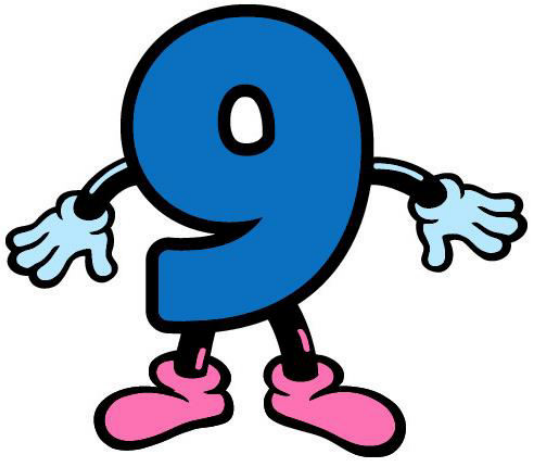
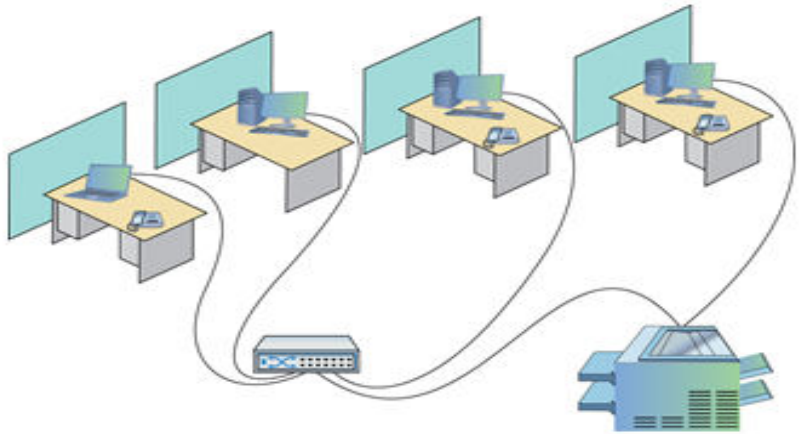


Routing

- Routing
- Router
- Routing table
- Static & Dynamic Routing
- Routing protocols



A real-world network....ish

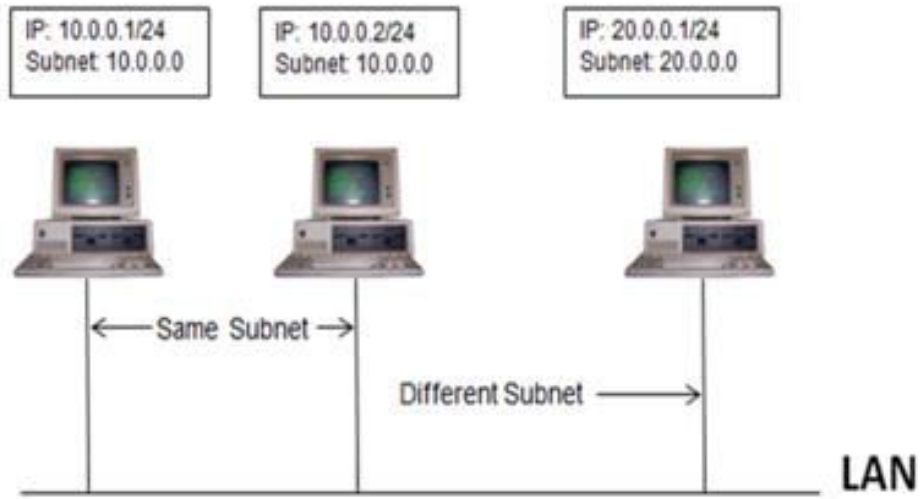
You rarely have a switch without a router

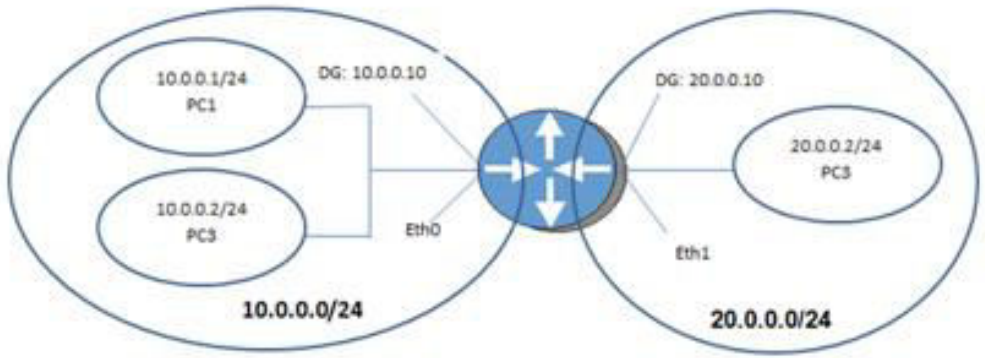
No router → no connection to the Internet

Routers connect separate networks (TCP/IP networks)

Routing is the act of forwarding network packets from a source network to a destination network
(determined by the ANDing process)

Only a **router** has the internetwork information and logic required to make correct decisions about how to best forward a packet





Routers route packets between different subnets

Connect 2 or more network segments

Router

Connects different separate LANs (LAN → WAN)

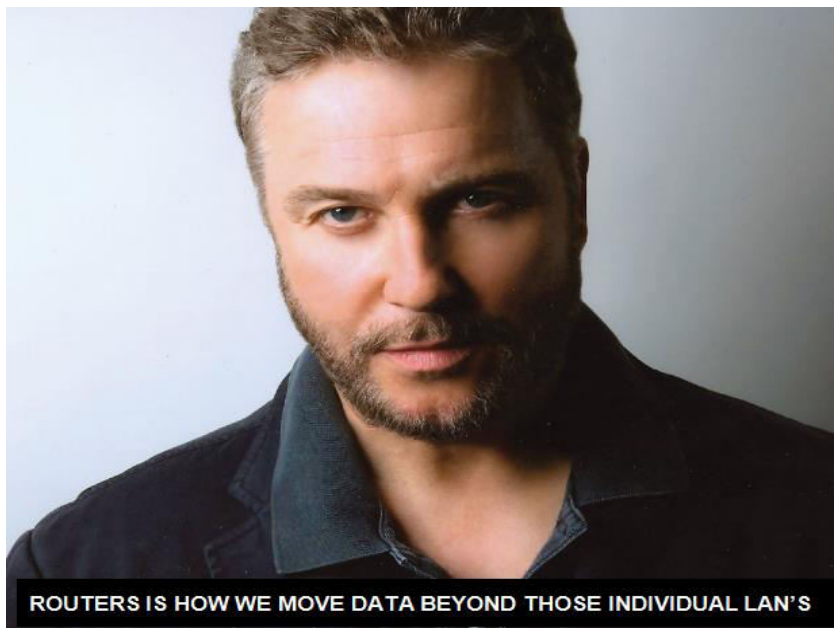
Primary Function: forward packets between networks based on destination IP address

Layer 3 device

"A computer" running code (**Cisco IOS** (**Internetwork Operating System)** that determines how and where to forward/route packets bound for other networks

Each port, or interface connects to a different local network or subnet

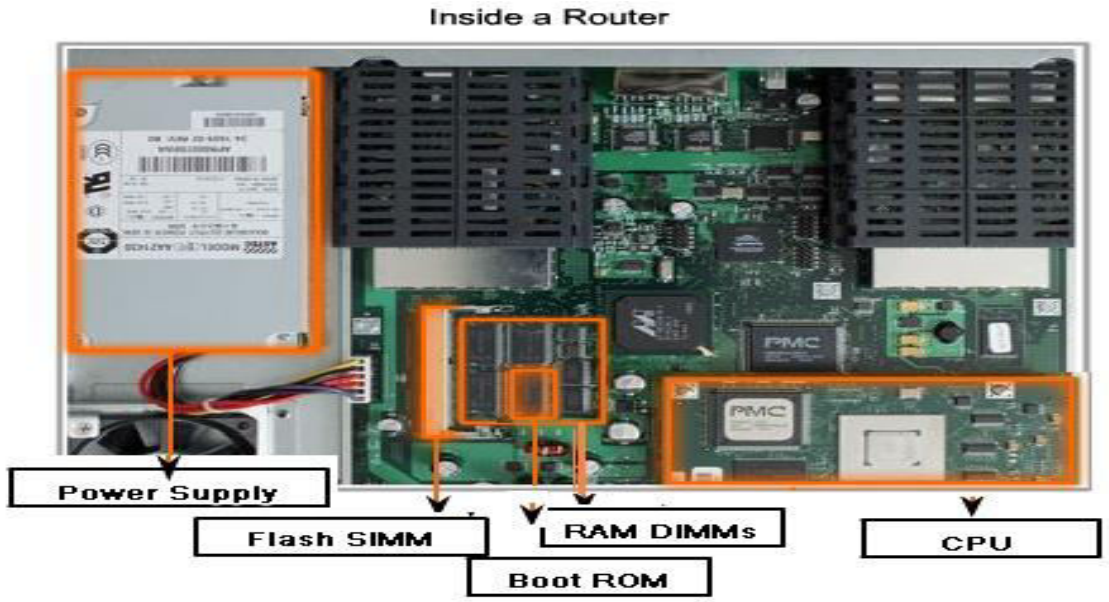
Switching is how we move data around a LAN



Router

Highly specialized computer that specialize in sending packets over the data network.

CPU
RAM
OS
Motherboard
BIOS
NIC (s)
I/P Ports
Power Supply
Chassis



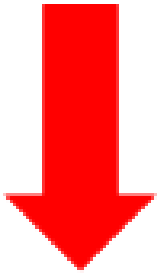
Operating System

Interact with Cisco Router via Cisco IOS.

Current version is IOS Version 15

IOS provides a CLI which allows us to check status of router and allows us manage and configure the router.

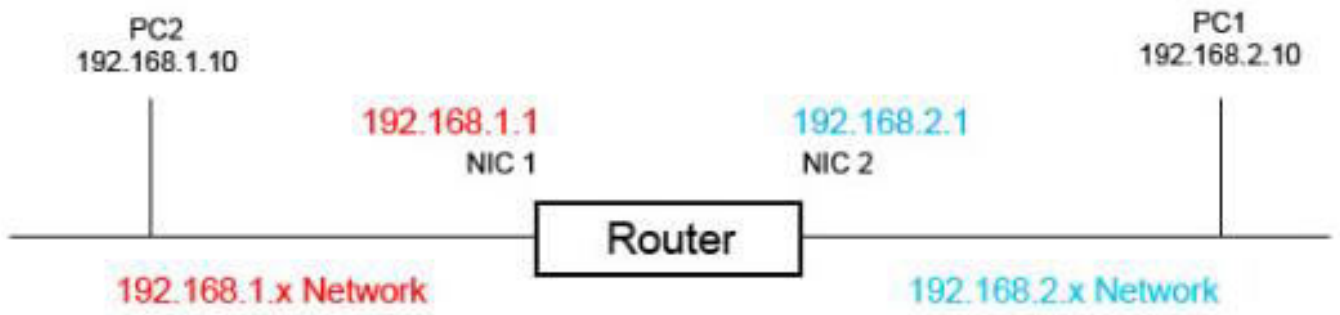
Router does not become functional until it loads the IOS



Without the IOS, the hardware has no capability

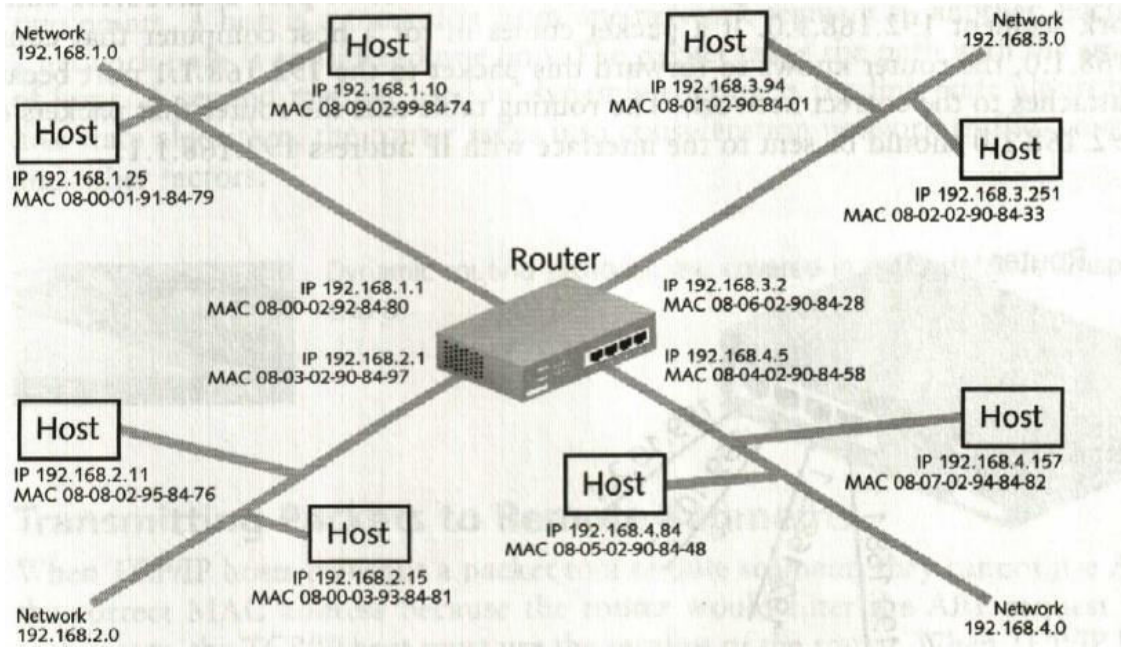
Router will have at least two network cards (NIC's)
(1 physically connected to one network and the other 1 physically connected to another)

Router can connect multiple networks together, provided it has a dedicated NIC for each network



Routers requires a separate identity for each network that's connected to it.

