Security - Networking

Note Title 2/24/2011

Announcements

- Extension for Lab 2 - due Friday
- Office hours tomorrow & Monday: 1:30-3:30
- Review sheet for midterm posted tonight
- Midterm in one week

Goals for today

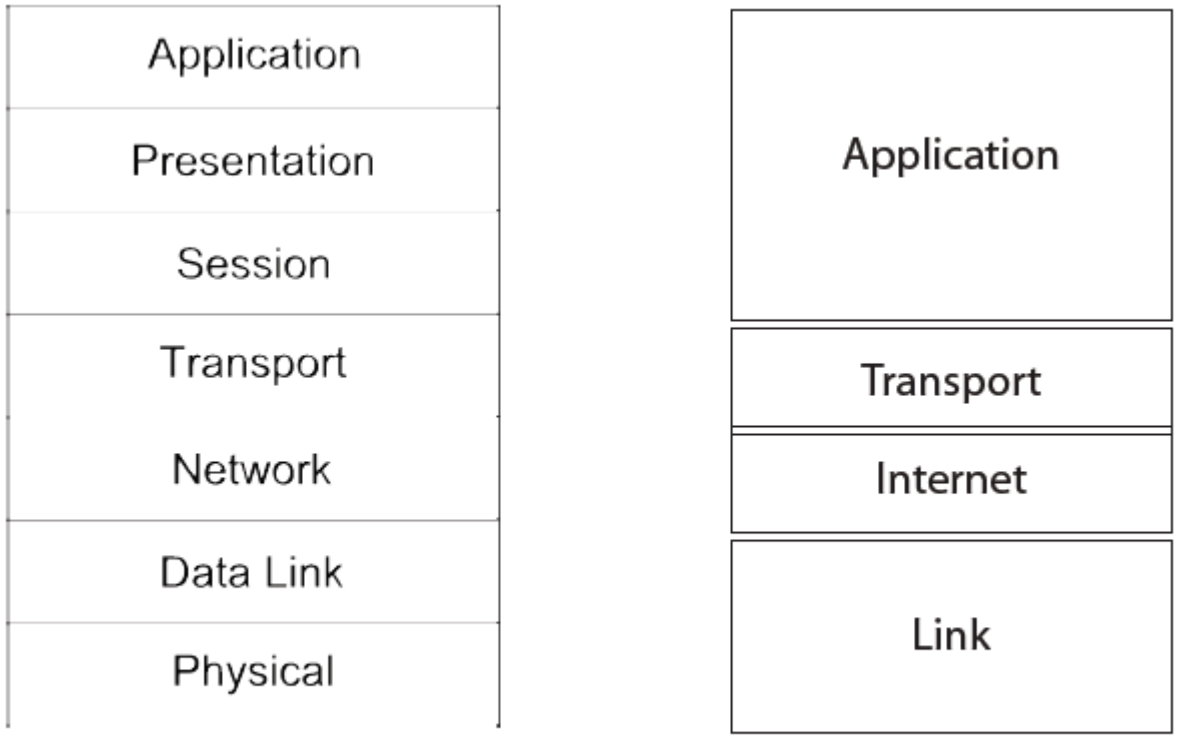
Networking Concepts:

- network topologies
- hubs & switches
- ARP
- Network sniffing: tcpdump
- Basic Attack: SYN floods

