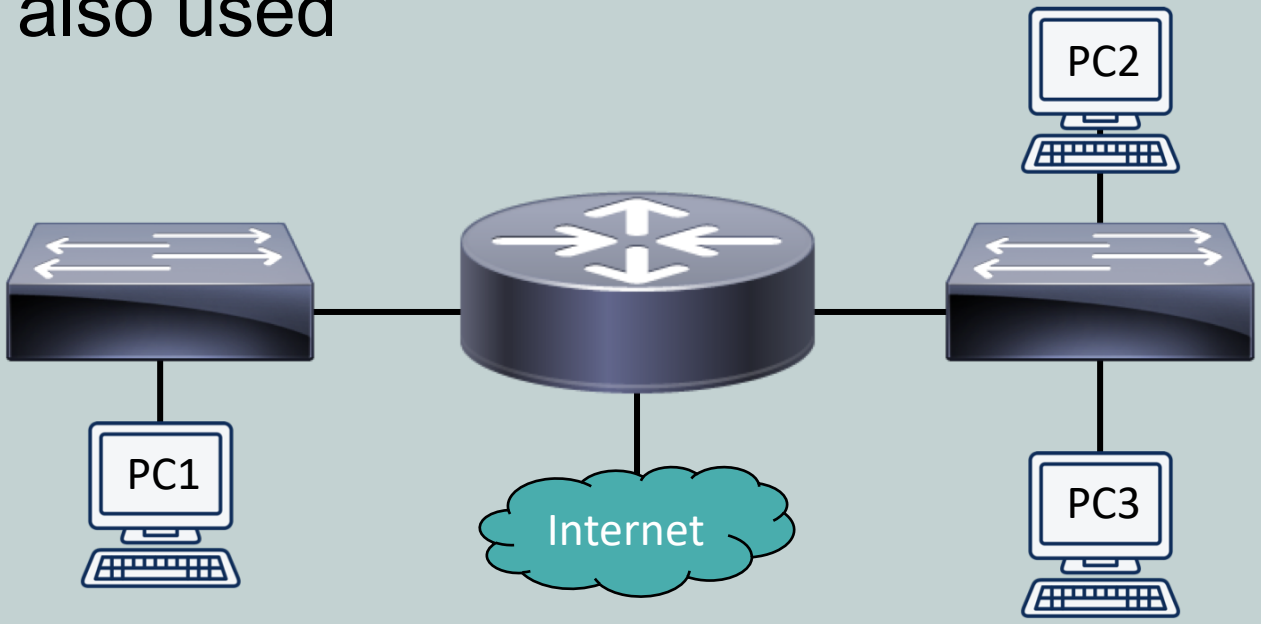
Routing Fundamentals

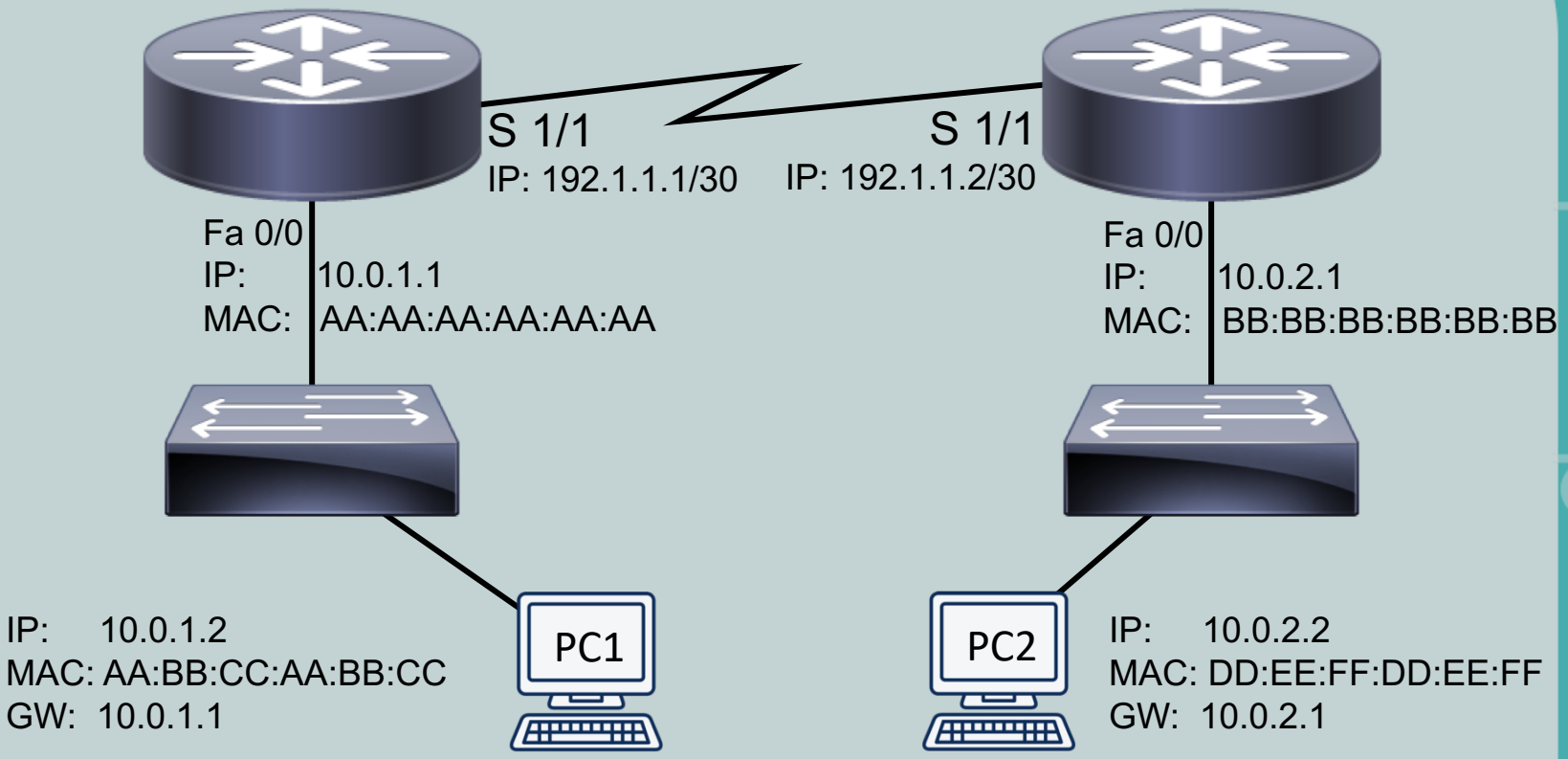
CompTIA Network+ (N10-007)

Routing Fundamentals

- Traffic is routed to flow between subnets
- Each subnet is its own broadcast domain
- Routers are the layer 3 devices that separate broadcast domains, but multilayer switches are also used