IP address for each network segment + a separate NIC for each port or network segment.



Router connects 4 different network segments must have 4 different IP addresses and 4 different network interfaces.

Packet Filtering

Router monitors packets entering from public side and then allowing/denying them access to n/w based on defined rules/criteria

Traffic Control

Forward only packets that addressed to hosts on other n/w's → Routers create CD's and BD's

LET'S BE CLEAR

Routing determines where to forward IP data packets that are destined for addresses not on the same network or subnet

Things to Consider

To insure the successful delivery of packets

When should you route?

What is the best route?

How is the best route determined?

What if the network topology changes?

What if there is a network fault?

What if the destination does not exist?

Routing Process

(starts at the workstation)

Local workstation starts the communication i.e. determines if the destination workstation is local or not

(ANDing process)

Packets destined for computers not on their local network get sent to the **default gateway.**

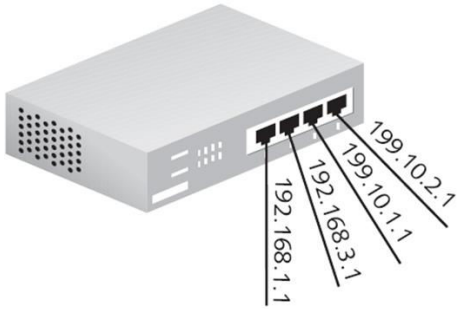
Router recognizes that the destination is on a different subnet.

Router must determine which subnet should receive the frame.

Router removes the layer 2 information as it contains its MAC address (no longer necessary as the router now has the packet).

Host got the routers MAC address by looking in its ARP cache or send ARP request if the address was not in the ARP table.

Router then analyses the destination IP address (the IP address is not that of the router, but of the final destination



Use IP address to route packets to correct network segment.

Router connecting 4 different network segments. Each port has its own unique IP address and the addresses are on different networks.

Routers filter traffic based on logical address NOT like bridge/switch which filter based on physical address

Like bridge/switch, routers use a **table** to determine how to forward packets

Simplified view of routing table

Code	Network, Mask	AD/Metric	Next Hop	Interface
O	10.0.0.0/8	110/120	200.1.1.1	S0
O	172.16.0.0/16	110/15	200.1.1.1	S0
O	192.168.1.0/24	110/20	200.2.2.2	S1
C	210.1.1.4/30	0/0	Directly connected	E0

All TCP/IP hosts that wish to send IP datagrams across a network must be capable of making routing decisions

Every TCP/IP host and router with a valid IP address **must** have a built in routing table.

A device uses the routing table to determine how an IP datagram is delivered in an IP network

Simply, routing table contains information about how an IP datagram should be routed.

Workstations have very brief routing tables

Purpose of local route table: provides the host with information about how to handle the forwarding of packets exiting the workstation.

Once the ANDing process has determined that a packet needs to be routed, the local route table is consulted to determine where to forward the packet.

Command to see workstation route table
c:\>route print or netstat –r, or netstat –rn

```
Routing Table
===========================================================================
Interface List
0x1 ...........................MS TCP Loopback Interface
0x000003.....00 50 DA 12 55 16.....3COM EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination    Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0      127.0.0.1    127.0.0.1       1
        192.168.1.0    255.255.255.0  192.168.1.100  192.168.1.100       1
      192.168.1.100  255.255.255.255      127.0.0.1    127.0.0.1       1
      192.168.1.255  255.255.255.255  192.168.1.100  192.168.1.100       1
          224.0.0.0  255.255.255.255  192.168.1.100  192.168.1.100       1
    255.255.255.255  255.255.255.255  192.168.1.100              2       1
Default Gateway       192.168.1.1
===========================================================================
Persistent Routes:
  None
```

- 127.0.0.0 –Although 127.0.0.1 is assigned to the local NIC, if this entries was not in the routing table your PC would try to send these to the default gateway as the next entry it would closely match would be the 0.0.0.0 one.
- 192.168.1.0 – These next 3 lines are for your local network. The first one is the entire 192.168.111.x range as defined by the netmask of 255.255.255.0.. These are created automatically like the others when you configure your TCP/IP settings.
- 224.0.0.0 – These are also default entries for multicasting.
- 255.255.255.255 – This is also a default entry and can be ignored.

When an IP datagram arrives at a decision point (either a host or a router)

Destination IP address is compared against each entry in the routing table.

Entry with the longest string of matching bits is used to determine which interface best supports delivery of the datagram

Routing in a nutshell…..

Routing process starts with the host that creates the IP packet.

Host asks the question “Is the destination IP address of this new packet in my local subnet?”

If the destination is local, send directly

Find the destination host’s MAC address.

Use the already-known Address Resolution Protocol (ARP) table entry, or use ARP messages to learn the information.

Encapsulate the IP packet in a data-link frame, with the destination data-link address of the destination host.

If the destination is not local, send to the default gateway

Find the default gateway’s MAC address.

Use the already-known Address Resolution Protocol (ARP) table entry, or use ARP messages to learn the information.

Encapsulate the IP packet in a data-link frame, with the destination data-link address of the default gateway

Router receives the frame

For each received data-link frame, router chooses whether or not to process the frame.

Process the frame if

Frame has no errors

As per the data-link trailer Frame Check Sequence [FCS] field)

Router discards/ignores all frames that had bit errors during transmission

Router makes no attempt at error recovery i.e. does not ask the sender to retransmit the data

+

Frame's destination data-link address is the router's address

(or an appropriate multicast or broadcast address).

Router can actually receive a frame sent to some other unicast MAC address, and routers should ignore these frames

LAN switches forward unknown unicast frames: frames for which the switch does not list the destination MAC address in the MAC address table.

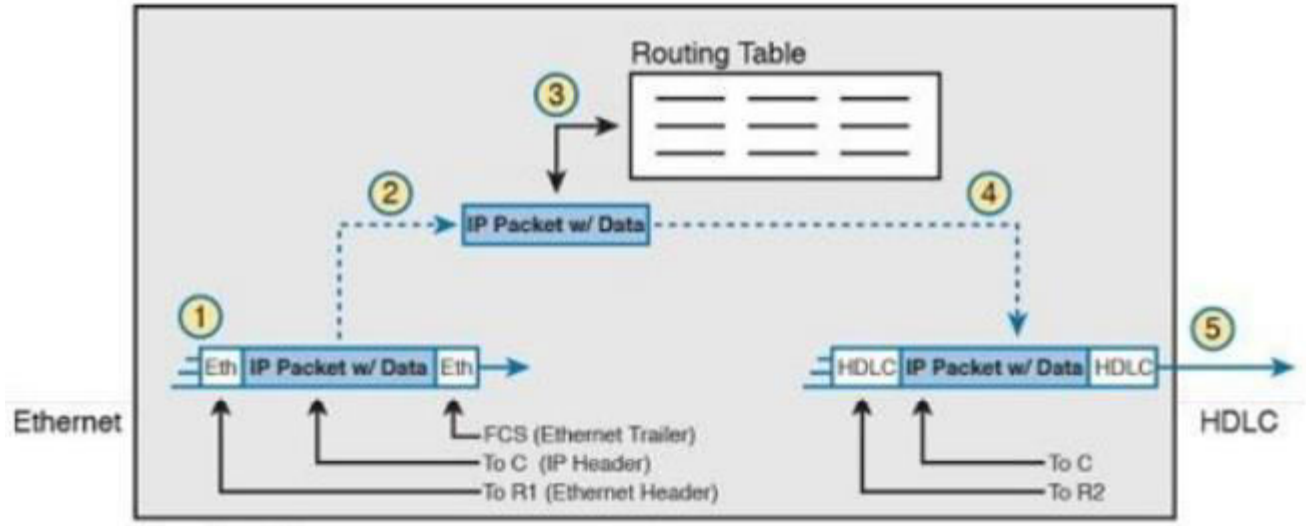
LAN switch floods those frames resulting routers sometimes receive frames destined for some other device

Router decides to process the frame

De-encapsulate the packet from inside the data-link frame.

In router memory, the router no longer needs the original frame's data-link header and trailer

So the router removes and discards them, leaving the IP packet



Make a routing decision

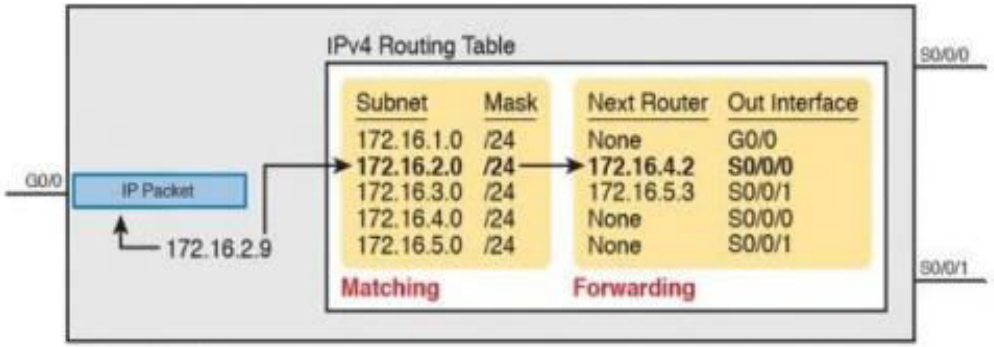
Router compares the packet's destination IP address to the routing table (range of addresses defined by each subnet) and find the route that matches the destination address

This route identifies the outgoing interface (via the forwarding information in the route) of the router and possibly the next-hop router.

Part of each route is used to match the destination address of the packet, while the rest of the route lists forwarding instructions: where to send the packet next.

Routes for remote subnets typically list both an outgoing interface and next-hop router IP address.

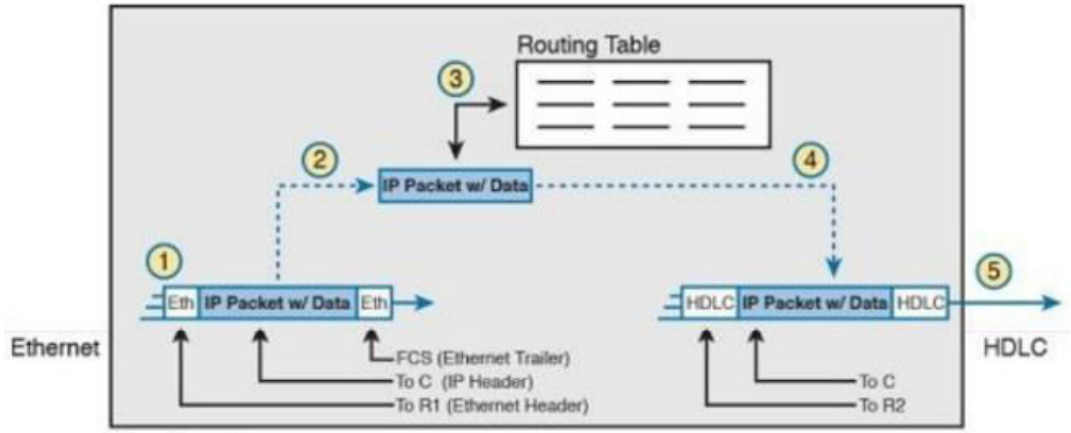
Routes for subnets that connect directly to the router list only the outgoing interface as these packets to these destinations do not need to be sent to another router



Router knows how it will forward the packet.

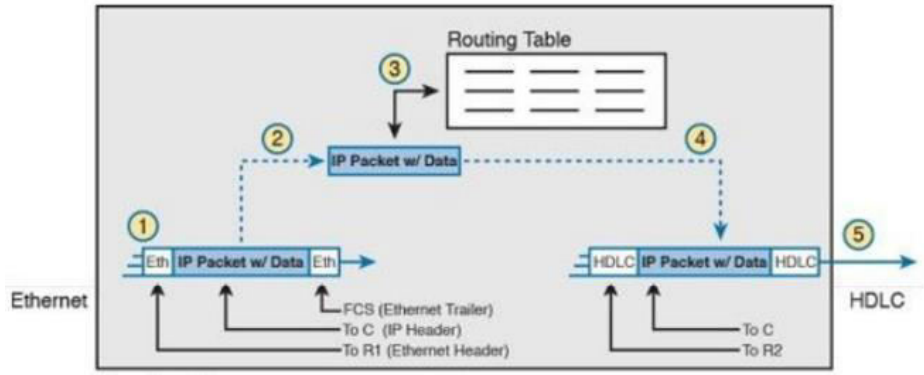
Encapsulate the packet into a data-link frame appropriate for the outgoing interface.

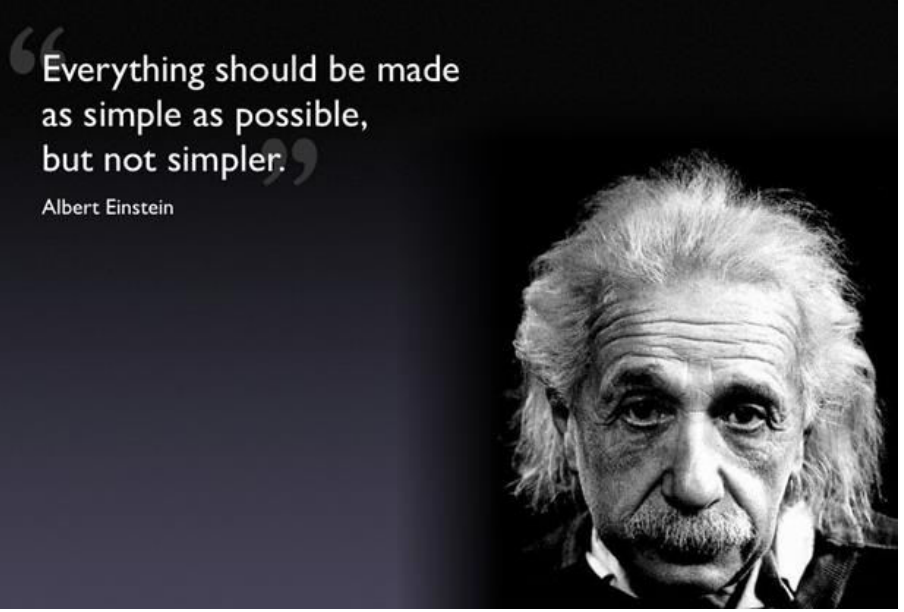
When forwarding out LAN interfaces, use ARP as needed to find the next device's MAC address.



