Chapter 4
Routing Algorithm and Protocols

Routing Algorithm

- The ***main function*** of the network layer is ***routing packets*** from the source machine to the destination machine.
- ***Routing*** is the process of forwarding of a packet in a network so that it reaches its intended destination.
- A ***Routing Algorithm*** is a set of step-by-step operations used to direct internet traffic efficiently. When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.
- A **Routing Algorithm** is a method for determining the routing of packets in a node. For each node of a network, the algorithm determines a routing table, which in each destination, matches an output line.

Properties/Goals of Routing Algorithm

- **Properties of routing algorithm**: *correctness, simplicity, robustness, stability, fairness, and efficiency*.
- ***Correctness:*** The routing should be done properly and correctly so that the packet may reach their proper destination.
- ***Simplicity:*** The routing should be done in a simple manner so that the overhead is as low as possible.
- ***Robustness***
  - Once a major network become operative, it may be expected to run continuously for years without any failures.
  - The algorithm designed for routing should be robust enough to handle hardware and software failures and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted.

Properties/Goals of Routing Algorithm

- ***Stability***
  - The routing algorithms should be stable under all possible circumstances**.**
  - A ***stable algorithm*** reaches equilibrium and stays there. It should converge quickly too, since communication may be disrupted until the routing algorithm has reached equilibrium.
- ***Fairness:*** Every node connected to the network should get a fair chance of transmitting their packets.
- ***Optimality:*** The routing algorithms should be optimal in terms of throughput and minimizing mean packet delays.
- ***There is a trade-offs between fairness and efficiency, we must decide what it is we seek to optimize.***

Properties/Goals of Routing Algorithm

- Suppose that there is enough traffic between *A* and *A′*, between *B* and *B′*, and between *C* and *C′* to saturate the horizontal links. To maximize the total flow, the *X* to *X′* traffic should be shut off altogether. Unfortunately, *X* and *X′* may not see it that way.

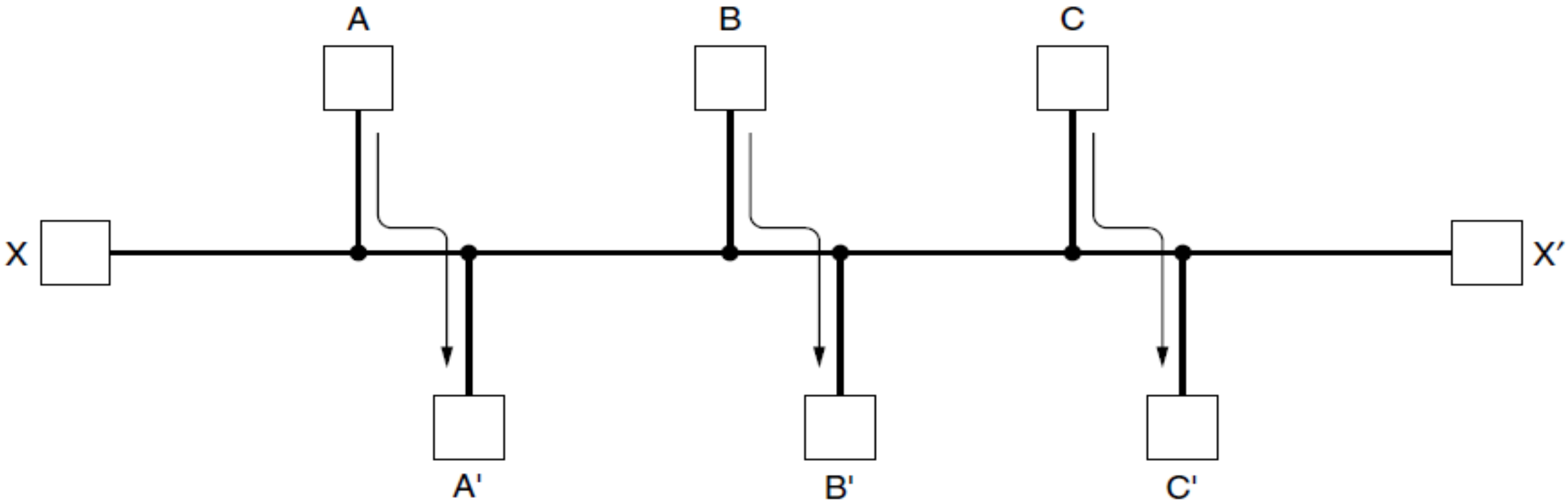


Figure 5-5. Network with a conflict between fairness and efficiency.

Classification of Routing Algorithm

- ***Two major classes: non-adaptive and adaptive***.
- **Non-adaptive algorithms**
  - These algorithm do not base their routing decisions on any ***measurements or estimates of the current topology and traffic***.
  - Instead, the choice of the route to use to get from I to *J* is computed in advance, offline, and downloaded to the routers when the network is booted.
  - This procedure is sometimes called **static routing**.
  - It **does not respond to failures**, static routing is mostly useful for situations in which the routing choice is clear.

Classification of Routing Algorithm

- **Adaptive algorithms**
  - **Adaptive algorithms** change their routing decisions to reflect changes in the topology, and sometimes changes in the traffic as well.
  - These **dynamic routing** algorithms differ in where they get their information (e.g., locally, from adjacent routers, or from all routers), when they change the routes (e.g., when the topology changes, or every ΔT seconds as the load changes).
  - The optimization parameter are the distance, number of hops, or estimated transit time.

Static Vs. Dynamic Routing Algorithm

- **Static routing manually sets** up the optimal paths between the source and the destination computers. On the other hand, the **dynamic routing** uses **dynamic protocols** to update the routing table and to find the optimal path between the source and the destination computers.
- The routers that use the static routing algorithm do not have any controlling mechanism if any faults in the routing paths. These routers **do not sense the faulty computers** encountered while finding the path between two computers or routers in a network. The dynamic routing algorithms are used in the dynamic routers and these routers **can sense a faulty router in the network**.
- The **static routing** is suitable **for very small networks** and they cannot be used in large networks. Dynamic routing is used **for larger networks**. The dynamic routers are based on various routing algorithms like OSPF, IGRP and RIP .
- The static routing has **the advantage that it requires minimal memory**. Dynamic router, however, have quite a few memory overheads, depending on the routing algorithms used.

Routing Table

- A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.
- A basic routing table includes the following information:
  - **Mask:** This field defines the mask applied for the entry.
  - **Network address:** This field defines the network address to which the packet is finally delivered.
  - **Next-hop address**s: This field defines the address of the next-hop router to which the packet is delivered.
  - **Interface:** The outgoing network interface the device should use when forwarding the packet to the next hop or final destination.
  - **Reference count:** This field gives the number of users of this route at the moment. For example, if five people at the same time are connecting to the same host from this router, the value of this column is 5.

Routing Table

- **Flags**: This field defines up to five flags.
  - **U (up).** The U flag indicates the router is up and running.
  - **G (gateway).** The G flag means that the destination is in another network.
  - **H (host-specific).** The H flag indicates that the entry in the network address field is a host-specific address.
  - **D (added by redirection).** The D flag indicates that routing information for this destination has been added to the host routing table by a redirection message from ICMP.
  - **M (modified by redirection).** The M flag indicates that the routing information for this destination has been modified by a redirection message from ICMP.
- **Use:** This field shows the number of packets transmitted through this router for the corresponding destination.

- **A routing table can be either static or dynamic**. A static table is one with manual entries. A dynamic table, on the other hand, is one that is updated automatically when there is a change somewhere in the internet.

Forwarding Techniques: Route Method Versus Next-hop Method

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Routing table for host A

Destination	Route
Host B	R2, host B

Routing table for R1

Destination	Route
Host B	Host B

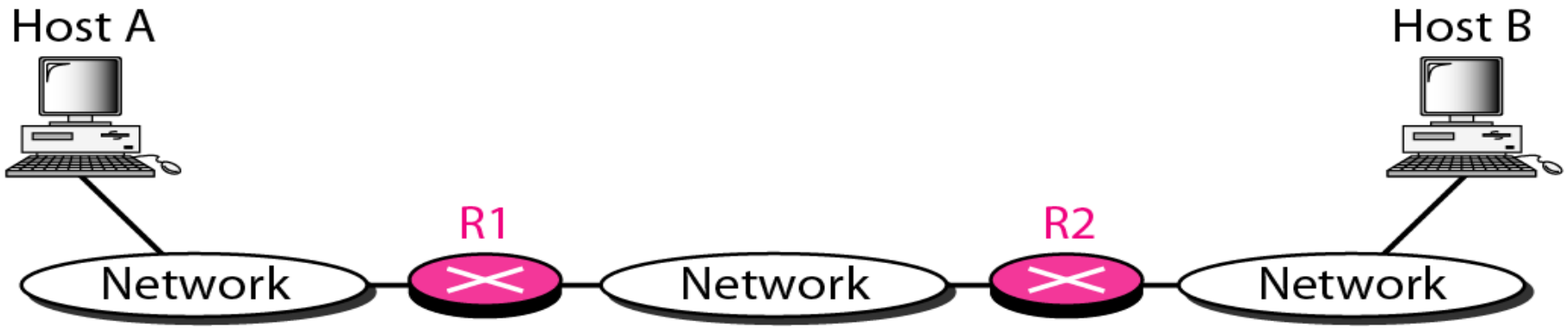
Routing table for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
Host B	R2

Destination	Next hop
Host B	---



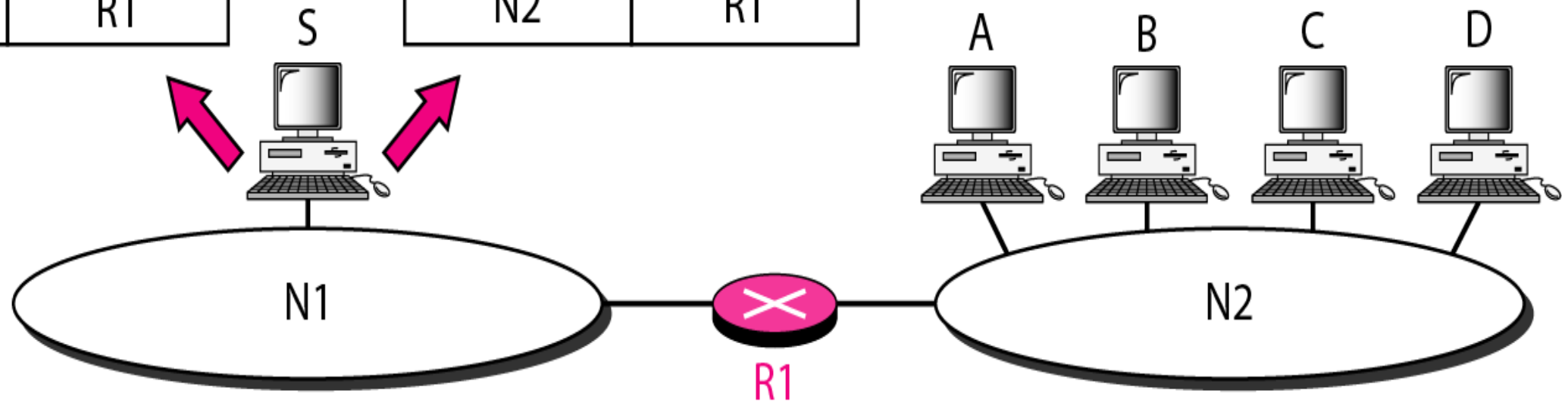
Forwarding Techniques: Host-specific versus network-specific method

Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based on network-specific method

Destination	Next hop
N2	R1



Routing Algorithm

- **Non- adaptive Routing**
  - Flooding
  - Shortest path algorithm
- **Adaptive Routing Algorithm**
  - Distance Vector Routing
  - Link State Routing

Non- adaptive Routing: Flooding

- A simple local technique is **flooding**, in which every incoming packet is sent out on every outgoing line except the one it arrived on.
- Flooding generates vast numbers of **duplicate packets**, in fact, an infinite number unless some measures are taken to **damp the process**.
- A hop counter contained in the **header of each packet** that is **decremented at each hop**, with the packet being discarded when the **counter reaches zero**.
- Ideally, the hop counter should be initialized to the **length of the path** from source to destination. If the sender does **not know how** long the path is, it can initialize the counter to the worst case namely, the **full diameter of the network**.
- Flooding with a hop count **can produce an exponential number of duplicate packets** as the hop count grows and routers duplicate packets they have seen before.
- **Better technique for damming the flood** is to have routers keep track of which packets have been flooded, **to avoid sending them** out a second time.

Non- adaptive Routing: Flooding

- One way to achieve this goal is to have the source router **put a sequence number** in each packet it receives from its hosts.
- Each router then needs a **list per source router** telling which sequence numbers originating at that source have already been seen**. If an incoming packet is on the list, it is not flooded.**
- **Some important uses of Flooding.**
  - **First, it ensures that a packet is delivered to every node in the network**. This may be wasteful if there is a single destination that needs the packet, but it is effective for broadcasting information.
  - **Second, flooding is tremendously robust**. Even if large numbers of routers are blown to bits (e.g., in a military network located in a war zone), flooding will find a path if one exists, to get a packet to its destination. Flooding also requires little in the way of setup. The routers only need to know their neighbors.

Shortest Path Algorithm

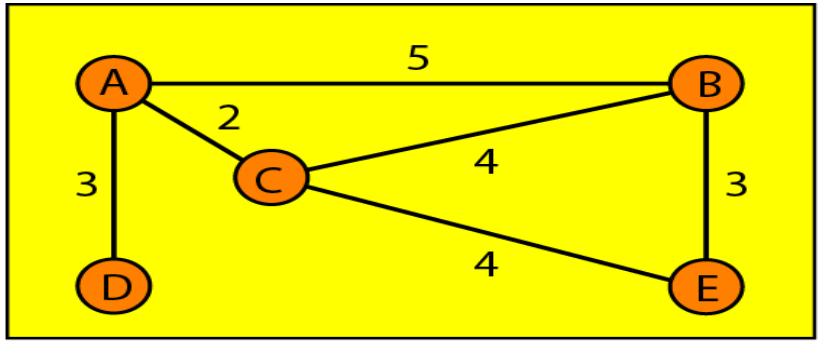
- Routing algorithms with a simple technique for computing optimal paths given a complete picture of the network.
- The idea is to build a graph of the network, with each node of the graph representing a router and each edge of the graph representing a communication line, or link.
- To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.
- In the general case, the labels on the edges could be computed as a function of the distance, bandwidth, average traffic, communication cost, measured delay, and other factors.
- By changing the weighting function, the algorithm would then compute the ‘‘shortest’’ path measured according to any one of a number of criteria or to a combination of criteria.

Shortest Path Algorithm

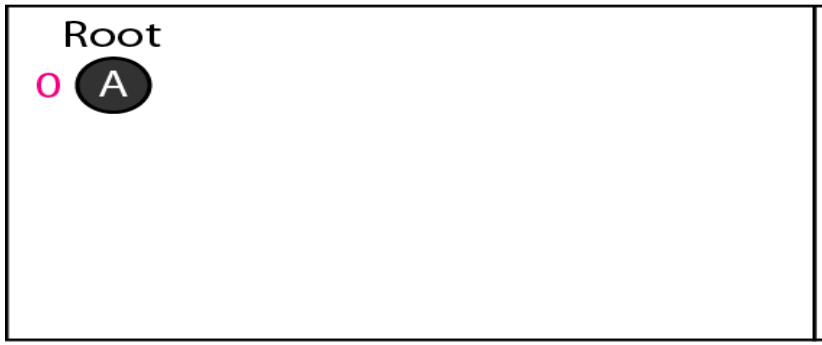
- With this graph labeling, the shortest path is the fastest path rather than the path with the fewest edges or kilometers.
- Algorithms for computing the shortest path between two nodes of a graph **Dijkstra (1959)** and it finds the shortest paths between **a source and all destinations in the network.**
- Initially, no paths are known, so all nodes are labeled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths.
- A label may be either tentative or permanent. **Initially, all labels are tentative**. When it is discovered that a **label represents the shortest possible path** from the source to that node, it is **made permanent** and **never changed thereafter.**

Table 22.2 *Routing table for node A*

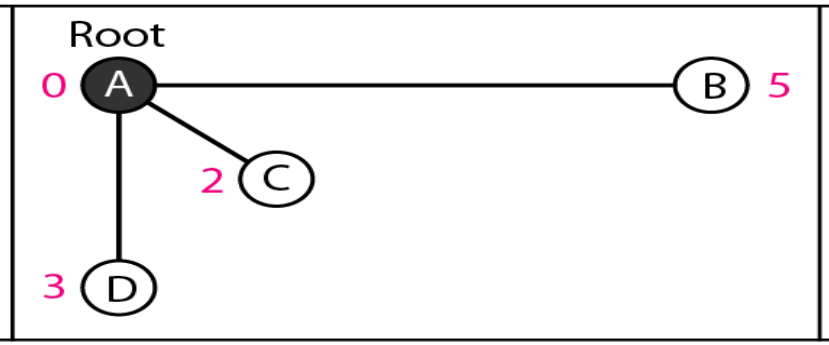
Node	*Cost*	*Next Router*
A	0	-
B	5	-
C	2	-
D	3	-
E	6	C



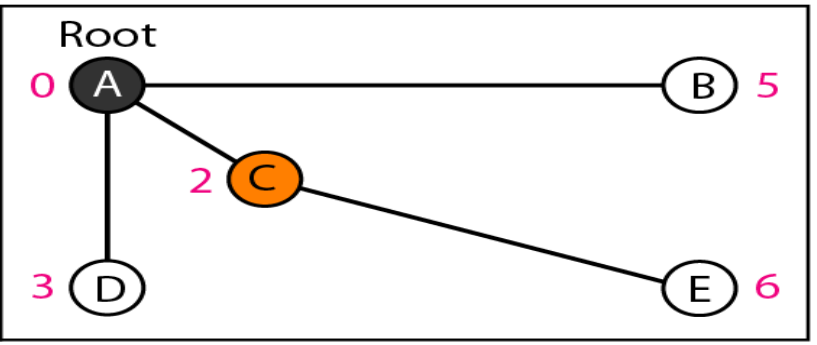
Topology



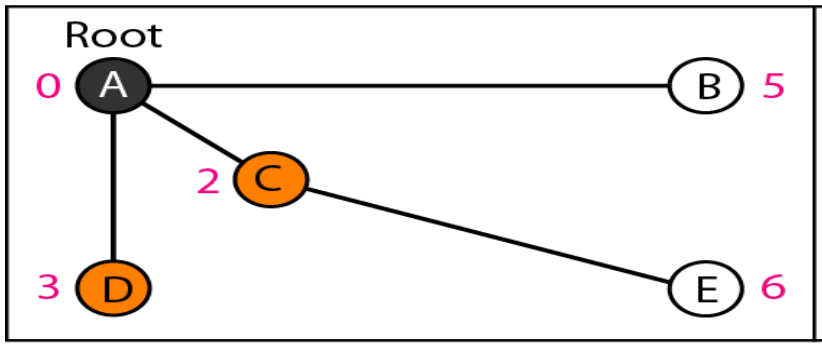
1. Set root to A and move A to tentative list.



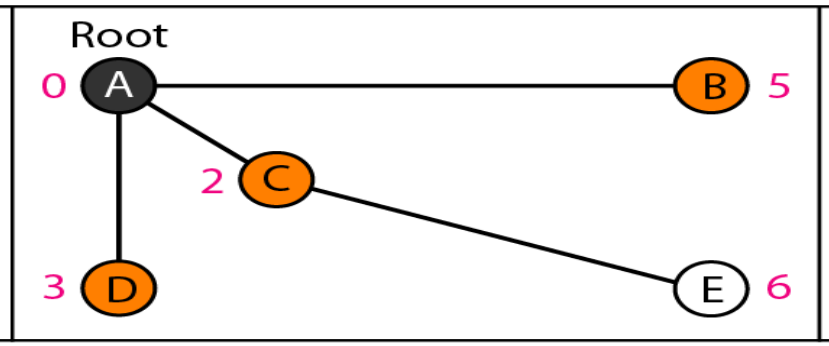
2. Move A to permanent list and add B, C, and D to tentative list.



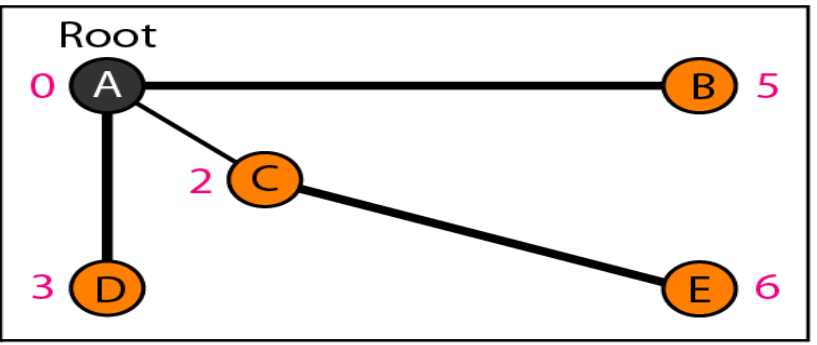
3. Move C to permanent and add E to tentative list.