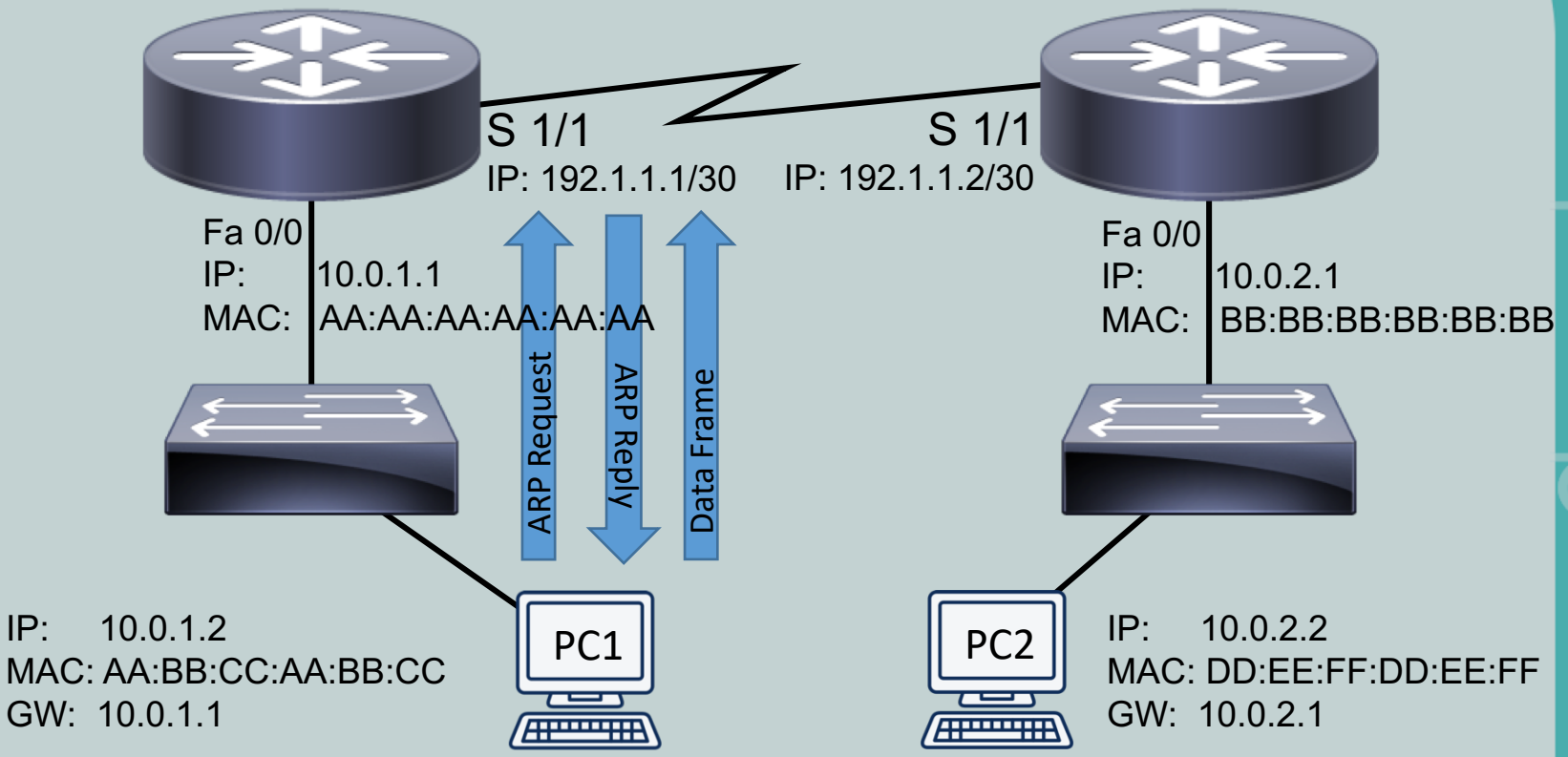


Basic Routing Process



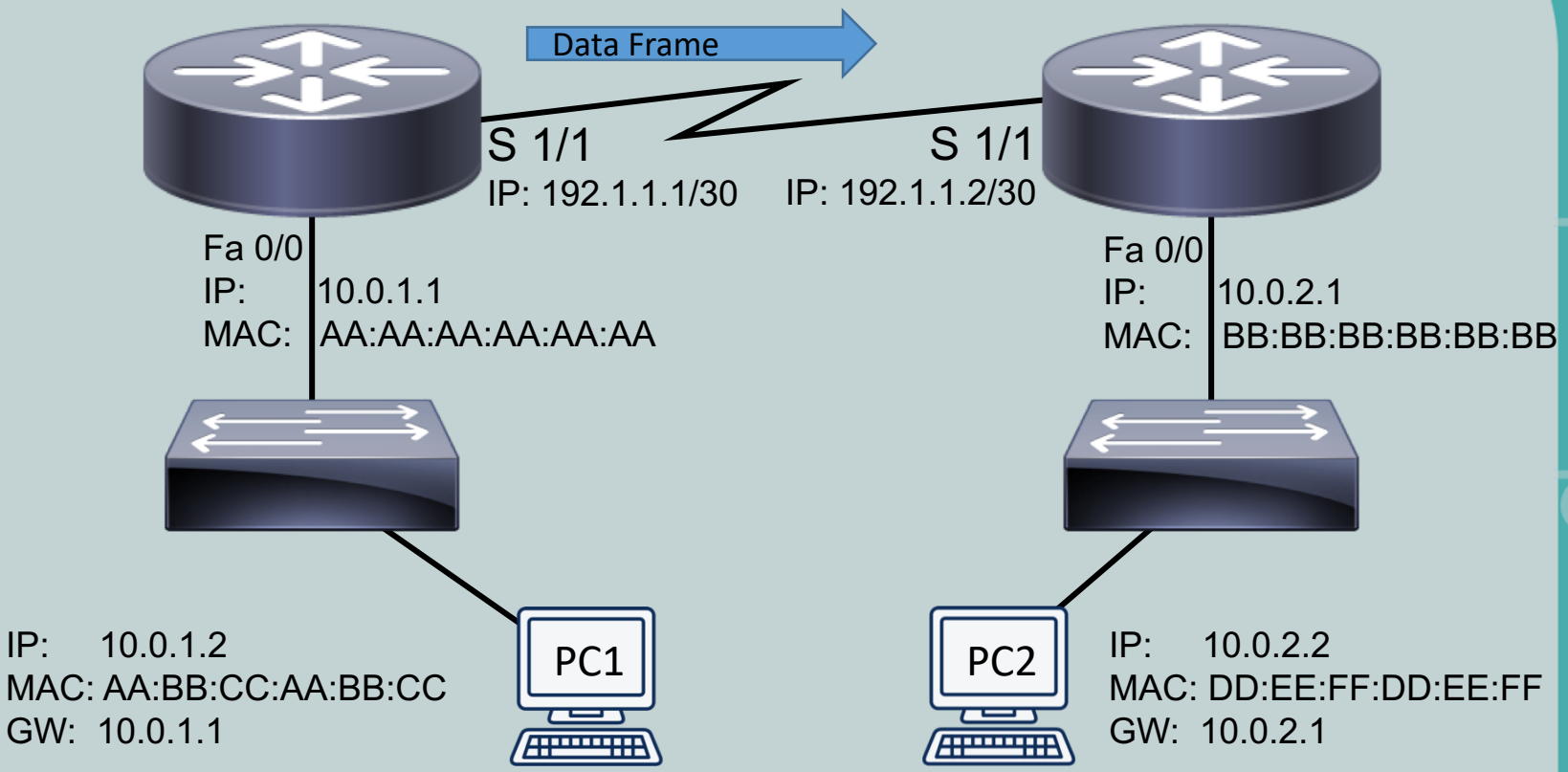
How does a packet from a source IP address of 10.0.1.2 (PC1) route to a destination IP address of 10.0.2.2 (PC2)?

Basic Routing Process



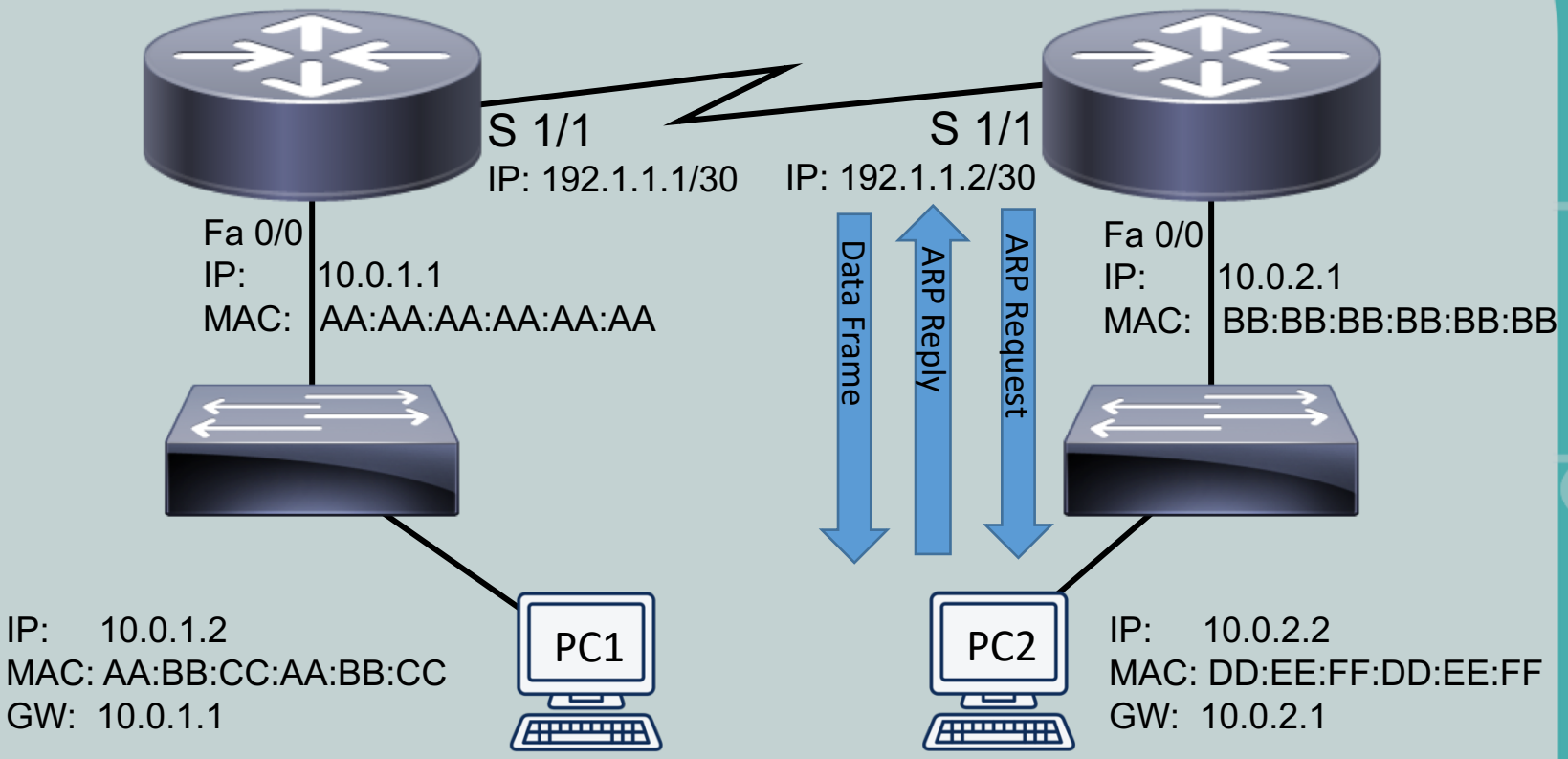
PC1 needs to determine MAC address of router, sends an ARP request, receives ARP reply, then forwards data frame to router's MAC address

Basic Routing Process



Router 1 receives data frame from PC1 and looks at the IP header. Determines best path by looking at routing table, decreases TTL by 1, and forwards data frame via Serial 1/1 (best route).

Basic Routing Process



Router 2 receives the data frame, it decreases TTL by 1. If TTL isn't 0, looks at IP header to determine destination network. If on Router 2's network, Router 2 sends ARP request to find destination (Server 1), receives reply, forwards data frame to Server 1's MAC address. If not, Router 2 forwards it to next Router.

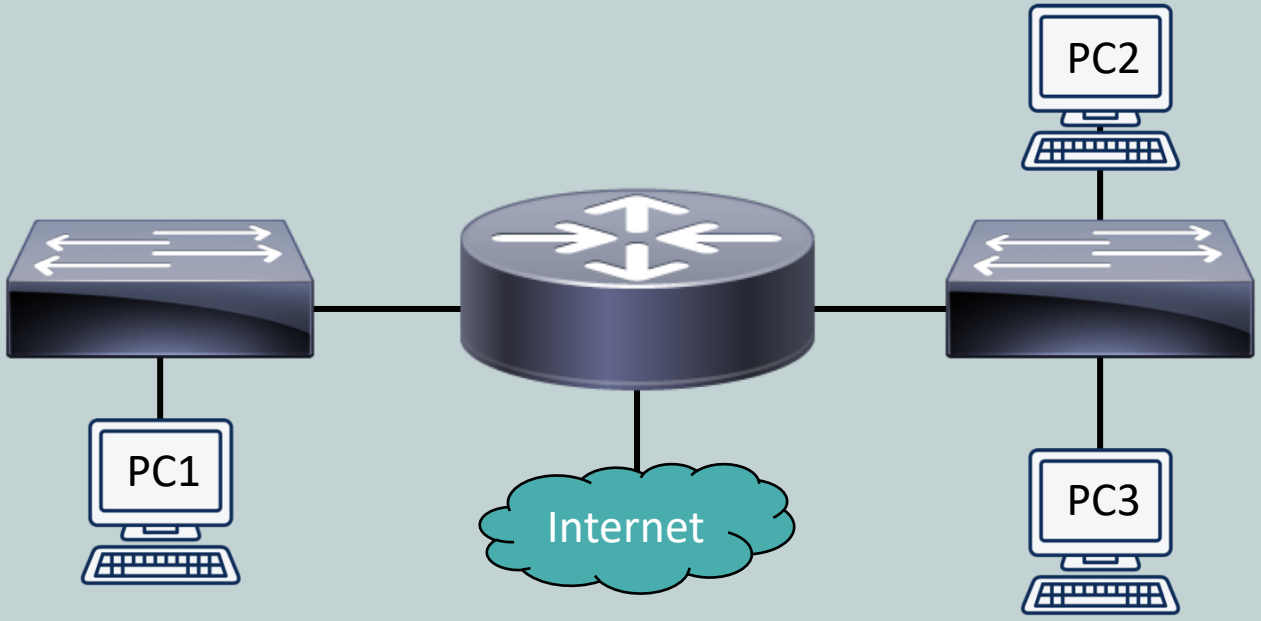
Routing Tables

CompTIA Network+ (N10-007)

Routing Decisions

- Layer 3 to Layer 2 Mapping
  - Router's use ARP caches to map an IP address to a given MAC address

- Make packet-forwarding decisions based upon their internal routing tables



Routing Tables

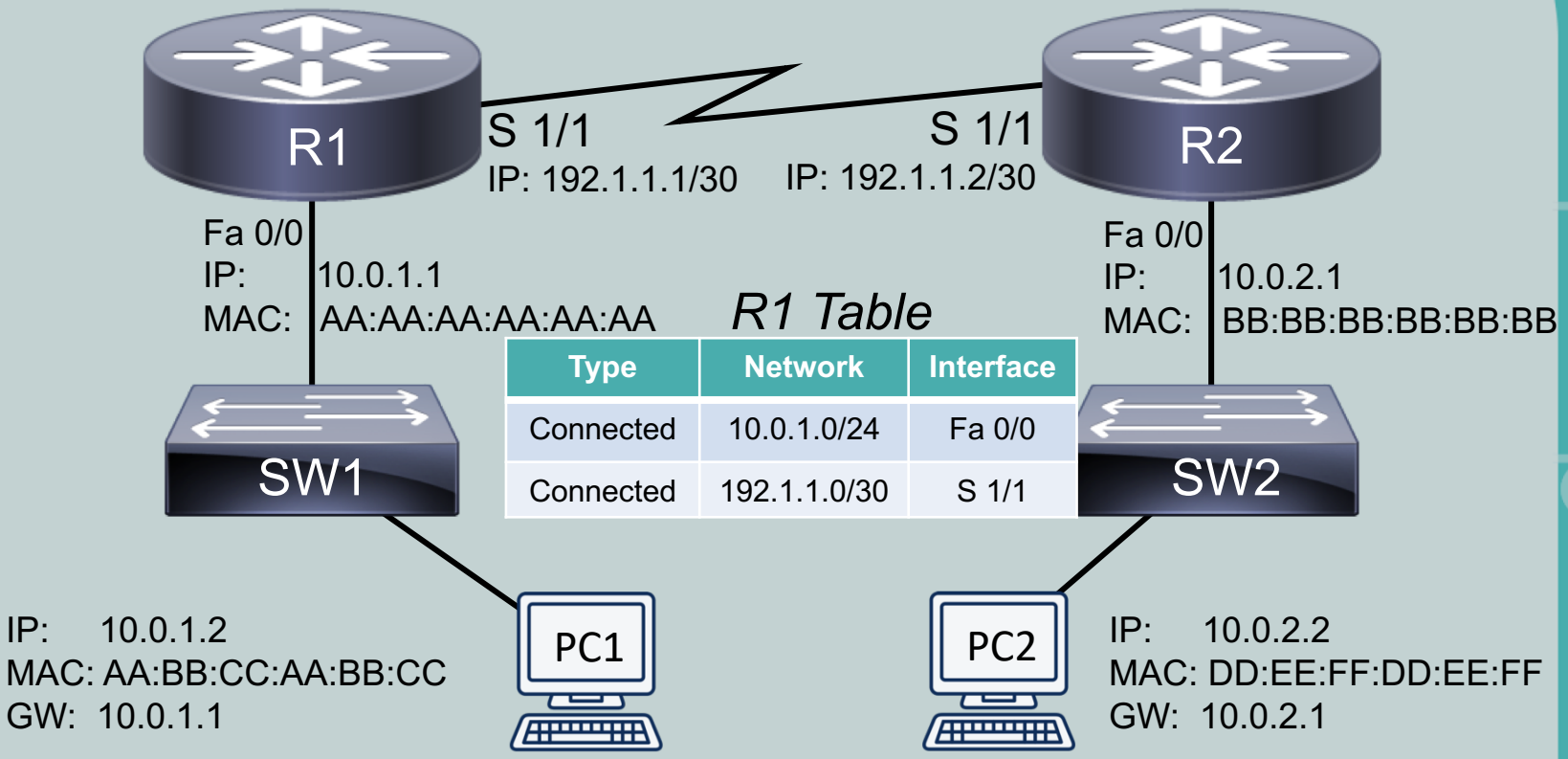
- Table kept by the router to help determine which route entry is the best fit for the network
- A route entry with the longest prefix is the most specific network
- 10.1.1.0/24 more specific than 10.0.0.0/8