Transmit the frame out the outgoing interface, as listed in the matched IP route.

Router might have to wait, particularly if other frames are already waiting their turn to exit the interface.





Router receives a frame

Router removes the packet from inside the frame

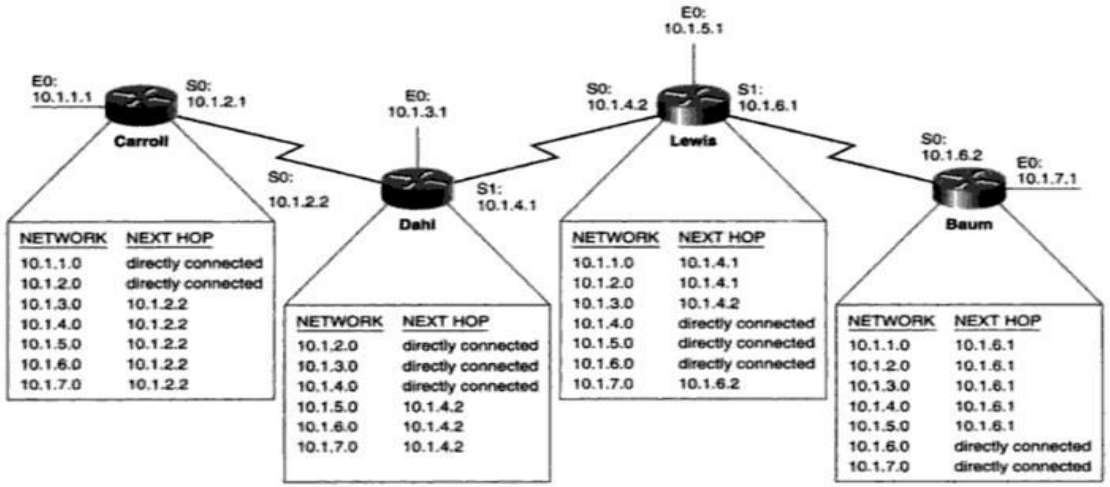
Router decides where to forward the packet

Router puts the packet into another frame

Router sends the frame

Destination addresses that the router can reach are listed in the Network column of the route tables.

Pointers to the destinations are in the Next Hop column.



Router Carroll receives a packet with a source address of 10.1.1.97 and a destination address of 10.1.7.35

Route table lookup determines that the best match for the destination address is subnet 10.1.7.0

Reachable via next-hop address 10.1.2.2, on interface S0

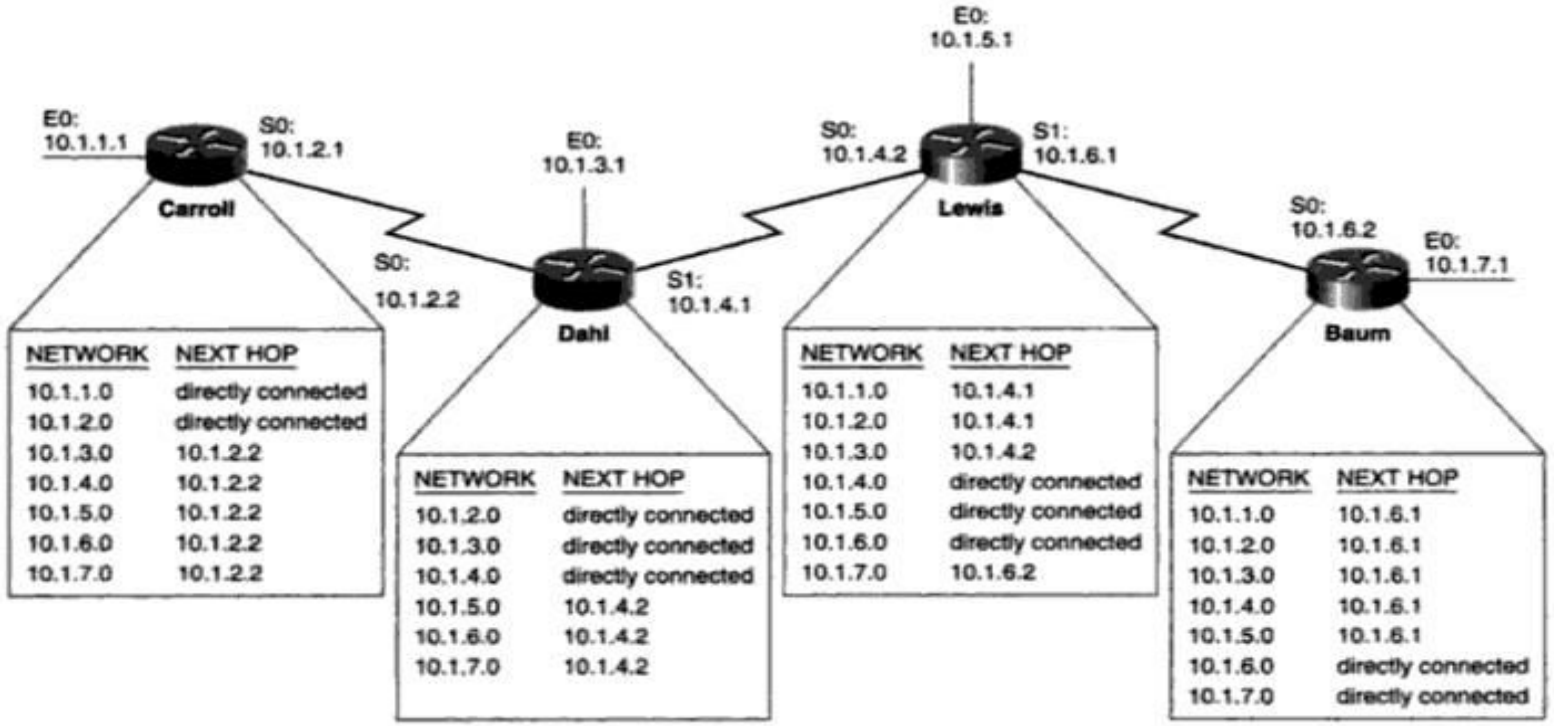
Packet is sent to that next router (Dahl)

Dahl does a lookup in its own table and sees that network 10.1.7.0 is reachable via next-hop address 10.1.4.2, out interface S1. This process continues until the packet reaches router Baum

Baum, receiving the packet on its interface S0, does a lookup, and sees that the destination is on one of its directly connected networks, out E0.

Routing is completed, and the packet is delivered to host 10.1.7.35 on the Ethernet link

Every router must have consistent and accurate information for correct packet switching to occur



In the example above an entry for network 10.1.1.0 is missing from Dahl's route table.

A packet from 10.1.1.97 to 10.1.7.35 will be delivered

But when a reply is sent from 10.1.7.35 to 10.1.1.97, the packet is passed from Baum to Lewis to Dahl.

Dahl does a lookup and finds that it has no entry for subnet 10.1.1.0

Packet is dropped, and an ICMP Destination Unreachable message is sent to host 10.1.7.35.

In a small office/home (< 10 PC's), you do not need a router that just does routing

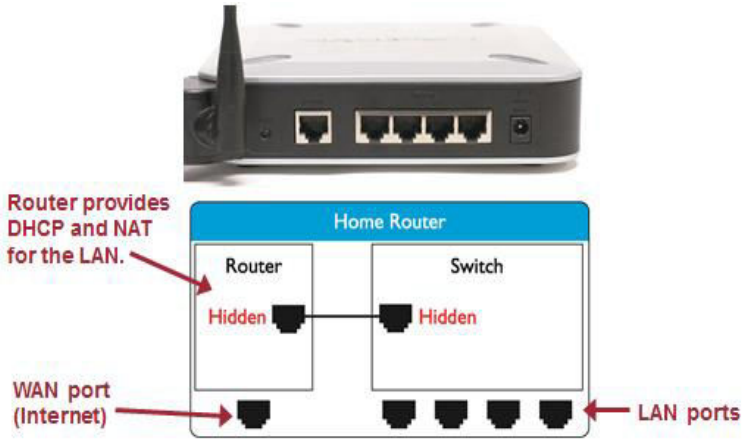
SOHO ROUTER

Combines multiple logical devices into one physical device

Not only a router

BUT A

Switch
Wireless Access Point
DHCP server
DNS server (just turn on/off, very little else you can do)
Port Forwarding
Firewall (blocks ports)
NAT server



Router routes packets
Uses a routing table to make these decisions

Routing Table

Routers depend upon route tables to determine how to route incoming packets

'heart of routing'

List every network that a router is aware of

Simplified view of routing table

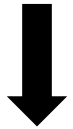
Code	Network, Mask	AD/Metric	Next Hop	Interface
O	10.0.0.0/8	110/120	200.1.1.1	S0
O	172.16.0.0/16	110/15	200.1.1.1	S0
O	192.168.1.0/24	110/20	200.2.2.2	S1
C	210.1.1.4/30	0/0	Directly connected	E0

Routers gather and maintain **routing information** to enable the transmission and receipt of data packets

Routing information takes the form of entries in a routing table with one entry for each identified route

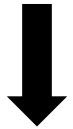
Route tables help packets along their way, one hop at a time.

NO single route table entry reveals the full path to the destination network.
(Best a routing entry can do is point to the next router along the path)



Code	Network, Mask	AD/Metric	Next Hop	Interface
O	10.0.0.0/8	110/120	200.1.1.1	S0
O	172.16.0.0/16	110/15	200.1.1.1	S0
O	192.168.1.0/24	110/20	200.2.2.2	S1
C	210.1.1.4/30	0/0	Directly connected	E0

(check note page for details on route table)



10.0.0.0
(first route in the list)

Table does not indicate precisely where is 10.0.0.0
Full path to the destination is not indicated.
Table does not indicate that to get to the 10.0.0.0 network, you must first get through the 63.0.0.0 network.
All the entry says about the path to 10.0.0.0 is that you must forward packets to the 200.1.1.1 via interface S0.
200.1.1.1 is the next hop router.

Router does not have to worry about how the packet gets to 10.0.0.0 (leaves that job to the next router down the line

Router checks its routing table to determine which of its interfaces is connected to the destination network or where to forward the packet.

Router then rebuilds the layer 2 information and sends frame out that interface.

Routing table is used to router packets from one network to another.

Simplified view of routing table

Code	Network, Mask	AD/Metric	Next Hop	Interface
O	10.0.0.0/8	110/120	200.1.1.1	S0
O	172.16.0.0/16	110/15	200.1.1.1	S0
O	192.168.1.0/24	110/20	200.2.2.2	S1
C	210.1.1.4/30	0/0	Directly connected	E0

Option A: If the router is directly connected to that network

It will readdress the frame at layer 2 with the Mac address of the destination host.
It will get the MAC address from its ARP cache.
If not found in the ARP cache, then it will send an ARP request on the destinations segment to get MAC address

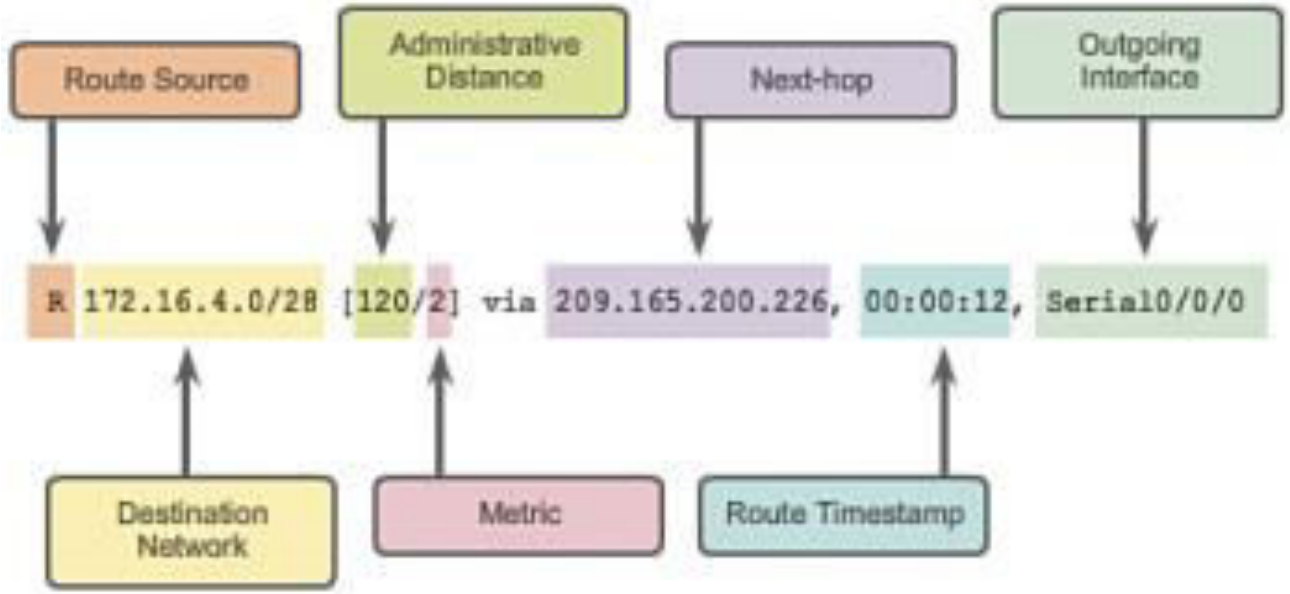
Option B: If the router is not directly connected to the network in question

It will send the packet to the next router in the path on the way to the destination.
The destination IP address will stay the same but the destination MAC address will be that of the next router

If there was a “rule of thumb” with regards to routing
Most specific route wins

Route with the longest subnet prefix that matches a given packet’s destination IP address will be used to route that packet.