4. Move D to permanent list.



5. Move B to permanent list.



6. Move E to permanent list (tentative list is empty).

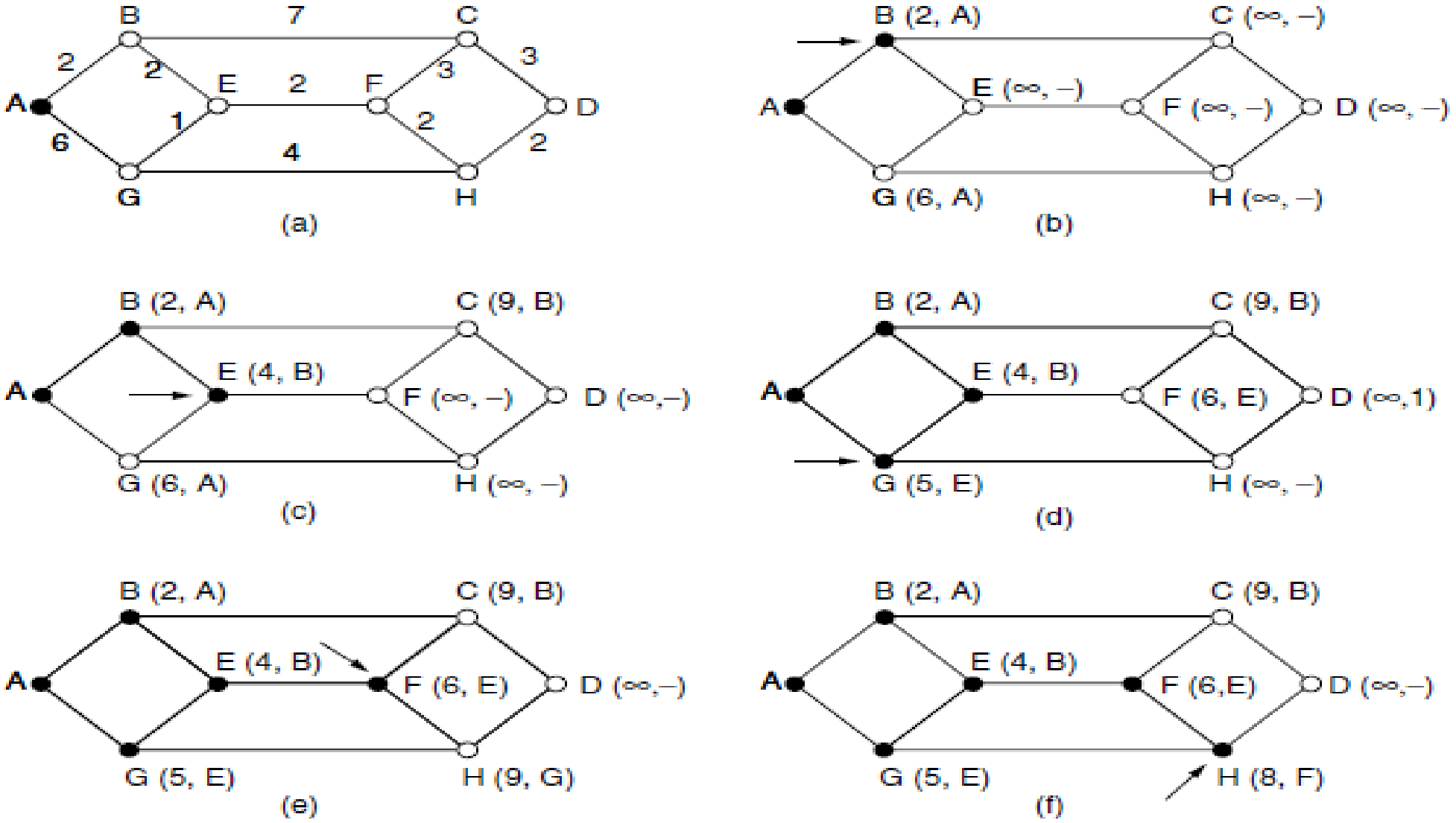
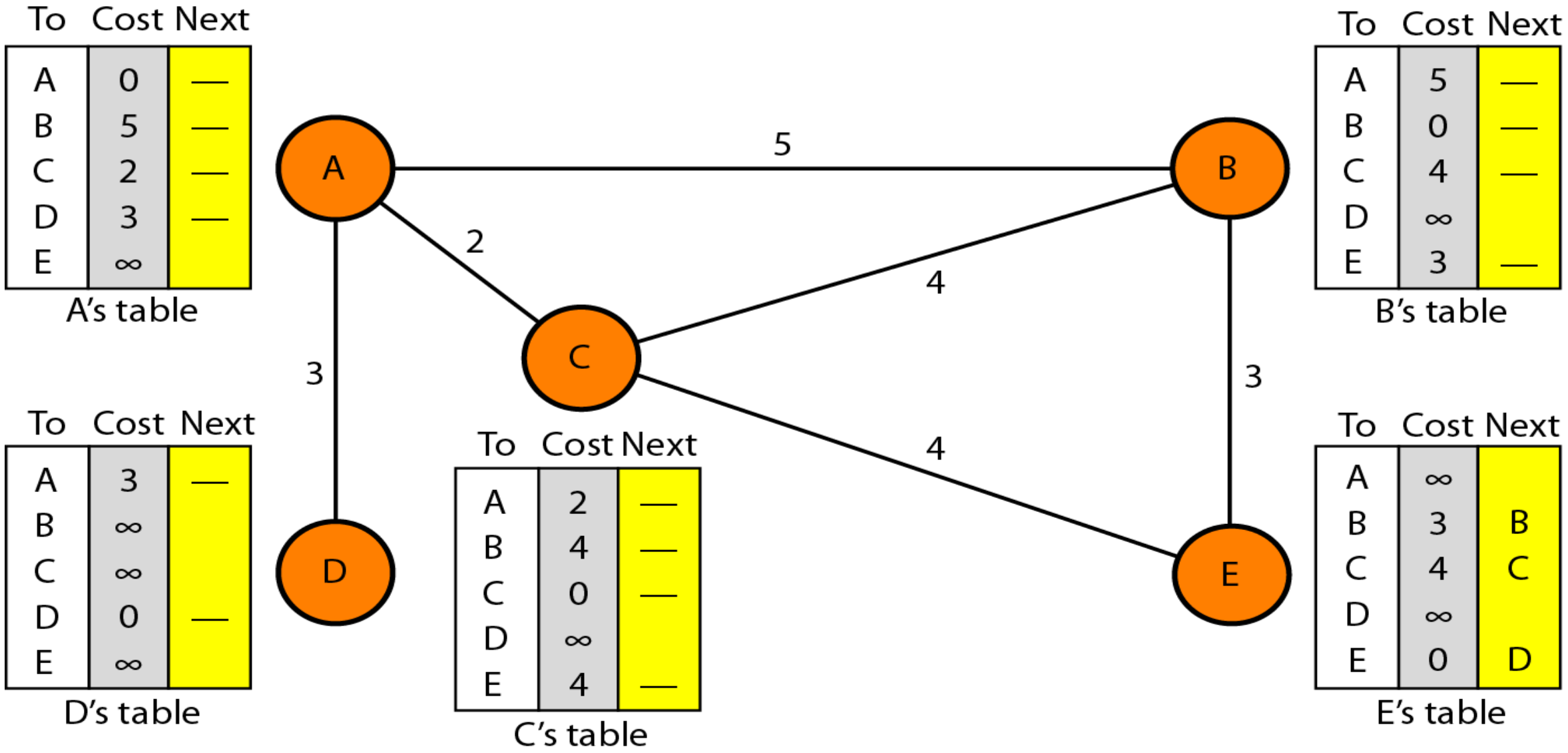


Figure 5-7. The first six steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

Distance Vector Routing

- The distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm, after the researchers who developed it (Bellman, 1957; and Ford and Fulkerson, 1962).
- In distance vector routing, the least-cost route between any two nodes is the route **with minimum distance**.
- In this protocol, each node maintains a **vector (table) of minimum distances** to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).
- ***Initialization***
  - Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.
  - we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors.

Initialization of tables in distance vector routing



Distance Vector Routing

- ***Sharing***
  - Distance vector routing is the sharing of information between neighbors.
  - Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E.
  - On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D.
  - There is only one problem. How much of the table must be shared with each neighbor?
  - The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard.
  - ***A node can send only the first two columns of its table to any neighbor.***

