Routing and Bandwidth Management

DOMAIN 2.0

MODULE 8

Routing and Bandwidth Management Topics

Routing Basics

Packet Delivery on the Same Network

IP Routing Across a Single Router

IP Routing Across Multiple Hops

Route Selection

RIP

OSPF

EIGRP

BGP

NAT/PAT

Bandwidth Management

Routing Basics

What is Routing?

The movement of packets from one network to the next

- Performed by routers
- Routers read the Layer 3 header destination address to determine what to do with a packet
- Layer 2 switches do not route

Routers "relay" a packet in a daisy chain until it reaches its final destination

Each router along the path passes the packet to the next router (hop)

The last router passes the packet to the final destination

Because routers exist along a packet's path they are sometimes called "intermediate systems"

Routers themselves can sometimes be the final destination

- Especially if you are remotely testing or managing the router

Static Routing

Administrator manually enters routes into the router

Only useful if you have very few routes with no redundancy

- If you enter multiple static routes with the same metric you will create a routing loop

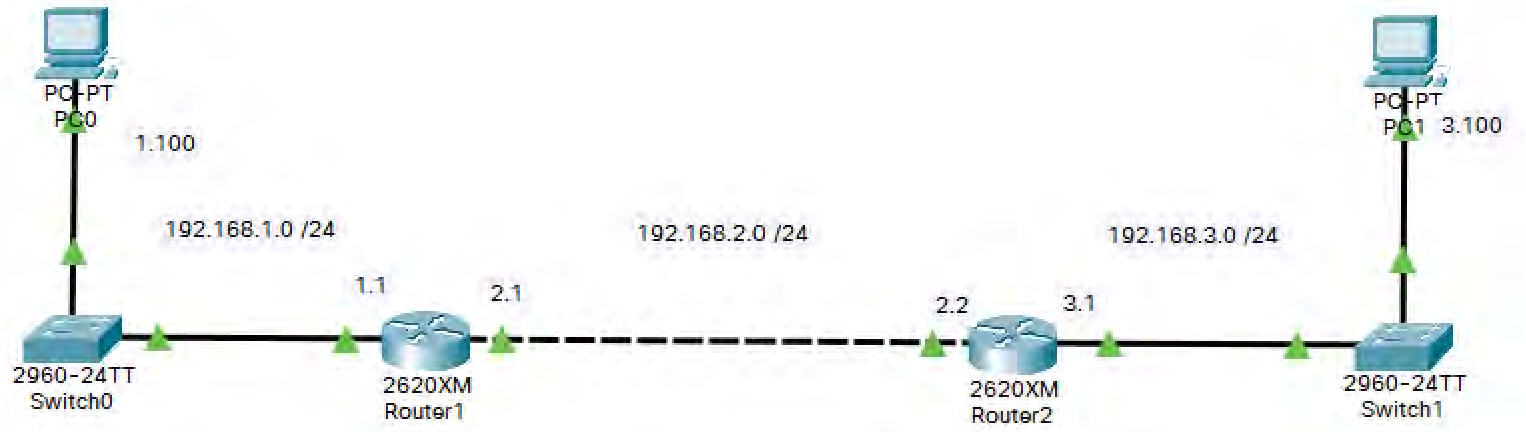
Benefits

- Fewer resources required by the router
- No routing updates consuming extra bandwidth
- More secure because route tables will not be poisoned by a rogue router advertising false routes

Disadvantages

- You need to know the complete network topology very well in order to configure routes correctly
- Topology changes require manual updates on all routers
- Can be time consuming and error prone

Static Routing Example




```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Ethernet1/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

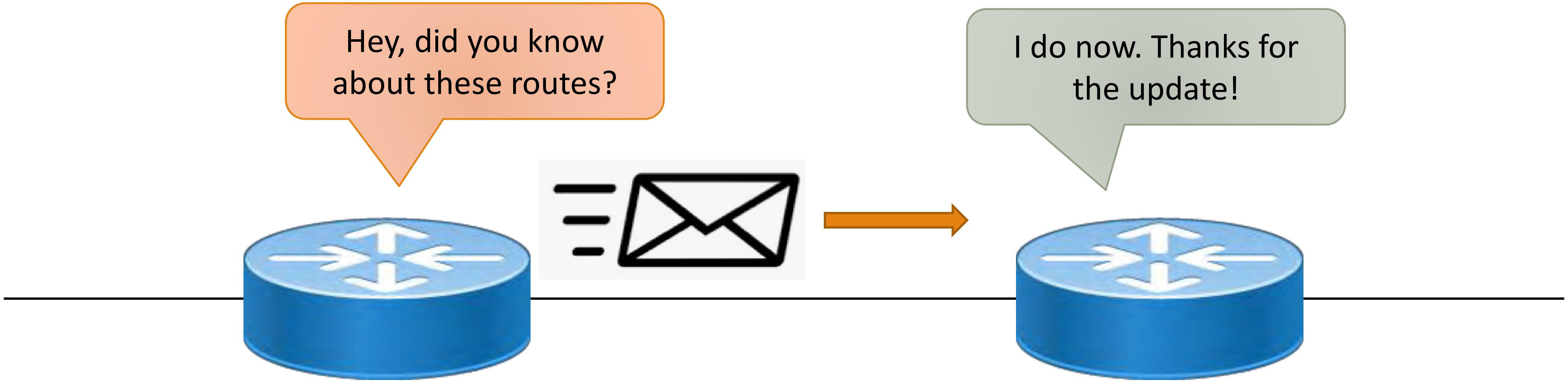
```
S    192.168.1.0/24 [1/0] via 192.168.2.1
C    192.168.2.0/24 is directly connected, Ethernet1/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Dynamic Routing

Routers use routing protocols to tell each other about distant routes

Routers initially only know the routes (segments) they are directly attached to

When new networks are added or removed, the routers update each other

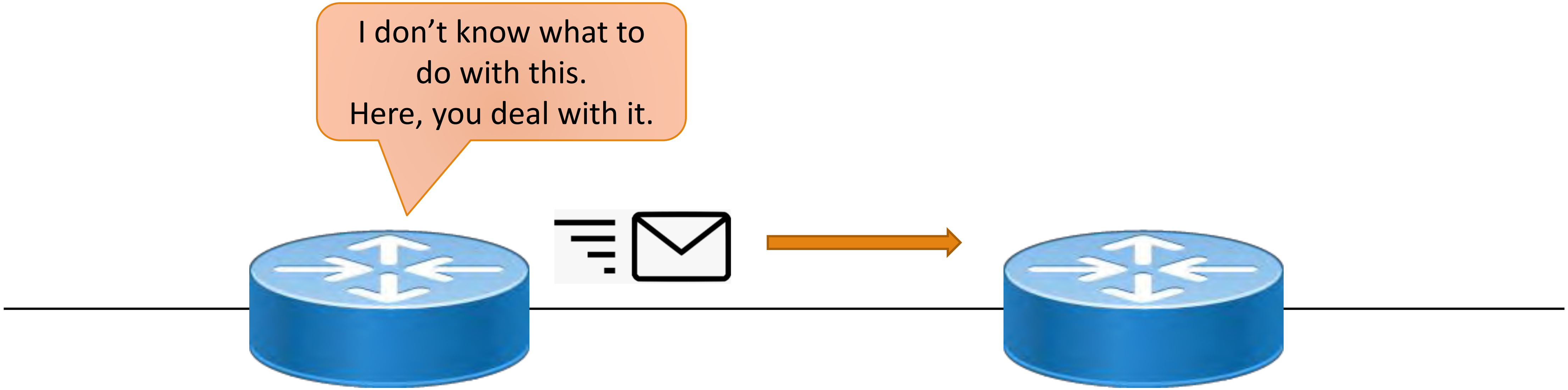


Default Routing

There is only one possible exit for the traffic to take

A host can specify its local router (default gateway)

A router can specify an upstream router



The Golden Rule(s) of Routing

Each router interface must belong to a different network

A router must know what to do with a packet
- It must be able to choose a legitimate route for a destination

It must have either:
- An entry for the destination in its route table
- A default route to pass the packet to

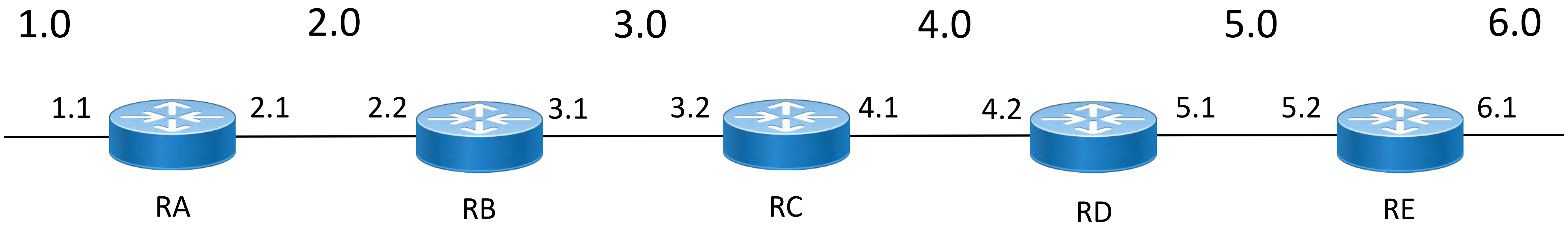
If neither exists, the router will drop the packet and send an ICMP unreachable message to the sender

If some routers lack a few routes (are not “fully converged”) you will have routing black holes
- Packets may disappear and be lost

When a router receives a packet, it must know how to return that packet to the source

The Golden Rule of Routing Example

Every router in this topology knows how to reach all routes
C = directly connected



RA
C - 1.0
C – 2.0
Default → 2.2

RB
Dest 1.0 → 2.1
C – 2.0
C – 3.0
Dest 4.0 → 3.2
Dest 5.0 → 3.2
Dest 6.0 → 3.2

RC
Dest 1.0 → 3.1
Dest 2.0 → 3.1
C – 3.0
C – 4.0
Dest 5.0 → 4.2
Dest 6.0 → 4.2

RD
Dest 1.0 → 4.1
Dest 2.0 → 4.1
Dest 3.0 → 4.1
C – 4.0
C – 5.0
Dest 6.0 → 5.2

RE
C – 5.0
C – 6.0
Default → 5.1

Note: Network IDs in this topology have been simplified for visual convenience

Packet Delivery on the Same Network

Packet Delivery on the Same Network Example

This example uses MAC addresses at Layer 2

Source (Host A) and Destination (Host B) are on the Same Network

A packet cannot be transmitted until the sender knows both the Layer 3 and Layer 2 destination addresses

1. A wants to send a packet to B
2. A checks to see if it already knows the IP address for B
3. A determines that it does not know B's IP address
4. A performs a DNS lookup to find B's IP Address *
5. A puts the address of B in the IP header destination field
6. A uses its own subnet mask to determine if B is on the same or different network
7. A determines that B is on the same network

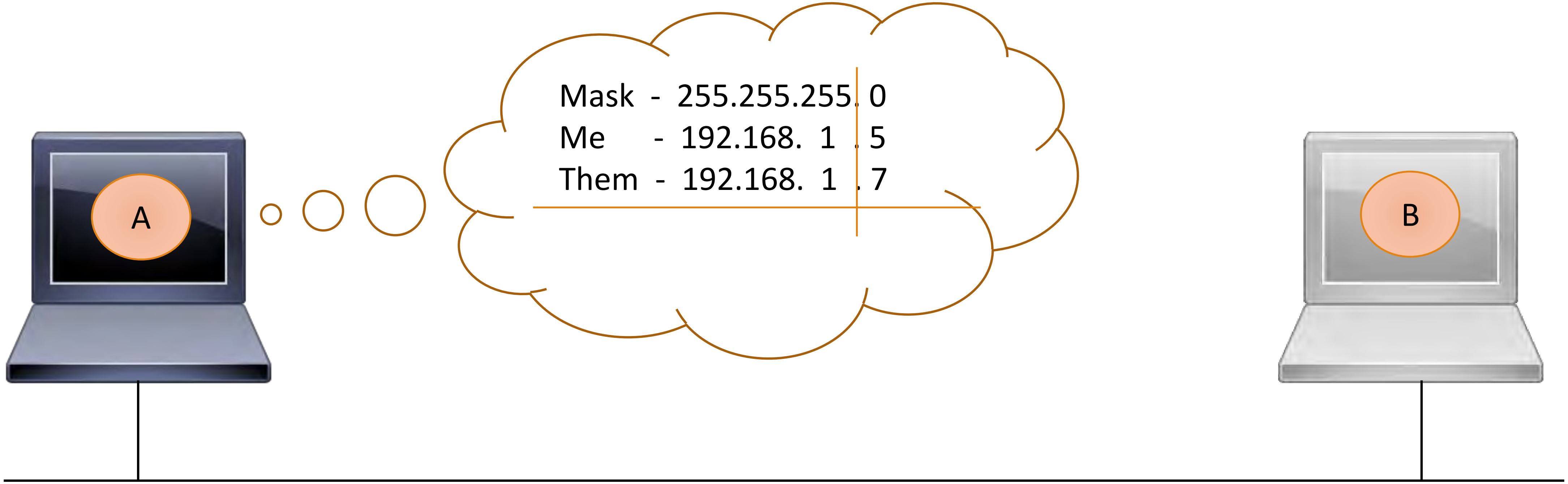
* Depending on the OS, a sender might also broadcast or use a Microsoft WINS server to determine the destination IP

Packet Delivery on the Same Network Example (cont'd)

8. A checks its ARP cache to see if it already knows B's MAC address
9. If A does not have B's MAC address in its ARP cache, A will use ARP to learn B's MAC address
10. A puts B's MAC address in the Ethernet header destination field
11. A transmits the frame onto the media and hopes that B will pick it up
12. The frame passes by B's NIC
13. B notices that the destination MAC address is its own address, and picks up the frame
14. B processes the frame and its payload
15. If B needs to respond, it will use the same steps to transmit back to A

The switch will consult its MAC table to determine which port B can be found on. If it has no record of B, it will flood the frame out all ports (including uplinks and trunk links).

Using the Subnet Mask to Evaluate the Destination

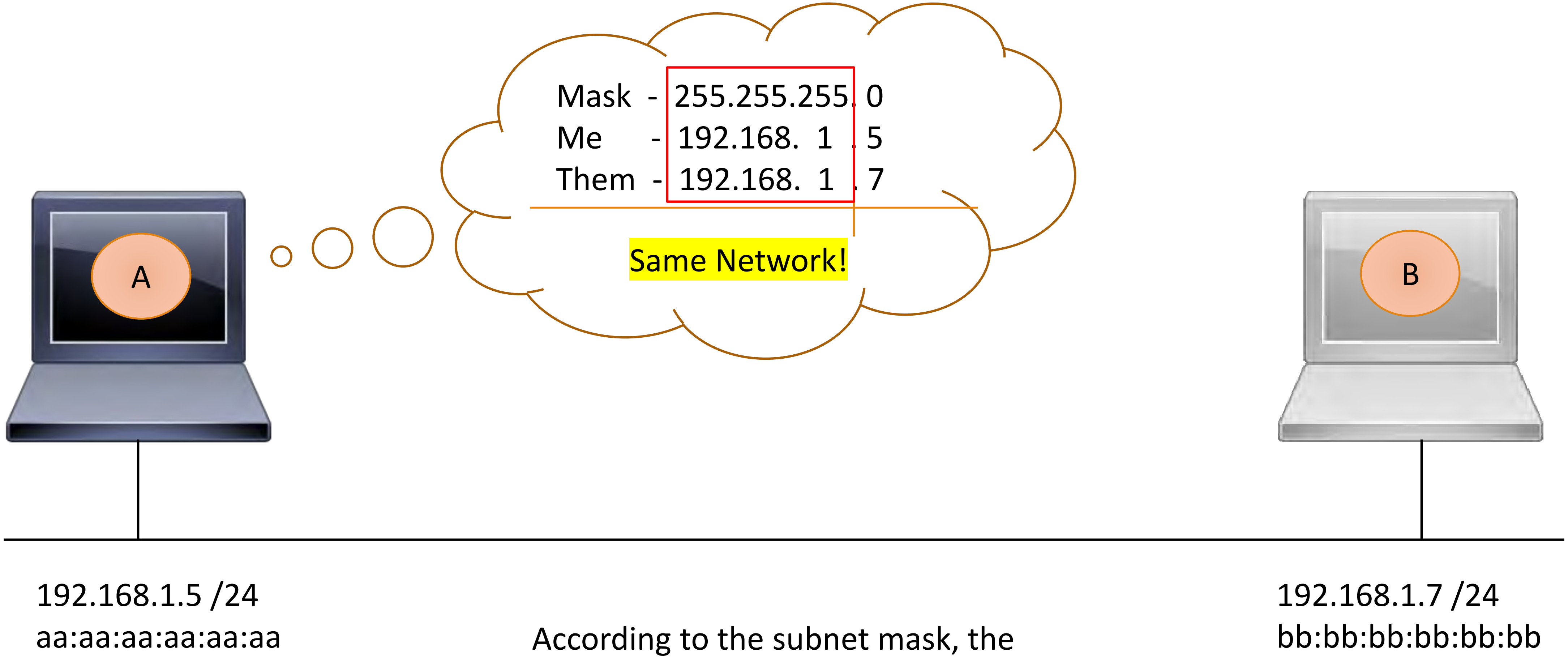


192.168.1.5 /24
aa:aa:aa:aa:aa:aa

After learning the destination IP address,
A (source) uses its subnet mask to determine if B
(destination) is on the same or different network

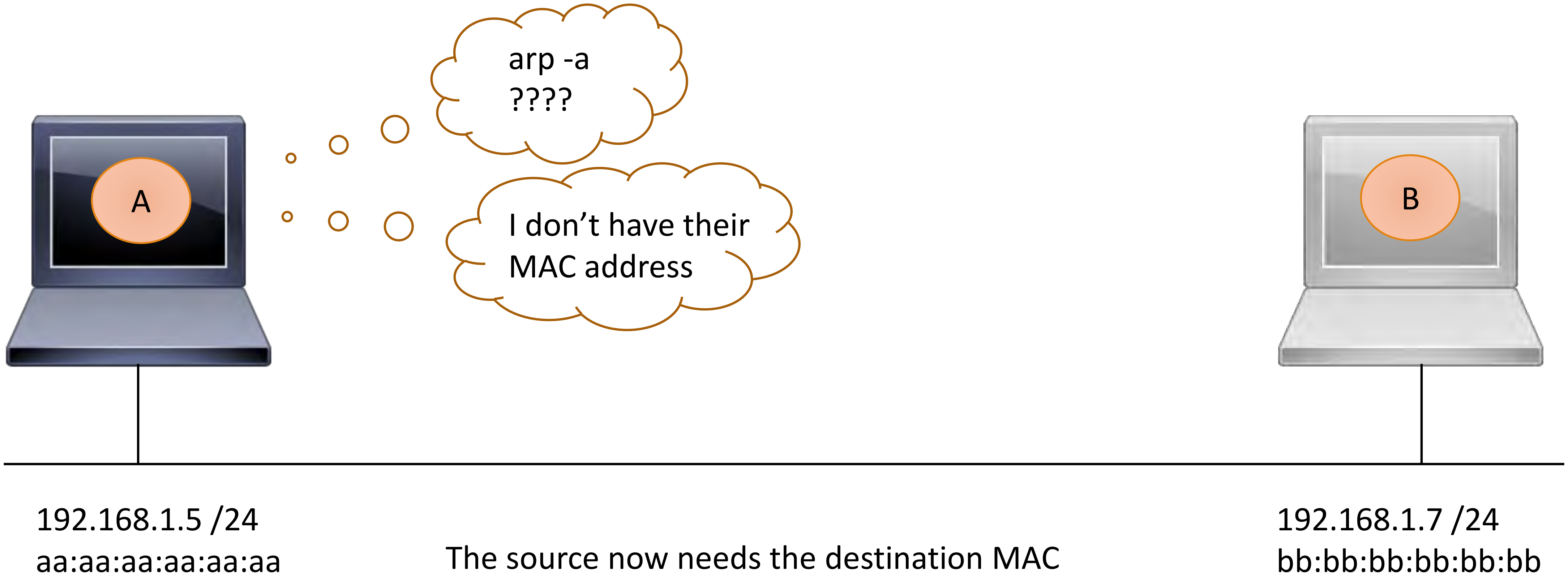
192.168.1.7 /24
bb:bb:bb:bb:bb:bb

Using the Subnet Mask to Evaluate the Destination (cont'd)



