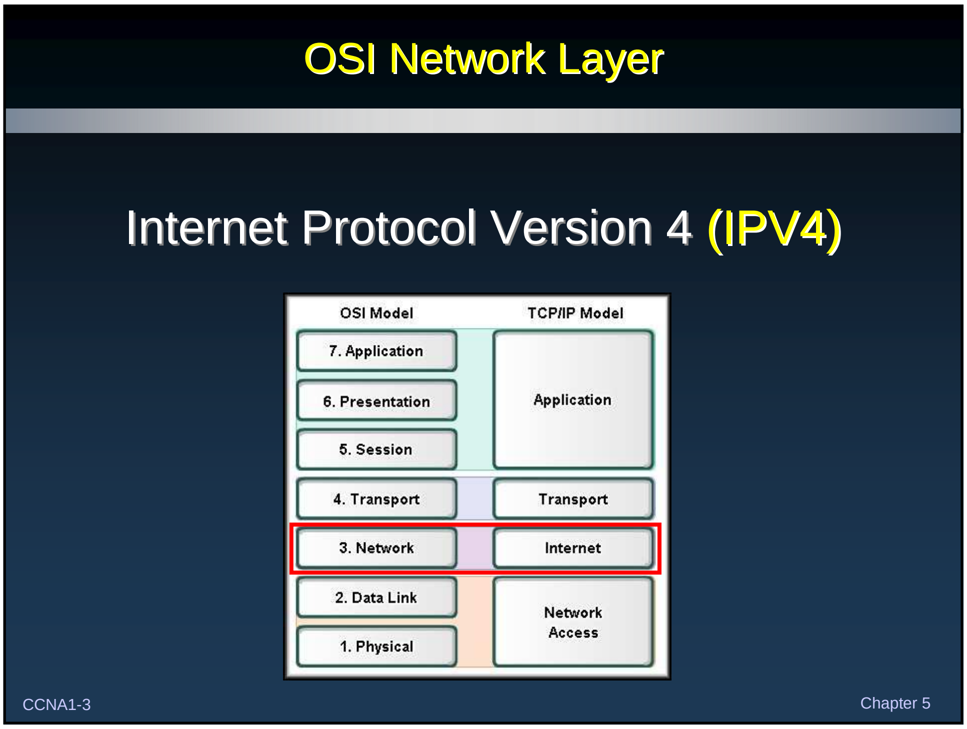
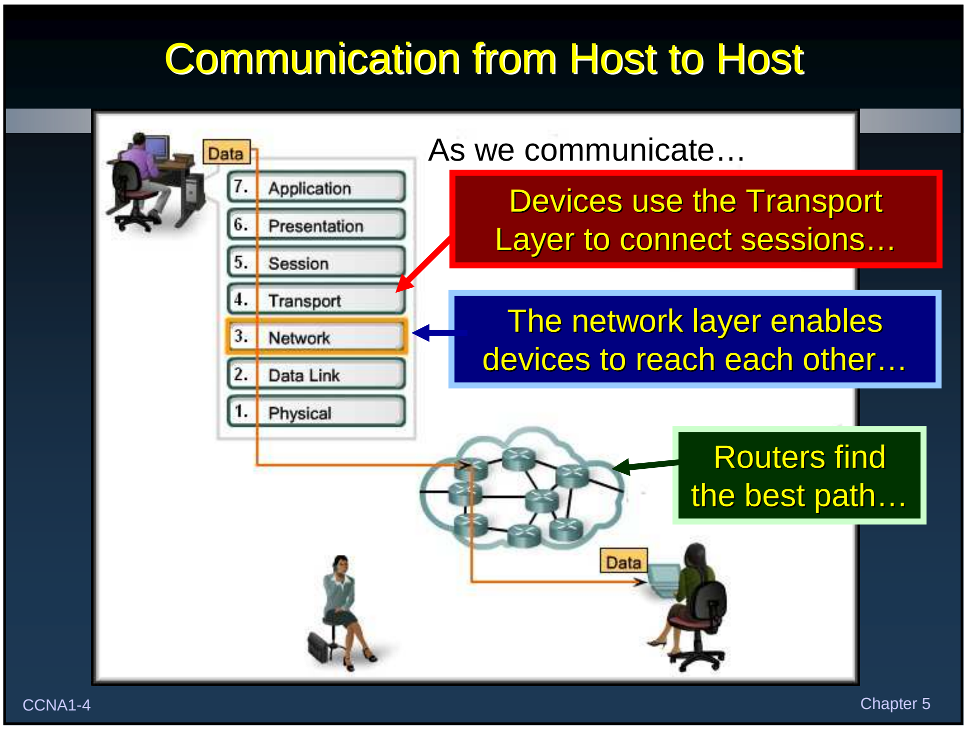
Chapter 5

OSI Network Layer

Note for Instructors

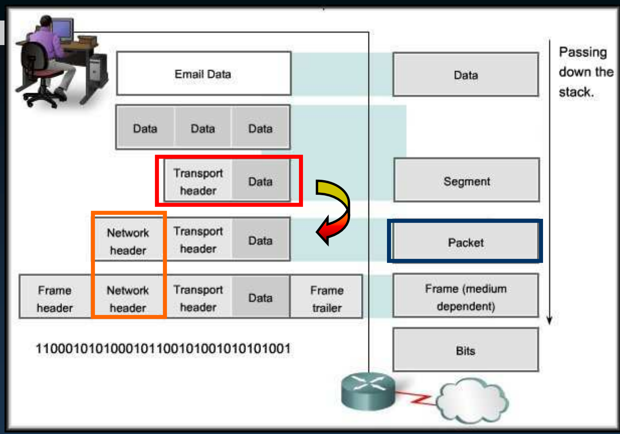
- These presentations are the result of a collaboration among the instructors at St. Clair College in Windsor, Ontario.
- Thanks must go out to Rick Graziani of Cabrillo College. His material and additional information was used as a reference in their creation.
- If anyone finds any errors or omissions, please let me know at:
  - tdame@stclaircollege.ca.


OSI Network Layer
Internet Protocol Version 4 (IPV4)
OSI Model
TCP/IP Model
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Application
Transport
Internet
Network Access
CCNA1-3
Chapter 5


Communication from Host to Host
As we communicate…
Data
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Devices use the Transport Layer to connect sessions…
The network layer enables devices to reach each other…
Routers find the best path…
Data
CCNA1-4
Chapter 5

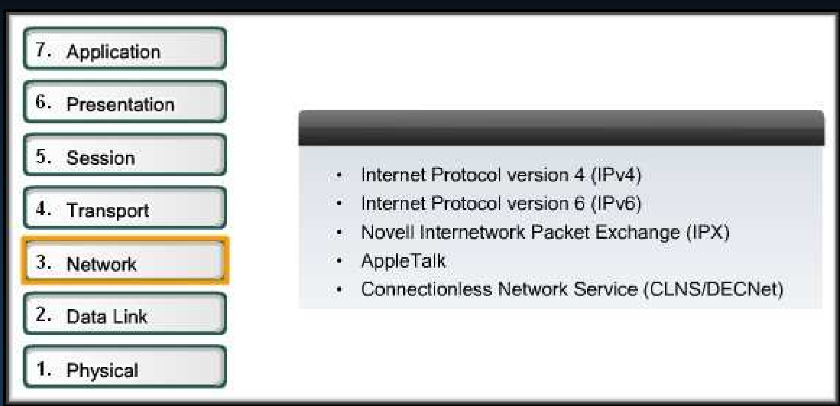
Communication from Host to Host

Network Layer



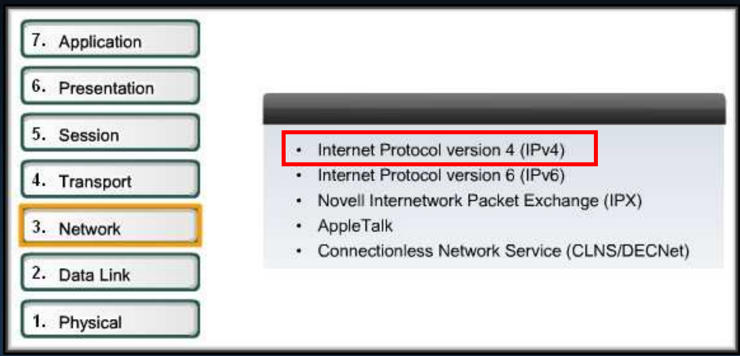
- Addresses packets with an IP Address.
- Encapsulates the packet.
- Routes the packet to the destination.
- Decapsulates the packet.

Network Layer Protocols



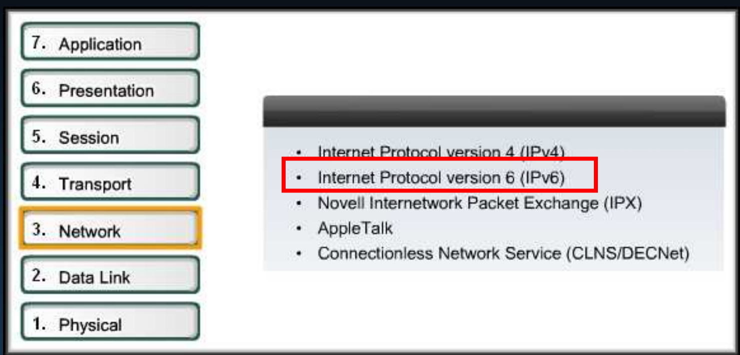
- We will be focusing on IPV4.