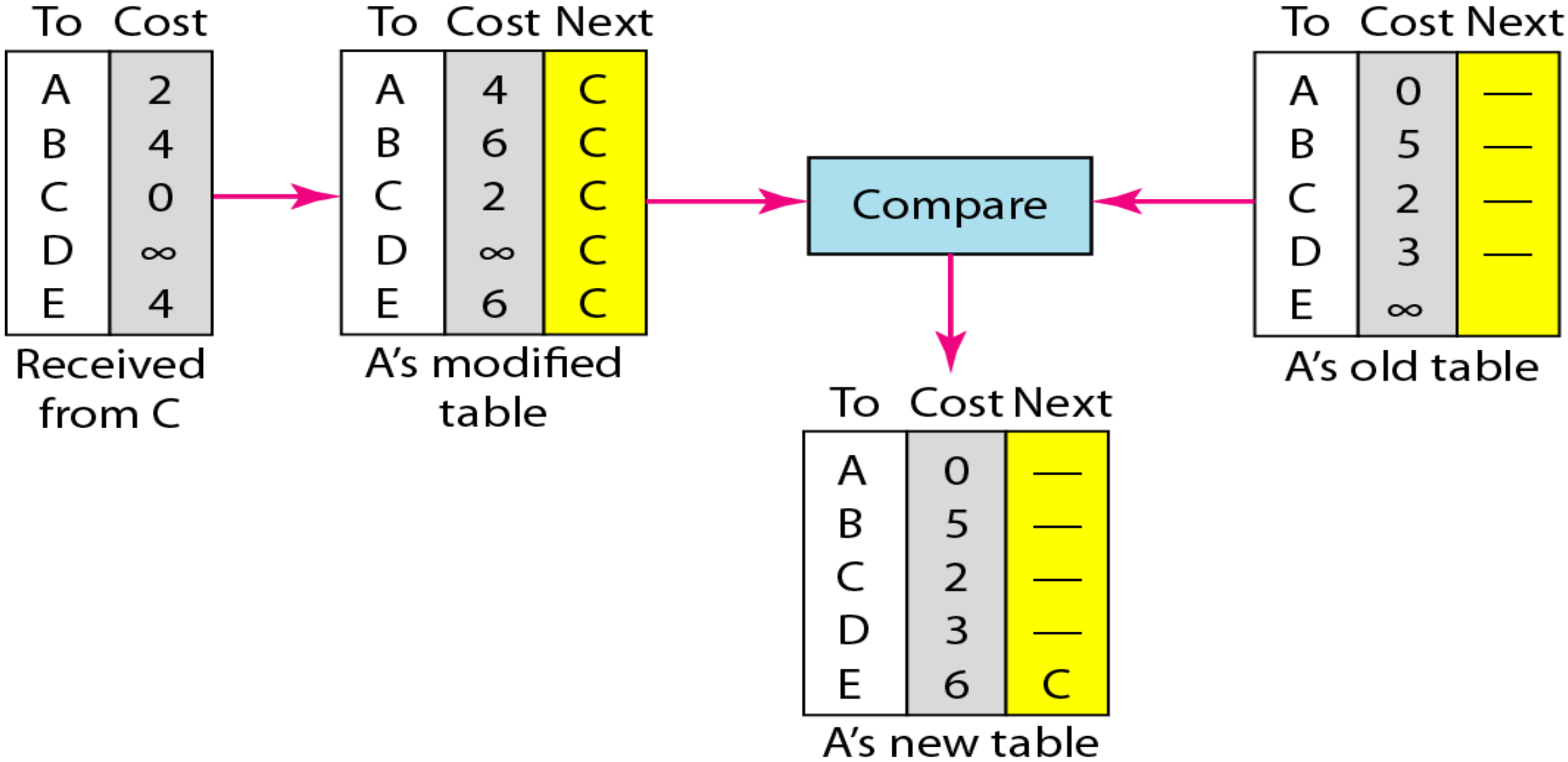
Distance Vector Routing

- ***Updating:*** When a node receives a two-column table from a neighbor, it needs to update its routing table. ***Updating takes three steps:***
  1) The receiving node needs to add the cost between itself and the sending node to each value in the second column.
  2) The receiving node needs to add the name of the sending node to each row as then third column if the receiving node uses information from any row. The sending node is the next node in the route.
  3) The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

     i. *If the next-node entry is different, the receiving node chooses the row with the smaller cost.*

     ii. If the next-node entry is the same, the receiving node chooses the new row.

Updating in distance vector routing



DVR:The Count-to-Infinity Problem

- The main issue with **D**istance Vector **R**outing (DVR) protocols is Routing Loops, since Bellman-Ford Algorithm cannot prevent loops.
- This routing loop in DVR network causes Count to Infinity Problem.
- Routing loops usually occur when any interface goes down or two-routers send updates at the same time.
- Imagine a network with a graph as shown below in figure

Link Between A & B is Broken

	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

DVR:The Count-to-Infinity Problem

- As you see in this graph, there is only one link between A and the other parts of the network. Now imagine that the link between A and B is cut.
- At this time, B corrects its table.
- After a specific amount of time, routers exchange their tables, and so B receives C's routing table. Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A).
- B receives this table and thinks there is a separate link between C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).
- Once again, routers exchange their tables. When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).
- **This process loops until all nodes find out that the weight of link to A is infinity.**

DVR: The Count-to-Infinity Problem

- One way to solve this problem is for routers to send information only to the neighbors that are not exclusive links to the destination. For example, in this case, C shouldn't send any information to B about A, because B is the only way to A.

	B	**C**	**D**
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	.....	....	....
∞	∞	∞	∞

Link State Routing

- In link state routing, each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)- the node can use Dijkstra's algorithm to build a routing table.
- Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology.
- The topology must be dynamic, representing the latest state of each node and each link. If there are changes in any point in the network, the topology must be updated for each node.

Link State Routing

- **Each router must do the following things to make it work:**
  1. Discover its neighbors and learn their network addresses.
  2. Set the distance or cost metric to each of its neighbors.
  3. Construct a packet telling all it has just learned.
  4. Send this packet to and receive packets from all other routers.
  5. Compute the shortest path to every other router.

Link State Routing

- **Learning about the Neighbors**
  - When a router is booted, its first task is to learn who its neighbors are.
  - It accomplishes this goal by sending a special HELLO packet on each point-to-point line.
  - The router on the other end is expected to send back a reply giving its name.
- **Setting Link Costs**
  - The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.
  - By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.

Link State Routing

- **Building Link State Packets**
  - Link State Packets carries a minimum amount of data: the node identity, the list of links, a sequence number, and age.
  - The first two, node identity and the list of links, are needed to make the topology.
  - The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones.
  - The fourth, age, prevents old LSPs from remaining in the domain for a long time. LSPs are generated on two occasions:
    - When there is a change in the topology of the domain.
    - On a periodic basis.

Link State Routing

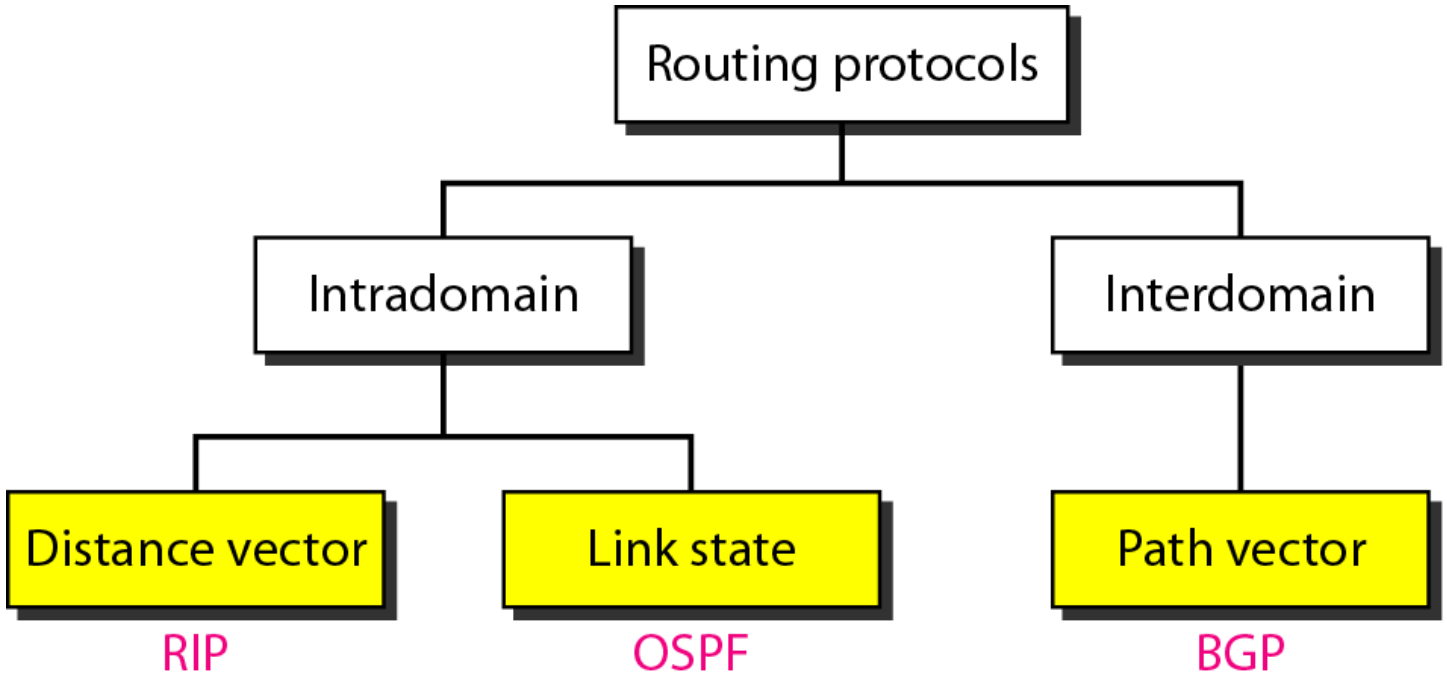
- **Distributing the Link State Packets**
  - After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors. The process is called flooding and based on the following:
    1) The creating node sends a copy of the LSP out of each interface.
    2) A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. If it is newer, the node does the following:
       a) It discards the old LSP and keeps the new one.
       b) It sends a copy of it out of each interface except the one from which the packet arrived. This guarantees that flooding stops somewhere in the domain (where a node has only one interface).

Link State Routing

- **Computing the New Routes**
  - Once a router has accumulated a full set of link state packets, it can construct the entire network graph because every link is represented. Every link is, in fact, represented twice, once for each direction.
  - Dijkstra's algorithm can be run locally to construct the shortest paths to all possible destinations.
  - The results of this algorithm tell the router which link to use to reach each destination. This information is installed in the routing tables, and normal operation is resumed.