Destination Network	Next Router	Port	Route Cost
125.0.0.0	137.3.14.2	1	12
161.5.0.0	137.3.6.6	1	4
134.7.0.0	164.17.3.12	2	10

Sources of Routing Information

- Directly Connected Routes
  - Learned by physical connection between routers
- Static Routes
  - Manually configured by an administrator
  - *Default static route (0.0.0.0/0)* is a special case
    - *"If I don't know where, then send out default static route."*
- Dynamic Routing Protocols
  - Learned by exchanging information between routers

Directly Connected Routes



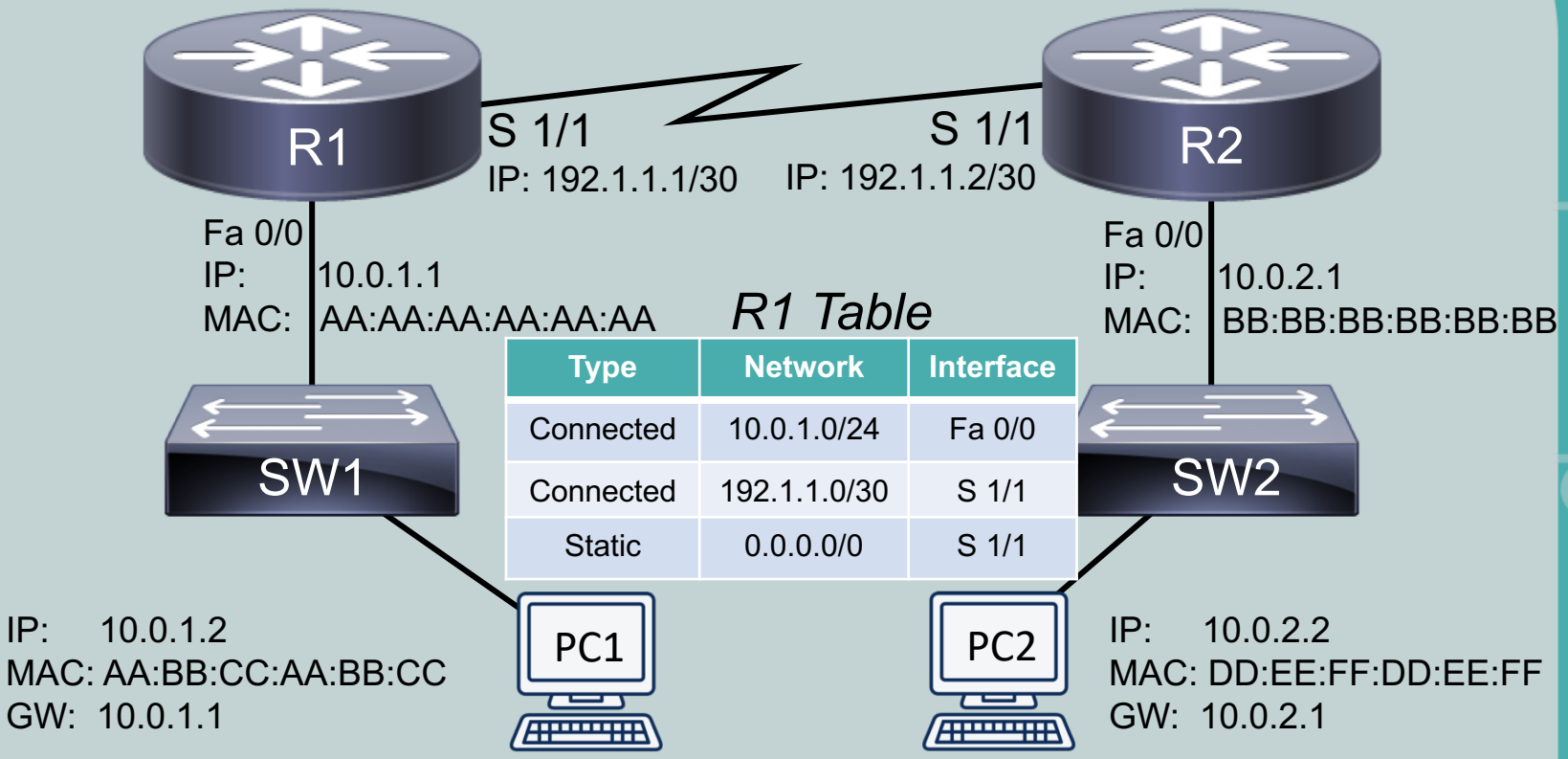
R1 Table

Type	Network	Interface
Connected	10.0.1.0/24	Fa 0/0
Connected	192.1.1.0/30	S 1/1

A router knows how to reach a destination because it has an interface directly participating in a network.

R1 knows how to connect to 10.0.1.0/24 network, since FastEthernet 0/0 is directly connected.

Static Routes



R1 Table

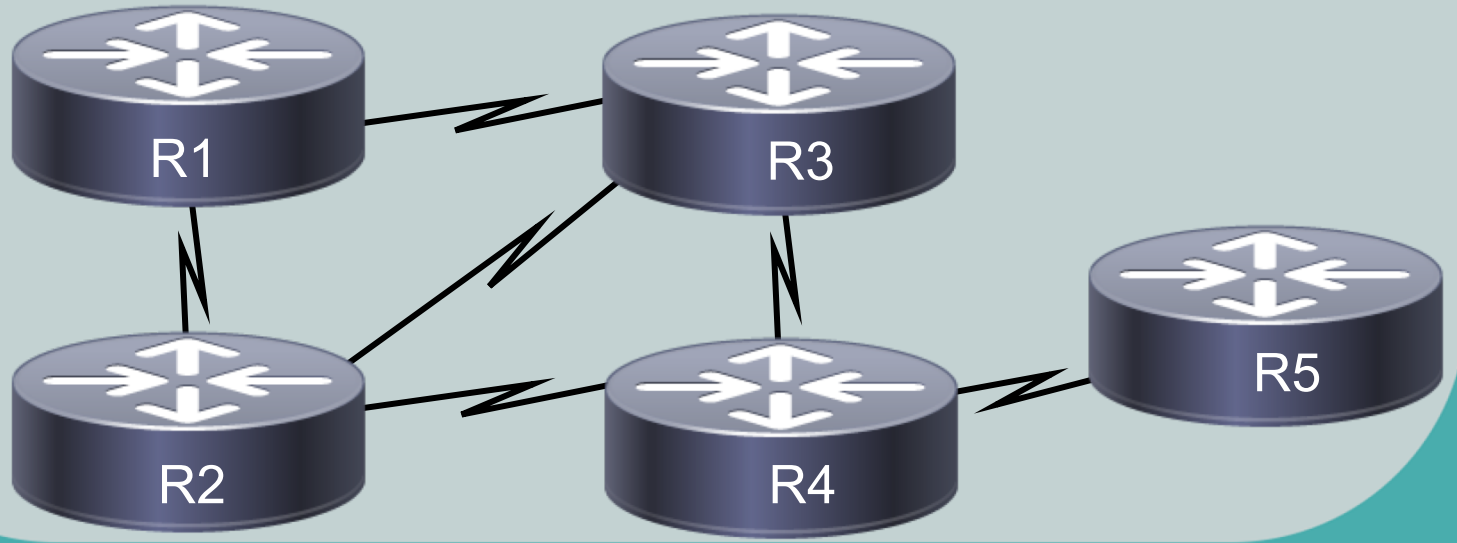
Type	Network	Interface
Connected	10.0.1.0/24	Fa 0/0
Connected	192.1.1.0/30	S 1/1
Static	0.0.0.0/0	S 1/1

A router knows how to reach a destination because the route has been statically (manually) configured by an administrator.

A *default static route* is a special route that states, “If traffic is not destined for a network currently in the routing table, send that traffic out this interface (like Serial 1/1 of Router 1).

Dynamic Routing Protocols

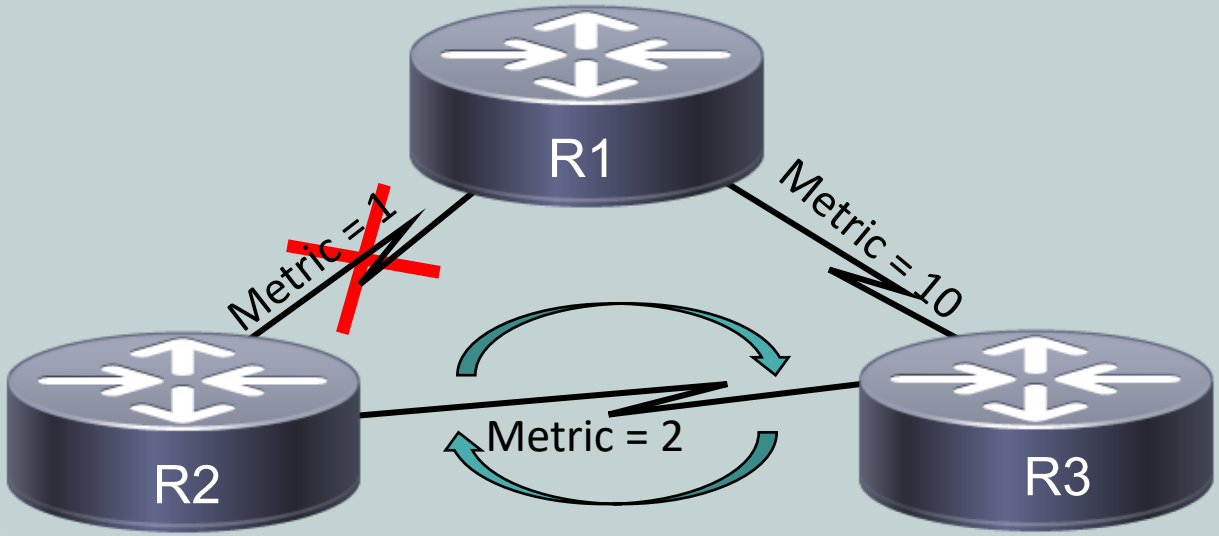
- More than one route can exist for a network
- Different protocols consider different criteria when deciding which route to give preference
- Based on number of hops (hop count in RIP), link bandwidths (OSPF), or other criteria