IPV4: Example Network Layer Protocol



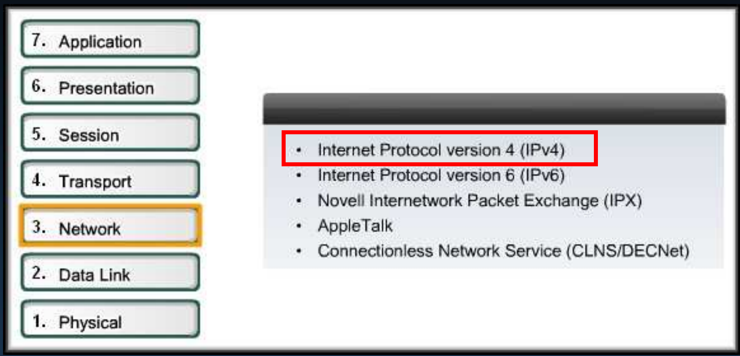
- Internet Protocol Version 4 (IPV4) is the most widely used version of IP.
- Only Layer 3 protocol used on the Internet.
- Focus of this course.

IPV4: Example Network Layer Protocol



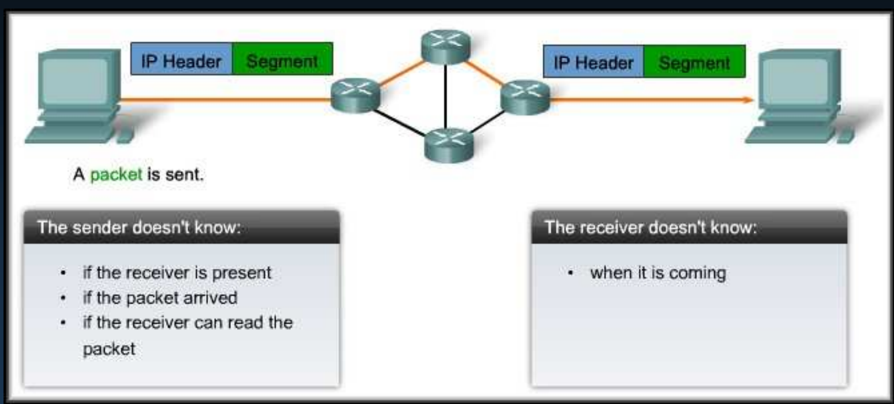
- Internet Protocol Version 6 (IPV6) is developed and slowly being implemented. *(More in CCNA-4)*
- Will eventually replace IPV4.
- Different characteristics than IPV4.

IPV4: Example Network Layer Protocol

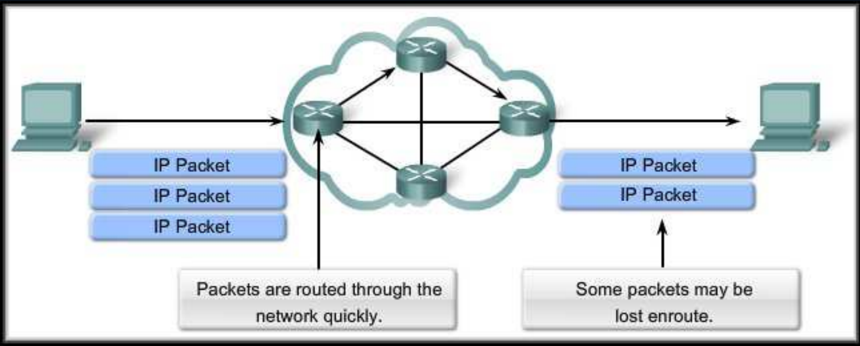


- Characteristics:
  - Connectionless
  - “Best Effort” Delivery (Unreliable)
  - Media Independent

Connectionless

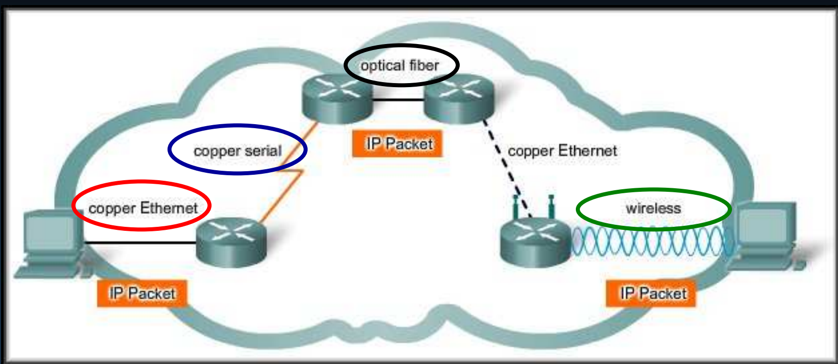


"Best Effort" Delivery (Unreliable)



- *Unreliable* means simply that IP does not have the capability to manage and recover from undelivered or corrupt packets.
- Since protocols at *other layers can manage reliability*, IP is allowed to function very efficiently at the Network Layer.

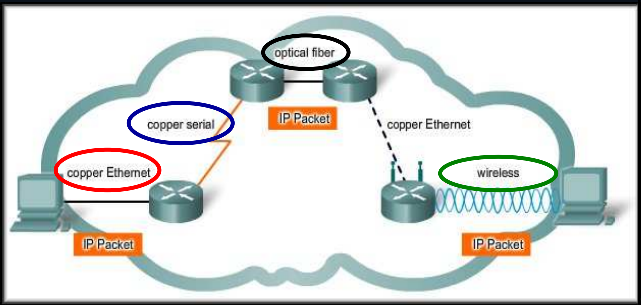
Media Independent



- Not concerned with the physical medium.
- Operates independent of the layers that handle the physical medium that carries the packet.

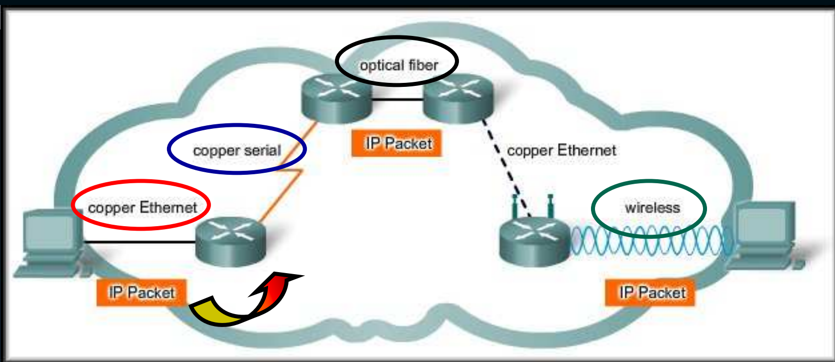
Media Independent

- Is concerned with the size of the packet or Maximum Transmission Unit (MTU).



- The MTU is established as part of the communication between the Data Link and Network Layers.
- Fragmentation:
  - At times, an intermediary device (router) will need to split up a packet when forwarding it from one media to a media with a smaller MTU.

Media Independent

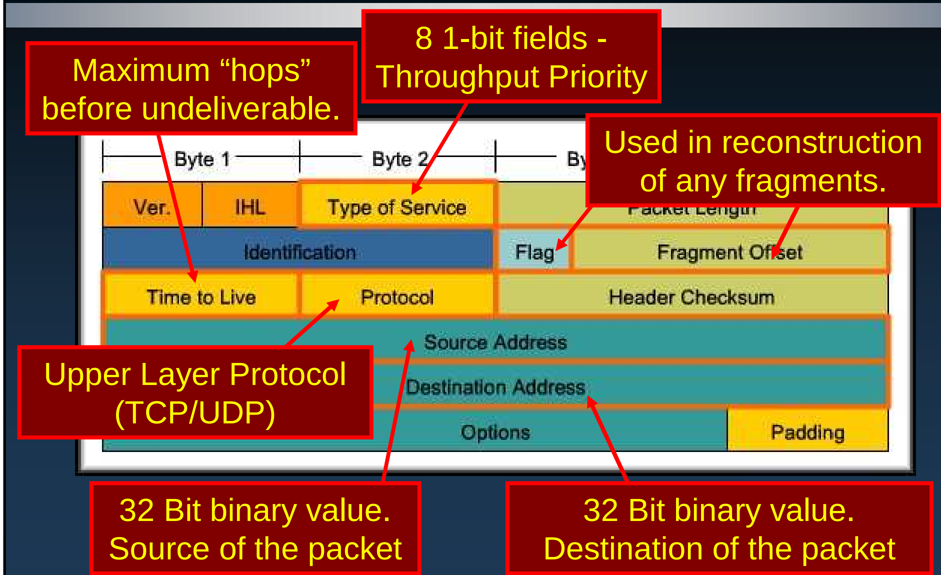


- Copper Ethernet: MTU = 1,518 bytes.
- Copper Serial: Frame Relay MTU = 512 bytes.
- Optical Fiber: ATM MTU = 17,966 bytes.
- Wireless: 802.11 MTU = 2272 bytes.