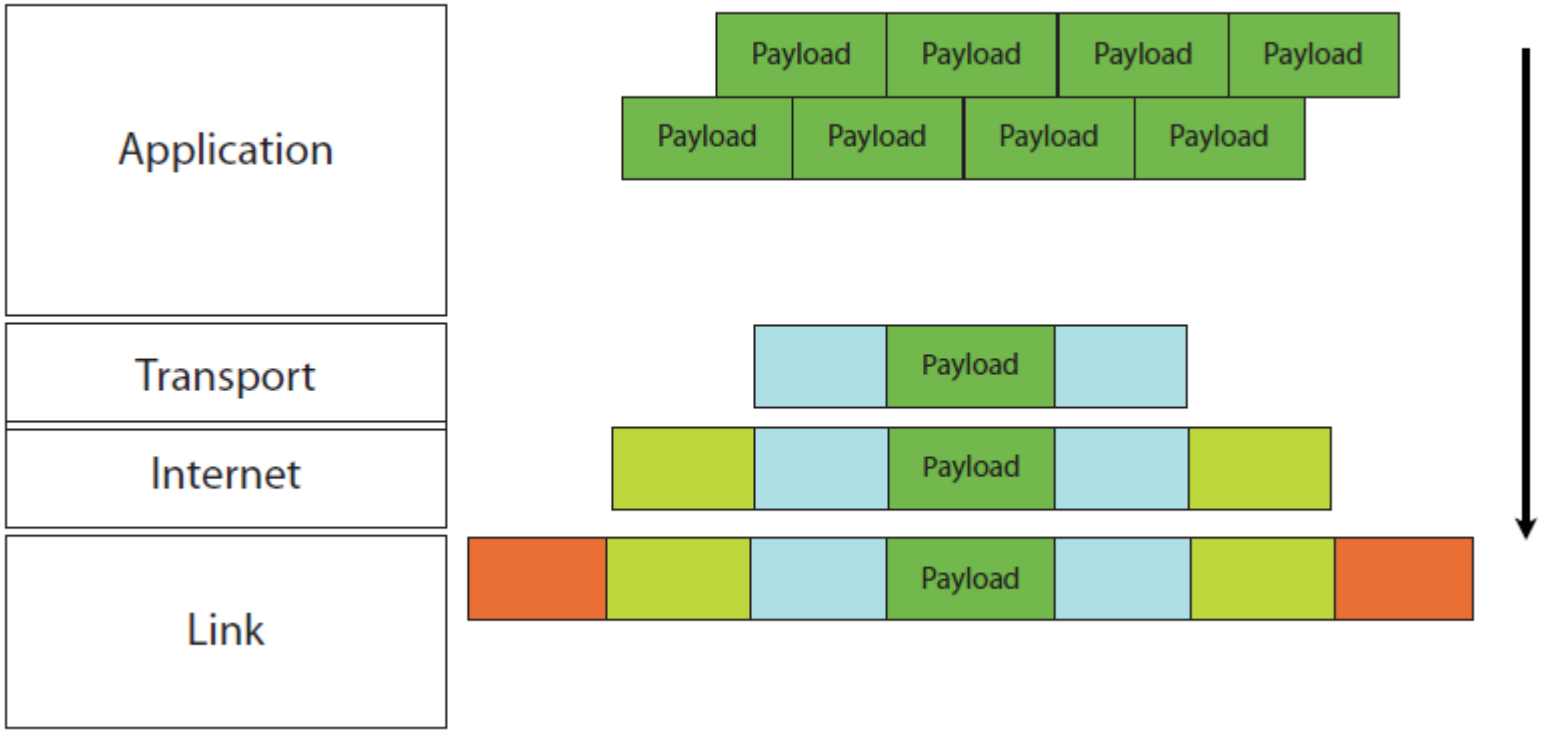
} next time

SYN

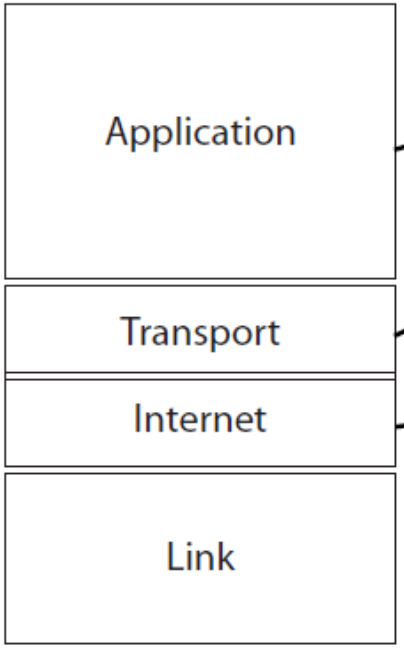
Recall: Internet Protocol Suite (TCP/IP)



Recall: Packets



More Detail:



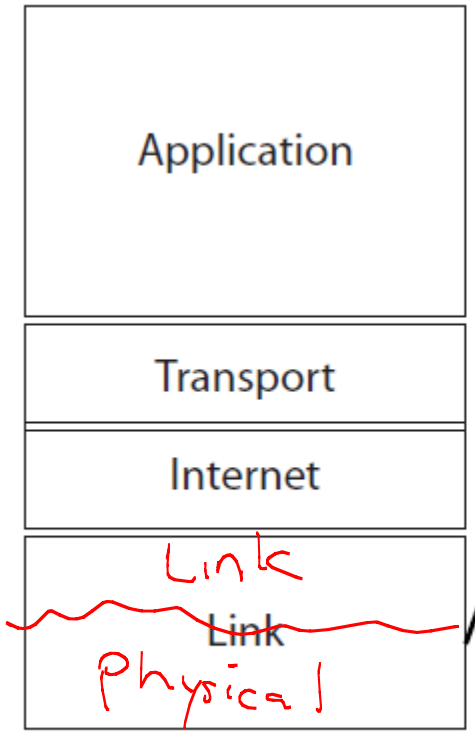
TCP/IP

Determines how an application should use the network.

Handles details of data transmission at the end-points of communication.

Expresses how packets should be forwarded and how packets should be addressed (also called **Network Layer**)

Lowest Level:



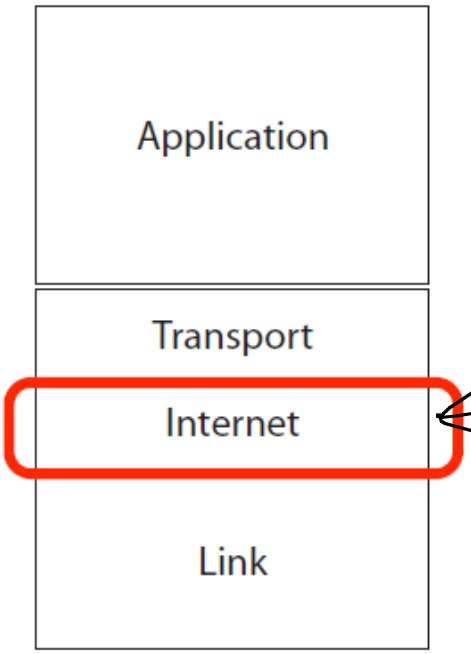
TCP/IP

Sometimes divided into Link Layer and Physical Layer.

Link Layer: Provides for synchronization and transfer of information. Defines how physical machines address each other.

Physical Layer: Defines electrical aspects of sending signals along a wire or wirelessly. Also addresses switch and router hardware.

Let's focus our attention:



TCP/IP

- Expresses how packets should be forwarded and how packets should be addressed (also called **Network Layer**)

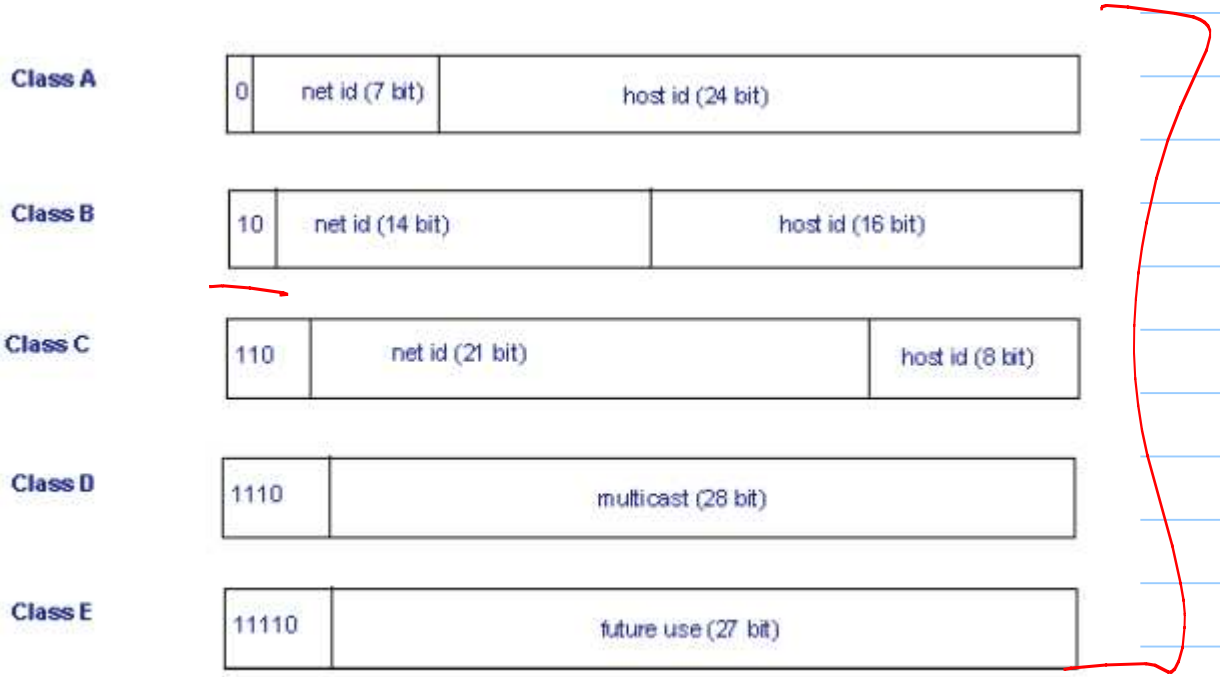
IPv4 Packet

- Divided into 32-bit pieces
- Headers (usually) are 5-32 bits long, with data at the end

bit offset	0–3	4–7	8–13	14-15	16–18	19–31
0	Version	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

Network Layer in IPv4 (cont.)