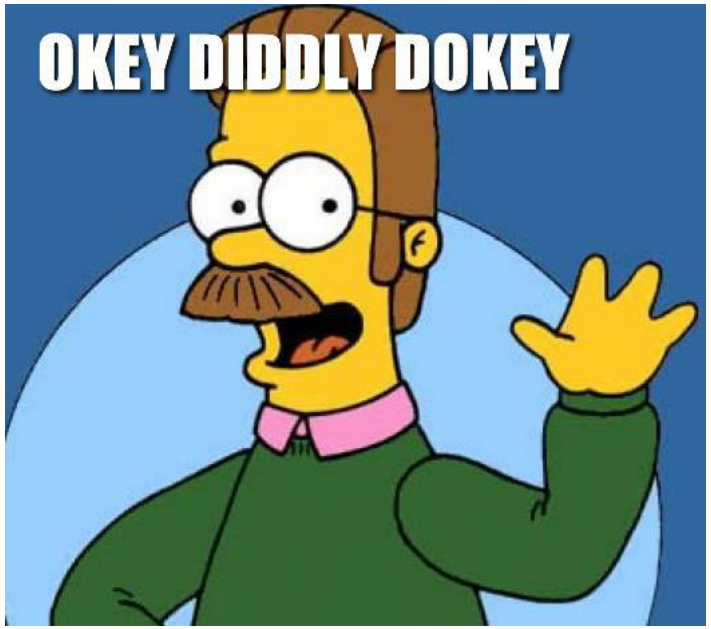
When there is a tie, there are other mechanisms that allow a route to be selected, such as administrative distance, and metric.



- **Route source**: Identifies how the route was learned.
- **Destination network**: Identifies the address of the remote network.
- **Administrative distance**: Identifies the trustworthiness of the route source.
- **Metric**: Identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
- **Next hop**: Identifies the IPv4 address of the next router to forward the packet to.
- **Route timestamp**: Identifies from when the route was last heard.
- **Outgoing interface**: Identifies the exit interface to use to forward a packet toward the final destination.

When packets take a certain route to their destination they DO NOT have to take the same route back.

Packets DO NOT record the route they take



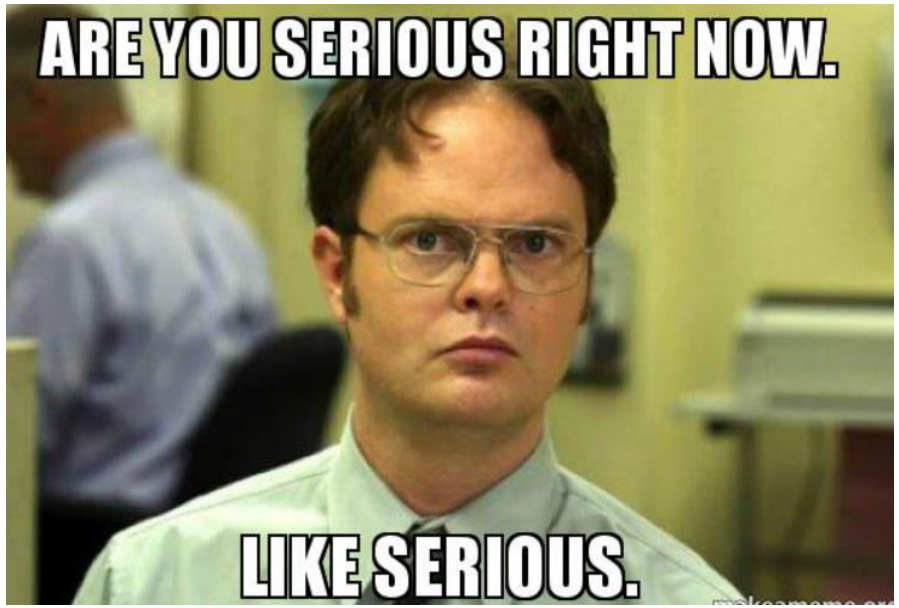
Packet will be transferred around the internetwork till the destination is found

Or

Till the hop count reaches its max.

Routers automatically discard packets that meet the packets max hop count i.e. no endless looping of packets around the network

Routers discard packets for many reasons, including bit errors, congestion, and instances in which no correct routes are known.



Populating Route Tables

(populated via one of the following sources)

Directly connected networks

Any network directly connected to the interface of a router is automatically added to the route table

Static network paths

Manually entered by the administrator by hand into the table i.e. static routes

Dynamic routing protocols

Routes a router learns from other routers via a routing protocol e.g. RIPv1, RIPv2, EIGRP, OSPF and BGP i.e. routes added automatically

Static Network Paths (Static Routes)

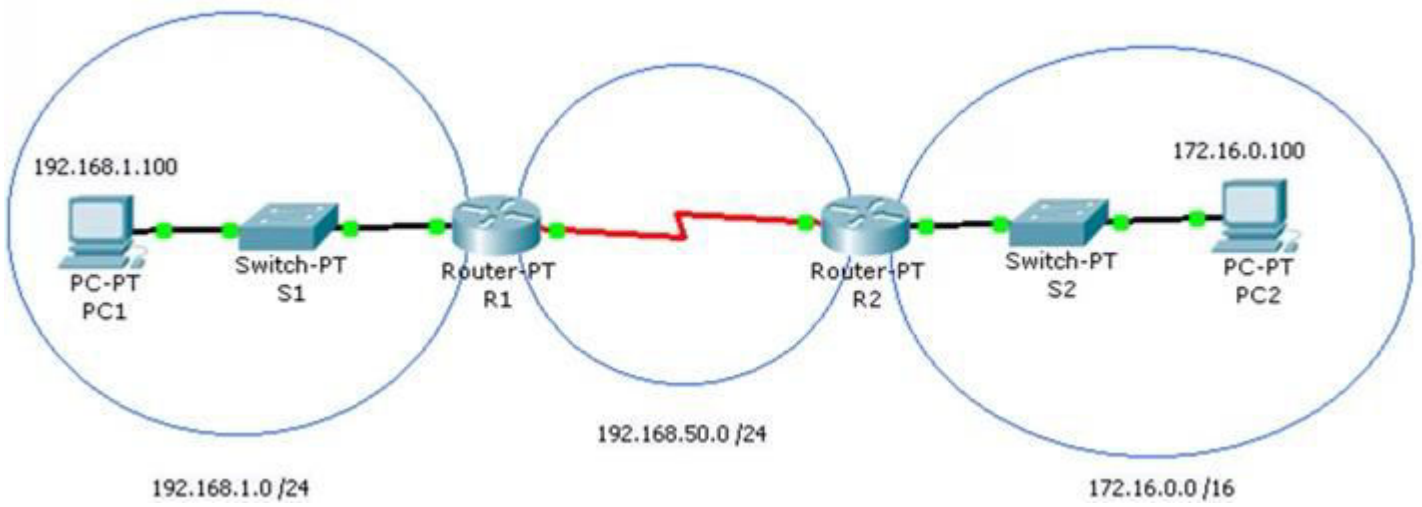
Manually populating a routing table with programmed routes to a destination network

All entries will remain the same unless they are changed manually

Entering static routes on large networks is time consuming

Used on small networks & with few network changes that effect routing

e.g. routers going up/down, networks been added/removed, network links changing



No static routes added
No routing protocols running

Just directly connected networks

Static Routes Highs

No routing protocol updates therefore no additional bandwidth usage between routers

No overhead on the router CPU

Enhanced security as the administrator can allow routing to only certain networks

Static Routes Lows

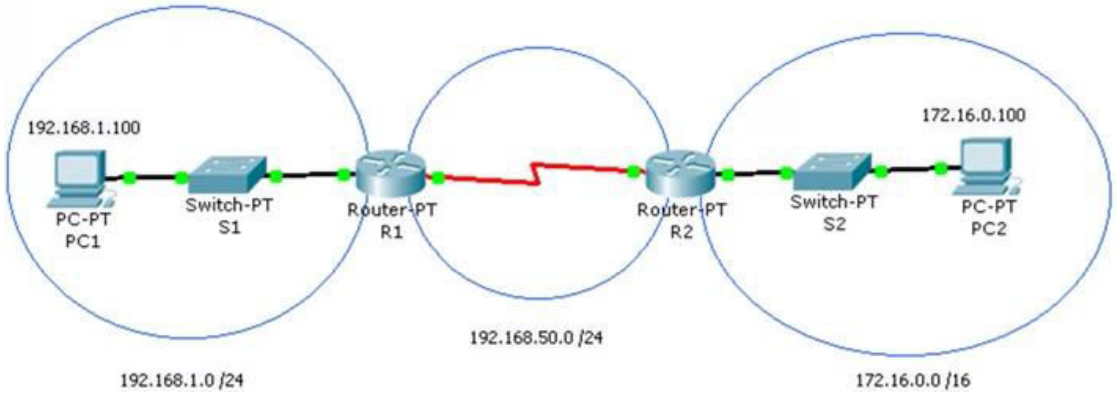
Can not adapt to network topology changes

Administrator must really understand how each router is connected in order to configure routes correctly

Not suitable in large networks as time consuming to maintain

```
Router>
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - m
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exte
       E1 - OSPF external type 1, E2 - OSPF external type
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.50.0/24 is directly connected, Serial2/0
Router#
```

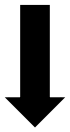
```
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mo
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exter
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, i
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.16.0.0/16 is directly connected, FastEthernet0/0
C    192.168.50.0/24 is directly connected, Serial2/0
```



Router 1 has no information in its routing table about how to forward packets to 172.16.0.0.

It would discard any packet bound for 172.168.0.0 from a host on the 192.168.1.0 network

Same for Router 2 in that it has no forwarding information about the subnet they are not directly connected to

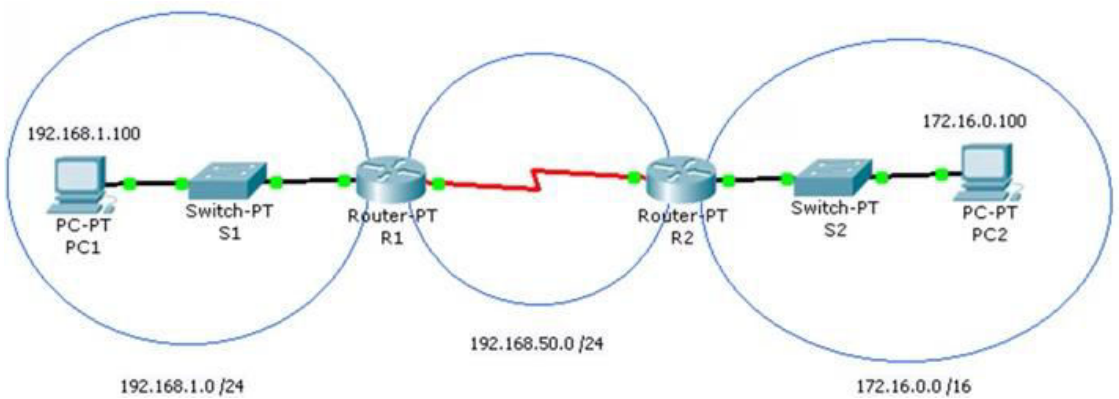


ADD IN STATIC ROUTES

Router1 (config)#ip route 172.16.0.0 255.255.0.0 192.168.50.0

(adds a static route to the 172.16.0.0)

```
Router>
Router>enable
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - m
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA exte
       E1 - OSPF external type 1, E2 - OSPF external type
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
       * - candidate default, U - per-user static route, o
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.50.0/24 is directly connected, Serial2/0
S    172.16.0.0 [1/0] via 192.168.50
```



Boston(config)**#ip route 172.16.30.0 255.255.255.0 172.16.20.2**

Configures a static route using the next-hop address

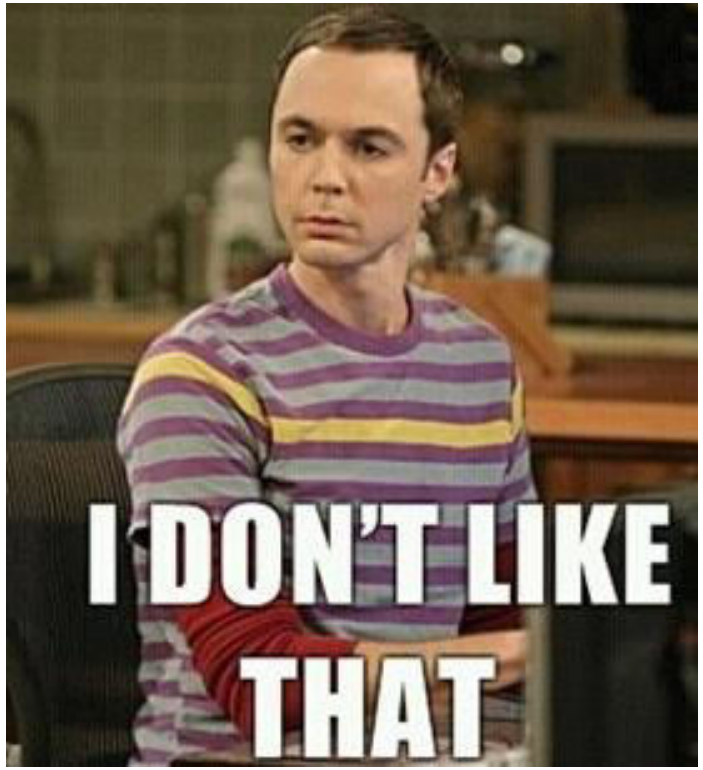
OR

Buffalo(config)**#ip route 172.16.10.0 255.255.255.0 s1**

Configures a static route using the exit interface

If the destination address of a packet fails to match any entry/path in the routing table