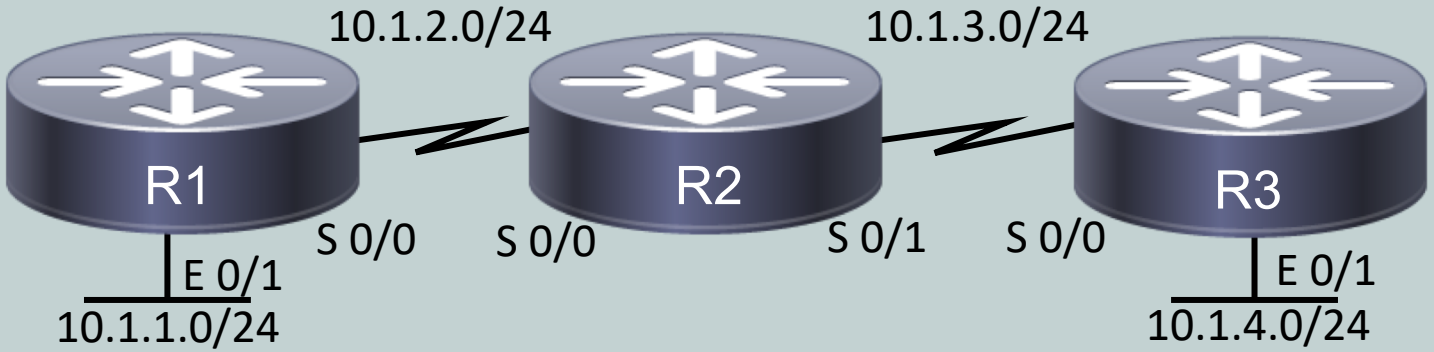
Preventing Routing Loops

- Split horizon
  - Prevents a route learned on one interface from being advertised back out of that same interface

- Poison reverse
  - Causes a route received on one interface to be advertised back out of that same interface with a metric considered to be infinite



Routing Loops



R2 Routing Table

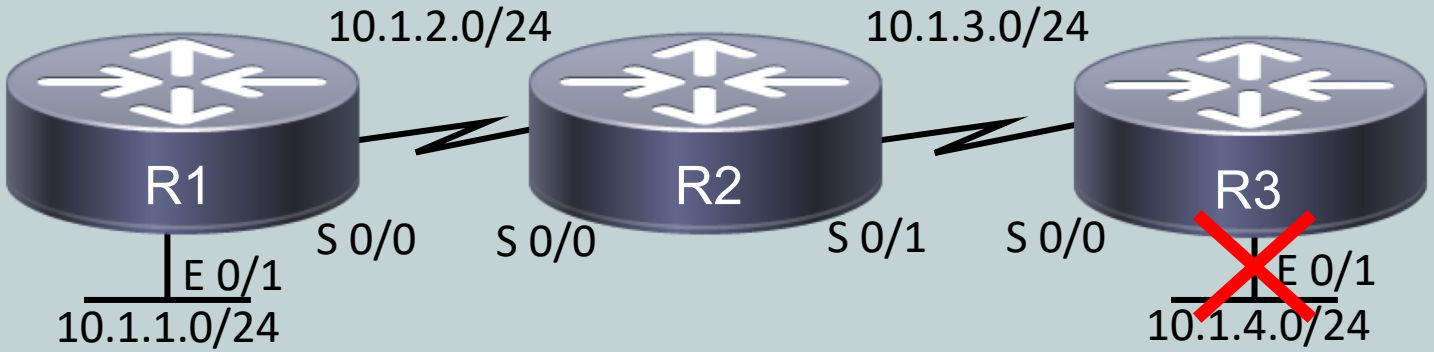
Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1

R3 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/1	0
10.1.4.0/24	E 0/1	0

Network with no issues

Routing Loops



R2 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1

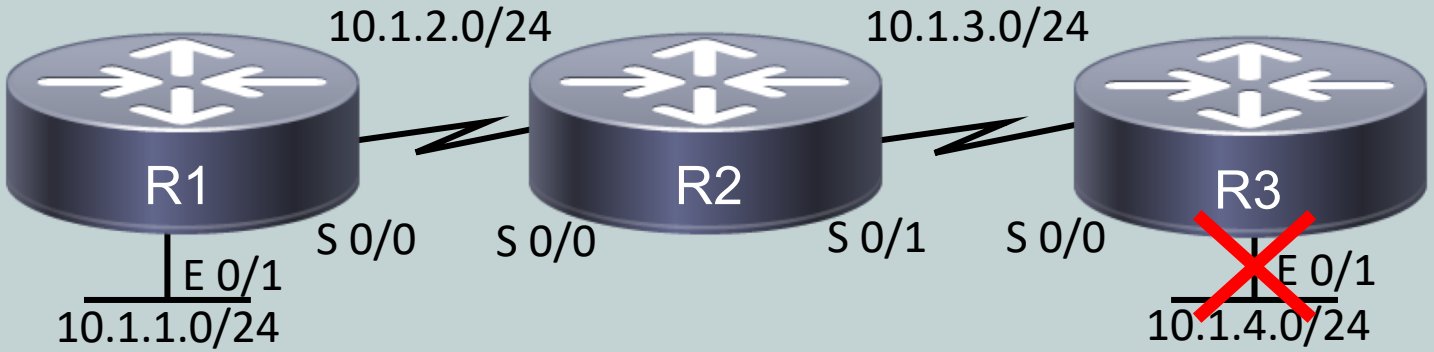
10.1.4.0/24 Hop Count 1

R3 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/1	0
10.1.4.0/24	E 0/1	0
10.1.4.0/24	S 0/0	2

Link goes down, so R3 gets information on how to connect to 10.1.4.0/24 from R2. Begins chain reaction of a routing loop.

Routing Loops



R2 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1
10.1.4.0/24	S 0/1	3

R3 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/1	0
10.1.4.0/24	E 0/1	0
10.1.4.0/24	S 0/0	2

…and the cycle continues, causing a routing loop until the metric gets so big that no one will use that route.

10.1.4.0/24 Hop Count 2

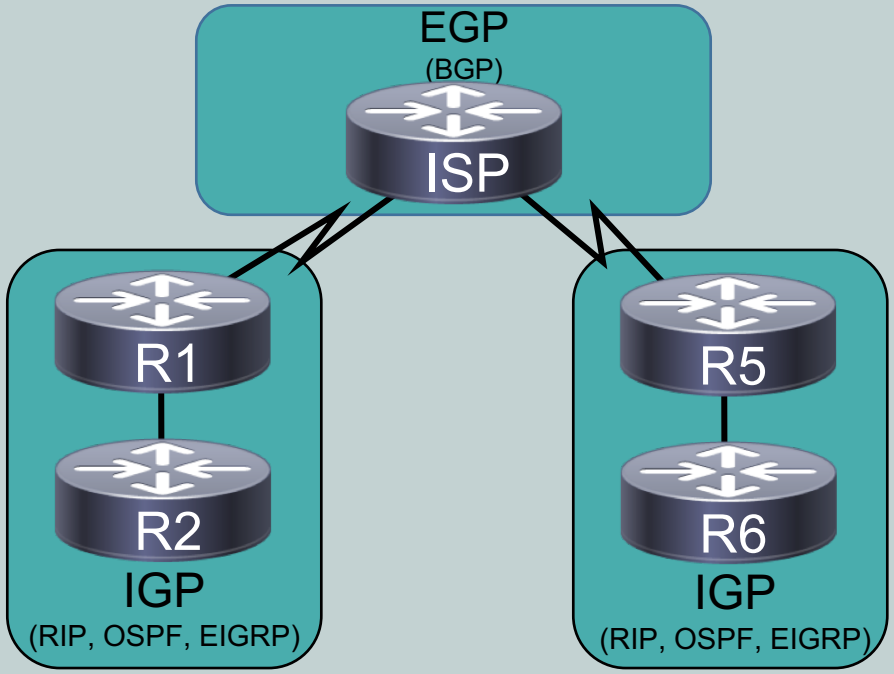
Routing Protocols

CompTIA Network+ (N10-007)

Internal and Exterior Routing Protocols

- Interior Gateway Protocols (IGP)
  - Operate within an autonomous system

- Exterior Gateway Protocols (EGP)
  - Operated between autonomous systems

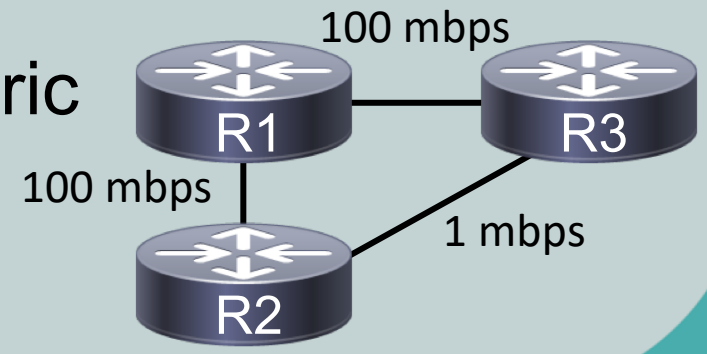


Router Advertisement Method

- Characteristic of a routing protocol
- How does it receives, advertises, and stores routing information
  - Distance vector
  - Link state
- Not every routing protocol fits neatly into one of these two categories (hybrids exist)

Distance Vector

- Sends full copy of routing table to its directly connected neighbors at regular intervals
- Slow convergence time
  - Time it takes for all routers to update their routing tables in response to a topology change
- Holding-down timers speeds up convergence
  - Prevents updates for a specific period of time
- Uses hop count as a metric

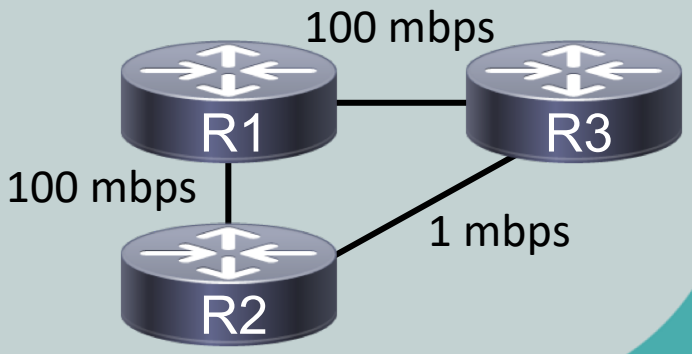


Link State

- Requires all routers to know about the paths that all other routers can reach in the network
- Information is flooded throughout the link-state domain (OSPF or IS-IS) to ensure routers have synchronized information
- Faster convergence time and uses cost or other factors as a metric
- Each router constructs its own relative shortest-path tree with itself as the root for all known routes in the network

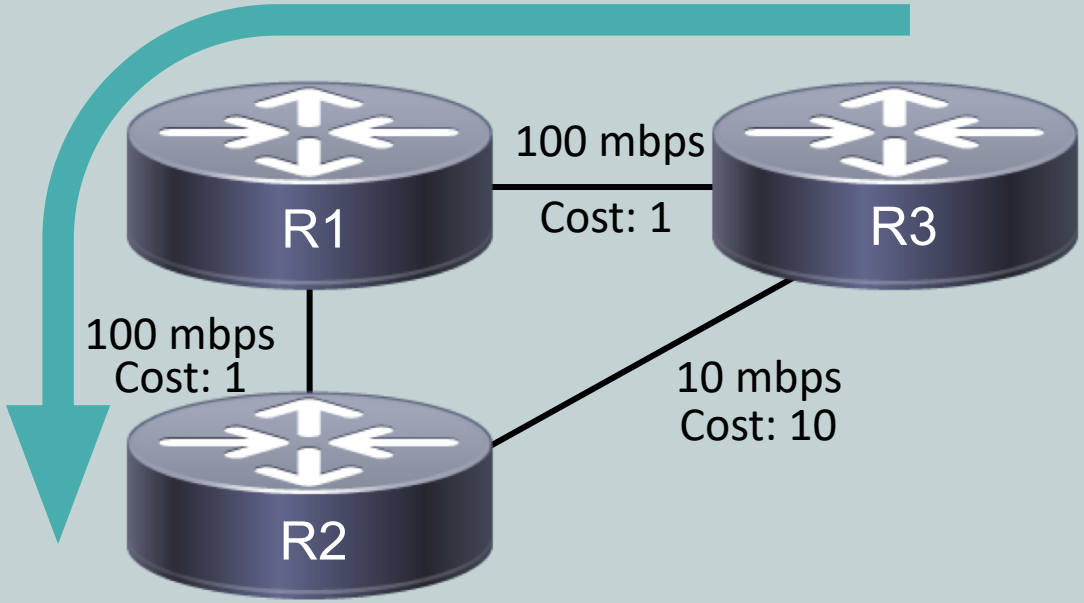
Routing Information Protocol (RIP)