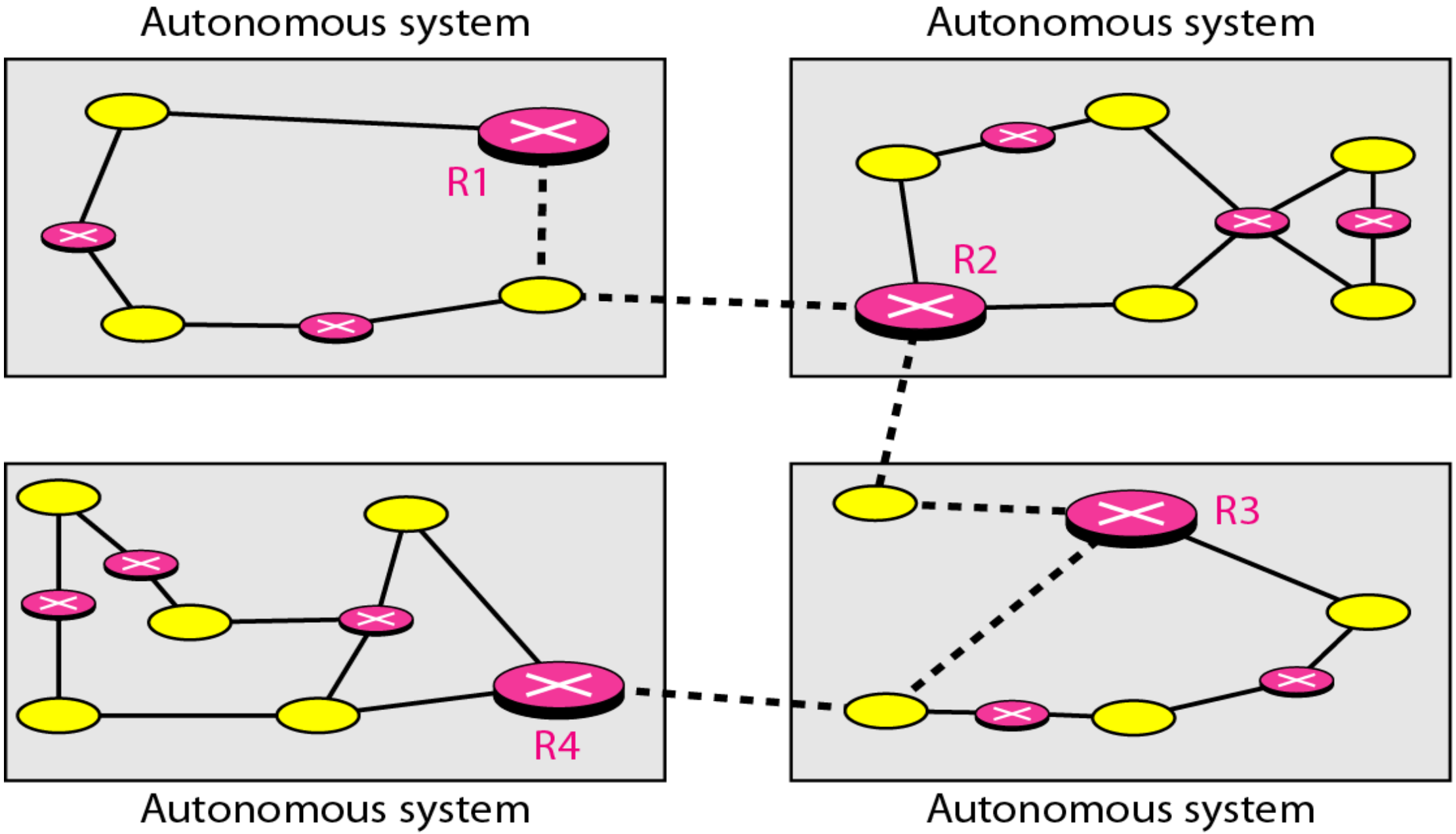
Routing Protocol

- Routing protocols have been created in response to the demand for dynamic routing tables.
- A routing protocol is a **combination of rules and procedures** that lets routers in the internet inform each other of changes.
- It allows routers to **share** whatever they know about the **internet or their neighborhood.**



Routing Protocol

- An internet is divided into autonomous systems.
- An **autonomous system (AS)** is a group of networks and routers under the authority of a single administration.
- Routing **inside an autonomous** system is referred to as **intradomain** routing.
- Routing **between autonomous** systems is referred to as **interdomain** routing.
- Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system.
- **Routing Information Protocol (RIP)** is an implementation of the distance vector protocol.
- **Open Shortest Path First (OSPF)** is an implementation of the link state protocol.
- **Border Gateway Protocol (BGP)** is an implementation of the path vector protocol.


Autonomous system
Autonomous system
R1
R2
R3
R4
Autonomous system
Autonomous system

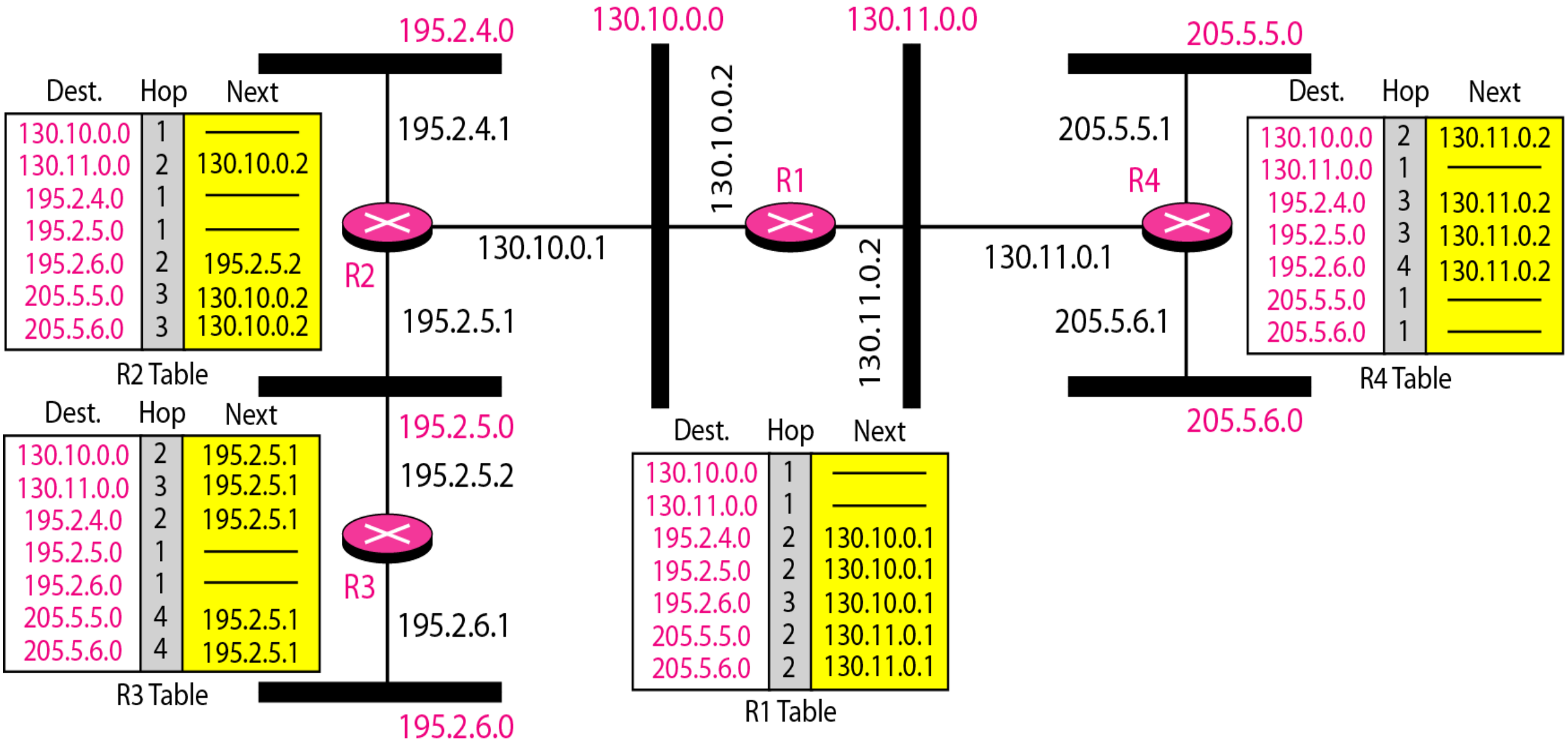
Routing Protocol

- Autonomous systems can divide into three categories: **stub, multihomed, and transit.**
  - **Stub** AS: A stub AS has only one connection to another AS. A good example of a stub AS is a small corporation or a small local ISP.
  - **Multihomed AS:** A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.
  - **Transit AS:** A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).

Routing Protocol: Routing Information Protocol (RIP)

- The Routing Information Protocol **(RIP) is an intradomain** routing protocol used **inside an autonomous** system. It is a very simple protocol based on distance vector routing.
- **RIP implements distance vector routing** directly with some considerations:
  1) In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.
  2) The destination in a routing table is a network, which means the first column defines a network address.
  3) The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.
  4) Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
  5) The next-node column defines the address of the router to which the packet is to be sent to reach its destination.

Example of a domain using RIP



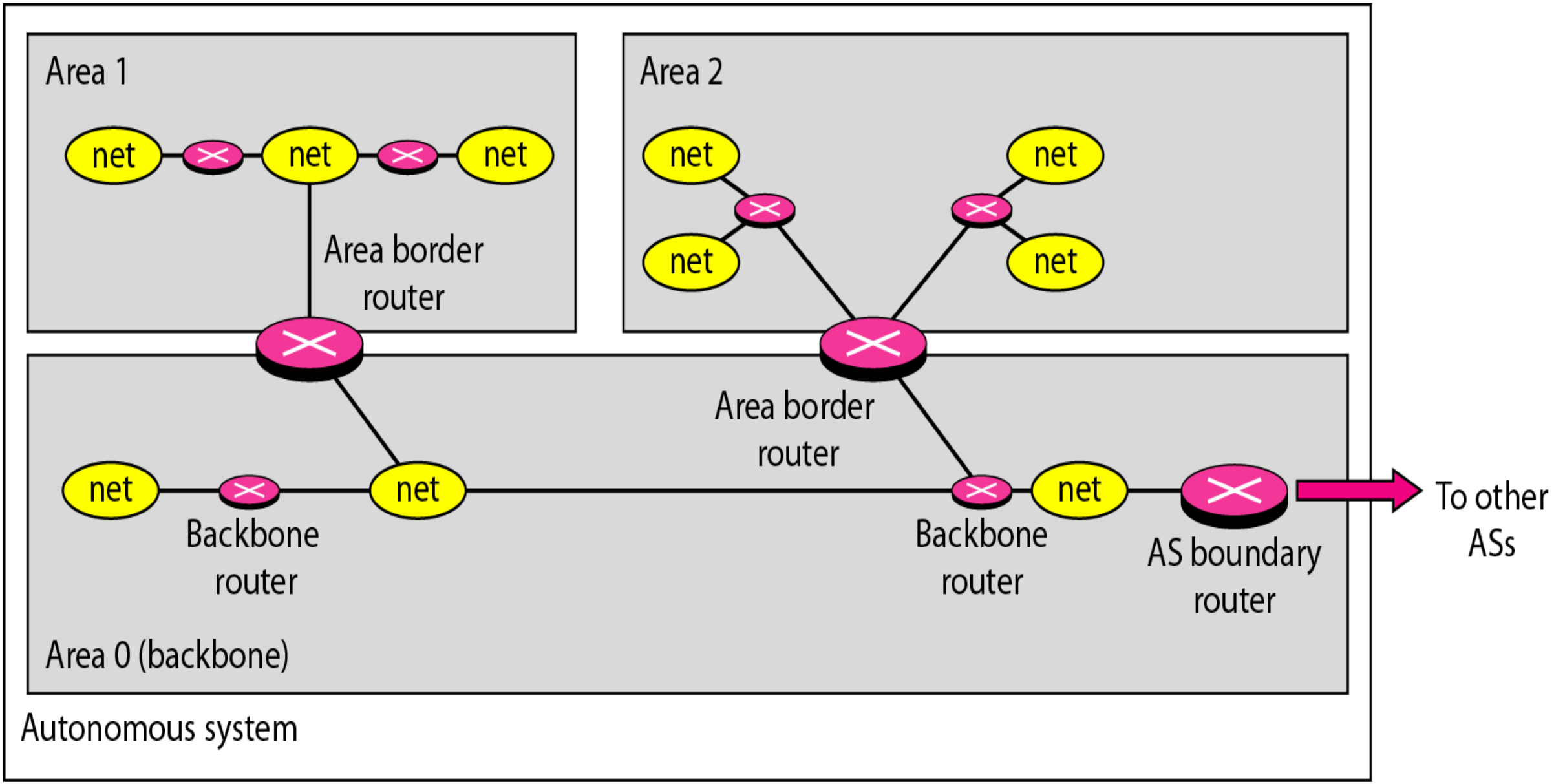
Routing Protocol: Routing Information Protocol (RIP)

- Let us look at the routing table for R1. The table has seven entries to show how to reach each network in the autonomous system.
- Router R1 is directly connected to networks 130.10.0.0 and 130.11.0.0, which means that there are no next-hop entries for these two networks.
- To send a packet to one of the three networks at the far left, router R1 needs to deliver the packet to R2.
- The next-node entry for these three networks is the interface of router R2 with IP address 130.10.0.1.
- To send a packet to the two networks at the far right, router R1 needs to send the packet to the interface of router R4 with IP address 130.11.0.1.
- The other tables can be explained similarly.