Packaging the Transport Layer PDU

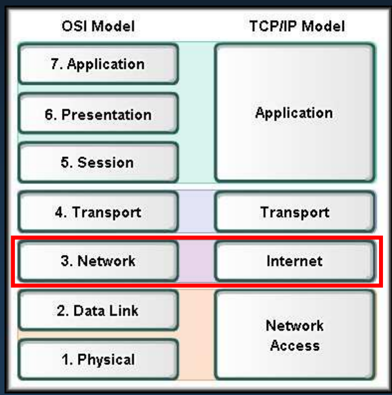
In TCP/IP based networks, the Network Layer PDU is the IP Packet.

IPV4 Packet Header

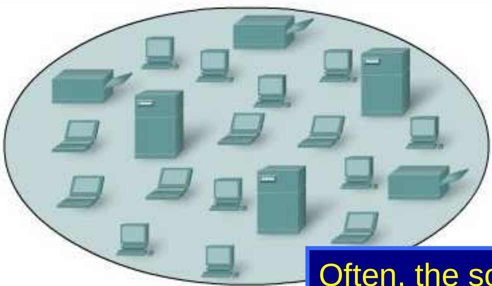


OSI Network Layer

Networks: Dividing Hosts into Groups



Dividing Hosts into Groups



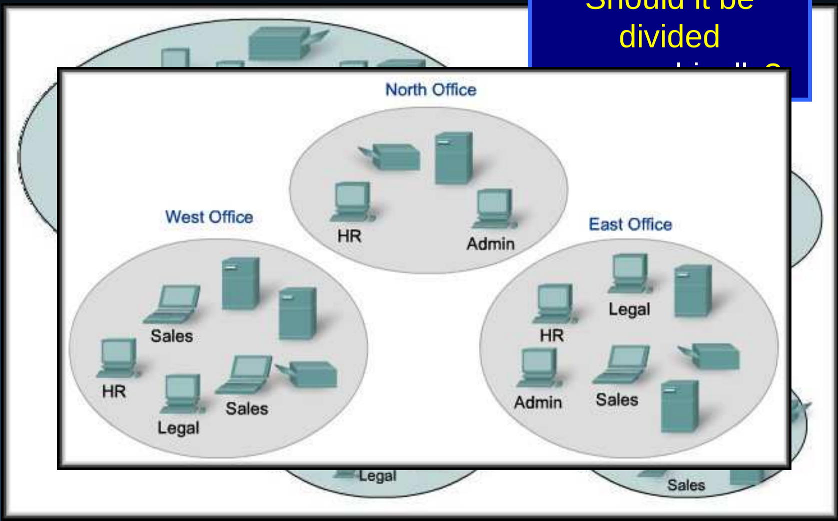
As networks grow, they become too unwieldy to manage as a single entity.

Often, the solution is to divide the large network into several more manageable sub-networks.

The question is…..HOW?

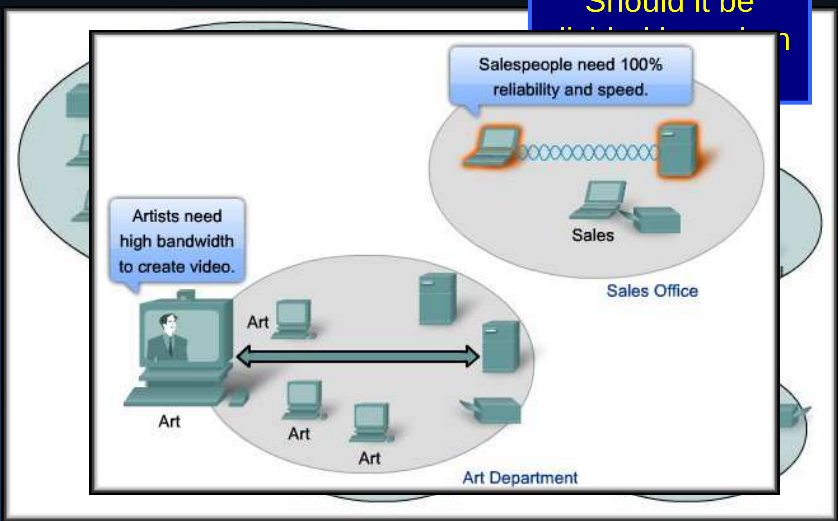
Dividing Hosts into Groups

Should it be divided



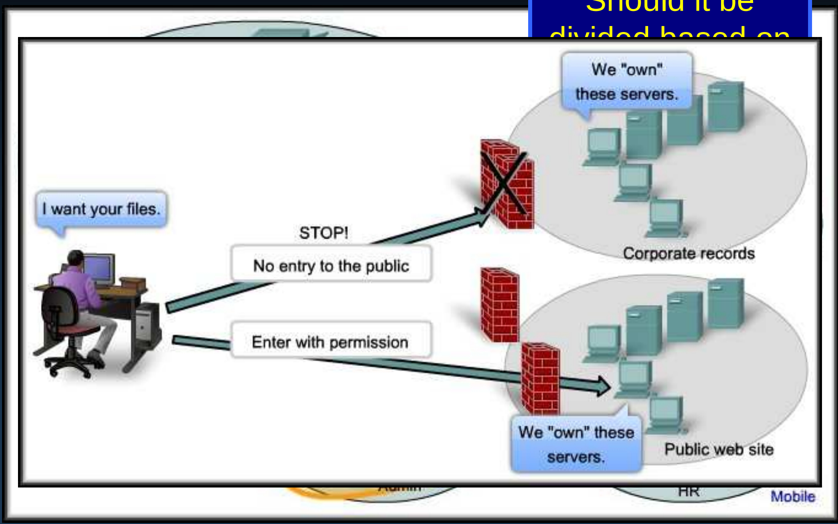
Dividing Hosts into Groups

Should it be

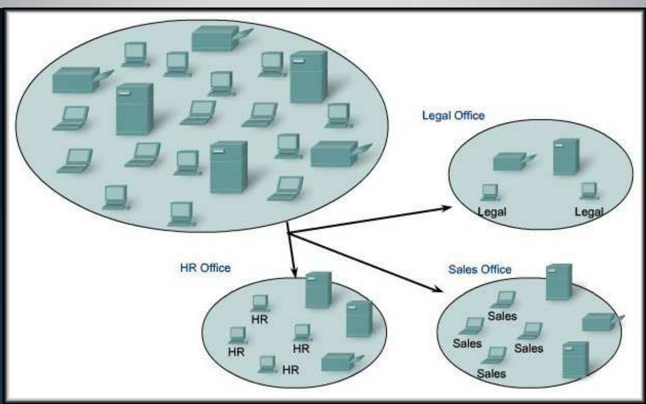


Dividing Hosts into Groups

Should it be

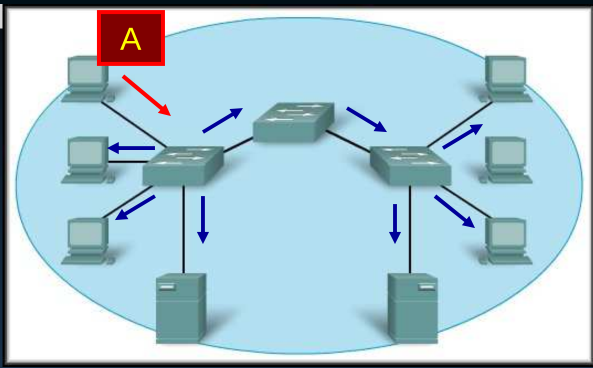


Why Separate Hosts into Networks?



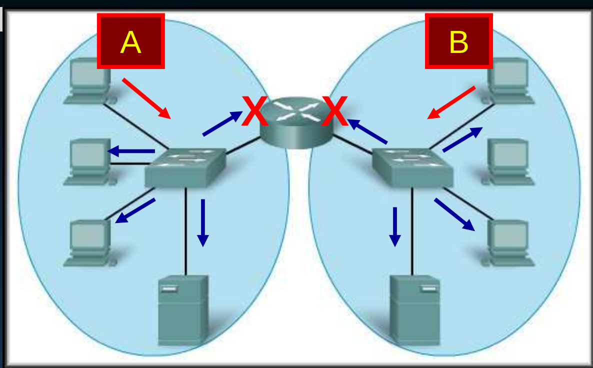
- Performance
- Security
- Address Management

Performance



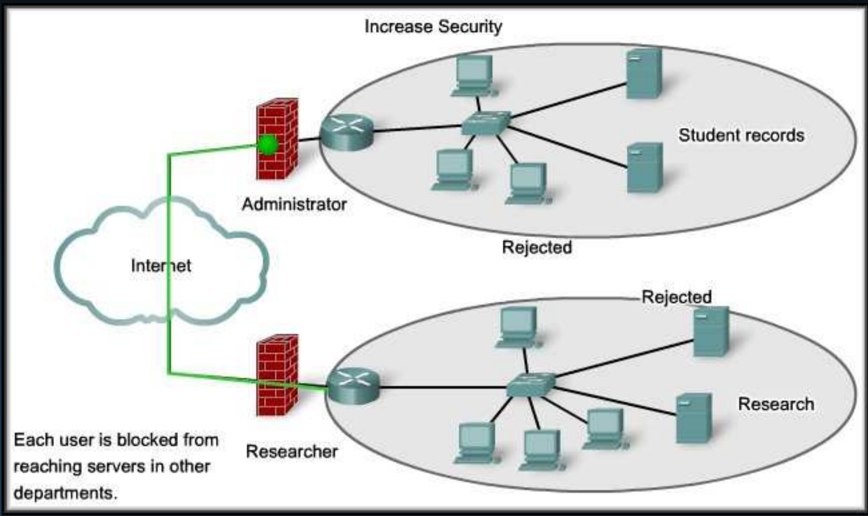
- Large numbers of hosts on a single network:
  - Actual Data
  - Overhead
- A big part of the overhead is **broadcasts**.
- In this context, each network is called a **broadcast domain**.
- Switches forward broadcasts to each device connected to a switch port.
- If we can reduce broadcast overhead, it would improve performance on the network.