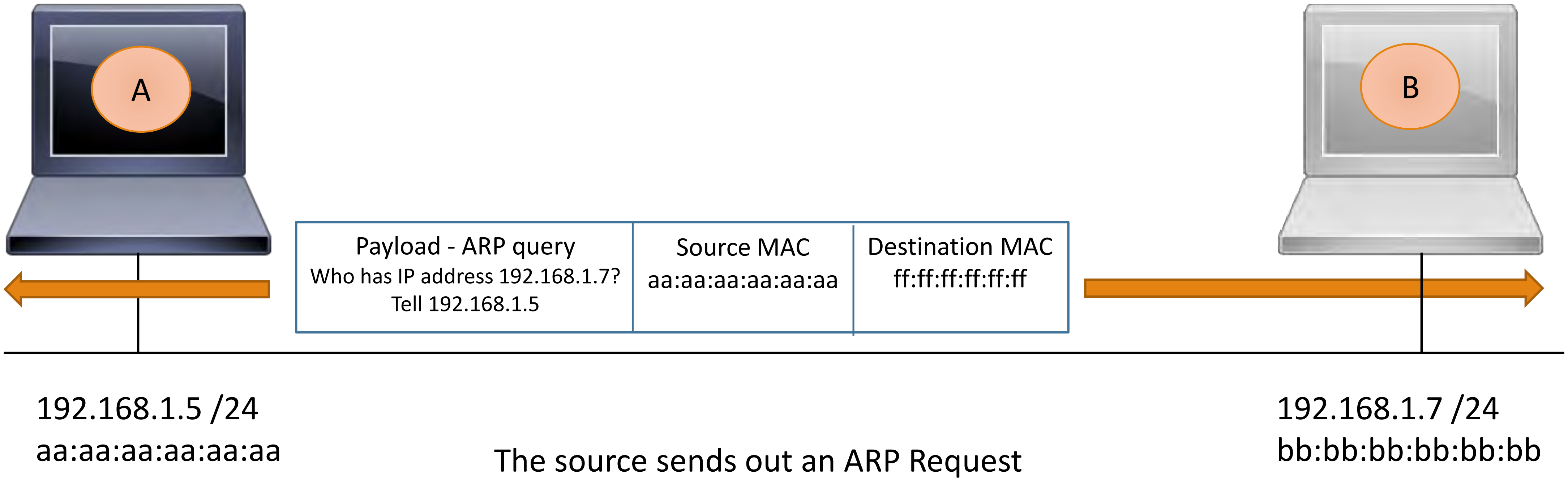
According to the subnet mask, the destination is on the same network

Checking to See if the Destination MAC Address Already Exists in the Sender's ARP Cache



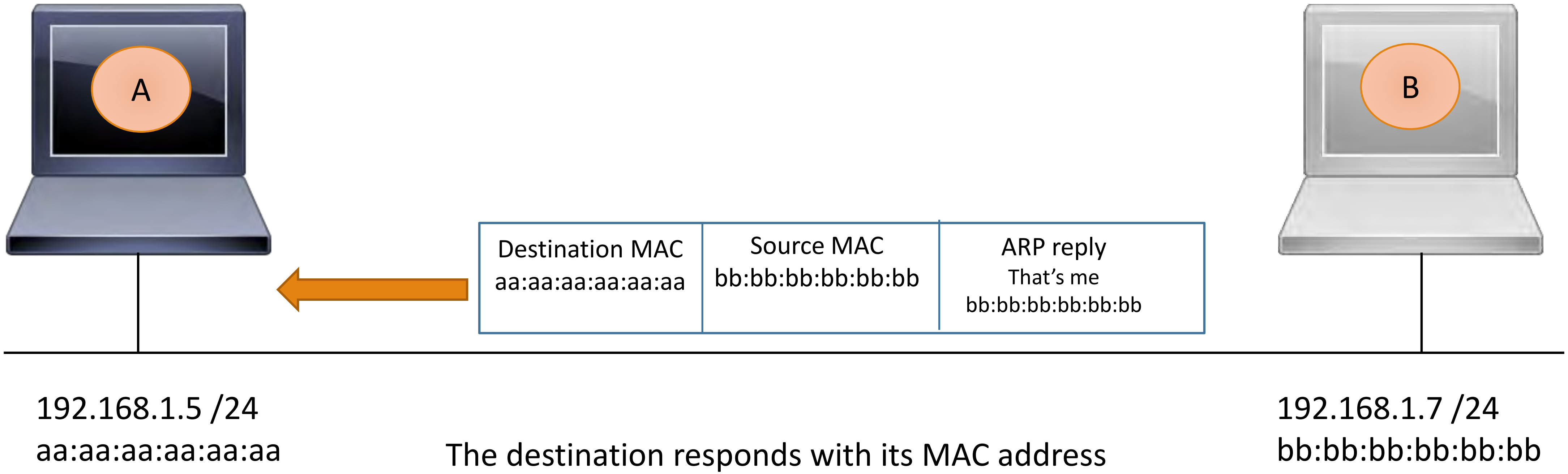
The source now needs the destination MAC address to create the frame

Broadcasting an ARP Request to Learn the Destination MAC Address



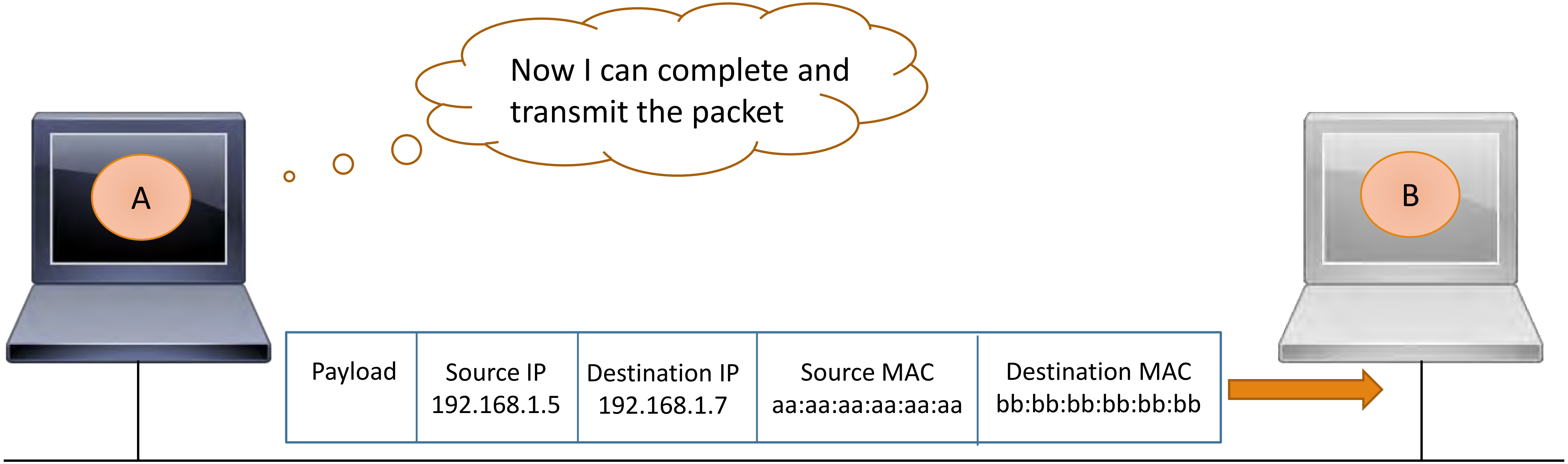
The source sends out an ARP Request via Layer 2 broadcast

Responding with an ARP Reply



The destination responds with its MAC address

Adding the Destination MAC Address to the Ethernet Header and Transmitting the Packet



192.168.1.5 /24
aa:aa:aa:aa:aa:aa

The source can now build the Ethernet frame complete with IP payload
It will transmit the frame and store the IP – MAC mapping in its ARP cache

192.168.1.7 /24
bb:bb:bb:bb:bb:bb

IP Routing Across a Single Router

IP Routing Across a Single Router

Source and Destination are on Different Networks

This example uses MAC addresses at Layer 2

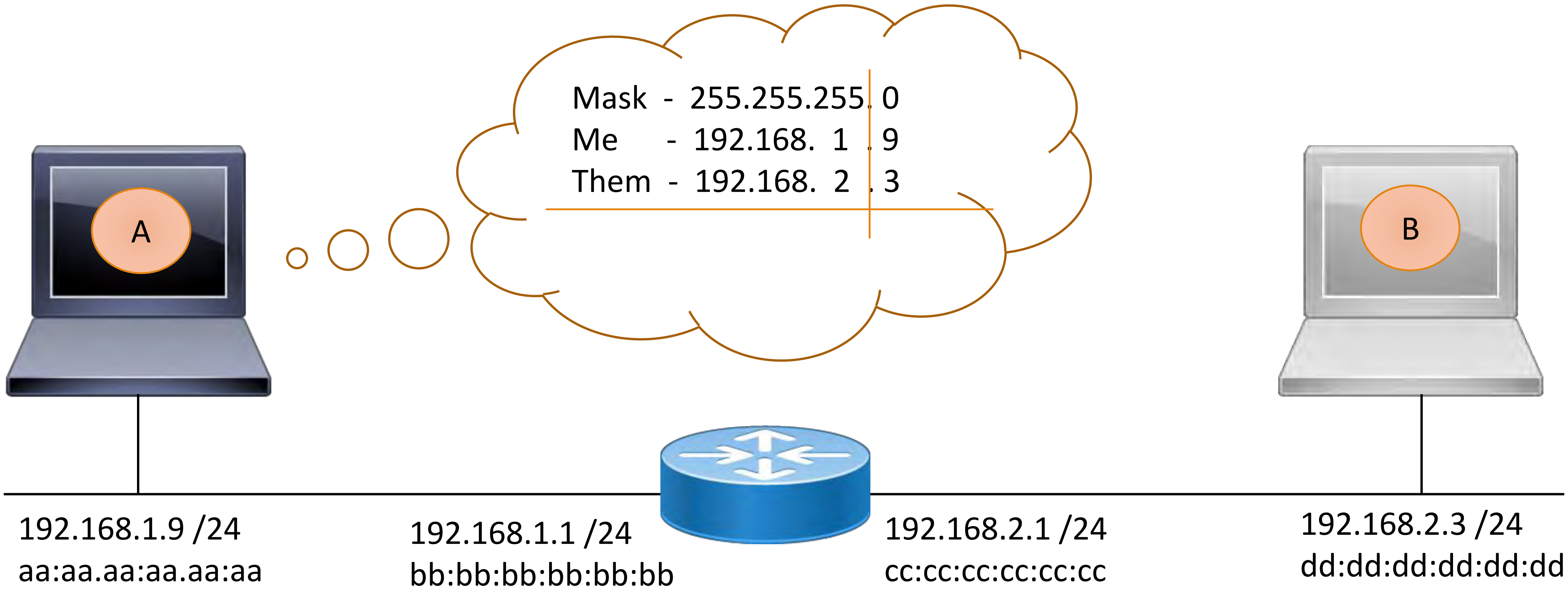
1. A uses its subnet mask to determine that B is on a different network
2. A checks to make sure it has a default gateway (router IP address) configured in its IP properties
3. If A does not have a default gateway, then the packet is undeliverable

   The user may or may not receive an error message
4. If A does have a default gateway, then A checks its ARP cache to see if it already knows the router's MAC address
5. If A does NOT know the router's MAC address, it performs and ARP broadcast to find out that information
6. A puts the router's MAC address in the Ethernet header destination field
7. A transmits the frame and hopes that the router will pick it up and know how to forward it on

IP Routing Across a Single Router (cont'd)

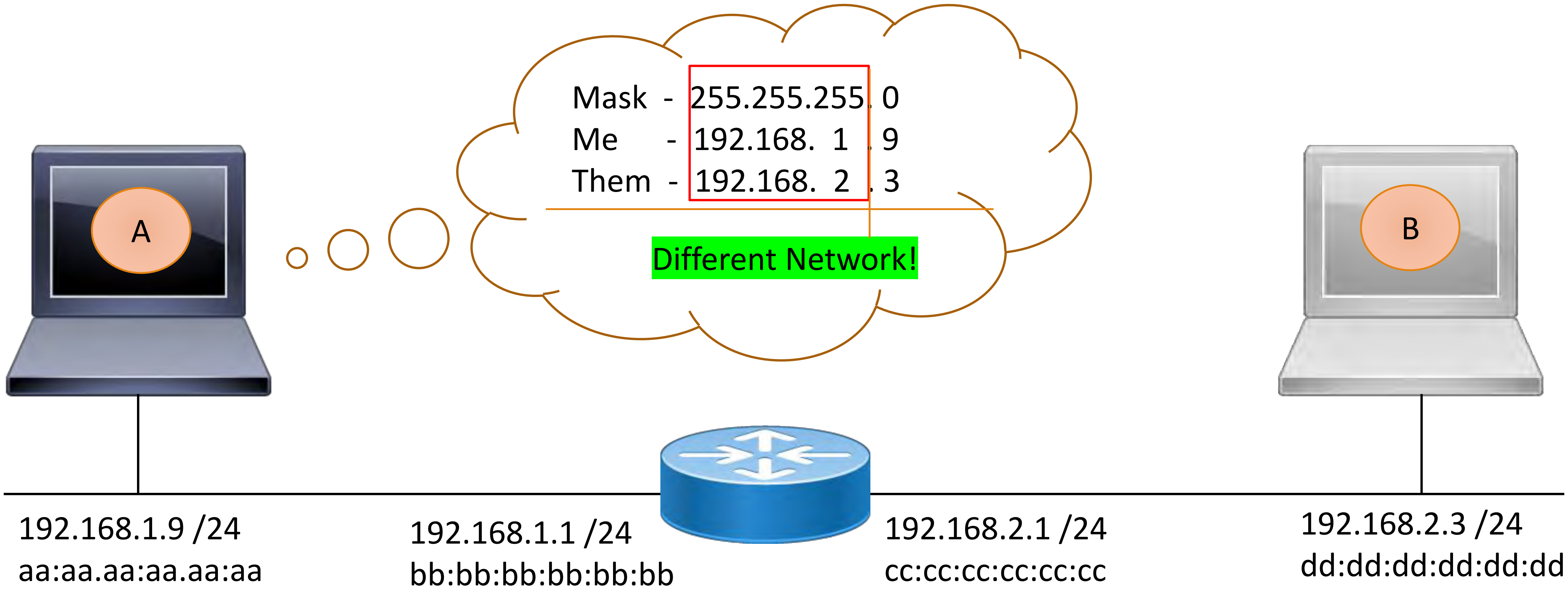
7. The router receives the frame
8. The router checks its route table to see if it has a route to the final destination
9. If it does not, the packet is undeliverable
   - The router sends an ICMP Destination Unreachable message to the sender
10. If the router has a route to the destination, it uses ARP to learn the MAC address of the destination
11. The router re-writes the Ethernet header of the packet, replacing the old source and destination MAC addresses
    - The new source is the MAC address of the router's outgoing port
    - The new destination is the MAC address of the final destination
    - The source and destination IP addresses remain the same
12. The router switches the frame between its two interfaces, transmitting the frame out to the final destination
13. The final destination receives the frame
14. The process is repeated if the destination needs to reply back to the source

IP Routing Across a Single Router Example



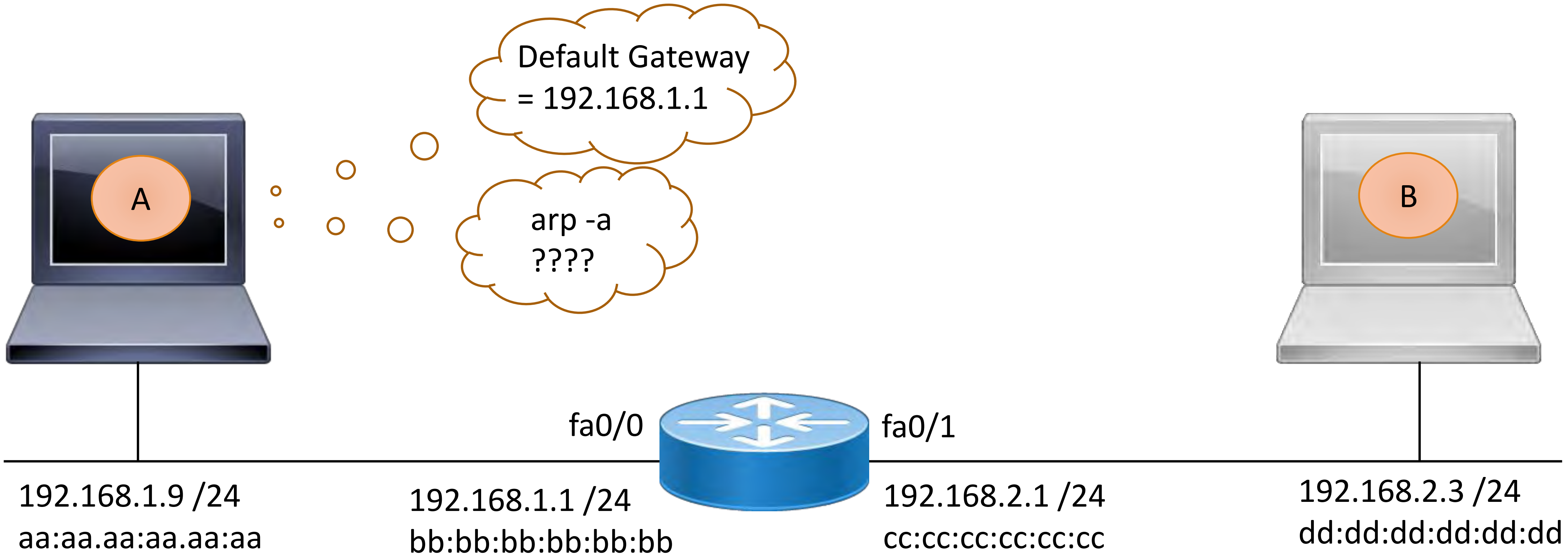
After learning the destination IP address, the sources uses its subnet mask to determine if the destination is on the same or different network

IP Routing Across a Single Router Example (cont'd)



