Routing

CCNA 200-301 V1.1

MODULE 5

Topics

5.1 Introducing the Router

5.2 Routing Basics

5.3 Packet Delivery on the Same Network

5.4 IP Routing Across a Single Router

5.5 IP Routing Across Multiple Routers

5.6 Routing Protocols Overview

5.7 Route Selection

5.8 Open Shortest Path First (OSPF)

5.9 First Hop Redundancy Protocol (FHRP)

5.10 Network Address Translation (NAT)

5.11 Review

5.1 Introducing the Router

CCNA 200-301 v1.1

Module 5

What is a Router?

Router Interface Configuration

Basic Router Configuration Commands

Configuring a Point-to-Point Serial Link

Router Serial Link Commands

What is a Router?

A device that makes forwarding decisions based on Layer 3 (IP) addresses

Can be hardware or software based

Can connect many types of network segments and media types

What is a Router? (cont'd)

Builds a route table to determine the best path

The packet can be sent:
- To the next hop along the path
- Out an interface (on a point-to-point WAN link)
  - The next hop is presumed to be on the other end of the WAN link

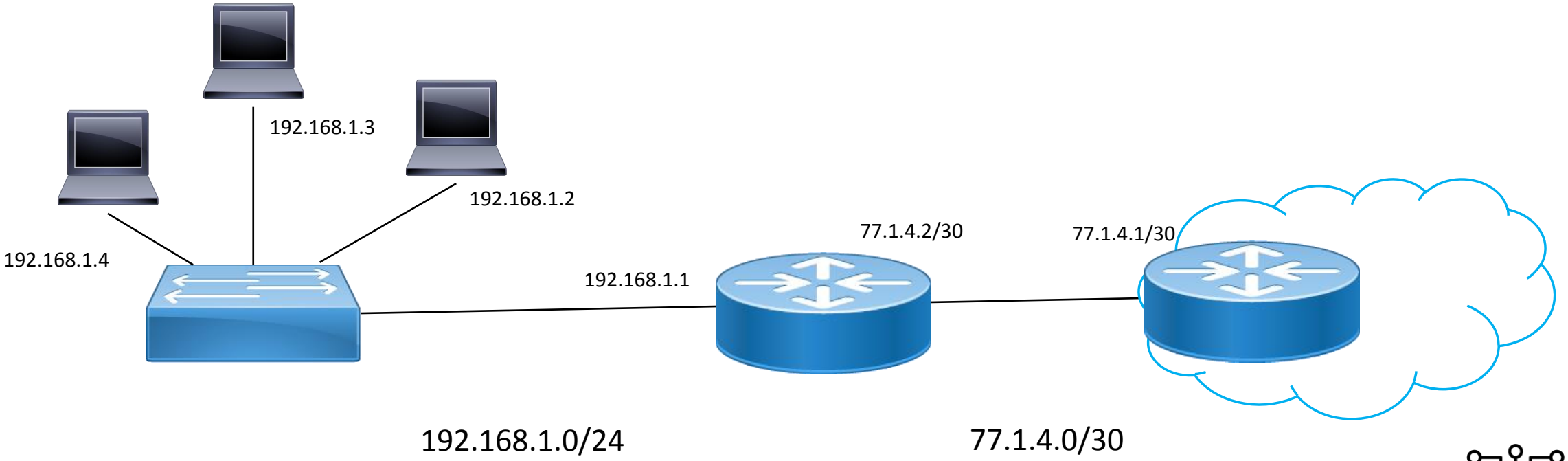
The router will replace or re-write the packet's Layer 2 header

Examples:
- Ethernet → Ethernet
- Ethernet → PPP
- Frame relay → HDLC

The router then switches the packet from one interface to another

The router that connects a network segment to the outside world is called the "default gateway"

Basic Router Implementation Example



Router Interface Configuration

In most cases, you should hard-code the IP address on each router interface

- R1(config-if)# `ip address 192.168.1.1 255.255.255.0`
- R1(config-if)# `no shut`

It is also possible to configure router (and switch) interfaces to be configured via DHCP

- AKA Dynamic IP Address Configuration
- R1(config-if)# `ip address dhcp`
- R1(config-if)# `no shut`

Basic Router Configuration Commands

Command	Description
`enable`	Enter privileged EXEC mode
`configure terminal`	Enter global configuration mode
`hostname <name>` `hostname Router1`	Give the router a name
`enable secret <password>` `enable secret letmein`	Set a password on the enable command
`interface <type><#>` `interface g0/1`	Enter interface configuration mode

Basic Router Configuration Commands (cont'd)

Command	Description

`[no] ip address <address> <subnet mask>`
`ip address 10.1.1.1 255.255.255.0`
`no ip address 10.1.1.1 255.255.255.0`
	Give an interface an IP address
	Remove the current IP address

`ip address dhcp`	Set the interface to obtain an IP address from DHCP
`no shut`	Turn on the interface
`end`	Jump to the top of privileged EXEC
`copy running-config startup-config`	Save the running configuration

Configuring a Point-to-Point Serial Link

Add a serial interface to both routers

Connect a serial link between the two

Set one side to be the clock master (DCE)

Set the other side to be the clock slave (DTE)

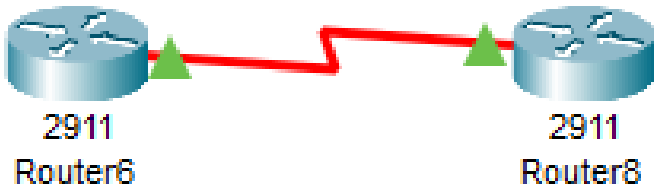
In packet tracer, you can select a DCE serial cable

- The first side you connect it to will automatically be the DCE
- The other side will automatically be the DTE
- The default link speed will be 2 mb/s
- The default Layer 2 protocol (encapsulation type) will be HDLC

Configure both sides with suitable IP addresses

- IPv4 prefer to use a /30 mask

No shut both interfaces and save router configurations



Router Serial Link Commands

Command	Description

`interface s0/3/0`
`encapsulation <hdlc | ppp>`
`ip address 172.16.0.1 255.255.255.252`
`clock rate <choose from list>`
`no shut`
	• Example of configuring a serial point-to-point link
	• Default encapsulation is Cisco HDLC, choose PPP for vendor-neutral implementations
	• On DCE only: if desired, change the link speed from default 2,000,000 bps (range 300 – 4,000,000 bps)

`show controller <controller number>` `show controller s0/3/0`	• Shows if you are DCE or DTE on that link • Controller number = interface number
`show interfaces <interface number>` `show interfaces s0/3/0`	Shows usual interface information including Layer 2 encapsulation protocol
`show ip interfaces brief`	Display a list of all interfaces, their IP address, and their up/down status

5.2 Routing Basics

CCNA 200-301 v1.1

Module 5

What is Routing?

Static Routing

Floating Static Route

Host Route

Default Route

VLAN Routing

The Golden Rule of Routing

The 2nd Golden Rule of Routing

Static Route Commands

Router Show Commands

Debugging

Debug Commands

What is Routing?

The movement of packets from one network to the next
- Performed by routers
- Routers read the Layer 3 header destination address
- The router consults its routing table 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 Route Configuration

IPv4 static route example:

R1(config)# ip route <destination network> <destination subnet mask> <next hop> [metric]

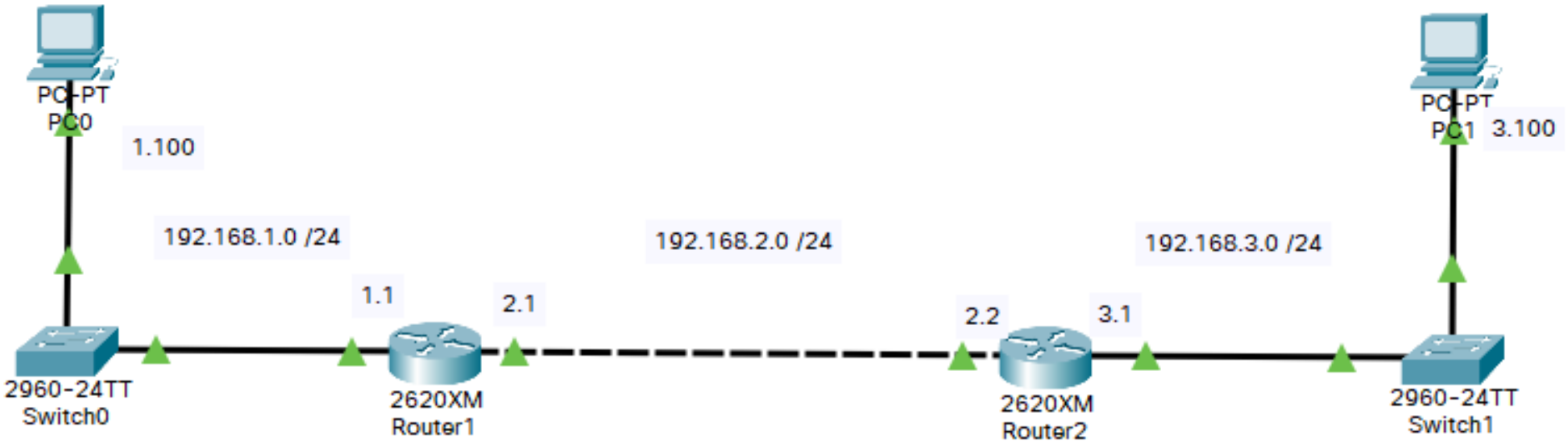
R1(config)# ip route 172.16.3.0 255.255.255.0 192.168.2.254

IPv6 static route example:

R1(config)# ipv6 route <destination_ipv6_prefix> <prefix_length> <next_hop_ipv6_address> [metric]

R1(config)# ipv6 route 2001:0db8:85a3::/64 2001:abcd::1234:8a2e:0370:7334

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
```

Floating Static Route

A type of static route that acts as a backup route

Often used for dial-up interfaces

Only takes effect if the primary route fails

You must assign it a higher administrative distance than the primary route

Example - Use this route in case all OSPF (AD 110) routes fail:

Router(config)# ip route 10.0.0.0 255.255.255.0 192.168.1.1 200

Router(config)# ipv6 route 2001:0db8:abcd::/64 2001:1234::aaaa:bbff:febb:cccc 200

Set the metric to be a higher AD than any of the routing protocols in use

Host Route

A specific type of route that directs traffic to a single host, rather than to an entire network

IPv4 has a subnet mask of /32 (255.255.255.255)

- A /32 mask ensures that only traffic destined for that specific IP will follow this route

IPv6 has a prefix of /128

Useful for directing traffic to a particular host while avoiding other routes

Example:

R1(config)# ip route 192.168.1.10 255.255.255.255 192.168.2.1

R1(config)# ipv6 route 2001:0db8:85a3::8a2e:0370:7334/128 2001:a:b:c:4:3:2:1

Default Route

AKA gateway of last resort

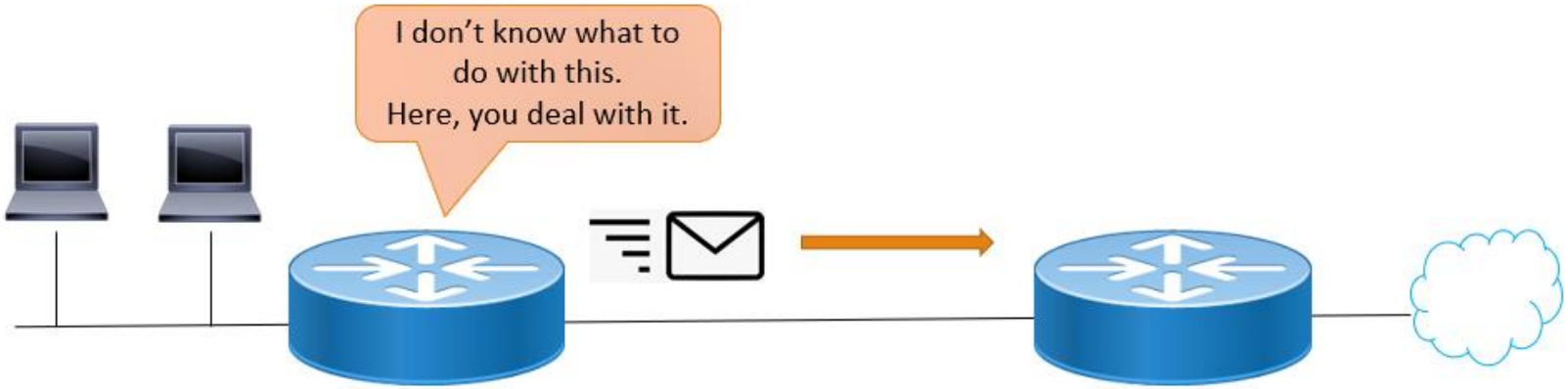
Used when there is:

- No other choice
- Only one possible exit for the traffic to take

A host will specify its local router (default gateway)

A router will specify an upstream router

- On a point-to-point WAN link, the router/route table can just specify the exit interface



Default Route Configuration

IPv4

R1(config)# ip route 0.0.0.0 0.0.0.0 < ip-address | exit-intf >

R1(config)# ip route 0.0.0.0 0.0.0.0 10.108.99.2

R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1

IPv6

R1(config)# ipv6 route ::/0 2001::DB8:2:124:5678

R1(config)# ipv6 route ::/0 Serial2/0

VLAN Routing

Because each VLAN has its own subnet, routers can route between VLANS
- The destination VLAN ID is part of the destination Layer 2 (Ethernet) header

VLAN routing can be accomplished in the following ways:
- The router has physical connections to each VLAN
- The router interface is configured as a trunk port, divided into sub-interfaces (one for each VLAN) – aka Router-on-a-Stick
- The router is actually a software process inside a multilayer switch
  - You need to create a VLAN interface for each VLAN that needs to be routed
  - Each VLAN interface must be configured with an IP address for that VLAN
  - All devices on the VLAN are configured to use that VLAN interface as their default gateway

Once there is a router interface that is responsible for that VLAN, the normal rules of routing (including using routing protocols) apply

Note: VLAN routing is covered in the Switching Module

The Golden Rule of Routing

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 you configure static routing, you must add an appropriate route on every router along the path

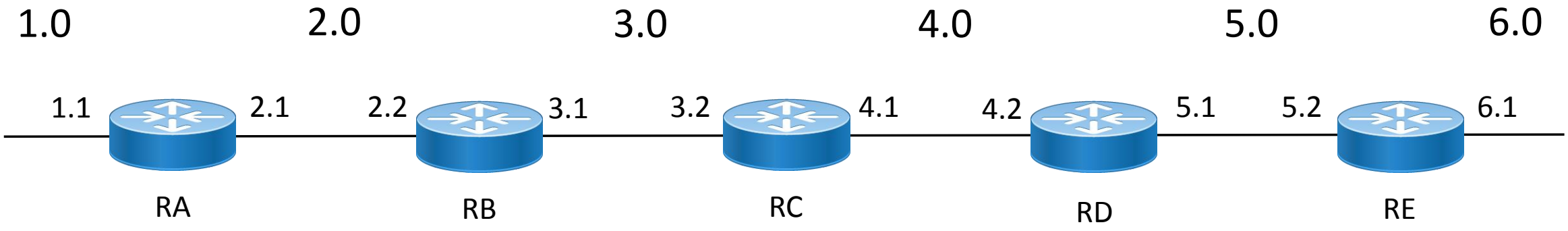
If a router along the path is missing the route (is not “fully converged”) you will have routing black holes

- Packets may disappear and be lost

When the other side replies, that router must also know where to send the reply

The Golden Rule of Routing Example

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



RA	RB	RC	RD	RE
C - 1.0 C – 2.0 Default → 2.2	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	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	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	C – 5.0 C – 6.0 Default → 5.1

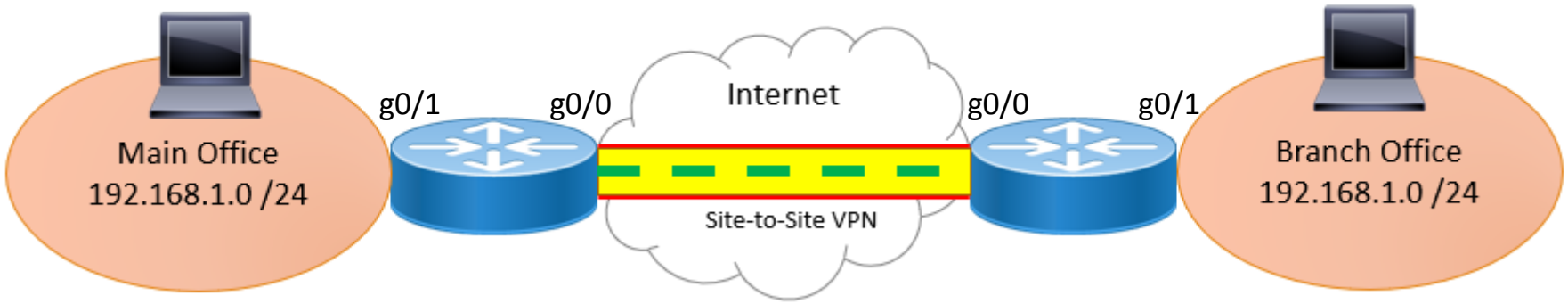
Note: Network IDs in this topology have been simplified for visual convenience

The 2nd Golden Rule of Routing

The router must be able to choose which interface to send the packet out of

Each router interface must belong to a different network

There may be multiple routes to the same destination going out different interfaces



What is wrong with this scenario?

Answer coming soon!

Static Route Commands

Command	Description
`ip route <destination network> <destination subnet mask> <next hop | outbound interface> [metric]`	Add a static route For IPv6 – write mask in CIDR
`ip route 172.16.3.0  255.255.255.0  192.168.2.254`	IPv4 static route example
`ipv6 route 2001:0db8:abcd::/64 2001:0db8:abcd:0000:0000:8a2e:0370:7334`	IPv6 static route example Notice the subnet mask is in CIDR notation

`ip route 172.16.3.0  255.255.255.0  192.168.2.254 200`
 	
`ipv6 route 2001:0db8:abcd::/64 2001:0db8:abcd::8a2e:0370:7334 200`
	IPv4 and IPv6 floating static route examples
	Metric (200) is set higher than AD of routing protocols

Static Route Commands (cont'd)

Command	Description
`ip route 192.168.1.10 255.255.255.255 192.168.2.1`	IPv4 host route example
`Ipv6 route 2601:140:8500:d3d0::7723/128 2001:0db8:abcd::8a2e:0370:7334`	IPv6 host route example

`ip route 0.0.0.0 0.0.0.0 < ip-address | exit-intf >`
`R1(config)# ip route 0.0.0.0 0.0.0.0 10.108.99.2`
`R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1`
	Add an IPv4 default route
	Default route to next hop
	Default route out serial interface on point-to-point WAN link

`R1(config)# ipv6 route ::/0 2001::DB8:2:124` `R1(config)# ipv6 route ::/0 Serial2/0`	IPv6 default route examples

Router Show Commands

Command	Description
`show ip route`	Display the IPv4 route table
`show ip route ?`	Find subcommands to help focus the route table output to subset of information
`show ipv6 route`	Display IPv6 route table entries
`show ipv6 static`	Display IPv6 static routes
`show ip interfaces brief`	List all interfaces, their status, and IPv4 address
`show ipv6 interfaces brief`	List all interfaces, their status, and IPv6 address
`show running-config`	Display the current running configuration
`show startup-config`	Display the current running configuration
`show version`	Display information about the router including hardware, IOS, and configuration register

Route Verification Commands

Command	Description

`show ip route`
`show ipv6 route`
`show ipv6 static`
	Display the IPv4 route table
	Display the IPv6 route table
	Display IPv6 static routes

`ping <destination IPv4 address>` `ping ipv6 <destination IPv6 address>`	Prove that traffic can find a path to a destination and back
`traceroute ip <IPv4 destination address or hostname>` `Traceroute ip 192.168.7.20`	Identify path to IPv4 destination node
`traceroute ipv6 <IPv6 destination address or hostname>` `Traceroute ipv6 2001::DB8:2:124`	Identify path to IPv6 destination node

Debugging

You can turn on debugging for various router activities

Allows you to watch every step of that particular process as it happens in real time

Performed at top of privileged EXEC

You can have multiple debugging sessions going on at once

Can be resource-intensive for the router