IP adresses are subdivided, since things must stay unambiguous



Example:

Consider this address:

128 64 32 4 1 128 64 8 1

10001000 11100101 11001001 0001000

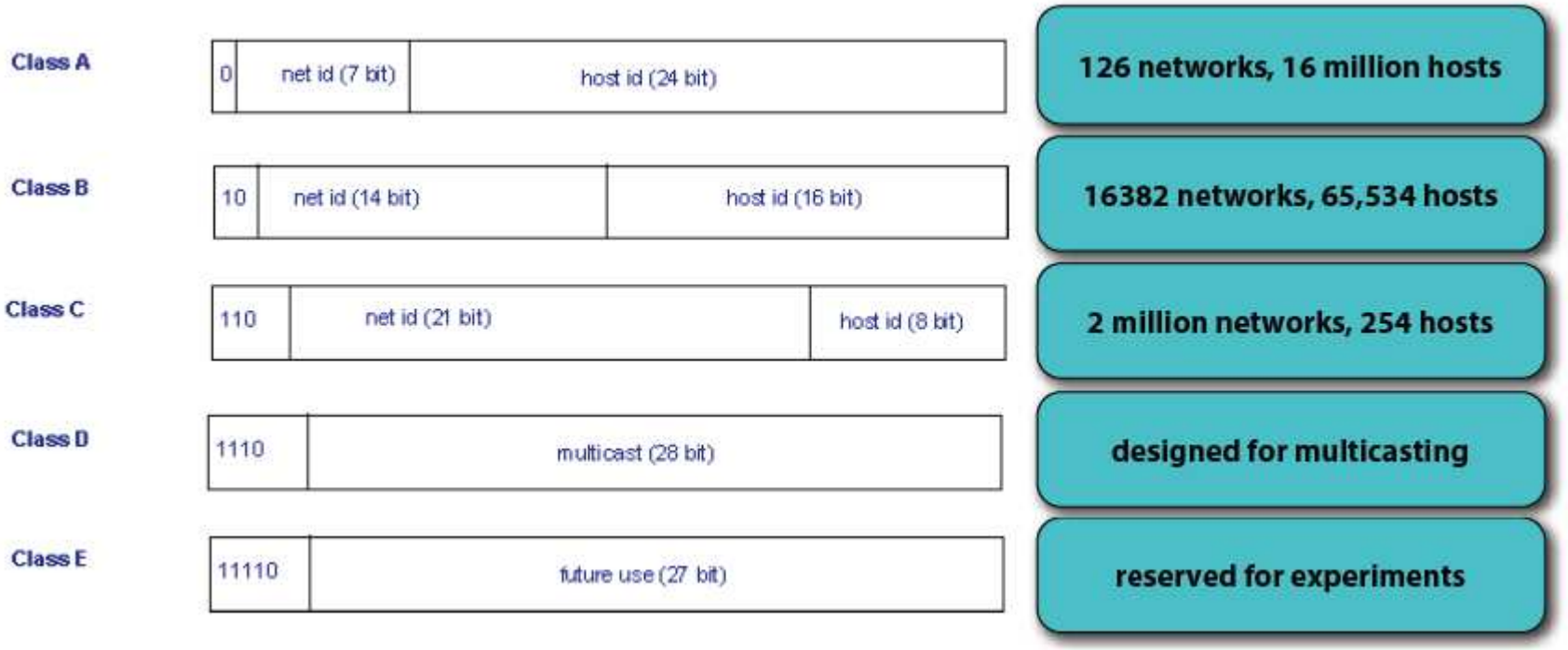
Class? B

What IP address?

136. 229. 205. 8

2^{32} possibilities

Total Counts



Conclusion: Out of IP addresses.

IPv4 issues: Out of Space!

- Designed in 1981 (out of date - before PCs)
- Solutions:
  - IPv6
  - NAT
  - Subnetting

NAT: Network Address Translation Protocol

A router stands between a private network and the outside world.

Maps internal IP addresses to a single IP address and port which is visible to the outside world.

Pros: Lets you by 1 IP address.

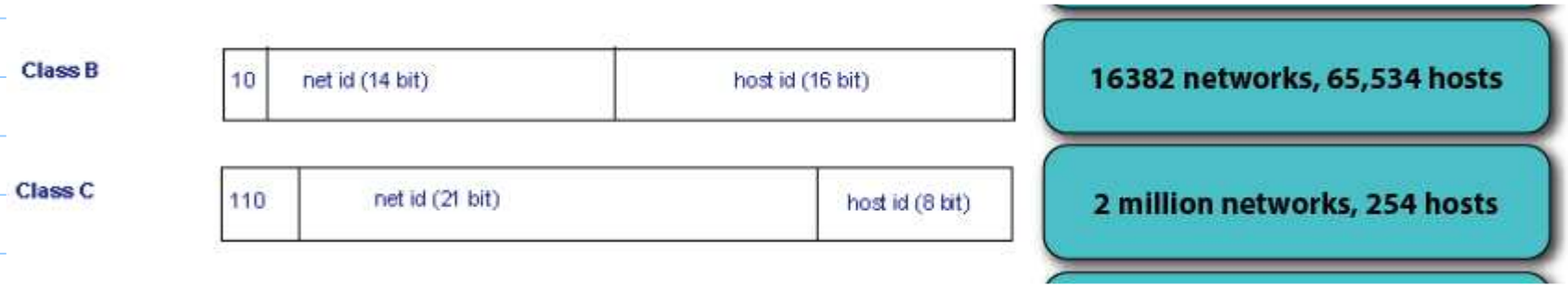
Cons: Traffic load.

② IPv6

- Invented in 1998
- Allows 128-bit addresses
- Deployment is very slow

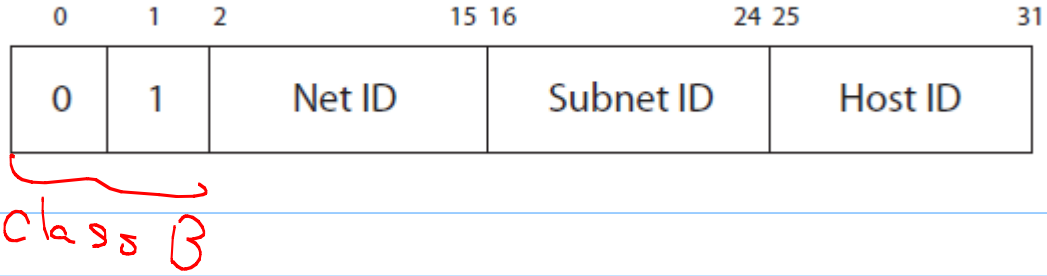
(3) Subnetting

There is quite a 'jump' between class B size and class C size:



People grab class B, even when it isn't necessary.