Routing Protocol: Open Shortest Path First (OSPF)

- **OSPF protocol is an intradomain routing protocol** based on link state routing. Its domain is also an autonomous system.
- An **intradomain routing protocol** is also called an **interior gateway routing protocol**.
- OSPF divides an autonomous system into **many different areas**. An area is a collection of networks, hosts, and routers all contained within an autonomous system. All networks inside an area must be connected.
- Routers inside an area **flood the area with routing information**. At the border of an area, special routers called **area border routers** summarize the information about the area and send it to other areas.
- Among the areas inside an autonomous system is a special area called the **backbone**; all the areas inside an autonomous system **must be connected** to the backbone. In other words, the **backbone serves as a primary** area and the **other areas as secondary areas**.

Areas in an autonomous system

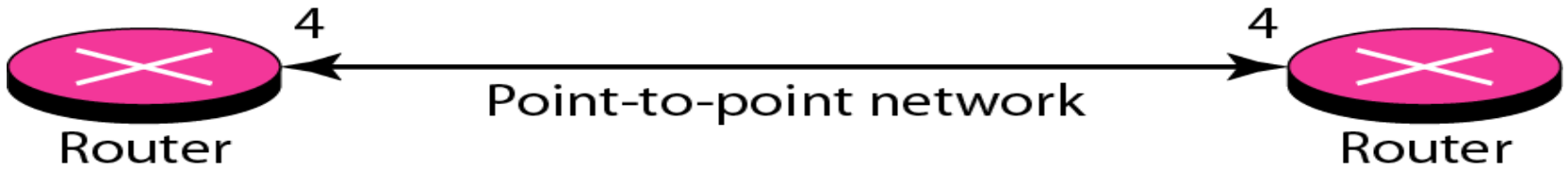


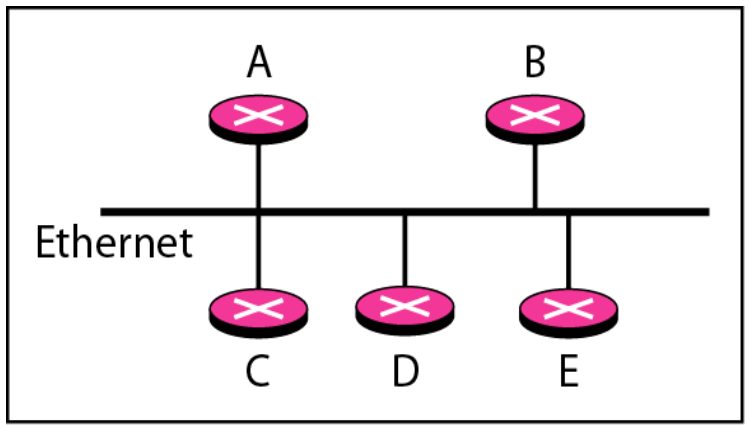
Routing Protocol: Open Shortest Path First (OSPF)

- ***OSPF had a long list of requirements that had to be met:***
  - **First,** the algorithm had to be published in the **open literature**, hence the **"O" in OSPF.**
  - **Second,** the new protocol had to support a **variety of distance metrics**, including physical distance, delay, and so on.
  - Third, it had to be a **dynamic algorithm**, one that adapted to changes in the topology automatically and quickly.
  - Fourth, and new for OSPF, it had to support **routing based on type of service**.
  - Fifth, OSPF had to do **load balancing**, **splitting the load over multiple lines**. Most previous protocols sent all packets over a single best route, even if there were two routes that were equally good.
  - Sixth, support for **hierarchical systems** was needed.
  - Finally, provision was needed for dealing with **routers that were connected to the Internet via a tunnel.**

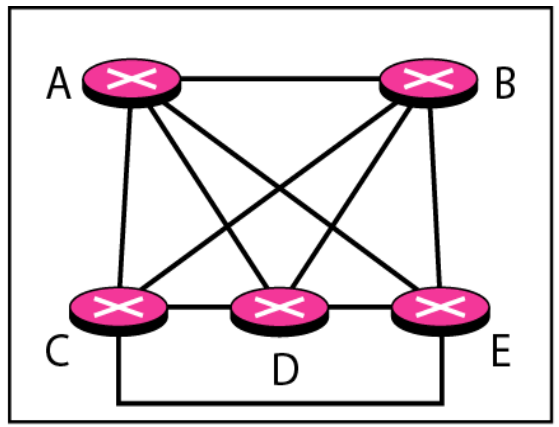
Routing Protocol: Open Shortest Path First (OSPF)

- In OSPF terminology, a connection is called a *link*. Four types of links have been defined: **point-to-point, transient, stub, and virtual.**
  - A **point-to-point link** connects two routers without any other host or router in between.
  - A **transient link** is a network with several routers attached to it. The data can enter through any of the routers and leave through any router.
  - A **stub link** is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same router.
  - When the link between two routers is broken, the administration may create a **virtual link** between them, using a longer path that probably goes through several routers.