```
Router#debug ip ?
  eigrp     IP-EIGRP information
  icmp      ICMP transactions
  nat       NAT events
  ospf      OSPF information
  packet    Packet information
  rip       RIP protocol transactions
  routing   Routing table events
```

Debug Commands

Command	Description
`debug ip ?`	List debug ip subcommands
`debug ip [eigrp | icmp | nat | ospf | packet | rip | routing ]`	Debug a specific IP activity
`no debug ip [eigrp | icmp | nat | ospf | packet | rip | routing ]`	Stop a running debug session
`no debug all`	Stop all running debug sessions
`undebug all` `u all`	Stop all running debug sessions

5.3 Packet Delivery on the Same Network

CCNA 200-301 v1.1

Module 5

Same network delivery process

Packet Delivery on the Same Network Example

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

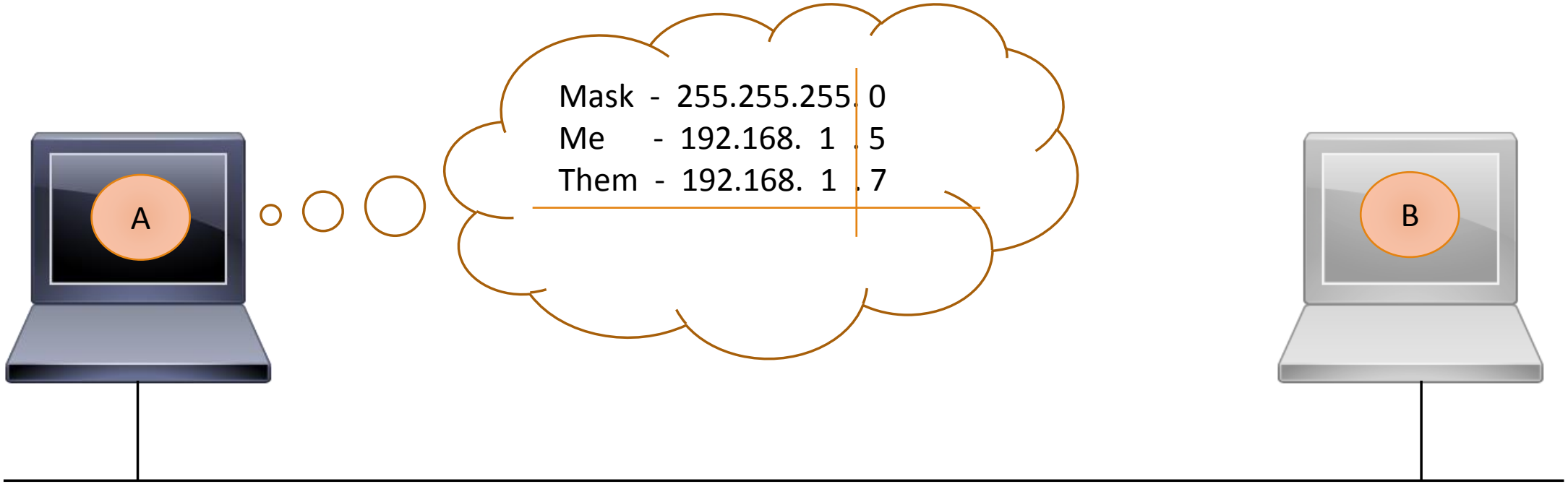
1. A wants to send a packet to B
2. A checks its DNS resolver cache to see if it already knows the IP address for B
3. A determines that it does not know B's IP address
4. A performs a DNS lookup to find B's IP Address
5. A puts the address of B in the IP header destination field
6. A uses its own subnet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

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

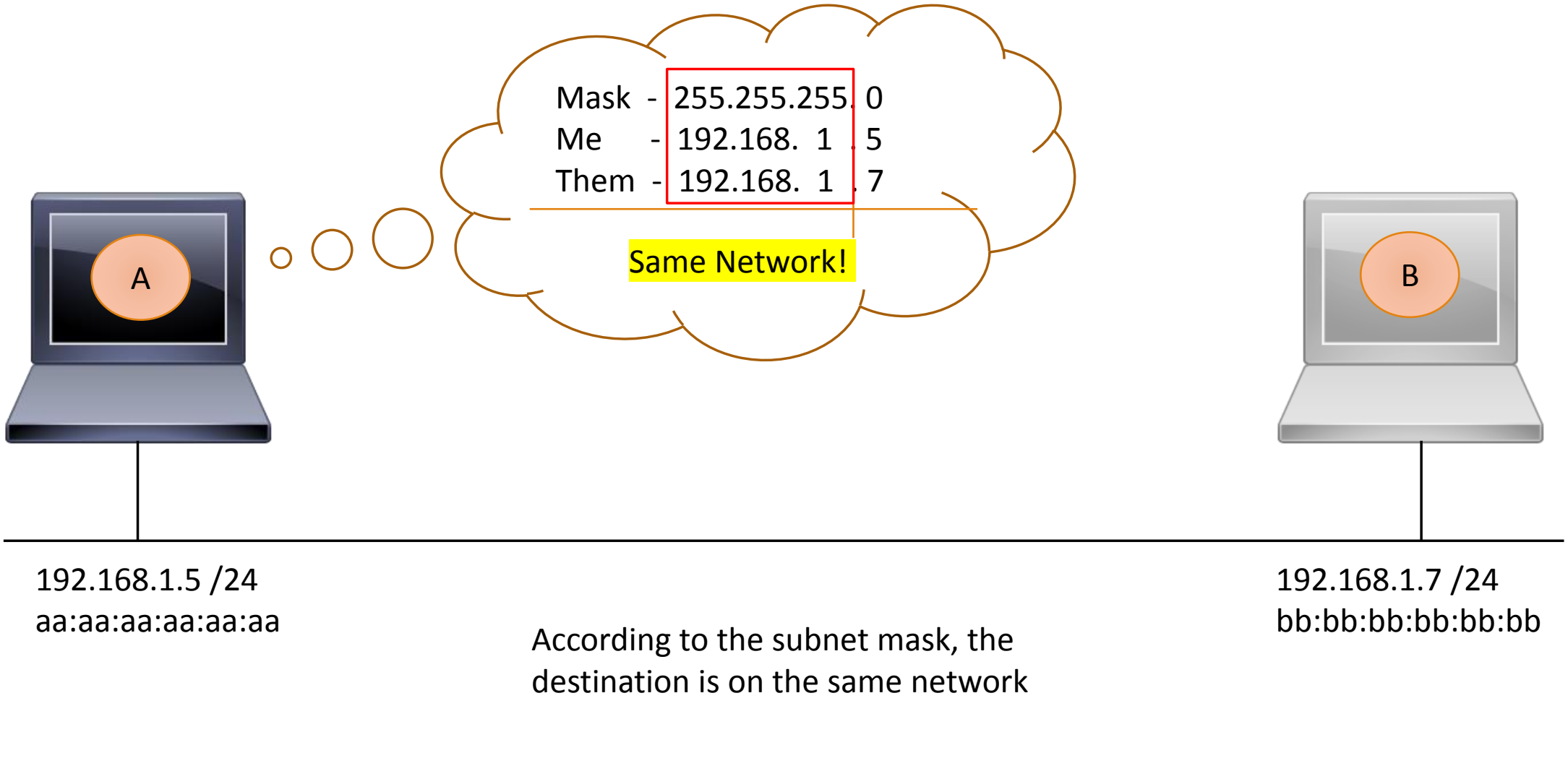


192.168.1.5 /24
aa:aa:aa:aa:aa:aa

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

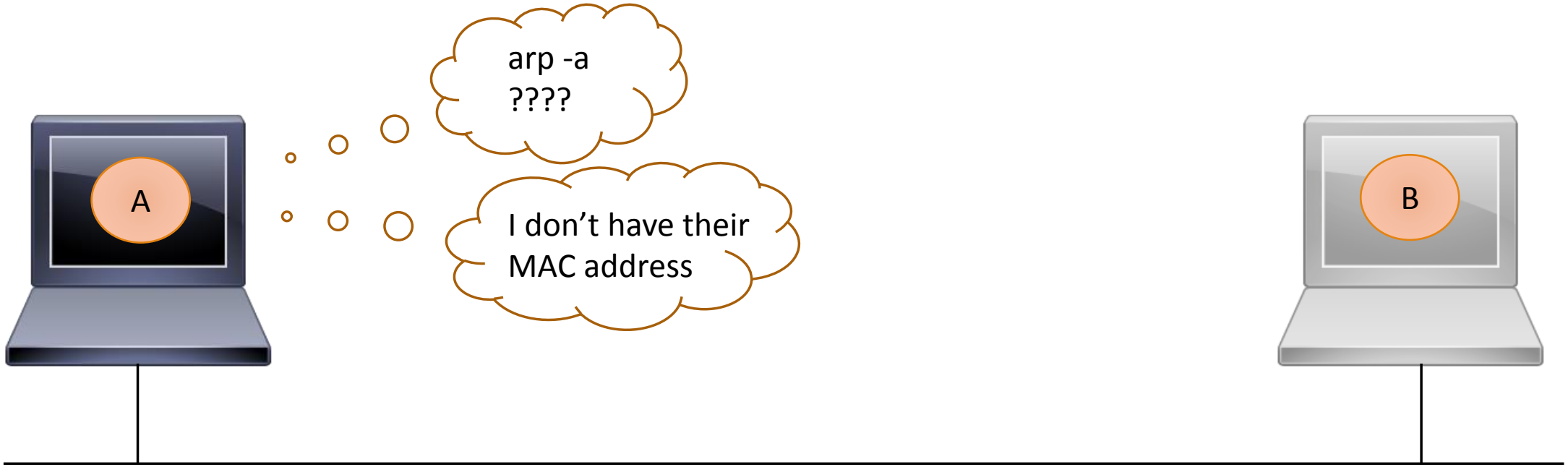
After learning the destination IP address,
A (source) uses its subnet mask to determine if B (destination) is on the same or different network

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



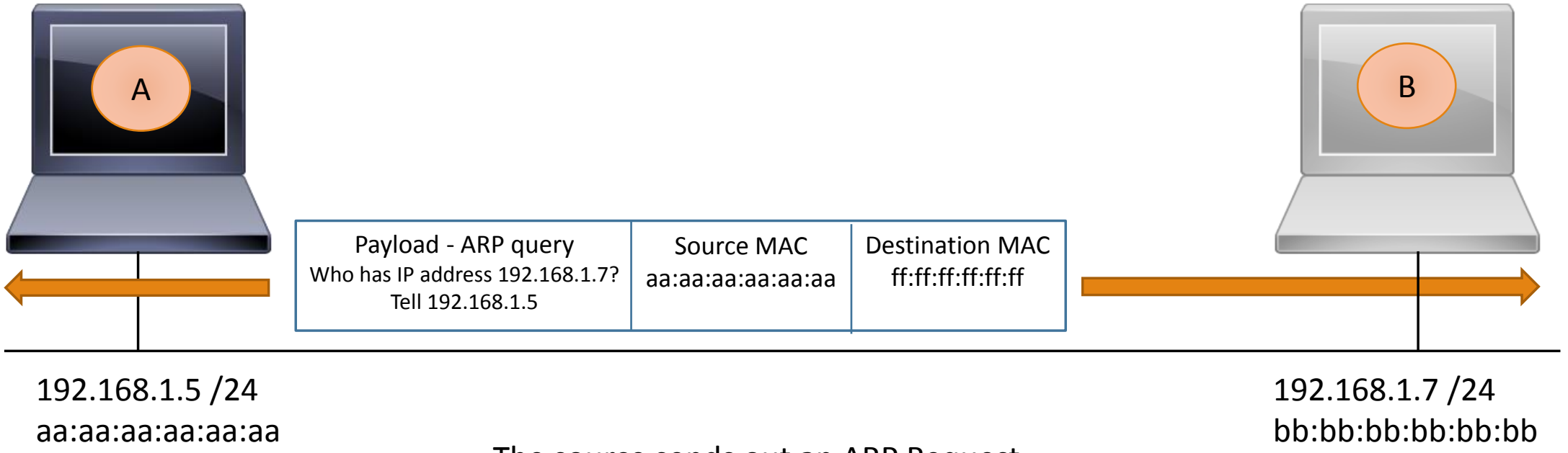
According to the subnet mask, the destination is on the same network

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



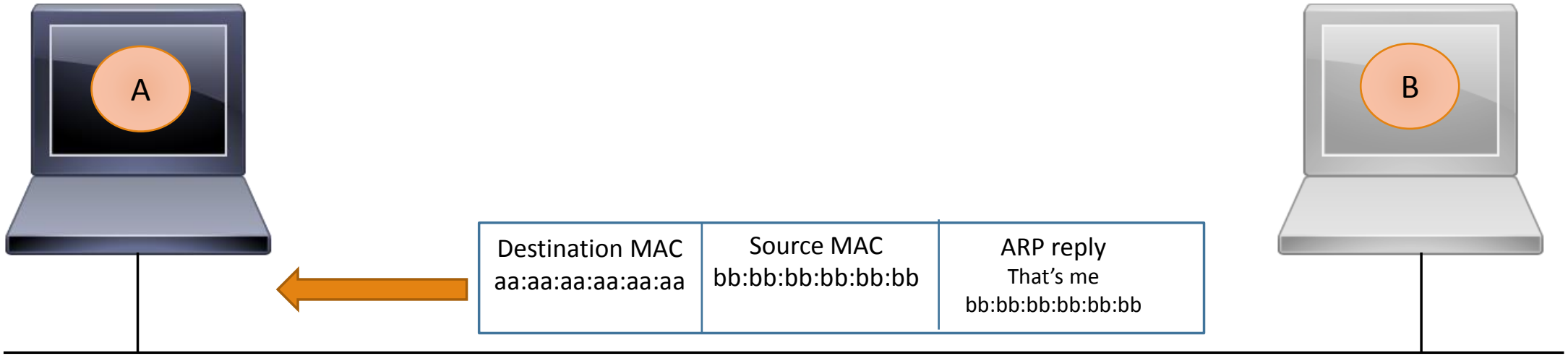
The source now needs the destination MAC address to create the frame

Broadcasting an ARP Request to Learn the Destination MAC Address



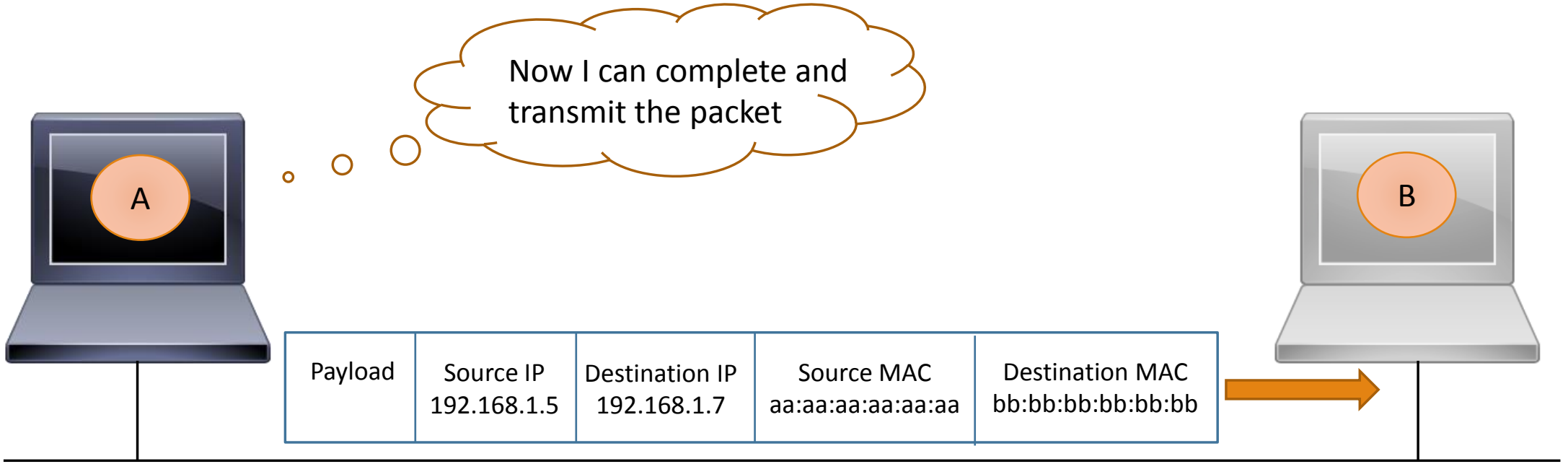
The source sends out an ARP Request via Layer 2 broadcast

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



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

5.4 IP Routing Across a Single Router

CCNA 200-301 v1.1

Module 5

Single hop delivery process

Single Hop Delivery Process

Source and Destination are on Different Networks

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

IP Routing Across a Single Router (cont'd)

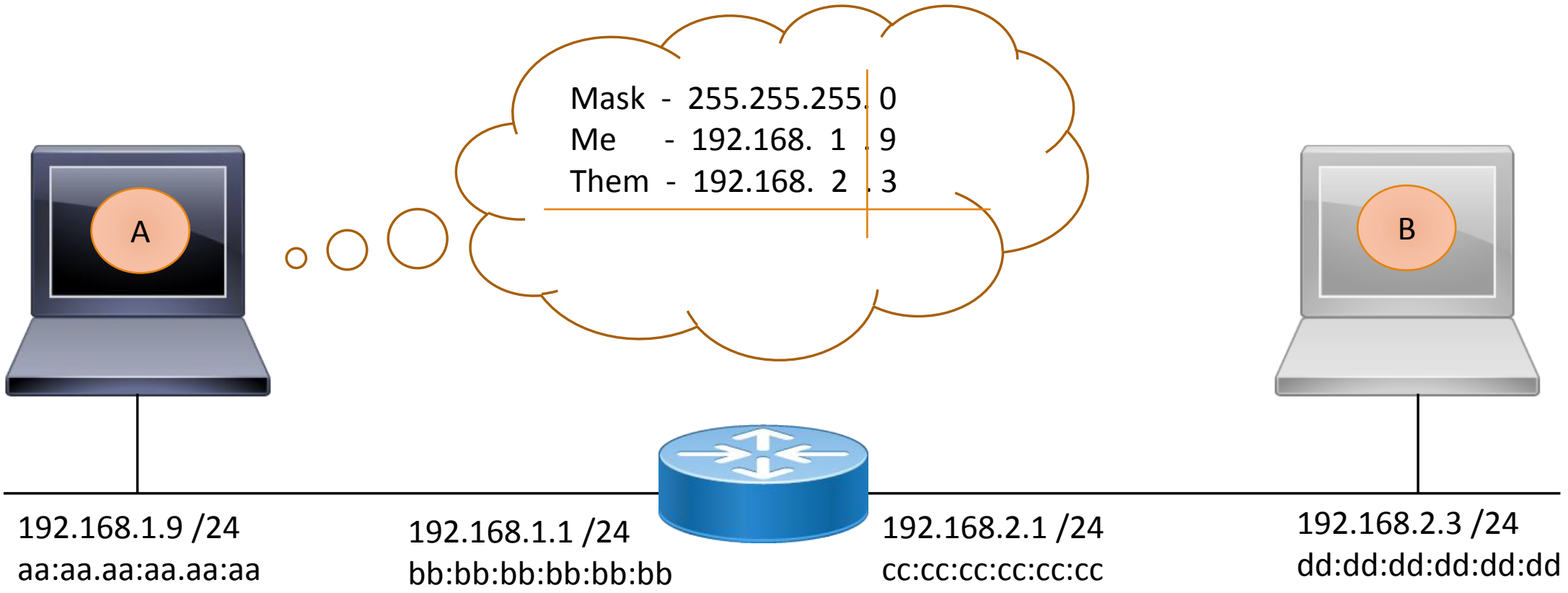
6. A puts the router's MAC address in the Ethernet header destination field
7. A transmits the frame and hopes that the router will pick it up and know how to forward it on
7. The router receives the frame
8. The router checks its route table to see if it has a route to the final destination
9. If it 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

IP Routing Across a Single Router (cont'd)

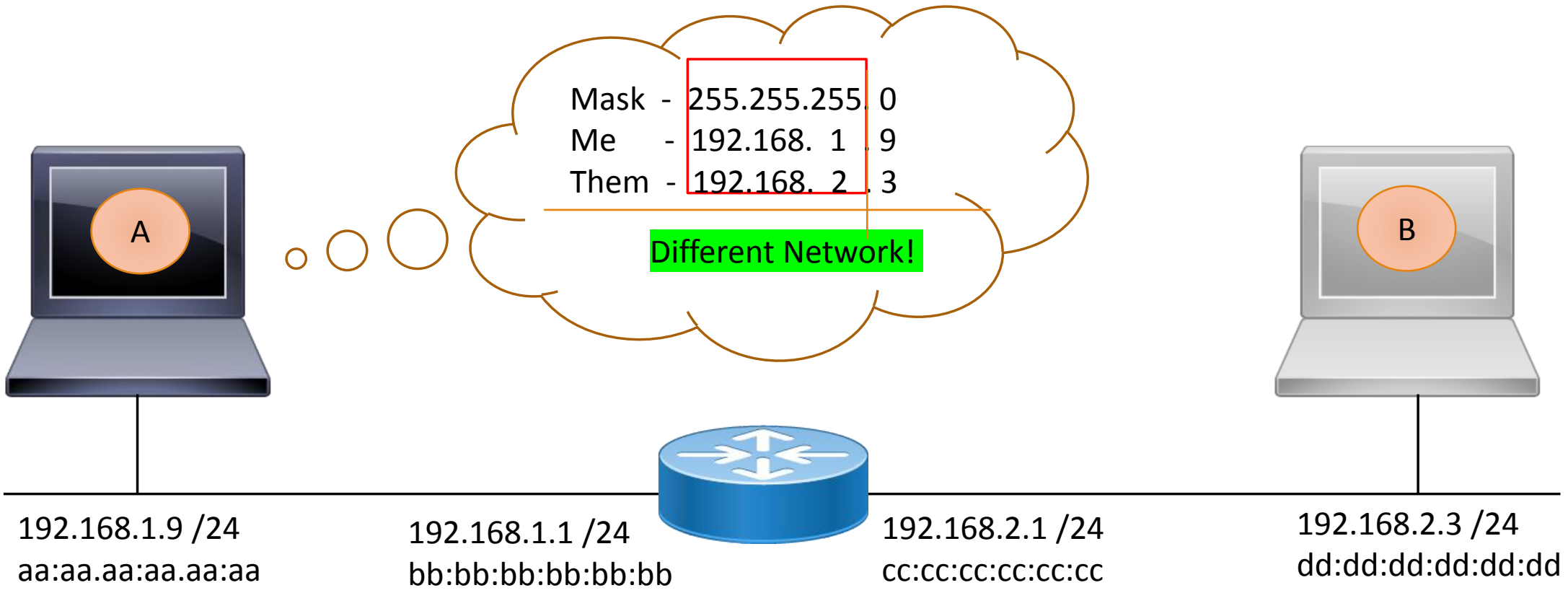
11. The router re-writes the Ethernet header of the packet, replacing the old source and destination MAC addresses
    - The new source is the MAC address of the router's outgoing port
    - The new destination is the MAC address of the final destination
    - The source and destination IP addresses 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



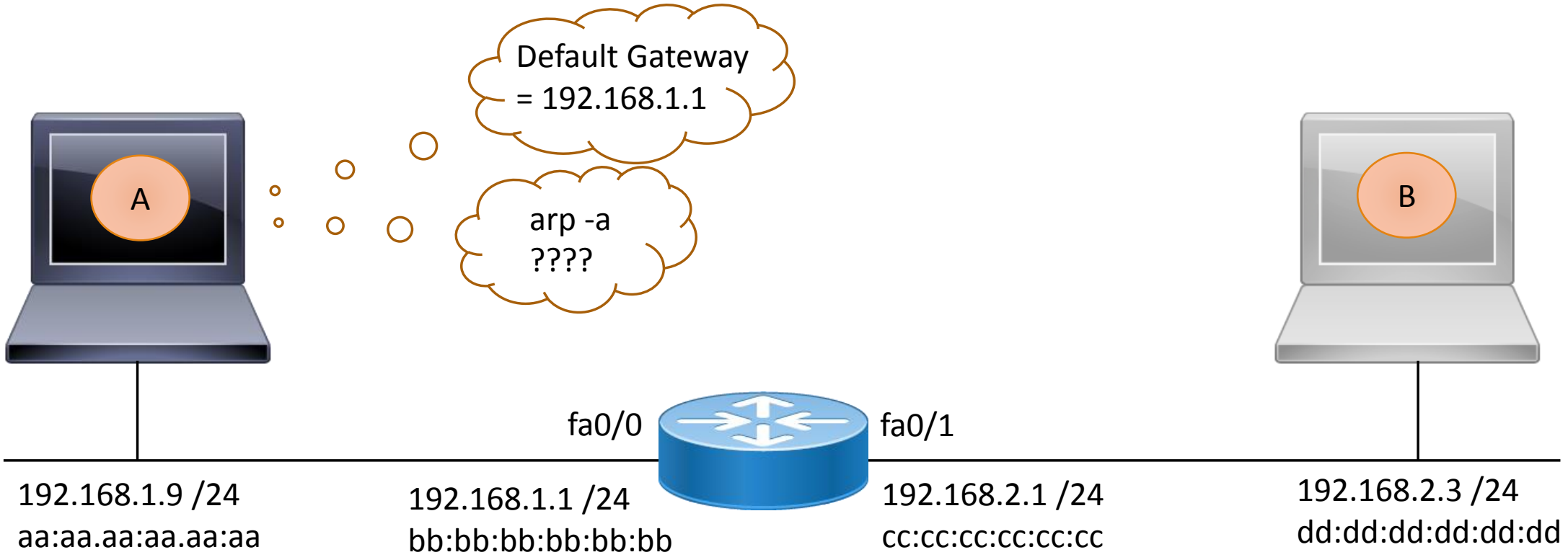
After learning the destination IP address, the sources uses its subnet mask to determine if the destination is on the same or different network

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



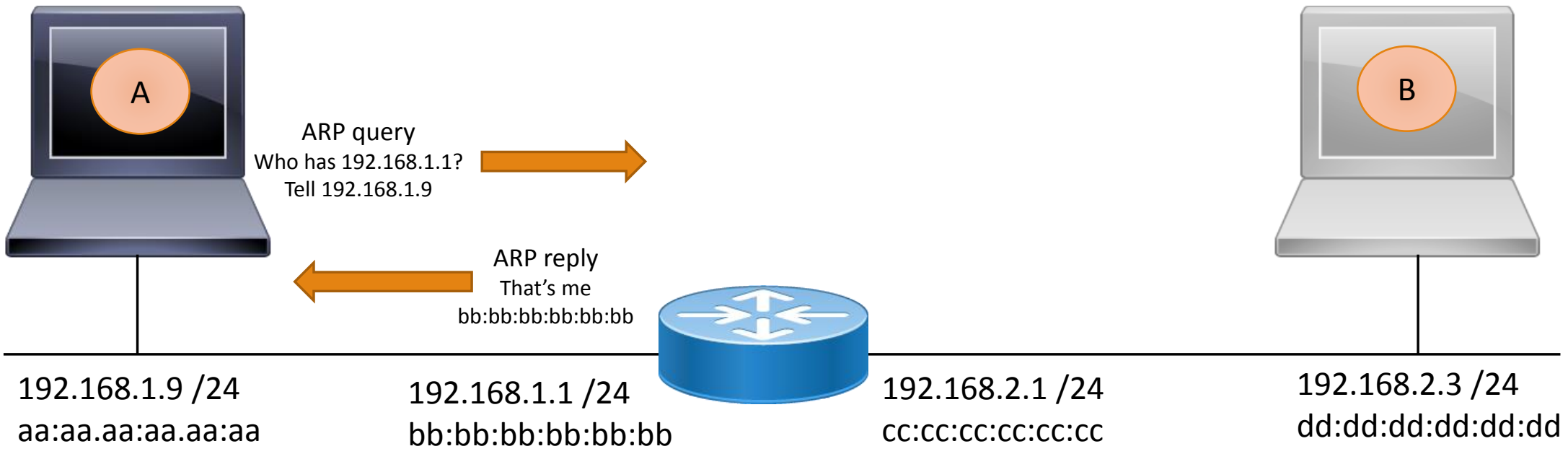
A determines that B is on a different network

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



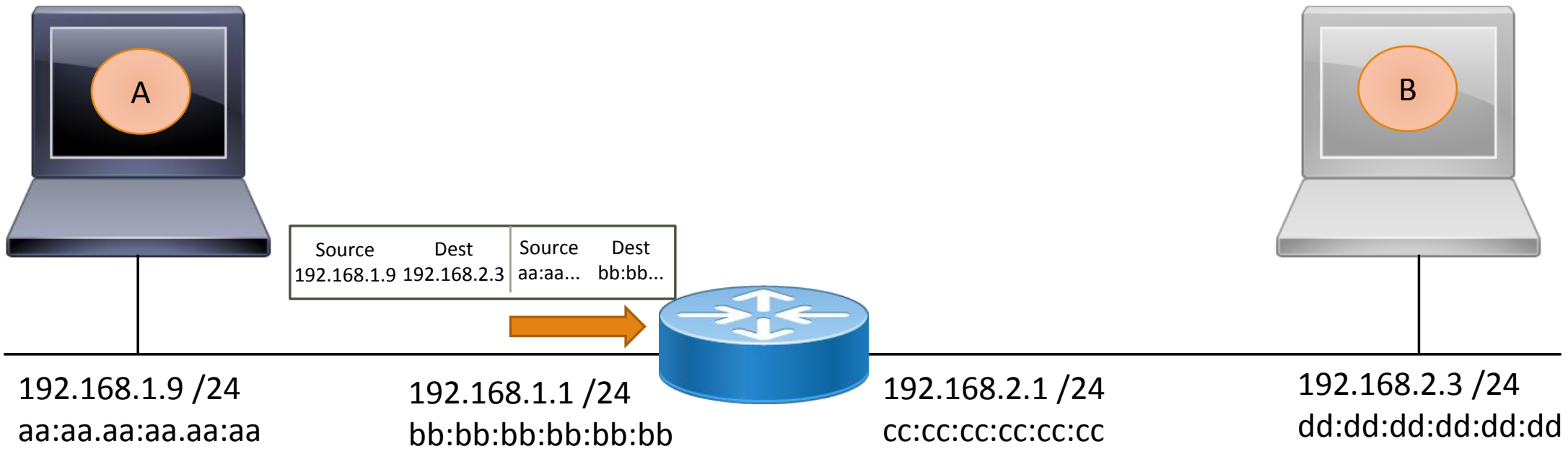
The source knows it must hand a packet destined for a remote network to its default gateway
It is already configured with the IP address of router, but it does not know the router's MAC address

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



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

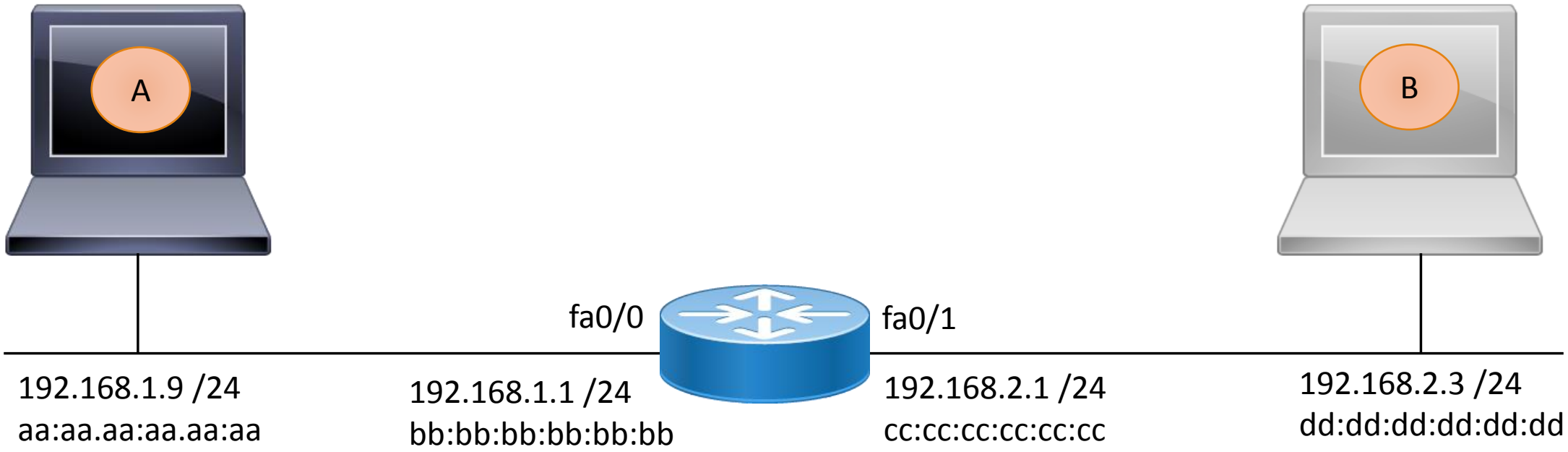
IP Routing Across a Single Router Example (cont'd)



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

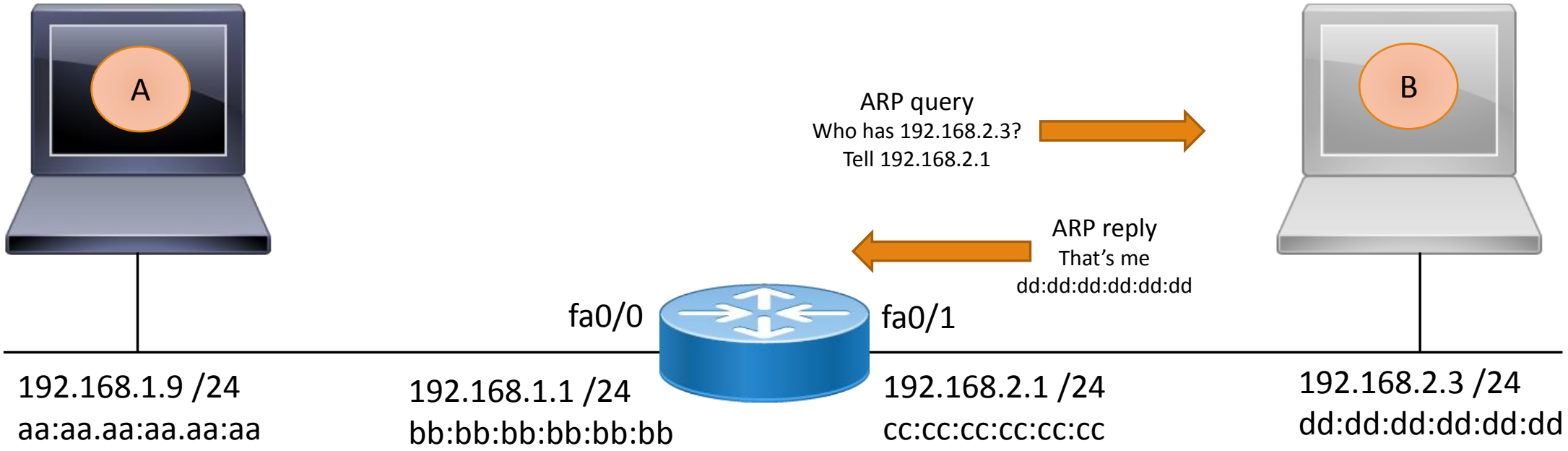
IP Routing Across a Single Router Example (cont'd)



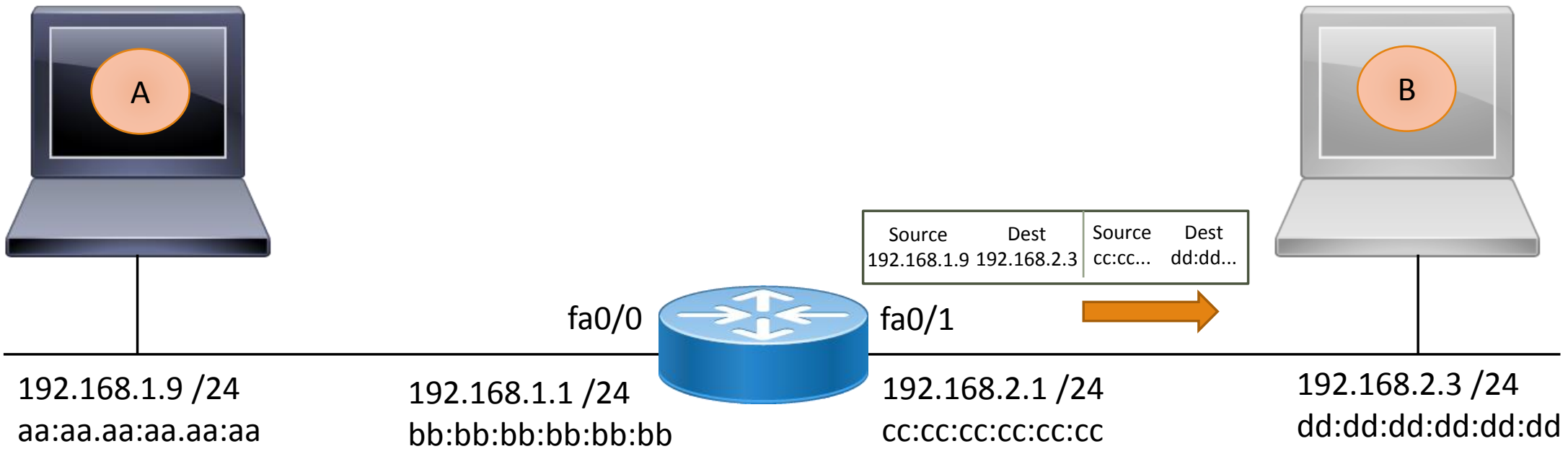