Subnetting: the solution



Divide host id into subnet ID and host ID.

Now, 512 subnets and 128 hosts.

But how is this implemented?

Every computer will get a subnet mask,
eg 255.255.255.0

11111111.11111111.11111111.00000000

As well as an IP address:

IP address: 128.96.34.15

10000000.01100000.00100010.00001111

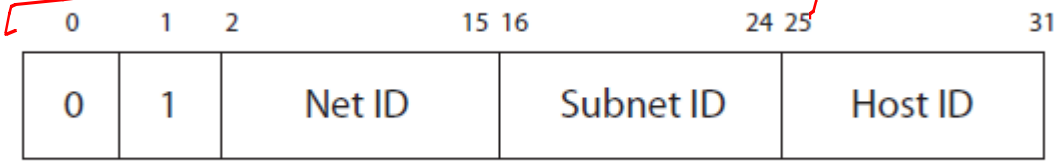
Take the bitwise AND of these:

255. 255. 255. 0

11111111.11111111.11111111.00000000

128. 96. 34. 15

10000000.01100000.00100010.00001111



These are useful when a large company or institution needs to subdivide into smaller networks.

Most will only own 1 class B address and will divide it up internally.

Note: Subnets need to be nearby for efficient routing!

LAN : Local Area Network

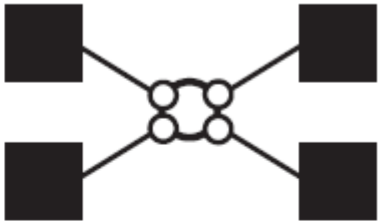
A LAN is a "small interconnection infrastructure that typically uses a shared transmission medium".

From Computer and Communication Networks by N. Mir

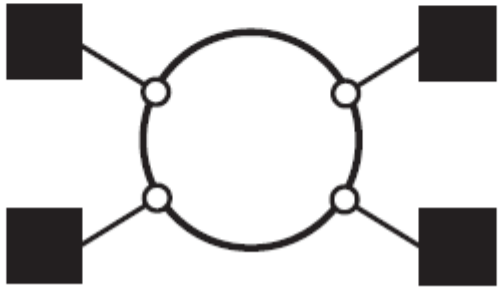
Note: A single LAN may contain thousands of machines, each separately managed by switches and routers.

LAN Topologies

Bus Configuration



Star Configuration



Ring Configuration

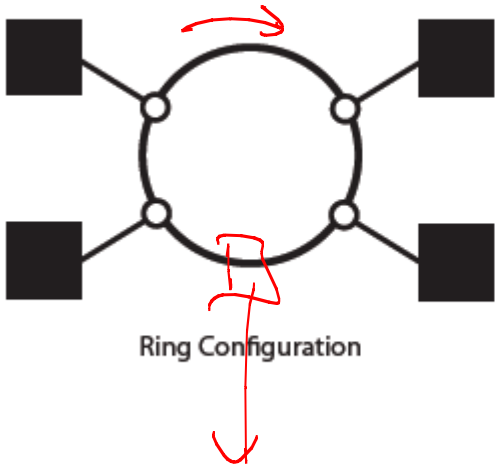
Bus Configuration

Bus Configuration

Bus Configuration:

Transmission from user is propagated on the bus in both directions; all users receive the frame.

Ring Configuration



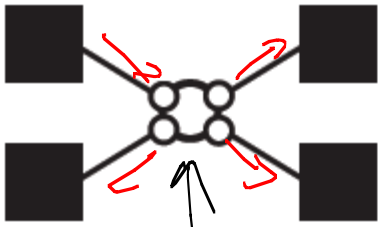
Ring Configuration

Ring Configuration:

Uses repeaters, depicted as small circles.

Sender forwards frame to repeater. Frame is forwarded by repeaters until it is repeated to destination. Frame is repeated until sender sees it again.

Star Configuration



Star Configuration

Star Configuration:

Center of star is a multi-port hub.

When a frame is received, it is sent to all users in the LAN.

Single hub

Note:

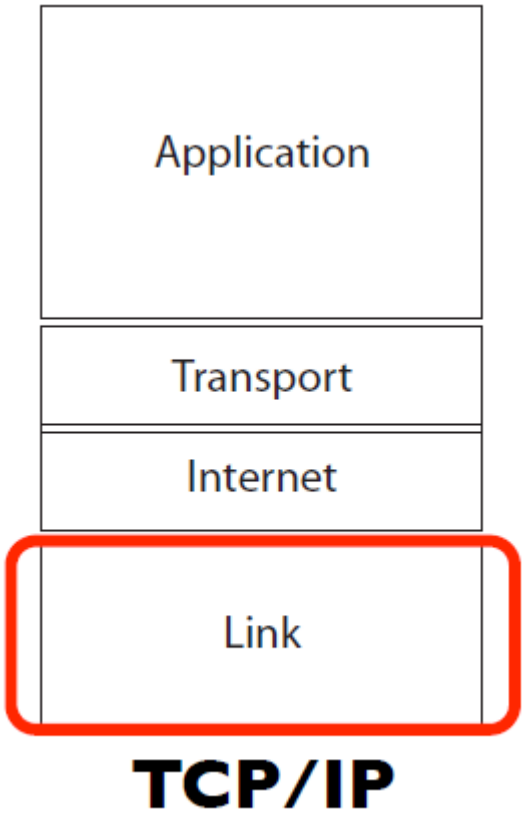
None of these have any security built in!

Any (& every) computer may see every packet.

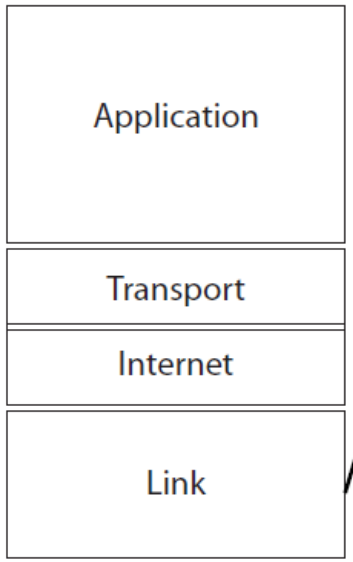
Security

How can we prevent network eavesdropping?