Performance

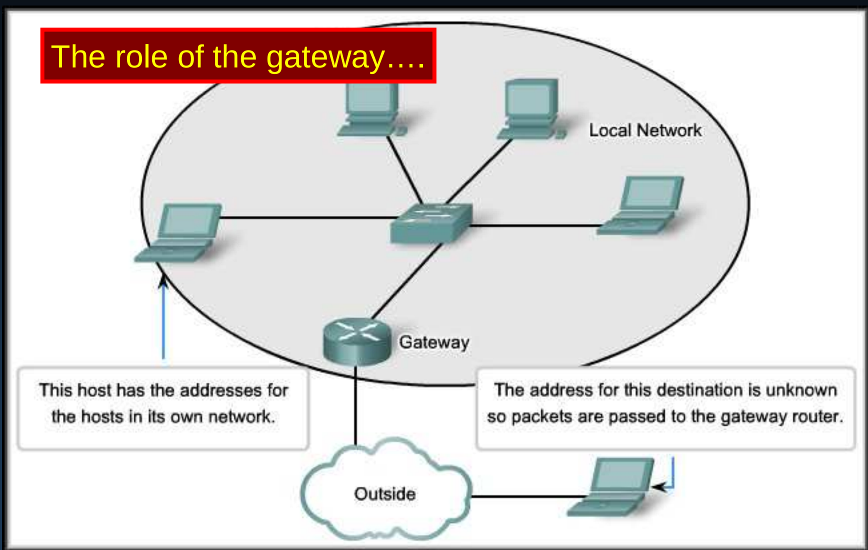


- **Routers block broadcasts** unless specifically configured to forward them.
- Replacing the switch in the diagram with a router, creates **two separate IP sub-networks and two broadcast domains.**
- Broadcasts are now contained within each network.

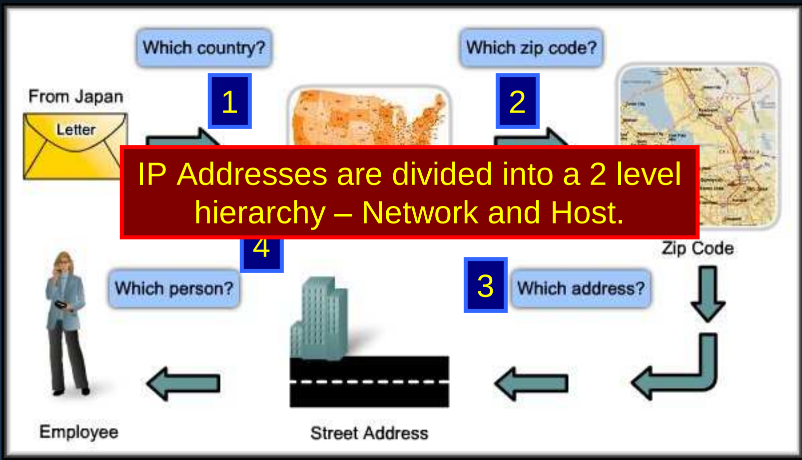
Security



Address Management



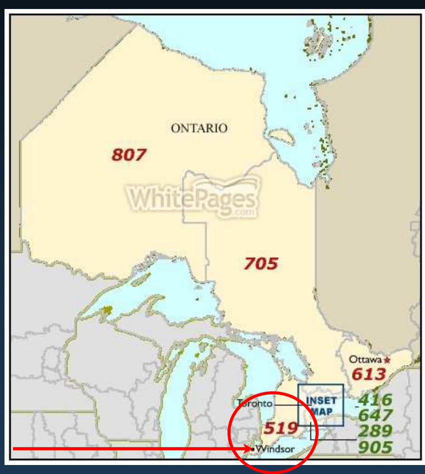
Hierarchical Addressing



IP Addresses are divided into a 2 level hierarchy – Network and Host.

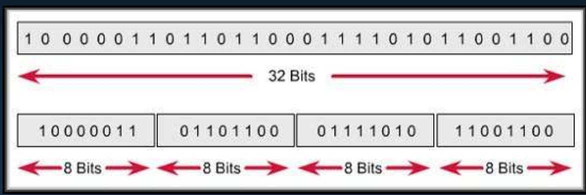
Dividing Networks from Networks

- The IP Version 4 Address contains elements that uniquely identify both the network and host.
- An IP Address is like a telephone number:
- 519-972-2727
  - 519 – Network Portion
  - 972-2727 – Host Portion
  - 519 – Windsor area
  - 972-2727 - St. Clair College



Dividing Networks from Networks

IP Version 4 addresses are 32 bits in length.



Divided into four separate groups of 8 bits each – 4 Octets.

Convert from binary to decimal – Dotted Decimal Notation.

Dividing Networks from Networks

- An IP Version 4 address has two parts:
  - Network number
  - Host number

  - The network portion of the address is the same for all hosts on the network.
  - Each device is identified by a unique host portion.

- *This hierarchy means that routers only need to know the network portion – not the address of each individual host.*

Dividing Networks from Networks

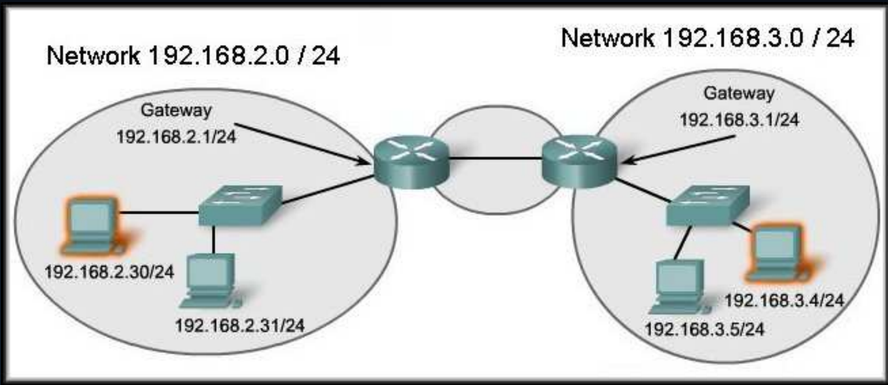
- There is a direct relationship, bit for bit, between the IP Address and it's associated subnet mask.
  - Any subnet mask bit that is a 1 means that the associated address bit belongs to the network number.
  - Any subnet mask bit that is a 0 means that the associated address bit belongs to the host number.

IP Address	192.	168.	1.	2
Subnet Mask	255.	255.	255.	0
Binary IP Address	11000000	10101000	00000001	00000010
Binary Subnet Mask	11111111	11111111	11111111	00000000

IP Addressing – The Subnet Mask

- There are two methods of expressing a subnet mask.
  - The traditional method is to use the decimal value of the 1 bits that apply to the network.
    - 192.168.1.2 255.255.255.0
      - This method is used for Classful Routing .
  - The new method is known as IP Prefix or CIDR.
    - Simply follow the IP address with a slash (/) and the number of bits that make up the network portion.
    - The remainder of the 32 bits are for the host number.
      - 192.168.1.2 / 24
        - This method indicates Classless Routing or Classless Interdomain Routing (CIDR).

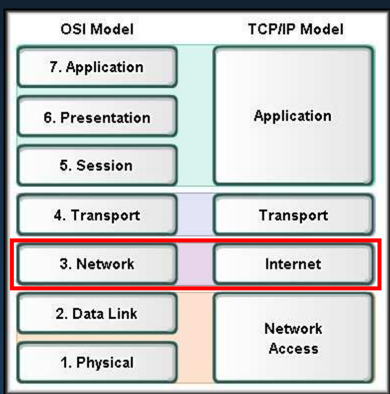
IP Addressing – The Subnet Mask



- The network portion of the IP address assigned to all hosts on a network segment must be the same.
  - All hosts on a segment have the same subnet mask.

