15}

130 . 50 . 128 . 0 /19 → 2^{13}

130 . 50 . 160 . 0 /19 → 2^{13}

130 . 50 . 192 . 0 /19 → 2^{13}

130 . 50 . 224 . 0/19 → 2^{13}

} ⇒ 65,536.

194.24.0.0 /19 → 194.24.0.0/20 → 194.24.000/0/0000.0
1
→ 194.24.16.0/20 →

⇒ 194.24.0.0/20 → 194.24.0.0/21
→ 194.24.8.0/21 → 194.24.8.0/22
→ 194.24.12.0/22

Address Aggregation / Example

Observe the following possible IP address allocation for three UK universities:

University	Network Address	First IP Address	Last IP Address	Number of Addresses
Cambridge	194.24.0.0/21	194.24.0.1	194.24.7.254	2048 – 2
Edinburgh	194.24.8.0/22	194.24.8.1	194.24.11.254	1024 – 2
(Available)	194.24.12.0/22	194.24.12.1	194.24.15.254	1024 – 2
Oxford	194.24.16.0/20	194.24.16.1	194.24.31.254	4096 – 2

= $2^{11}-2$

match
match, longest.

Routers outside the UK can aggregate all these entries into a single entry as follows:

194.24.0.0/19 **Forward to Next Hop to UK**

HW. Aggregate the 4 entries into 1. ?

⇒
take /22 with /22
to give /21
take it with the other one /21
to give /20
/20 & /20 ⇒ /19

Subnetting / Example

- Assume a medium-size business with four departments has acquired the IP address space **128.5.0.0/16**. Each one of its four departments has a separate physical LAN, and these LANs are connected together using routers. Show how you can divide the address space using subnet addressing, assuming:
  - Each department has **equal number** of computers.
  - Some departments have more computers than others.
- Show what type of information is stored at both: routers internal to the business and routers external to the business (e.g., the router that connects the business to its own ISP).

Scanned by CamScanner

Aggregate :

194.24.0.0/21 = 194.24. 0000 0000 . 0

with

194.24.8.0/21 = 194.24. 0000 1000 . 0

/20

= 194.24.0.0/20

IPd = 194.24.12.2

match /19

match /22

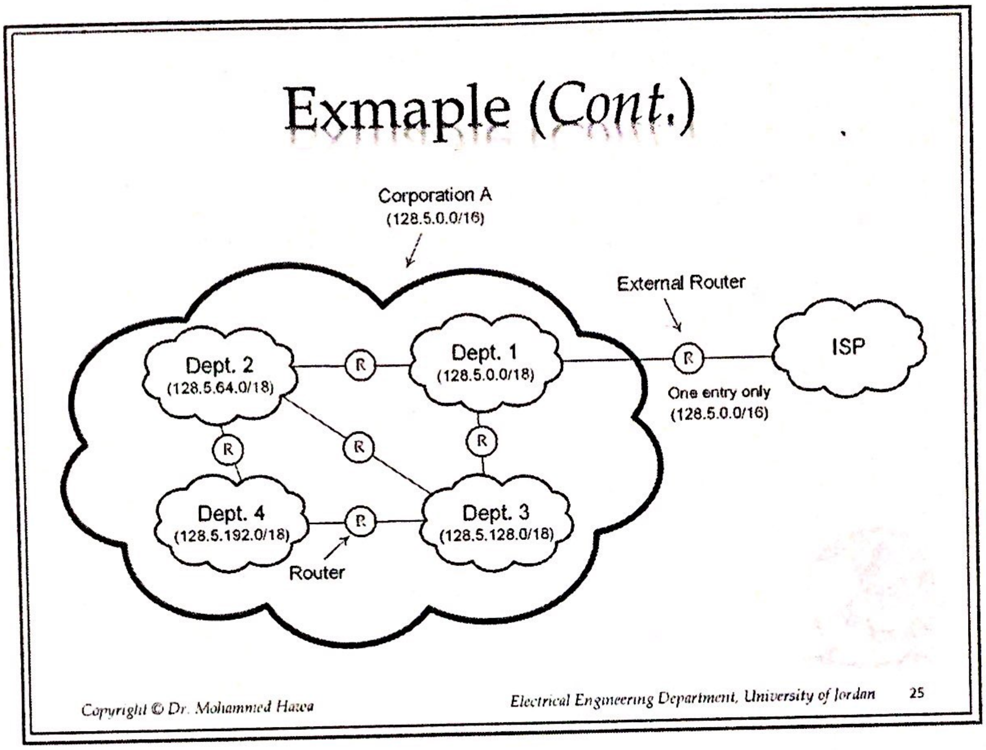
longest.

IPd = 194.24.0.1

match/19

doesn't match/22

Scanned by CamScanner



Exmaple (*Cont.*)

Corporation A
(128.5.0.0/16)

External Router

Dept. 2
(128.5.64.0/18)

R

Dept. 1
(128.5.0.0/18)

R

ISP

One entry only
(128.5.0.0/16)

R

R

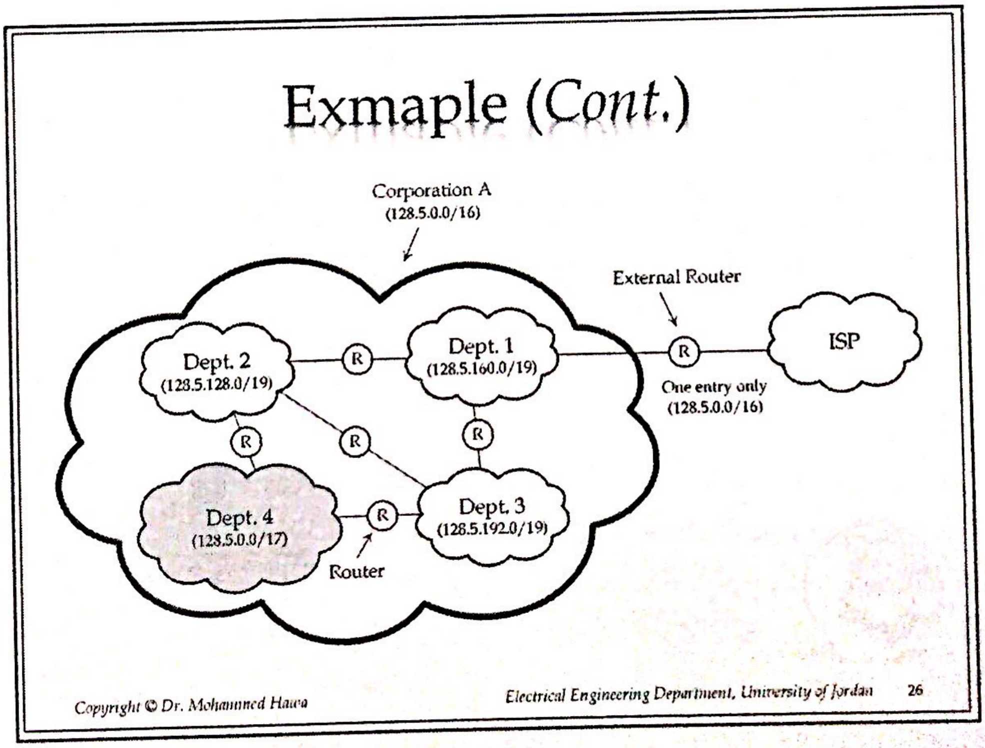
R

Dept. 4
(128.5.192.0/18)

R

Dept. 3
(128.5.128.0/18)

Router



Exmaple (*Cont.*)

Corporation A
(128.5.0.0/16)

External Router

Dept. 2
(128.5.128.0/19)

R

Dept. 1
(128.5.160.0/19)

R

ISP

One entry only
(128.5.0.0/16)

R

R

R

Dept. 4
(128.5.0.0/17)

R

Dept. 3
(128.5.192.0/19)

Router

Scanned by CamScanner

Communication Networks

Spring 2017/2018

Dr. Mohammad HAWA

By: Mohammad
Abu Hashya.