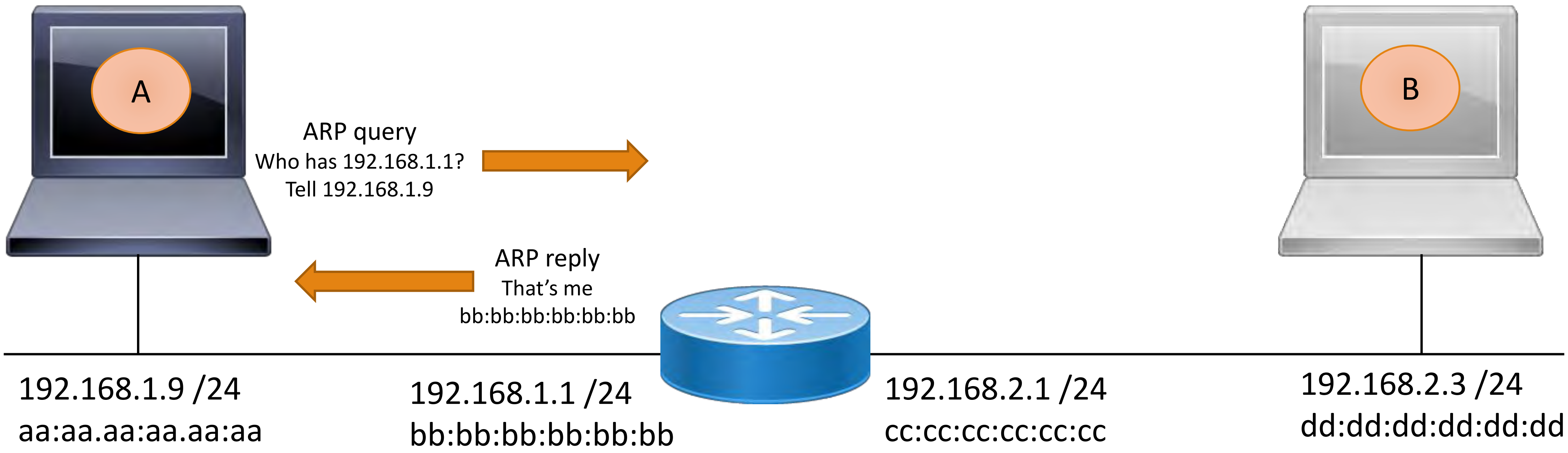
A determines that B is on a different network

IP Routing Across a Single Router Example (cont'd)



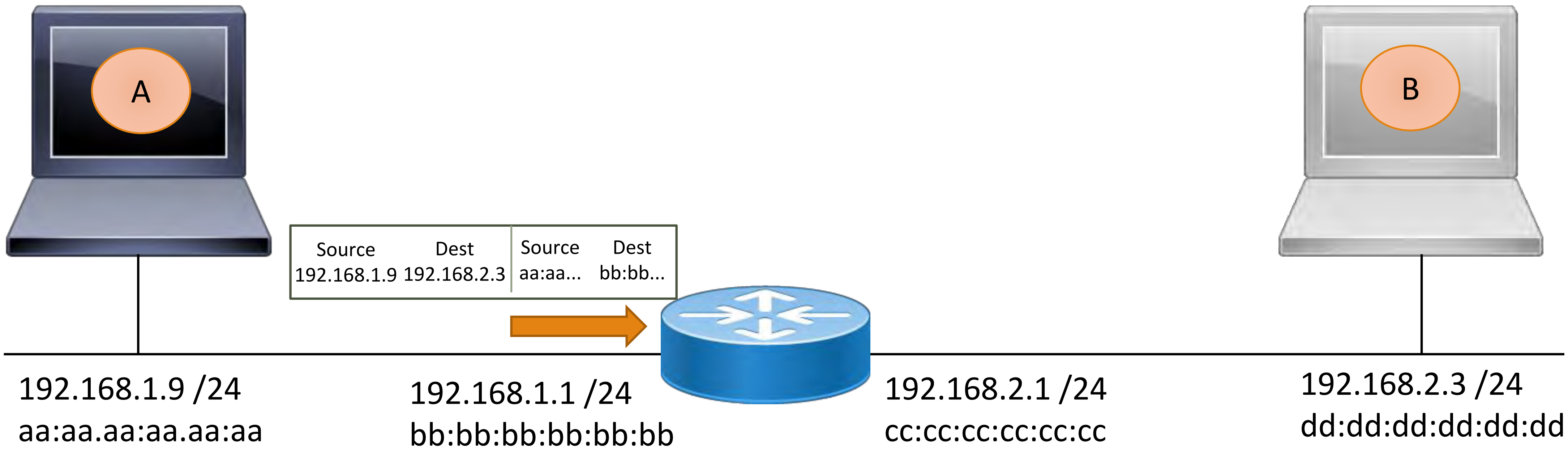
The source knows it must hand a packet destined for a remote network to its default gateway.
It is already configured with the IP address of router, but it does not know the router's MAC address.

IP Routing Across a Single Router Example (cont'd)



The source uses ARP to learn the MAC address of the default gateway

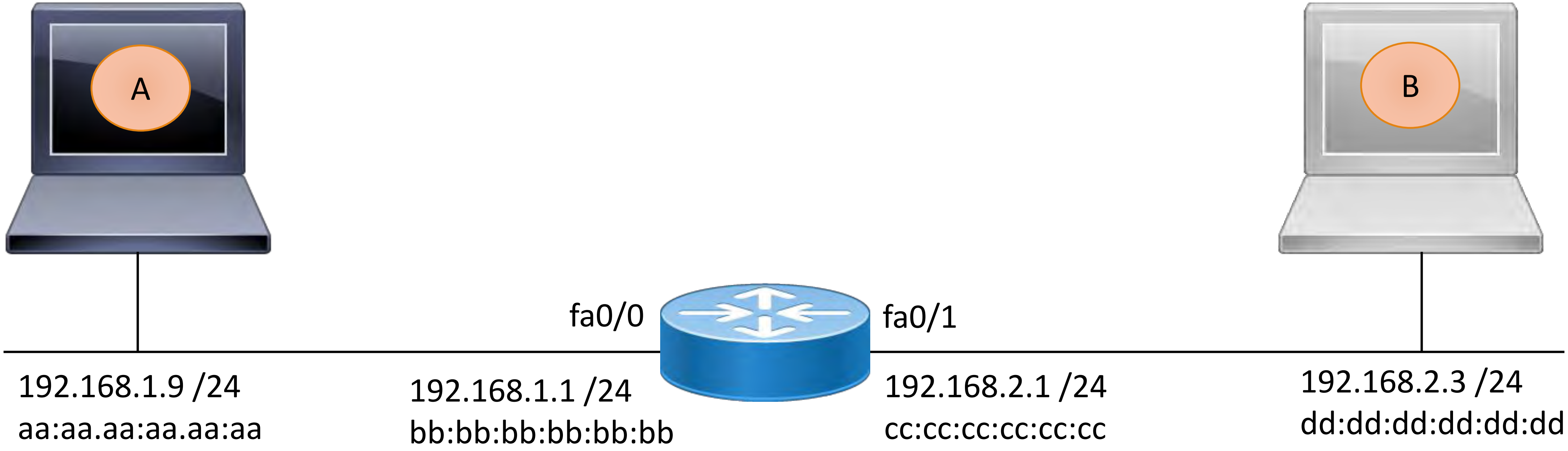
IP Routing Across a Single Router Example (cont'd)



The source creates the Ethernet frame with B as the destination IP, but the router as the destination MAC

The frame is sent to the router MAC address bb:bb:bb:bb:bb:bb

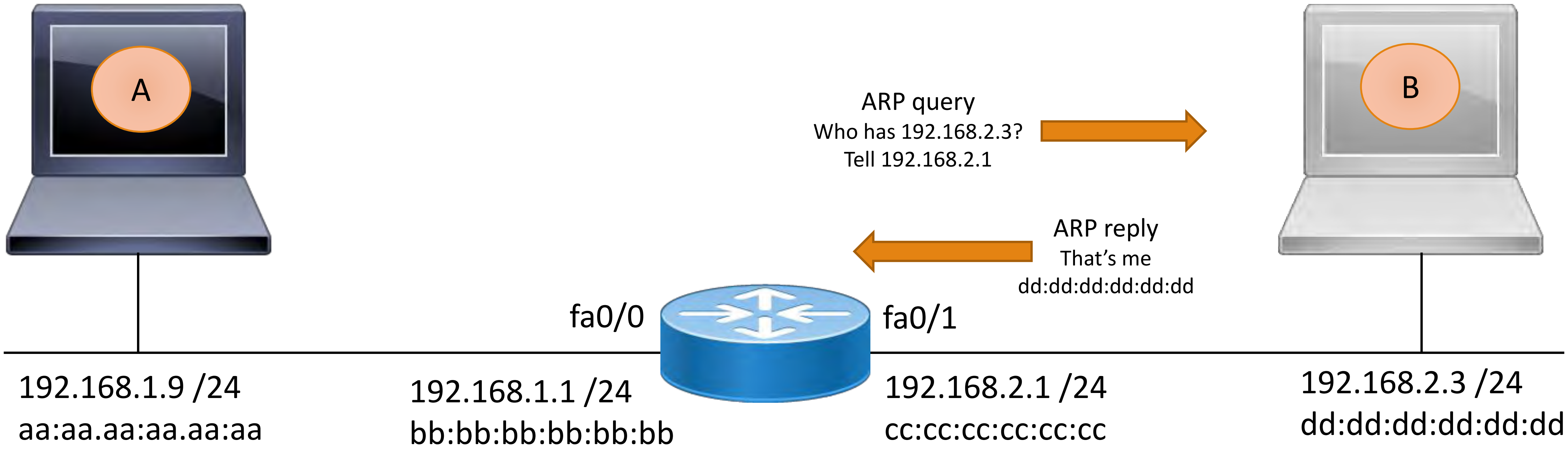
IP Routing Across a Single Router Example (cont'd)



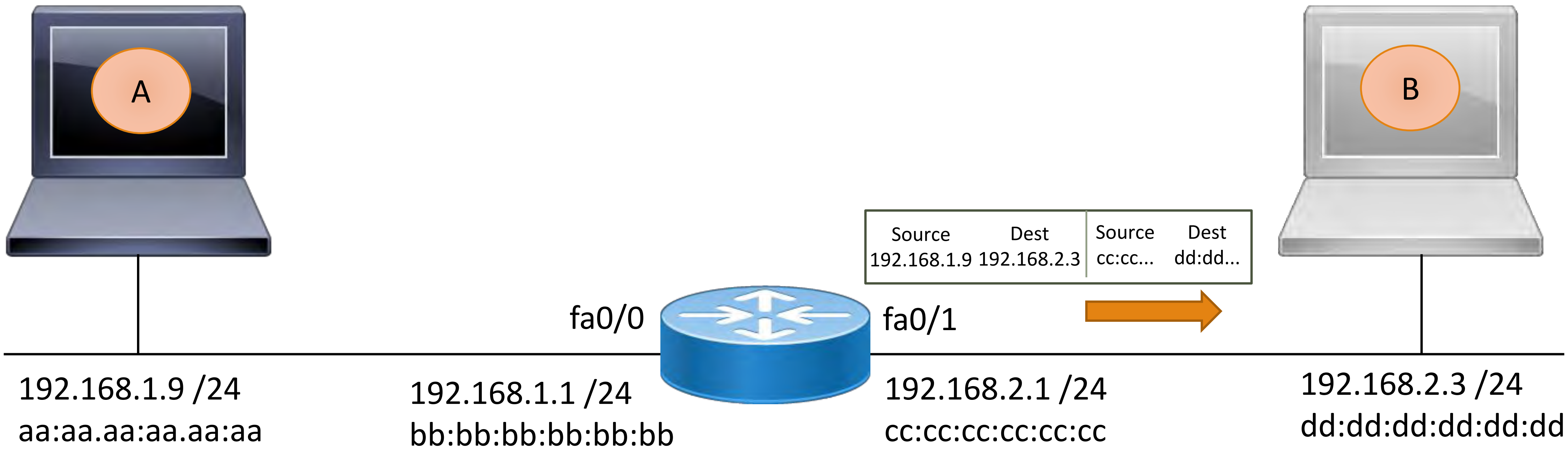
The router receives the frame
It checks its route table to see if it has a route for the Layer 3 destination
Since it does have a route, it must discover the MAC address of the next hop (the final destination)

IP Routing Across a Single Router Example (cont'd)

The router uses ARP to learn the MAC address of the final destination



IP Routing Across a Single Router Example (cont'd)



- The router switches the packet from its incoming interface fa0/0 to its outgoing interface fa0/1
- The router re-writes the packet's Ethernet header with the new source (fa0/1) and destination (B) MAC addresses
    - The source and destination IP address remain the same (A and B)
- The router transmits the packet which is received by B

IP Routing on Across Multiple Hops

IP Routing Across Multiple Routers

Each router reads the Destination IP address to determine the next hop

- Unless you configure security, a router will not read the source IP of the packet

Each router decrements the packet's Time-to-Live field by one as it forwards the packet to the next hop

- A router that receives a packet with a TTL of 0 or 1 will discard it and send an ICMP Time Exceeded message to the sender

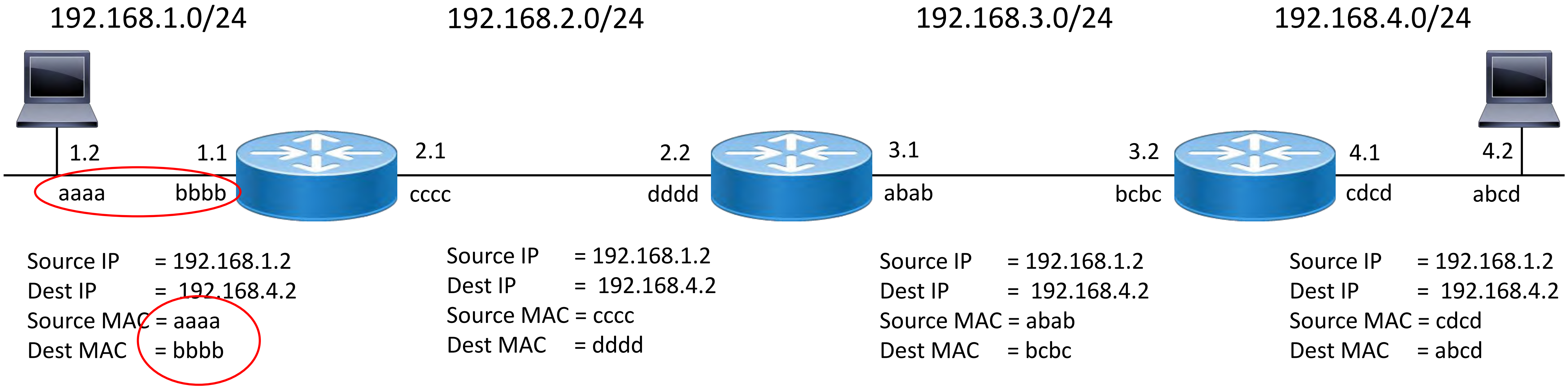
Unless translated, the source and destination IP address remain the same from end to end

Each router changes the source and destination MAC address for the next segment

- The purpose of the Layer 2 header is to get the packet to the next hop until it reaches its final destination

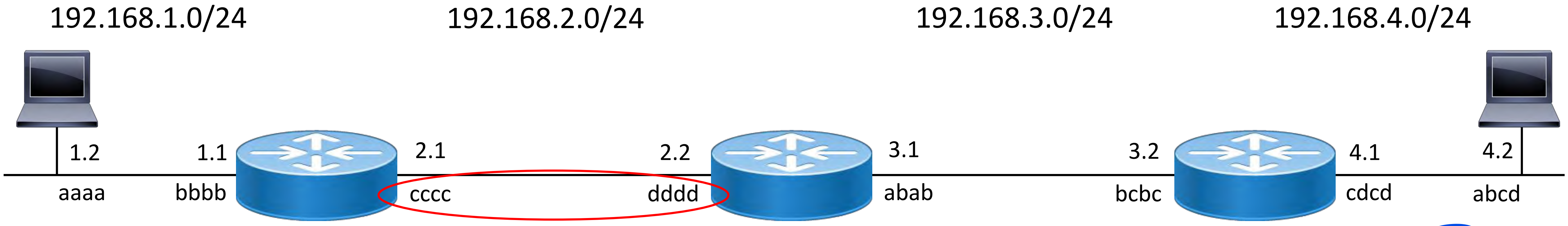
The last router actually delivers the packet to its final destination

Routing Across Multiple Hops Example



Note: MAC addresses in this example have been shortened and simplified for visual convenience

Routing Across Multiple Hops Example (cont’d)



Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = aaaa
Dest MAC = bbbb

Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cccc
Dest MAC = dddd

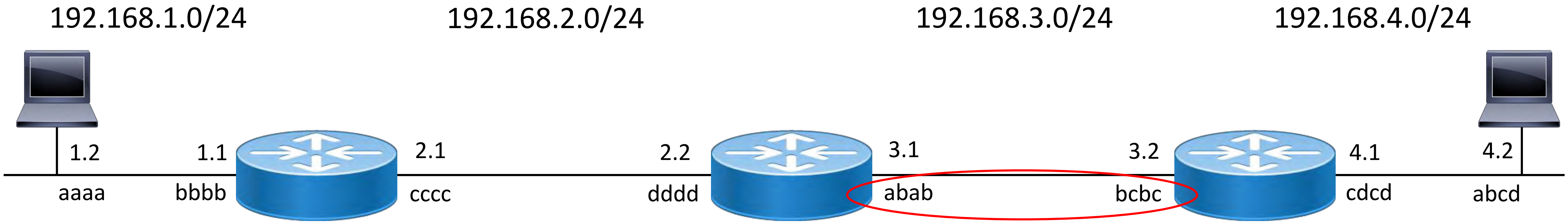
Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = abab
Dest MAC = bcbc

Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cdcd
Dest MAC = abcd

the sourec and destination IP are the same they neverr change

Note: MAC addresses in this example have been shortened and simplified for visual convenience

Routing Across Multiple Hops Example (cont'd)



Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = aaaa
Dest MAC = bbbb

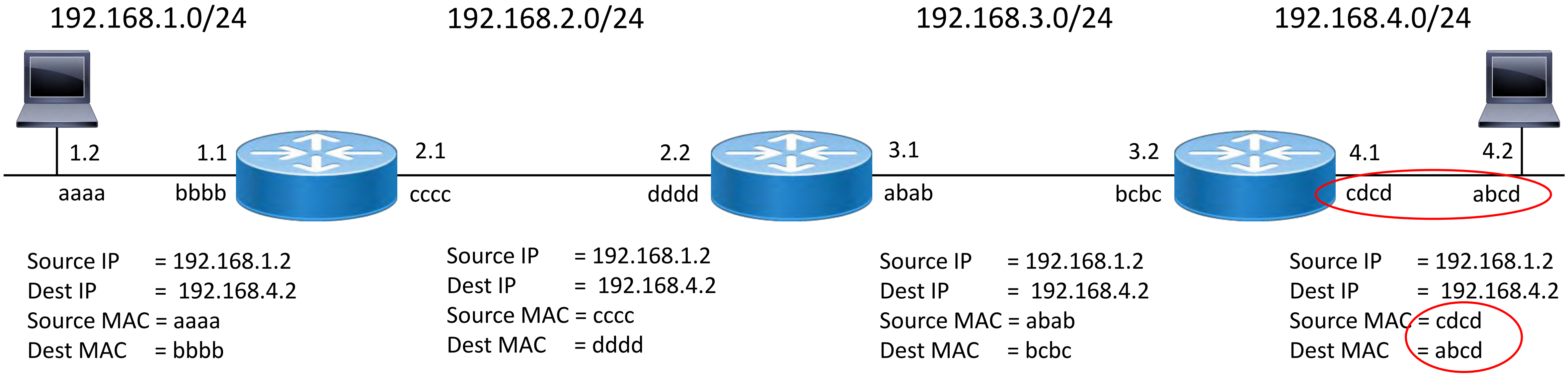
Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cccc
Dest MAC = dddd

Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = abab
Dest MAC = bcbc

Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cdcd
Dest MAC = abcd

Note: MAC addresses in this example have been shortened and simplified for visual convenience

Routing Across Multiple Hops Example (cont'd)



Note: MAC addresses in this example have been shortened and simplified for visual convenience

Route Selection

Choosing a Route

Routers may or may not have multiple routes to choose from

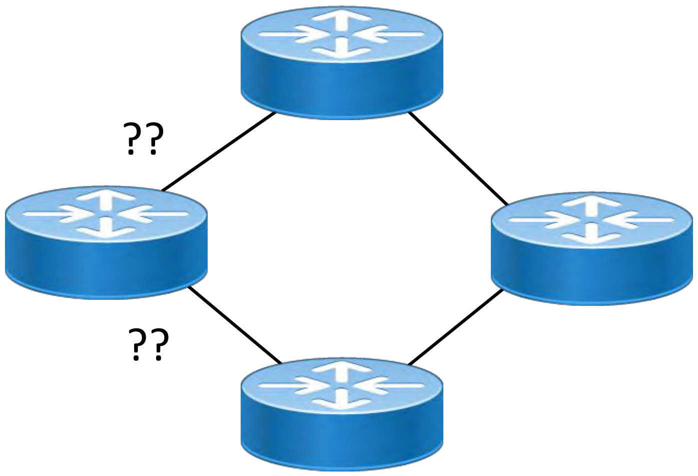
The “best” route will be placed in the router’s route table

Criteria for choosing a route is based on:

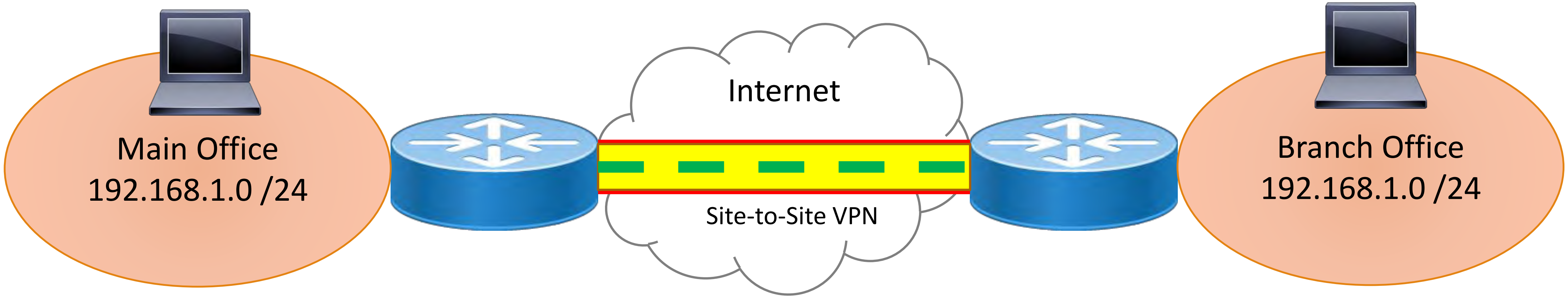
- 1. Administrative Distance
- 2. Metric

Every route in a route table must be viable

- Otherwise the router will not be able to choose the right path
- It might choose a path that is invalid

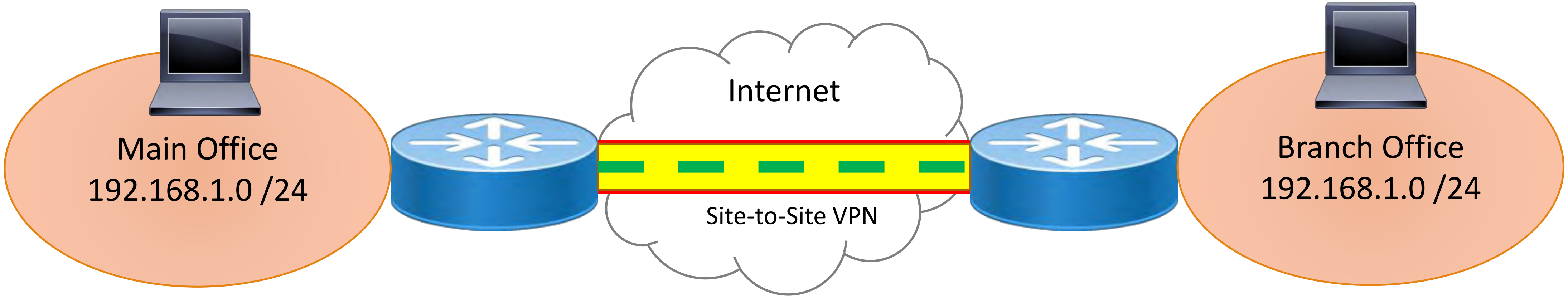


A Common Example of a Bad Implementation



Can you tell what's wrong?

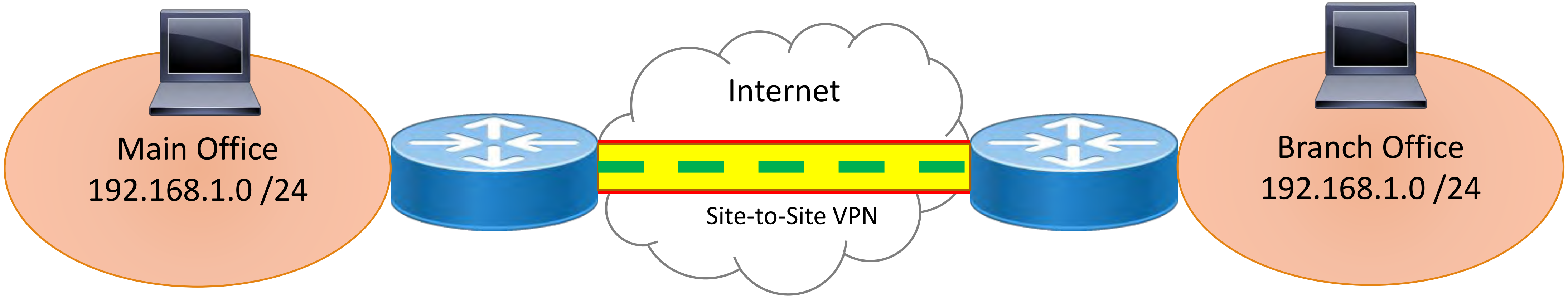
A Common Example of a Bad Implementation



Can you tell what's wrong?

The routers cannot tell if destination 192.168.1.x is local or should be sent across the VPN to the other office

A Common Example of a Bad Implementation

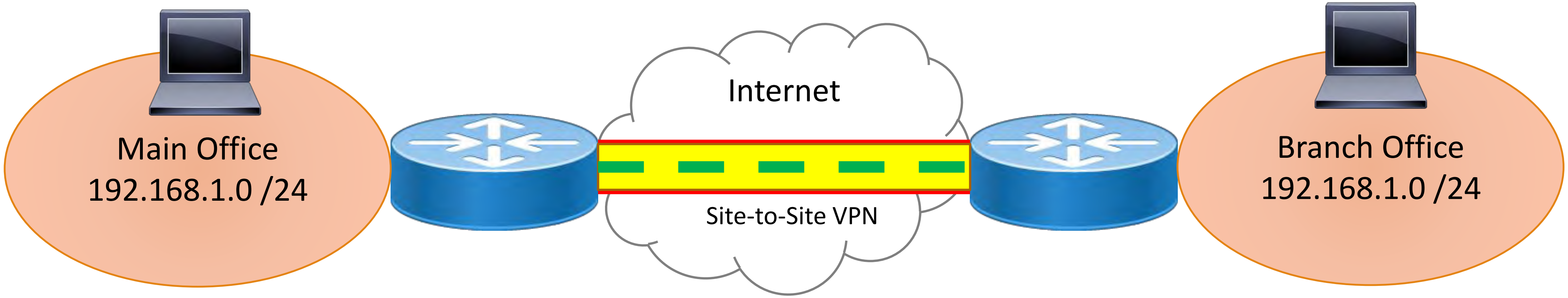


Can you tell what's wrong?

The routers cannot tell if destination 192.168.1.x is local or should be sent across the VPN to the other office

How would you fix this?

A Common Example of a Bad Implementation



Can you tell what's wrong?

The routers cannot tell if destination 192.168.1.x is local or should be sent across the VPN to the other office

How would you fix this?

Change the subnet on one of the sides to something different, such as 192.168.2.0 /24

Administrative Distance

"Believability" of a route source (routing protocol)

Each routing protocol has an assigned administrative distance

If two or more routing protocols offer routes to the same destination, the route with the lower administrative distance will be used

- The router must be configured to use multiple routing protocols

Cisco Administrative Distances

Routing Protocol	Administrative Distance
Directly connected	0
Statically entered	1
(Exterior) BGP	20
EIGRP	90
OSPF	110
RIP	120
Unreachable	255

Note: Although not technically routing protocols, directly connected links and statically entered routes are assigned administrative distances, and are treated as routing protocols by the router

Metric

The cost/desirability of a particular route compared with other routes learned from the same routing protocol

- If the same routing protocol offers multiple routes to the same destination, the route with the best (lowest) metric will be used

Can be based on:

- Hop count
- Bandwidth + delay
- Cumulative link cost
- Other factors such as link reliability and MTU

Cisco IP Route Table Example

```
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

S    192.168.1.0/24 [1/0] via 192.168.2.1
C    192.168.2.0/24 is directly connected, Ethernet1/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R    192.168.5.0/24 [120/1] via 192.168.2.1, 00:00:12, Ethernet1/0
C    192.168.6.0/24 is directly connected, Ethernet1/1
```

Administrative Distance

Metric

Next Hop

Your local outbound interface

Routed vs Routing Protocols

Routed protocols = the actual user traffic

- Example: IP

Routing protocols = the language routers use to compare and update each other’s route tables

- Process is dynamic
- A router can use more than one routing protocol for compatibility
- Used by both IPv4 and IPv6
- Examples: RIP, OSPF, EIGRP, BGP

Routing Protocol Types

Distance Vector

- How far / What direction
- Old style / simple
- Routers update each other on a fixed interval
- Slow convergence
- Good for small networks
- Very easy to implement
- RIP

Link State

- Routers maintain a database of the entire network and all routes
- If a link changes state, routers immediately update each other
- Fast convergence
- Good for large internal networks
- Requires a carefully planned, hierarchical network
- Can be complex to implement
- Requires more resources from the router
- OSPF

Hybrid

- Uses the best features of distance vector and link state
- Very fast convergence
- Excellent for large internal networks that grew organically / were not well designed
- All routers must belong to the same autonomous system
- Easy to implement
- EIGRP

Path Vector

- A variation on distance vector
- A “hop” is an entire network, not just a single router
- All routers in a hop belong to the same autonomous system
- Used on the Internet between ISPs
- Very slow convergence
- Complex to implement
- Requires a very large network to be worthwhile
- BGP

Interior vs Exterior Routing Protocols

Also called Interior and Exterior Gateway Protocols

Interior Routing Protocol

- Used within an organization’s internal/private network
- RIP, OSPF, EIGRP

Exterior Routing Protocol

- Used between ISPs on the Internet
- BGP

RIP

Routing Information Protocol (RIP) v1

The original distance vector routing protocol

A very simple interior gateway protocol

- Layer 7 protocol
- UDP 520

Does not understand VLSM

- Assumes all networks use classful subnet masks
- Cannot handle customized subnet masks with discontiguous networks

Uses broadcasting for route updates

- Full routing table is broadcast out all interfaces every 30 seconds

Routing Information Protocol (RIP) v1 (cont'd)

Router convergence is slow

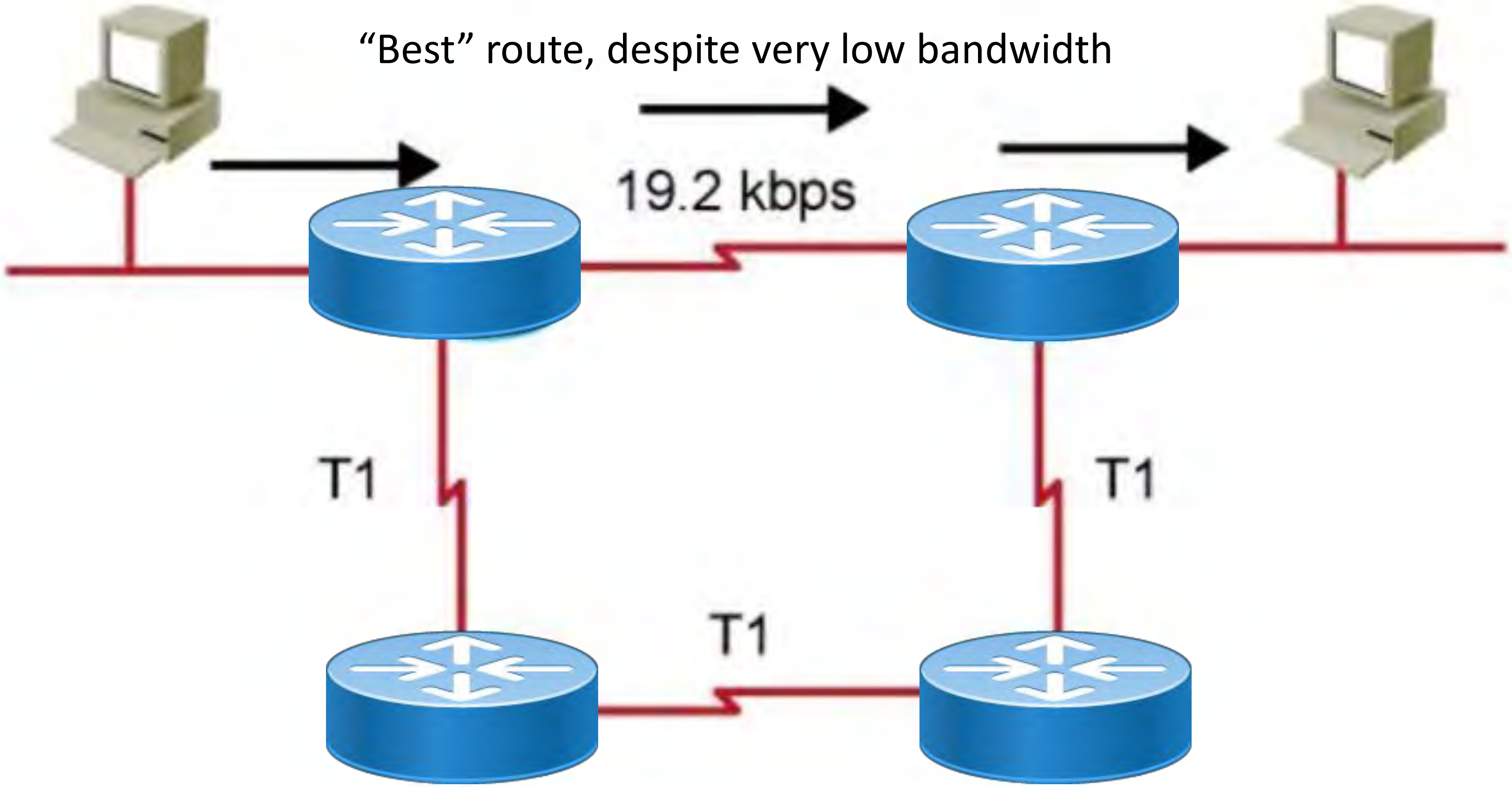
- If many routers are daisy-chained together, can take several minutes for the far end router to be fully updated
- This can cause "black holes" if routers try to send traffic to routes that are no longer viable

Incoming RIP advertisements from neighboring routers are accepted and added to the route table with no verification of source or validation of route

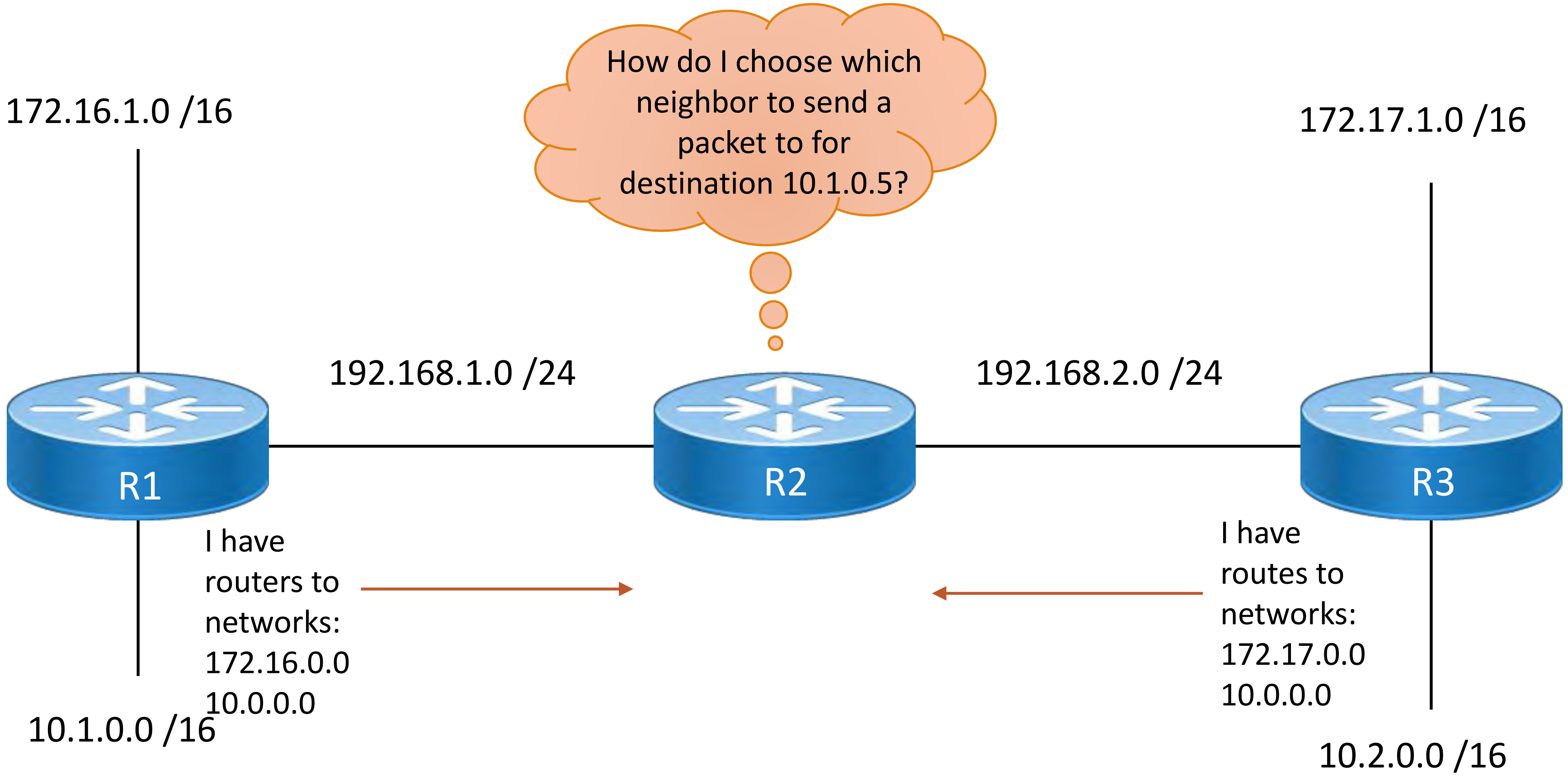
Metric = hop count

- How many more routers must the packet pass through to reach the destination
- All network speeds treated equally - no regard for bandwidth, delay, or other conditions on a particular link
- Has a maximum hop count (in any one direction) of 15

