TNE20003 - Internet and Cybersecurity for Engineering Applications

Network devices: Routers and Switches

Network Model

2 basic models:

OSI & TCP/IP

Each of these has a number of specific devices that carry out the various tasks at the various layers.

In the next few slides we work our way through the various layers

Also note that networking and network communication follows a hierarchical structure, as this is the most efficient method for transferring information. For example, the telephone system which is (country code+state id+actual number) gives a unique identifier. +61039214832 2 Same as the postal service ….

The first layer is the physical layer and is incorporated by the mechanism of that medium, ie electricity, light, electromagnetic waves.

Encapsulation and the Ethernet Frame Layer 2

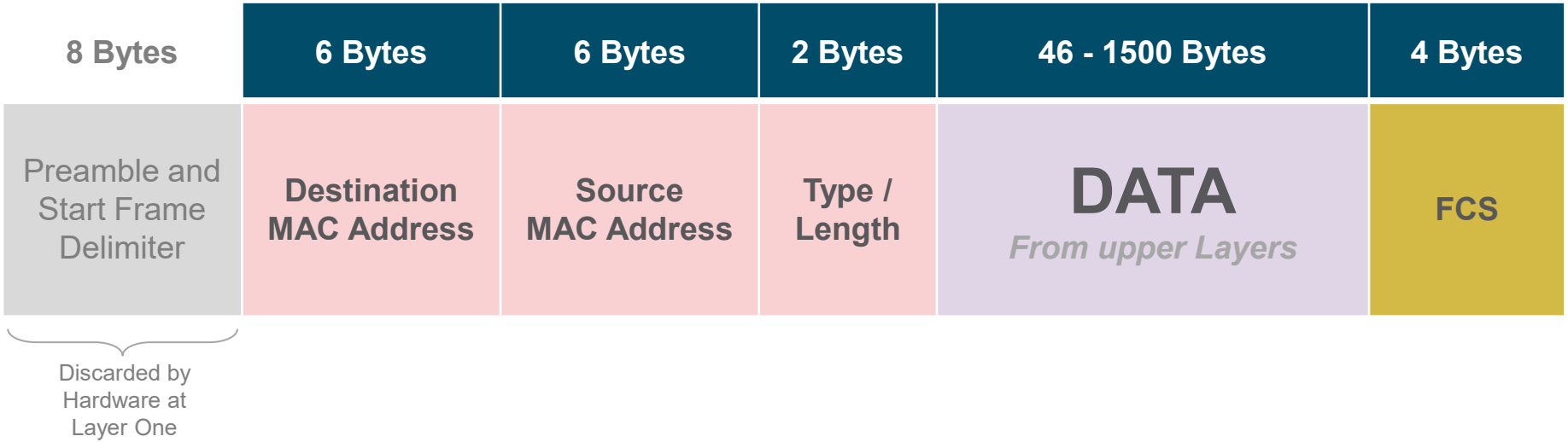
Each message is encapsulated into a specific format, called a frame, that includes the source and destination addresses.

- An example is how a letter is put (encapsulated) inside an envelope.

For communication on an IP network, the format is very specific and includes a source and destination IP address.

Encapsulation and the Ethernet Frame Fields

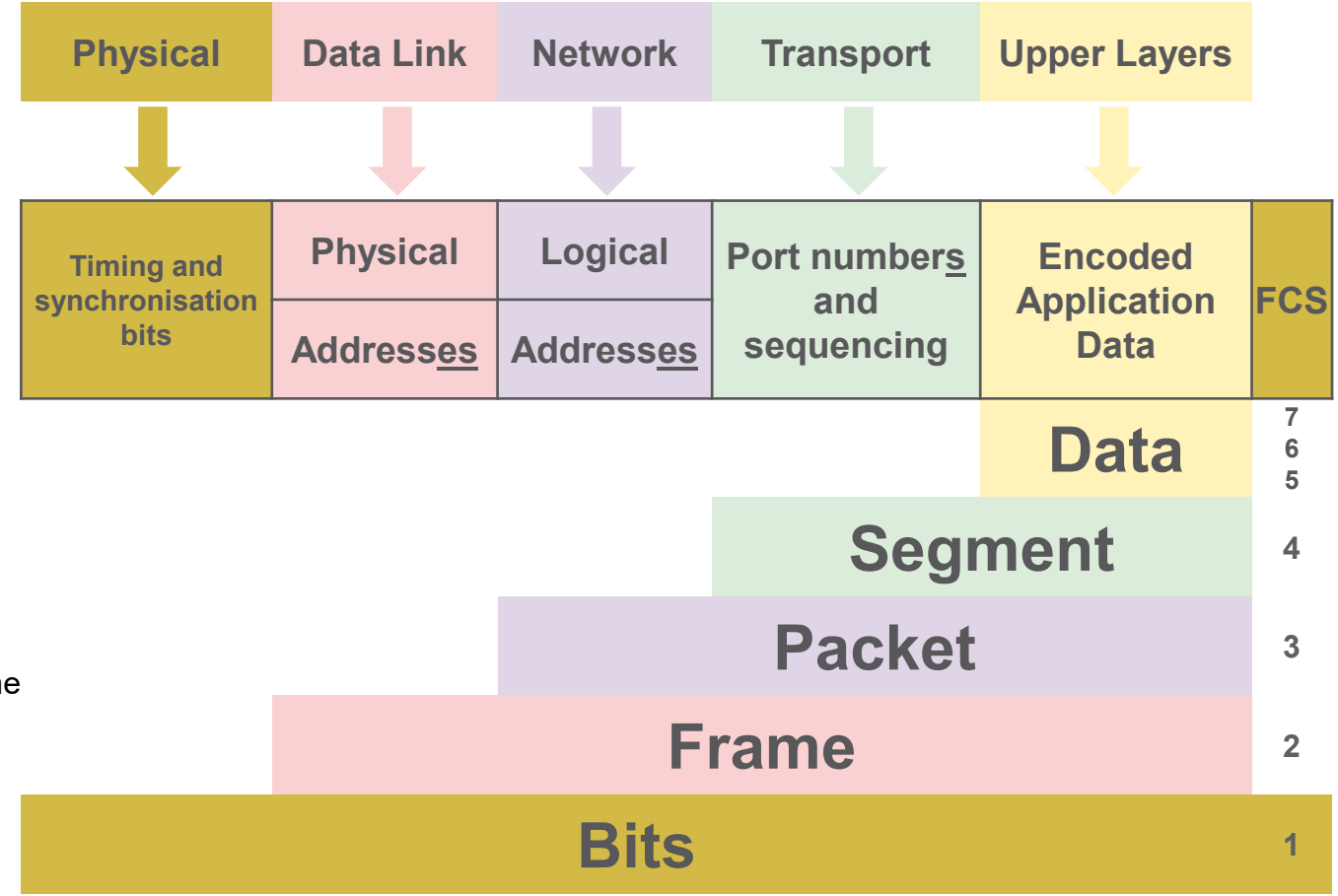
On an Ethernet network, messages are put into a Frame or Layer 2 Protocol Data Unit.



What are the minimum and maximum Frame sizes ?

Encapsulation and the Ethernet Frame

- **Network Addresses**
  - Layer Three Packet
  - Source IP address
  - Destination IP address
  - Deliver the IP packet from the original source to the final destination, either on the same network or to a remote network.
- **Data Link Addresses**
  - Layer Two Frame
  - Source data link address
  - Destination data link address
  - Deliver the data link frame from one network interface card (NIC) to another NIC on the same network.