Solution lies in the link layer.



Dividing the link layer:



TCP/IP

Sometimes the Link Layer is divided further into:

Logical Link Layer: Defines how physical machines address each other. Determines the mechanism needed to transmit the frame.

Medium Access Control Layer: Provides the mechanism specific to the medium of transmission for synchronization and transfer of information.

Physical Layer: Defines electrical aspects of sending signals along a wire or wirelessly. Also addresses switch and router hardware.

MAC

- The MAC header contains the MAC address of the source & destination.

(MAC address & ethernet addresses are interchangable)

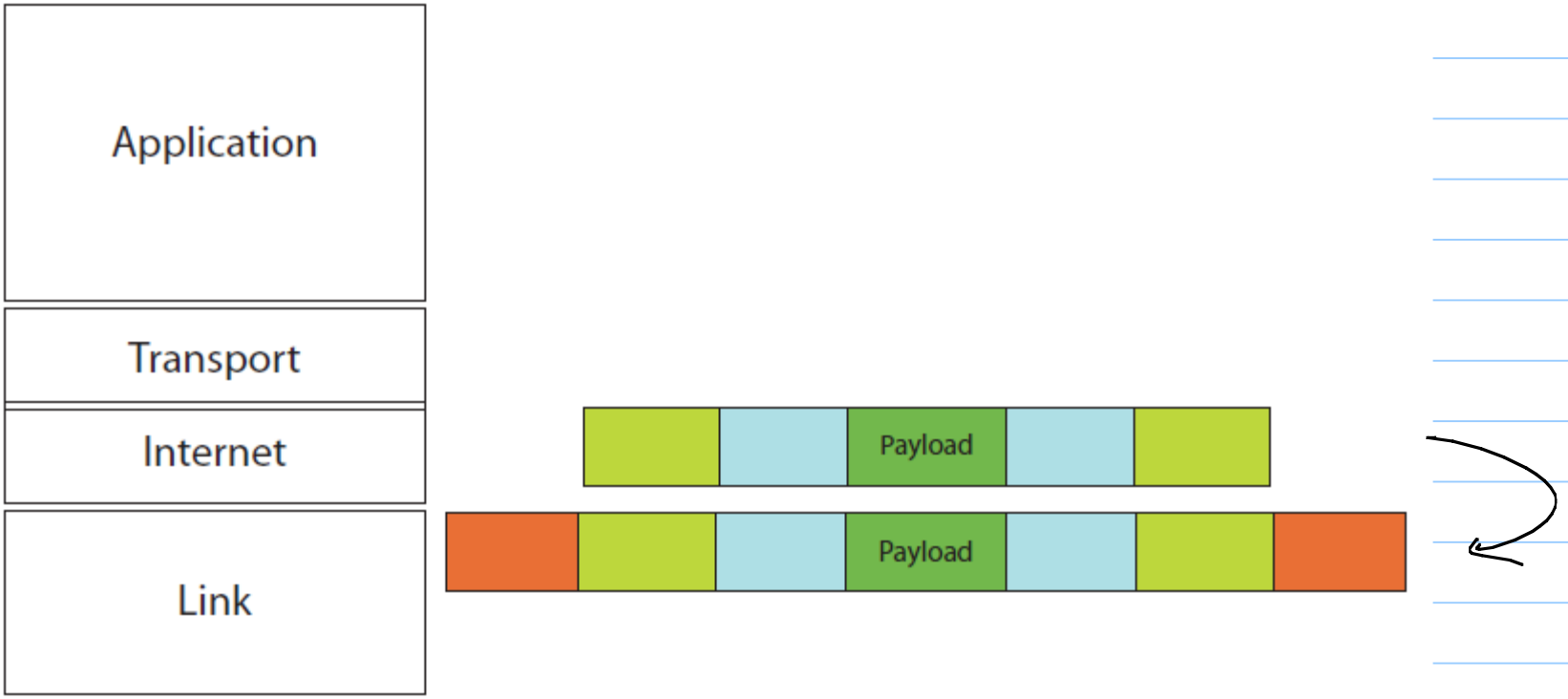
Ex:

00-40-33-25-85-BB

or

00:40:33:25:85:BB

IP to MAC



Any IP must be translated to a MAC address.

ARP: Address Resolution Protocol

Every node in the network stores an ARP table.

Example:

IP Address	Ethernet Address
223.1.2.1	08-00-39-00-25-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Example taken from RFC1180 "A TCP/IP Tutorial"
by T. Socolofsky and C. Kale. January 1991.

On a Linux machine, type:

```
$ arp -a
```

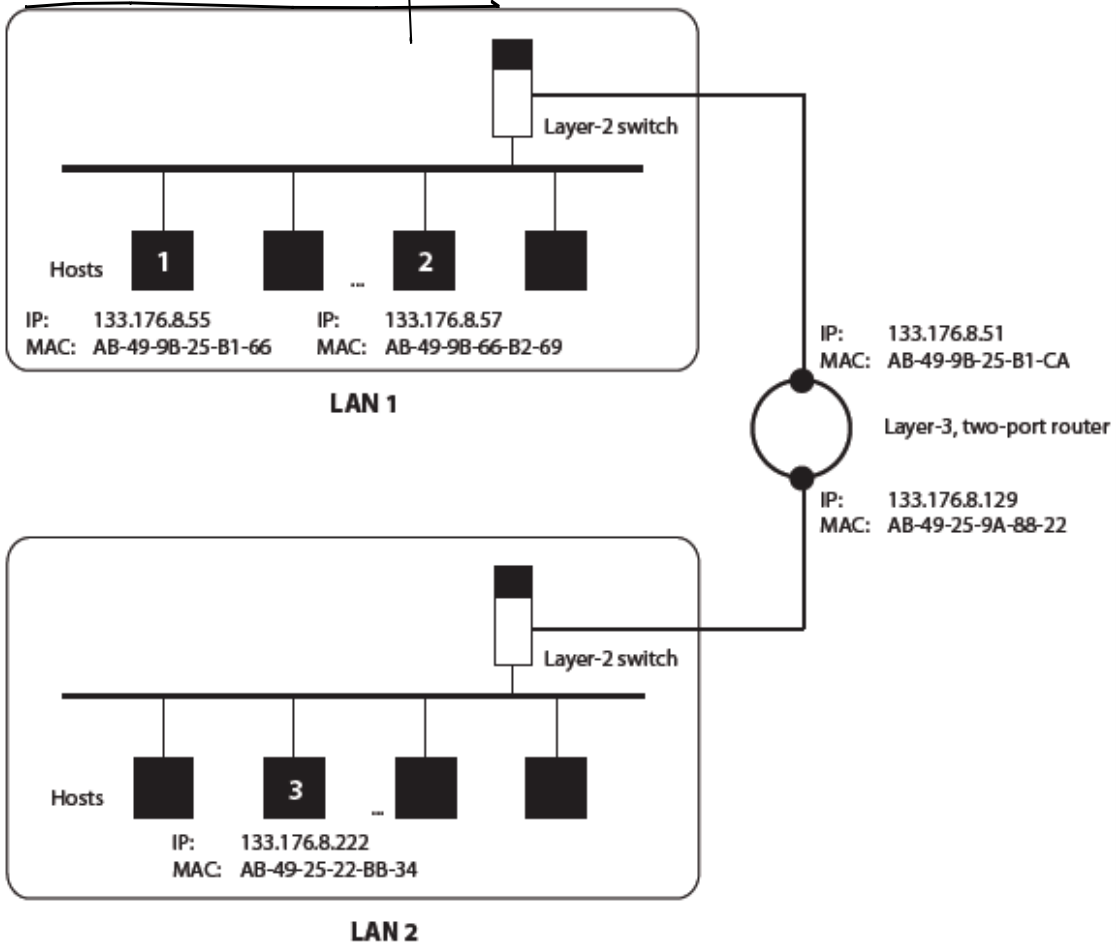
to view.