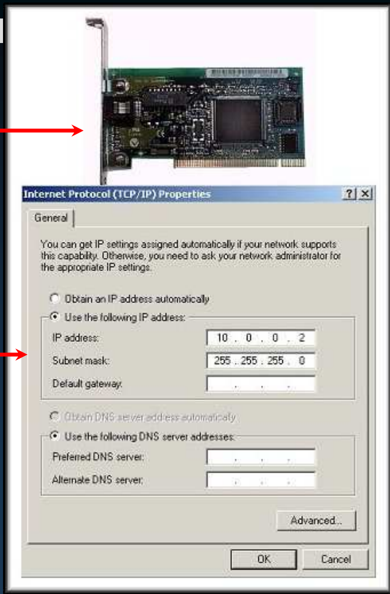
OSI Network Layer

Routing: How Data Packets Are Handled

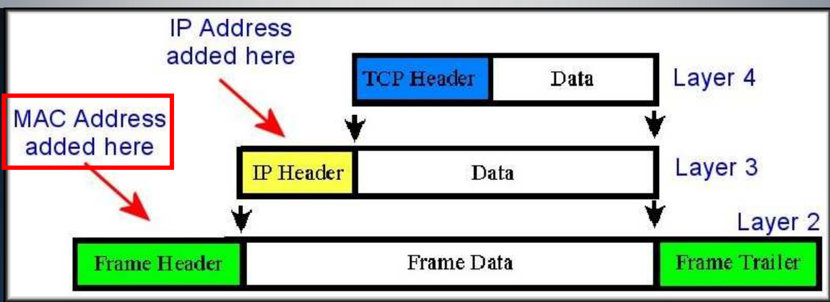


Address Types

- Two address types:
  - MAC address:
    - Physical address of the host
    - Burned in to the NIC
    - Layer 2 address
  - Network Address:
    - Logical address of the host
    - Assigned by network administrator
    - Layer 3 address

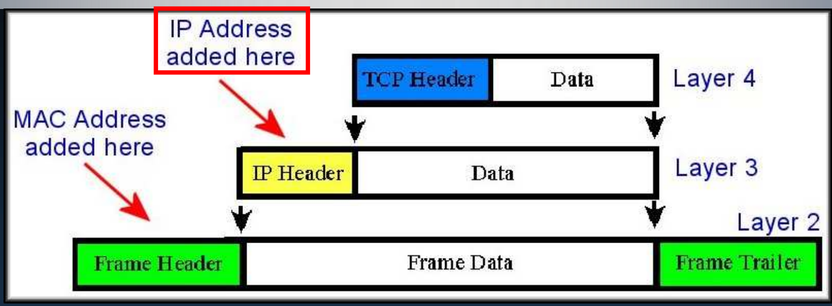


Each Host Has Two Addresses



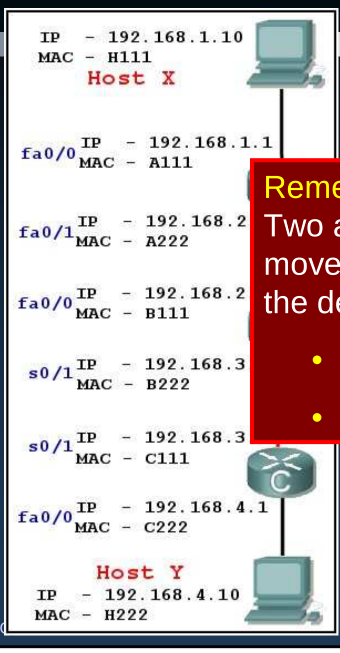
- Physical (MAC):
  - The physical address uniquely identifies the host from all other hosts on all other networks at Layer 2.
  - This is the address that is absolutely necessary to get the information into the host. The IP address by itself won't accomplish that.

Each Host Has Two Addresses



- Logical (IP):
  - The logical address uniquely identifies the host and the network to which it belongs at Layer 3.
  - Routers base their decisions on the NETWORK PORTION of the IP address when determining the best path for the packet.

IP Packets: Carrying Data End to End

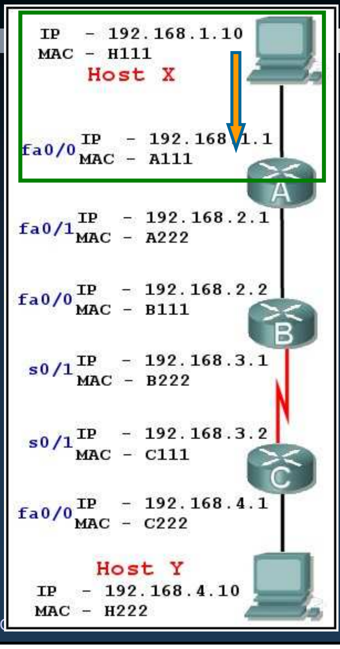


- Host X sends a packet to Host Y.
- A router generally relays a packet … ther, using … function – … rding … stages these routers use to route and switch this packet.

Remember:
Two addresses are needed to move a packet from the source to the destination.

- MAC Address
- IP Address

IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
A111	H111	192.168.4.10	192.168.1.10

- Host X begins by encapsulating a packet with Host Y's IP address and Router A's MAC address.

How does Host X know to forward the packet to Router A and not directly to Host Y?

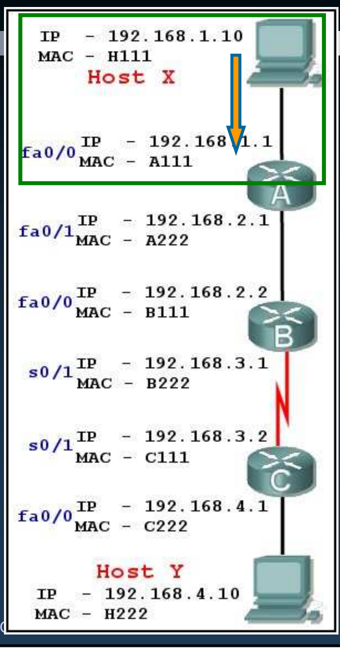
How does Host X obtain Router A's Layer 2 Address?

Host X determines that the destination is NOT on the same network. (More Later)

Queries the router for the router's MAC address (more later).

The packet is forwarded to the default gateway.

IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
A111	H111	192.168.4.10	192.168.1.10

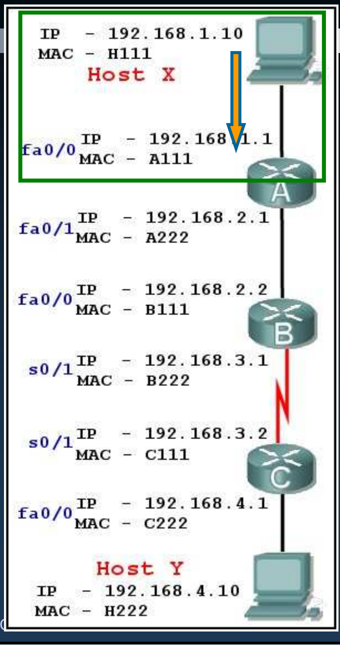
- Router A receives the packet on port fa0/0.

NOW what happens?

Router A uses the destination IP address to search its routing table for network 192.168.4.0/24.

It finds that it has a next hop address of 192.168.2.2 and an exit port of fa0/1.

IP Packets: Carrying Data End to End



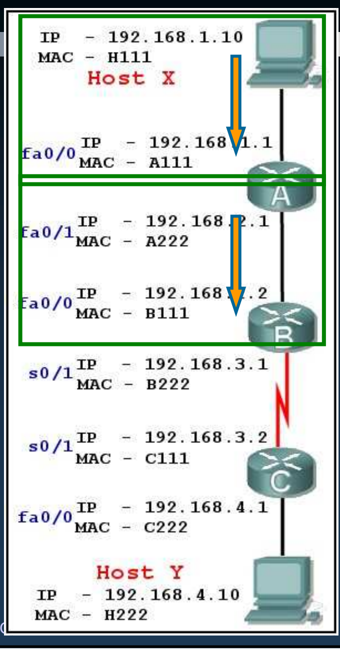
Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
A111	H111	192.168.4.10	192.168.1.10

- Router A knows that the exit port is an Ethernet interface.

NOW what happens?

Router A looks in a table of IP address to MAC address for all connected networks. If the network isn't there, it queries Router B for it's MAC address.

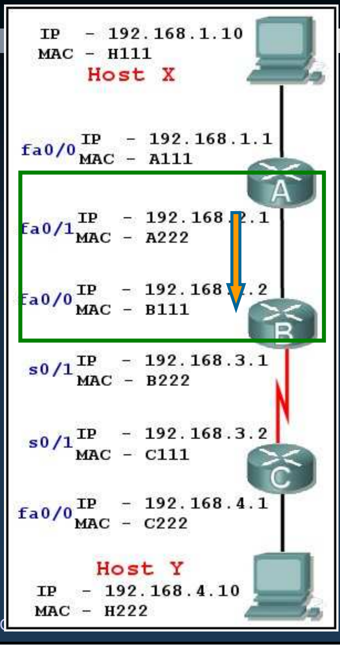
IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
B111	A222	192.168.4.10	192.168.1.10

- Router A now has all of the information it needs to forward the packet. It knows that the destination MAC address is B111 and that the exit port is fa0/0.
- Router A now re-encapsulates the frame, **changing the Layer 2 addresses** and forwards **(switches)** the frame out port fa0/1.