The router receives the frame
It checks its route table to see if it has a route for the Layer 3 destination
Since it does have a route, it must discover the MAC address of the next hop (the final destination)

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

5.5 IP Routing Across Multiple Routers

CCNA 200-301 v1.1

Module 5

Multiple hop delivery process

Multiple Hop Delivery Process

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 1 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

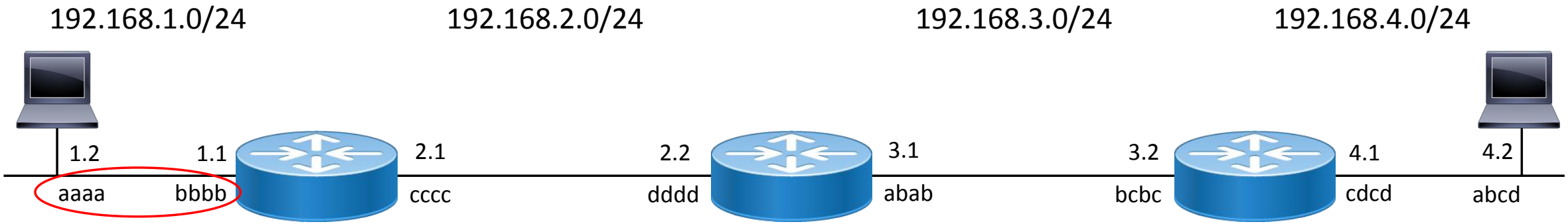
Unless translated, the source and destination IP address remain the same from end to end

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



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

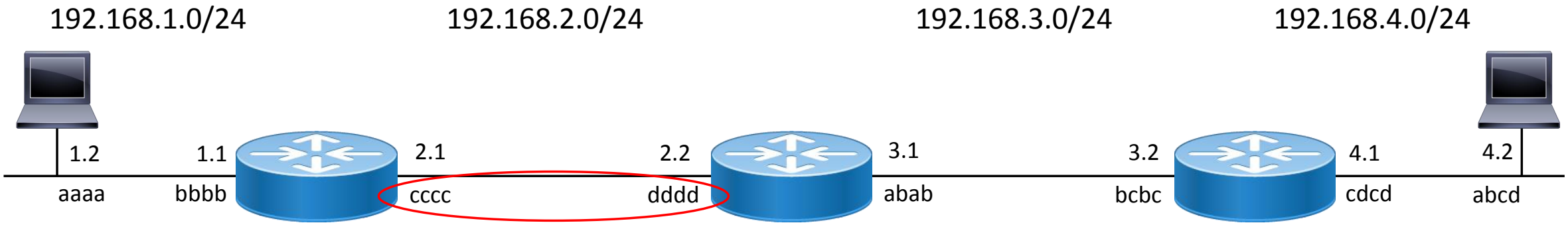
Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cccc
Dest MAC = dddd

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)



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

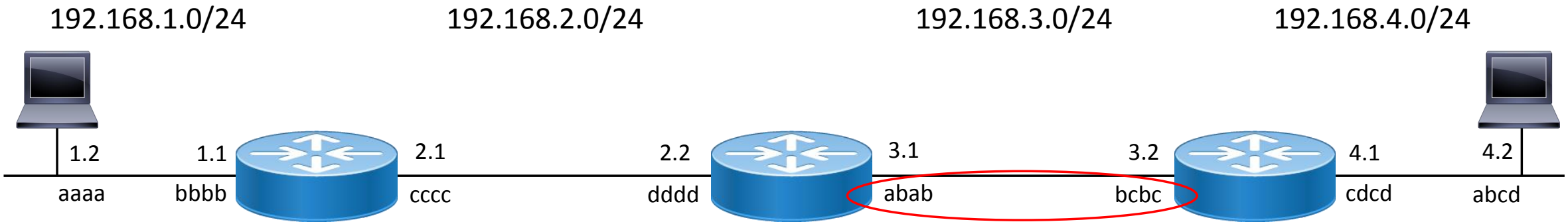
Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cccc
Dest MAC = dddd

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)



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

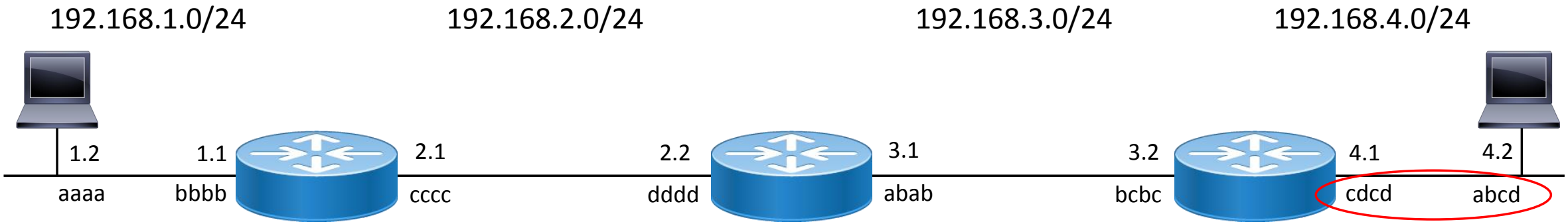
Source IP = 192.168.1.2
Dest IP = 192.168.4.2
Source MAC = cccc
Dest MAC = dddd

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)



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

5.6 Routing Protocols Overview

CCNA 200-301 v1.1

Module 5

Routed vs Routing Protocols

Dynamic Routing

Routing Protocol Types

Distance Vector Routing Protocols

Link State Routing Protocols

Hybrid Routing Protocols

Path Vector Routing Protocols

Interior vs Exterior Routing Protocols

Routing Protocol Commands

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

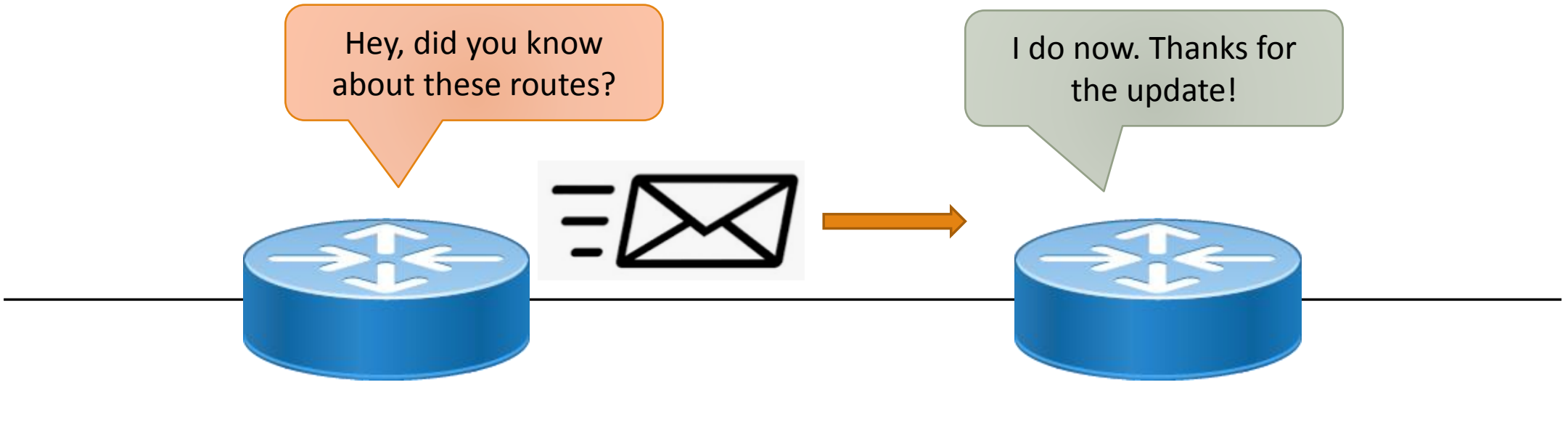
- Process is dynamic
- A router can use more than one routing protocol for compatibility
- Used by both IPv4 and IPv6
- Examples: RIP, OSPF, EIGRP, BGP

Dynamic Routing

Routers use routing protocols to tell each other about distant routes

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

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



Routing Protocol Types

Distance Vector

Link State

Hybrid

Path Vector

Distance Vector Routing Protocols

How far / What direction

Old style / simple

Routers update each other on a fixed interval

Slow convergence

- Runs risk of routing loops

Good for small networks

Very easy to implement

RIP

Routing Information Protocol (RIP)

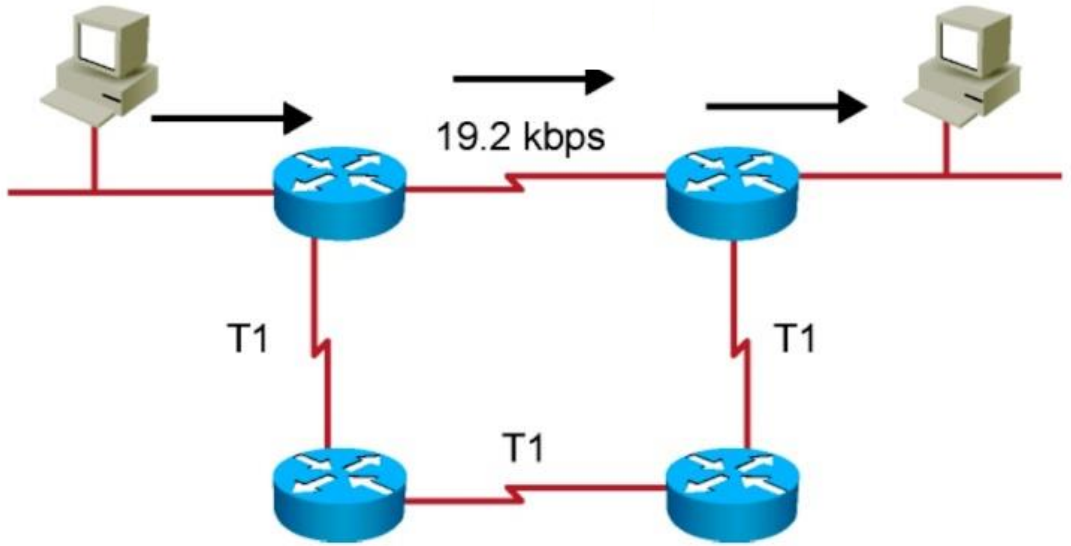
Vendor neutral

Easy to set up

Suitable for small, simple environments

Makes routing decisions purely on hop count

- Bandwidth, delay, link reliability, etc. don’t matter
- Slow convergence
- Has a maximum hop count of 15 in any direction



RIPv1 Broadcasts the entire route table to neighbors every 30 seconds

RIPv2 multicasts the entire route table to neighbors every 30 seconds

RIP Configuration Example

R1(config)# router rip

R1(config-router)# version 2

R1(config-router)# no auto-summary

R1(config-router)# network 192.168.1.0

R1(config-router)# network 10.1.1.0

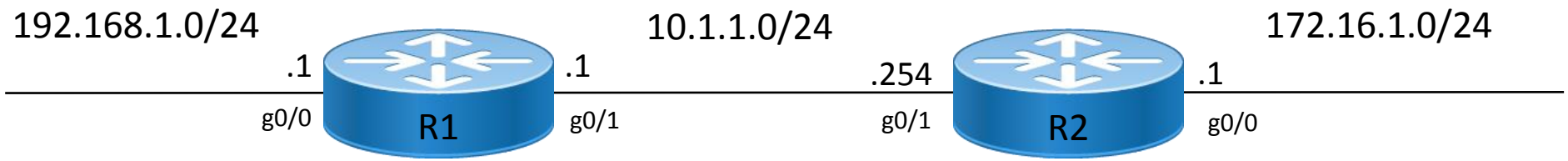
R2(config)# router rip

R2(config-router)# version 2

R2(config-router)# no auto-summary

R2(config-router)# network 10.1.1.0

R2(config-router)# network 172.16.1.0



Link State Routing Protocols

Routers maintain a database of the entire network and all routes

If a link changes state, routers immediately update each other

- There's an initial flood of routing information among routers
- After convergence, routers only send updates when a link changes state
- Hello packets keep the router neighbor relationships alive in between updates

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, IS-IS

OSPF

Vendor neutral

More complex to configure

Divides the network into areas

Only sends updates if a link changes state

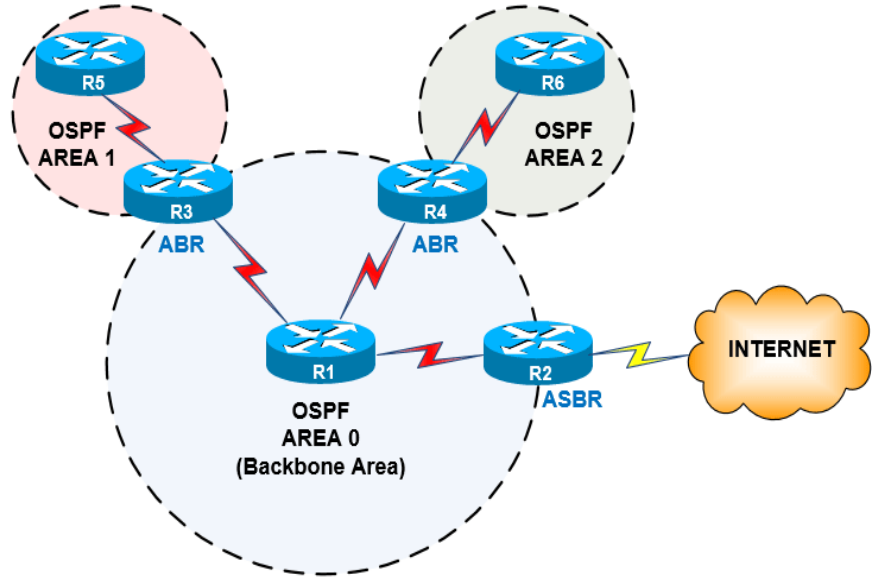
Best path is chosen based on cumulative link cost to a destination

Each network segment elects a router to manage update traffic

Each router maintains its own topology database for the area

Fast convergence

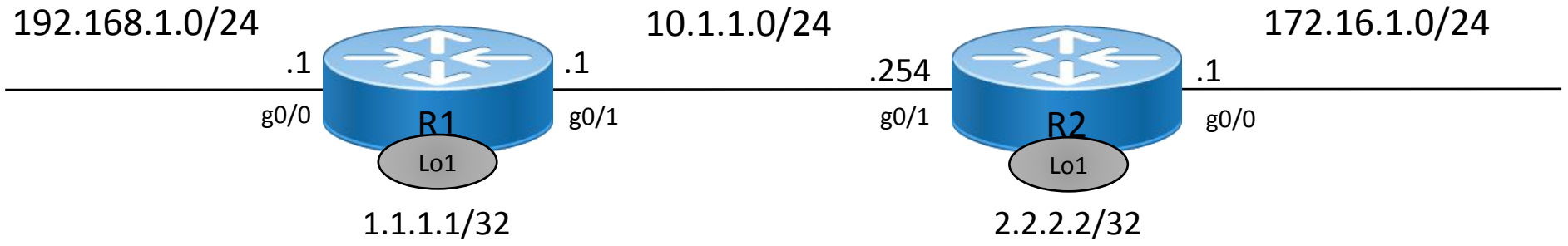
Requires a well-designed network with hierarchical IP addressing



OSPF Configuration Example

