SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

18CSS202J- COMPUTER COMMUNICATION

UNIT –V Contents

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Delivery - Types (Direct , Indirect)
- **Forwarding Techniques -**
  - Next -hop method
  - Route Method
  - Network specific Method
  - Host specific Method
  - Default Method
- **Forwarding Process:**

  Steps followed by Router

- **Routing**

  -Routing Table contents

  -Types of Routing - Static & Dynamic

  (including tables).

- **Autonomous system**
- Intradomain & Interdomain routing

- Types of Routing.
  - Distance vector Routing
  - Link state Routing
- Path vector Routing
- PROBLEM SOLVING

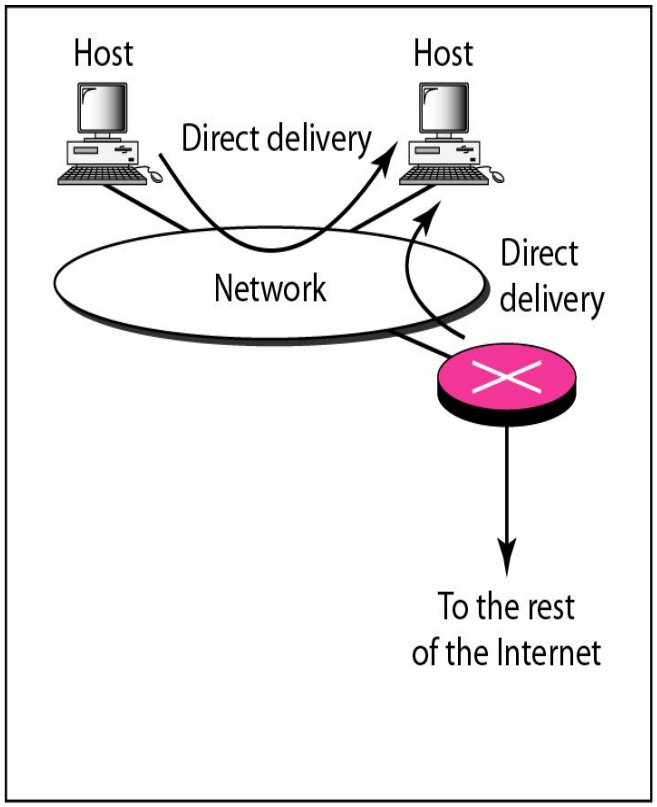
- RIP version 1 & RIP version2
- OSPF
- Comparison
- EIGRP
- BGP

22-1 DELIVERY

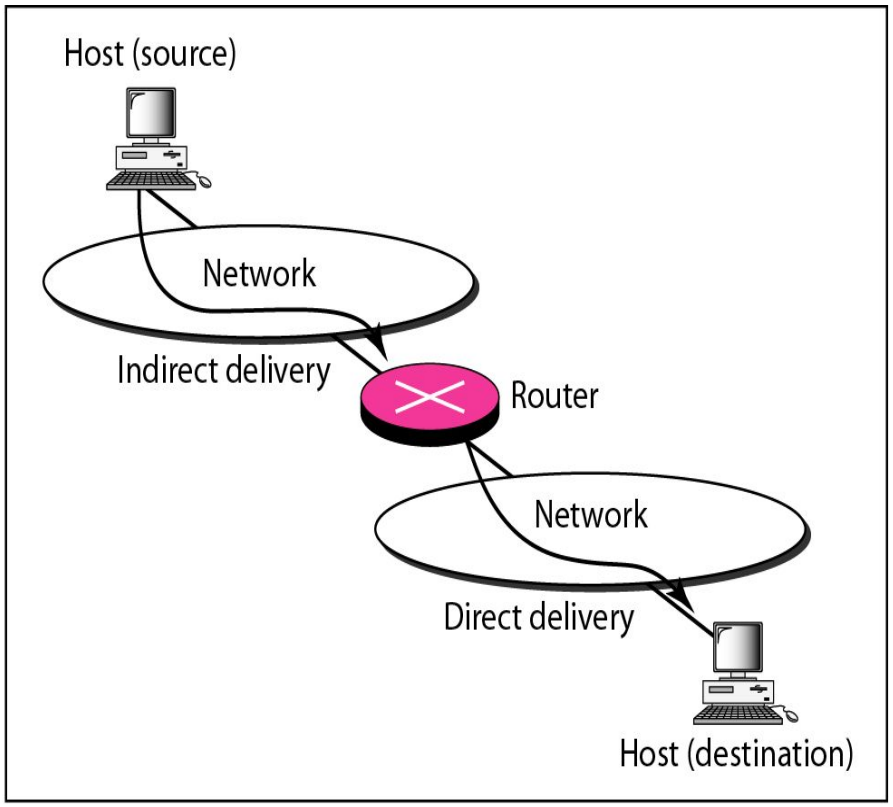
The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.