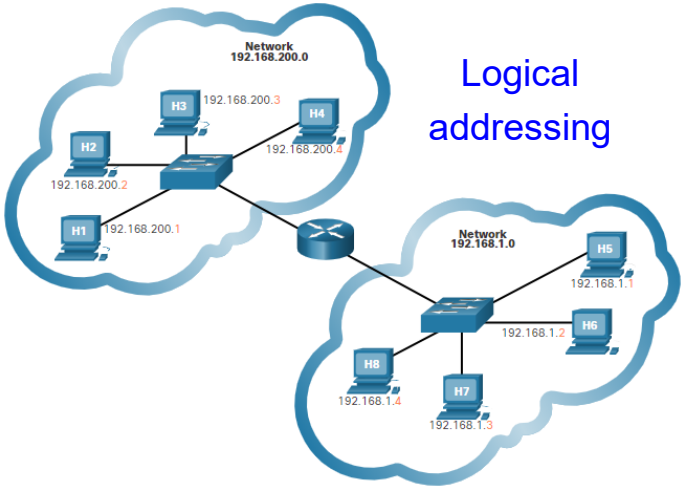


Hierarchical Network Design

Hierarchical Network Design

Both physical and logical addresses are needed for a device to communicate in an Ethernet network.

- A physical address (MAC address) does not change.
  - Burned into the NIC (Network Interface Card)
- A logical address (IP address) can change and is commonly assigned by a network administrator.
  - Two parts: Network and Host - in the below example: **N.N.N.H**



Logical addressing

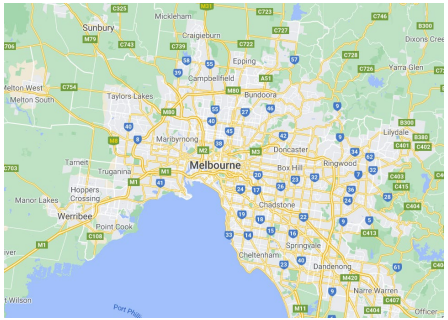
L3	IP	192.168.11.12
L2	MAC	11:22:33:44:55:66

Hierarchical Network Design

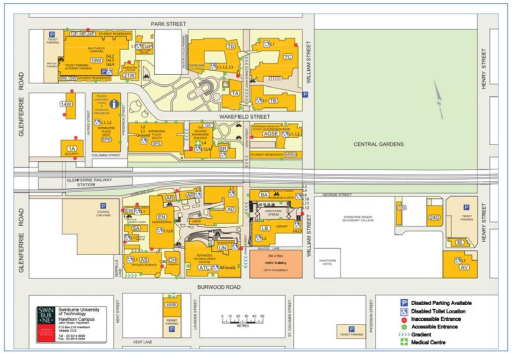
Network addressing is done in a hierarchical fashion.

Australia

Victoria

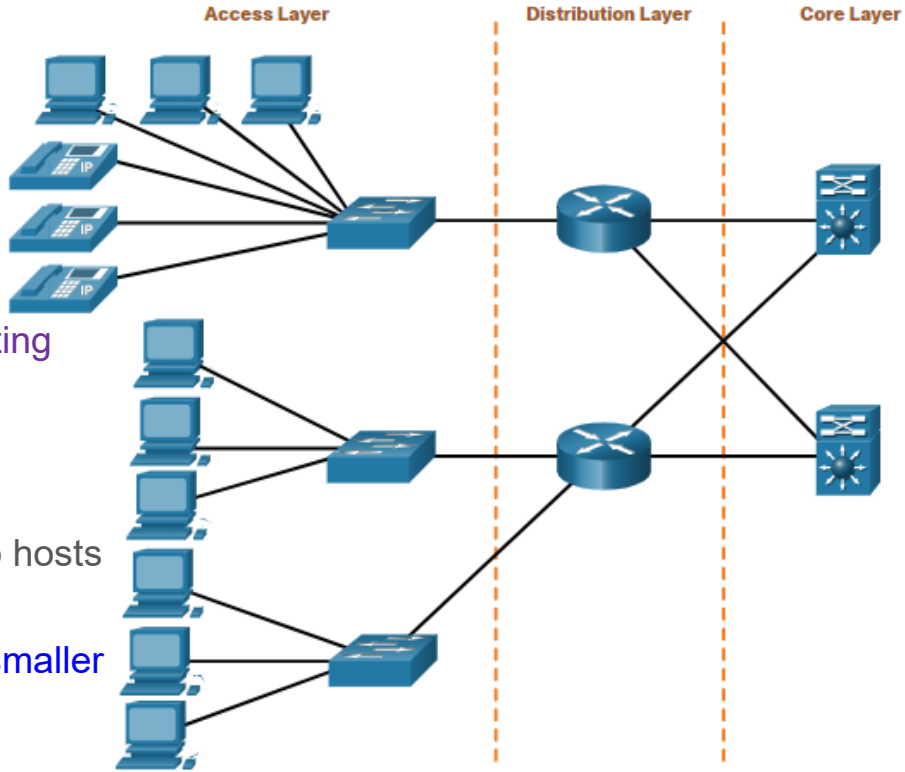


Melbourne



Hawthorn Campus

Hierarchical Network Design



A hierarchical, layered design provides:

- Increased efficiency
- Optimization of function
- Increased speed
- A way in which to scale the network without impacting the performance of existing ones

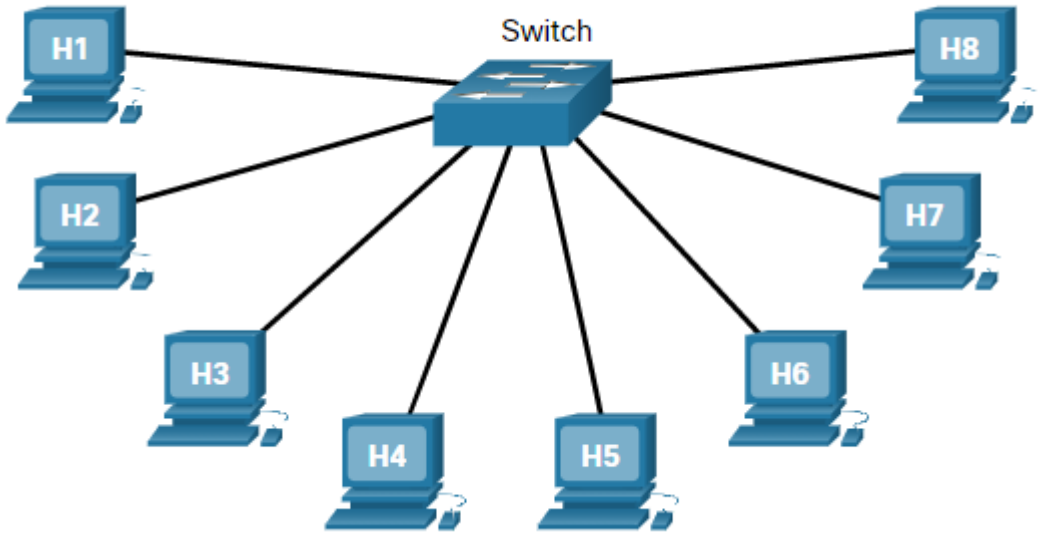
Three layers:

- **Access Layer** - This layer provides connections to hosts in a local Ethernet network.
- **Distribution Layer** - This layer interconnects the smaller local networks.
- **Core Layer** - This layer provides a high-speed connection between distribution layer devices.