RIP Hop Count Example



RIP v1 Discontiguous Network Example



RIP v1 does not include the destination subnet mask in its route updates

RIP v2

Update to RIP v1

Uses multicasting 224.0.0.9 for route updates

Understands VLSM
- The subnet mask is part of the RIP v2 route update
- Routes are automatically summarized
- You can also manually summarize routes as desired

Updates are sent by multicast, not broadcast
- This relieves non-router devices on the segment from having to process a broadcast that is not meant for them

Routers can be configured to authenticate each other
- Plain text
- MD5

Routers can be configured to transmit/receive v1, v2, or both

Note: RIPng is an extension of RIP v2 used for IPv6

Challenges and Solutions of RIP

Invalid routes can stay in a route table for several minutes

- This leads to routers sending traffic to "black holes"
- Solution: if one of your links goes down, transmit an immediate update out all other links with no delay

"Flapping" route (link keeps going up and down)

- Solution: If a neighbor sends you an immediate update, place a hold on the old route before deleting it from your own table

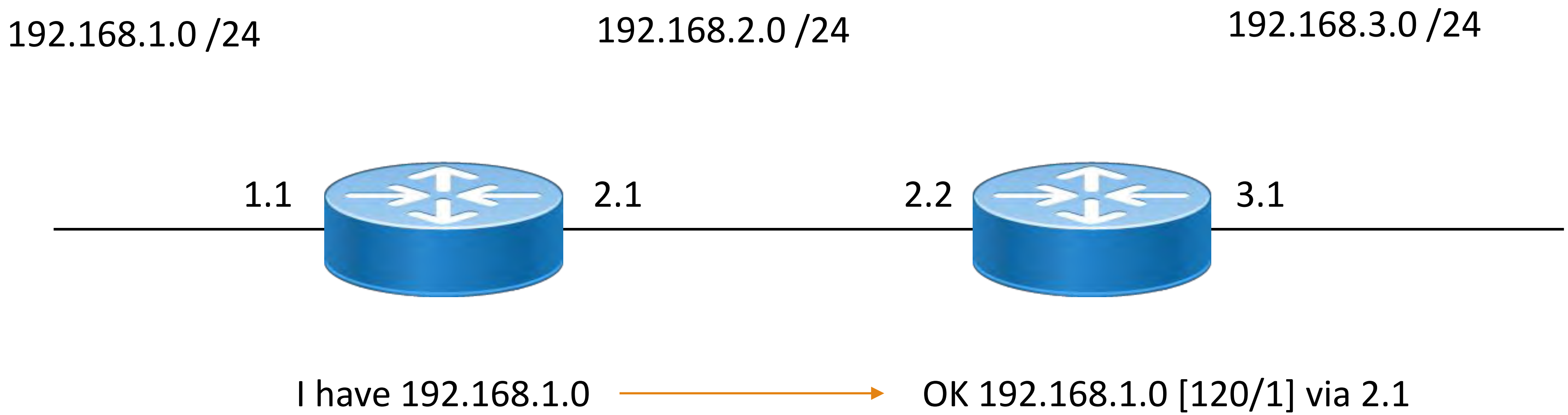
"Count to Infinity"

- Two routers keep feeding each other false updates in a runaway process
- Solutions:
  - Maximum hop count of 15 (in any one direction from that router)
  - Split horizon - Router will not advertise out an interface where route was learned
  - Poison reverse - immediately mark a downed route as unreachable (16 hops) and inform your neighbor of the change

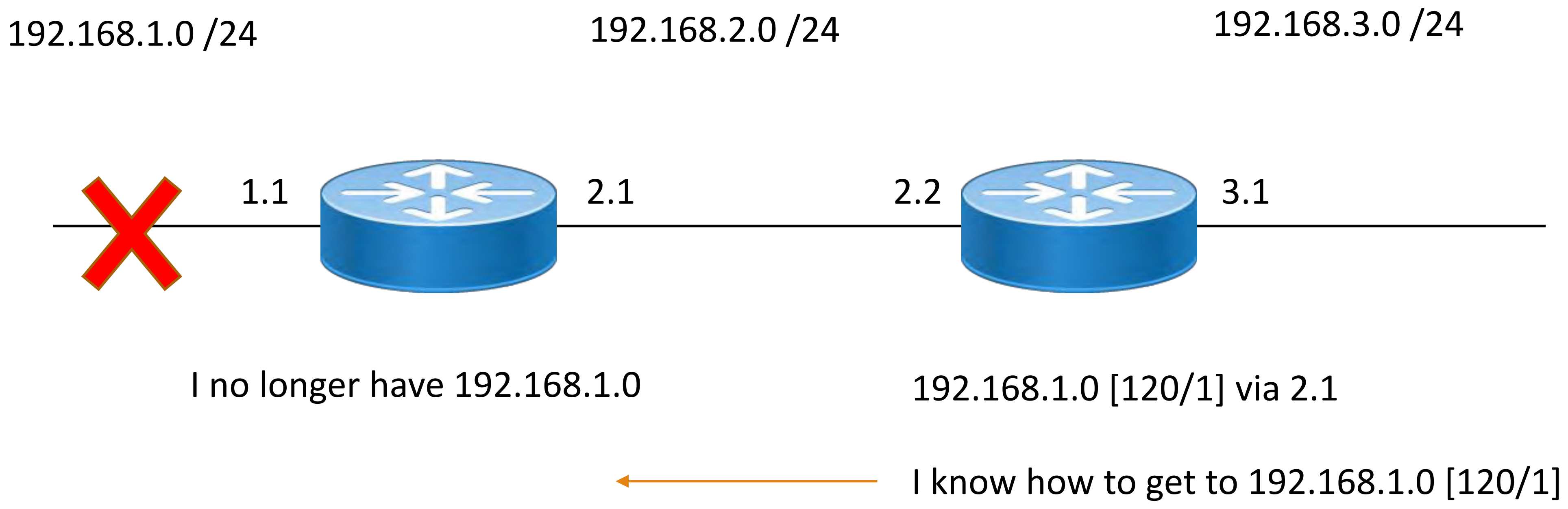
Does not scale well to larger networks

- Use EIGRP!

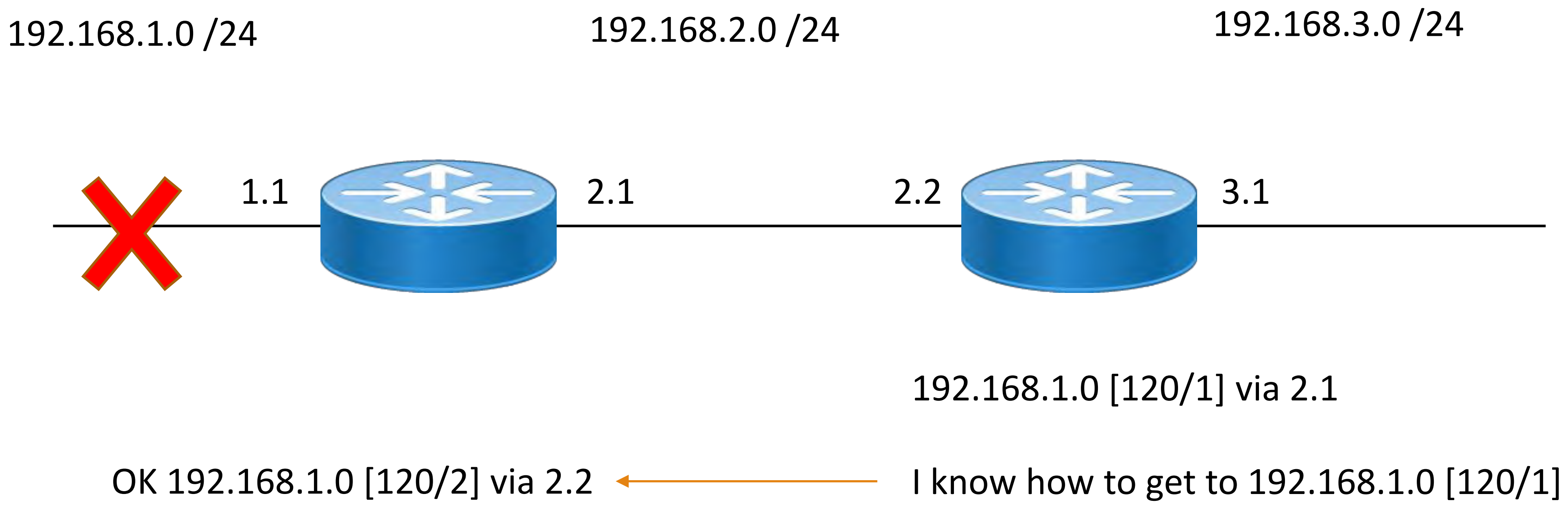
RIP Counting to Infinity



RIP Counting to Infinity



RIP Counting to Infinity

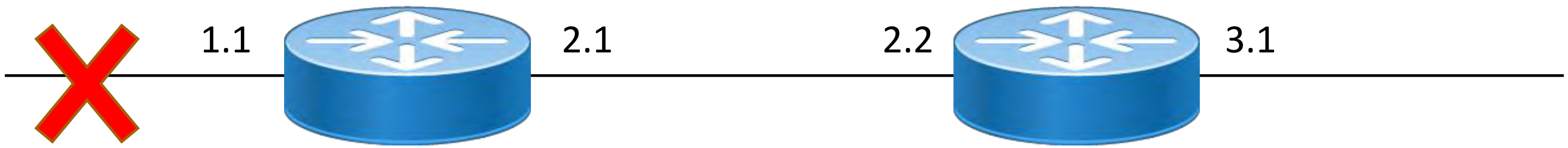


RIP Counting to Infinity

192.168.1.0 /24

192.168.2.0 /24

192.168.3.0 /24



192.168.1.0 [120/1] via 2.1

192.168.1.0 [120/2] via 2.2

I know how to get to 192.168.1.0 [120/1]

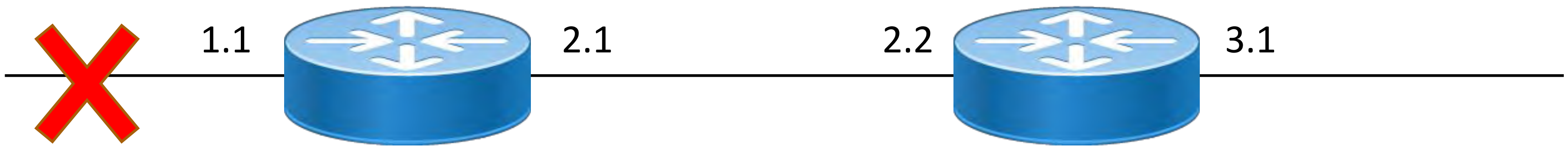
Route update 192.168.1.0 [120/2]

RIP Counting to Infinity

192.168.1.0 /24

192.168.2.0 /24

192.168.3.0 /24

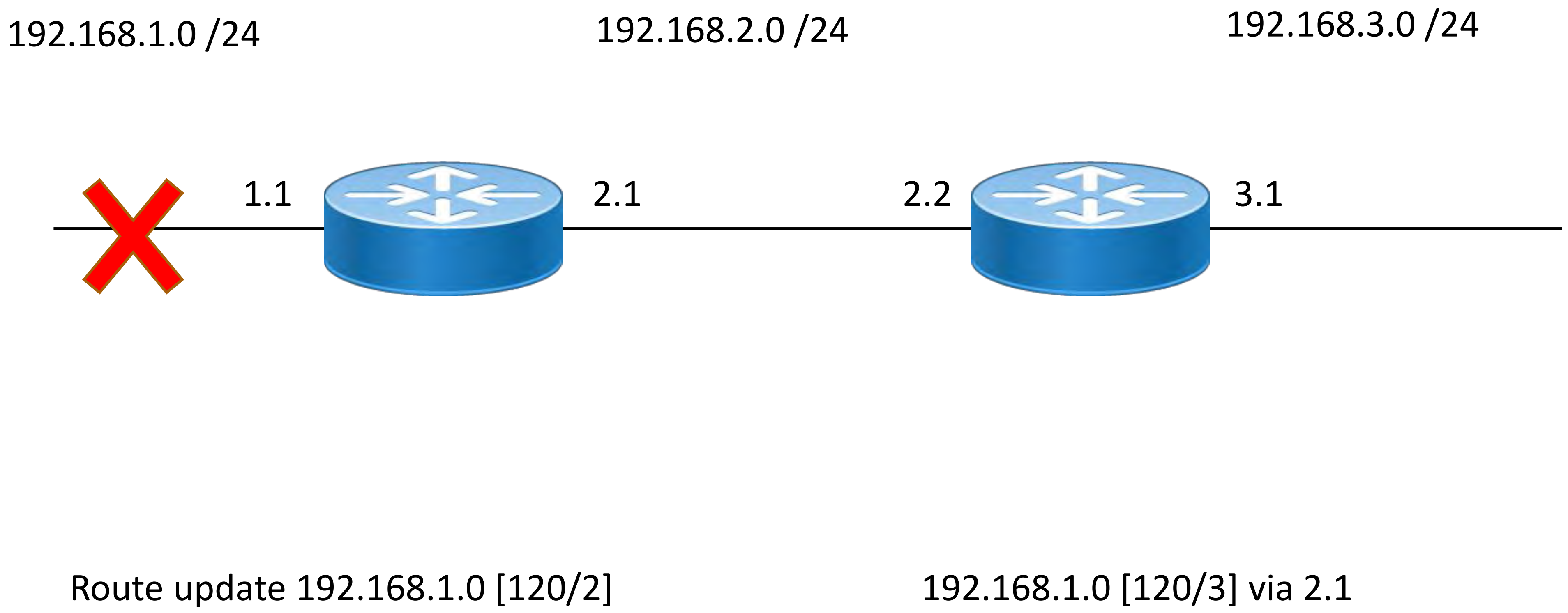


192.168.1.0 [120/1] via 2.1

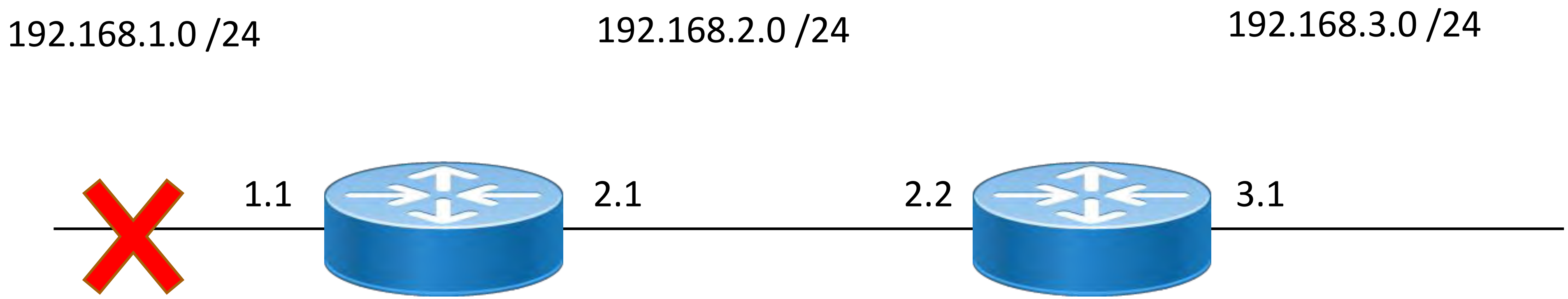
192.168.1.0 [120/2] via 2.2

Route update 192.168.1.0 [120/2] → OK 192.168.1.0 [120/3] via 2.1

RIP Counting to Infinity



RIP Counting to Infinity

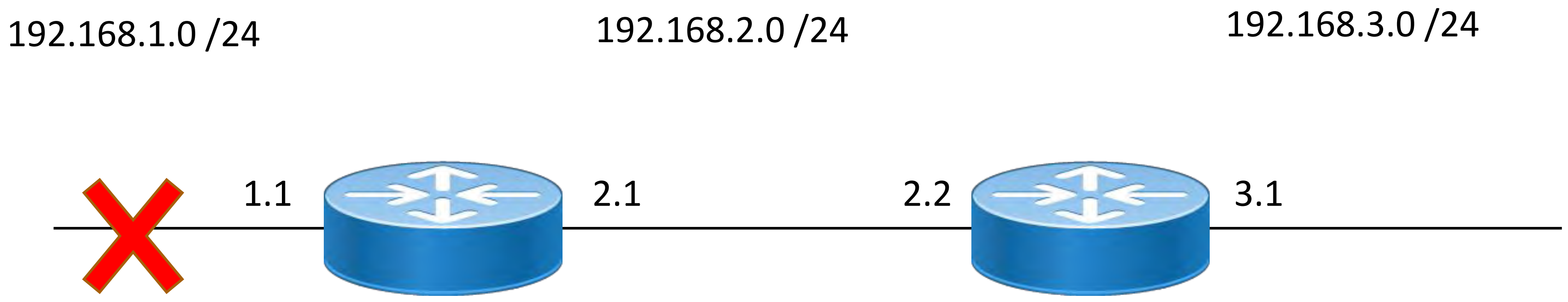


Route update 192.168.1.0 [120/2]

192.168.1.0 [120/3] via 2.1

OK 192.168.1.0 [120/4] via 2.2 ← Route update 192.168.1.0 [120/3]