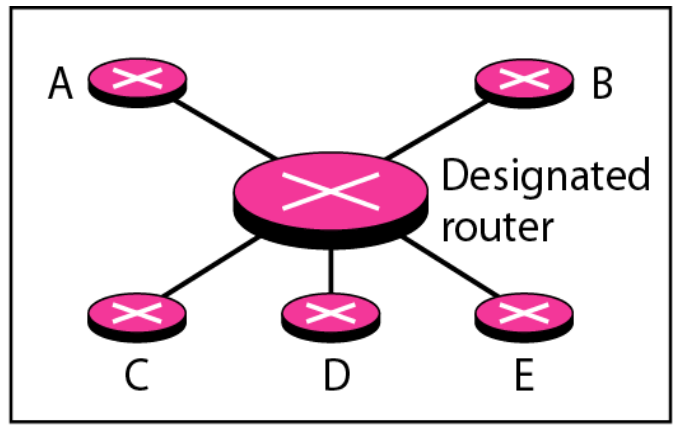




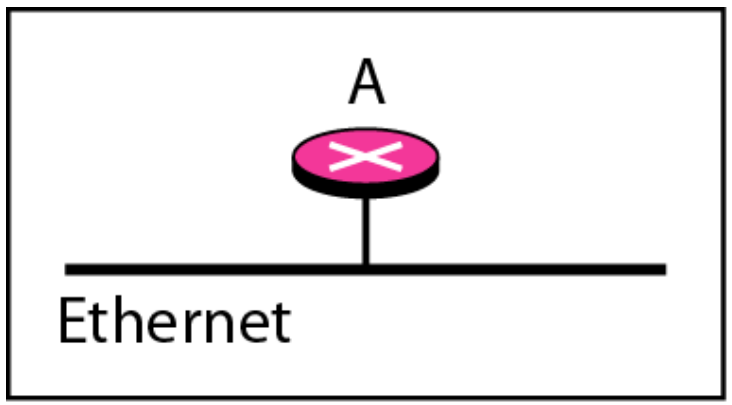
a. Transient network



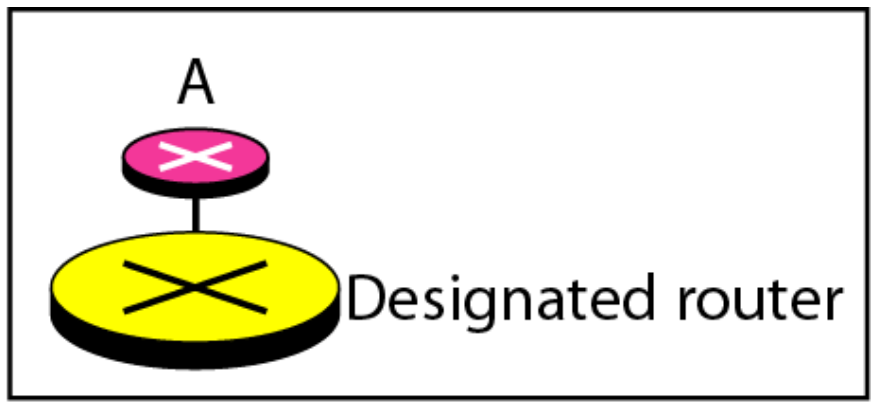
b. Unrealistic representation



c. Realistic representation



a. Stub network



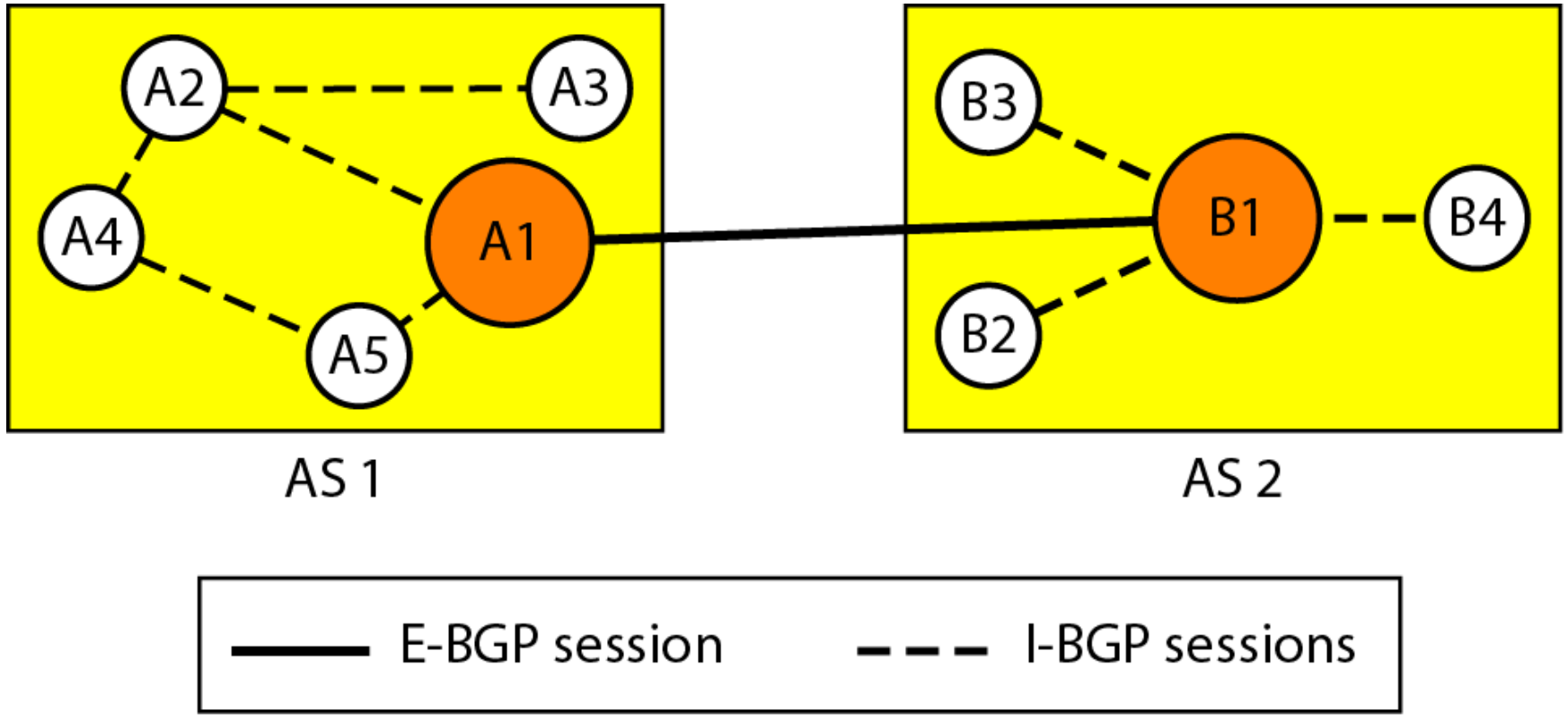
b. Representation

Message type	Description
Hello	Used to discover who the neighbors are
Link state update	Provides the sender's costs to its neighbors
Link state ack	Acknowledges link state update
Database description	Announces which updates the sender has
Link state request	Requests information from the partner

Figure 5-66. The five types of OSPF messages.

Routing Protocol: Border Gateway Protocol (BGP)

- Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing.
- All an intradomain protocol has to do is move packets as efficiently as possible from the source to the destination.



Routing Protocol: Border Gateway Protocol (BGP)

- The exchange of routing information between two routers using BGP takes place in a session. A session is a connection that is established between two BGP routers only for the sake of exchanging routing information.
- To create a reliable environment, BGP uses the services of TCP.
- BGP can have two types of sessions: external BGP (**E-BGP**) and internal BGP (**I-BGP**) sessions.
- The **E-BGP session** is used to exchange information **between two speaker nodes belonging to two different autonomous systems**.
- The **I-BGP session**, on the other hand, is used to **exchange routing information between two routers inside an autonomous system.**
- An AS might be a small company, or an international backbone network. There is no way of telling from the route. BGP does not even try because different ASes may use different intradomain protocols whose costs cannot be compared. Even if they could be compared, an AS may not want to reveal its internal metrics. This is one of the ways that interdomain routing protocols differ from intradomain protocols.

Enhanced Interior Gateway Protocol (EIGRP)

- EIGRP stands for Enhanced Interior Gateway Protocol which allows router to share information to the neighboring routers which are within the same area.
- Instead of sending the entire information to the neighboring router, the information which is needed are shared which reduces the workload and amount of data needs to be transmitted.
- EIGRP (Enhanced Interior Gateway Protocol) designed by CISCO system which can be used only in CISCO routers, but in 2013 it became open source, so it can be used in other routers.

Interior Gateway Routing Protocol (IGRP)

- IGRP stands for Interior Gateway Routing protocol which uses distance vector protocol (interior) to exchange data within a system .
- It supports multiple metrics for each node which includes delay, load and bandwidth, in order to compare the 2 routes which are combined into single metrics.
- The port number for IGRP is 9 which are used for communication and by default every 90 seconds it updates the routing information .

Intermediate-System to Intermediate - System (IS- IS)

- IS-IS stands for Intermediate-system to Intermediate - system which uses link-state routing algorithm for high speed data transmission.
- IS-IS (Intermediate-system to Intermediate system) uses Dijkstra’s algorithm in which independent database built by each IS-IS router for computing the best path for transmission in a network.
- It is standardized by ISO .

Unicast And Multicast Routing Protocols

Unicast

- In **unicast communication**, there is one source and one destination. The relationship between the source and the destination is **one-to-one**.
- In unicasting, the router **forwards the received** packet through **only one of its interfaces.**
- The router may **discard the packet** if it **cannot find the destination** address in its routing table.
- In **multiple unicasting**, several packets start from the source. If there are **five destinations**, for example, the source **sends five packets**, each with a different unicast destination address. Note that there may be multiple copies traveling between two routers.
- **For example**, when a person **sends an e-mail message to a group of people**, this is multiple unicasting.

Unicast And Multicast Routing Protocols

- **Multicast**
  - In multicast communication, there is one source and a group of destinations. The relationship is **one-to-many**.
  - In this type of communication, the source address is a unicast address, but the destination address is a group address, which defines one or more destinations.
  - A multicast packet starts from **the source S1 and goes to all destinations that belong to group G1.**
  - In multicasting, when a router receives a packet, it may forward it through several of its interfaces.
- In **broadcast communication**, the relationship between the source and the destination is **one-to-all**. There is only one source, but all the other hosts are the destinations.

ICMP (Internet Control Message Protocol)

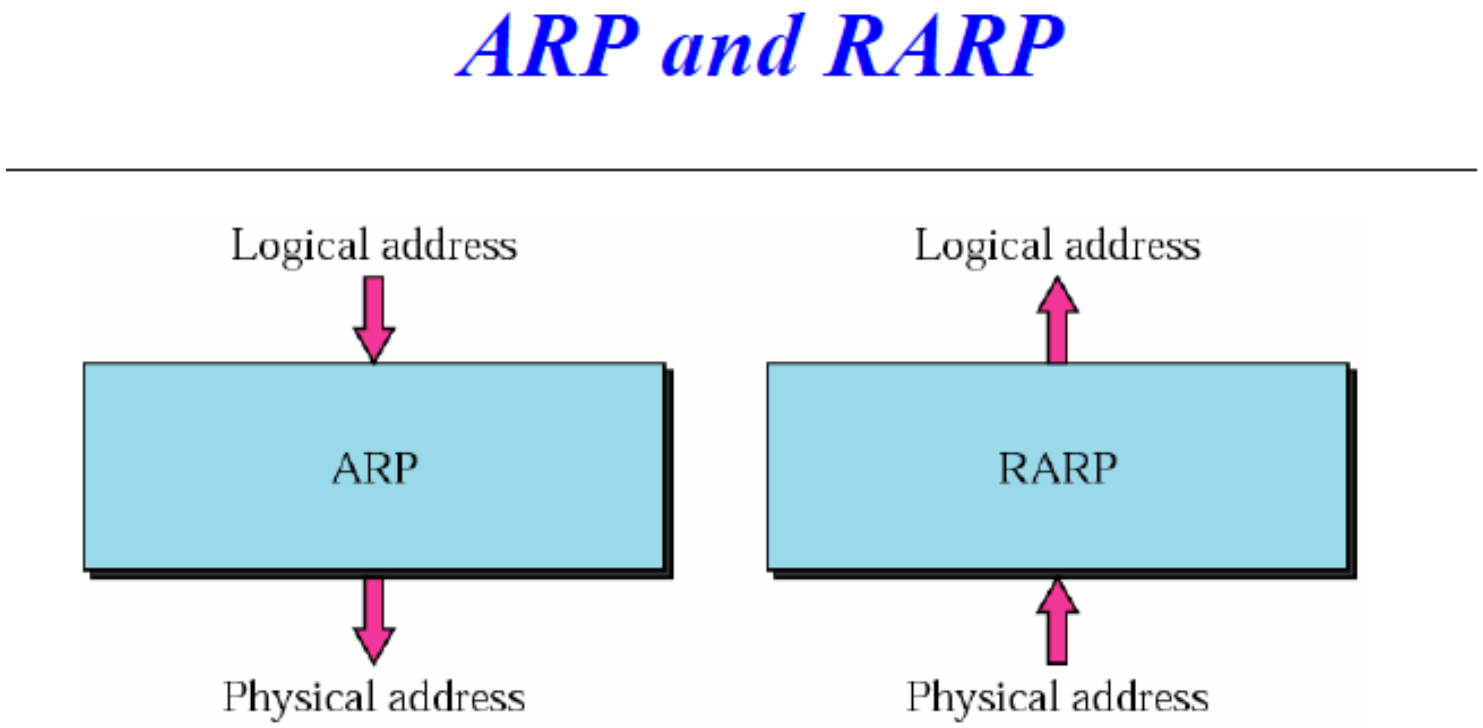
- The operation of the Internet is **monitored closely** by the routers. When something **unexpected occurs** during packet processing at a router, the event is **reported to the sender by the ICMP.**
- ICMP is also used to test the Internet. About a dozen types of ICMP messages are defined. Each ICMP message type is carried encapsulated in an IP packet.
- The **Destination Unreachable** message is used when the router cannot locate the destination.
- The **Time Exceeded** message is sent when a packet is dropped because its *(Time to live)* counter has reached zero.
- The **Parameter Problem** message indicates that an illegal value has been detected in a header field.
- The **Redirect** message is used when a router notices that a packet seems to be routed incorrectly.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

Figure 5-60. The principal ICMP message types.