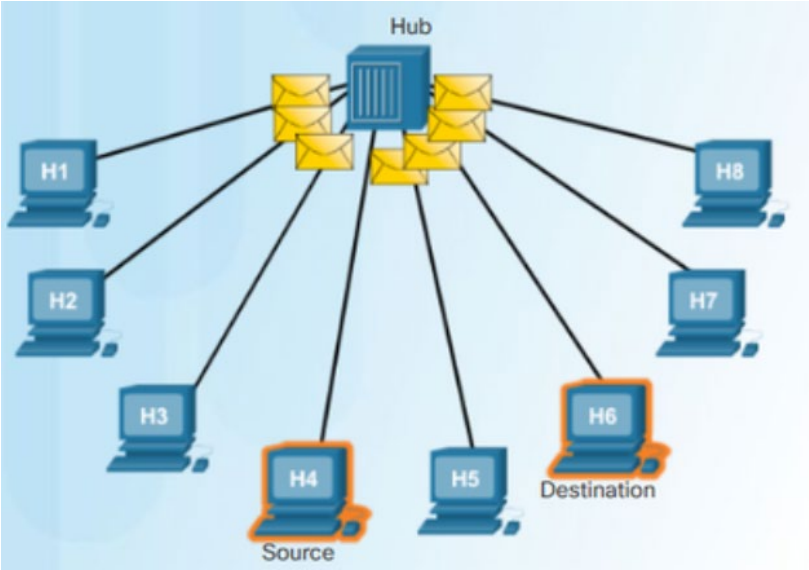
The Access Layer

The Access Layer

- Access layer devices provide access, so hosts can join a wired (or wireless) network.
- In a wired network, each host connects to an access layer network device such as a switch.



The Access Layer

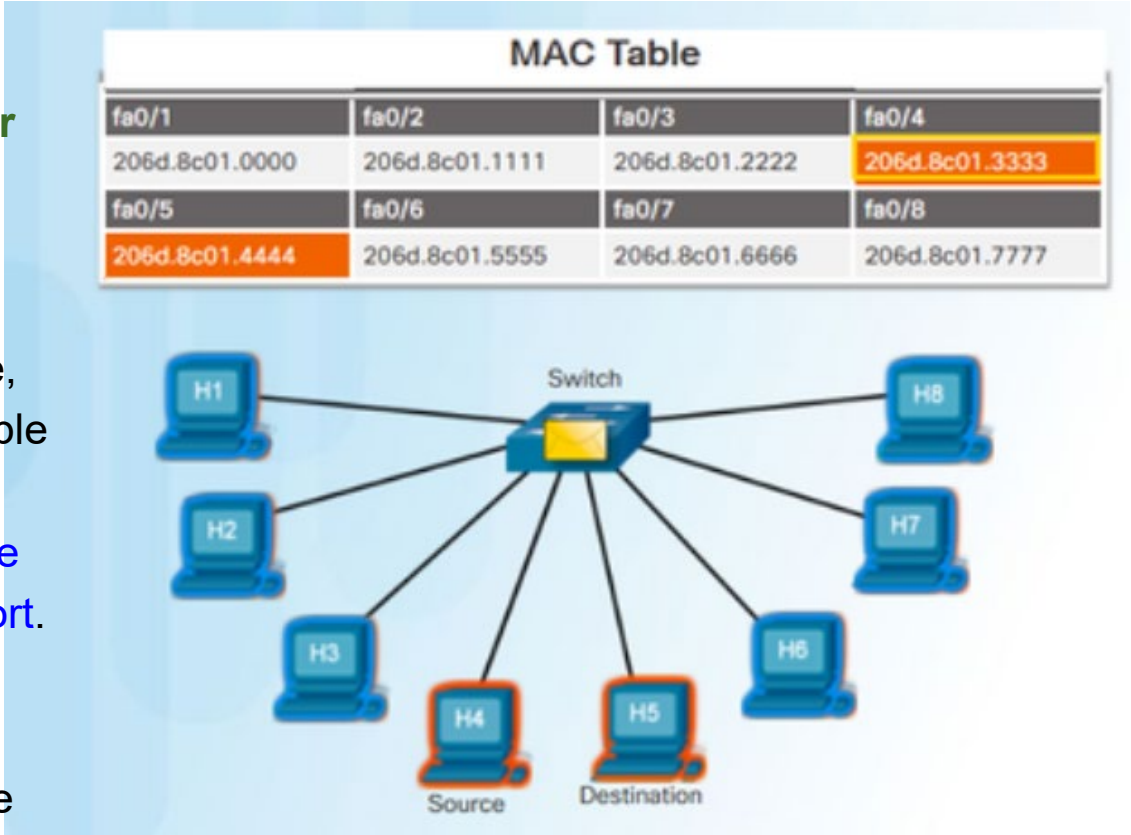


- Only one message can be sent through an Ethernet hub at a time.
- Hubs take signals from one port and sends the message out all of the other ports.
- This is a problem due to collisions!! Very large collision domain

The Access Layer

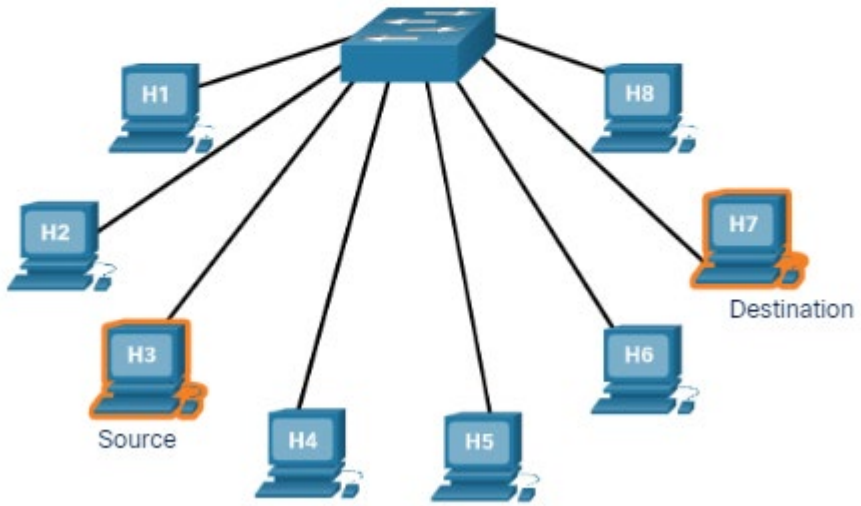
An Ethernet switch is an access layer device. It's purpose is to provide micro-segmentation of the collision domain.

- A switch builds a MAC address table, known as a CAM (content addressable memory) table.
- A switch uses the MAC address table to send the message to a specific port.
- In this case if H4 wants to talk to H5 they have their own collision domain due to the switch. The switch will use the CAM table to forward the traffic.



The Access Layer

MAC Table			
fa0/1	fa0/2	fa0/3	fa0/4
260d.8c01.0000	260d.8c01.1111	260d.8c01.2222	260d.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
260d.8c01.4444	260d.8c01.5555		260d.8c01.7777