- Interior Gateway Protocol
- Distance-vector protocol using *hop count*
- Maximum hops of 15, 16 is infinite
- Oldest dynamic routing protocol, provides updates every 30 seconds
- Easy to configure and runs over UDP



Open Shortest Path First (OSPF)

- Interior Gateway Protocol
- Link-state protocol using *cost*
- Cost is based on link speed between routers



Intermediate System to Intermediate System (IS-IS)

- Interior Gateway Protocol
- Link-state protocol using *cost*
- Cost is based on link speed between two routers
- Functions like OSPF protocol, but not as popular or widely utilized

Enhanced Interior Gateway Routing Protocol (EIGRP)

- Interior Gateway Protocol
- Advanced distance-vector protocol using bandwidth and delay making it a hybrid of distance-vector and link-state
- Proprietary Cisco protocol that is popular in Cisco-only networks

Border Gateway Protocol (BGP)

- External Gateway Protocol
- Path vector using the number of autonomous system hops instead of router hops
- Widespread utilization, this protocol runs the backbone of the Internet
- Does not converge quickly, though, when the topology changes

Route Believability

- If a network is using more than one routing protocol, how does it choose which routing protocol to make decisions from?
- Some routing protocols are considered more believable than others, so routers use an index of believability called *administrative distance* (AD)
- If a route has a lower the administrative distance (AD), the route is more believable

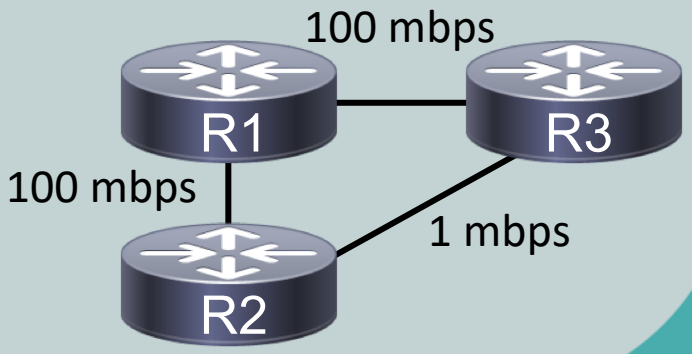
Route Believability

Routing Information Source	Administrative Distance
Directly connected network	0
Statically configured network	1
EIGRP	90
OSPF	110
RIP	120
External EIGRP	170
Unknown or Unbelievable	255 (unreachable)

Metrics

- If a routing protocol knows multiple paths to reach a network, how does it choose its path?
  - Metrics are the values assigned to a route
  - Lower metrics are preferred over higher metrics

- Metrics calculated differently for each protocol (RIP, OSPF, IS-IS, EIGRP, and BGP)
  - Hop count
  - Bandwidth
  - Reliability
  - Delay
  - Other metrics



Routing Protocol Summary

Routing Protocol	Abbreviation	Type	Interior/ Exterior
Routing Information Protocol	RIP	Distance vector	Interior
Open Shortest Path First	OSPF	Link state	Interior
Enhanced Interior Gateway Routing Protocol	EIGRP	Advanced distance vector	Interior
Intermediate System-to-Intermediate System	IS-IS	Link state	Interior
Border Gateway Protocol	BGP	Path vector	Exterior

A network can simultaneously support more than one routing protocol through *route redistribution*. This allows a router to participate in OSPF on one interface and EIGRP on another interface. The router can than translate from one protocol for redistribution as the other protocol.

Address Translation (NAT & PAT)

CompTIA Network+ (N10-007)

Address Translation

- *Network Address Translation* (NAT) is used to conserve the limited supply of IPv4 addresses
- NAT translates *private* IP addresses to *public* IP addresses for routing over public networks
- *Port Address Translation* (PAT) is a variation of address translation that utilizes port numbers instead of IP addresses for translation

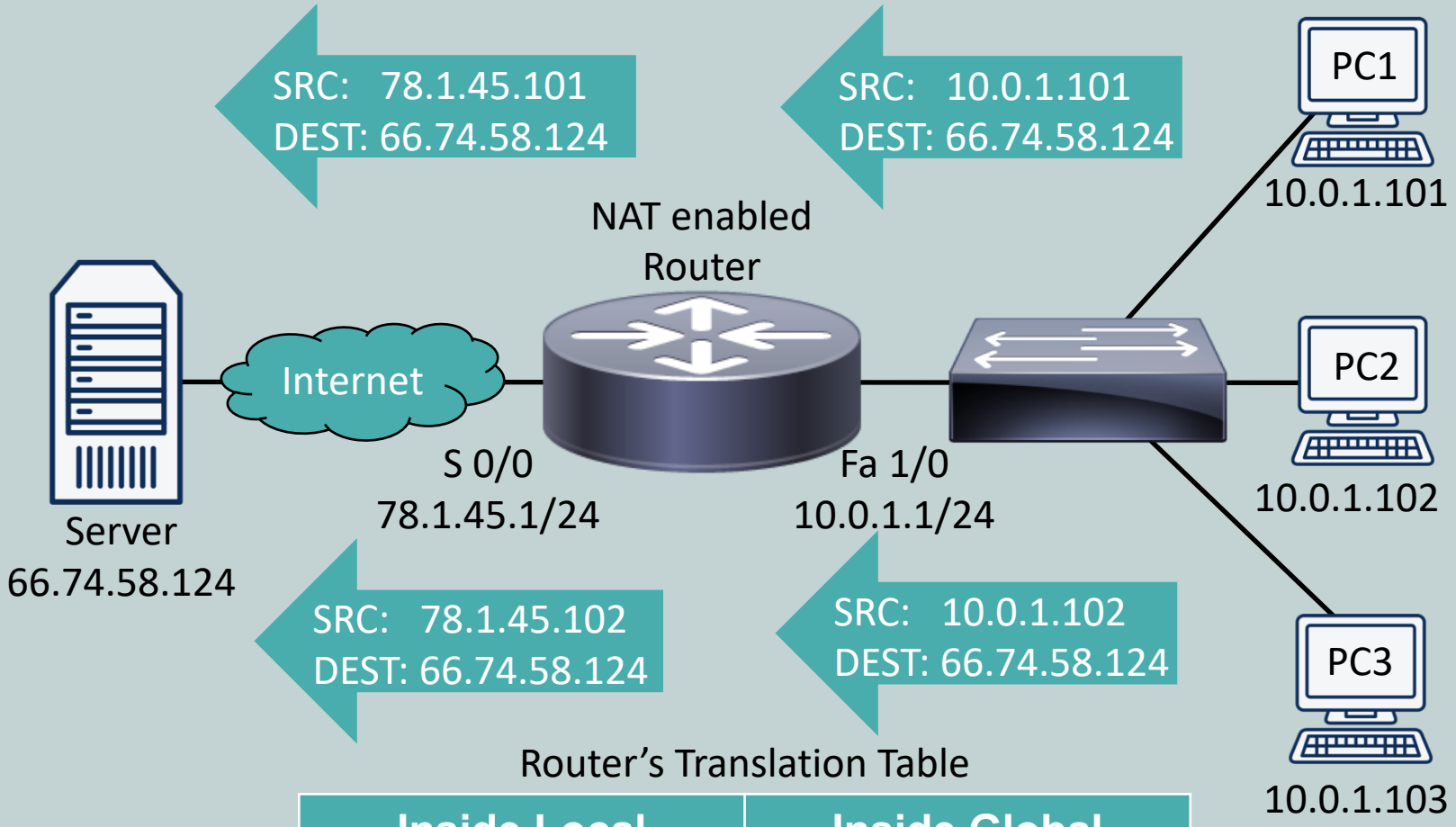
Types of Address Translation

- Dynamic NAT (DNAT)
  - IP addresses automatically assigned from a pool
  - One-to-one translations
- Static NAT (SNAT)
  - IP addresses manually assigned
  - One-to-one translations
- Port Address Translation (PAT)
  - Multiple private IP addresses share one public IP
  - Many-to-one translation
  - Common in small networks

Names of NAT IP Addresses

- Inside local
  - Private IP address referencing an inside device
- Inside global
  - Public IP address referencing an inside device
- Outside local
  - Private IP address referencing an outside device
- Outside global
  - Public IP address referencing an outside device

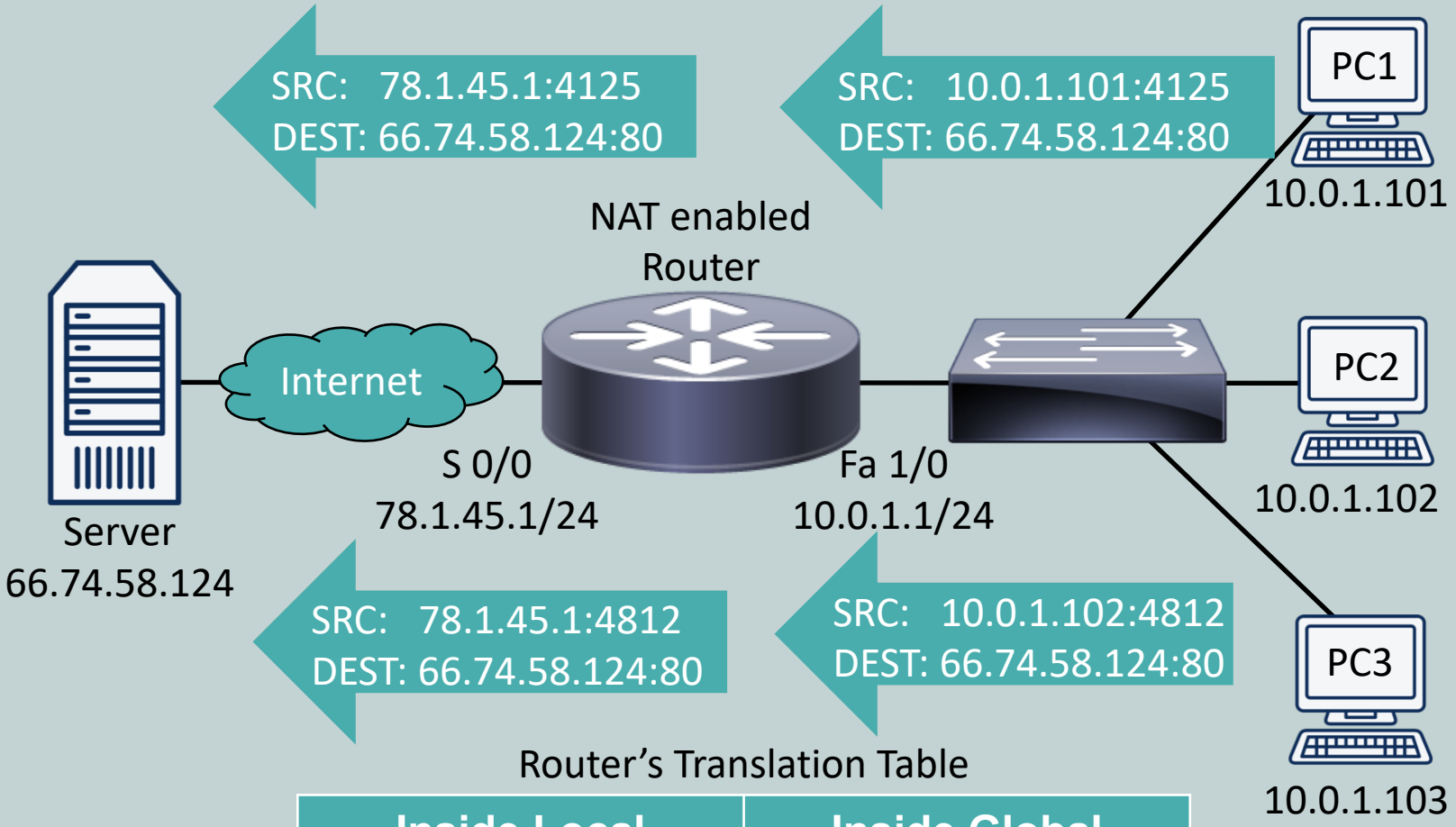
How NAT Works



Router's Translation Table

Inside Local Address	Inside Global Address
10.0.1.101	78.1.45.101
10.0.1.102	78.1.45.102