(Go through network info in other systems)

Output example:

```
? (10.16.0.1) at 0:0:c:7:ac:0 on en2 [ethernet]
```

An example

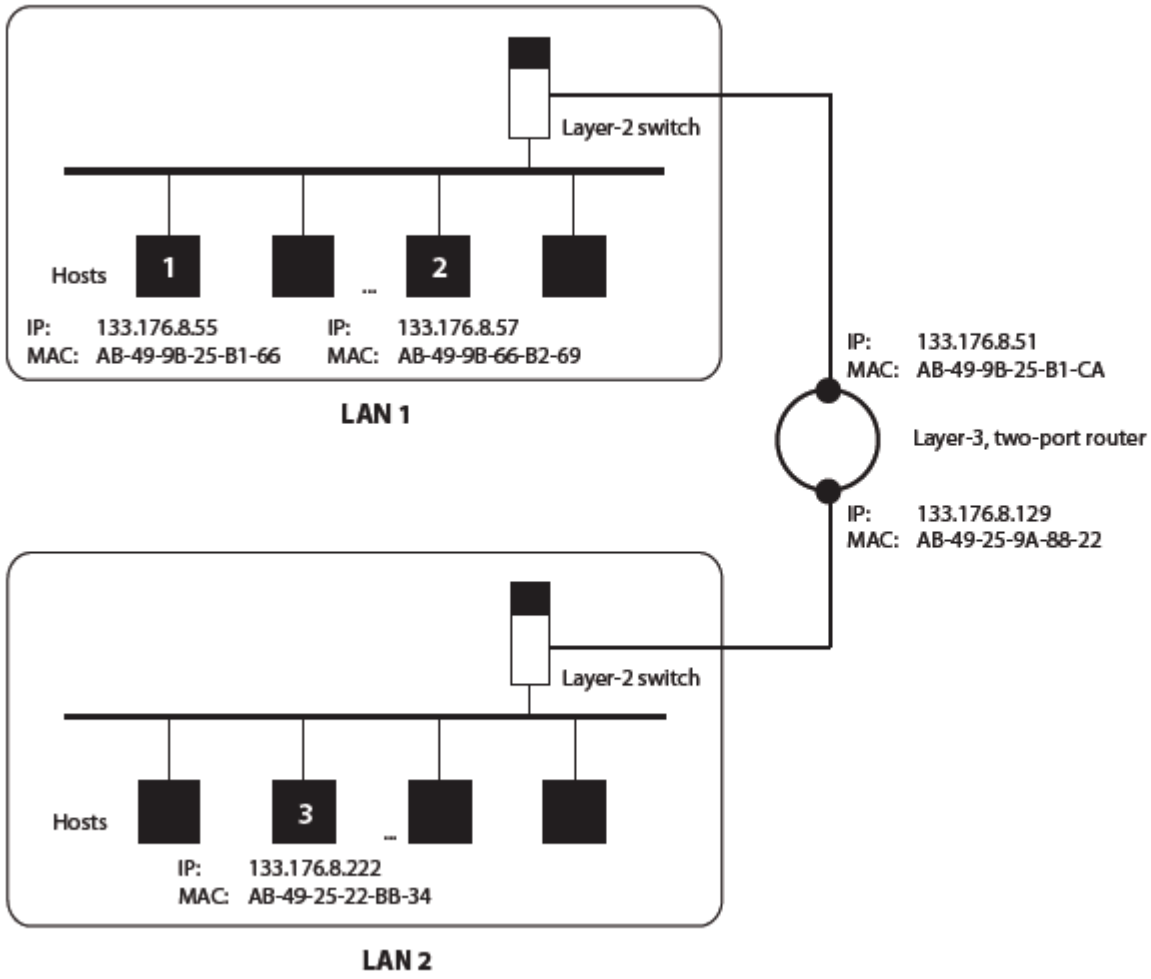


Scenario A
Host 1 transmits to Host 2

No entry in table.

Host 1 broadcasts an ARP request on LAN 1.

"If your IP is 133.176.8.57, then reply with your MAC address."