* * *

Scanned by CamScanner

Lecture 13: Address Resolution Protocol (ARP)

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

EE426: Communication Networks

---

we assign an IP address for the interface using the located network @that interface

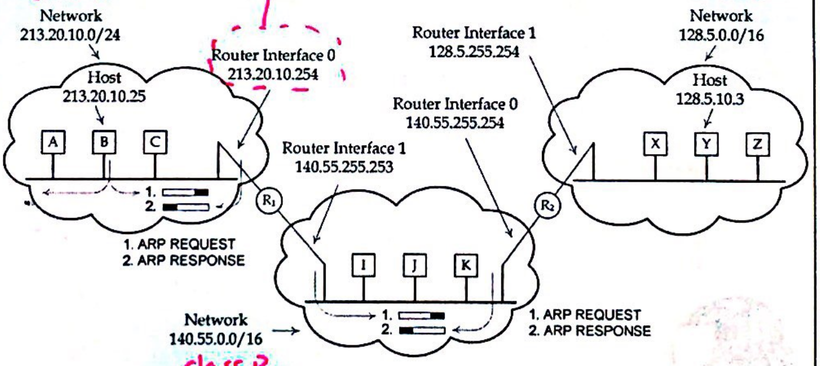
Example

what is the available range?

213.20.10.1
⋮
213.20.10.254

class C

class B



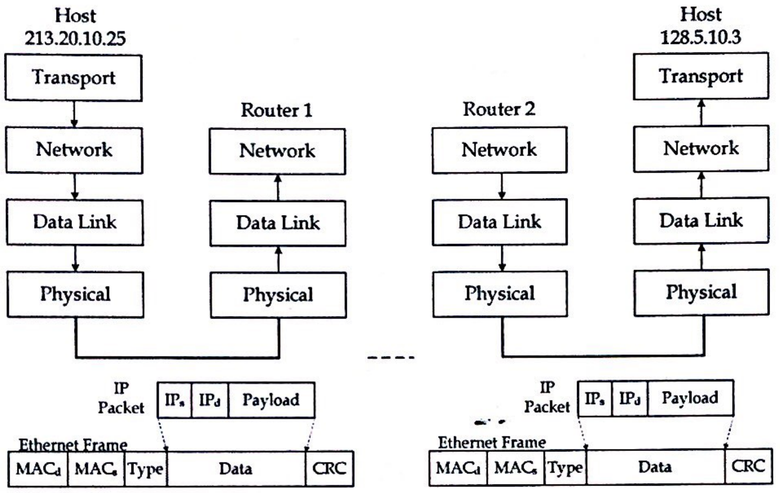
class B

Copyright © Dr. Mohammed Hawa

Electrical Engineering Department, University of Jordan 2

www.google.com
↓
128.5.10.3

Scanned by CamScanner



IP_s = 213.20.10.25
IP_d = 128.5.10.3
MAC_s = Host B MAC
MAC_d = Router 1 MAC

IP_s = 213.20.10.25
IP_d = 128.5.10.3
MAC_s = Router 2 MAC
MAC_d = Host Y MAC

→ IP router 1 Int0 → MAC router Int0

ARP

- **Address resolution**: The process of translating a host's IP address into the equivalent MAC address.
- A machine can resolve the address of another machine only if both machines are on the same physical network.
- For hosts outside of the network machines resolve the address of the default gateway (next hop).
- ARP (described in RFC 826) can perform address resolution.
- ARP is commonly used to resolve IP addresses into Ethernet MAC addresses, but it can map any type of address to any other address type.
- ARP allows a machine to build an **address binding table**. The machine starts with an empty address binding table (except for an entry to its own address).

Scanned by CamScanner

memorize this name:

Address Binding Table

IP Address	Hardware (MAC) Address	Type
213.20.10.25	0A:07:4B:12:82:55	Static
213.20.10.1	0A:1C:28:71:32:8D	Dynamic
213.20.10.23	0A:11:C3:68:01:99	Dynamic
213.20.10.200	0A:74:59:32:CC:1F	Dynamic
213.20.10.201	0A:04:BC:00:03:28	Dynamic
213.20.10.254	08:77:81:0E:52:FA	Dynamic

- To see the table on your Windows machine:

```
C:\> arp -a
```

every machine has a table like this.

static means that this entry is put manually (By hand).

ARP

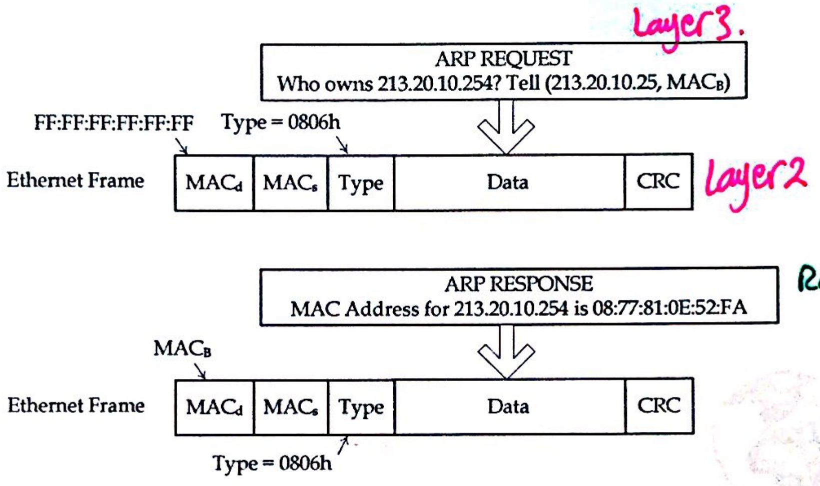
- ARP is executed to fill the table as follows:
  - The machine broadcasts an ARP REQUEST message to all hosts on the physical network.
  - Each machine on the network receives the REQUEST message. All stations (and especially the destination) are required to read this binding and update their cache with the new entry. Only the machine that has the IP address replies with an ARP RESPONSE.
- The address binding table is treated as a cache:
  - Oldest entry is removed when the table runs out of space.
  - Entries are removed after a long period of time (e.g., 20 minutes).
  - New information overrides old information.
- An optimization is to have every machine broadcast its mapping when it boots (Who owns my IP address?).

for Example in slide 2:
if B doesn't Know the address of R_1.
it will ask:
Who owns this IP address:
213.20.10.254
please tell
213.20.10.25
with MAC
0A:07:4B:12:82:55

for machine B once it Boots:
it send ARP REQUEST & ask who owns IP address
213.20.10.25
Tell 213.20.10.25
MAC 0A:07:4B:12:82:55

Scanned by CamScanner

ARP Messages



Layer3.