How PAT Works



Router's Translation Table

Inside Local Address:Port	Inside Global Address:Port
10.0.1.101:4125	66.74.58.124:4125
10.0.1.102:4812	66.74.58.124:4812

Multicast Routing

CompTIA Network+ (N10-007)

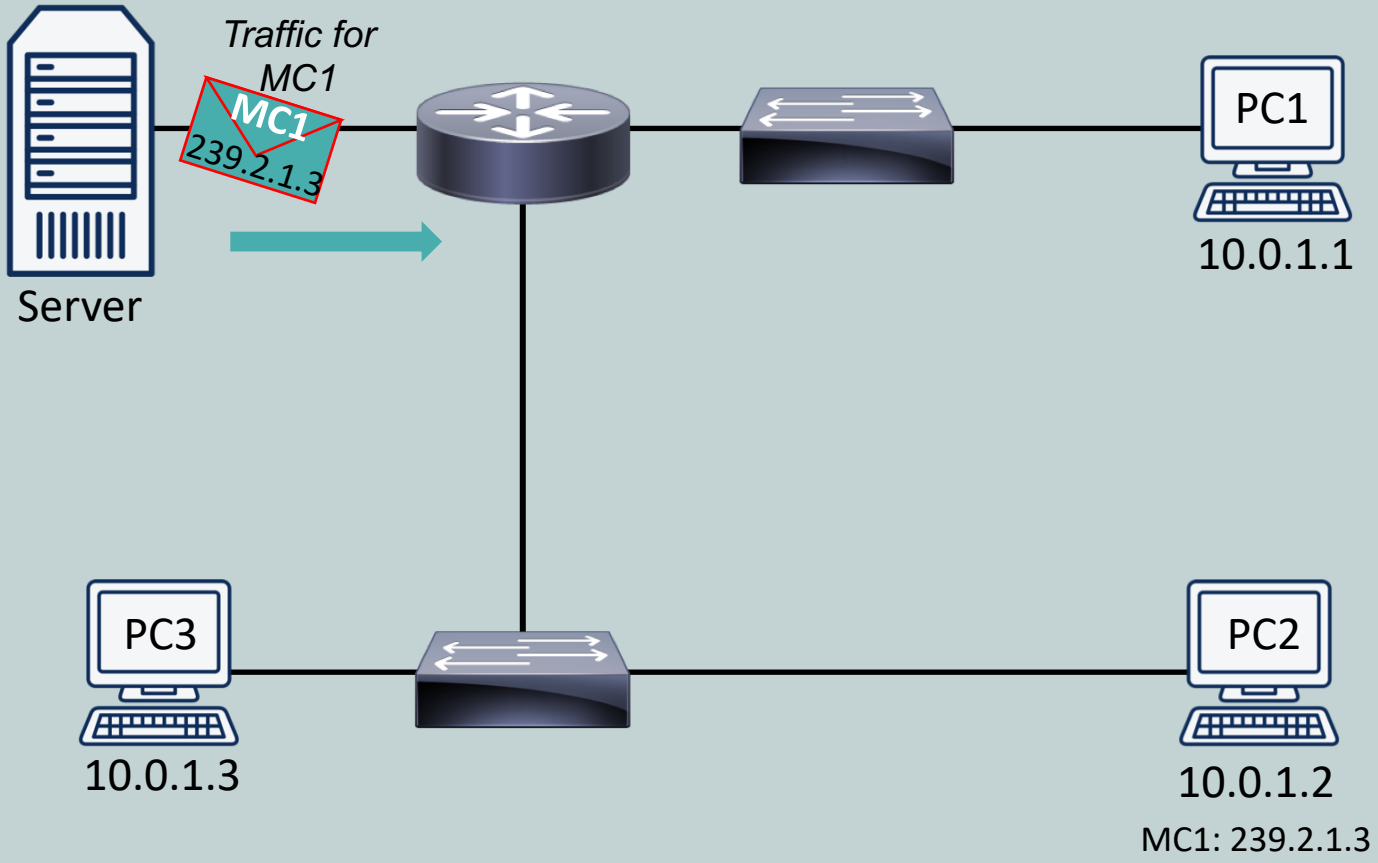
Multicast Routing

- Multicast sender sends traffic to a Class D IP Address, known as a multicast group
- Goal
  - Send the traffic only to the devices that want it
- Two primary protocols
  - Internet Group Management Protocol (IGMP)
  - Protocol Independent Multicast (PIM)

Internet Group Management Protocol (IGMP)

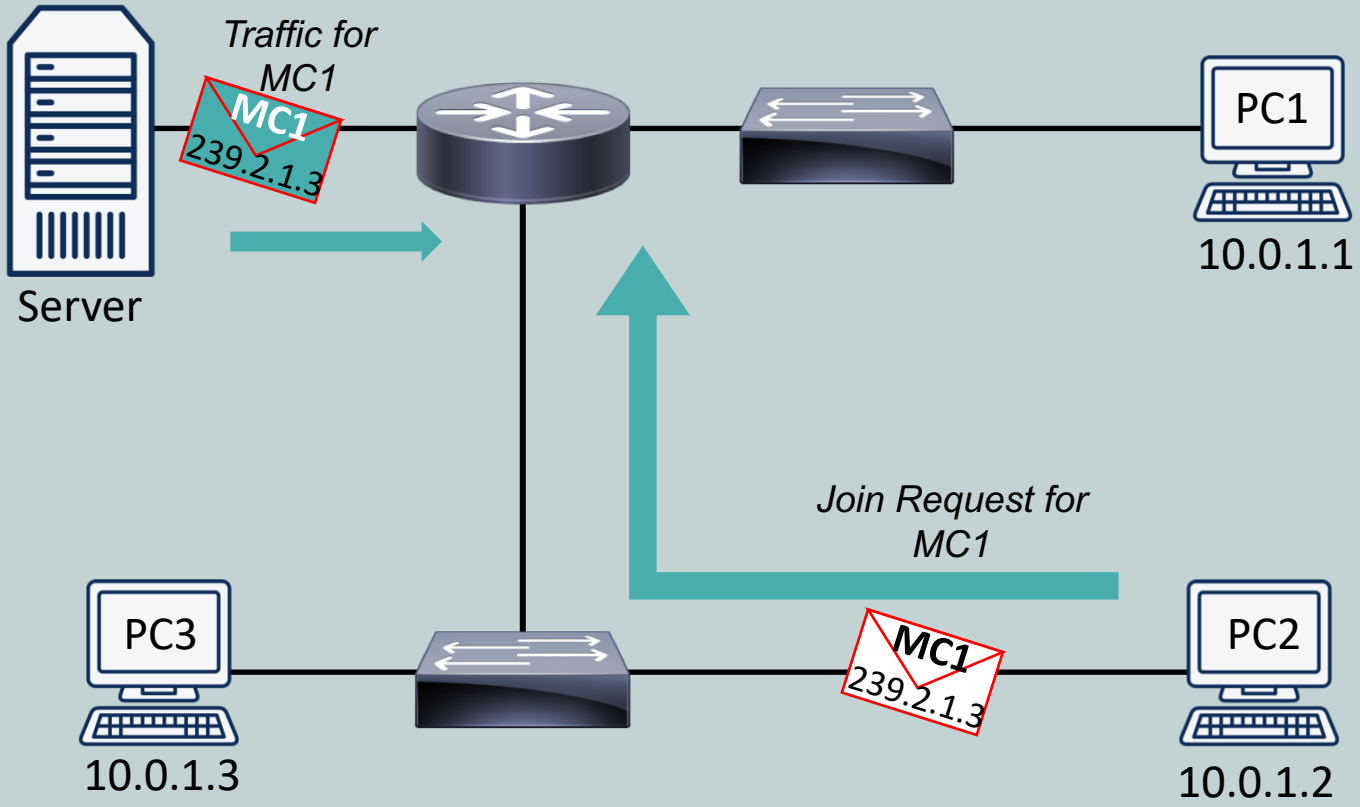
- Used by clients and routers to let routers known which interfaces have multicast receivers
- Used by clients to join a multicast group
- Versions
  - IGMPv1
    - Clients requests joining the group and is asked every 60 seconds if it wants to remain in the group
  - IGMPv2
    - Client can send a *leave* message to exit multicast group
  - IGMPv3
    - Client can request multicast from only specific server
    - Called *source-specific multicast* (SSM)
    - Allows multiple video streams to single multicast

Internet Group Management Protocol (IGMP)



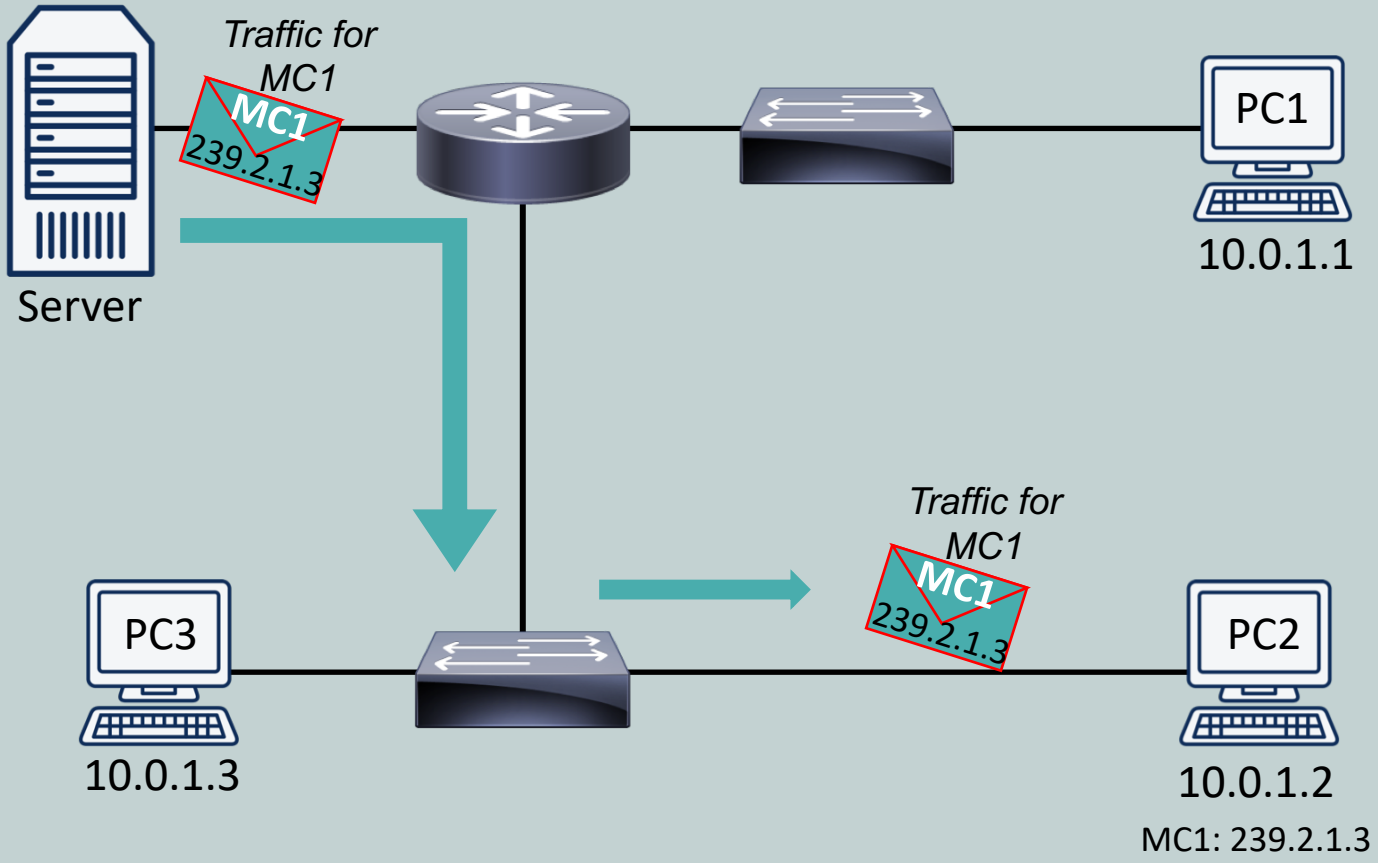
Router doesn't' forward the traffic because no clients are in the Multicast Group 1

Internet Group Management Protocol (IGMP)