ARP And RARP

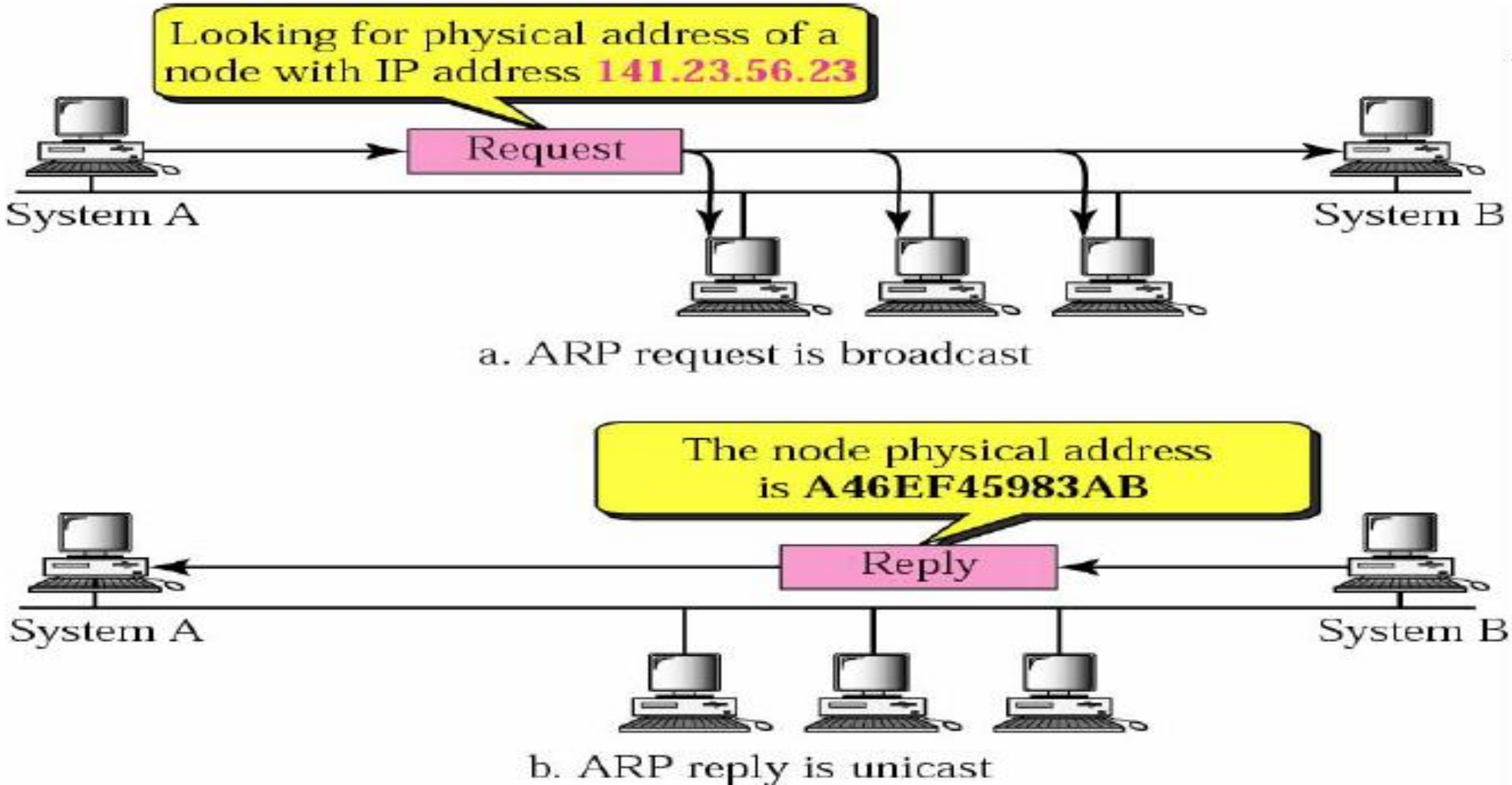
- **ARP —The Address Resolution Protocol**
- **RARP —The Reverse Address Resolution Protocol**



ARP Operation

- **To find the physical address of another host or router on its network**
  - Send an ARP request message
- **ARP request message**
  - *The physical address of the sender and The IP address of the sender*
  - *The physical address of the receiver is 0s and The IP address of the receiver*
- **Then, ARP request message is broadcast by the physical layer**
  - For example: in Ethernet, MAC header's destination address is all 1s (broadcast address)
  - Received by every station on the physical network
- **The intended recipient send back an ARP reply message**
  - ARP reply message packet is unicast

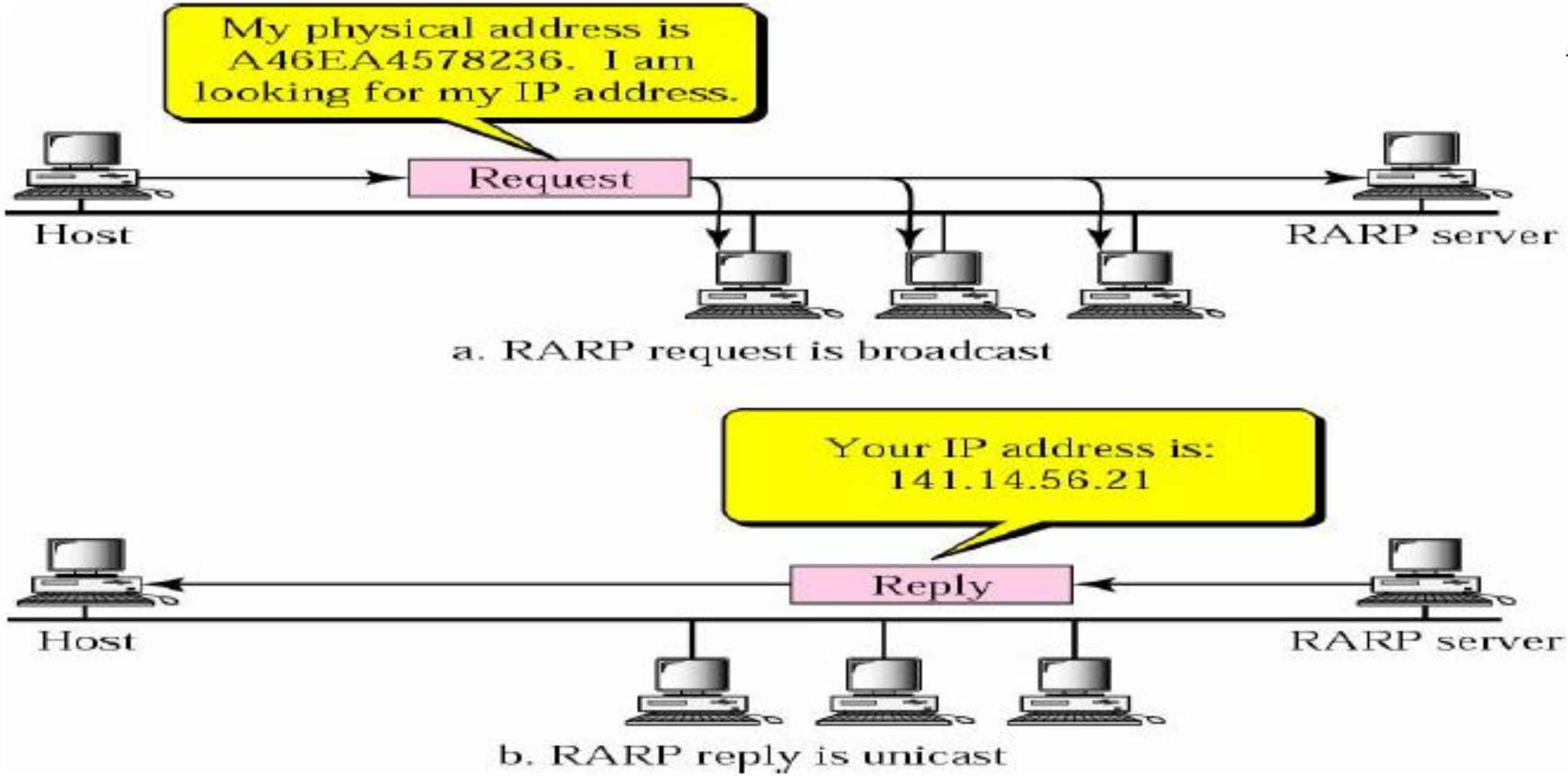
ARP Operation



RARP

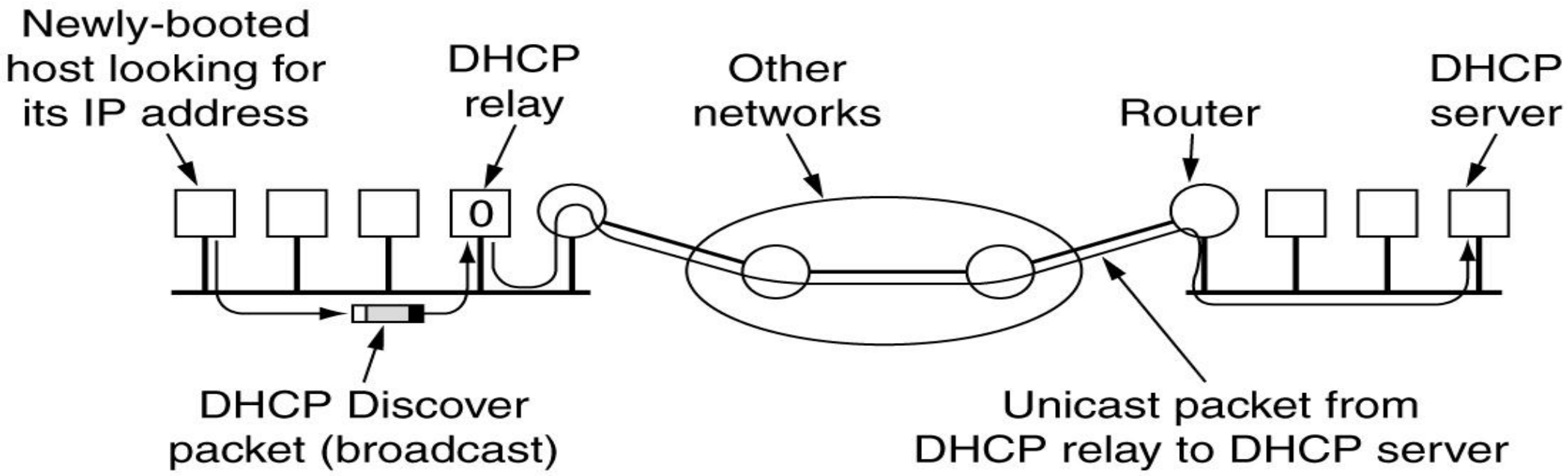
- It cannot include the IP address
  - IP address are assigned by the network administrator
- Obtain its logical address by the physical address using the RARP protocol
- The RARP request packets are broadcast; the RARP reply packets are unicast.

RARP Operation



Dynamic Host Configuration Protocol

Operation of DHCP.



Acquiring IP

- DHCPDISCOVER Broadcast
- DHCP SERVER Receives and send DHCPOFFER to sender
- DHCPREQUEST broadcast (Multiple DHCP)
- DHCPACK By server to sender (If available)
- DHCPNACK By server to sender (If not available)

When disconnecting or remove from network

- DHCPRELEASE to server
- DHCPINFORM to server if manually configured.

Thank You
???

References:

- Data Communications and Networking " Behrouz A. Forouzan" Fourth Edition.
- Computer Networks "A. S. Tanenbaum" Fifth Edition
- Data and Computer Communications "William Stallings" Tenth Edition.