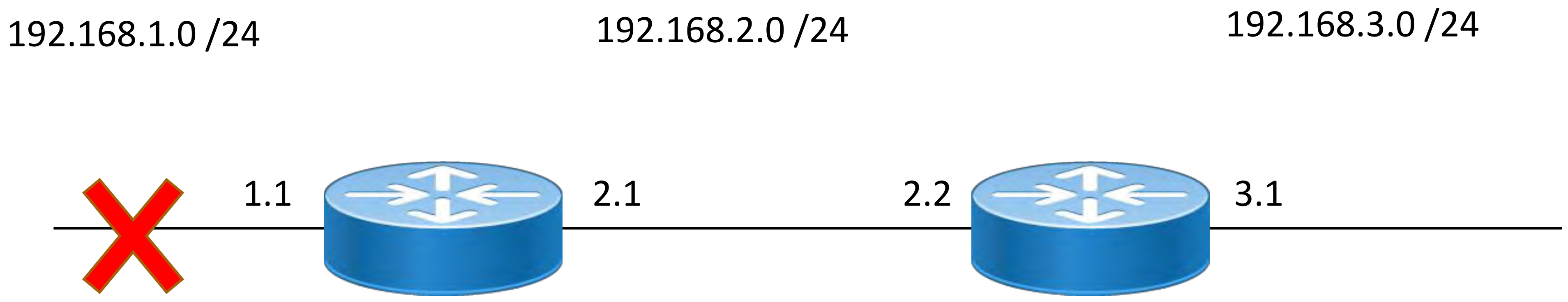
RIP Counting to Infinity



192.168.1.0 [120/3] via 2.1

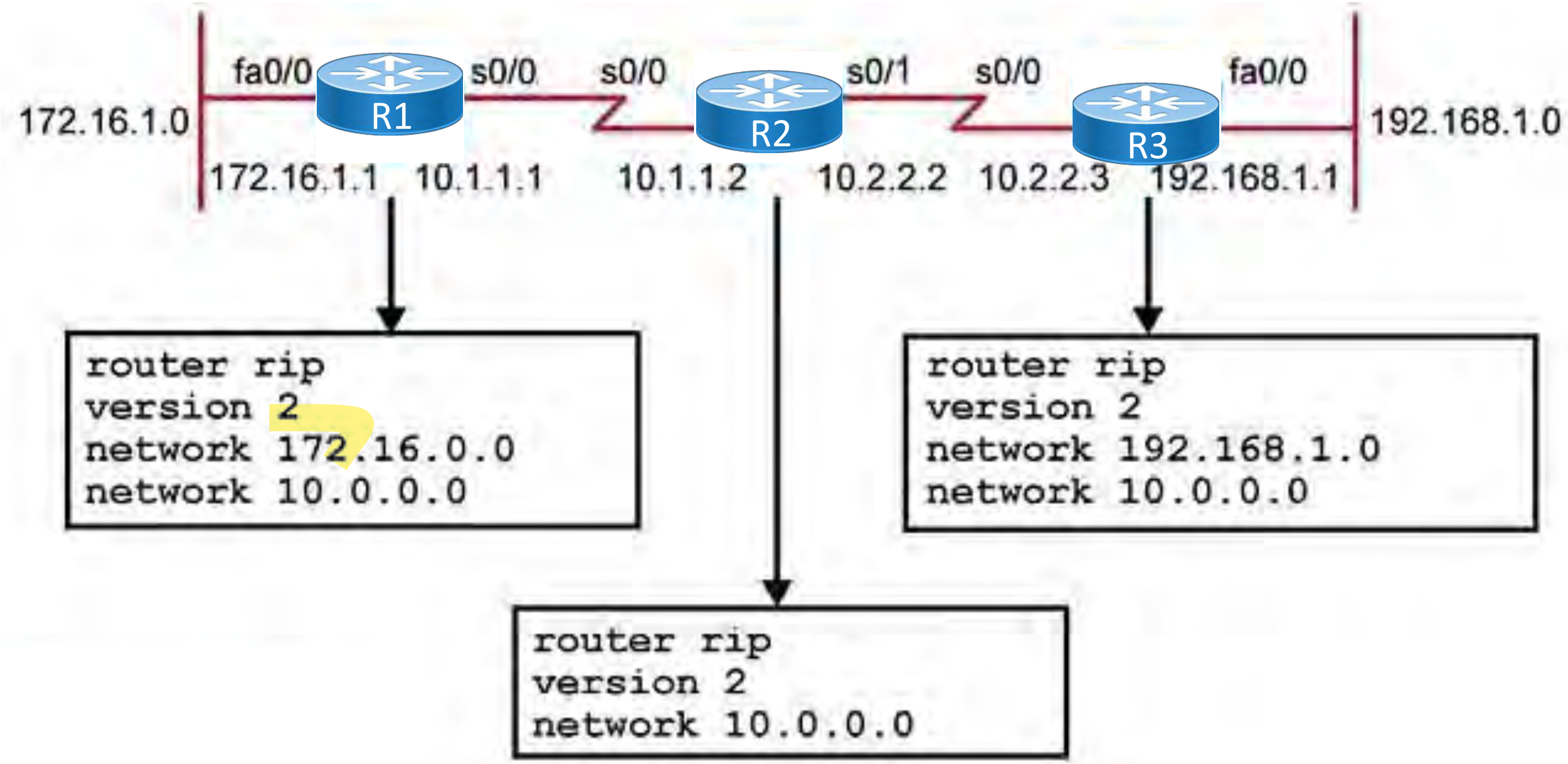
192.168.1.0 [120/4] via 2.2 ← Route update 192.168.1.0 [120/3]

RIP Counting to Infinity



The routers will keep updating each other
They miss the key point that there is NO route to that destination
They could keep going on to infinity
So we put a 15 hop count limit on any route
Once a route reaches metric 16, the route is considered “unreachable”

Configuring RIP Example



Each router declares (advertises) its own directly connected networks. Do NOT enter someone else's networks in the network statement! Routers will learn about other networks from their neighbors.

OSPF

Open Shortest Path First (OSPF)

Very widely used link state interior gateway protocol

Layer 3 protocol
- Protocol ID 89
- Direct payload of IP

Works well with VLSM
- Can be used to manually summarize routes

Route updates are sent only when a link changes state
- Hello keepalives maintain the OSPF neighbor relationships between route updates

Routers are organized into "areas" (each with max of 400 routers)
- Each area should contain a contiguous block of IP addresses that can be summarized at the area border router
- Networks IPs within one area should be hierarchically organized to take advantage of CIDR and route summarization
- Subnets from one area should not exist in another area
- Traffic between areas travels through the backbone "Area 0"

An Area Border Router (ABR) connects an area to the backbone

Open Shortest Path First (OSPF) (cont'd)

OSPF routers typically use loopback addresses to identify themselves

- The loopback interface is virtual so it never "goes down"
- Loopback interfaces can use addresses other than 127.0.0.1
- You can ping/remotely access a router via its loopback if you allow OSPF to advertise it to neighbors along with other destinations

Routers form master/slave or designated/backup designated relationships among themselves

- help stay organized and reduce router update traffic

Routers (mostly) use multicast addresses to communicate with each other

- 224.0.0.5 to send information to all OSPF routers
- 224.0.0.6 to send information to designated or backup designated routers
- Will use unicasts if the network does not permit multicasting

Open Shortest Path First (OSPF) (cont'd)

Every router builds its own topology table (routing database) of the entire area

- The best route from the topology table goes into the route table
- If the router learns that a particular link has gone down, it consults its own database for the next best route
- If links do not change state, simple keepalives with route summaries are sent to neighbors to minimize traffic

Requires more RAM and processing power on a router to calculate and maintain the routing database

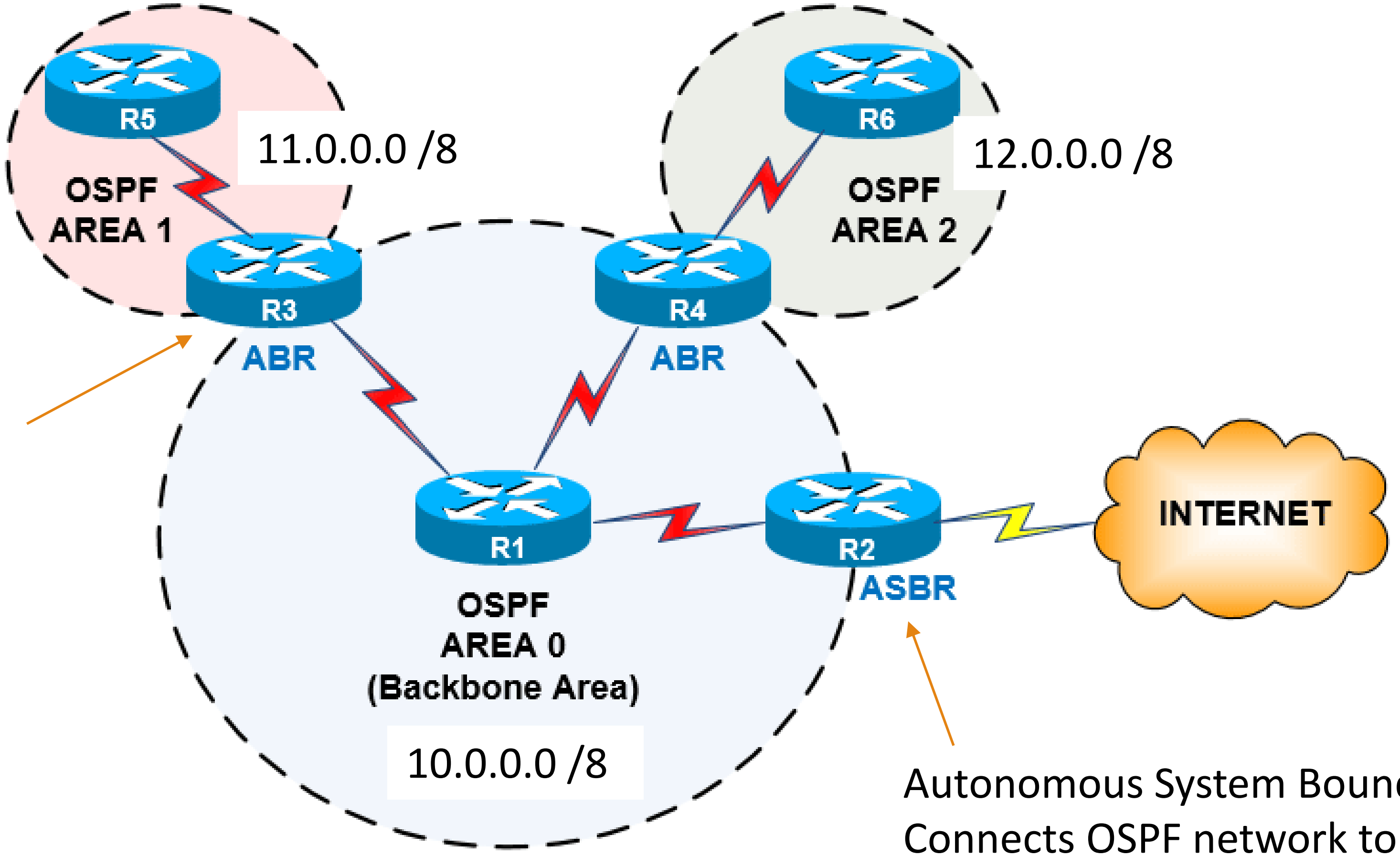
Router convergence is very fast

- Routers quickly update each other on the state of their links
- Routers do not update other routers outside their own area

An Autonomous System Boundary Router (ASBR) connects the OSPF backbone to the outside world

Note: OSPFv3 is used for IPv6

OSPF Example

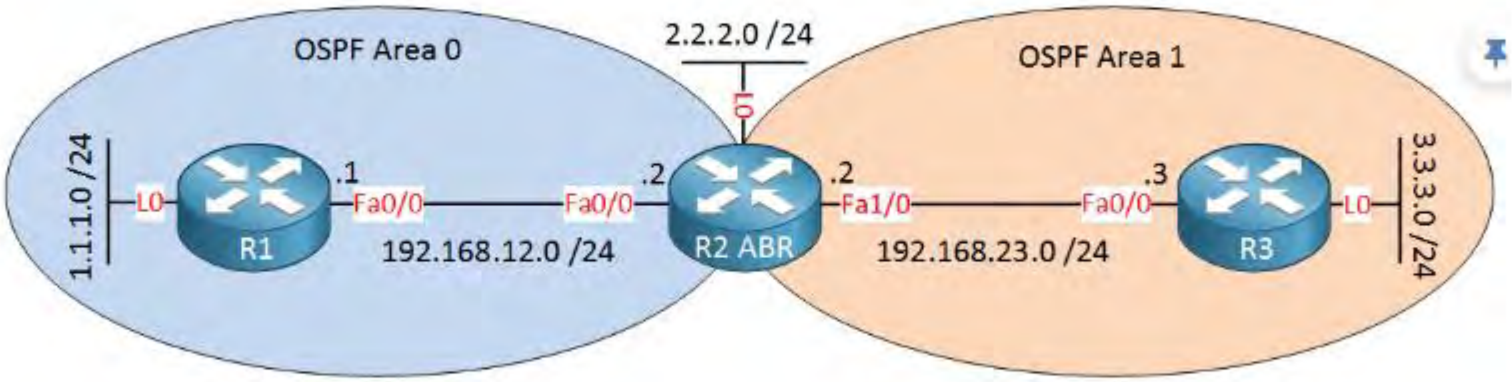


Area Border Router
Connects an area
to the backbone

Autonomous System Boundary Router
Connects OSPF network to outside world

Configuring OSPF Example

in general




```
R1(config)#router ospf 1
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 1.1.1.0 0.0.0.255 area 0

R2(config)#router ospf 1
R2(config-router)#network 192.168.12.0 0.0.0.255 area 0
R2(config-router)#network 192.168.23.0 0.0.0.255 area 1

R3(config)#router ospf 1
R3(config-router)#network 192.168.23.0 0.0.0.255 area 1
R3(config-router)#network 3.3.3.0 0.0.0.255 area 1
```

EIGRP

Enhanced Interior Gateway Protocol (EIGRP)

A hybrid interior gateway protocol

- Layer 3 protocol ID 88
- Direct payload of IP
- Uses multicast address 224.0.0.10 to communicate

Originally Cisco proprietary

- Now an open standard

Actual route updates are sent only as needed

- Hello keepalives maintain router neighbor relationships between route updates
- Uses few network (bandwidth) resources

Uses 5 “K” constants to determine the metric:

- Bandwidth, delay, load, reliability, MTU
- Default is bandwidth + delay

Enhanced Interior Gateway Protocol (EIGRP) (cont'd)

Works well with VLSM
- Can be used to automatically summarize routes

Selects the route with the lowest cumulative metric
- Can load balance traffic across unequal paths
- Uses the DUAL algorithm to ensure there are no routing loops

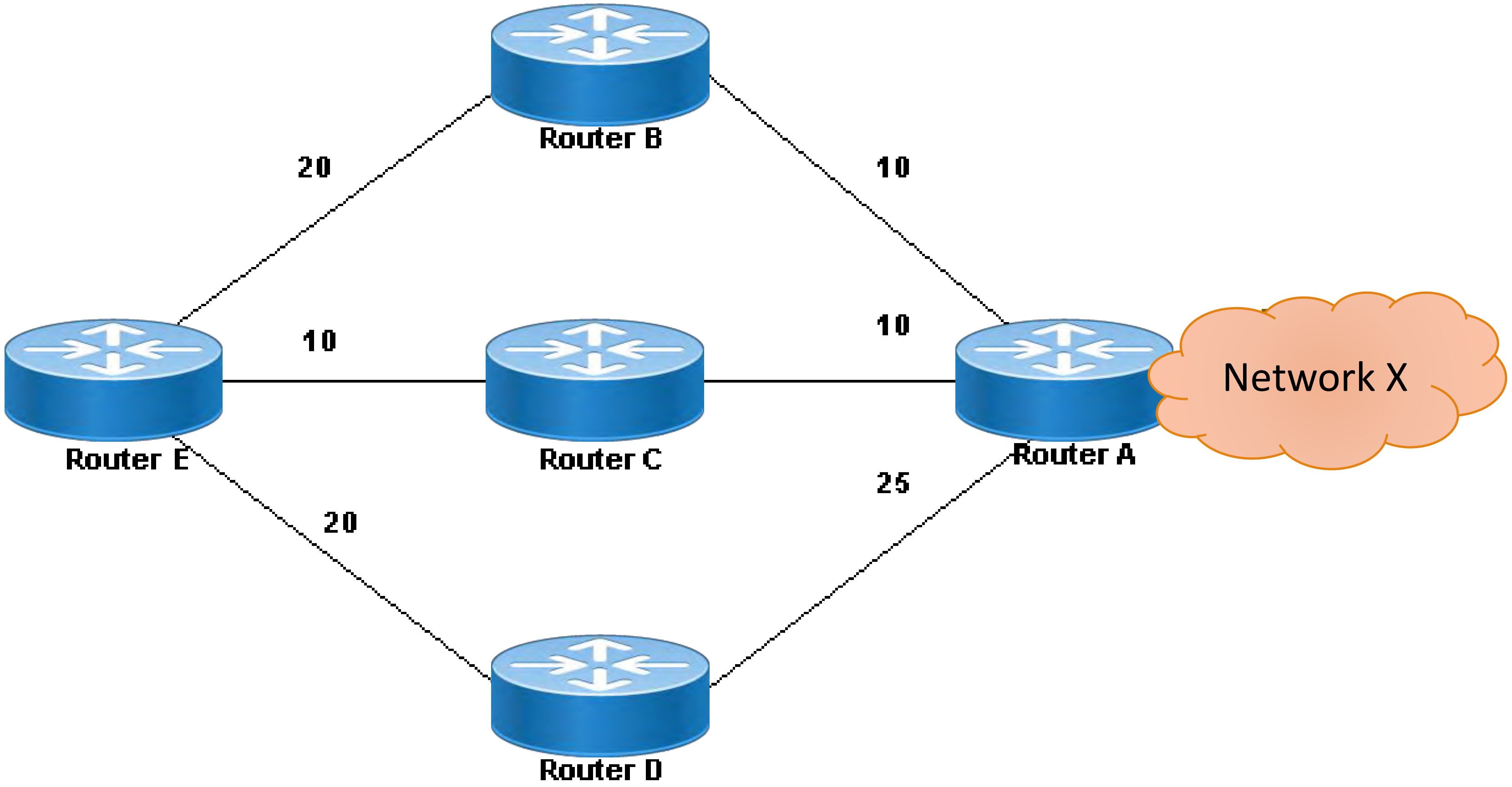
Router convergence is very fast (seconds)

Generally the preferred interior routing protocol
- Works very well in any interior network
- Even if the network is disorganized and poorly designed

Network boundaries are defined by the Autonomous System (AS) number the routers belong to
- An AS is a network that falls under a single administrative umbrella

Note: EIGRP can be configured for either IPv4 or IPv6

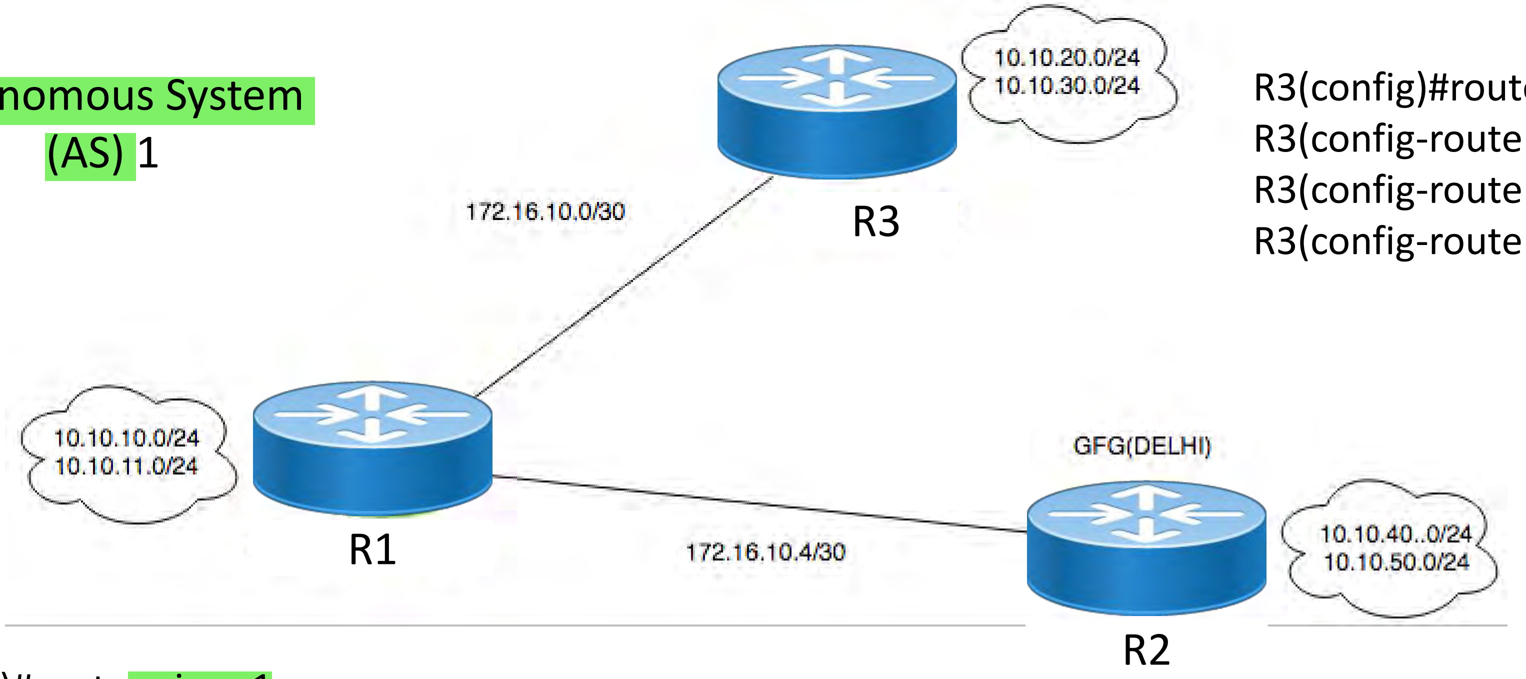
EIGRP Example



Router E sends traffic through Router C to reach Network X

Configuring EIGRP Example

Autonomous System (AS) 1



R3(config)#router eigrp 1
R3(config-router)#network 172.16.10.0
R3(config-router)#network 10.10.20.0
R3(config-router)#network 10.10.30.0

R1(config)#router eigrp 1
R1(config-router)#network 10.10.10.0
R1(config-router)#network 10.10.11.0
R1(config-router)#network 172.16.10.0
R1(config-router)#network 172.16.10.4

R2(config)#router eigrp 1
R2(config-router)#network 172.16.10.4
R2(config-router)#network 10.10.50.0
R2(config-router)#network 10.10.40.0

BGP

Border Gateway Protocol (BGP)

THE exterior gateway protocol (the only one used on the Internet)

A Path Vector protocol

- Used for routing between autonomous systems
- Views an entire autonomous system as a hop
- Unicast on TCP 179

BGP is always used between ISPs

- BGP peers (neighbor routers) are manually configured
- Does not have a concept of border routers

Most ISPs also use an interior version of BGP within their own network

Large corporations/private organizations will use an interior gateway protocol such as OSPF or EIGRP within its AS

Note: BGP can be configured for either IPv4 or IPv6

Border Gateway Protocol (BGP) (cont’d)

Most complex of all the routing protocols to implement

- Uses a number of criteria for best path selection
  - “Weight” of an interface
  - Administrator-configured “local preference”
  - Source of a path
  - Path length
  - Preferred path
  - Preferred AS entry point
  - Router ID
- If used incorrectly, a private organization could accidentally become a public “transit network” between two ISPs!