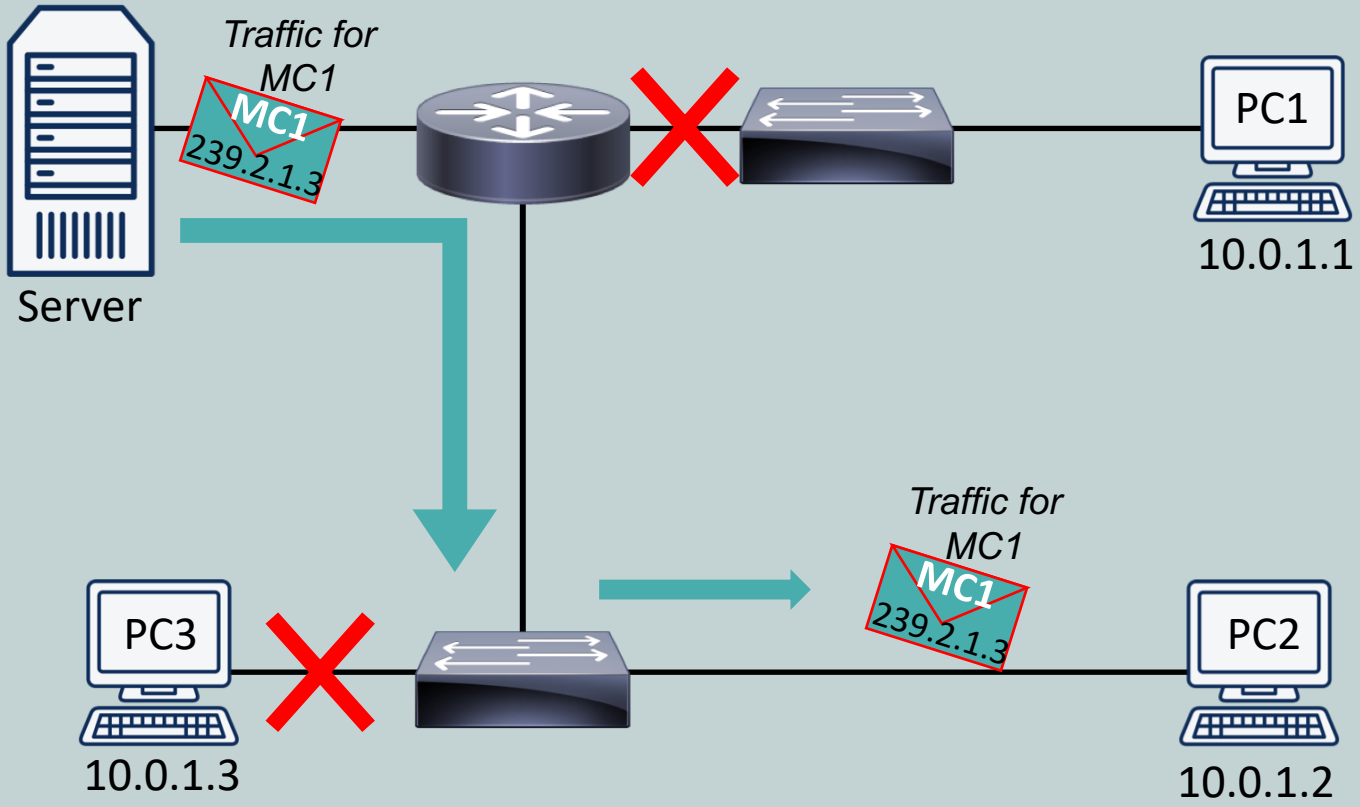
PC2 joins the multicast traffic by sending the "join message" to its default gateway

Internet Group Management Protocol (IGMP)



Router remembers that PC2 is now part of Multicast Group 1

Internet Group Management Protocol (IGMP)

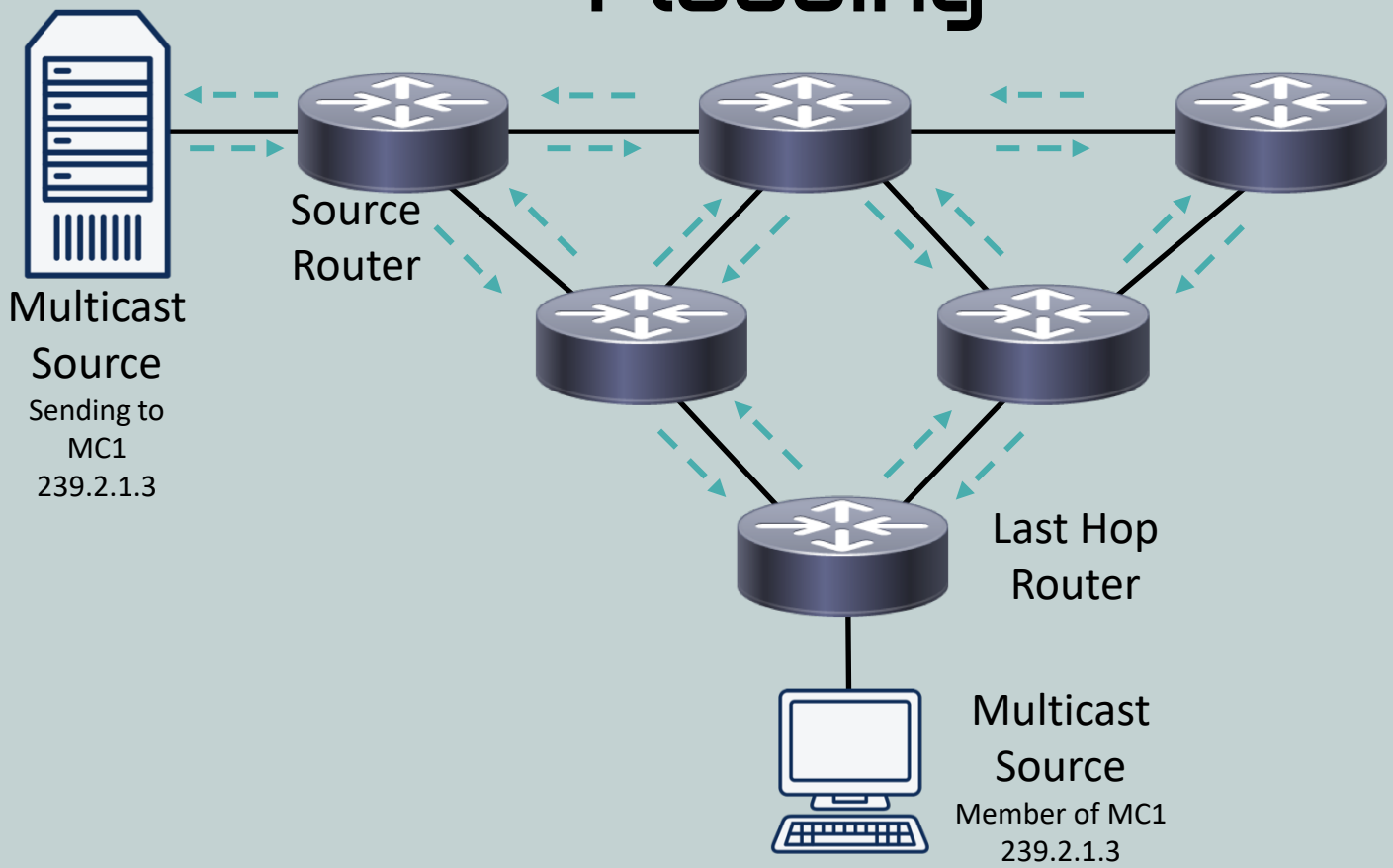


Router forward traffic for 239.1.2.3 to PC2 and blocks it from going to other clients

Protocol Independent Multicast (PIM)

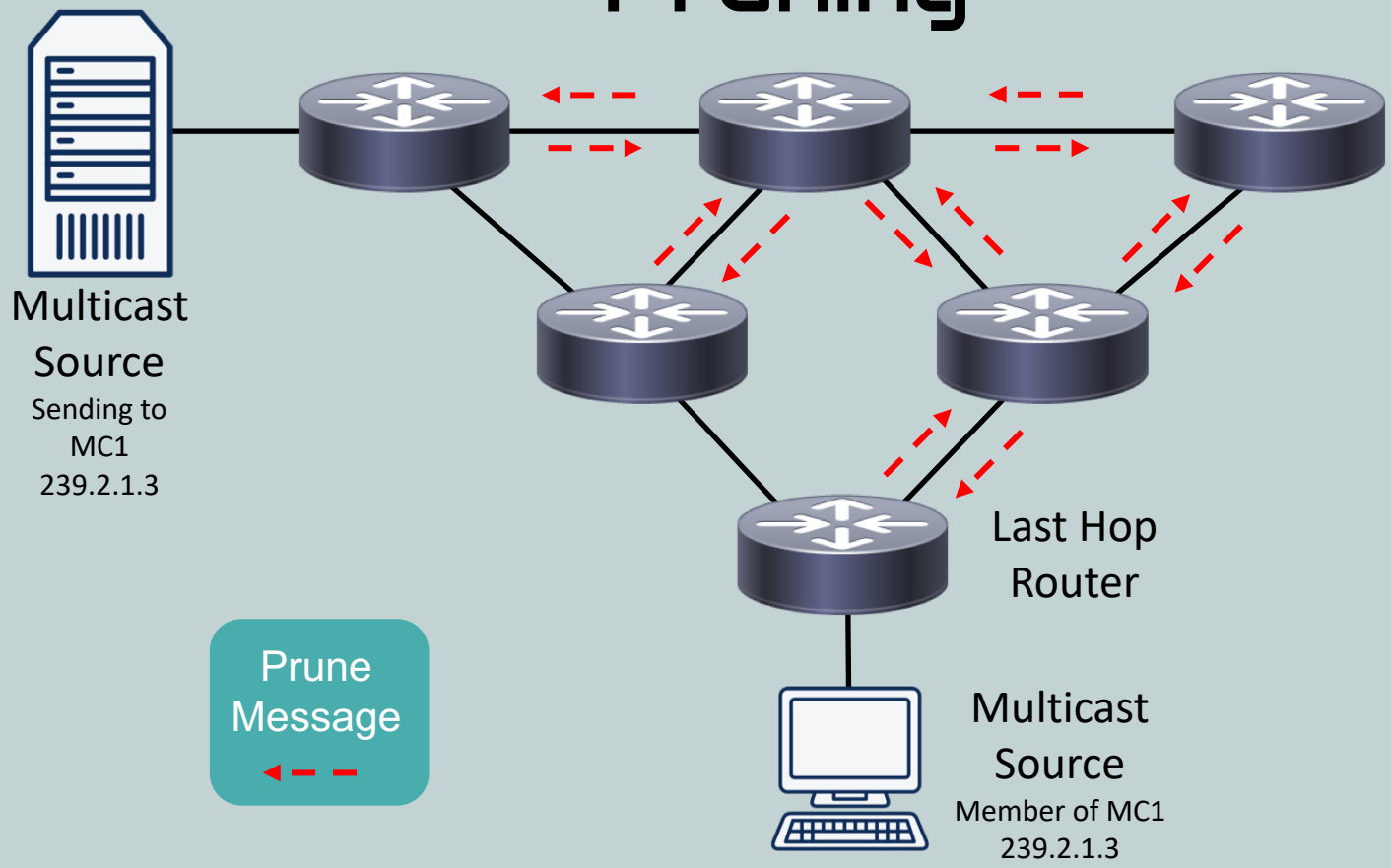
- Routes multicast traffic between multicast-enabled routers
- Multicast routing protocol forms a *multicast distribution tree*
- Modes
  - PIM Dense Mode (PIM-DM)
    - Uses periodic ***flood and prune behavior*** to form optimal distribution tree
    - Causes a negative performance impact on the network
    - Rarely used in modern networks
  - PIM Sparse Mode (PIM-SM)
    - Initially uses a shared distribution tree, which may be suboptimal, but…
    - Eventually creates an optimal distribution tree through shortest path tree (SPT) switchover