Layer2

Router will respond (L3).

* Why we don't use broadcast Replies?
To avoid having Broadcast storms.

* ARP is L2.5.

* ARP request ⇒ Broadcast
But ARP respond do NOT Broadcast.

Scanned by CamScanner

Communication Networks

Spring 2017/2018

Dr. Mohammad HAWA

By: Mohammad
Abu Hashya.

* * *

Scanned by CamScanner

* Classful IP addressing is inefficient.
(Why?)
- Because it is LOW Utilization.

Lecture 14: DHCP and NAT

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

IPv4 Address Shortage

- Classless IP addressing solved IPv4 address shortage temporarily, but the exponential growth of the Internet presented yet again the challenge of running out of IP addresses.
- Solutions:
- *Future*: migrating from IPv4 (with 32 bit IP address) to IPv6 (with 128 bit IP address).
- DHCP (Dynamic Host Configuration Protocol).
- NAT (Network Address Translation).

solutions for IPv4 Address shortage.

IPv4 (32 Bit IP address) ⇒ 2^{32} without reserved.
IPv6 (128 Bit) ⇒ 2^{128}.

Dynamic Host Configuration Protocol (DHCP)

- DHCP is described in RFC 2131, RFC 2132 and others.
- Was extremely helpful for ISPs with dial-up subscribers. An ISP with /16 (formerly class B) addresses dynamically assigns an IP address (through a DHCP server) to a computer when it calls up and logs in, then takes back that IP address when the session ends.
- This way, a single /16 address space serves few hundred thousand customers, since less than 65,534 are active users at any time.
- With ADSL modems, fiber connections and business customers (i.e., always-on Internet), DHCP is now seen as a tool to simplify the job of the administrator.

** DHCP is No Longer a good solution But

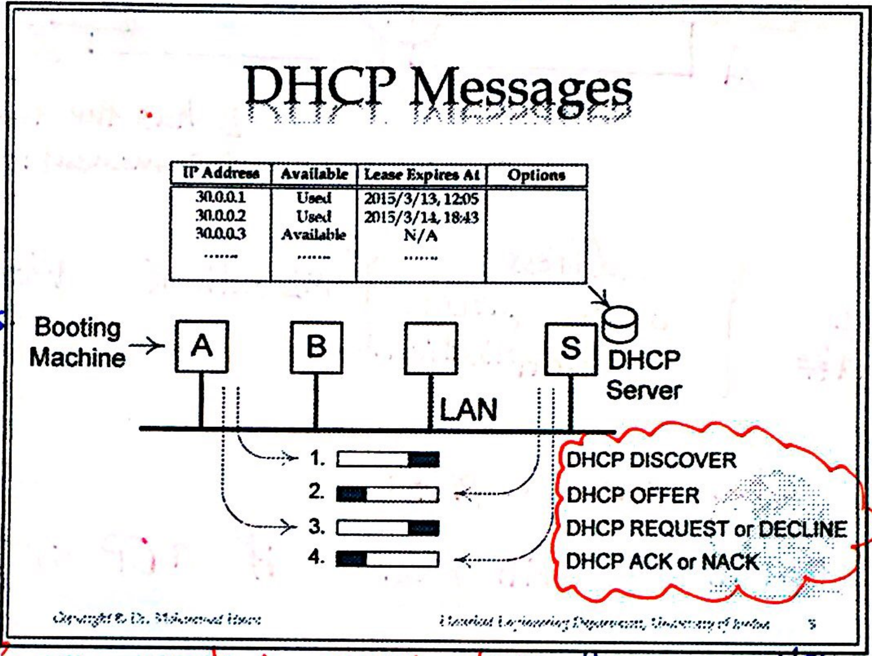
Dynamic Host Configuration Protocol (DHCP)

- A DHCP server supplies clients with the following IP configuration information:
  - A unique IP address for the host
  - Subnet mask
  - Default gateway
  - Other IP configuration parameters, such as the domain name.
- This happens through 4 sequence message exchange between the DHCP client and the DHCP server.

Scanned by CamScanner

* once the Lease expired you are forbidden to use the IP address.

Lease
↓ Renew lease Before it expires



DHCP Messages

IP Address	Available	Lease Expires At	Options
30.0.0.1	Used	2015/3/13, 12:05	
30.0.0.2	Used	2015/3/14, 18:43	
30.0.0.3	Available	N/A	
....	......	....	

DHCP DISCOVER
DHCP OFFER
DHCP REQUEST or DECLINE
DHCP ACK or NACK

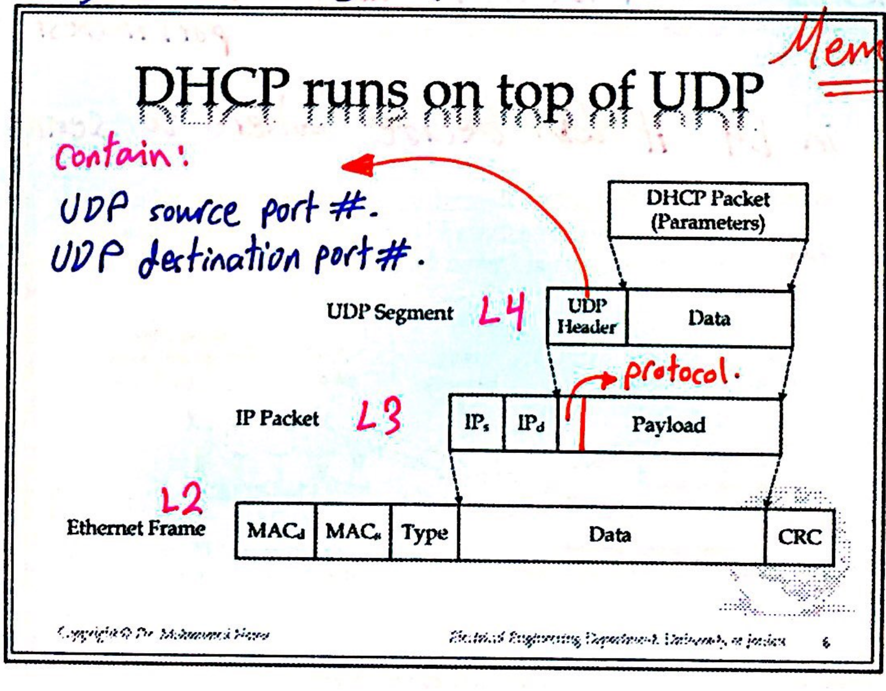
Copyright © Dr. Mohammed Hawa
Electrical Engineering Department, University of Jordan 5

4-main steps. (memorize).

* if we want to renew alease there is NO need to go through the 4-steps again (DHCP dicover & OFFER are not DONE agin).

Memorize.

for Booting:
4 msgs.
for Renew:
only 2 msgs.



DHCP runs on top of UDP

contain:
UDP source port #.
UDP destination port#.