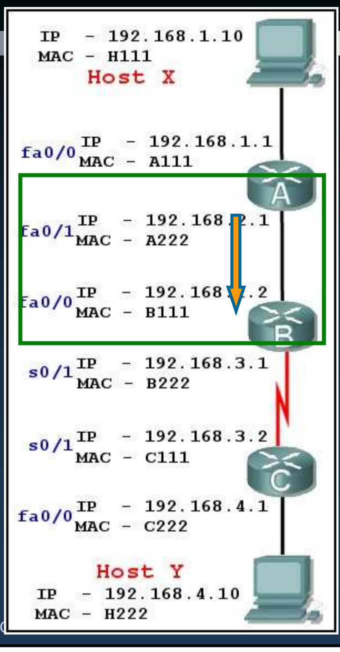
IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
B111	A222	192.168.4.10	192.168.1.10

- Notice that the Layer 3 addresses in the packet ***DID NOT*** change!
- Also notice that the ***routing table*** was used to find:
  - The next hop Layer 3 address
  - The next hop Layer 2 address
  - The exit port to use to forward the frame.

IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
B111	A222	192.168.4.10	192.168.1.10

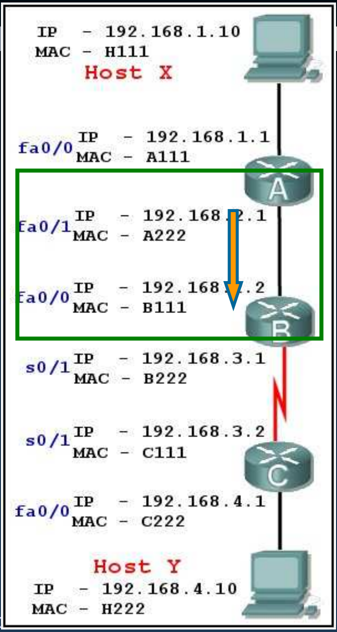
- Router B receives the packet.

NOW what happens?

Router B uses the destination IP address to search its routing table for network 192.168.4.0/24.

It finds that it has a next hop address of **192.168.3.2** and an exit port of **s0/1 – a serial interface.**

IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
B111	A222	192.168.4.10	192.168.1.10

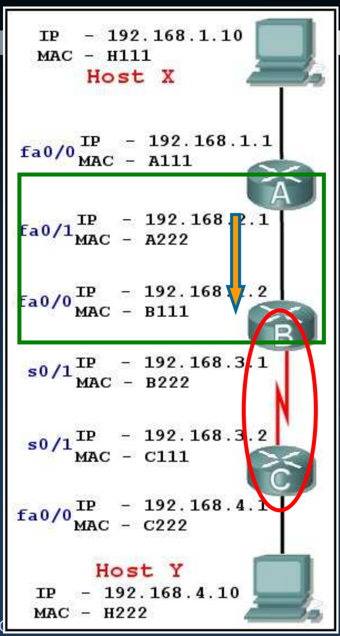
- Router B knows that the exit port is a **serial interface**.

NOW what happens?

Since the exit interface is a serial interface, **NOT** an Ethernet interface, Router B ***does not need*** the Layer 2 address for the next hop.

Remember, serial interfaces are like a pipe – one way in and one way out.

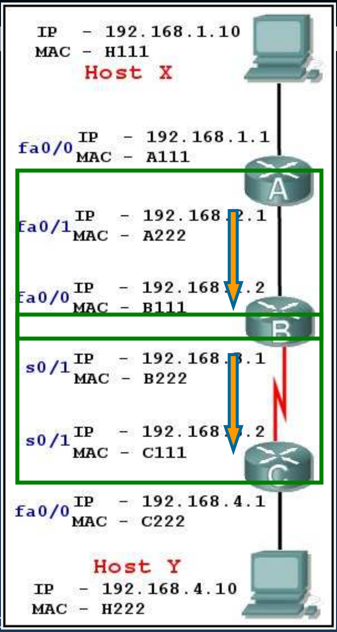
IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
B111	A222	192.168.4.10	192.168.1.10

- When the interface is a point-to-point serial connection, the routing table process does not even look at the next-hop IP address.
- Router B now encapsulates the IP packet into the proper data link frame, using the proper serial encapsulation (HDLC, PPP, etc.).

IP Packets: Carrying Data End to End



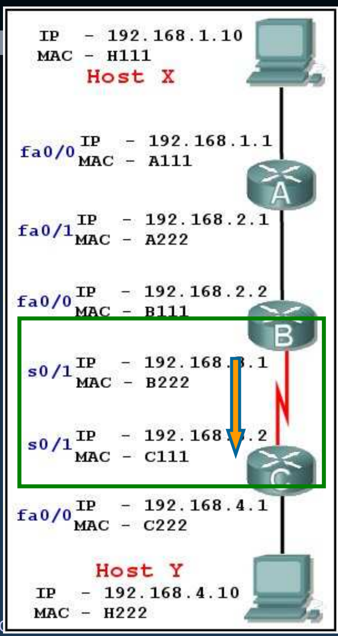
Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
FFFF	B222	192.168.4.10	192.168.1.10

The destination Layer 2 address is set to a **broadcast** since there is only one other end to the pipe.

The source Layer 2 address is set to the **exit port of Router B** – the source of the frame.

Finally, the frame is forwarded **(switched)** out port s0/1 on Router B.

IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
FFFF	B222	192.168.4.10	192.168.1.10

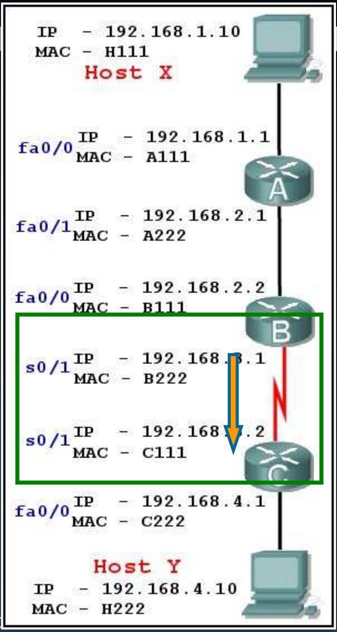
- Router C receives the frame on the serial interface - port s0/1

NOW what happens?

Router C uses the destination IP address to search its routing table for network 192.168.4.0/24.

It finds that the network is a **directly connected network** with an exit interface of fa0/0.

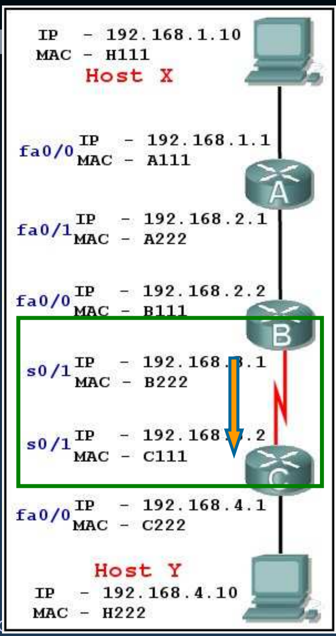
IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
FFFF	B222	192.168.4.10	192.168.1.10

- Router C realizes that this destination IP address is on **the same network as one of its interfaces** and it can send the packet ***directly to the destination*** and not another router.
- Since the exit interface is on an directly connected Ethernet network, Router C must obtain the destination's MAC address.

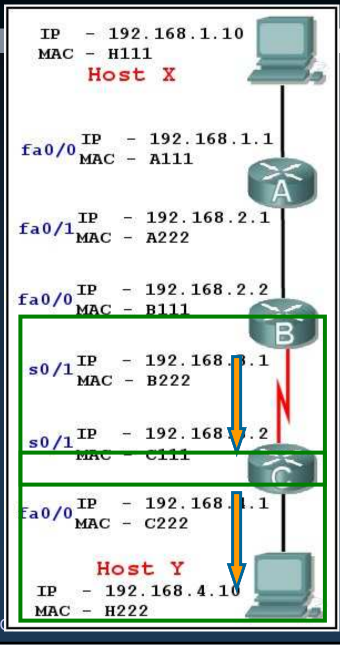
IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
FFFF	B222	192.168.4.10	192.168.1.10

- Router C looks in a table of IP address to MAC address for all connected networks.
- If the entry was not in the table, Router C would need to send a query out fa0/0 that says, **"What is the MAC address for this IP address?"**
- Host Y would send back a reply that says, **"This is the MAC address that matches the IP Address you sent."**

IP Packets: Carrying Data End to End



Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
H222	C222	192.168.4.10	192.168.1.10

Router C encapsulates the Ethernet frame and uses the **destination MAC address** of Host Y.

The source Layer 2 address becomes the MAC address of the **router's fa0/0 port**.

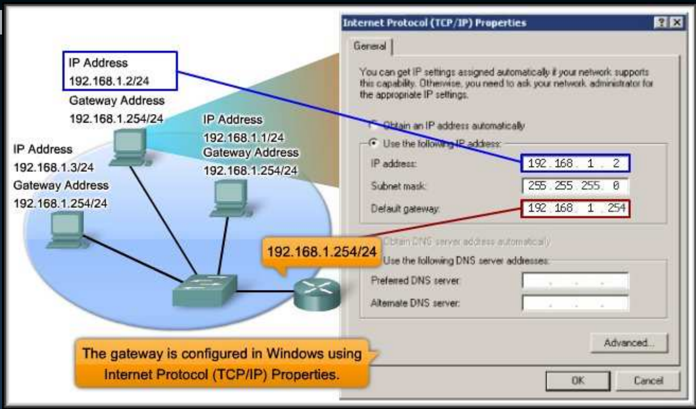
The frame is forwarded **(switched)** out port fa0/0 to the destination host – Host Y.