Very slow convergence by default

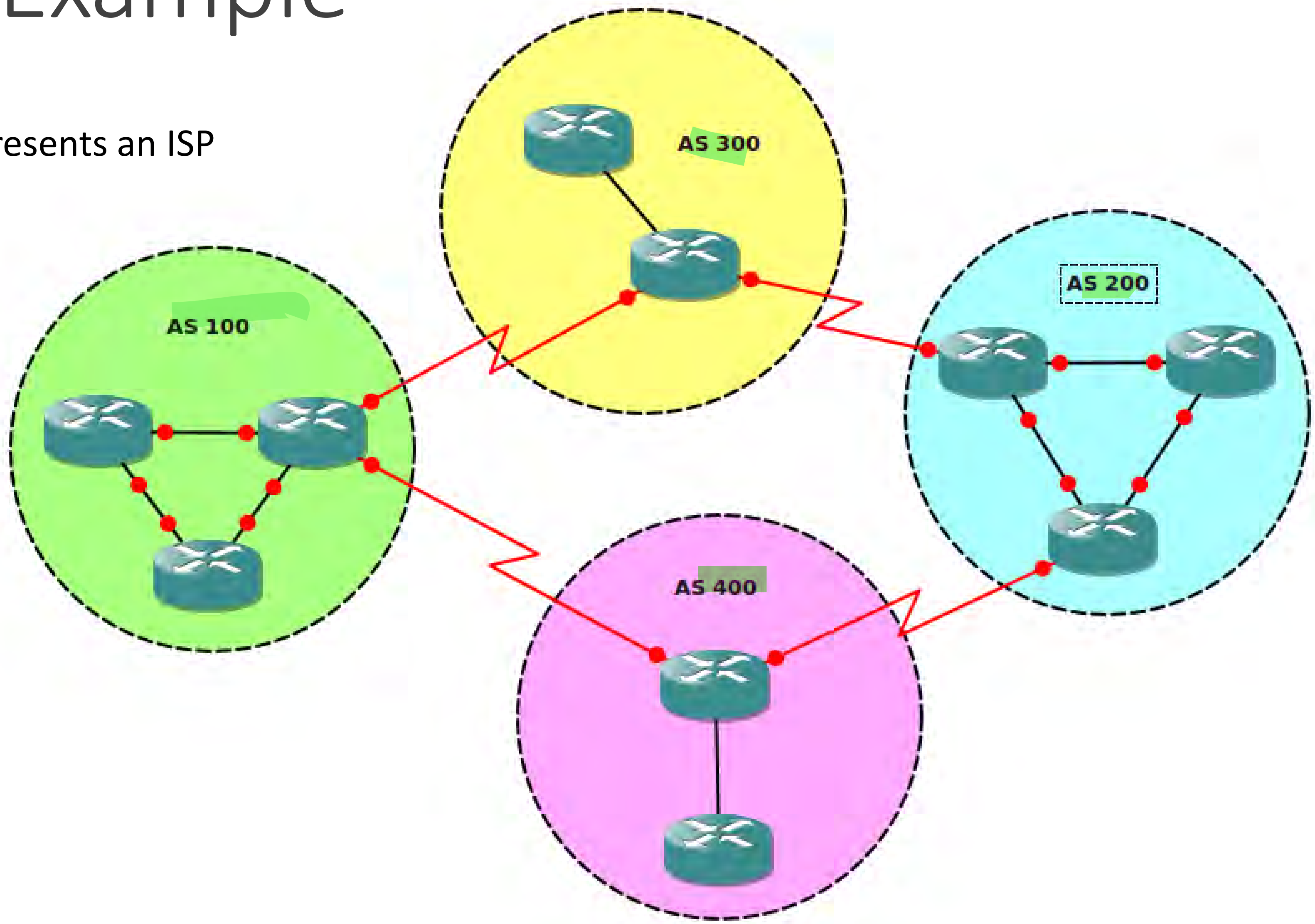
- Time can be dramatically improved with careful tuning

The focus of BGP design and implementation is on security and scalability

Note: BGP can be configured for either IPv4 or IPv6

BGP Example

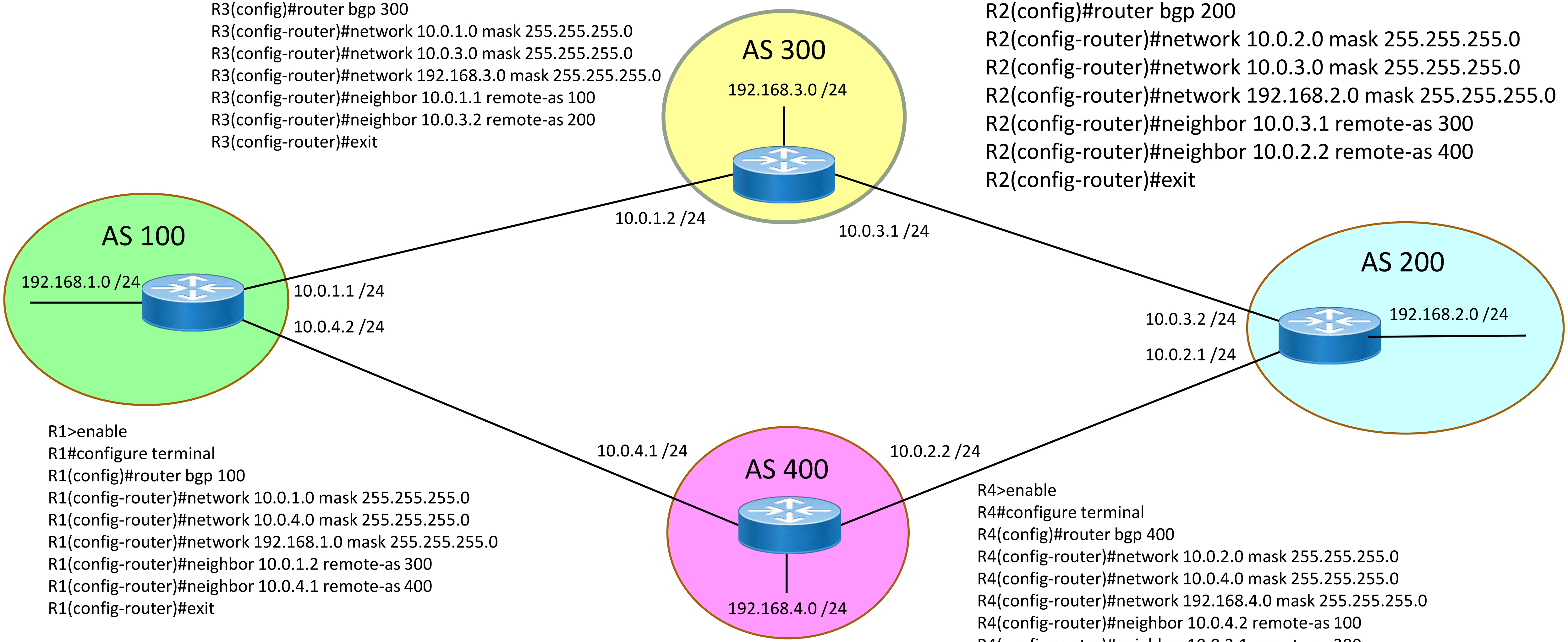
Each AS represents an ISP



Configuring BGP Example

```
R3>enable
R3#configure terminal
R3(config)#router bgp 300
R3(config-router)#network 10.0.1.0 mask 255.255.255.0
R3(config-router)#network 10.0.3.0 mask 255.255.255.0
R3(config-router)#network 192.168.3.0 mask 255.255.255.0
R3(config-router)#neighbor 10.0.1.1 remote-as 100
R3(config-router)#neighbor 10.0.3.2 remote-as 200
R3(config-router)#exit
```

```
R2>enable
R2#configure terminal
R2(config)#router bgp 200
R2(config-router)#network 10.0.2.0 mask 255.255.255.0
R2(config-router)#network 10.0.3.0 mask 255.255.255.0
R2(config-router)#network 192.168.2.0 mask 255.255.255.0
R2(config-router)#neighbor 10.0.3.1 remote-as 300
R2(config-router)#neighbor 10.0.2.2 remote-as 400
R2(config-router)#exit
```




```
R1>enable
R1#configure terminal
R1(config)#router bgp 100
R1(config-router)#network 10.0.1.0 mask 255.255.255.0
R1(config-router)#network 10.0.4.0 mask 255.255.255.0
R1(config-router)#network 192.168.1.0 mask 255.255.255.0
R1(config-router)#neighbor 10.0.1.2 remote-as 300
R1(config-router)#neighbor 10.0.4.1 remote-as 400
R1(config-router)#exit
```

```
R4>enable
R4#configure terminal
R4(config)#router bgp 400
R4(config-router)#network 10.0.2.0 mask 255.255.255.0
R4(config-router)#network 10.0.4.0 mask 255.255.255.0
R4(config-router)#network 192.168.4.0 mask 255.255.255.0
R4(config-router)#neighbor 10.0.4.2 remote-as 100
R4(config-router)#neighbor 10.0.2.1 remote-as 200
```

NAT / PAT

Network Address Translation (NAT)

Can be used by routers and firewalls

A router dynamically translates "inside" addresses to "outside" addresses as it forwards traffic out to remote destinations

- The "inside" is typically the internal network with private IP addresses
- The "outside" is typically the Internet with public IP addresses

The router changes the source IP address to an address suitable for the outside

- To the outside world, it seems as if many connections are being initiated from the router's public interface
- Remote hosts are not aware that the router is relaying traffic back to internal hosts
- NAT mappings are stored for a limited time in the router's NAT table (in memory)

Note: NAT can be used to translate IPv4 → IPv4, IPv6 → IPv4, IPv6 → IPv6

Network Address Translation (NAT) (cont’d)

As replies are returned, the router translates the address back to the original address

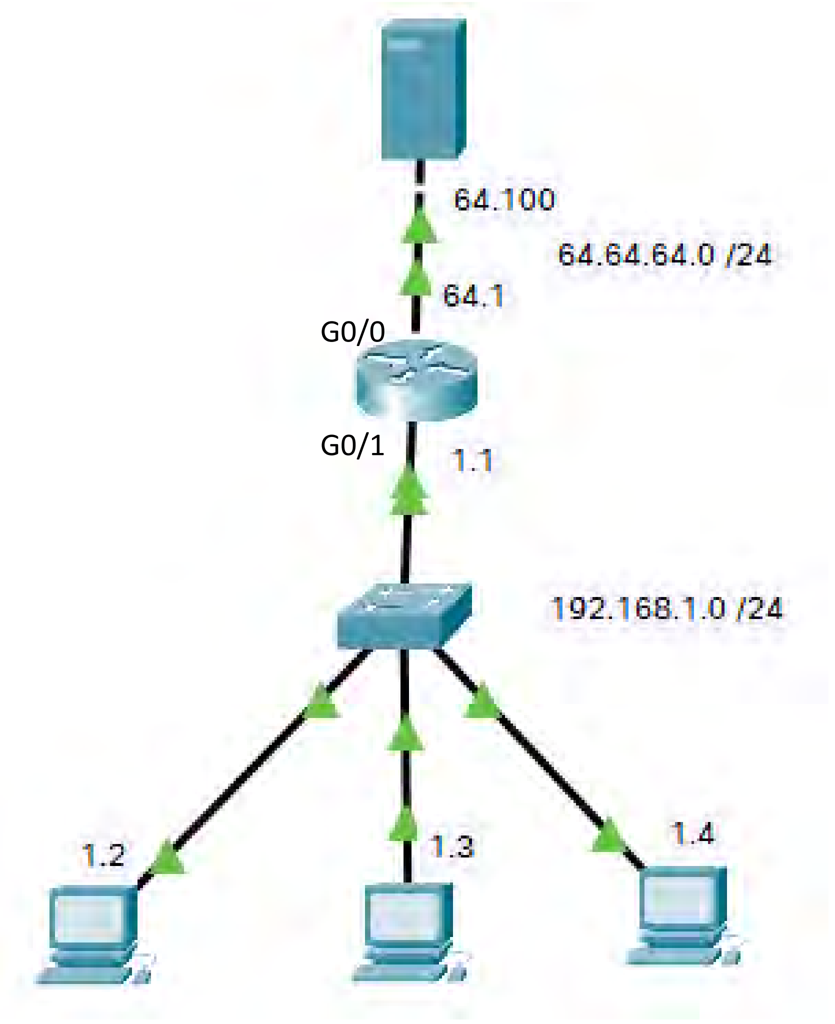
- Typically, only source IP addresses are changed

NAT requires a separate public IP address for every internal address that is translated

- A router can be configured with a pool of public addresses for NAT
- If the organization wishes to make an internal host available to the public, it can dedicate a public IP address to it, statically mapping the public IP to that particular internal host
  - This is known as “publishing” the internal host

Note: NAT can also be configured to translate destination IP addresses

Configuring NAT on a Cisco Router Example




```
Router> enable
Router# configure terminal
```

2

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 64.64.64.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

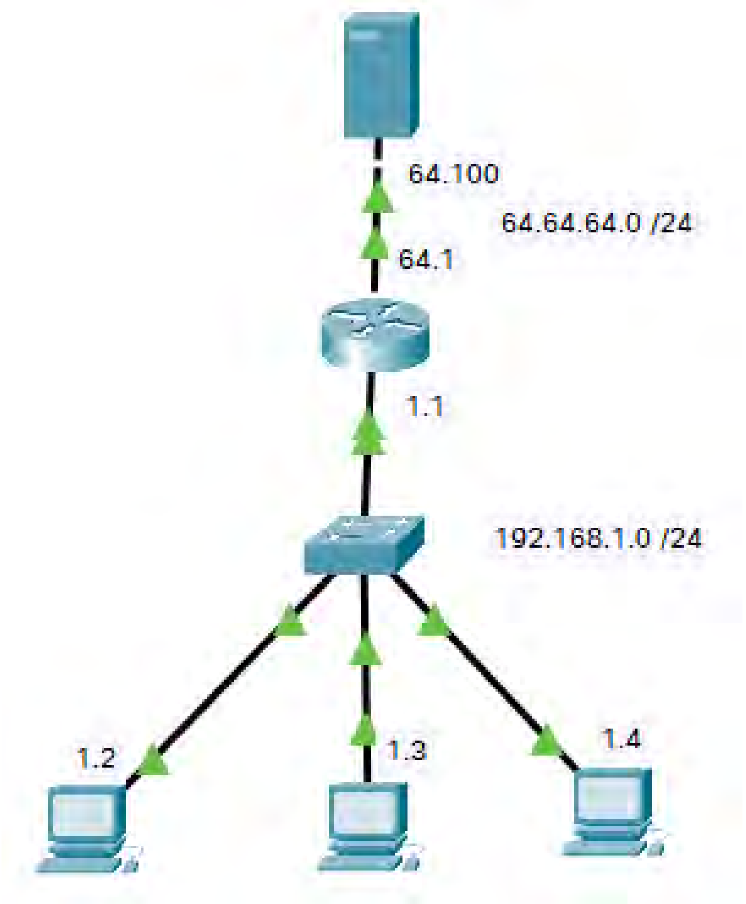
3

```
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

4

```
Router(config)# ip nat pool sales 64.64.64.2 64.64.64.10 netmask 255.255.255.0
Router(config)# access-list 1 permit 192.168.1.0  0.0.0.255
Router(config)# ip nat inside source list 1 pool sales
Router(config)# int g0/0
Router(config-if)# ip nat outside
Router(config-if)# int g0/1
Router(config-if)# ip nat inside
Router(config-if)# end
Router# copy run start
```

NAT Table Example