```
R1(config)# interface Loopback0
R1(config-if)# ip address  1.1.1.1  255.255.255.255
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# router-id  1.1.1.1
R1(config-router)# network 192.168.1.0  0.0.0.255  area  0
R1(config-router)# network 10.1.1.0  0.0.0.255  area  0
```

```
R1(config)# interface Loopback0
R1(config-if)# ip address  2.2.2.2  255.255.255.255
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# router-id 2.2.2.2
R1(config-router)# network 10.1.1.0  0.0.0.255  area  0
R1(config-router)# network 172.16.1.0  0.0.0.255  area  0
```



Hybrid Routing Protocols

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

Easy to implement

EIGRP

EIGRP

Cisco proprietary

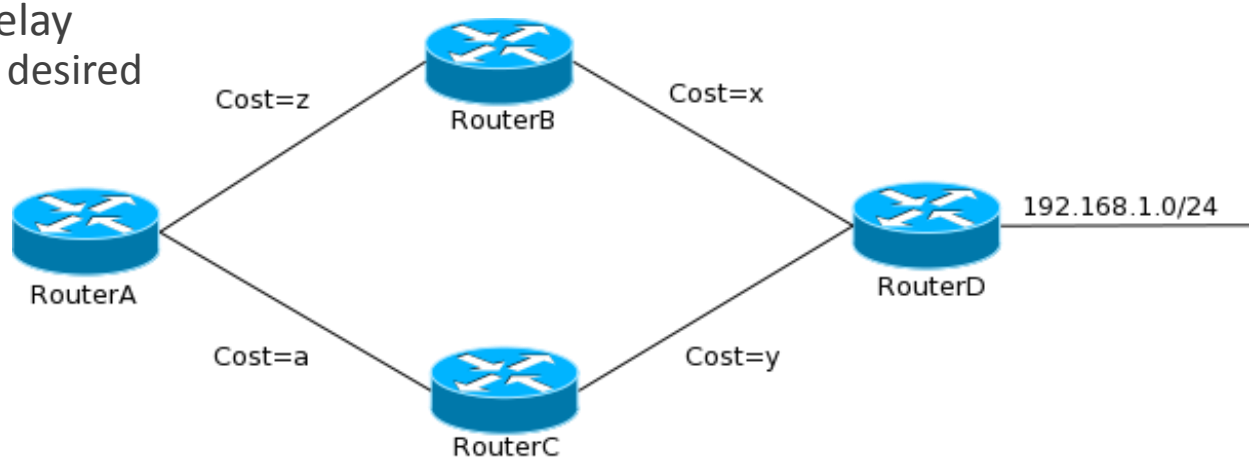
Easy to configure

Every router maintains a topology table of the entire network

Makes routing decisions based on bandwidth + delay
- You can also factor in load, reliability, and MTU if desired

Advertised distance =
- The cost from the neighbor to the destination

Feasible distance =
- The total cost to the final destination
- Cost to the neighbor + their advertised distance



Very fast convergence

All neighbors must belong to the same autonomous system (AS)
- Autonomous System = Network under a single administrative umbrella
- AS number can be internally assigned (need not be public)

EIGRP Configuration Example

R1(config)# router eigrp 100

R1(config-router)# network 192.168.1.0

R1(config-router)# network 10.1.1.0

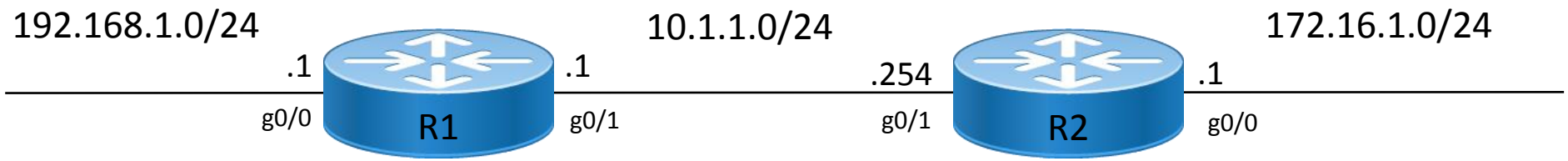
R1(config-router)# no auto-summary

R1(config)# router eigrp 100

R1(config-router)# network 10.1.1.0

R1(config-router)# network 172.16.1.0 0.0.0.255

R1(config-router)# no auto-summary



Path Vector Routing Protocols

A variation on distance vector

A “hop” is an entire autonomous system, not just a single router

- All routers in a hop belong to the same autonomous system

Very slow convergence

Complex to implement

Requires a very large network to be worthwhile

BGP

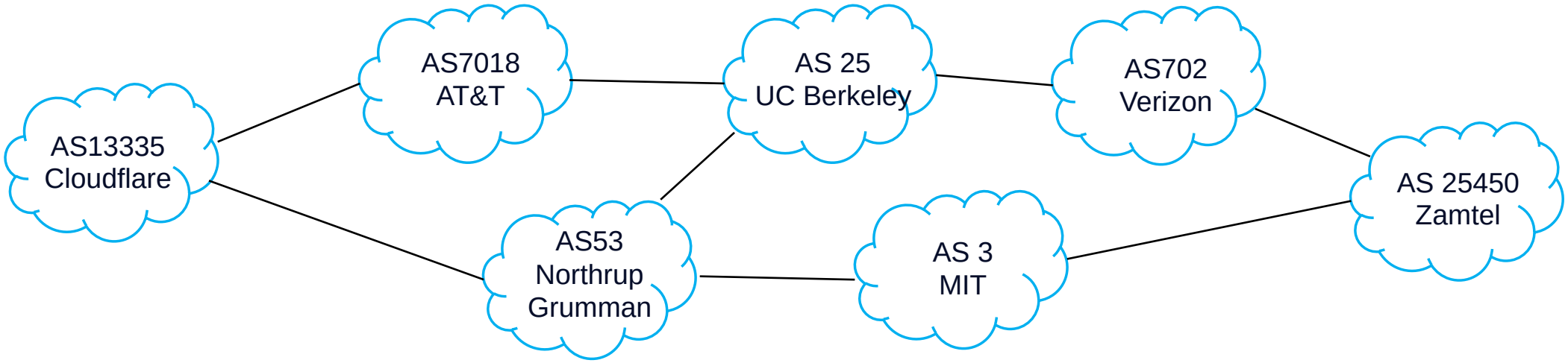
Border Gateway Protocol (BGP)

Used on the Internet

Treats entire Autonomous Systems as hops

Complex to configure

Path selection based on multiple attributes including AS hop count, path “weight”, origin, path lifetime (oldest is best), router ID, neighbor IP address, etc.



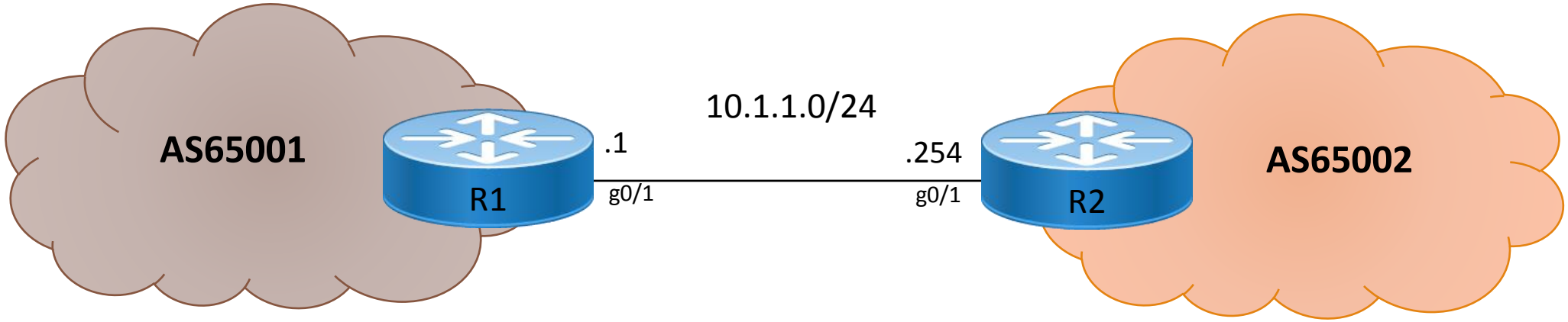
BGP Configuration Example

R1(config)# router bgp 65001

R1(config-router)# neighbor 10.1.1.254 remote-as 65002

R1(config)# router bgp 65002

R1(config-router)# neighbor 10.1.1.1 remote-as 65001



Interior vs Exterior Gateway Protocols

Also called Interior and Exterior Routing Protocols

Interior Gateway Protocol

- Used within an organization's internal/private network
- RIP, OSPF, EIGRP, IS-IS, iBGP

Exterior Gateway Protocol

- Used between ISPs and other organizations on the Internet
- BGP

Routing Protocol Commands

Command	Description
`show running-config`	Display the current running configuration
`show ip route`	Display the routing table
`show ip protocols`	Display information about any configured routing protocols
`show ip rip`	Display information about any configured RIP instance
`show ip ospf`	Display information about any configured OSPF instance
`show ip eigrp`	Display information about any configured EIGRP instance
`show ip bgp`	Display information about any configured BGP instance

5.7 Route Selection

CCNA 200-301 v1.1

Module 5

Routing Table Information

Router Forwarding Decisions

Longest Prefix Match

Administrative Distance (AD)

Routing Protocol Metric

Routing Table and Related Commands

Challenge Problem

Routing Table Information

Routing Protocol Code

- Indicates the source that provided the route
- Can be a routing protocol, a directly connected link, or statically entered

Prefix

- The destination network ID

Network Mask

- The subnet mask used by the destination network

Next Hop

- The next router to hand the packet to

Routing Table Information (cont'd)

Administrative Distance (AD)

- The desirability/believability of a route based on its source

Metric

- The cost of a route within one routing protocol

Gateway of Last Resort

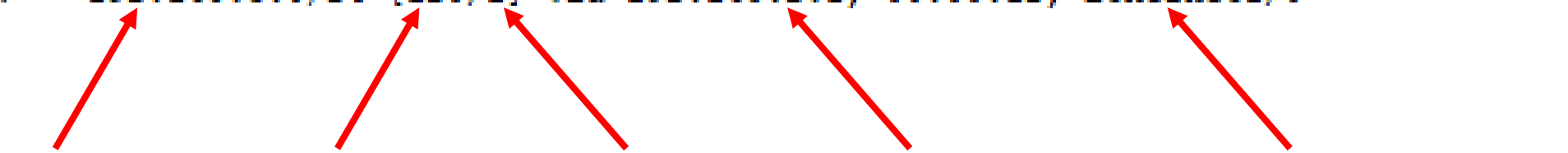
- The default route
- Who to hand it to if there is no other route

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
```