IP Packets: Carrying Data End to End

Step	Layer 2 Destination	Layer 2 Source	Layer 3 Destination	Layer 3 Source
Host X to Router A	A111	H111	192.168.4.10	192.168.1.10
Router A to Router B	B111	A222	192.168.4.10	192.168.1.10
Router B to Router C	FFFF	B222	192.168.4.10	192.168.1.10
Router C to Host Y	H222	C222	192.168.4.10	192.168.1.10

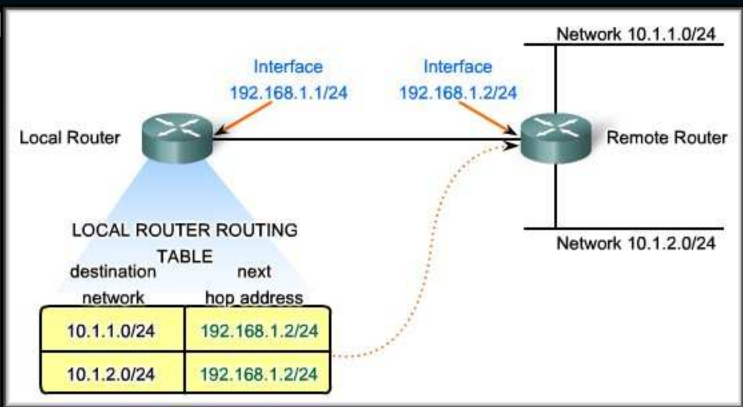
NOTICE THAT THE SOURCE AND DESTINATION IP ADDRESSES REMAIN UNCHANGED!!!

Gateway: The Way Out of the Network



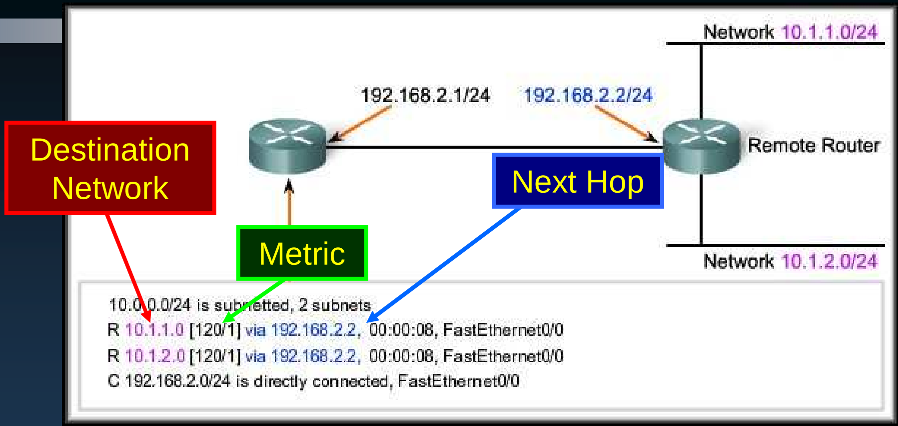
- Default Gateway is defined to all hosts on the network.
- Gateway address is the address of the router interface.
  - Network portion must be on the same network as all of the hosts.

Gateway: The Way Out of the Network



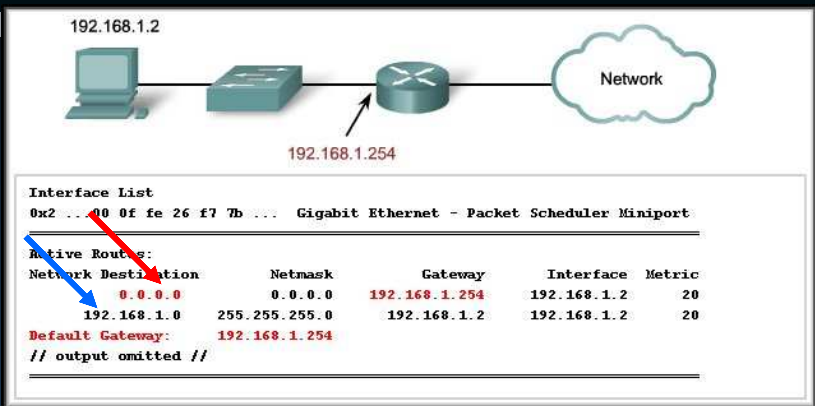
- Additionally, no packet can be forwarded without a route.
- A router makes a forwarding decision for each packet that arrives at the gateway interface.
- The destination may be one or more hops away.

Route: A Path to a Network



- The routing table stores information about directly connected and remote networks.
- Remote networks are networks not directly connected to the router (manual configuration or learned dynamically).

Host Routing Table



- Hosts also require a local routing table so that Network layer packets are directed to the correct destination network.
- Unlike a router, the host routing table usually contains only the host's address and the default gateway.

Destination Network - Routing Table Entries

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/0
C     192.168.1.0/24 is directly connected, FastEthernet 0/0
S*    0.0.0.0/0 [1/0] via 192.168.2.2
```

- The hierarchical nature of Layer 3 addressing means that…
  - One route entry could refer to a large general network.
  - Another entry could refer to a subnet of that same network.
  - When forwarding a packet, the router will select the most specific route.

Destination Network - Routing Table Entries

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/0
C     192.168.1.0/24 is directly connected, FastEthernet 0/0
S*    0.0.0.0/0 [1/0] via 192.168.2.2
```

- The default route in a routing table performs much the same function as a default gateway in a PC.
  - If a route for a packet cannot be found in the routing table, and a default route is present, that route will be used to forward the packet.

Destination Network - Routing Table Entries

Destination Network

Metric

Next Hop

```
Gateway of last reso    168.2.2 to network 0.0.0.0
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/0
C     192.168.1.0/24 is directly connected, FastEthernet 0/0
S*    0.0.0.0/0 [1/0] via 192.168.2.2
```

- If a packet arrives destined for **207.23.124.56**, the router would check the table in the following order:
  - 10.1.1.0
  - 10.1.0.0
  - 10.0.0.0
  - 0.0.0.0

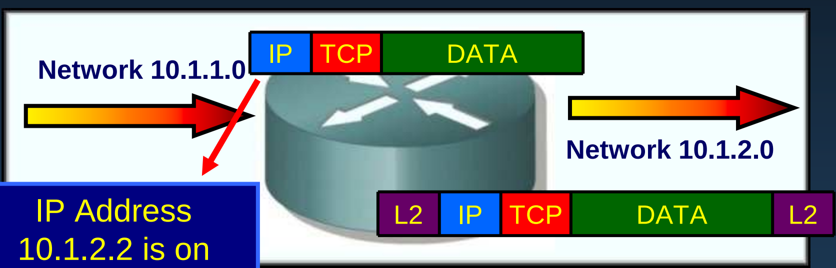
Since the route doesn't exist and a default route is configured, the packet would be forwarded to the next hop.