PIM Dense Mode: Flooding



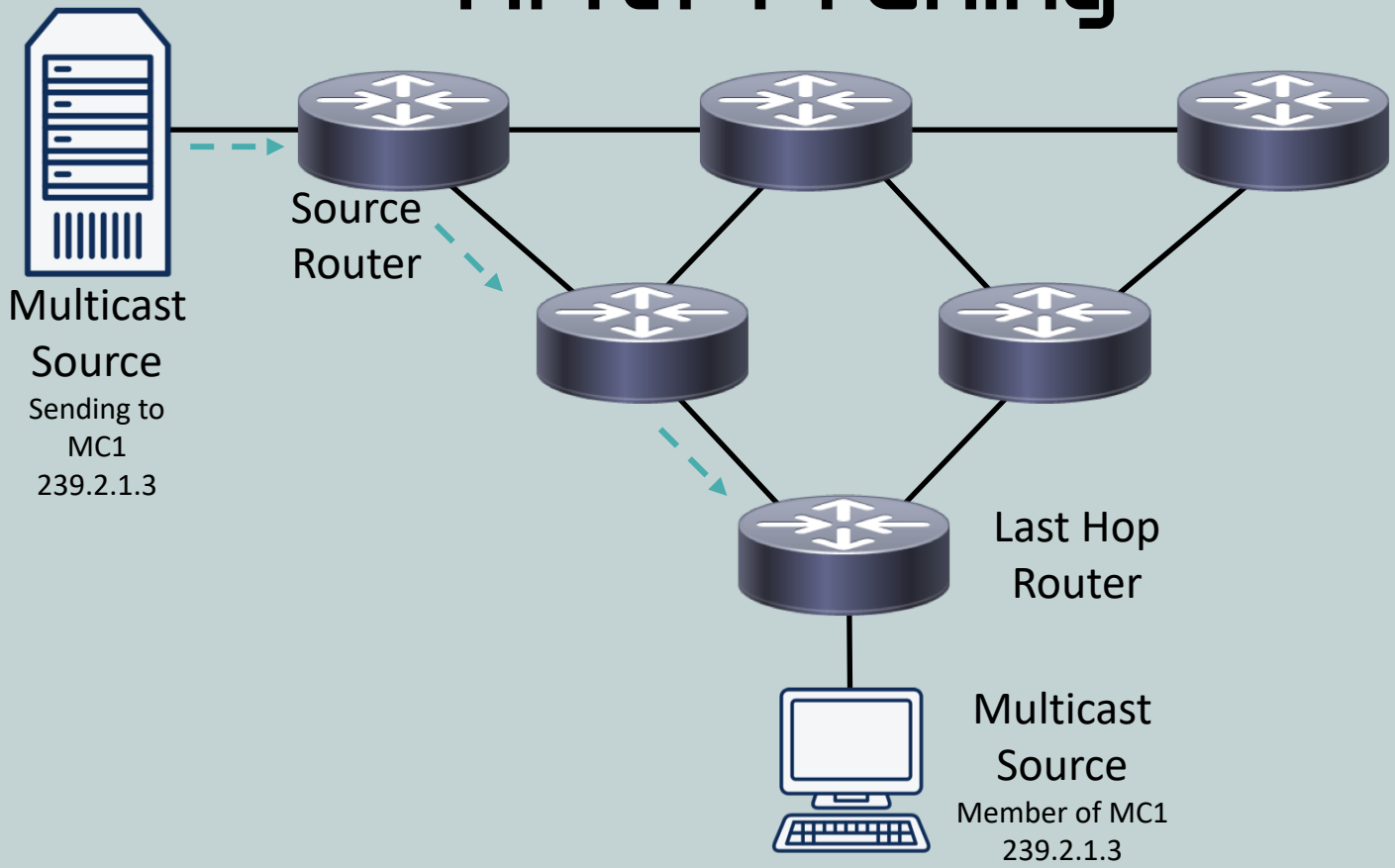
Uses source distribution tree (SDT) to form an optimal path between source router and lap-hop router. Before the optimal path is formed, entire network is initially flooded and consumes unnecessary bandwidth.

PIM Dense Mode: Pruning



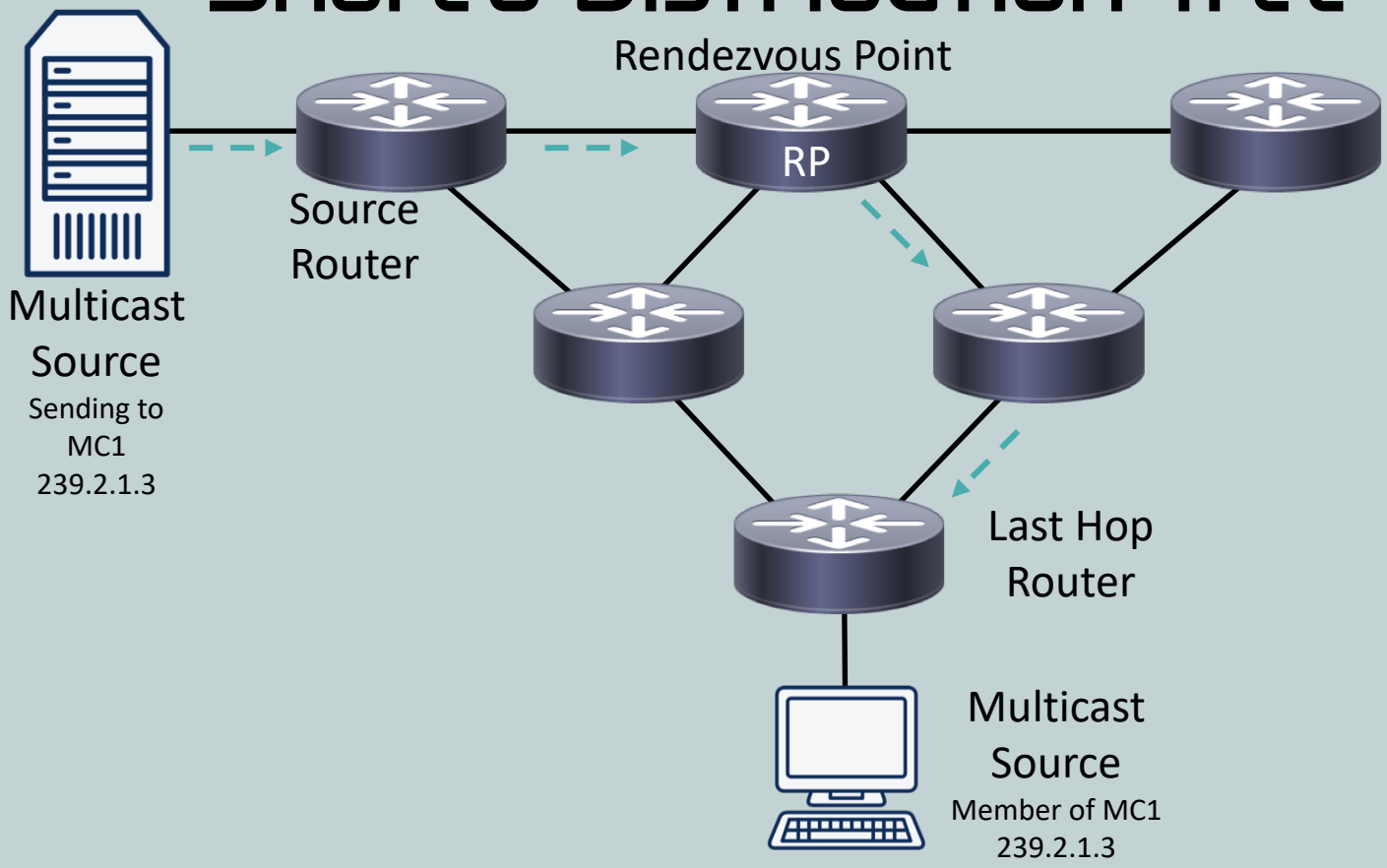
If a router receives multicast traffic in the initial flood and the traffic is not needed, then the router sends a prune message asking to be removed from the source distribution tree.

PIM Dense Mode: After Pruning



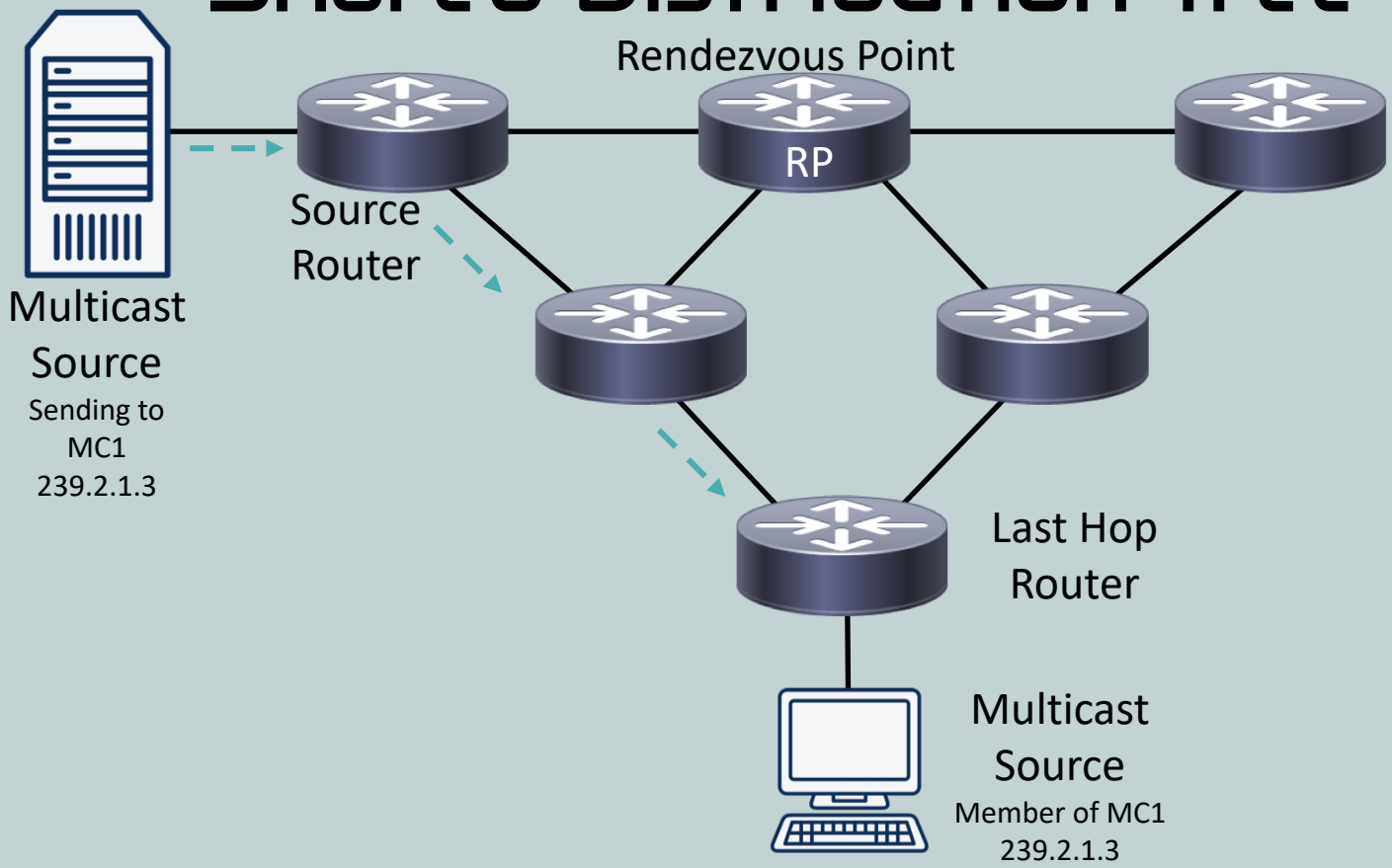
After sending prune messages, the resulting source distribution tree has an optimal path between source router and last-hop router. Flood and prune repeats every 3 minutes which can cause excessive performance impacts on the network.

PIM Sparse Mode: Shared Distribution Tree



An optimal path between the source and last-hop routers is not initially created. Instead, a multicast source sends traffic directly to a rendezvous point (RP). All last-hop routers send join messages to the RP.

PIM Sparse Mode: Shared Distribution Tree



Originally provides a suboptimal distribution tree, but when first multicast packet is received by last-hop router, then optimal distribution tree is created based on unicast routing table. Unneeded branches are pruned during Shortest Path Tree (SPT) switchover.