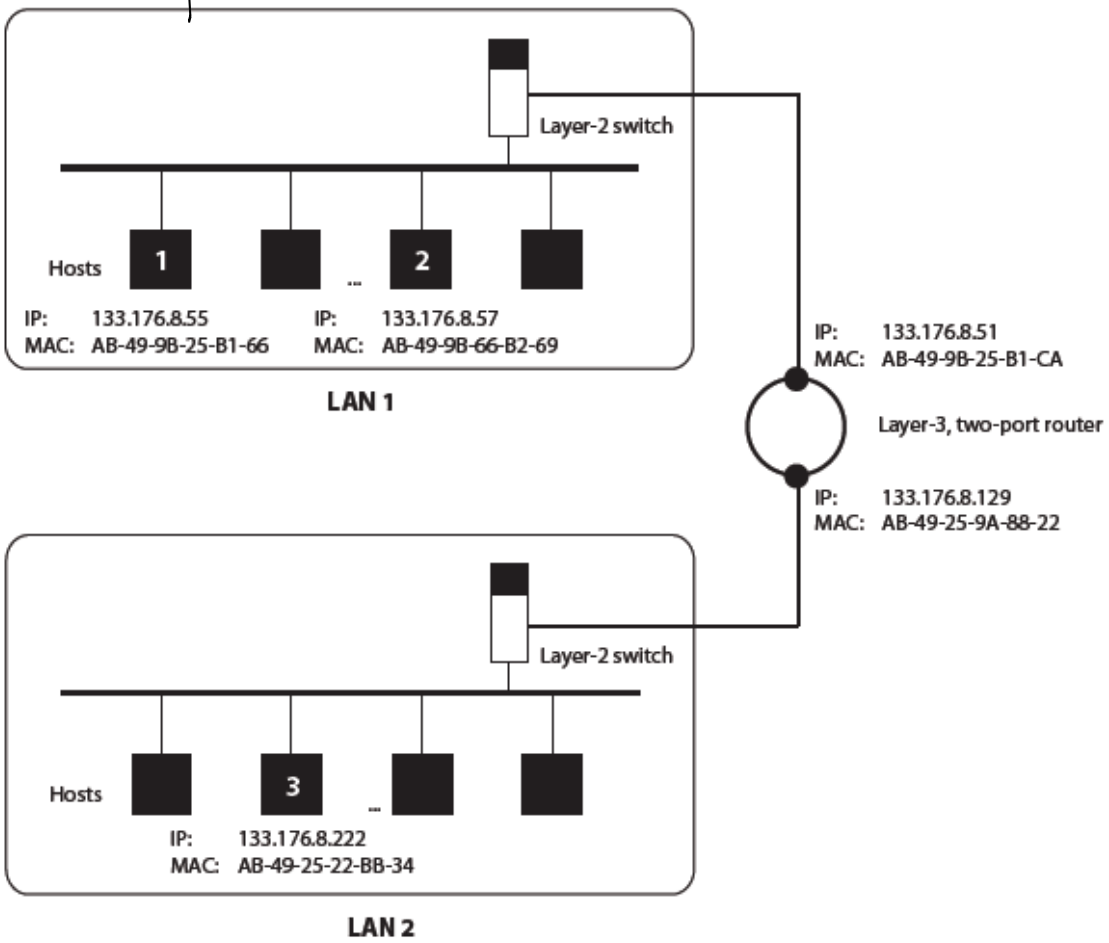


Scenario A
Host 1 transmits to Host 2

Host 2 replies with
AB-49-9B-66-B2-69

Entry is added to ARP table.
Transmission proceeds.

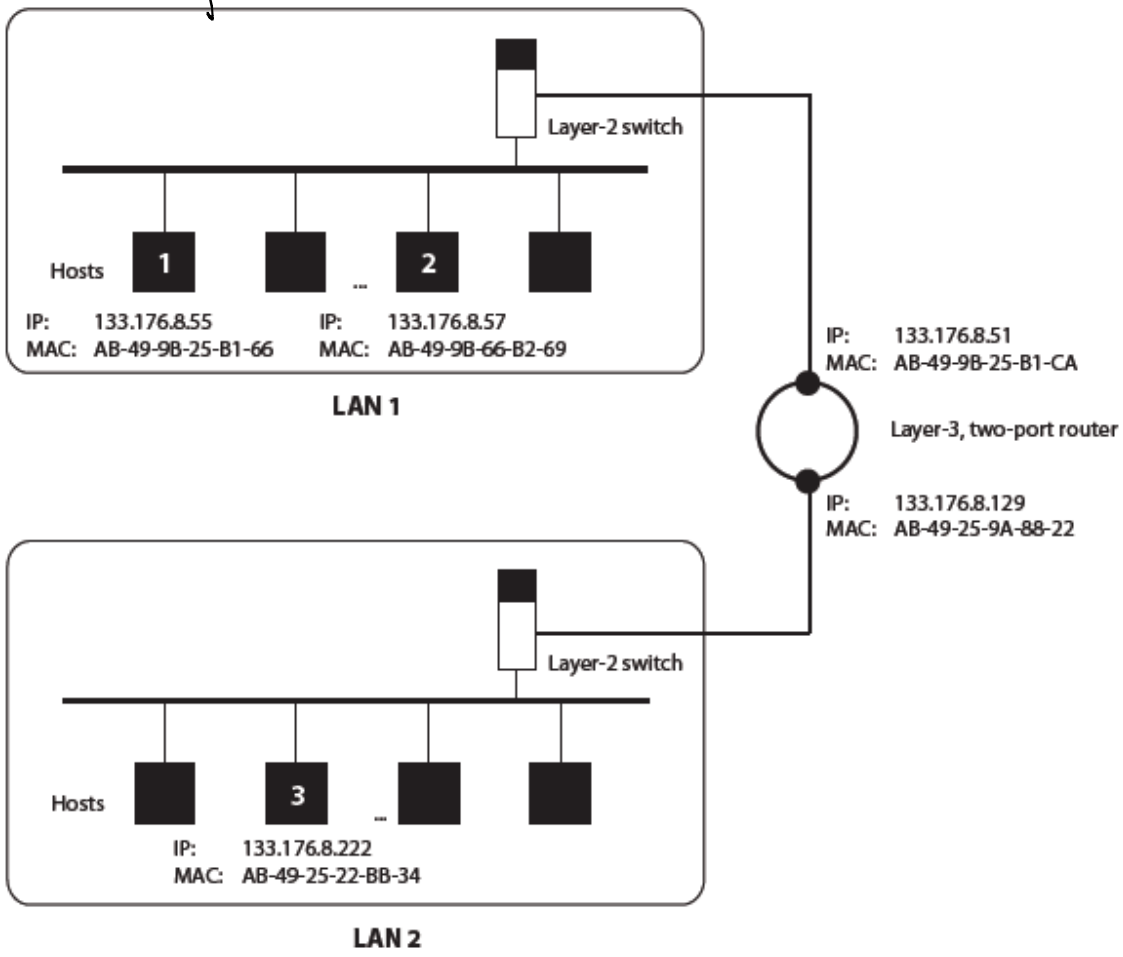
Example 2:



Scenario B
Host 1 transmits to Host 2 again

Entry is available in the ARP table. Just use that.