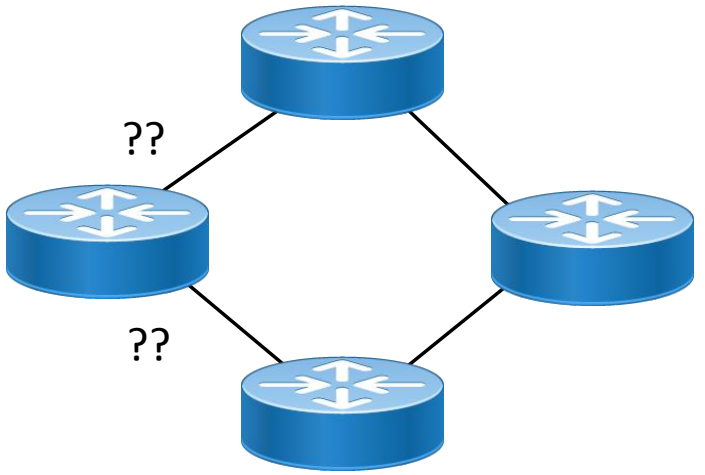


Router Forwarding Decisions

Choosing a Route

Route is chosen based on this order:

1. Prefix length
2. Administrative Distance
3. Metric



Router Forwarding Decisions

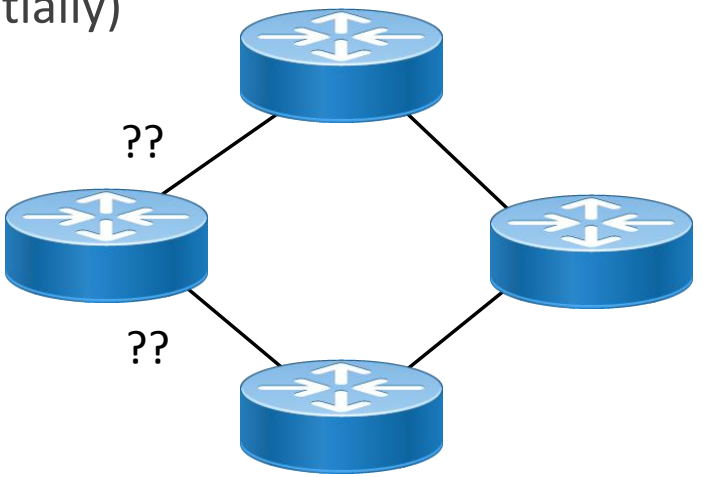
Routers may or may not have multiple routes to choose from

- The “best” route for each prefix (network ID) will be placed in the router’s routing table
- But the routing table might have multiple related prefixes

A router makes routing decisions based on three criteria (sequentially)

If there is a tie, move to the next criterion:

1. Longest Prefix Match
2. Administrative Distance
3. Routing Protocol Metric



Longest Prefix Match

The first criterion for choosing a route

If there are multiple routes to the same destination, choose the one with the longest prefix

- Prefix is determine by the length of the network mask (the most binary 1s / largest CIDR number)
- Longer prefix = more specific = closer to the actual destination
- Choose longest match regardless of source

Examples:

Choose This	Over This
10.1.1.0/24	10.0.0.0/8
192.168.1.35/32	19.168.1.0/24
172.16.77.0/24	172.16.0.0/16

Administrative Distance (AD)

The second criterion for route selection, after longest prefix match

“Believability” of a route source

A source can be:

- Directly connected network
- Statically entered by an administrator
- A routing protocol

Each source has an assigned administrative distance

An admin can create a route with a custom AD

- Statically enter a route with a higher (worse) AD than all the other sources
- AD of 200 is a common choice for “floating static” (backup) routes

Cisco Administrative Distances

Routing Protocol	Administrative Distance
Directly connected	0
Statically entered (default value)	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

Routing Protocol Metric

AKA metric

Third and last criterion for choosing a route

The cost of a particular route compared with other routes with the same AD
- Best (lowest) metric wins

Can be based on:
- Hop count (RIP, BGP)
- Bandwidth + delay (EIGRP)
- Cumulative link cost (OSPF)
- Other factors such as:
  - Reliability, MTU, loading (EIGRP)
  - Router attributes (BGP)

Routing Table and Related Commands

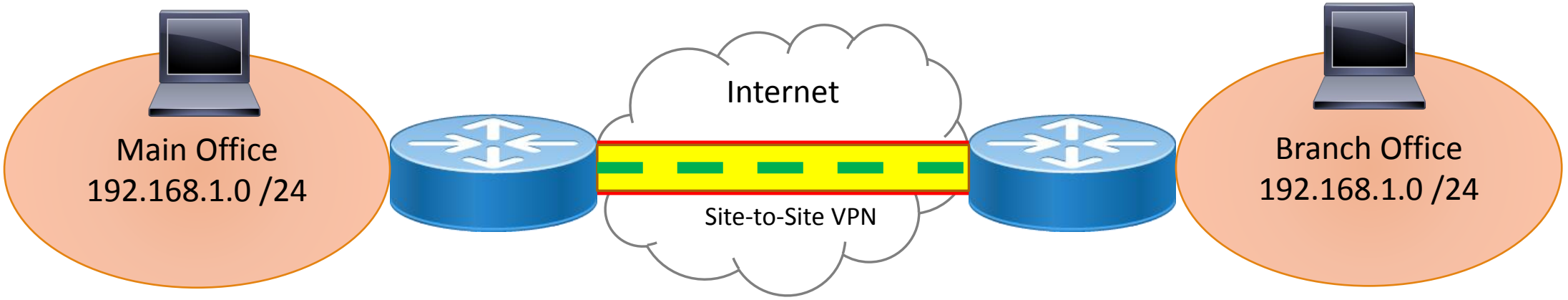
Command	Description
`ip route 10.0.0.0 255.255.255.0 192.168.1.1 150`	Configure a static route with a custom administrative distance
`show ip route`	Display the routing table
`show ip route <destination>` `show ip route 173.45.67.0`	Display routes for a specific network or prefix
`show ip route <next-hop-ip>` `show ip route 10.1.1.254`	Display routes learned from a specific next-hop IP address

Routing Table and Related Commands (cont'd)

Command	Description
`show ip route interface <interface>` `show ip route interface g0/0`	Display routes for a specific interface
`show ip route summary`	Display a summary of the routing table
`ping <destination>` `ping 192.168.1.25`	Send ICMP echo to a destination to see if it responds; proves network connectivity at layer 3
`ping`	Extended ping. Add parameters when prompted
`show ip interfaces brief`	Display all interfaces with status and IP address

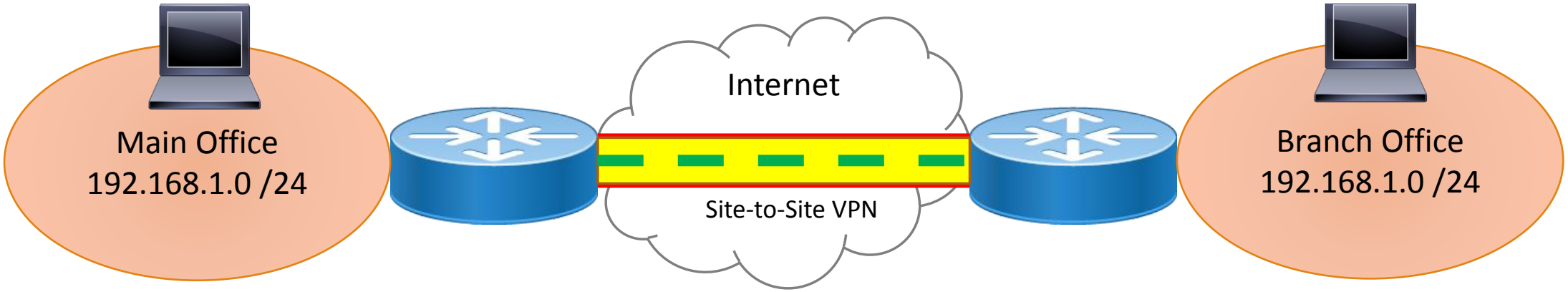
Challenge Problem

Can you solve this problem?



Can you tell what's wrong?

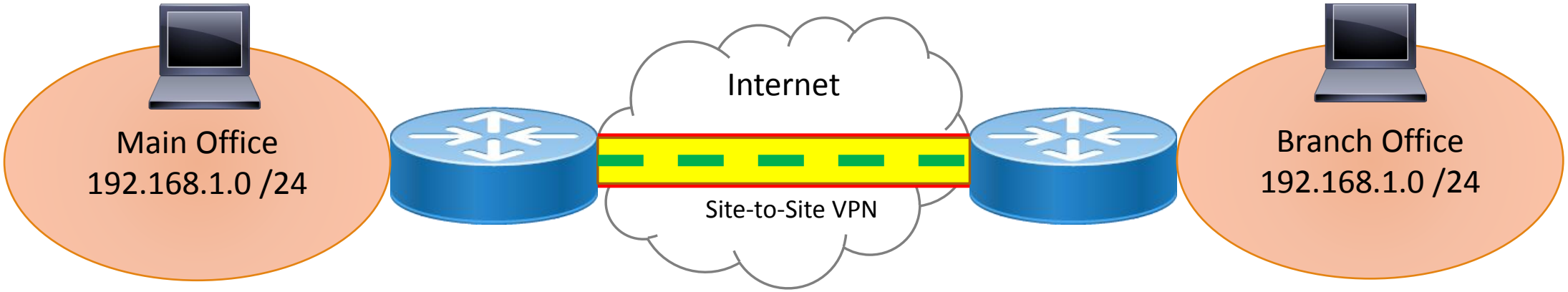
Can you solve this problem?



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

Can you solve this problem?

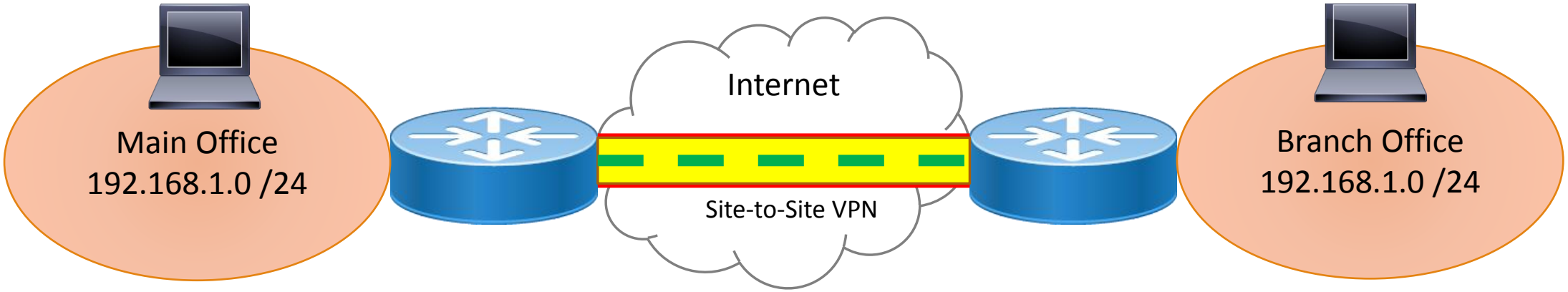


Can you tell what's wrong?