The packet can not be forwarded and will be dropped by the router



Static Default Route or Default Gateway

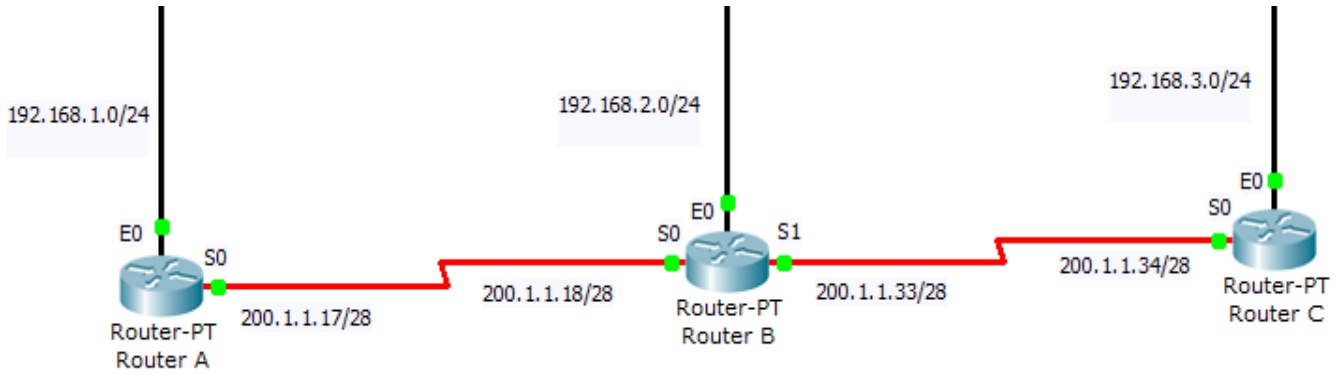
(Setup on each router)

Default route = “none of the above” or “route of last resort”

Place to forward packets when there is no match in the route table for the destination address, rather than drop packet

Cisco Routers default route “gateway of last resort”

Remember: Workstations rely on default routes to forward packets off the local networks



Routers A + C only have 1 interface connecting to other networks

Since there is only one possible interface to forward outbound packets to
Set a default route/gateway instead of adding each individual network to the route table.

⬇

Any packet bound for a network not directly connected will be sent to the ‘Gateway of last resort’

Programmed Router A with a static default route

(points to next hop router)

Configured by administrator by configuring a default route with both destination and mask being 0.0.0.0.

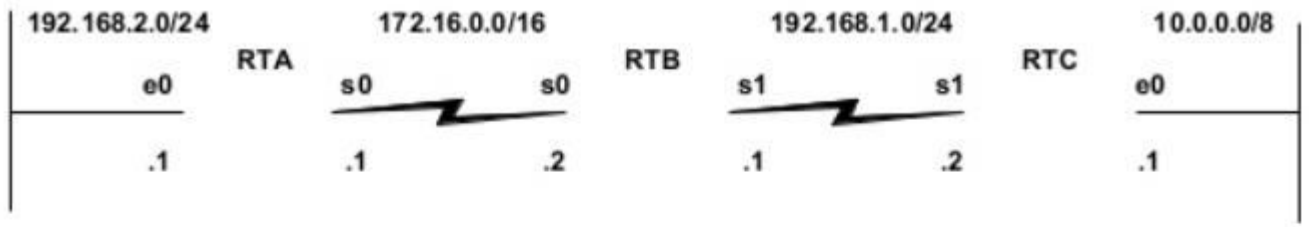
routerA (config)#ip route 0.0.0.0 0.0.0.0 200.1.1.118

Router A now has a 'Gateway of last resort' (static default route)

```
routerA#show ip route
Codes:  C – connected,  S – static,  I – IGRP,  R – RIP,  M – mobile,  B – BGP
        D – EIGRP,  EX – EIRGP external,  O – OSPF,  IA – OSPF inter area
        N1 – OSPF NSSA external type 1,  N2 – OSPF NSSA external type 2,  E – EGP
        i – IS-IS,  L1 – IS-IS level-1,  L2 – IS-IS level 2,  * - candidate default
        U – per-user static route, o – ODR
        T – traffic engineered route

Gateway of last resort is 200.1.1.18 to network 0.0.0.0

C       192.168.1.0 [0/0] is directly connected, Ethernet0
C       200.1.1.16  [0/0] is directly connected, Serial0
```

Routing Table prior to any interface configuration

(Currently, there area no routes in the routing table)




```
RTA#show ip route
Codes: C - connected, S - static, I - IGRP, 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, * - candidate default
       U - per-user static route, o - ODR

Gateway of last resort is not set

RTA#
```

Populating Route Tables

(populated via one of the following sources)

1. **Directly connected networks**: any network directly connected to the interface of a router is automatically added to the route table
2. **Static network paths**: manually entered by the administrator by hand into the table i.e. static routes
3. **Dynamic routing protocols:** routes a router learns from other routers via a routing protocol e.g. RIPv1, RIPv2, EIGRP, OSPF and BGP i.e. routes added automatically

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, 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

C    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.0.0/24 is directly connected, FastEthernet0/0
```

```
C       172.16.0.0 is directly connected, FastEthernet0/0
R       172.16.1.0 [120/1] via 192.168.1.30, 00:00:25, FastEthernet2/0
C       172.16.0.64 is directly connected, FastEthernet0/1
R       172.16.1.64 [120/1] via 192.168.1.30, 00:00:25, FastEthernet2/0
```