Copyright © Dr. Mohammed Hawa
Electrical Engineering Department, University of Jordan 6

Scanned by CamScanner

For example: if we want to send from A → B

B has the following at the moment:

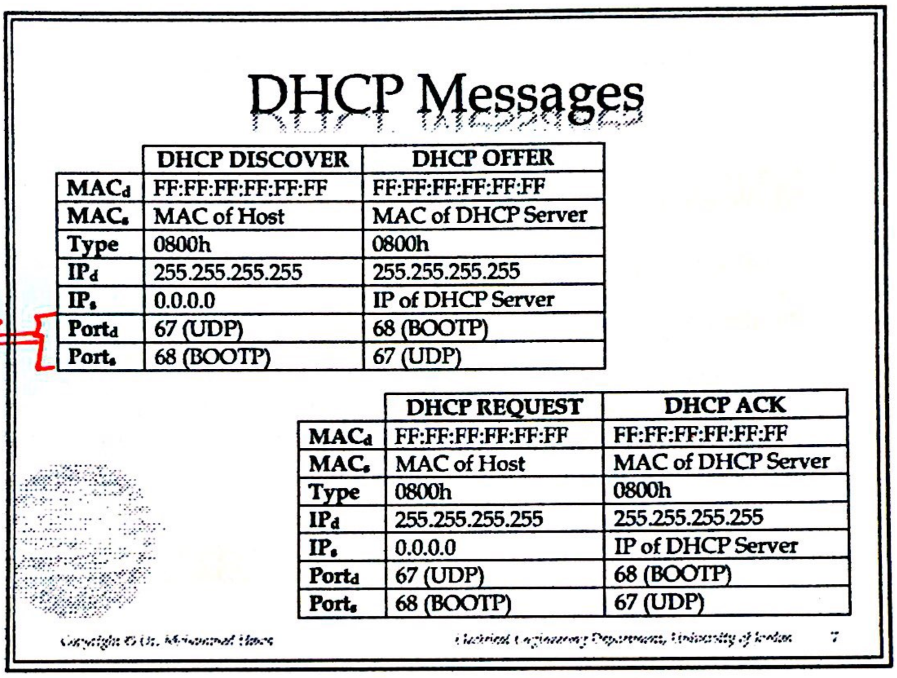
L4 port# { address of the process ≡ Application. { MS outlook Word Internet Explorer

so when send a pKt:

protocol in L3 will decide if TCP or UDP

Both TCP & UDP have : port # src ⇒ 16-bit
port # dest ⇒ 16-bit

so in L4 it will decide where to send the PKt.

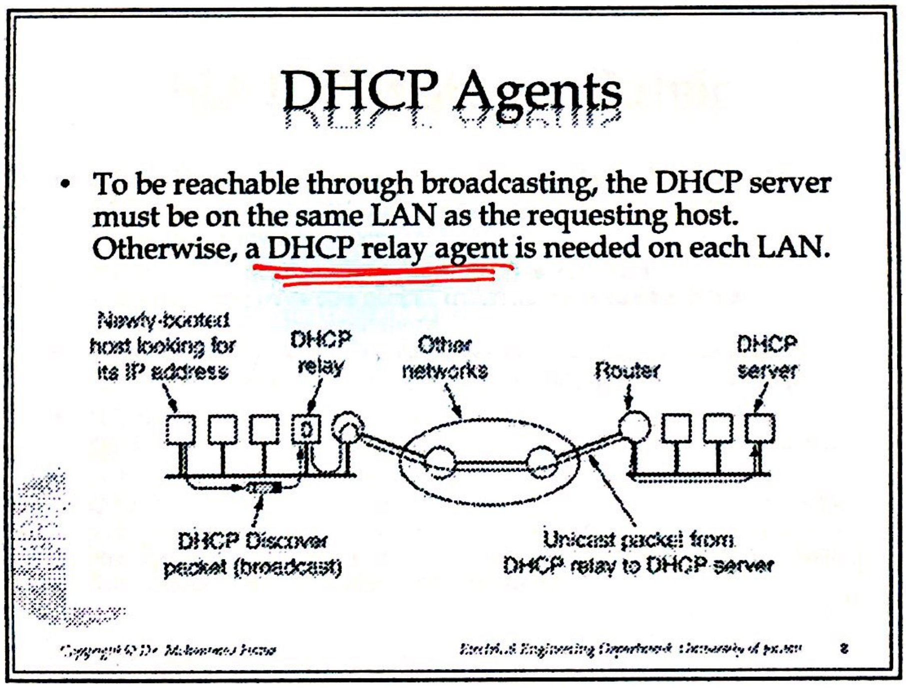


DHCP Messages

	DHCP DISCOVER	DHCP OFFER
MAC_d	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF
MAC_s	MAC of Host	MAC of DHCP Server
Type	0800h	0800h
IP_d	255.255.255.255	255.255.255.255
IP_s	0.0.0.0	IP of DHCP Server
$Port_d$	67 (UDP)	68 (BOOTP)
$Port_s$	68 (BOOTP)	67 (UDP)

Memorize ⟸

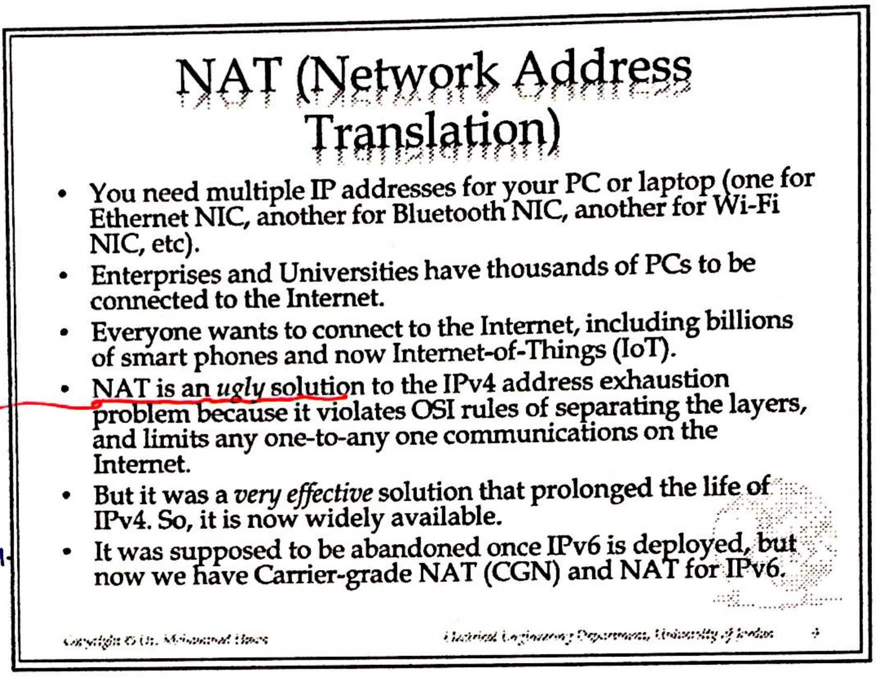
	DHCP REQUEST	DHCP ACK
MAC_d	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF
MAC_s	MAC of Host	MAC of DHCP Server
Type	0800h	0800h
IP_d	255.255.255.255	255.255.255.255
IP_s	0.0.0.0	IP of DHCP Server
$Port_d$	67 (UDP)	68 (BOOTP)
$Port_s$	68 (BOOTP)	67 (UDP)



DHCP Agents

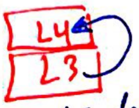
- To be reachable through broadcasting, the DHCP server must be on the same LAN as the requesting host. Otherwise, a DHCP relay agent is needed on each LAN.