```
Router#show ip nat translation
Pro  Inside global       Inside local        Outside local       Outside global
tcp 64.64.64.2:1030     192.168.1.2:1030    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.2:1031     192.168.1.2:1031    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.2:1032     192.168.1.2:1032    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.2:1033     192.168.1.2:1033    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.3:1026     192.168.1.3:1026    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.3:1027     192.168.1.3:1027    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.3:1028     192.168.1.3:1028    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.4:1026     192.168.1.4:1026    64.64.64.100:80     64.64.64.100:80
tcp 64.64.64.4:1027     192.168.1.4:1027    64.64.64.100:80     64.64.64.100:80
```

Port Address Translation (PAT)

Used if a router has more internal clients than public IP addresses available for NAT

- The most common implementation is when the organization has only one public IP address

Internal clients share the public IP address(s)

The router keeps internal clients separate by including their TCP or UDP source port as part of the mapping

The router attempts to leave the source port at the original number

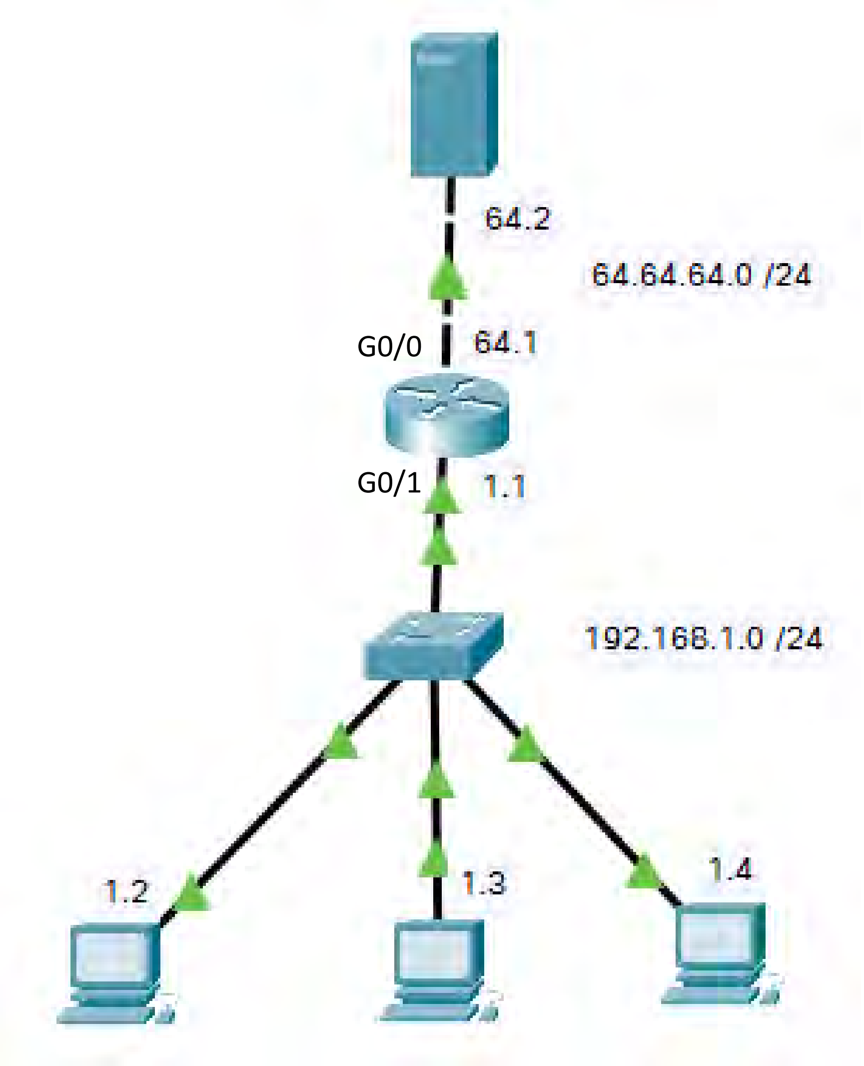
It will change the source port if another client is already using that port

As replies from external hosts come back to the router, the router translates the IP address (and port if necessary) back to the original

Destination addresses and ports are typically not modified

Note: The router can also be configured to first use a pool of public IP addresses
If the router has only one public IP address left, it will then begin to PAT

Configuring PAT on a Cisco Router



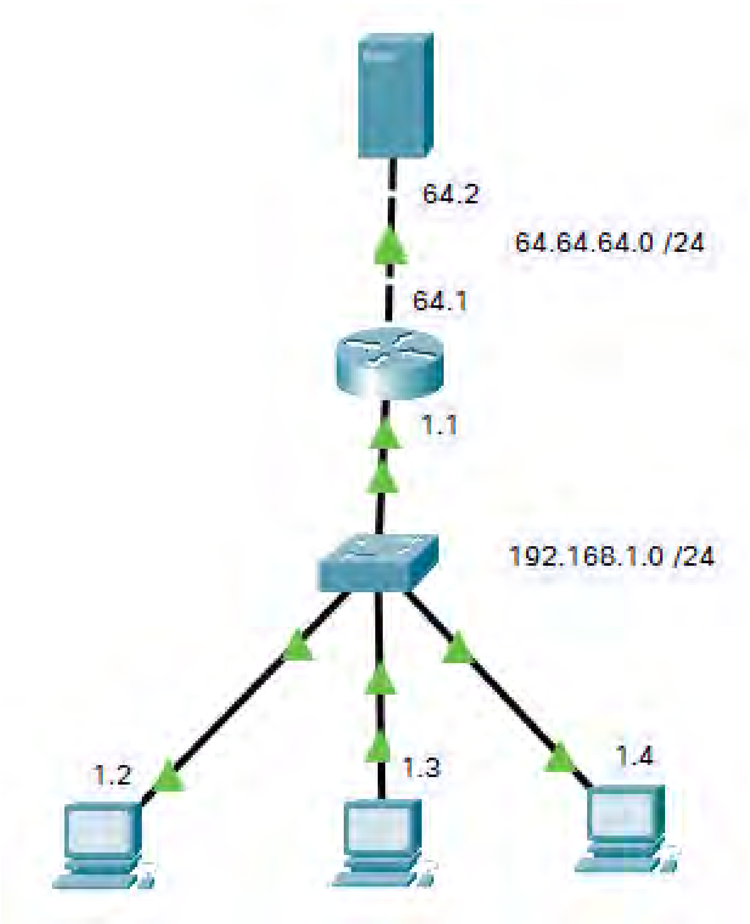

```
Router> enable
Router# configure terminal

Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 64.64.64.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 int g0/0 overload
Router(config)# end
Router# copy run start
```

PAT Table Example




```
Router#show ip nat translation
Pro  Inside global       Inside local        Outside local       Outside global
tcp 64.64.64.1:1024     192.168.1.3:1025    64.64.64.2:80       64.64.64.2:80
tcp 64.64.64.1:1025     192.168.1.2:1025    64.64.64.2:80       64.64.64.2:80
tcp 64.64.64.1:1026     192.168.1.4:1025    64.64.64.2:80       64.64.64.2:80
```

Bandwidth Management

Traffic Shaping

Also known as:

- Packet shaping
- Quality of Service (QoS)
- Bandwidth management

The manipulation and prioritization of network traffic

Reduces network congestion for applications that need high or realtime priority:

- Voice
- Video
- Teleconferencing
- Telemedicine
- Network management

Used to optimize or guarantee performance, improve latency, or increase usable bandwidth

Quality of Service (QoS)

Aka traffic shaping

Helps manage packet loss, delay and jitter on your network infrastructure

Also an important factor in supporting the growing Internet of Things (IoT)

Applied to applications that benefit from managing packet loss, delay and jitter

- Voice
- Video

To be meaningful, must be supported by every device (switch, router) along the packet's path

- Impossible to enforce on the Internet

Differentiated Services Code Point (Diffserv)

A way to identify and mark traffic priority level

- Allows higher priority traffic to receive preferential treatment

Also known as DSCP

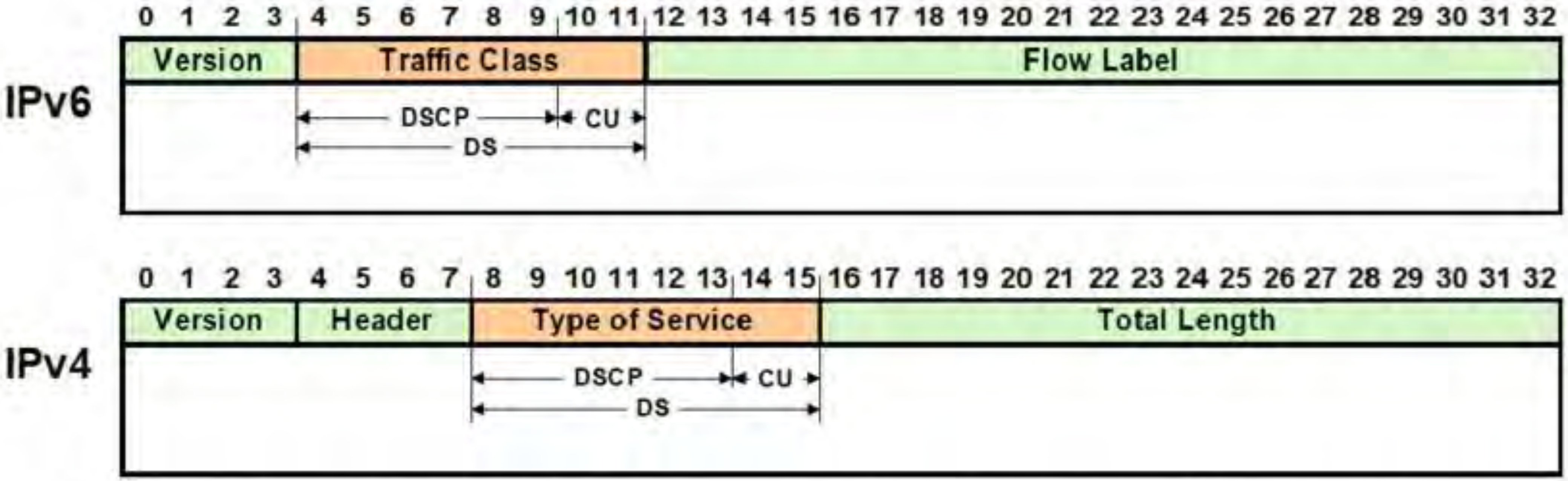
Marking placed in Layer 3 packet header

- Various applications can be marked differently
- Range of 0 (lowest) to 63 (highest) priority

Enforced by routers

- Packets with different priorities are placed in different outbound queues

DSCP in the IP Header

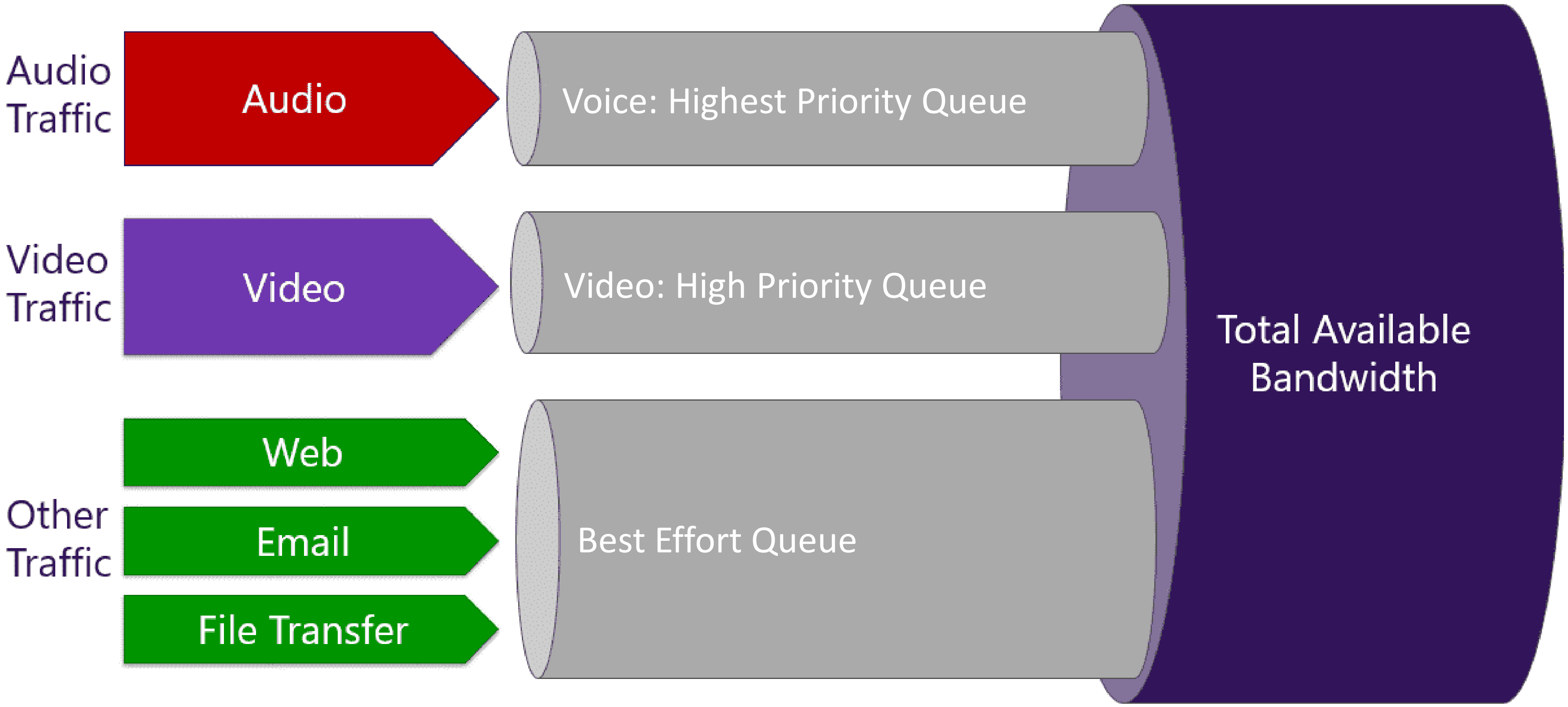


DS – *Differentiated Service* , **DSCP** – *Differentiated Service Code Point*, **CU** – *Currently Unused*

Cisco Baseline DSCP Recommended Values

Application	DSCP Value	Description
Routing	48	Network control
Voice	46	VoIP telephony
Interactive video	34	Multimedia conferencing
Streaming video	32	Multimedia streaming
Mission critical data	26	Defined by organization
Call signaling	24	SIP, H.323
Transactional data	18	Low-latency data
Network management	16	Operations/administration
Bulk data	10	High-throughput data
Scavenger	8	Low priority data
Best effort	0	whatever

DSCP Example Queues on a Router



Class of Service (CoS)

A Layer 2 QoS mechanism

- Enforced by switches
- 802.1p

3 bit field in an Ethernet header

- Exists inside a VLAN tag (802.1q)

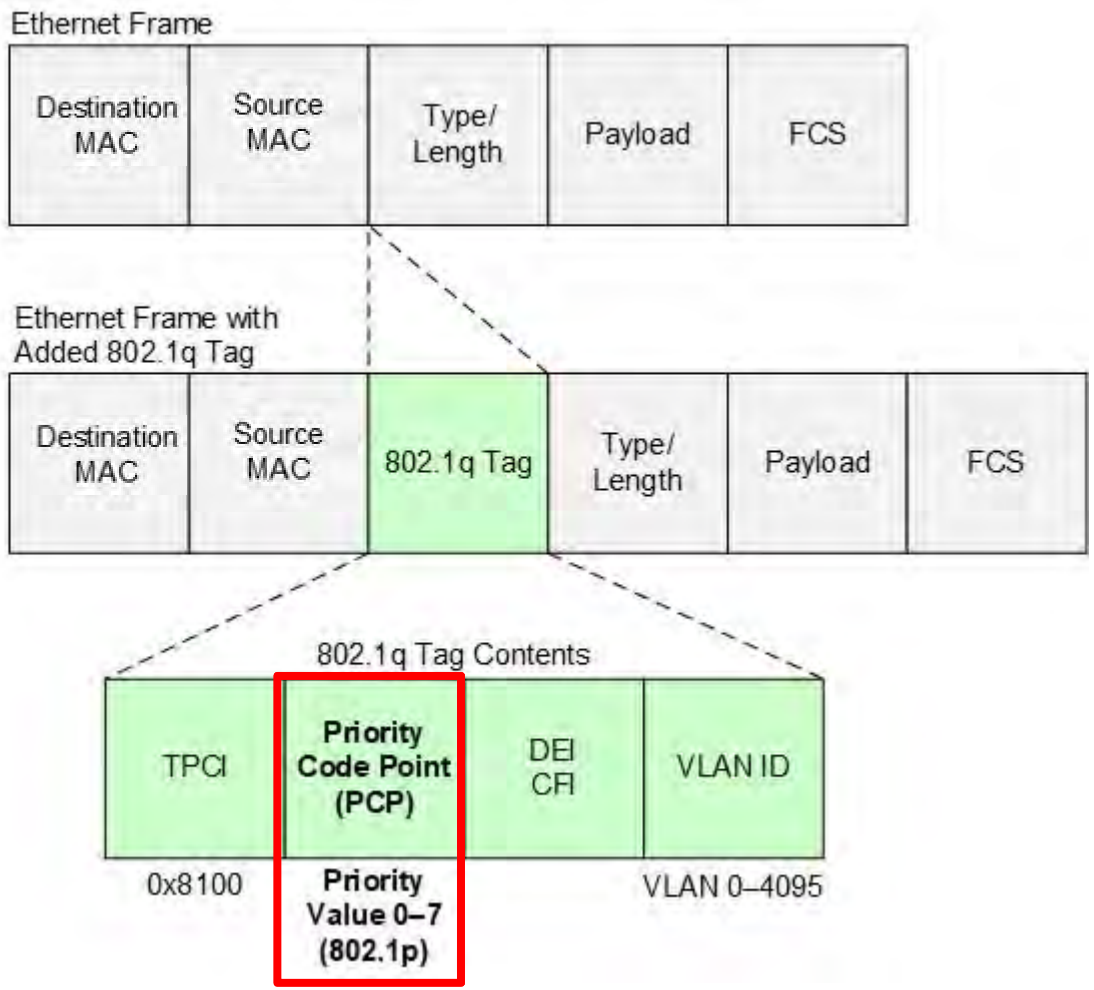
Priority of 0 (lowest) through 7 (highest)

Different applications can be marked differently

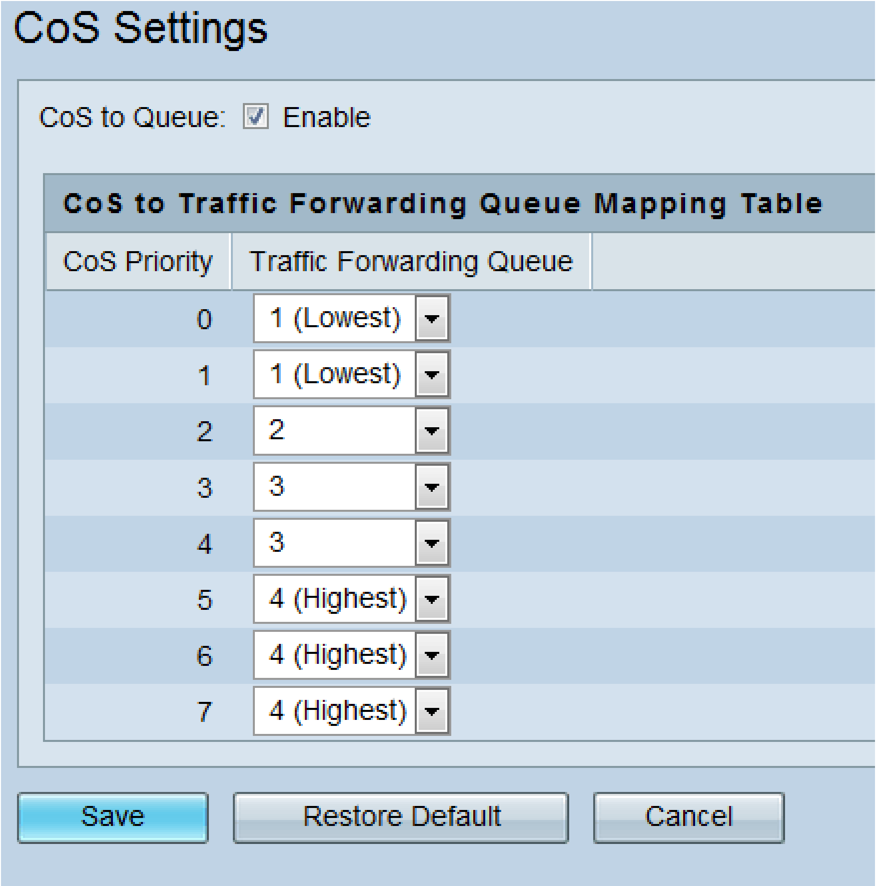
- Client or server operating system performs the marking

Class	Description
7	Network Control
6	Internetwork Control
5	Voice
4	Video
3	Critical Applications / Call signaling (SIP, H.323)
2	High priority
1	Medium priority
0	Routine / Best Effort

Class of Service Field in Ethernet Header



Configuring Class of Service Example



Class of Service Traffic Forwarding Queues

1 (Lowest) — Packet gets the lowest priority
2 — Packet gets a low priority
3 — Packet gets a medium priority
4 (Highest) — Packet gets the highest priority