```
S    192.168.4.0/24 [1/0] via 192.168.3.254
S    192.168.1.0/24 [1/0] via 192.168.2.253
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
```

Packet arrives at a router.

MAC address is examined.

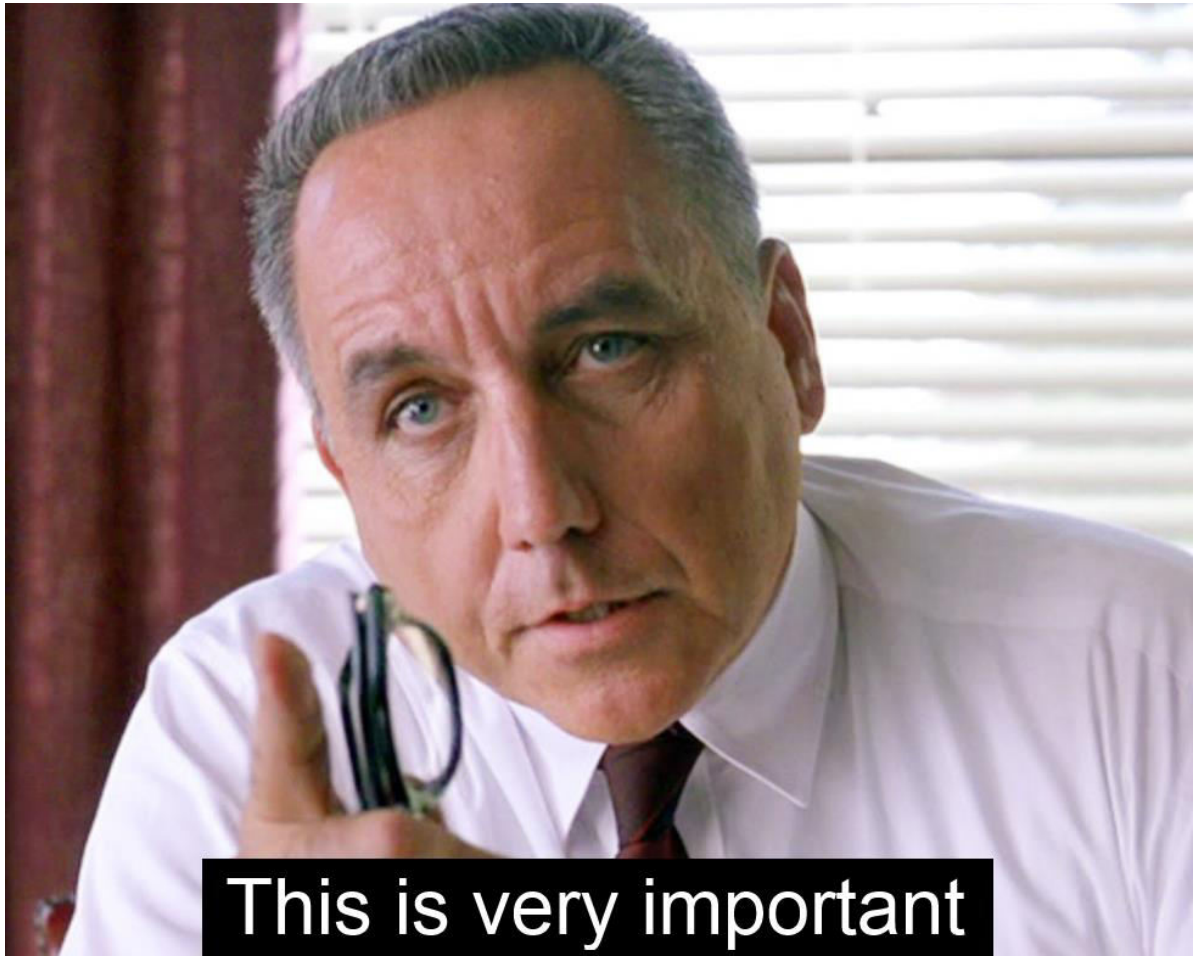
If the packet contains router's MAC address, router strips off the frame & passes the packet to network layer.

At the network layer, the destination IP address is examined.

If the destination is the IP of the router or broadcast address, protocol field is examined and data sent to appropriate process.

Any other destination address calls for **ROUTING**.

The address could be for another host on another network to the router is connected
or
for a host on a network not directly connected to the router.



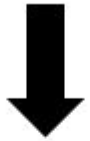
If the destination address of a packet can not be matched to any route in the route table

Packet is dropped

Destination unreachable ICMP is sent to the source address.

Virtually impossible for an administrator to keep the network up via manipulation of static routes in route tables.

A single downed router or network link may require dozen of routers to be reconfigured with alternate routes



Dynamic Routing

Routers learn about the condition of the network automatically & modify their route table on-the-fly without human intervention

Deployed on any size network

Routing protocol is what enables the concept of dynamic routing.

Routing Protocol

Specialized form of a protocol that allows 2 or more routers to exchange information about the networks they know about.

Enable routers to dynamically discover, maintain and update routes while not dependent on administrator to make changes

Routing Protocols

Goal: build and maintain the routing table
(contains learned networks and associated ports for these networks)

Language a router speaks with other routers to share information about their reachability (path determination) & status of networks

Defines the set of rules used by a router when it communicates with neighboring routers

1) How to send updates

2) What knowledge is contained in the packets

3) When to send the knowledge

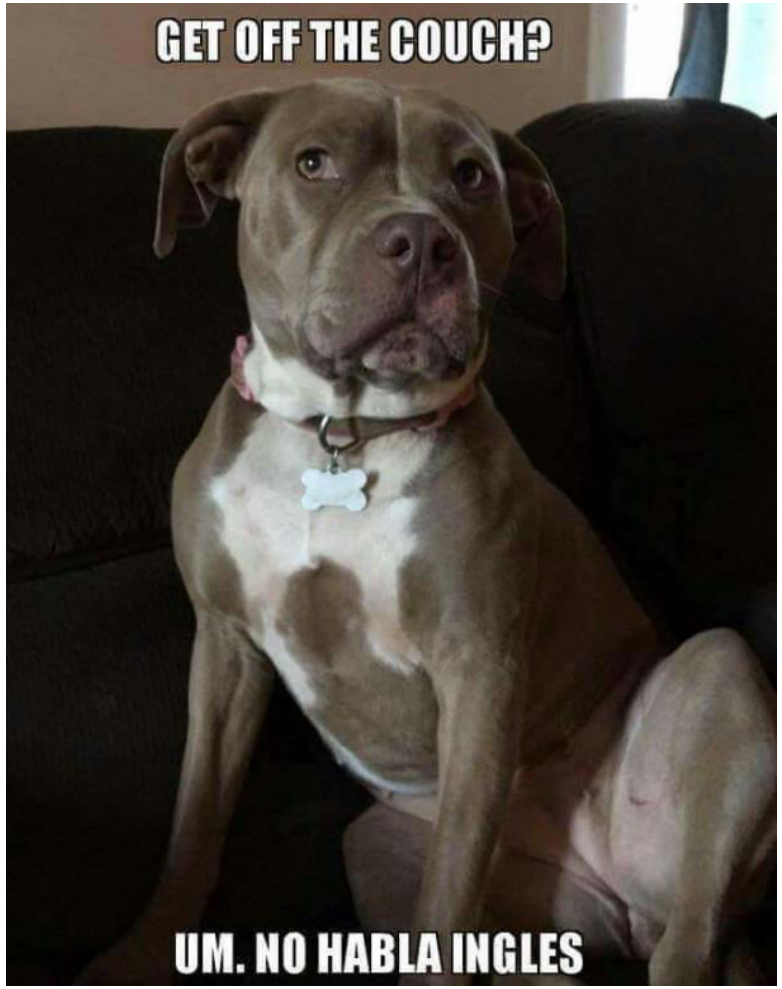
4) How to locate recipients of the updates

Routing Protocols also determine the next best path if the best path to a destination becomes unusable.

Adjust to topology changes → most important advantage of dynamic routing over static routing

Routers must use the same protocol to communicate.

One speaks RIP and another speaks OSPF, then they can not share information as not speaking same language



Routing protocols are sometimes unnecessary

Routing protocols create unnecessary traffic and inefficient use of router processor resources

Routing Protocols Goals

To dynamically learn and fill the routing table with a route to each subnet in the internetwork.

If more than one route to a subnet is available, to place the best route in the routing table.

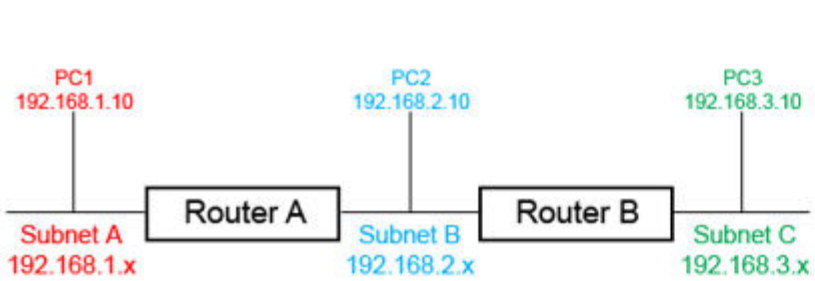
To notice when routes in the table are no longer valid, and to remove them from the routing table.

If a route is removed from the routing table and another route through another neighboring router is available, to add the route to the routing table.

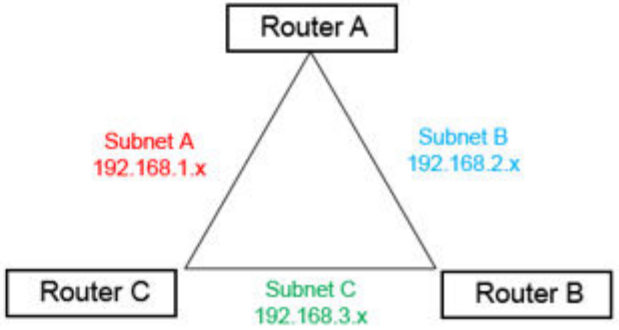
To work quickly when adding new routes or replacing lost routes. (The time between losing the route and finding a working replacement route I = convergence time.)

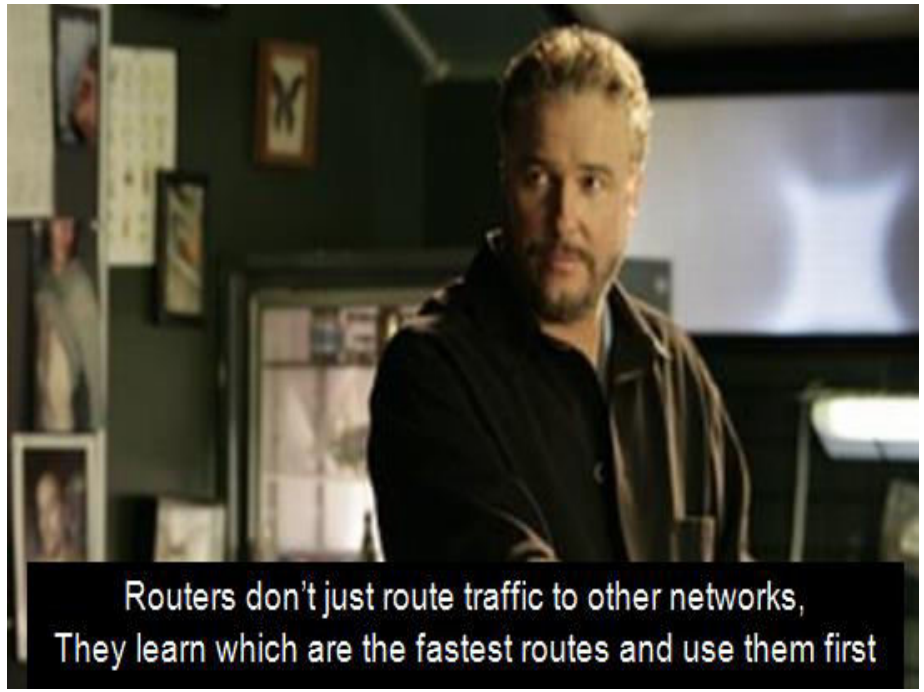
To prevent routing loops.


OK CLASS, HERE IS A QUESTION FOR YOU
WHICH OF THESE SETUPS IS BETTER?


PC1
192.168.1.10
PC2
192.168.2.10
PC3
192.168.3.10
Router A
Router B
Subnet A
192.168.1.x
Subnet B
192.168.2.x
Subnet C
192.168.3.x

OR

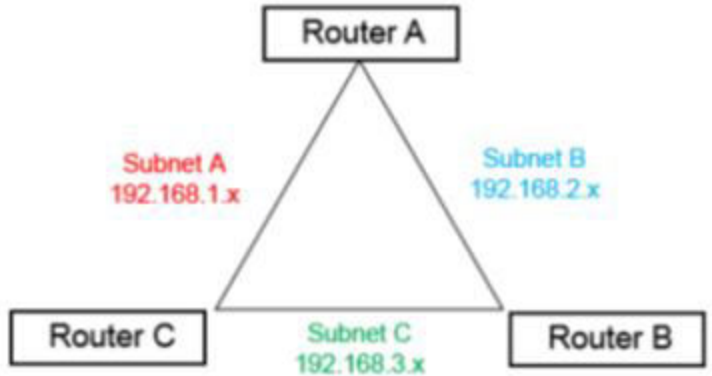

Router A
Subnet A
192.168.1.x
Subnet B
192.168.2.x
Router C
Subnet C
192.168.3.x
Router B



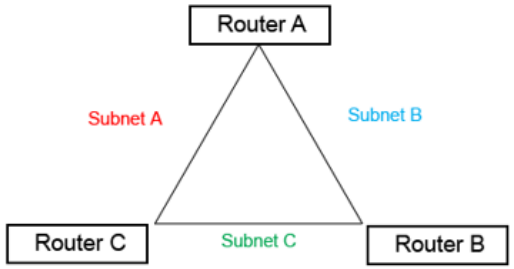
Subnet A has two routes to subnet C

One directly through Router C (1 hop)

One through Router A then B (2 hops)



How does the router know to take the quickest and most efficient route i.e. directly through Router C first



If a routing protocol learns about more than one path to the same network

It must have a means of evaluating which route is best to use

Metric

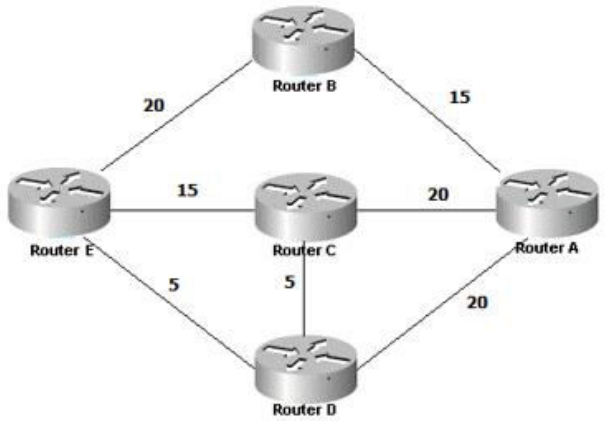
Used by a router to decide whether one particular route should be chosen over another

Each route learned by a routing protocol is assigned a metric value

Each router chooses the best route that has the lowest metric (most efficient)

If the route with the lowest metric goes down, next best route is used

What is the best route from B → C?



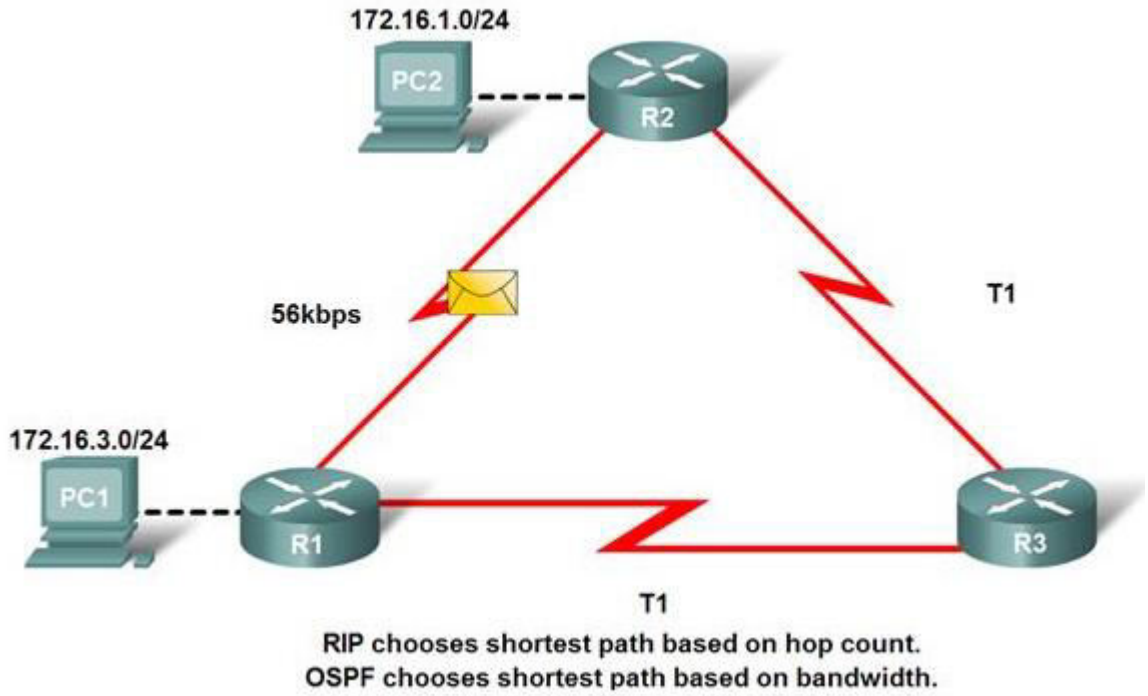
Metric has no meaning if the protocol has discovered only one route to a particular network

Different protocols use different metrics

e.g. hop count, bandwidth, load, delay, path reliability

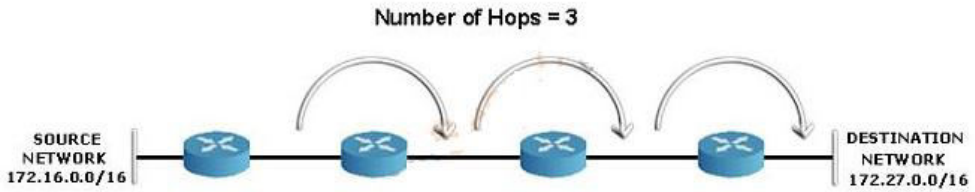
RIP defines the ‘best route’ as the one with the least number of hops

EIGRP defines the ‘best route’ based on a combination of lowest bandwidth along the route + total delay of the route



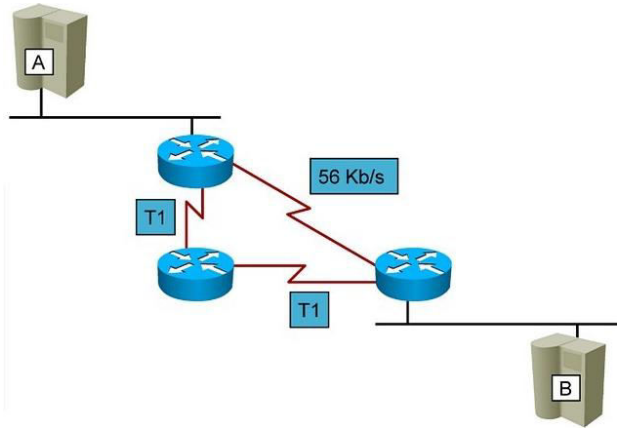
Hop Count

Number of routers (hops) from the source router to reach the destination network
Each router on the network represents one hop
e.g. network with 4 routers has 3 hops between first and last route
Does not take into account bandwidth i.e. T-1 links faster than DS-0 link



Bandwidth

Speed of links between routers.
Data capacity of a link e.g. 100 Mbps Ethernet link
Choose higher over lower bandwidth link.
What if the T1 links are heavily loaded with traffic while the 56K link is lightly loaded?
What if the higher bandwidth link has a higher delay?



Path Reliability

Measures the likelihood that the link will fail in some way
Variable – number of times a link has failed or number of errors (error rate) it has received within a certain timeframe