Scanned by CamScanner

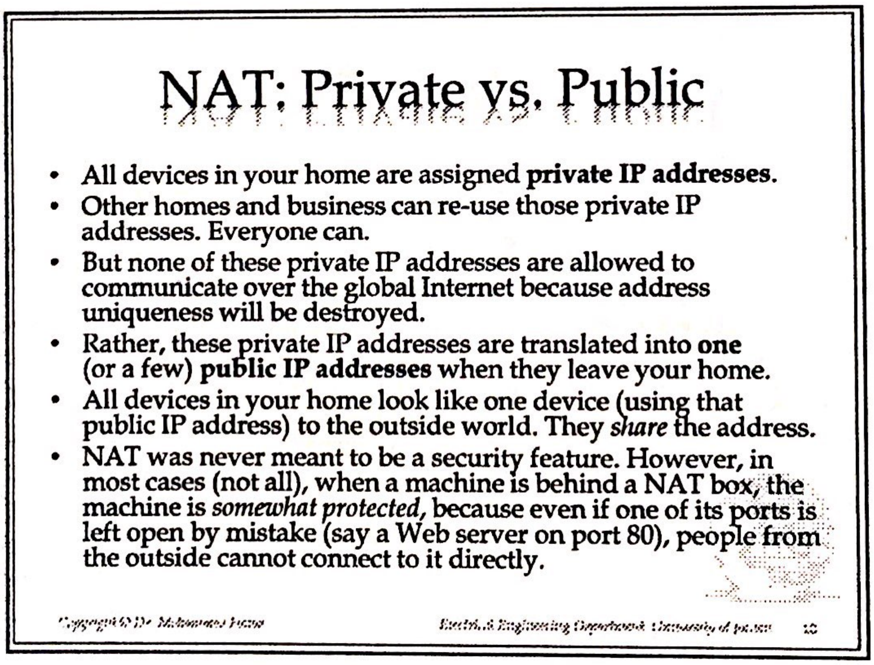


NAT (Network Address Translation)

- You need multiple IP addresses for your PC or laptop (one for Ethernet NIC, another for Bluetooth NIC, another for Wi-Fi NIC, etc).
- Enterprises and Universities have thousands of PCs to be connected to the Internet.
- Everyone wants to connect to the Internet, including billions of smart phones and now Internet-of-Things (IoT).
- NAT is an *ugly* solution to the IPv4 address exhaustion problem because it violates OSI rules of separating the layers, and limits any one-to-any one communications on the Internet.
- But it was a *very effective* solution that prolonged the life of IPv4. So, it is now widely available.
- It was supposed to be abandoned once IPv6 is deployed, but now we have Carrier-grade NAT (CGN) and NAT for IPv6.



L3 depend on L4 so NAT is an ugly solution.



NAT: Private vs. Public

- All devices in your home are assigned **private IP addresses.**
- Other homes and business can re-use those private IP addresses. Everyone can.
- But none of these private IP addresses are allowed to communicate over the global Internet because address uniqueness will be destroyed.
- Rather, these private IP addresses are translated into **one** (or a few) **public IP addresses** when they leave your home.
- All devices in your home look like one device (using that public IP address) to the outside world. They *share* the address.
- NAT was never meant to be a security feature. However, in most cases (not all), when a machine is behind a NAT box, the machine is *somewhat protected,* because even if one of its ports is left open by mistake (say a Web server on port 80), people from the outside cannot connect to it directly.

for U of J :

/27

$\Rightarrow 2^{32-27} = 2^5$

$= 32 - 2$ for reserved

$= 30$ Public IP addresses

private 4000 PC's.

Scanned by CamScanner

Private IP Addresses

Memorize:

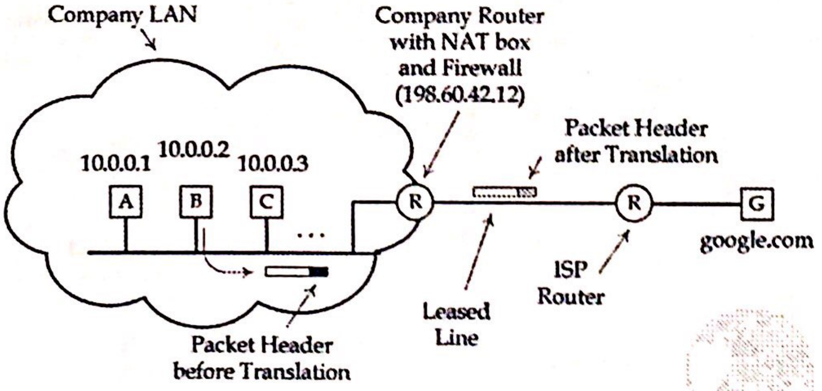
The three **reserved** ranges for **NAT** are:

Address Range	Private IP Addresses	Number of Addresses
10.0.0.0/8 class A	10.0.0.1 – 10.255.255.254	16,777,216 – 2
172.16.0.0/12 classless.	172.16.0.1 – 172.31.255.254	1,048,576 – 2
192.168.0.0/16 class B	192.168.0.1 – 192.168.255.254	65,536 – 2

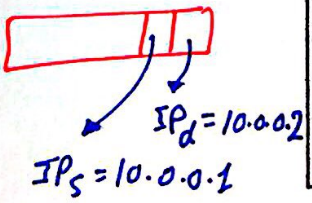
Be carful for 127.0.0.0/8 this is for loop back.

The range 10.0.0.0/8 is used by Windows machines by default.
The range 192.168.0.0/16 is used by default for many routers (*inside* the same box for Ethernet switches and Wi-Fi access points).

Example



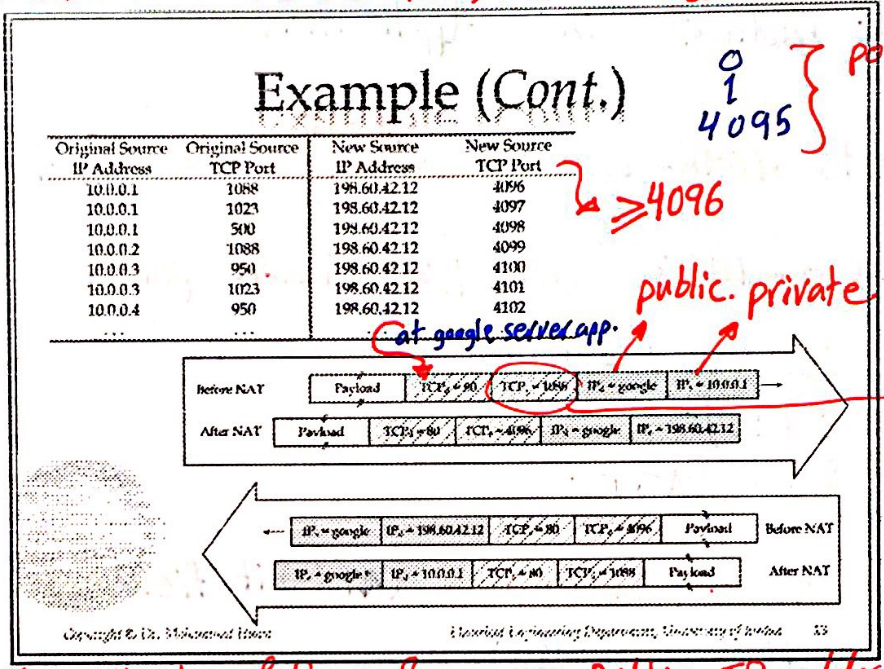
A to B



- A wants to send a PKt to google server.
- google sends back a PKt to A.