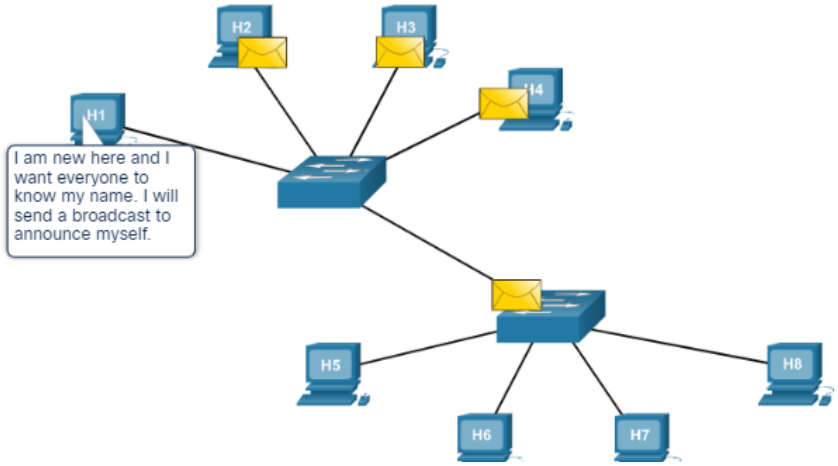


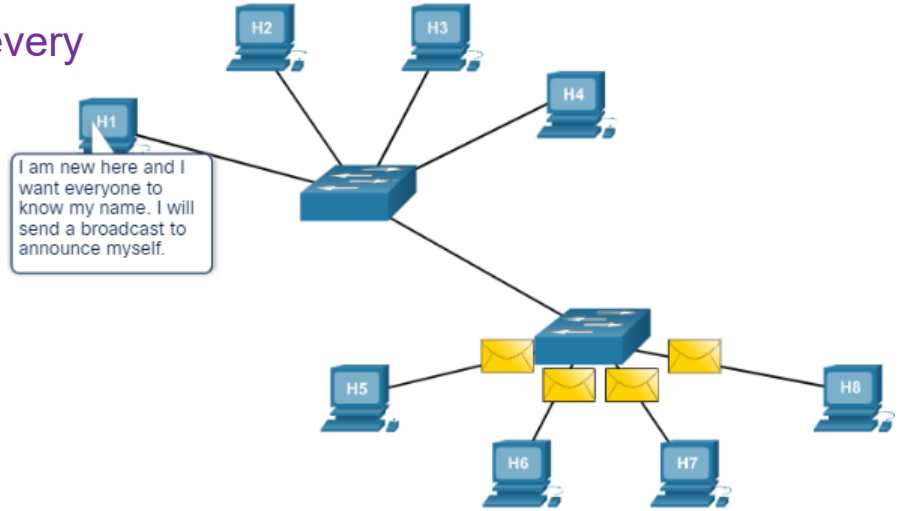
- A switch builds a MAC address table by examining a frame as it comes into the switch.
- A switch adds the source MAC address of the device connected to the port through which the frame came in on.
- A switch forwards a frame out to a specific port when the destination MAC address is in the MAC address table.
- A switch forwards a frame out to all hosts (except the sending host) when the destination MAC address is not in the MAC address table.

Broadcast Containment

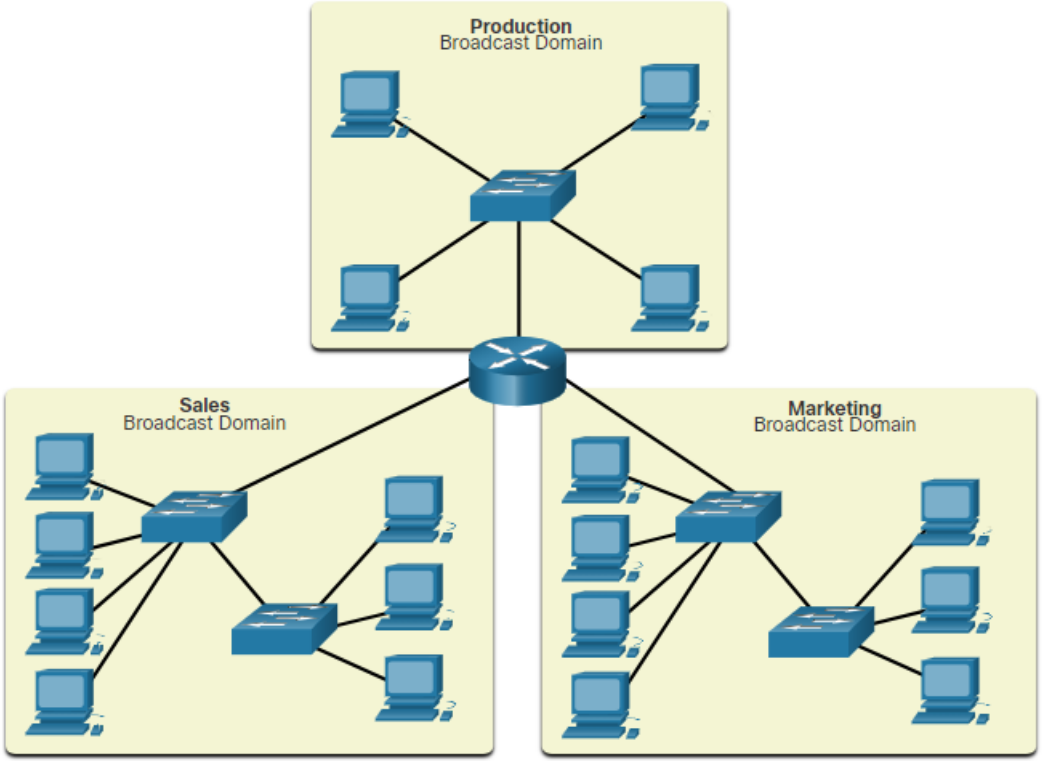
Broadcast Containment

- All is good as long as both source and destination MAC address are known, but if destination MAC is unknown the data needs to be broadcast.
- A broadcast message is used to contact every other device on the local network.
- An Ethernet broadcast is all 1s in the destination MAC address – FFFF.FFFF.FFFF.





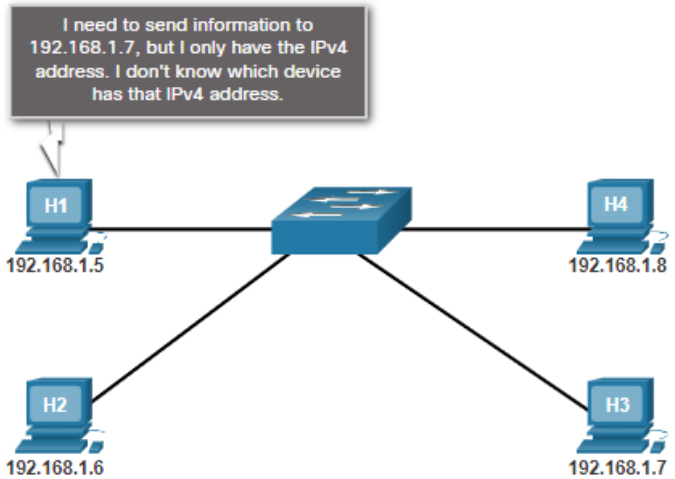
Broadcast Containment



- A broadcast domain is the area through which a broadcast message can travel.
- Each local Ethernet network is a broadcast domain.
- Routers are used to divide the network into multiple broadcast domains.

Broadcast Containment

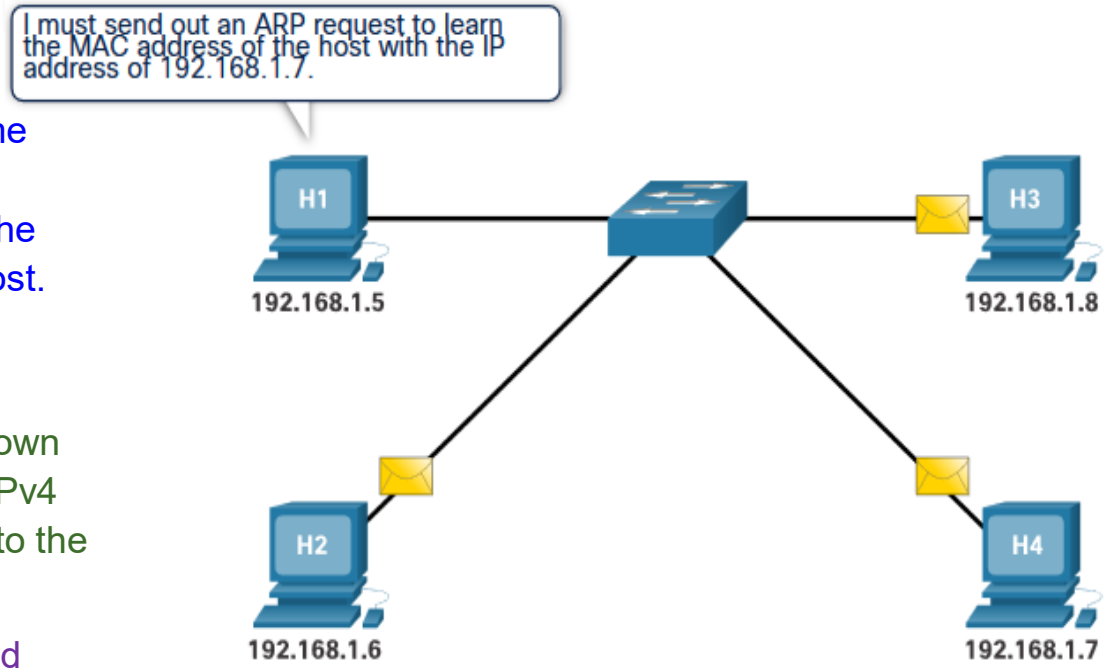
- In order to send information from a device that is on an Ethernet network, the device must supply its own source MAC address, a destination MAC address, its own source IP address, as well as a destination IP address.
- The address resolution protocol (ARP) is used to discover the MAC address of a device on the same local network.