Fixed – based on known qualities of a link as determined by network administrator

Load

Amount of traffic utilizing the links along the path i.e. lowest load = best path
Unlike hop count and bandwidth, load on route changes so metric will change which leads to route flapping.
Route flapping – frequent changes of routes can lead t o adverse effects on routers CPU, bandwidth on data links

Delay

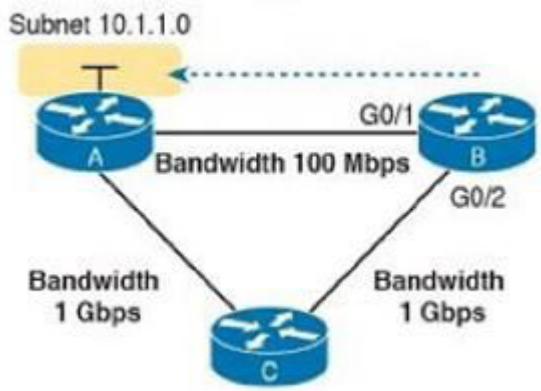
Length of time (milliseconds) to move packet along each link i.e. least delay = best path
Also takes into account router latency and queueing delays.

Cost

Configured by network administrator to reflect more or less preferred routes
Defined by any policy or link characteristic or reflect judgement of administrator

RIP's hop count - that shortest route may have the slowest links

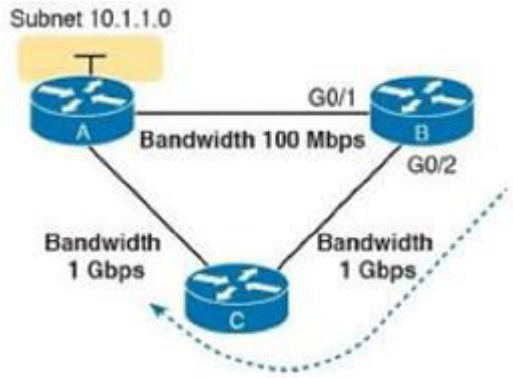
Image shows RIP choosing the one-hop route from Router B to subnet 10.1.1.0, even though it crosses the slower 100-Mbps link instead of the two-hop route over two 1-Gbps links.



Routing protocol whose metric was based (at least in part) on link bandwidth might be a better choice in the following image.

EIGRP does base its metric in part on link bandwidth.

EIGRP chooses the route that happens to have more links through the network (and more hops), but both links have a faster bandwidth of 1 Gbps on each link.



Some enterprises use multiple IP routing protocols.

More than one routing protocol can run on a single router

So 1 router might learn of multiple routes to a particular subnet using different routing protocols.
Each protocol may learn of the same network and each will apply its native metrics to determine which path is most efficient

Each protocol presents a candidate path to the same network for inclusion in the route table.

Which route should be installed?

RIP uses the hop count as the metric

EIGRP uses a math formula with bandwidth and delay as inputs.

A route with RIP metric 1 might need to be compared to an EIGRP route, to the same subnet, but with metric 4,132,768

As the numbers have different meanings, there is no real way to compare the metrics.

An arbitrator is needed to choose which one → **Administrative Distance**

"Measure of trustworthiness of the source of the route"

Code	Network, Mask	AD/Metric	Next Hop	Interface
O	10.0.0.0/8	110/120	200.1.1.1	S0
O	172.16.0.0/16	110/15	200.1.1.1	S0
O	192.168.1.0/24	110/20	200.2.2.2	S1
C	210.1.1.4/30	0/0	Directly connected	E0

AD: used by a router to select the best path when there are two or more different routes to the same destination from two different routing protocols

Administrative distance is a value assigned to every method for identifying network routes

i.e. directly connected, statically entered route or a route discovered by routing protocol

Lowest AD is always installed into the route table

Static routes have precedence over dynamically learned routes

Static route will always be choose over a route learned from any routing protocol.

Directly connected routes have a higher precedence over static

Directly connected = 0 (highest selection priority)
Static route = 1
EIGRP = 5
BGP = 20
EIGRP (internal) = 90
IGRP = 100
OSPF = 110
RIP = 120

What should a router do when it learns multiple routes for the same subnet but the metrics tie?

With RIP's hop-count metric, ties can easily happen.

So RIP needs options for how to deal with a tie.

RIP's default behavior when it learns more than one route that ties is to put multiple routes into the routing table and use them all.

Once in the routing table, the router's forwarding logic balances the packets across those equal-metric routes.

Cisco refers to this feature of using multiple equal-metric routes to the same destination as **equal-cost load balancing**.

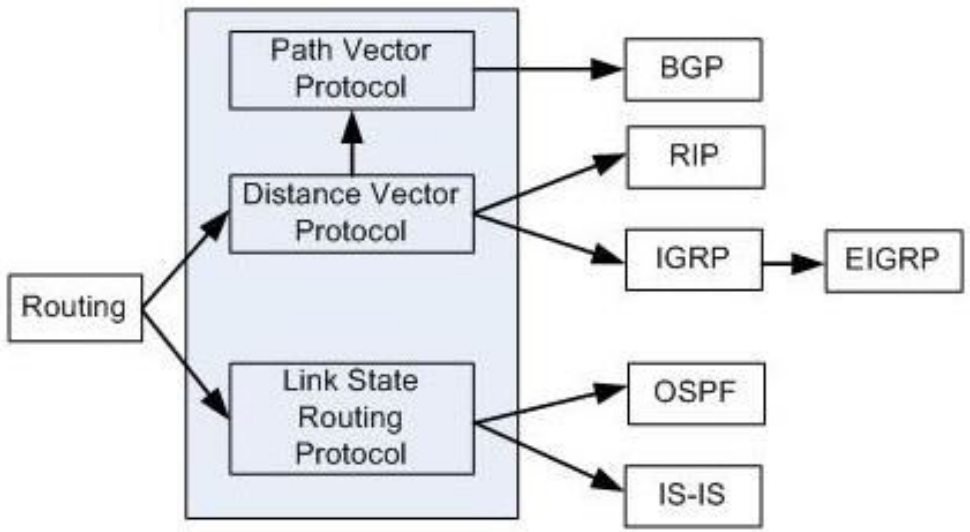
RIP controls this behavior with the **maximum-paths** *number-of-paths* RIP subcommand i.e. default of 4 routes in a table

A value of 1 means disabling this feature and places the first learned equal-metric route into the routing table

Many different types of dynamic routing protocols

Differ mainly in the way they discover and make calculations about routes

Each uses a different method for determining the best route (metric) to a destination network



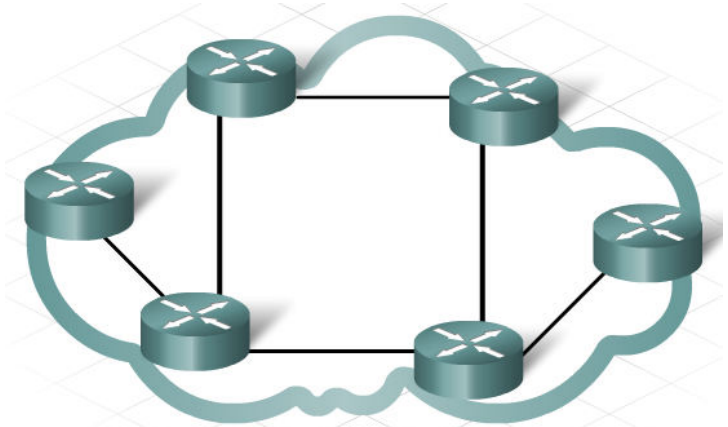
Autonomous Systems

Internet is divided up into collections of networks → AS (in the early 80's)

Network under a single administrative control e.g. Your org's network

Each AS is identified by a unique AS number (ASN)

e.g. of an AS is the ISP, large company, college



Autonomous System = Networks under a single administration

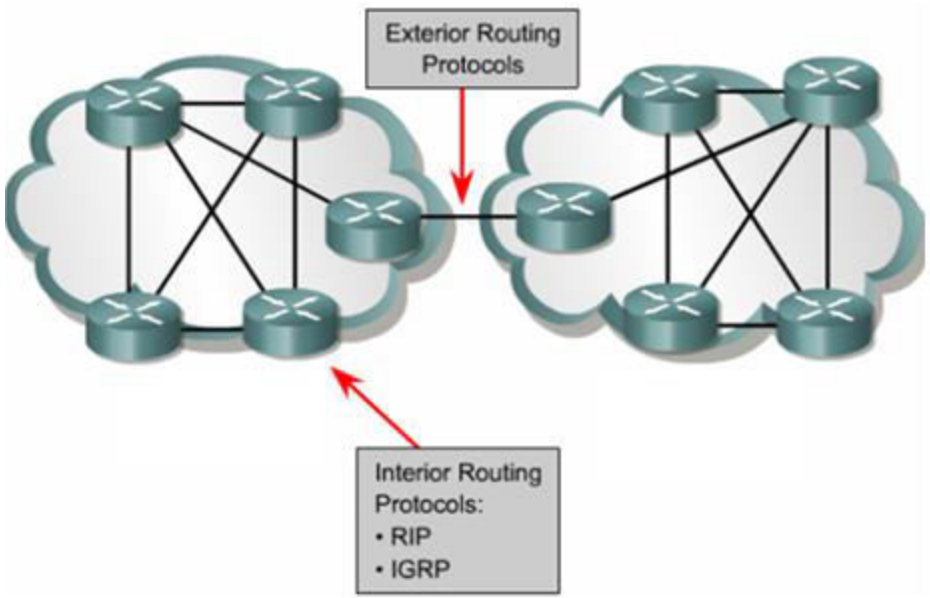
Interior Routing Protocols (IGP – Interior Gateway Protocol) - developed to facilitate routing within an autonomous system
Exterior Routing Protocols (ERP - Exterior Gateway Protocols) – developed to facilitate routing between autonomous systems

To connect your org's network to another org's network and share routing information then you need an exterior routing protocol

Interior Gateway Protocols (IGP)

Protocols used to exchange routing information between routers within a LAN or interconnected LAN's

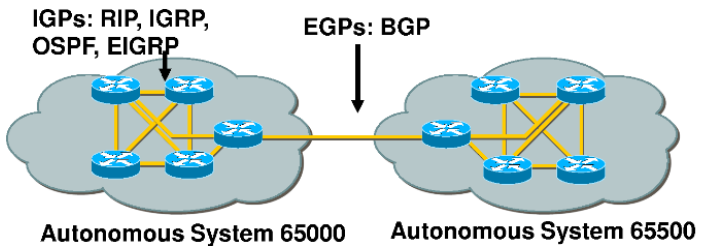
IGP's fall into two categories i.e. Distance Vector (RIP, IGRP) and Link State (OSPF and IS-IS)



Exterior Gateway Protocols (EGP)

Route information outside the network e.g. BGP (Border Gateway Protocol)

BGP is the only actively used EGP on the Internet



Border Gateway Protocol (BGP): …associated with Internet

Exchanges routing information between Autonomous Systems (allow AS to communicate)

Distance Vector

1st to appear in TCP/IP routing world

'Routing by rumor' or 'second-hand information' (information did not come directly from source)