*What is the Job of L4 port#?
Identify application (process) on a Host.

.see this slide on the Website for better view.



Example (Cont.)

Original Source IP Address	Original Source TCP Port	New Source IP Address	New Source TCP Port
10.0.0.1	1088	198.60.42.12	4096
10.0.0.1	1023	198.60.42.12	4097
10.0.0.1	500	198.60.42.12	4098
10.0.0.2	1088	198.60.42.12	4099
10.0.0.3	950	198.60.42.12	4100
10.0.0.3	1023	198.60.42.12	4101
10.0.0.4	950	198.60.42.12	4102
...	...		

0
1
4095 } port #'s are reserved by the standard.

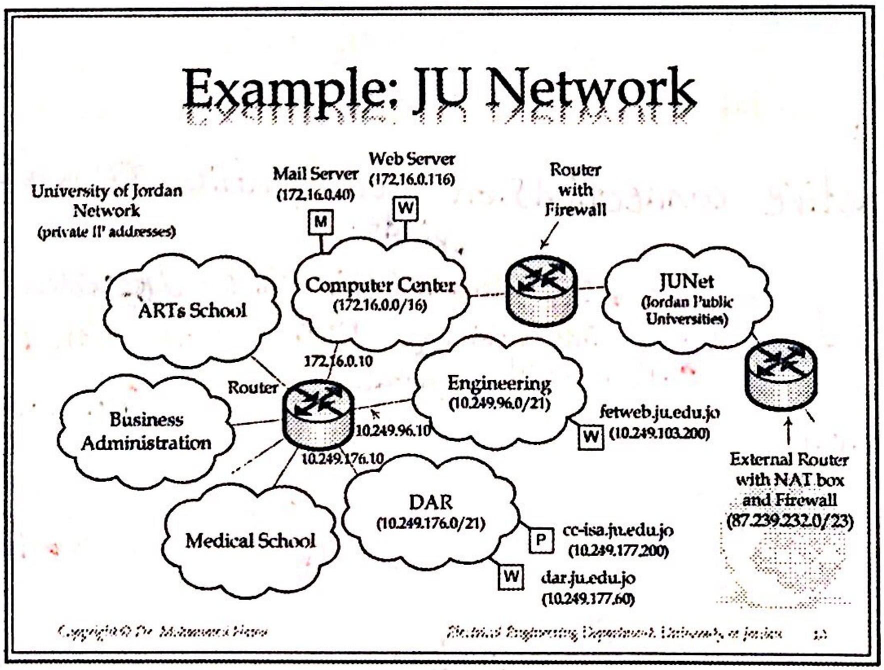
≥4096

public. private

at google server app.

TCP=1088 (Internet Explorer).

Max. Number of lines for one public IP address
= 65,536 − 4096 = max. # of active connections on one public IP address.



Example: JU Network

Scanned by CamScanner

* L4:

- The first 0 - 4095 ports are reserved To indicate the Application.

- ports 4096- ___ are Typically used By NAT.

- ports 0 - 1023 are Well-Known ports

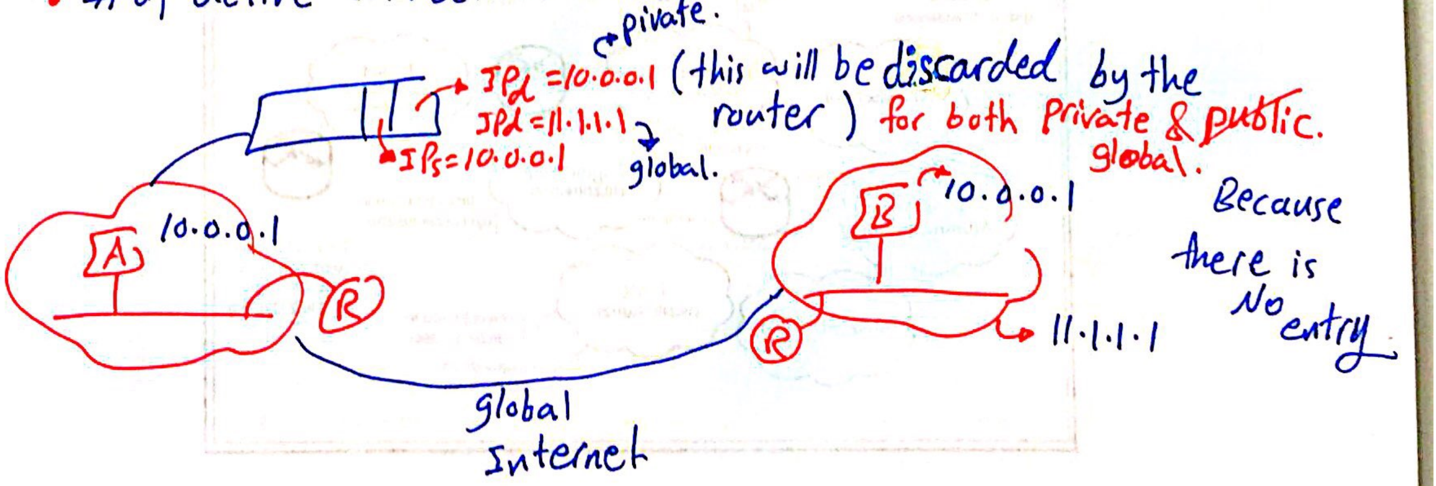
  80 : Web server.
  23 : ftp
  21 : SMTP.

* port # in TCP & UDP is a 16-bit field

  possible 0 - (2^{16}-1)
  0 - 65,535

* Limitation :

- # of active connections on one public IP address.



(this will be discarded by the router) for both Private & ~~public~~ global.

Because there is No entry.

Communication Networks

Spring 2017/2018

Dr. Mohammad HAWA

By: Mohammad
Abu Hashya.

* * *

Scanned by CamScanner

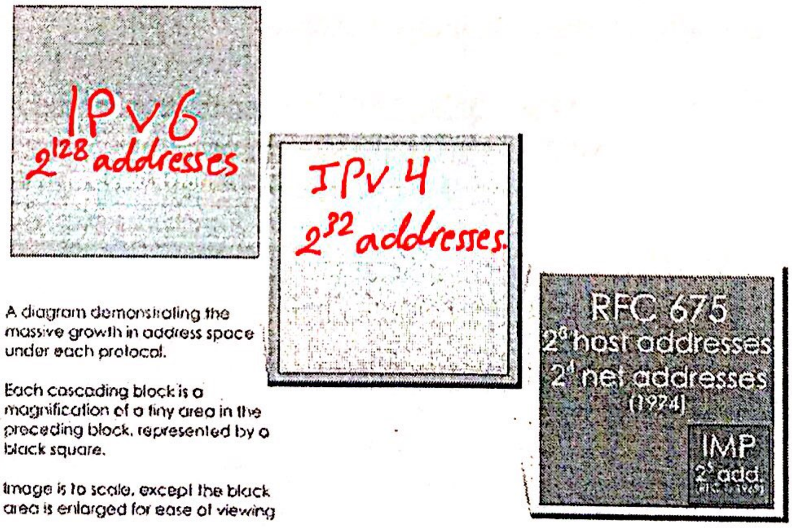
Lecture 15: Internet Protocol Version 6 (IPv6)

Dr. Mohammed Hawa
Electrical Engineering Department
University of Jordan

EE426: Communication Networks

IPv6 addressing

- IPv4 uses **32 bit = 4 bytes** addresses, IPv6 uses **128 bit = 16 bytes** addresses.