Broadcast Containment

ARP uses Three steps to discover and store the MAC address of a host on the local network when only the IPv4 address of that host is known.

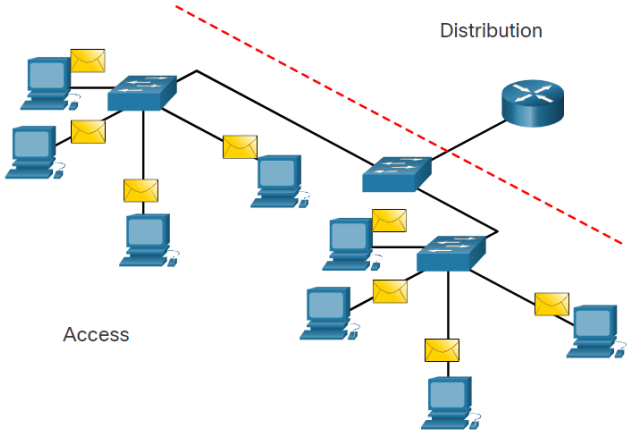
1. The sending host creates and sends a frame addressed to a broadcast MAC address. Contained in the frame is a message with the IPv4 address of the intended destination host.
2. Each host on the network receives the broadcast frame and compares the IPv4 address contained in the message with its own IPv4 address. The host with the matching IPv4 address sends its own MAC address back to the original sending host.
3. The sending host receives the message and stores the MAC address and the IPv4 address in an ARP table.



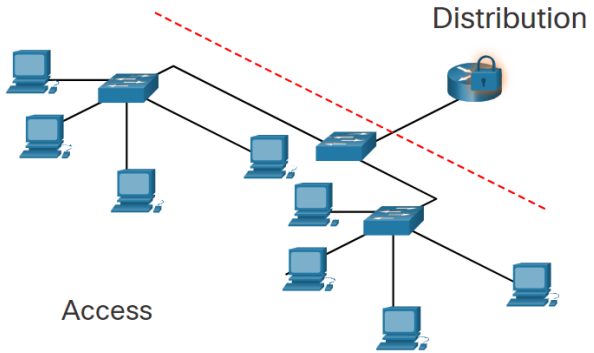
How to Contain Broadcasts

The Need for Routing

Broadcast Containment
Routers in the distribution layer can limit broadcasts to the local network where they need to be heard. Although broadcasts are necessary, too many hosts connected on the same local network can generate excessive broadcast traffic and slow down the network.

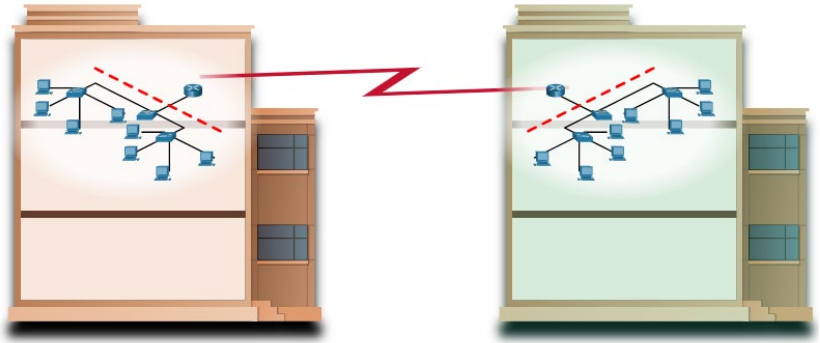


Security
Routers in the distribution layer can separate and protect certain groups of computers where confidential information resides. Routers can also hide the addresses of internal computers from the outside world to help prevent attacks, and control who can get into or out of the local network.

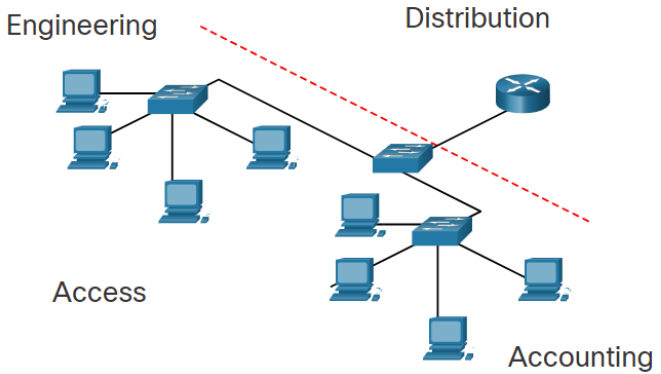


The Need for Routing

Locations
Routers in the distribution layer can be used to interconnect local networks at various locations of an organization that are geographically separated.



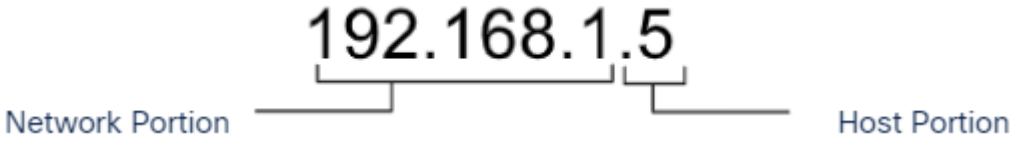
Logical Grouping
Routers in the distribution layer can be used to logically group users, such as departments within a company, who have common needs or for access to resources.



The Need for Routing

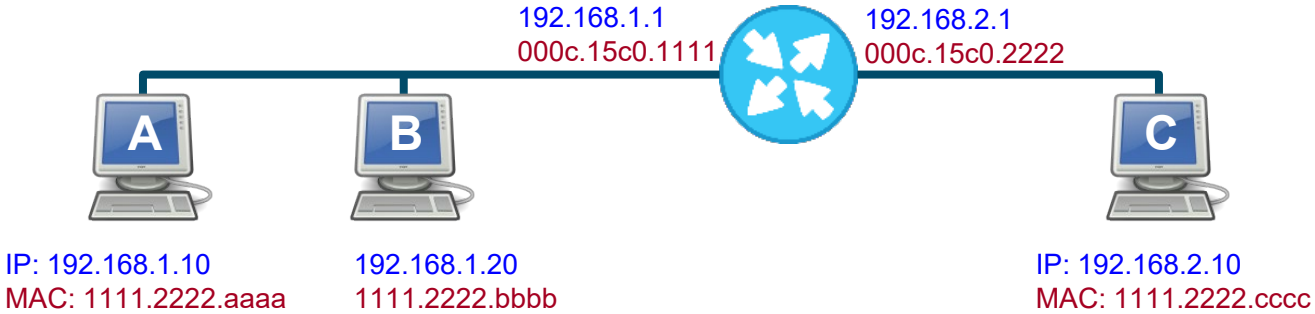
A switch examines MAC addresses.

A router examines IP addresses.



What Address Goes Where ?

- ARP is the process of Mapping a known IP Address to an unknown MAC Address.
- Applications use Naming systems like WINS and DNS to map human friendly information to IP Addresses. eg: www.facebook.com = 157.240.8.35
- **For Network transmission to function as efficiently as possible, all data that moves through a network needs *both* MAC and IP Addresses !**



When PC __ talks to PC __ what will be the:

Source and Destination MAC Address ?