Each router learns routes from its neighboring routers perspective and then advertises these routes from its own perspective.

Each router sends periodic updates of full routing table only to its directly connected neighbors at predetermined intervals & depends on them to pass the update info along to their neighbors

(interval depends on protocol e.g. 30-90 seconds i.e. each router will broadcast its entire routing table every 30 seconds)

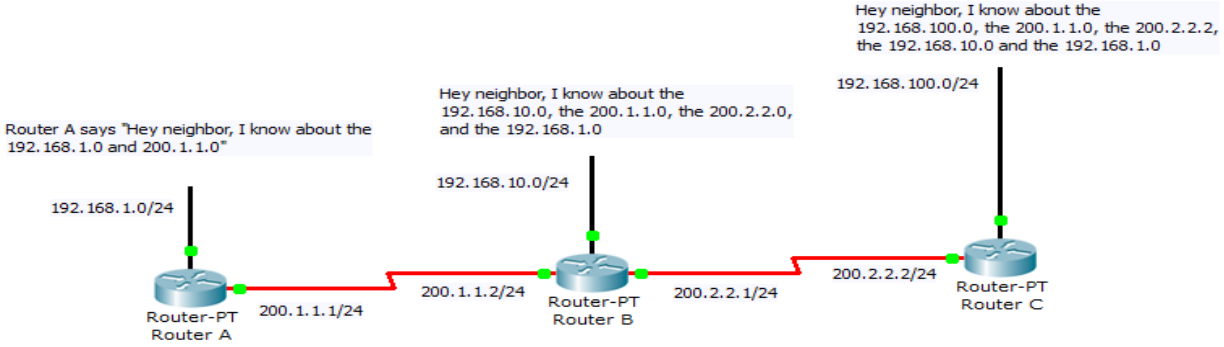
Each router will merges the received routing tables with its own table, and then transmit the merged table to its neighbors

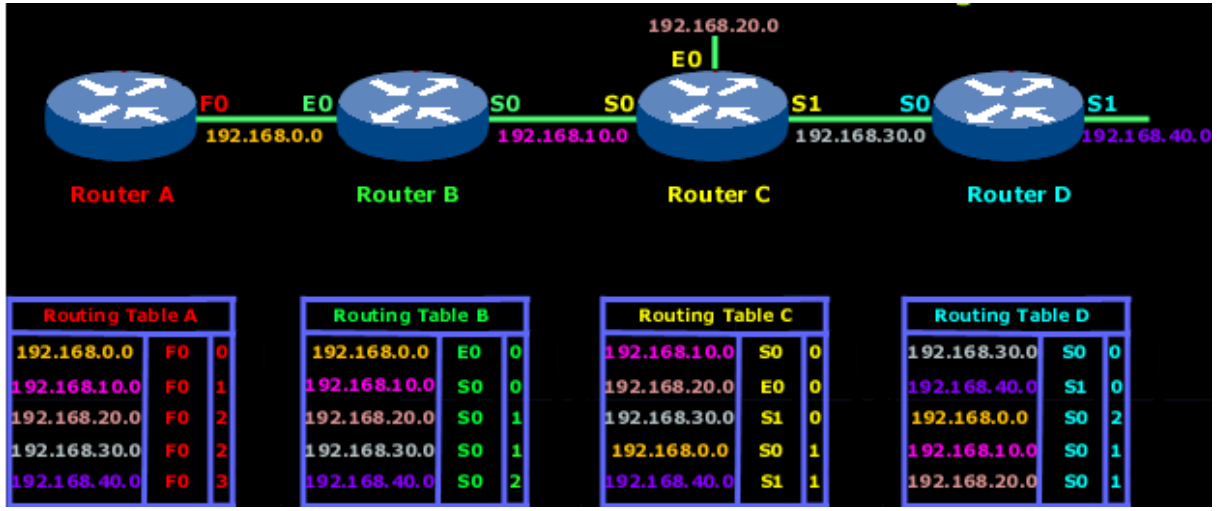
Generates loads of network traffic

Communication between distance vector routers = HOP (metric that distance vector protocols use to keep track on how far away a particular network is)

If 2 networks are connected directly to the router's interface, they will have a value of zero (0) in the router's table entry.

Each router represents one hop e.g. network with 6 routers has 5 hops (total cost = 5)

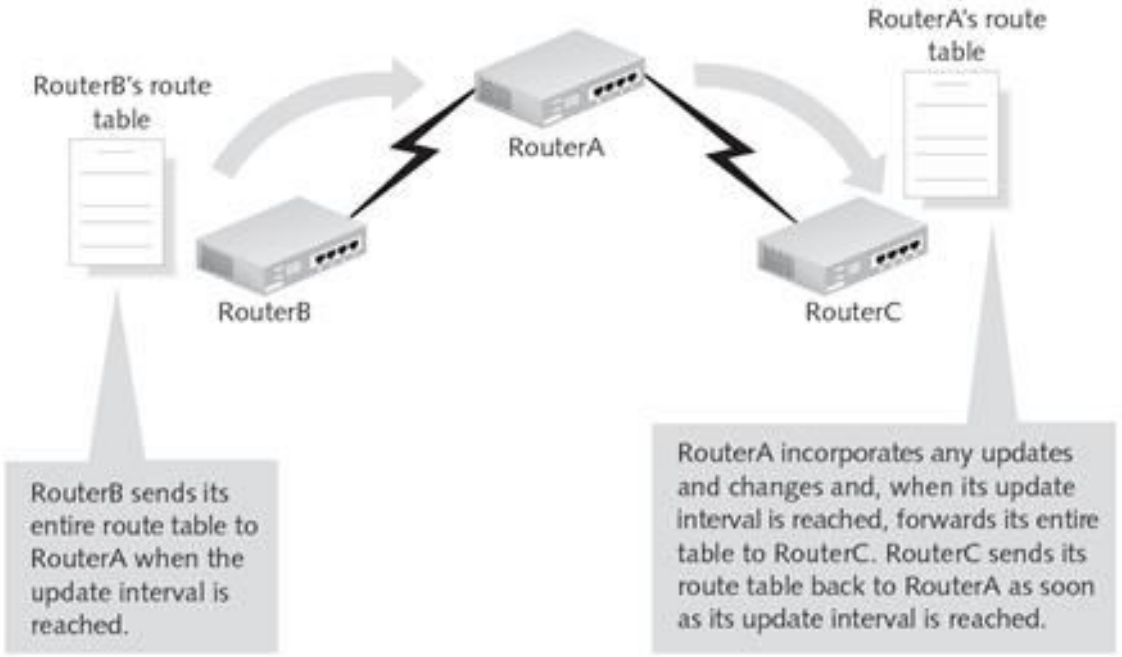




Use the Bellman–Ford algorithm, Ford–Fulkerson algorithm, or DUAL FSM to calculate paths

As the updates propagates throughout the network, router C will only receive info about router B's routing table via router A "routing by rumor"

'Routing by rumor' is an issue with distance vector as in this case, RC will not learn about topology changes on RB for up to a minute



When a router becomes active on the network, it finds other routers and announces its presence by sending **broadcast updates** to the broadcast address (255.255.255.255)

Neighbor routers speaking the same protocol will hear the broadcasts and take action.
Other hosts/devices will just drop the packets (routing updates)

All distance vector protocols are ‘chatty’

Conversations between routers consume network resources

After running the DV protocol and populating the routing table, entire table is broadcast to its neighbors every 30 seconds.

Route tables can get quite large and transmitting that entire table can impact on network bandwidth

Also, periodic updates make the update process slow & create large amounts of network traffic

READ MY LIPS

Updates sent automatically every 30-60 seconds (depends on protocol)
Updates are used to compile their routing tables
Convergence point at which the updating of routing tables is complete for all routers.

Convergence

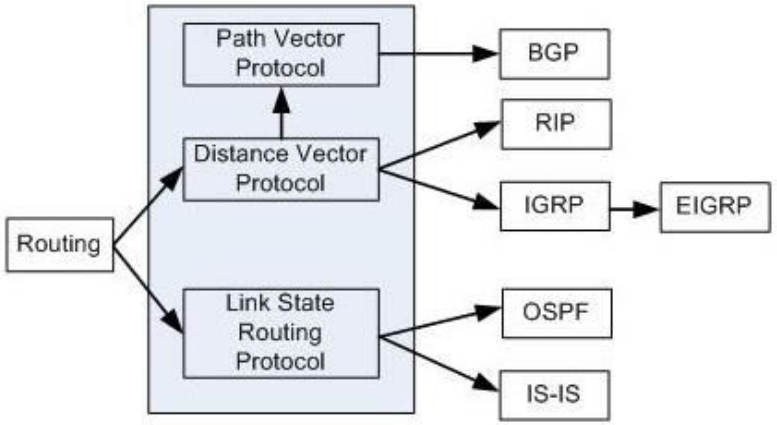
Process of bringing the reachability information in route tables of all routers to a state of consistency.

Convergence Time

Time it takes to share information across a network and for all routers to calculate best paths.

Routing errors (loops) occur during the time when routers are updating but not have updated as yet & contain old info i.e. link failure

The faster a network can reconverge after a topology change the better!



Routing Information Protocol (RIP) or RIPv1

Oldest distance vector routing protocol
(1960's but first full version dates from the 80's)

Uses hop count as the metric for path selection

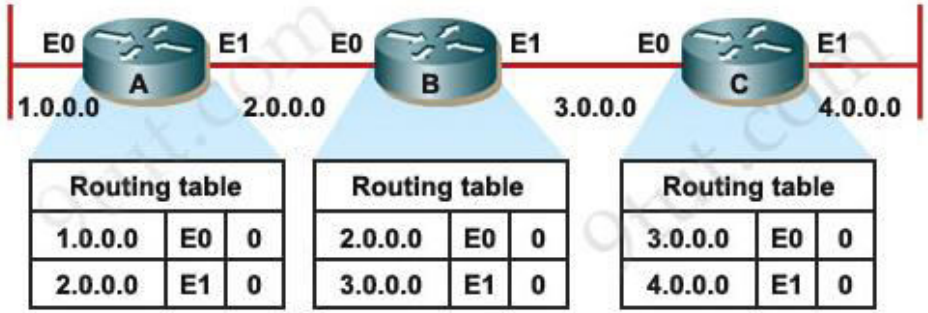
Limited to 15 hops
(hop count greater than 15 as an unreachable route)

Router updates to be transmitted every 30 seconds

Does not support router authentication
(vulnerable to attacks by hackers sending false routing table information)

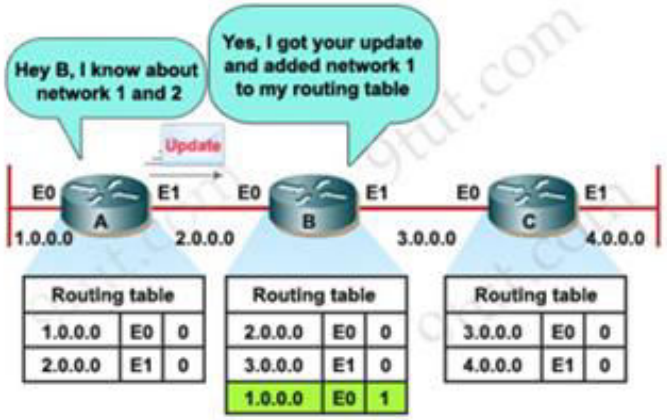
No routing protocol is turned on

Router A, network 1.0.0.0 has already been known because it is directly connected through interface E0
&
Metric (of a directly connected network) is 0



Now turn on RIP on these routers

A sends a copy of its routing table to B, B already knew about network 2 but now B learns about network 1 as well



Router B has now learned about network 1 from A via E0 interface so the metric now will be 1 hop

After updating its routing table, the router immediately begins transmitting routing updates i.e. **triggered updates**

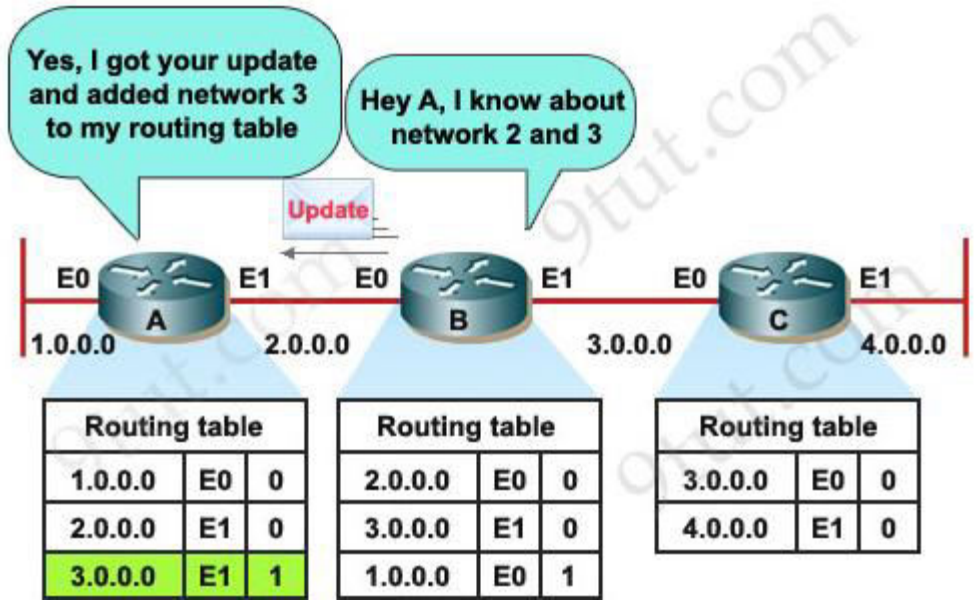
These updates are sent independently of the regularly scheduled updates

Each router receives a routing table from its direct neighbor.

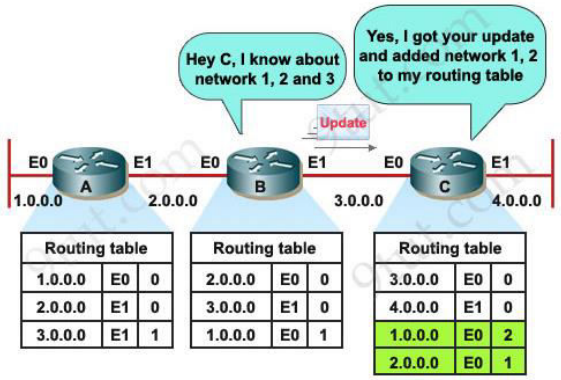
Router B receives information from Router A about network 1 and 2.

It then adds a distance vector metric (such as the number of hops), increasing the distance vector of these routes by 1.

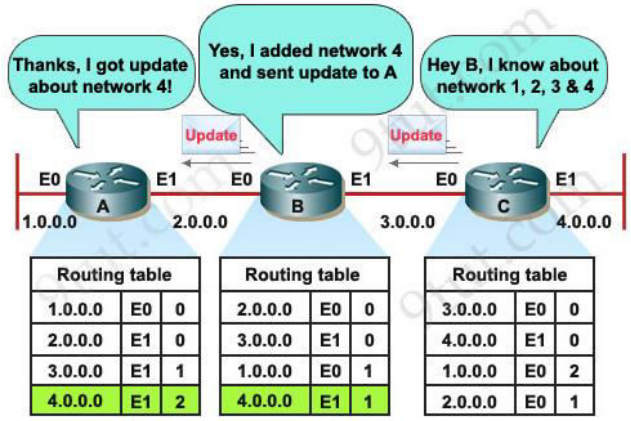
B also exchanges its routing table with A about network 2 and 3.



B then passes the routing table to its other neighbor, Router C.



Router C also sends its update to B and B sends it to A.



Network is now converged.

RIPv2

Adopted in 1994

Includes authentication

Still supports limit of 15 hops

Usually used unless the equipment cannot support RIPv2

RIP v1 is a classful routing protocol but RIP v2 is a classless routing protocol

Classful routing protocols do not include the subnet mask with the network address in routing updates

Link-State

Build topology maps of entire system by talking to all routers in the area & holds that map in memory
(allow s each router to know how many routers out there and w hat networks are connected to each other)

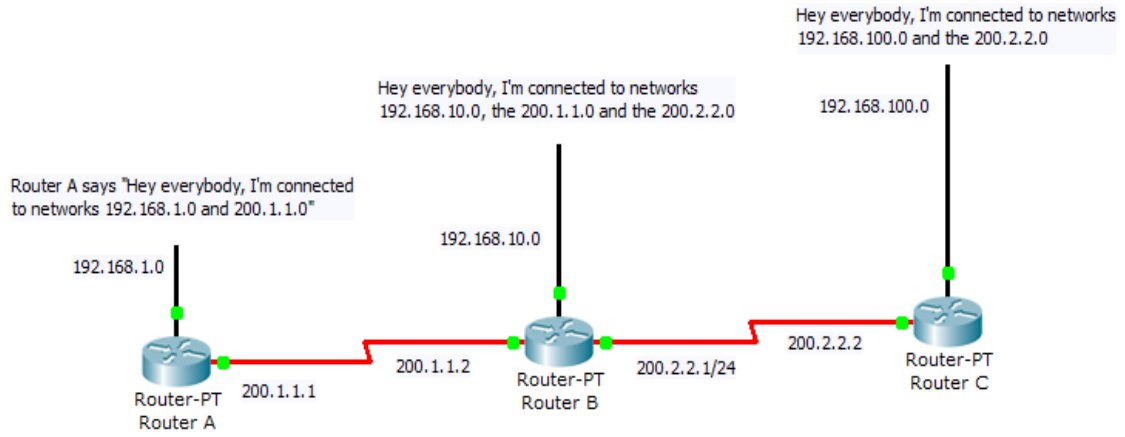
Don't advertise the entire routing table i.e. advertise information about a network topology (directly connected links, neighboring routers (sends only link state information)

In theory, all nodes have same info and will independently calculate its own best path

Routers receive first-hand routing information from each router (LSA's) in the network NOT via hearsay
(each router speaks only for itself describing its direct links through advertisements i.e. Link-State Advertisements (LSA's)

LSA's are only sent when the status of a link changes i.e. topology change (less updates so generates less network traffic)

Classless routing protocol




and that's a wrap