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?

Can you solve this problem?



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 side to something different such as 192.168.2.0 /24

5.8 Open Shortest Path First (OSPF)

CCNA 200-301 v1.1

Module 5

What is OSPF?

OSPF Areas

Router Process ID

Loopback Interface

OSPF Router IDs

OSPF Neighbors

OSPF Elections

Designated Router (DR)

Backup Designated Router (BDR)

DROther

OSPF Route Update Process

OSPF Convergence

OSPF Timers

Wildcard Mask

OSPF Network Statement

Configuring OSPF on a Point-to-Point Serial Link

OSPF Commands

What is OSPF?

A 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

OSPF requires the network to be well-designed with hierarchical addressing for route summarization

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

Each router maintains its own OSPF database
- Contains a complete topology of the entire OSPF area
- Best route for each destination is put in the route table
- When there is a network change, the router consults its own database to choose the new route

Note: OSPFv3 is used for IPv6

OSPF Areas

Routers are organized into “areas” (each with max of 400 routers)

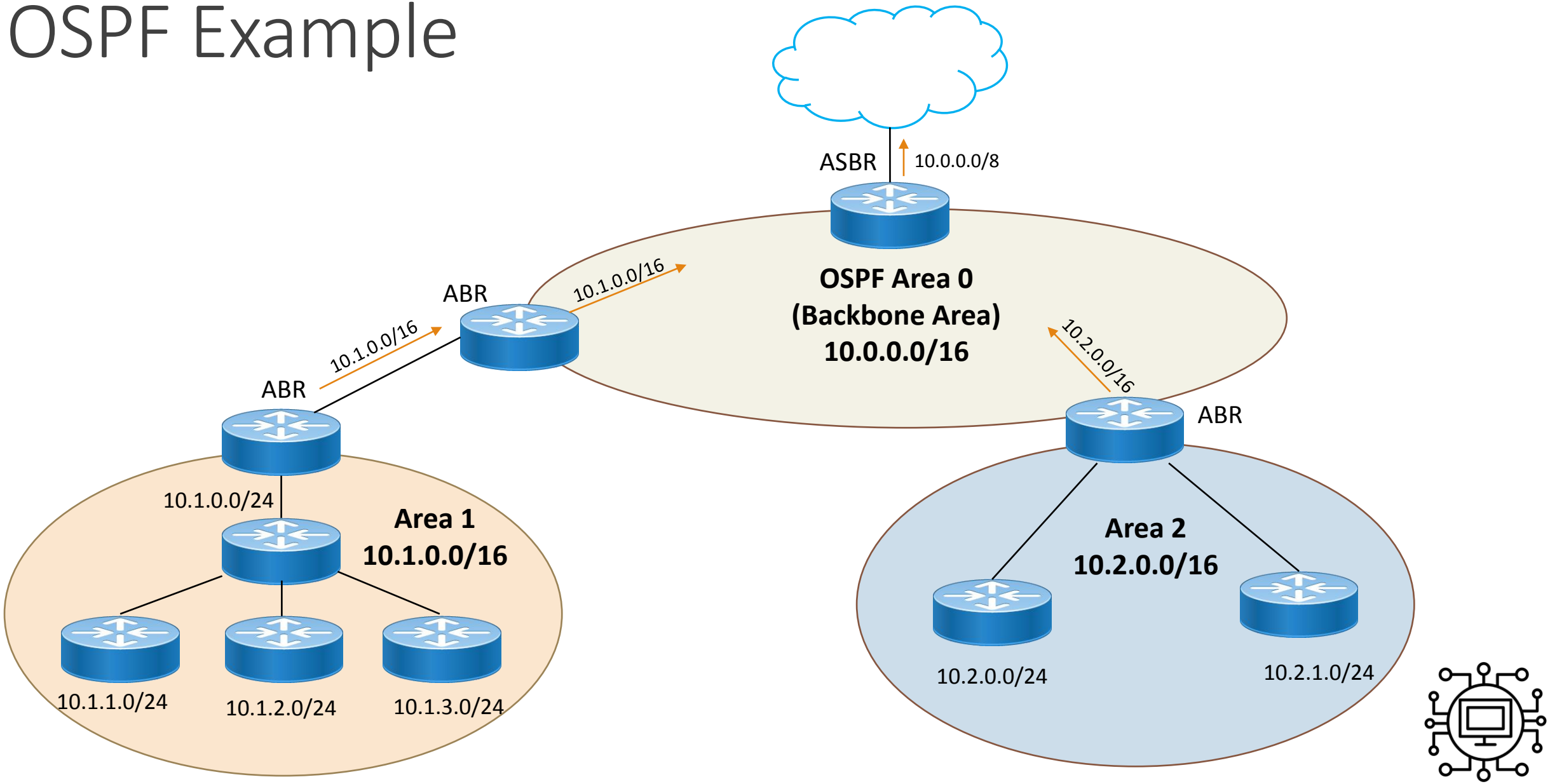
- Each area should contain a contiguous block of IP addresses that can be summarized at the area border router
- Networks IPs within one area should be hierarchically organized to take advantage of CIDR and route summarization
- Subnets from one area should not exist in another area

An Area Border Router (ABR) connects an area to the backbone (“Area 0”)

Traffic between areas travels through the backbone

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

OSPF Example



Router Process ID

A number chosen by the admin

Identifies that particular instance of OSPF running on that router

A router can run multiple instances of OSPF

- Each instance needs its own Process ID

The Process ID only has meaning on that particular router

Different routers can use the same process ID number

- They are not related in any way

```
Router(config)# router ospf 1
```

Loopback Interface

A loopback is a virtual interface inside a router

Should be configured as its own “one IP address subnet” with a /32 subnet mask

- No other nodes are on this “network”
- The router can route to it because it is “directly connected”

You can use the loopback as the Router ID in OSPF

Treat it like any other destination

- Advertise it in a routing protocol network statement
  - Or create static routes to it
- If all routers have a route to the loopback, you can ping/SSH/telnet to it

Example:

```
R1(config)# interface Loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# no shut
```

OSPF Router IDs

Unique identifier for an OSPF router

Can be manually assigned

- You must choose an already existing IPv4 address on a “live” interface (loopback or physical)

The order of preference for a router to choose its OSPF ID is:

1. Manually-assigned
2. Highest loopback IP address
3. Highest physical interface IP address

If the interface providing the Router ID goes down, the router must change its ID to an interface that is up

- Prefer to use a loopback rather than a physical interface for the Router ID
- A loopback is always stable, never goes down
- A loopback can also be advertised as a regular destination “network” to other OSPF routers
- You can ping, SSH or telnet to the loopback address

Configuring the Router ID

Create Loopback

Router(config)# interface loopback0

Router(config-if)# ip address 1.1.1.1 255.255.255.255

Router(config-if)# no shut

Manually Assign

Router(config)# router ospf 1

Router(config-router)# router-id 1.1.1.1

OSPF Neighbors

A “neighbor” is a directly-connected router also running OSPF

- Must be in the same OSPF area

Neighbors form adjacencies (relationships) among themselves

- They will automatically discover each other if they are on the same segment and their Hello (and other) timers match

Adjacencies are used to update neighbors with new route information

OSPF Elections

On multiaccess (Ethernet) segments:

- OSPF neighbors hold an election to determine two roles, Designated Router (DR) and Backup Designated Router (BDR)
  - They compare Router IDs via multicast Hellos (224.0.0.5)
  - Highest Router ID becomes the DR
  - 2nd highest Router ID becomes the BDR
- The DR is responsible for receiving and sending route updates on the segment
- The BDR is a backup router that takes over if the DR fails

Note: In this context, an Ethernet segment is also its own subnet

OSPF Elections (cont’d)

On point-to-point WAN links:

- Neighbors compare router IDs to form a master/slave adjacency
- The router with the higher ID becomes the master
- The router with the lower ID becomes the slave

Note: In this context, WAN links are also subnets

Designated Router (DR)

Used on a multi-access network segment such as Ethernet

Acts as the central point of communication for all OSPF routers on that segment

Responsible for generating and distributing Link State Advertisements (LSAs) on behalf of all routers in the network segment

- This reduces the number of OSPF adjacencies and the amount of OSPF traffic on the segment
- Makes the network more efficient

Backup Designated Router (BDR)

A backup to the DR

On the same multi-access segment as the DR

Listens passively and takes over the role of the DR if the current DR fails

Ensures network stability and continuity

The BDR is also elected on each multi-access network segment

DROther

A router on a multi-access segment that is neither DR nor BDR

Does not establish adjacencies with other DROthers

Only establishes adjacencies with the DR and BDR

If both the DR and BDR fail, the DROther routers will participate in a new election to select a new DR and BDR

OSPF Route Update Process

All OSPF update activity remains confined to an OSPF area

1. A link on an OSPF router changes state / the router receives some kind of update
2. The DROther and BDR routers sends a Link-State Update (LSU) to the DR/BDR multicast address 224.0.0.6
3. The DR repeats the LSU to all other routers in the segment using the multicast address 224.0.0.5

The LSU contains one or more Link-State Advertisements (LSAs)

- LSAs are the actual route update

Neighbors receiving the LSU:

1. Process the contained LSA(s)
2. Update their OSPF database if the information is new
3. Acknowledge the LSU
4. If the LSA is new, they will use an LSU to pass it along to neighbors in other network segments

On a point-to-point link, master and slave routers send LSUs to each other's unicast address

- The master router controls the convergence process

OSPF Convergence

How long it takes for all routers to have the same routing information

Most routers will belong to more than one network segment

- The router will participate in as many elections as the segments it is connected to
- Might be a DR or BDR in one segment, a DROther in another segment, and a master or slave in yet another segment

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

- Includes routes from neighbors of every segment
- The best route for each destination goes into the route table
- If a router learns that a particular link has gone down, it consults its own database for the next best route

OSPF convergence in a single area is very fast

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

OSPF Timers

If links do not change state, simple Hello keepalives with route summaries are sent to neighbors to minimize traffic

OSPF timers must match for neighbors to form adjacencies

Hello Interval

- How often an OSPF router sends Hello packets to its neighbors
- These Hello packets are used to establish and maintain OSPF neighbor relationships
- Default Values:
  - 10 seconds on broadcast and point-to-point networks
  - 30 seconds on non-broadcast and point-to-multipoint networks (Frame-relay, X.25, ATM, and certain VPN networks)

OSPF Timers (cont'd)

Dead Interval

- How long a router will wait without receiving any Hello packets before it declares that neighbor down
- Default values:
  - 4 times the Hello interval
  - 40 seconds on broadcast and point-to-point networks
  - 120 seconds on non-broadcast and point-to-multipoint networks

Other OSPF timers:

- Wait, Retransmit, LSA Aging, LSA Refresh, LSA Hold, LSA Delay, SPF Calculation, Adjacency Hold

Wildcard Mask

Specifies the range of IP addresses on a network segment

Inverse of the subnet mask

- When added to the subnet mask, will result in 255.255.255.255

Used when configuring router access control lists (ACLs), OSPF, and optionally EIGRP

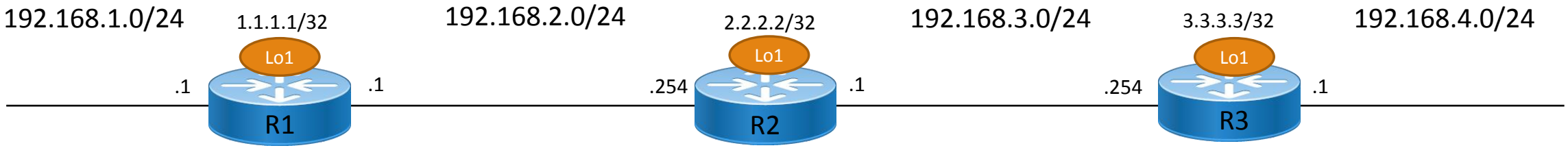
Examples:

Subnet Mask	Wildcard Mask
255.0.0.0	0.255.255.255
255.255.192.0	0.0.63.255
255.255.255.0	0.0.0.255
255.255.255.240	0.0.0.15
255.255.255.252	0.0.0.3
255.255.255.255	0.0.0.0

OSPF Network Statement

Create a network statement for every directly-connected network

- Must be YOUR network - directly connected - not some distant network
- Tells any interfaces on that network to participate in OSPF
- Advertises that network to other routers
- Include loopback “networks” if you wish to be able to remotely connect to those interfaces



network 192.168.1.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
network 192.168.2.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
network 192.168.3.0 0.0.0.255 area 0

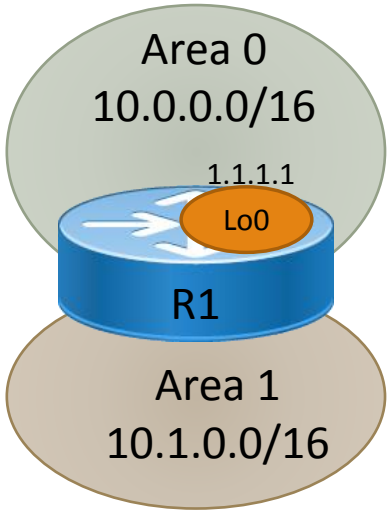
network 192.168.3.0 0.0.0.255 area 0
network 3.3.3.3 0.0.0.0 area 0
network 192.168.4.0 0.0.0.255 area 0

OSPF Configuration Example

```
# Enable OSPF and assign a process ID
R1(config)# router ospf 1

# (Optional) Manually choose the router-ID
R1(config-router)# router-id 1.1.1.1

# Enter network statements including wildcard mask and area
R1(config-router)# network 1.1.1.1  0.0.0.0  area  0
R1(config-router)# network 10.0.0.0  0.0.255.255  area  0
R1(config-router)# network 10.1.0.0  0.0.255.255  area  1
```



Configuring Single Area OSPF Example

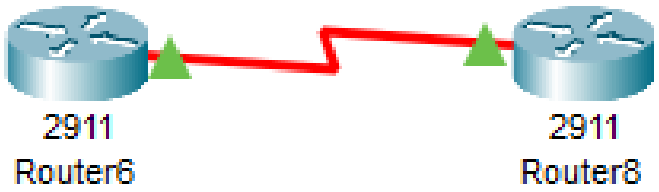
```
R1(config)# interface Loopback0
R1(config-if)# ip address 1.1.1.1  255.255.255.255
R1(config-if)# no shut
R1(config-if)# interface GigabitEthernet0/1
R1(config-if)# ip address  10.0.0.1  255.255.255.0
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.0.0.0 0.0.0.255  area  0
R1(config-router)# network 1.1.1.1  0.0.0.0  area  0
R1(config-if)# end
R1# copy running-config startup-config
```

If you configure OSPF (with same area and default timers) on all routers on a link, they will very quickly recognize each other as neighbors and establish adjacencies accordingly.

Configuring OSPF on a Point-to-Point Serial Link

Create a point-to-point serial link with:

- IP addresses (prefer 255.255.255.252 subnet mask)
- Configure OSPF as usual on the routers



Add network statements on both sides for the WAN link

- Ensure wildcard mask reflects the subnet mask
- R1(config-router)# network 172.16.5.0 0.0.0.3 area 0
- If this is an Area Border Router, put the WAN link in area 0

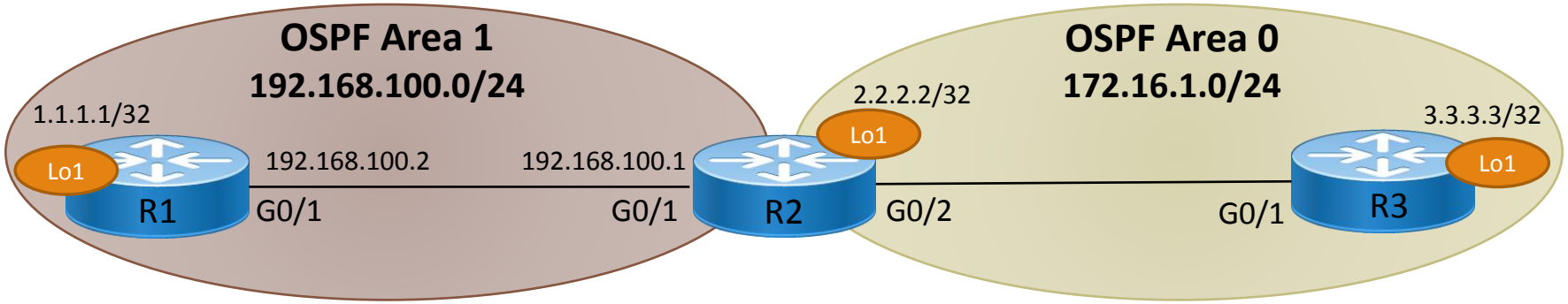
You'll notice that the higher Router ID will immediately become the Master

The lower Router ID will immediately become the Slave

They will at once form a neighbor adjacency

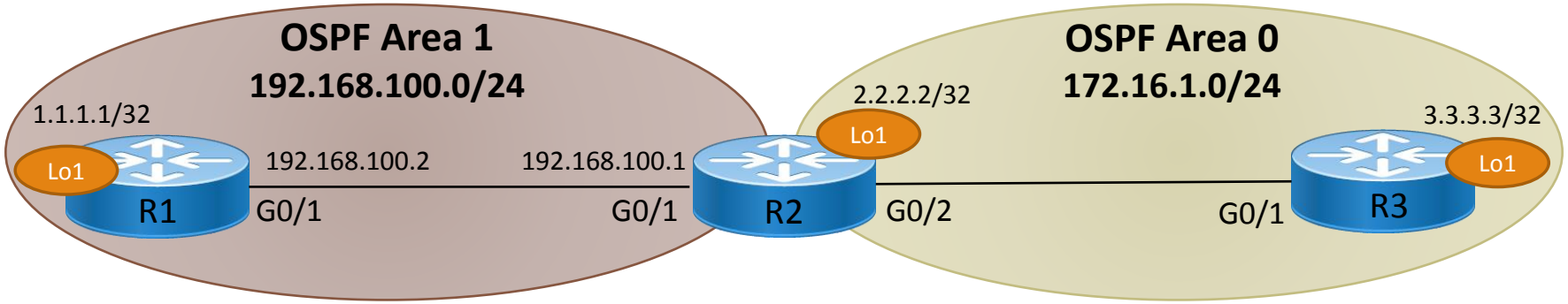
- They will trade hellos, LSUs, load their databases and become converged