A diagram demonstrating the massive growth in address space under each protocol.

Each cascading block is a magnification of a tiny area in the preceding block, represented by a black square.

Image is to scale, except the black area is enlarged for ease of viewing

Scanned by CamScanner

this is the last update.

memorize

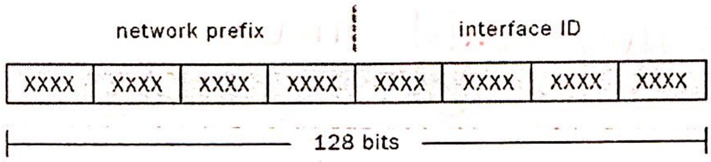
IPv6 is described in RFC 8200. The IPv6 addressing architecture is described in ~~RFC 3513 and RFC 4193~~. The 128-bit-long addresses are represented in hexadecimal format:

128 bits = xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx } 8 chunks = 8 16-bit words = 16 Bytes

16 bits

4 bits.

where xxxx is a 16-bit hex field. Notice that a total of 8 fields results in 16 bytes = 128 bits.



XXXX = 0000 through FFFF

0010 0001 1100

Examples:

it is Hexa NOT Decimal.

2001:0DB8:C003:0001:0000:0000:0000:F00D
2001:0db8:85a3:0000:0000:8a2e:0370:7334
2001:0db8:0000:0000:0000:0000:1428:57ab

Short-hand notation

Remove leading zeros; double-colon :: option *only once*:

2001:DB8:C003:1:0:0:0:F00D
2001:db8:85a3:0:0:8a2e:370:7334
2001:db8:0:0:0:0:1428:57ab

0000:0000:0000

since we have 5 chunks so there are 3 zero's missing chuncks.

2001:DB8:C003:1::F00D
2001:db8:85a3::8a2e:370:7334
2001:db8::1428:57ab
::1

Loop back.

Scanned by CamScanner

* write the following as short-hand Notation:

2001:0000:0000:0531:0000:0000:0000:5AAC

⇒ 2001:0:0:531::5AAC

(::) used only once.

2001::0531::5AAC (wrong).

since you will NOT know where the missing chunks are.

Scanned by CamScanner

just memorize the Types → Unicast/Anycast/Multicast.

Address Types

Unicast: one-to-one (global, link local, unique local, compatible)
Anycast: one-to-nearest (allocated from Unicast)
Multicast: one-to-many (also replaces broadcast addresses)

Don't memorize.

Type	Binary	Hex
Aggregatable Global Unicast	001	2000::/3
Link-Local Unicast	1111 1110 10	FE80::/10
Unique Local Unicast	1111 1100 1111 1101	FC00::/8 FD00::/8
Multicast	1111 1111	FF00::/8

Address Allocation & Aggregation

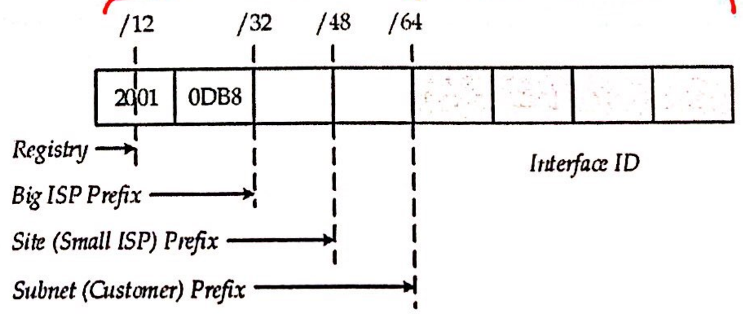
ICANN allocates address space to each regional registry:

- RIPE NCC (EMEA)
- APNIC (Asia Pacific)
- ARIN (North America)
- LACNIC (Latin America)
- AfriNIC (African Region)

host IP ddresses = 2^{64}.

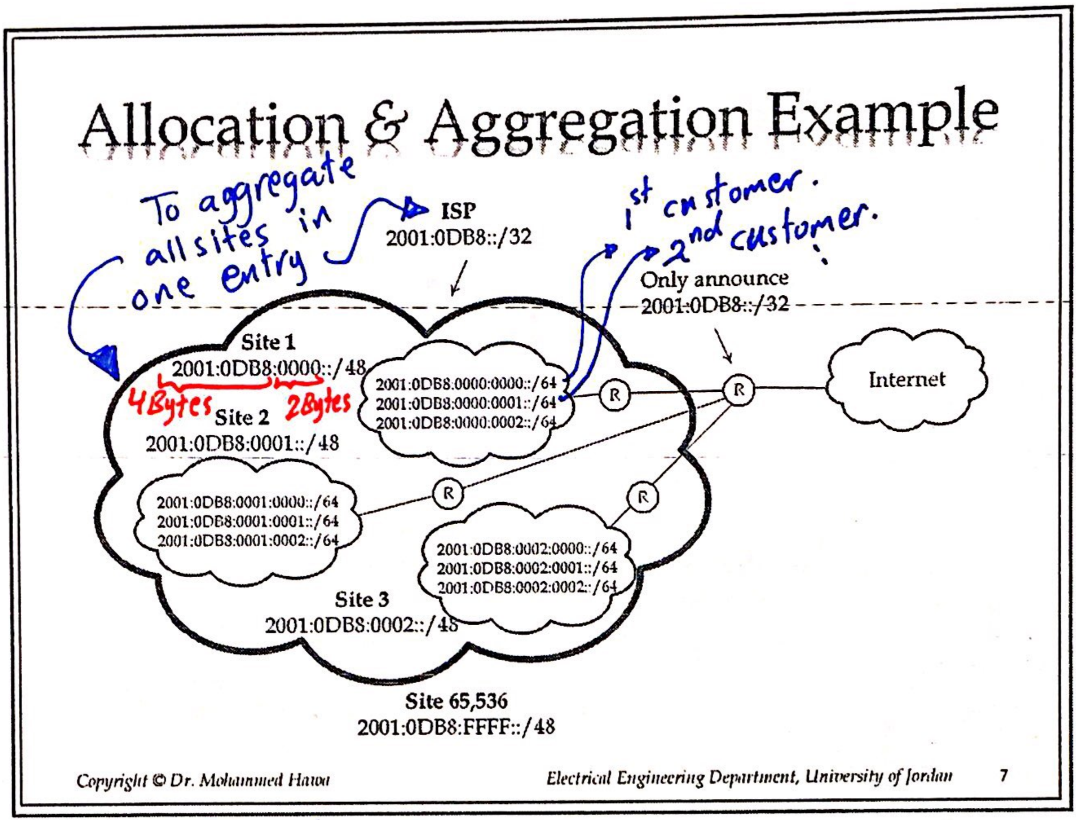
8 Bytes.