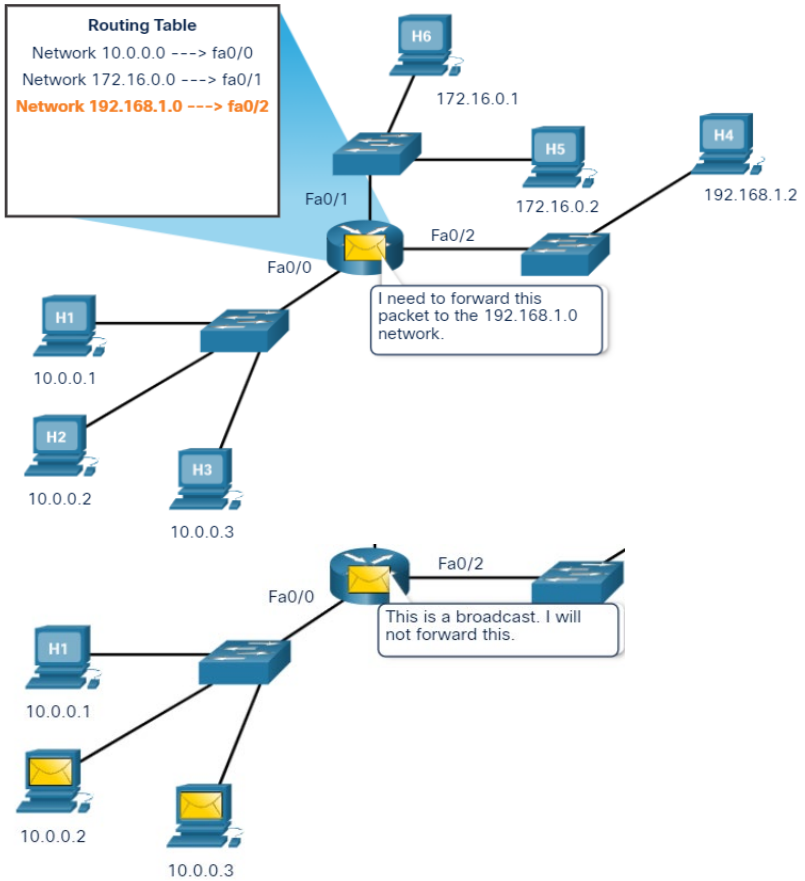
Source and Destination IP Address ?

Let us work through all possible combinations….

The Routing Table

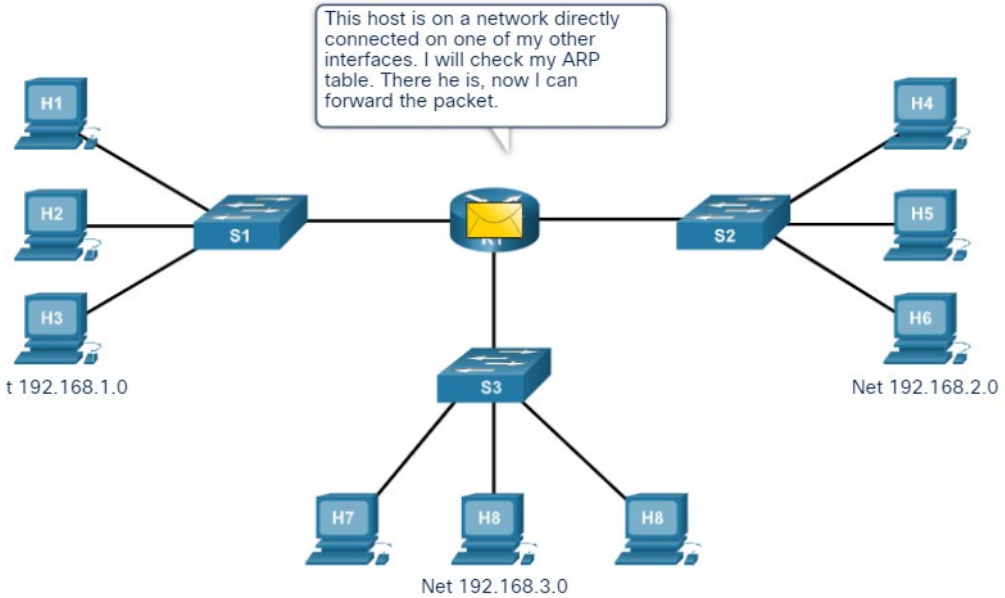
The Routing Table

- Each router interface connects to a different network.
- A routing table contains information for how to reach local and remote networks.
- The destination IP address is used and compared with the networks in the routing table to determine the interface to forward the packet out of.
- Routers **DO NOT** forward broadcast messages.



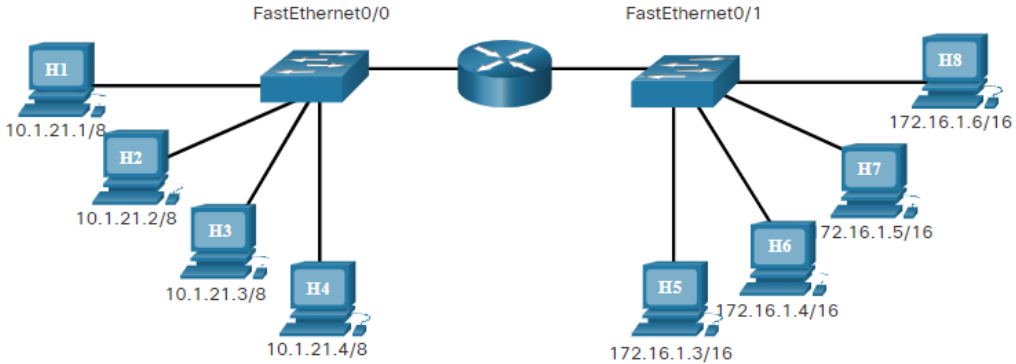
The Routing Table

- The destination MAC address is used to forward the packet to either the router if the destination IP address is for a different network or a specific network device on the local network.
- The ARP table shows a mapping of IP address to MAC address.



The Routing Table

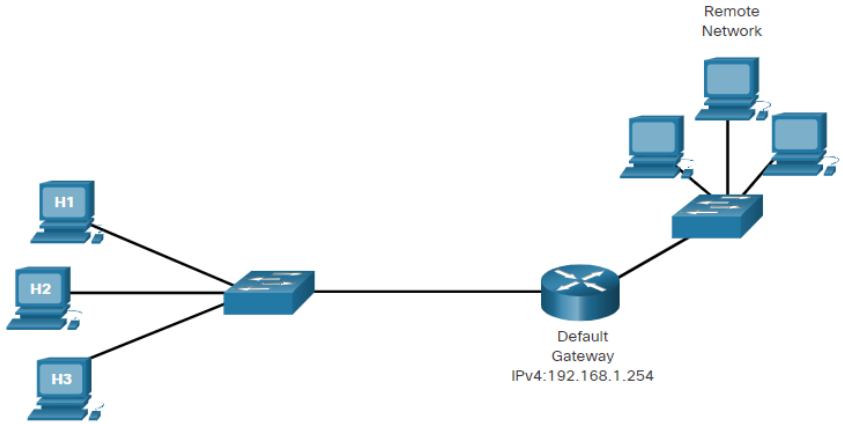
- A routing table contains network addresses and the best path to reach a network.
- Two ways routes can be added to a routing table
  - Dynamically learned from other routers
  - Manually entered by a network administrator
- A default route is the router interface used when forwarding packets to a destination that is not in the routing table.
- If a packet is destined for a network that is not in the routing table and no default route exists, the packet will be dropped.
  - Q: Can this router find a way to Facebook ?