Configuring Multi-area OSPF with Loopback Example



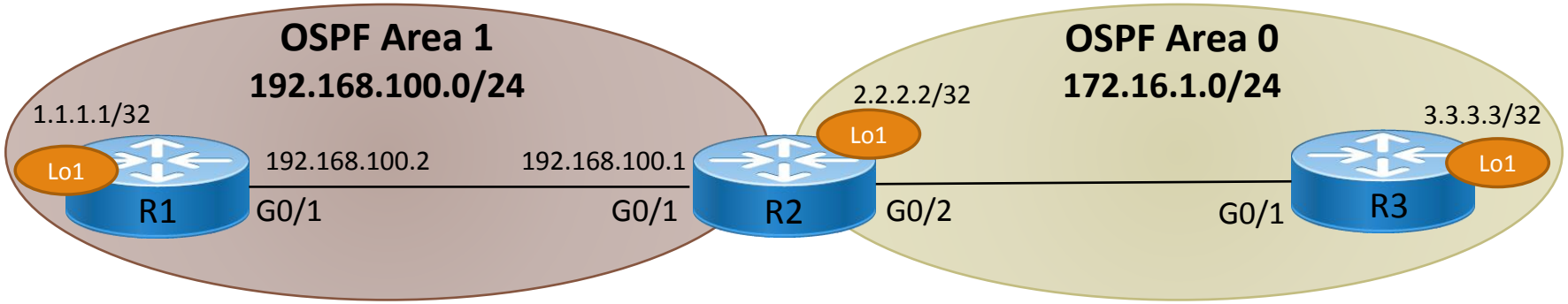

```
R1(config)# interface Lo1
R1(config-if)# ip address  1.1.1.1  255.255.255.255
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# router  ospf  1
R1(config-router)# network  192.168.100.0  0.0.0.255  area  1
R1(config-router)# network  1.1.1.1  0.0.0.0  area 1
```

Configuring Multi-area OSPF with Loopback Example




```
R2(config)# interface Lo1
R2(config-if)# ip address  2.2.2.2  255.255.255.255
R2(config-if)# no shut
R2(config-if)# exit
R2(config)# router  ospf  1
R2(config-router)#network  172.16.1.0  0.0.0.255  area  0
R2(config-router)#network  2.2.2.2  0.0.0.0  area  0
R2(config-router)#network  192.168.100.0  0.0.0.255  area  1
```

Configuring Multi-area OSPF with Loopback Example




```
R3(config)# interface Lo1
R3(config-if)# ip address  3.3.3.3  255.255.255.255
R3(config-if)# no shut
R3(config-if)# exit
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.0 0.0.0.255 area 0
R3(config-router)#network 3.3.3.3 0.0.0.0 area 0
```

OSPF Commands

Command	Description

`interface Loopback 1`
`ip address 1.1.1.1 255.255.255.255`
`no shut`
	Create a loopback interface example

`router ospf <process ID>` `router ospf 1`	Enable OSPF and set the process ID
`router-id <live IP address used to identify the router>` `router-id 1.1.1.1`	Manually choose which interface IP to be the Router ID

`network <connected network> <wildcard mask> area <#>`
`network 1.1.1.1 0.0.0.0 area 0`
`network 77.88.0.0 0.0.255.255 area 0`
`network 66.55.44.0 0.0.0.255 area 1`
	Create network statements

OSPF Show Commands

Command	Description
`show ip protocols`	Display routing protocol configurations
`show ip ospf`	Display OSPF configurations and statistics
`show ip ospf <process ID>`	Display OSPF configurations and statistics for that OSPF process
`show ip ospf interface`	Display information on interfaces participating in OSPF, including timers, their role, and neighbor adjacencies
`show ip ospf neighbor`	Display OSPF neighbors, their ID, role, and synchronization status
`show ip route ospf`	Display any routes in the routing table learned by OSPF
`show ip ospf border-routers`	Display ABR and ASBR information
`show ip ospf database`	Display a summary of the OSPF database

OSPF Debugging Commands

Command	Description
`debug ip ospf adj`	Show ospf neighbor adjacency events as they happen
`debug ip ospf events`	Show all ospf events as they happen
`undebug all`	Turn off debugging

5.9 First Hop Redundancy Protocol (FHRP)

CCNA 200-301 v1.1

Module 5

First Hop Redundancy Protocol (FHRP)

Hot Standby Router Protocol (HSRP)

Virtual Router Redundancy Protocol (VRRP)

Gateway Load Balancing Protocol (GLBP)

First Hop Redundancy Protocol (FHRP)

Reduce routing failures with multiple routers acting together as a single default gateway

- All participating routers share a virtual IP address and a virtual MAC address
- Traffic is sent to the virtual addresses
- The virtual addresses are automatically generated/assigned by the FHRP

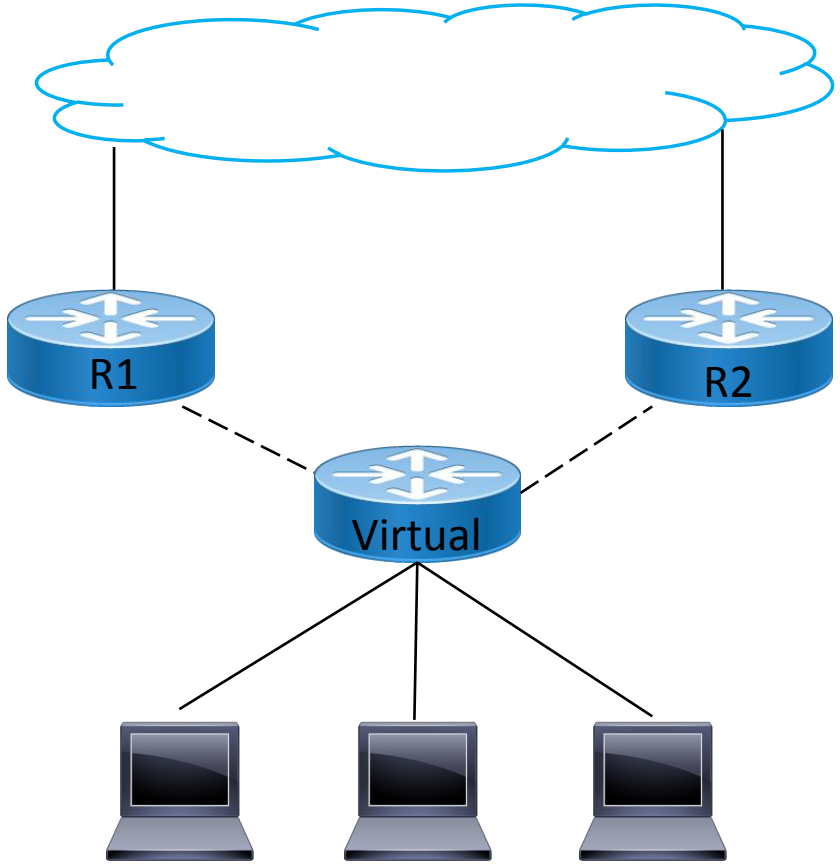
Common use cases:

- Configured on physical routers to provide redundancy for the network's edge
- Configured on Layer 3 switch VLAN interfaces to provide a redundant default gateway for VLAN clients

Common FHRPs include:

- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)

FHRP Example



Hot Standby Router Protocol (HSRP)

Cisco proprietary

Multiple routers share a single virtual IP address and MAC address

- Does not natively support load balancing
- Primarily provides failover capabilities

Clients send traffic to the virtual IP

- It is their default gateway

The active router forwards all traffic sent to the virtual IP

The standby router monitors the active router's status

- It is ready to take over if the active router fails

Virtual Router Redundancy Protocol (VRRP)

IETF non-proprietary standard

Similar to HSRP

Routers to form a group with a virtual IP address

The VRRP master router handles traffic

Backup routers are ready to take over if the master fails

Does not natively support load balancing

It is possible to configure multiple VRRP groups for different subnets to balance traffic manually

Gateway Load Balancing Protocol (GLBP)

Developed by Cisco

Provides both load balancing and redundancy

Multiple routers share the same virtual IP address

GLBP actively balances the traffic load among these routers

The Active Virtual Gateway (AVG) manages traffic distribution

Active Virtual Forwarders (AVFs) forward traffic

All routers can actively forward traffic, allowing load balancing

For more information on FHRP, HSRP, VRRP and GLBP see:
https://www.cisco.com/c/en/us/products/ios-nx-os-software/first-hop-redundancy-protocol-fhrp/index.html

5.10 Network Address Translation (NAT)

CCNA 200-301 v1.1

Module 5

Understanding Network Address Translation (NAT)

NAT Terminology

Overload

NAT Interfaces

NAT Access List

NAT Pool

Configuring Dynamic NAT

Configuring Static NAT

Translating the Other Way

Port Address Translation (PAT)

Managing the NAT Table

NAT Debugging

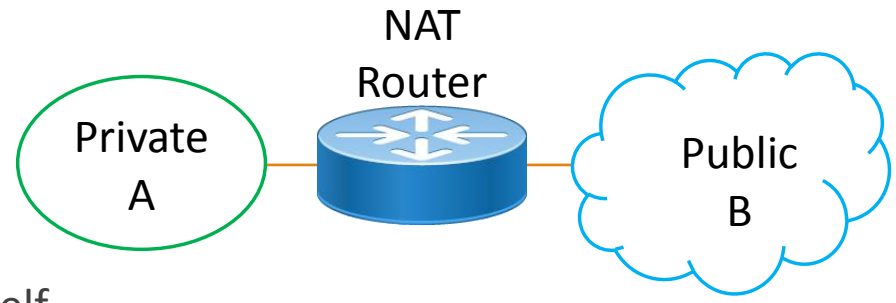
NAT/PAT Commands

Understanding Network Address Translation (NAT)

It all starts when one side has no idea how to send traffic to the other side
- A can send traffic to B
- B doesn't know how to respond back
- Private network has a default gateway to public network
- Public network doesn't use private addresses, so it has no routes back to the private network

We must temporarily change the *private* source address to be a *public* source address
- Whenever you NAT, you are translating SOURCE addresses

Our router acts as a relay between both worlds
- It has one interface on the private side, one on the public side
- As we send traffic out into the world, the router performs NAT
- In the packet's IP header, it replaces the source IP with its own IP



To the world, it looks like the traffic originated from the router itself
- Websites respond back to the router
- The router has a table that keeps track of what it has swapped
- It changes the address back to private
- Routes the packet to the original host

NAT Terminology

Computers

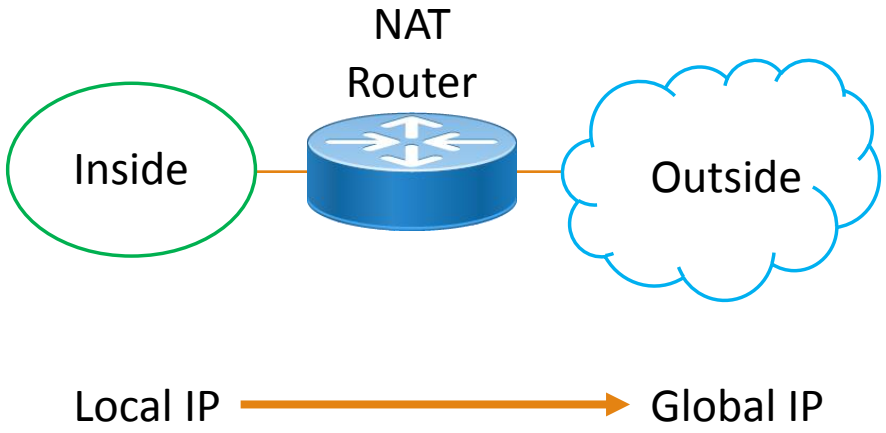
Inside
- The network or device under your control
- Usually the private/internal network
- Where your traffic originates from

Outside
- Refers to the network or device not under your control
- Typically the public Internet

Addresses

Local
- The IP address as it is known within your network
- Typically your untranslated private address

Global
- The IP address as it is known to the outside world
- Your public address after translation
- A website's public IP address



NAT Terminology in Action Example

Inside is translated from Local to Global

Outside is usually not translated

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.0.0.100:1	192.168.1.2:1	10.0.0.254:1	10.0.0.254:1
icmp	10.0.0.100:2	192.168.1.2:2	10.0.0.254:2	10.0.0.254:2
icmp	10.0.0.100:3	192.168.1.2:3	10.0.0.254:3	10.0.0.254:3
icmp	10.0.0.100:4	192.168.1.2:4	10.0.0.254:4	10.0.0.254:4

Us Translated

Us Original

Us

Them Translated

Them Original

Them

NAT Configuration Steps

1. Specify which is the inside interface
   - Connected to the private network
   - Has a local IP address
2. Specify which is the outside interface
   - Connected to the public network
   - Has a global IP address
3. Specify NAT type
   - Static
     - One-to-one constant mapping
     - Good for “publishing” inside servers to the outside world
   - Dynamic
     - Borrow from a pool of global addresses
     - When inside host closes the session, the global address is returned to the pool
     - Also create an access list to restrict which local addresses can be mapped

Overload

Turns NAT into PAT (port address translation)

NAT command keyword specifying that multiple local addresses can use the same global address

- Inside clients are differentiated by their TCP or UDP source port

Can be used directly when there is only one global address

Or can be used when the a pool runs out of global addresses

- Inside clients share the last available global address

NAT Interfaces

The router interfaces that will participate in NAT

Specify the inside interface

Router(config)# interface g0/1

Router(config-if)# ip nat inside

Specify the outside interface

Router(config)# interface g0/0

Router(config-if)# ip nat outside

NAT Access List

A standard access list that specifies which IP addresses are permitted to be translated

```
access-list < 1 – 99 > permit < source IP address> < wildcard mask >
```

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

NAT Pool

A group of global addresses that can be used for translation

- Typically provided by ISP

ip nat pool < name > < start_address end_address > {netmask <subnet mask> | prefix-length < bits >}

Router(config)# ip nat pool MY_POOL 203.0.113.2 203.0.113.62 netmask 255.255.255.192

Router(config)# ip nat pool MY_POOL 203.0.113.2 203.0.113.62 prefix-length 26

Configuring Dynamic NAT

NAT syntax has many variables

- More variables are added depending on your choices
- Can get confusing

ip nat [inside | outside] source [list | static] …

ip nat inside source list < ID > [interface | pool] < name > overload

ip nat inside source list 1 interface g0/0 overload

ip nat inside source list 1 pool my_pool overload

- Use PAT on the last global address

Configuring Static NAT

Specify a static one-to-one mapping that will forever remain in effect

No need for overload

Perfect for when you want to publish an inside server to the outside world

Internet clients send traffic to the global IP to access the server

ip nat [inside | outside] source [list | static]

Router(config)# ip nat inside source static <local IP> <global IP>

Router(config)# ip nat inside source static 192.168.1.10 203.0.113.10

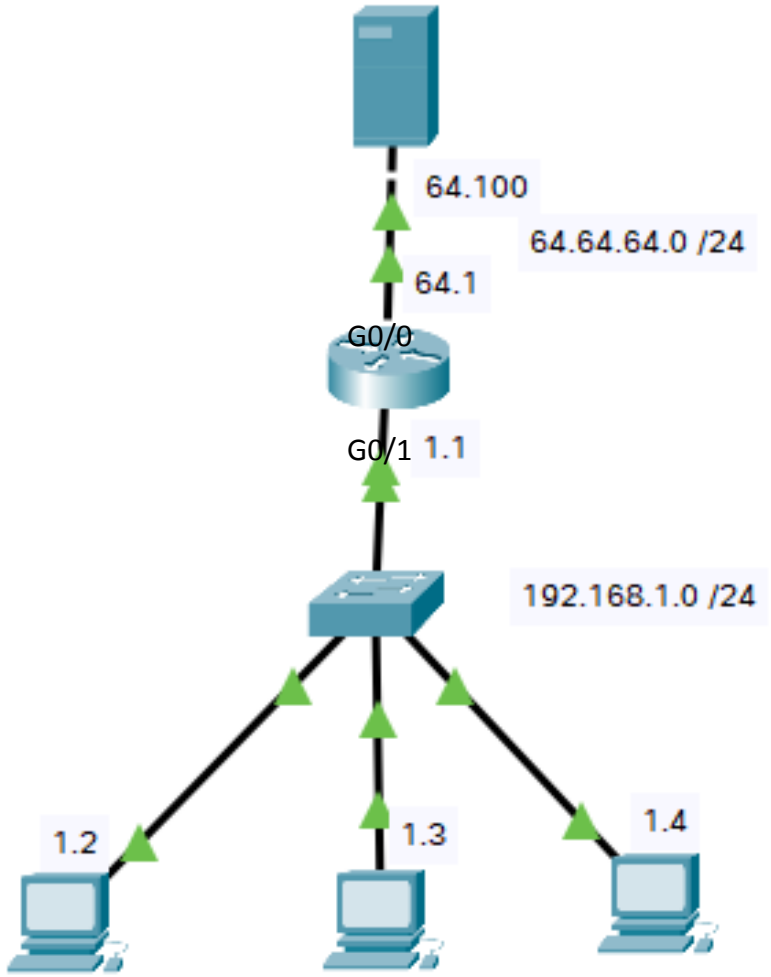
Static NAT Example

```
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)# exit

Router(config)# interface GigabitEthernet0/2
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config-if)# ip nat outside
Router(config-if)# exit

Router(config)# ip nat inside source static 192.168.1.10 203.0.113.10
```

Typical NAT Example



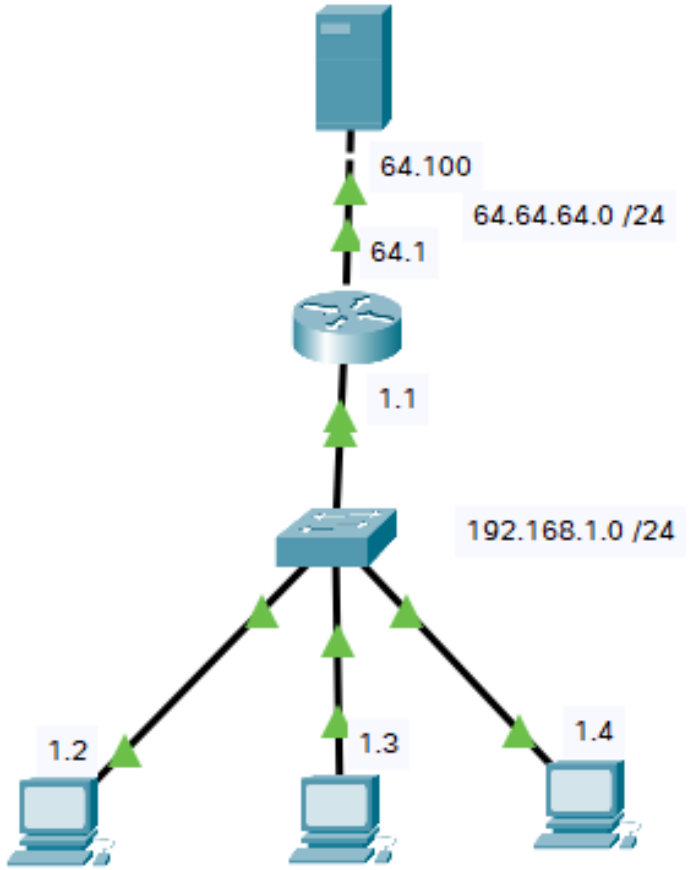

```
Router> enable
Router# configure terminal

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)# 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)# 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 overload
Router(config-if)# end
Router# copy running-config startup-config
```