8 Bytes suffix host ID.



Scanned by CamScanner

5/2/2018



Allocation & Aggregation Example

To aggregate all sites in one entry

ISP
2001:0DB8::/32

1st customer.
2nd customer.
:

Only announce
2001:0DB8::/32

Site 1
2001:0DB8:0000::/48

4Bytes 2Bytes

2001:0DB8:0000:0000::/64
2001:0DB8:0000:0001::/64
2001:0DB8:0000:0002::/64

Site 2
2001:0DB8:0001::/48

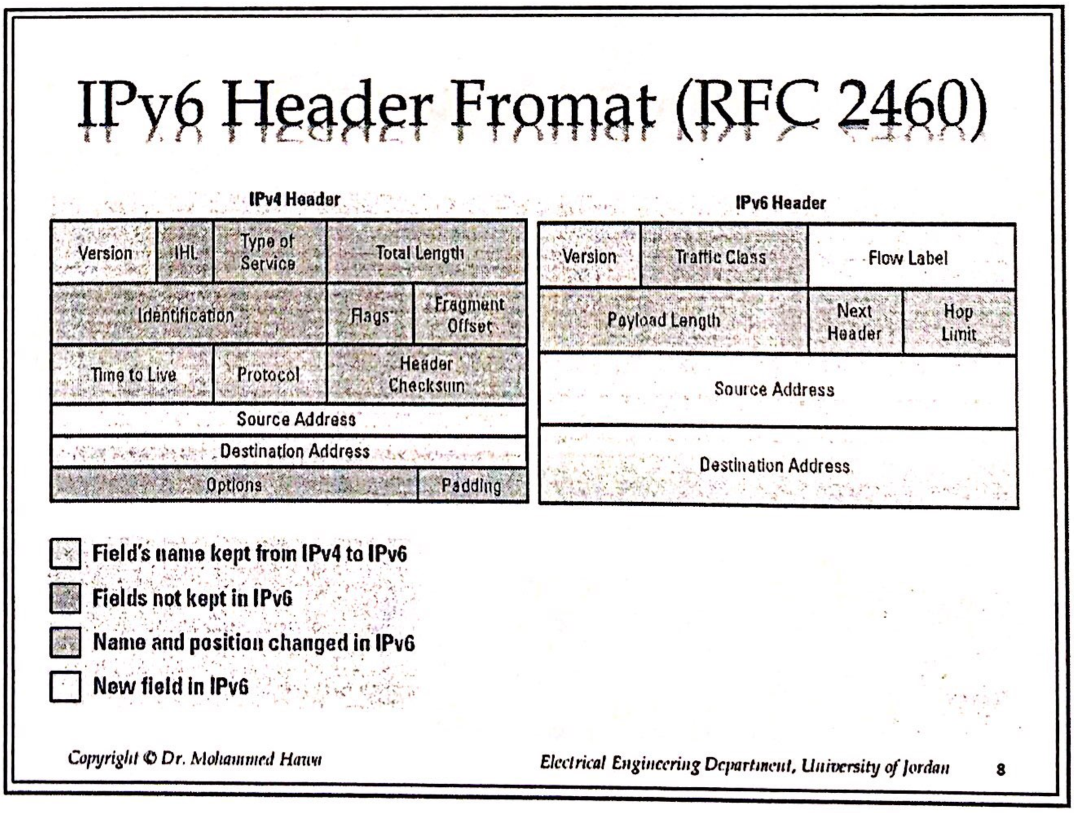
2001:0DB8:0001:0000::/64
2001:0DB8:0001:0001::/64
2001:0DB8:0001:0002::/64

2001:0DB8:0002:0000::/64
2001:0DB8:0002:0001::/64
2001:0DB8:0002:0002::/64

Site 3
2001:0DB8:0002::/48

Site 65,536
2001:0DB8:FFFF::/48

Next slides NOT INCLUDED.



IPv6 Header Fromat (RFC 2460)

IPv4 Header

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

IPv6 Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

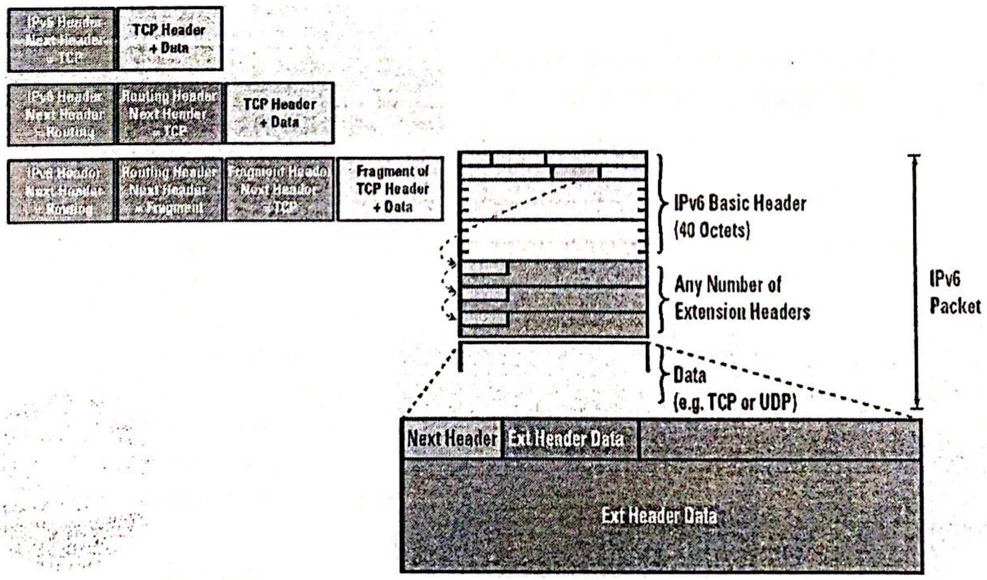
- ▨ Field's name kept from IPv4 to IPv6
- ■ Fields not kept in IPv6
- ▩ Name and position changed in IPv6
- ☐ New field in IPv6

Scanned by CamScanner

Changes to the Heade

- Revised
  - Time To Live -> Hop Limit
  - Protocol -> Next Header
  - Precedence and TOS -> Traffic class
  - Addresses increased 32 bits -> 128 bits
- Extended
  - Flow Label field added.
- Removed:
  - Header length field eliminated
  - Header checksum eliminated
- Streamlined (using the idea of extended headers):
  - Fragmentation fields moved out of base header
  - IP options moved out of base header
  - Length field excludes IPv6 header
  - Alignment changed from 32 to 64 bits

Extended Headers



Scanned by CamScanner

Extended Headers (*Cont.*)

Table 1. Summary of Header Types and Values

Header Type	Next Header Value
Hop-by-Hop Options Header	0
Destination Option Header	60
Routing Header	43
Fragment Header	44
Authentication Header (RFC 1826) and ESP Header (RFC 1827)	51
Upper-Layer Header	6 (TCP) 17 (UDP)
Mobility Header	135

Extended Headers (*Cont.*)

- When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:
  - IPv6 header
  - Hop-by-hop options header
  - Destination options header (routing header associations)
  - Routing header
  - Fragment header
  - Authentication header
  - Encapsulating security payload header
  - Destination options header (options processed by final destination)
  - Upper-layer header

Scanned by CamScanner