Type	Network	Port
C	10.0.0.0/8	FastEthernet0/0
C	172.16.0.0/16	FastEthernet0/1

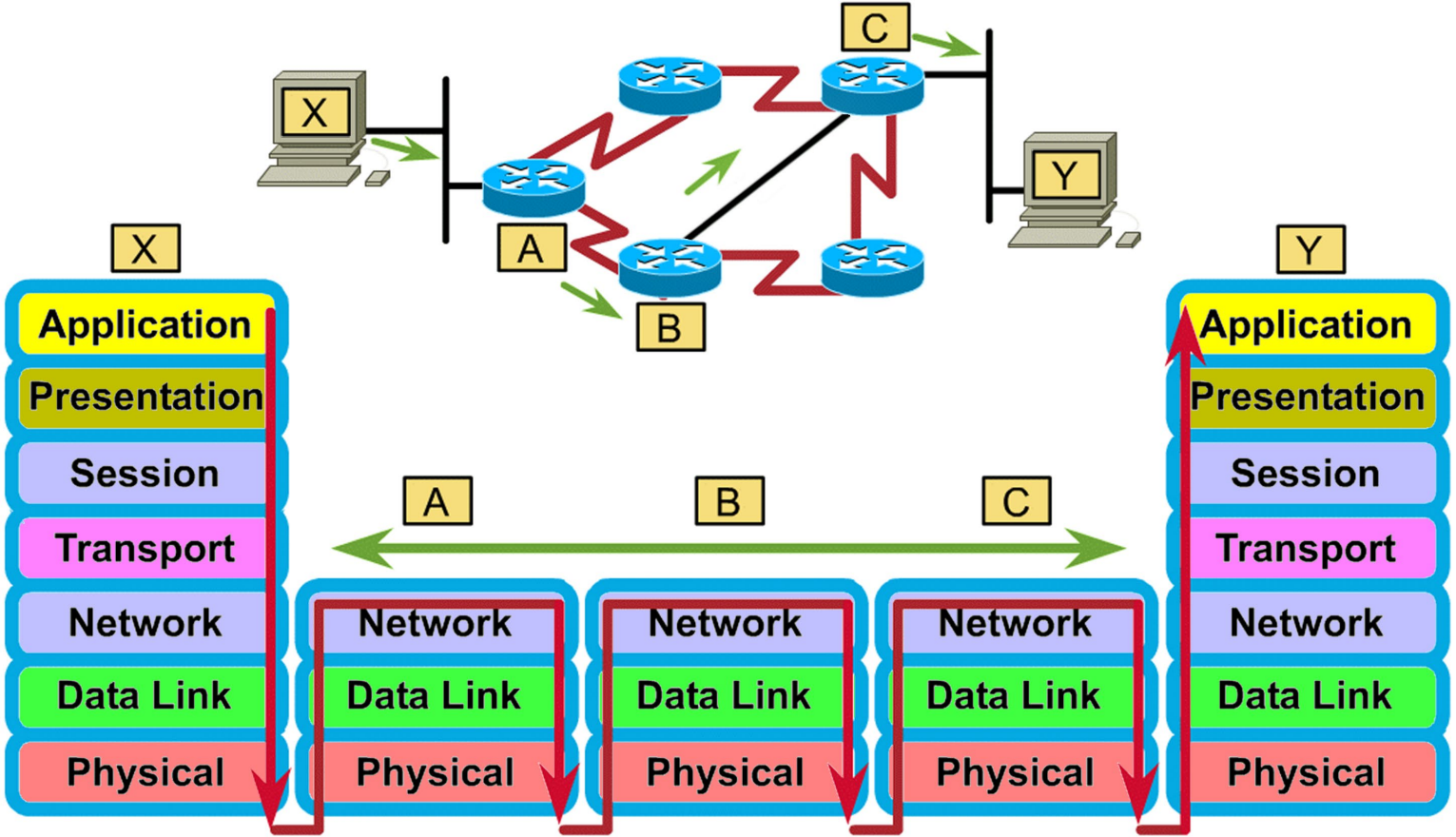
The Routing Table

- When a host sends a message to a device on the same network, it forwards the message directly and uses ARP to discover the MAC address.
- When a host sends a message to a device on a remote network, the hosts uses the MAC address of the Router as the destination, but still has the IP address of the remote host as the Layer 3 destination.
- It is very important that each host has the correct default gateway that is the IP address of the router on the same network.



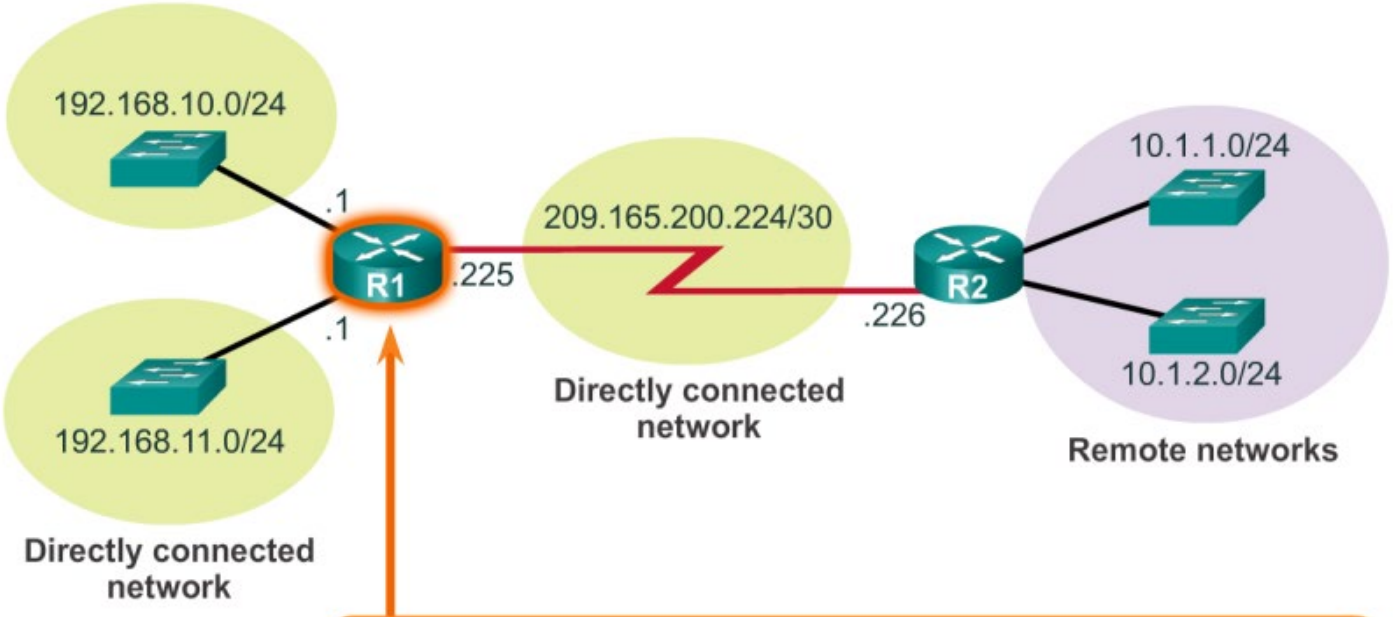
PC	IPv4 Address	Subnet Mask	Default Gateway
H1	192.168.1.1	255.255.255.0	192.168.1.254
H2	192.168.1.2	255.255.255.0	192.168.1.254
H3	192.168.1.3	255.255.255.0	192.168.1.254

So, what have we learned so far ?