Packet Forwarding: Route Found

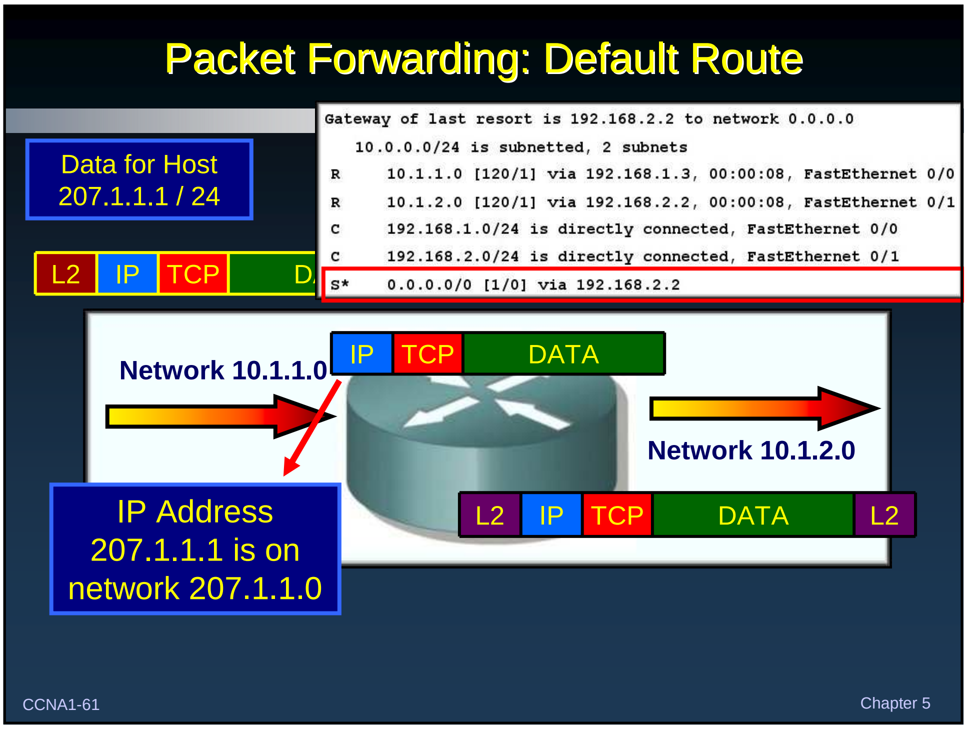
Data for Host 10.1.2.2 / 24

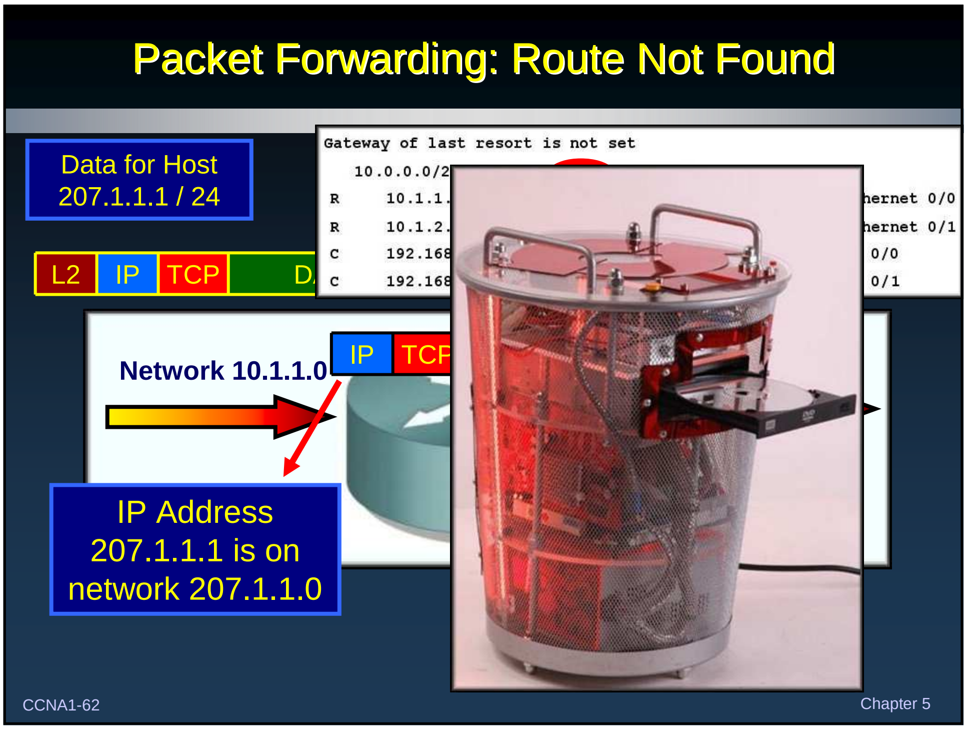
L2 | IP | TCP | D...

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.1.3, 00:00:08, FastEthernet 0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/1
C     192.168.1.0/24 is directly connected, FastEthernet 0/0
C     192.168.2.0/24 is directly connected, FastEthernet 0/1
S*    0.0.0.0/0 [1/0] via 192.168.2.2
```



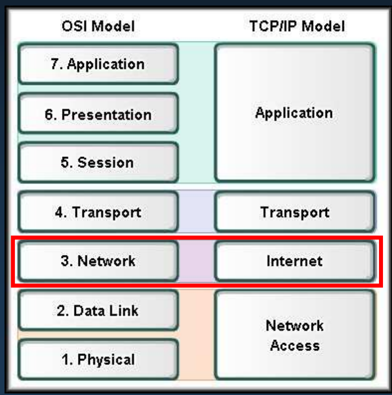
IP Address 10.1.2.2 is on network 10.1.2.0


Packet Forwarding: Default Route
Data for Host 207.1.1.1 / 24
L2 IP TCP D
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
10.0.0.0/24 is subnetted, 2 subnets
R 10.1.1.0 [120/1] via 192.168.1.3, 00:00:08, FastEthernet 0/0
R 10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet 0/1
C 192.168.1.0/24 is directly connected, FastEthernet 0/0
C 192.168.2.0/24 is directly connected, FastEthernet 0/1
S* 0.0.0.0/0 [1/0] via 192.168.2.2
IP TCP DATA
Network 10.1.1.0
Network 10.1.2.0
IP Address 207.1.1.1 is on network 207.1.1.0
L2 IP TCP DATA L2
CCNA1-61
Chapter 5

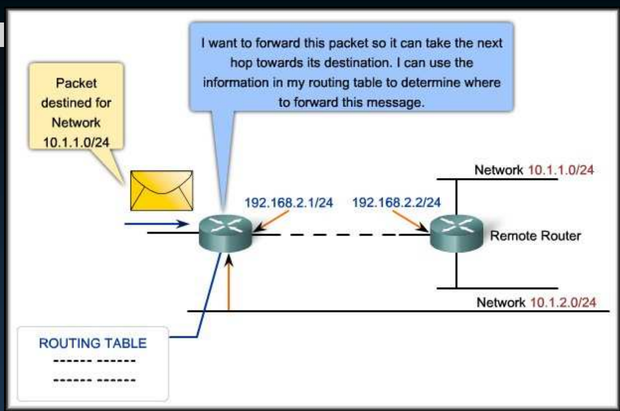

Packet Forwarding: Route Not Found
Data for Host 207.1.1.1 / 24
L2 IP TCP D
Gateway of last resort is not set
10.0.0.0/2
R 10.1.1.
R 10.1.2.
C 192.168
C 192.168
ernet 0/0
ernet 0/1
0/0
0/1
IP TCP
Network 10.1.1.0
IP Address 207.1.1.1 is on network 207.1.1.0
CCNA1-62
Chapter 5

OSI Network Layer

Routing Processes: How Routes Are Learned

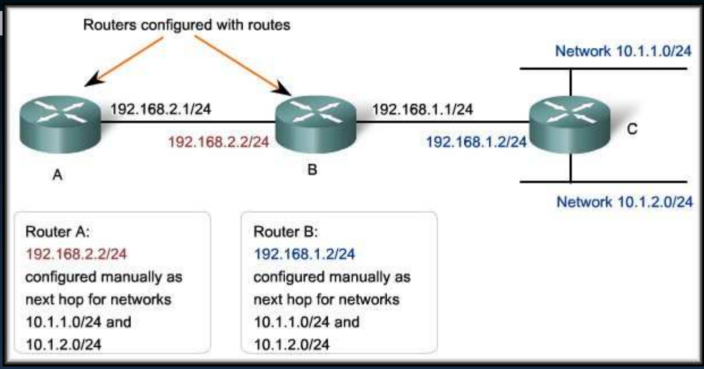


Routing Processes: How Routes Are Learned



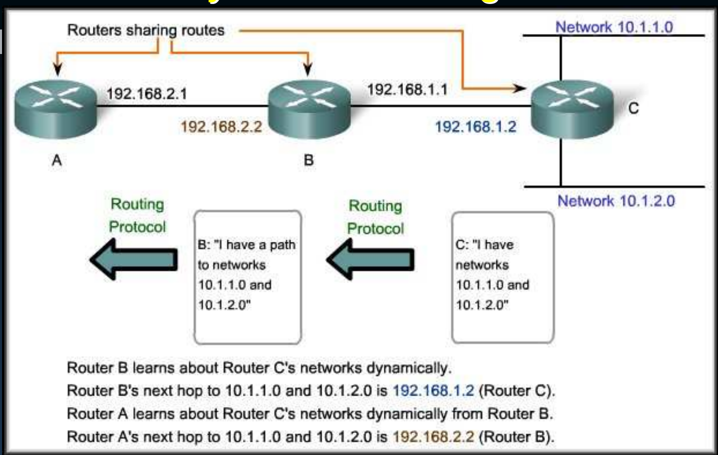
- Routing requires that every hop, or router, along the path to a packet's destination have a route to forward the packet.
- The routing table contains the information to make packet forwarding decisions.
- Information is learned in two ways:
  - Manual configuration of the information (Static)
  - Information received from another router (Dynamic)

Static Routing



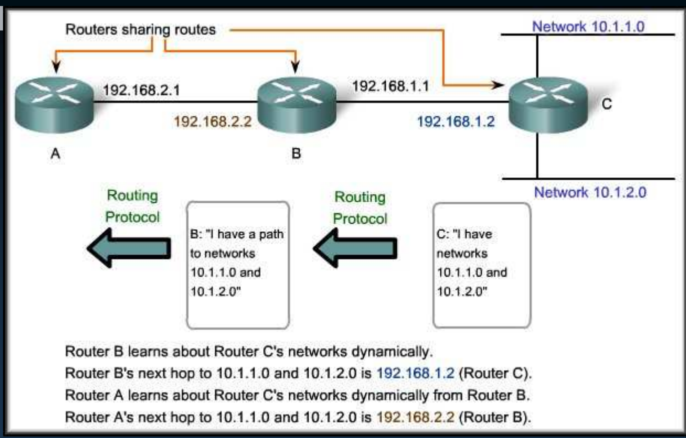
- Manually configured.
- Must know network structure.
- Every router between each source and destination must have routes.
- Changes to the topology require static route changes.

Dynamic Routing



- Routing information is exchanged among the routers using a **routing protocol**.
- Route always up to date with little administration but creates overhead.

Routing Protocols



- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Protocol (EIGRP)
- Open Shortest Path First (OSPF)