Example 3

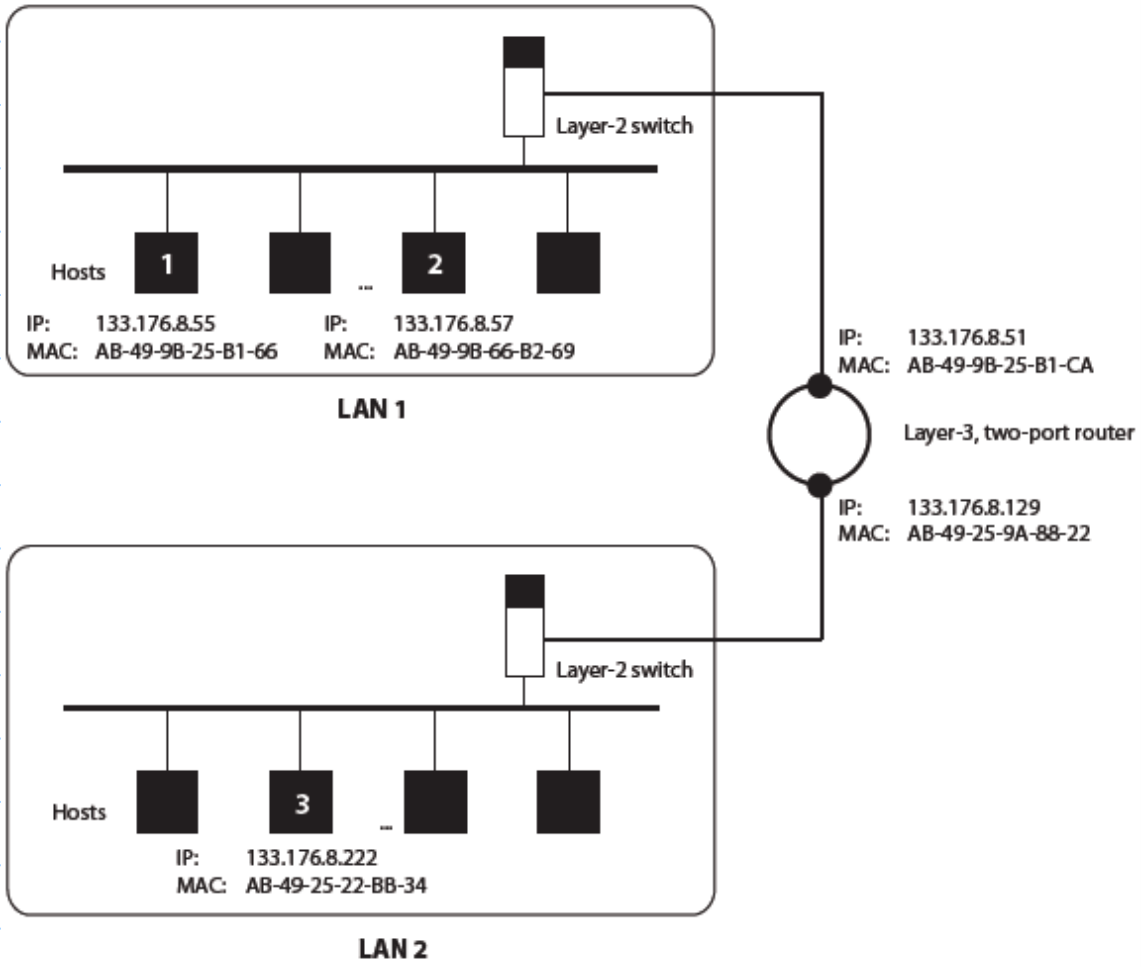


Scenario C
Host 1 transmits to Host 3

No entry in table.

Host 1 broadcasts an ARP request on LAN 1.

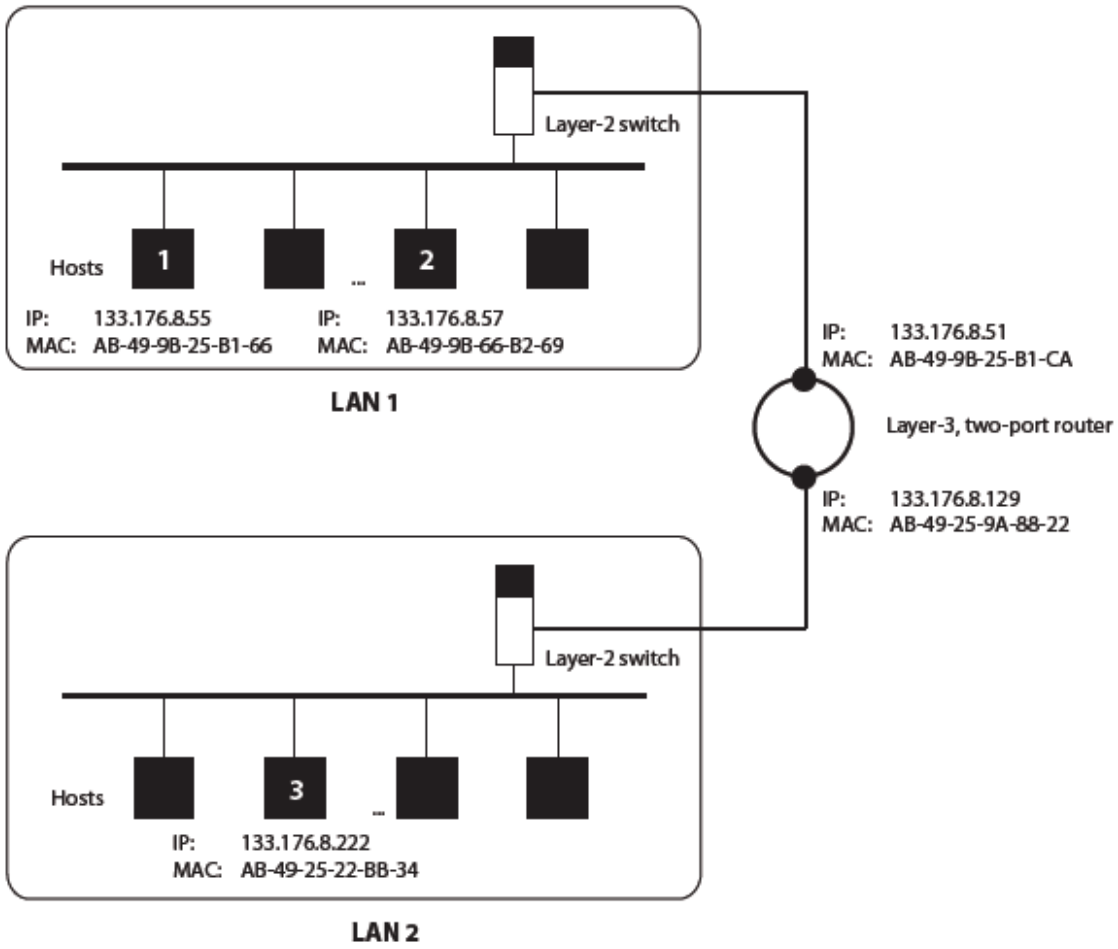
"If your IP is 133.176.8.222, then reply with your MAC address."



Scenario C
Host 1 transmits to Host 3

No reply is received.

Host 1 transmits a frame with destination IP address 133.176.8.222 and a destination MAC address of AB-49-9B-25-B1-CA



Scenario C
Host 1 transmits to Host 3

The two-port router receives frame, observes destination IP.

Either the IP is in its ARP table or it sends out an ARP request on all ports.