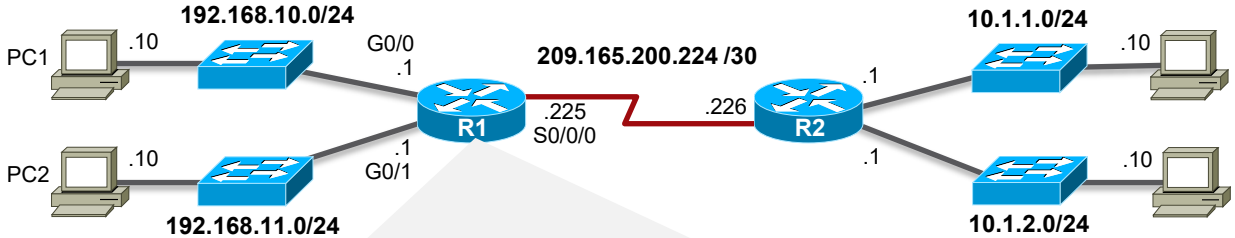
How many unique IP and MAC Addresses were used to get one message from PC-X to PC-Y ?

Router Packet Forwarding Decision



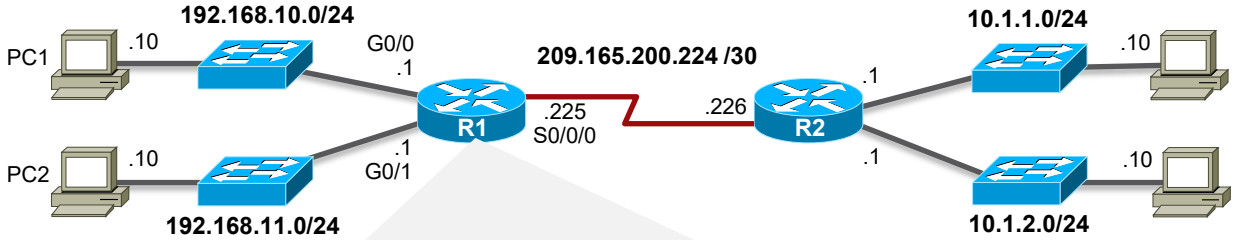
Therefore, Routers must know where Networks are in order to move Data towards them….

IPv4 Router Routing Table




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D        10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D        10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
C        209.165.200.224/30 is directly connected, Serial0/0/0
R1#
```

IPv4 Router Routing Table - IOS v15 *and above…*

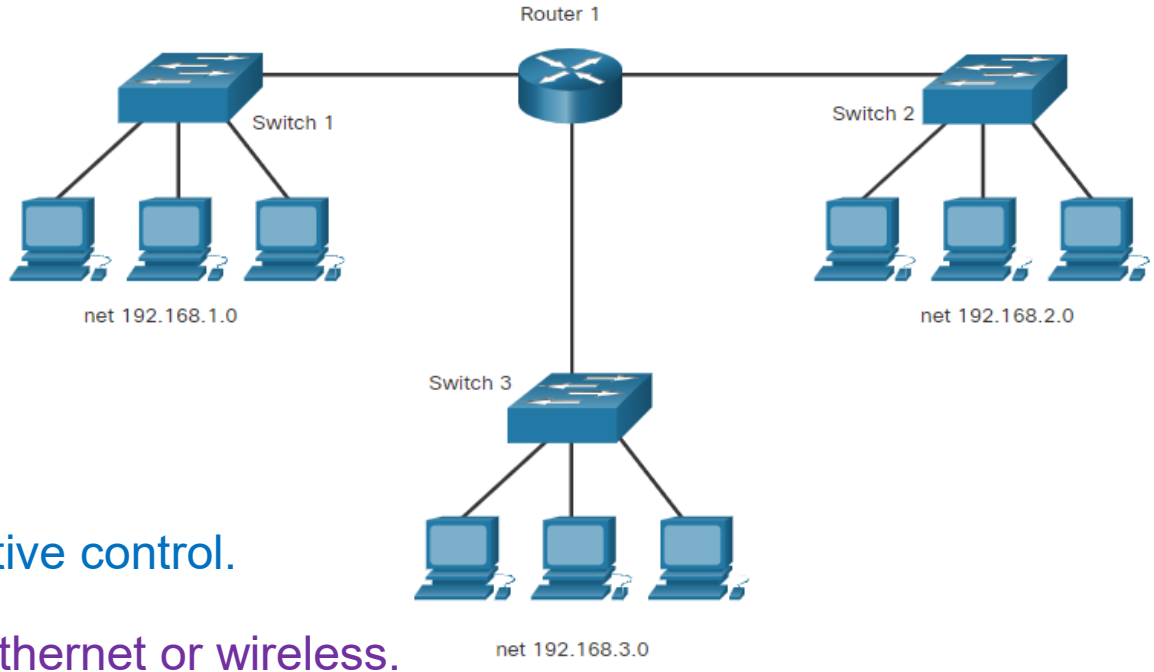



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D        10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D        10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

← *IOS v15+*

Create a LAN

Create a LAN



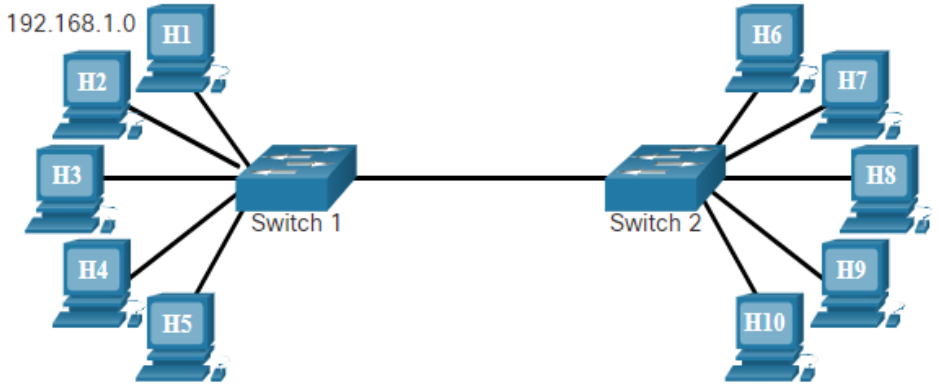
- LANs are under one administrative control.
- LANs are usually either wired Ethernet or wireless.

Create a LAN

Advantages of a single local segment:

- Appropriate for simpler networks
- Less complexity and lower network cost
- Allows devices to be "seen" by other devices
- Faster data transfer - more direct communication
- Ease of device access

All Hosts in One Local Segment



Disadvantages of a single local segment:

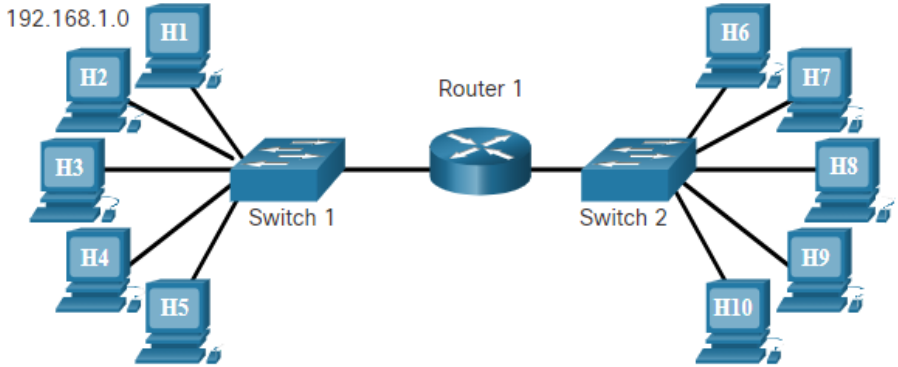
- All hosts are in one broadcast domain which causes more traffic on the segment and may slow network performance
- Harder to implement QoS
- Harder to implement security

Create a LAN

Advantages of having hosts on a remote segment:

- More appropriate for larger, more complex networks
- Splits up broadcast domains and decreases traffic
- Can improve performance on each segment
- Makes the machines invisible to those on other local network segments
- Can provide increased security
- Can improve network organization

Hosts on a Remote Segment



Disadvantages of having hosts on a remote segment:

- Requires the use of routing (distribution layer)
- Router can slow traffic between segments
- More complexity and expense (requires a router)