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
```

Translating the Other Way

In most cases, NAT is only performed on traffic that originates from the inside private network

- Inside Local → Inside Global
- Traffic that originates from the outside public network is usually not translated

However, you might have a (rare) situation where you need to translate from outside to inside

- Outside Global → Outside Local
- Outside clients need to come in to your network
- *They* may have a route to *you*, but *you* don't have a route to *them*
- You have no need to communicate with them
- They might sometimes want to communicate with you
- The outside needs to change their source IP to come in
- The inside never needs to change in any way
- You change *their* source IP from global to local
- Their traffic looks to you like it came from the inside (router's inside interface)
- You respond to the router, which translates back to their address and relays response to them

Remember:
You are always on the inside no matter how NAT is configured

Outside – In NAT Example

```
# Configure the outside interface
interface GigabitEthernet0/0
 ip address 200.200.200.1  255.255.255.0
 ip nat outside
 no shutdown

# Configure the inside interface
interface GigabitEthernet0/1
 ip address 192.168.1.1  255.255.255.0
 ip nat inside
 no shutdown
```

Outside – In NAT Example (cont'd)

Create an access list to allow certain global addresses to be translated to local
- Which outsiders are allowed to come in

Router(config)# access-list 2 permit ip 203.0.113.0 0.0.0.255

Define a NAT pool for translation
- These are local addresses that outsiders will borrow as their traffic comes in
- Make sure they don't conflict with inside addresses you are already using

Router(config)# ip nat pool my_local_address_pool 192.168.1.200 192.168.1.250 netmask 255.255.255.0

Configure NAT using the outside source list, translating to the local address pool

Router(config)# ip nat outside source list 2 pool my_local_address_pool

Port Address Translation (PAT)

AKA “overload”

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 same public IP address

Because multiple sessions are using the same public IP, each session must be distinguished by a different source TCP or UDP port

During translation, the router attempts to retain the client’s original source port

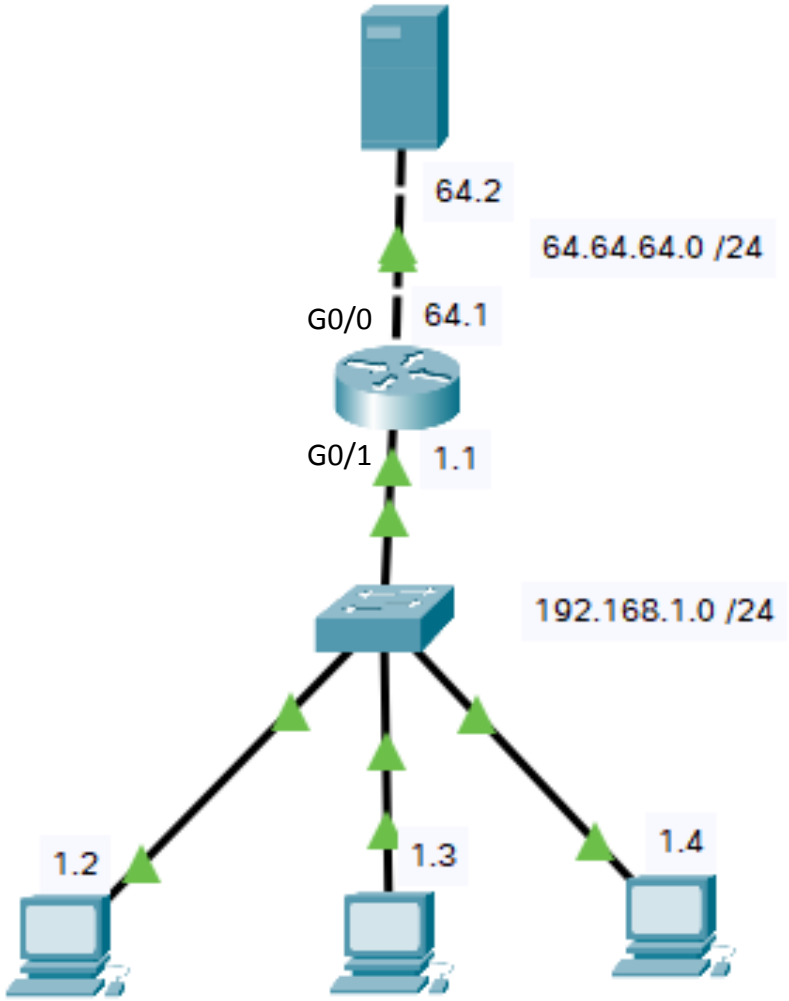
If another client is already using that port, the router will increment the source port

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

Destination IP addresses and ports (Outside Global) are not changed

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 on the last public IP

PAT Configuration Example




```
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 running-config startup-config
```

Managing the NAT Table

You can view or clear the NAT table

```
show ip nat translations

show ip nat statistics

clear ip nat translation
```

```
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
```

NAT Debugging

You can watch NAT events in real time

```
debug ip nat
undebug ip nat
undebug all
```

```
Router# debug ip nat
IP NAT debugging is on

*Aug 31 12:34:56.123: NAT: s=192.168.1.10->203.0.113.10, d=198.51.100.5 [25]
*Aug 31 12:34:56.126: NAT: s=203.0.113.10, d=198.51.100.5->192.168.1.10 [25]
*Aug 31 12:34:57.456: NAT: s=192.168.1.11->203.0.113.11, d=198.51.100.6 [80]
*Aug 31 12:34:57.459: NAT: s=203.0.113.11, d=198.51.100.6->192.168.1.11 [80]
*Aug 31 12:34:58.789: NAT: s=192.168.1.12->203.0.113.12, d=198.51.100.7 [443]
*Aug 31 12:34:58.792: NAT: s=203.0.113.12, d=198.51.100.7->192.168.1.12 [443]
```

NAT Commands

Command	Description
ip nat inside	Specifies this interface is on the inside
ip nat outside	Specifies this interface is on the outside
access-list < 1 – 99 > permit < source IP> < wildcard mask > access-list 1 permit 192.168.1.0 0.0.0.255	Create a standard access list allowing specified local addresses to be translated to global
ip nat pool < name > < start_address end_address > {netmask <subnet mask> | prefix-length < bits >} Router(config)# ip nat pool MY_POOL 203.0.113.2 203.0.113.62 netmask 255.255.255.192 Router(config)# ip nat pool MY_POOL 203.0.113.2 203.0.113.62 prefix-length 26	Create a pool of global addresses that can be used for translation

NAT Commands (cont'd)

Command	Description
ip nat inside source list < ID > [interface | pool] < name > overload ip nat inside source list 1 interface g0/0 overload ip nat inside source list 1 pool my_pool overload	Enable PAT using an access list to permit certain inside clients to be translated PAT using one global address PAT using global addresses from a pool
ip nat inside source static <inside IP> <outside IP> ip nat inside source static 192.168.1.10 203.0.113.10	One-to-one static mapping
ip nat outside source list <ID> pool <name> ip nat outside source list 2 pool my_local_address_pool	Enable outside-in NAT

Verifying NAT

Command	Description
`show ip nat translations`	Display the NAT table
`show ip nat statistics`	Display usages statistics for the NAT interfaces, access list and pool
`clear ip nat translations`	Clear the NAT table
`debug ip nat`	Debug NAT events
`no debug ip nat`	Stop debugging NAT events
`undebug ip nat`	Stop debugging NAT events
`undebug all` `u all`	Stop all debugging

5.11 Review

CCNA 200-301 v1.1

Module 5

Review

Review

A router is a device that makes forwarding decisions based on layer 3 IP addresses

The router builds a route table to determine the best path

A router will replace or rewrite a packet's Layer 2 header before it sends the packet out to the next segment

A router that connects a network to the outside world is called the default gateway

In most cases you would hard code the IP address on each router interface

It is possible to configure router interfaces for DHCP

Review (cont’d)

Routing is the process of moving a packet from one network to the next

Routing is performed by routers

Routers read the Layer 3 destination address to determine what to do with a packet

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

Routers themselves can sometimes be the final destination

Review (cont’d)

Static routing is when an administrator manually enters routes into the router

Static routing should only be performed when you have very few routes with no redundancy

Static routing has the benefit of using fewer resources on the router

Static routing has the disadvantage of requiring the administrator to know their network topology very well, and to manually update all routers in case the topology changes

Review (cont'd)

A floating static route is one that acts as a backup route
- It only takes effect if the primary route fails
- You manually configure it giving it a higher administrative distance than the normal routes

A host route directs traffic to a single host, rather than to an entire network
- In IPv4, the host route will have a subnet mask of /32 or 255.255.255.255
- A host route in IPv6 will have a prefix of /128

A default route is also known as the Gateway of Last Resort
- It is the route that is taken when there is no other choice with only one possible exit for the traffic to take

VLAN routing is the act of routing between VLANs
- Each VLAN should also have its own subnet ID
- The only way you can route between VLANs is to connect the VLAN to a router interface
- In most cases, that router interface will be a virtual interface called a VLAN interface that resides on a multi-layer switch

Review (cont'd)

The Golden Rule of Routing is that a router must know what to do with a packet

- If it does not have an entry for the destination in its route table, or if it does not have a default route, the router will drop the packet and send an ICMP unreachable message to the sender
- If you configure static routing, you must put an appropriate route in every hop along the path

The second Golden Rule of routing is that the router must be able to choose which interface to send the packet out of

- Each router interface must belong to a different network

Review (cont'd)

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

Layer 2 source and destination MAC addresses change with each network segment

- Before a host on an Ethernet or Wi-Fi network can even send a packet to its neighbor or to the default gateway, it must know the MAC address of that router or host
- It will perform an ARP broadcast to find the MAC address of the next top

Layer 3 IP addresses do not change along the entire path

- The exception is using NAT or PAT to translate from private to public IP addresses and back

A host will use its subnet mask to determine if the destination is on the same network or a different network

If the destination network is different, the host will pass the packet to its default gateway

The default gateway will look in its route table to determine the next router it should pass the packet to

In some cases the destination is directly connected to the default gateway's other interface

Review (cont'd)

When routing across a single router, the networks will be directly connected to the various router interfaces

If you send a packet across a router, and you expect a reply of some kind (such as with TCP or ping) hosts on both sides of the router must know the IP address and MAC address of their local router (default gateway) interface

If you send a packet across multiple routers, the routers relay the packet from hop to hop until it reaches its final destination

At each hop, the source and destination MAC addresses will change with each router pair, but the source and destination IP addresses will stay the same from end to end

Review (cont’d)

A routed protocol is the user traffic such as IP

A routing protocol is the language that routers use to compare and update each other's route tables

Routing Protocols are dynamic; routers regularly update each other as the network changes

A router can use more than one routing protocol for compatibility

Examples of routing protocols include RIP, OSPF, EIGRP and BGP

There are four basic routing protocol types: Distance Vector, Link State, Hybrid and Path Vector

Review (cont’d)

Distance Vector routing protocols determine how far a destination is and in what direction

In Distance Vector, routers update each other on a fixed interval

Distance Vector routing protocols are good for small networks and are easy to implement, but have slow convergence

RIP is a classic example of a Distance Vector routing protocol

Review (cont'd)

With Link State routing protocols, each router maintains a database of the entire network including all routes

Routers do not update each other until a link changes state

Link state routing protocols require a carefully planned, hierarchical network to be efficient

Configuring a Link State routing protocol can be complex

The Link State topology database requires extra resources from the router

Because each router already has a full topology map of the network, routers can quickly choose an alternate route should the original route go down

Convergence between routers is also very fast

Examples of Link State routing protocols include OSPF and IS-IS

Review (cont’d)

A hybrid routing protocol uses the best features of both Distance Vector and Link State

It has very fast convergence

It's excellent for large internal networks that grew organically and were not well designed

It's easy to implement

EIGRP is an example of a hybrid routing protocol

EIGRP is Cisco proprietary

It makes routing decisions based on bandwidth plus delay
- If you wish, you can also factor in load, reliability, and MTU as desired

It has two path cost concepts: Advertised Distance and Feasible Distance

Advertised distance is the cost from your neighbor to the destination

Feasible distance is the cost from you to your neighbor PLUS your neighbor's advertised distance
- In other words, the total cost from you to the final destination

Review (cont'd)

Path Vector routing protocols are a variation on Distance Vector

In Path Vector, a hop is not a single router but rather is an entire autonomous system

- An autonomous system is a network that is under a single administrative umbrella, such as a telecom or a company

Path Vector routing Protocols are used on the Internet between ISPs and other autonomous systems

Path Vector routing is complex to implement and very slow to converge

BGP is the Path Vector routing protocol that we use on the internet today

- It uses many attributes to make forwarding decisions

Review (cont'd)

A router may or may not have multiple routes to choose from

A routing table in a Cisco router will have certain types of information including:

- Routing protocol code, which indicates the source that provided the route (can be a routing protocol, a directly connected link, or statically entered)
- Prefix, which is the destination network ID
- Network mask, which is the subnet mask used on the destination network
- Next hop, which is the next router to hand the packet to
- Administrative distance, which is the believability or desirability of a route based on its source
- Metric, which is the cost of a route within a single routing protocol
- Gateway of Last Resort

A router has three criteria for choosing the best route to a destination:

- prefix length
- administrative distance
- metric

Review (cont'd)

Routers choose the best route based on three criteria, in this order:

- Longest prefix match
- Administrative distance
- Routing protocol metric

If there are multiple routes to the same destination, the route with the longest prefix match is chosen

- This means the longest subnet mask used by the destination network (most binary 1's in the subnet mask)
- Network destinations with a longer prefix are more specific
- The network will be smaller with fewer nodes, thus bringing you closer to the final destination

Review (cont'd)

If there are two routes that have the same prefix length, then the best (lowest) administrative distance is chosen

Cisco has the following administrative distances:

- Directly connected = 0
- Statically entered by an administrator = 1
- Exterior BGP = 20
- EIGRP = 90
- OSPF = 110
- RIP = 120
- An unreachable route is set to 255

Review (cont’d)

If there are two routes that come from the same source, then the metric as per that routing protocol is the final deciding factor

Different routing protocols have different metrics

RIP is based solely on hop count regardless of the speed of the link

OSPF is based on cumulative link cost from hop to hop to the final destination

EIGRP is based on bandwidth plus delay

- You can optionally add reliability, loading and MTU as desired

Review (cont'd)

OSPF is a widely used Link State Interior Gateway protocol

It works well with VLSM, but requires the network to be hierarchical and well-designed to be efficient

OSPF routers update each other only when a link changes state

Every router maintains its own OSPF database
- Contains the complete topology for that area

If a router needs to find a new path to a destination, the router can simply refer to its own database to find that route

OSPF divides the entire network into areas

Each area is a grouping of network IDs that can be aggregated together

Area border routers (ABRs) connect areas to the backbone area (Area 0)

Areas only speak to each other through the backbone

An autonomous system boundary router (ASBR) connects Area 0 to the Internet or other networks

Review (cont'd)

An OSPF neighbor is a directly connected router also running OSPF

Routers must be in the same OSPF area to become neighbors

Neighbors form relationships among themselves called adjacencies

OSPF routers identify themselves to their neighbors using a Router ID

The router ID will be chosen based on this order:

1. The admin manually configured the Router ID, in the format of an IPv4 address
2. The numerically highest IP address of any loopback interface on that router
3. The numerically highest IP address of any live physical interface on that router

Physical interfaces are the least desirable to use for Router IDs because if the link goes down, the Router ID is no longer valid and the router will need to choose a new Router ID

Review (cont'd)

On every multi-access Ethernet segment, OSPF routers will hold an election to determine the Designated Router (DR) and the Backup Designated Router (BDR)

The router with the highest Router ID will become the DR

The router with the second highest Router ID will become the BDR

On point-to-point WAN links, routers compare their Router IDs to determine which router is the master and which one is the slave

On an Ethernet segment, the DR acts as the central point of communication for all OSPF router updates

If any router on that segment receives an update, it sends a multicast Link State update (LSU) to the DR and BDR

The DR in turn repeats that LSU out another multicast address for all the other routers to receive

Review (cont'd)

The LSU is an envelope that carries one or more Link State Advertisements (LSAs)

The LSA is the actual route update

Routers that do not win the election are known as DROther

DROther routers do not establish adjacencies with other DROther routers

- They only establish adjacencies with the DR and BDR

If both the DR and BDR fail, the DROther routers will hold a new election to select a new DR and BDR

On a point-to-point link, the master and slave routers send LSUs to each other's unicast address, with the master managing the process

Review (cont'd)

OSPF routers uses HELLO timers to send keep alive packets to each other

The HELLO and other timers on all OSPF routers must be the same for adjacencies to form

OSPF uses the concept of a wild card mask to indicate a range of IP addresses on a network segment

The wild card mask is the inverse of the subnet mask used by that destination segment

- For example, if the subnet mask for that network is 255.255.255.0, the wildcard mask will be 0.0.0.255

Review (cont’d)

You can configure a loopback interface on a router with an IP address

The preferred subnet mask for a loopback address is /32, or 255.255.255.255

You can advertise the loopback as a network destination to other routers

- This allows you to make remote connections to the loopback to administer the router as opposed to making a connection to a physical interface which might go down

Review (cont'd)

A first hop redundancy protocol (FHRP) is one in which several routers share a virtual IP address and a virtual MAC address for redundancy's sake

- User traffic is sent to the virtual addresses

The virtual addresses are automatically generated and assigned by the FHRP

Hot standby router protocol (HSRP) is a Cisco proprietary protocol in which there is an active router and a standby router

- The standby router does not load balance, but it is ready to take over if the active router fails

Virtual Router Redundancy Protocol (VRRP) Is a vendor neutral standard similar to HSRP

- Routers form a group with a virtual IP address
- The VRRP Master router handles the user traffic
- Backup routers are ready to take over if the master fails
- It does not natively support load balancing

Review (cont’d)

Gateway Load Balancing Protocol (GLBP) was developed by Cisco to provide both load balancing and redundancy

- Multiple routers share the same virtual IP address
- The Active Virtual Gateway (AVG) manages traffic distribution
- Active Virtual Forwarders (AVFs) forward traffic
- All routers can actively forward traffic, allowing load balancing

Review (cont'd)

Network Address Translation (NAT) is a dynamic IP address translation mechanism in which a router will translate a local address to a global address

The local address is typically a private IP address from the internal network

The global address is typically a public IP address for use on the Internet

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

As outside hosts respond to the client, the router translates the public global address back to the original private local address

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

- The translation is one to one

Review (cont’d)

In most NAT scenarios, the translation goes from Local to Global

In some cases, you might need to NAT in the other direction, from Global to Local

To configure outside-in NAT, change the NAT statement from **ip nat inside** to **ip nat outside**

Review (cont'd)

Port Address Translation (PAT) Is a variation of NAT in which a router has only one outside address

To turn NAT into PAT, use the keyword **overload** at the end of the NAT statement

Instead of one to one mapping an internal IP address to an external IP address, all internal clients share the same public IP address

- But their sessions are given different port numbers

The router will attempt to retain the original TCP or UDP source port as part of the mapping

- If the source port is already taken by some other client, then the router will assign a new source port to the new mapping

As replies come back from external host to the router, the router translates the IP address and port combination back to the that of the original inside host

- The router then sends the packet to the original source

In PAT, destination addresses and ports are typically not modified