Topics discussed in this section:

Direct Versus Indirect Delivery



a. Direct delivery



b. Indirect and direct delivery

22-2 FORWARDING

Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

Topics discussed in this section:

Forwarding Techniques
Forwarding Process
Routing Table

Figure 22.2 *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	---

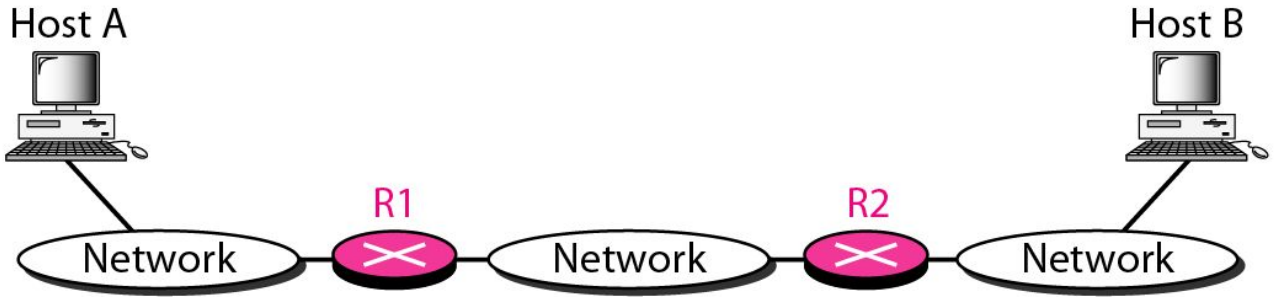


Figure 22.3 *Host-specific versus network-specific method*

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

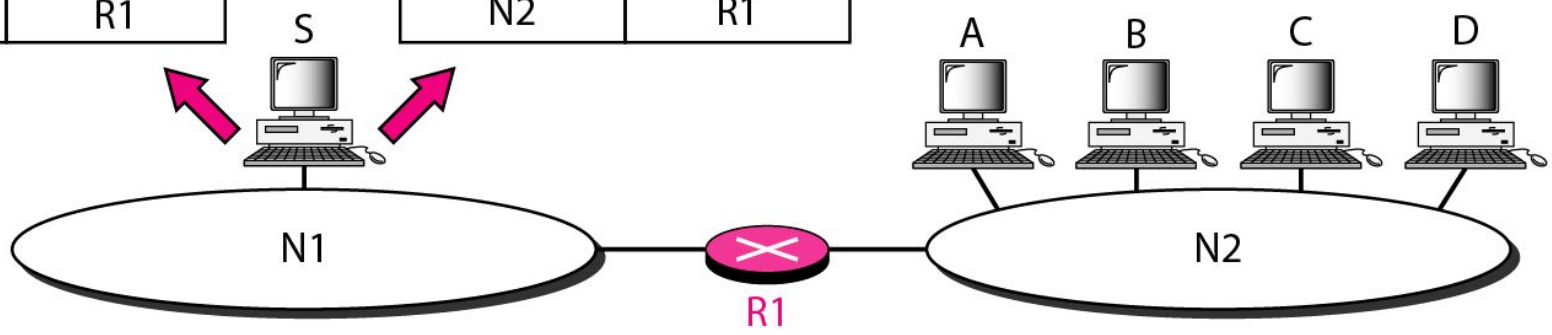
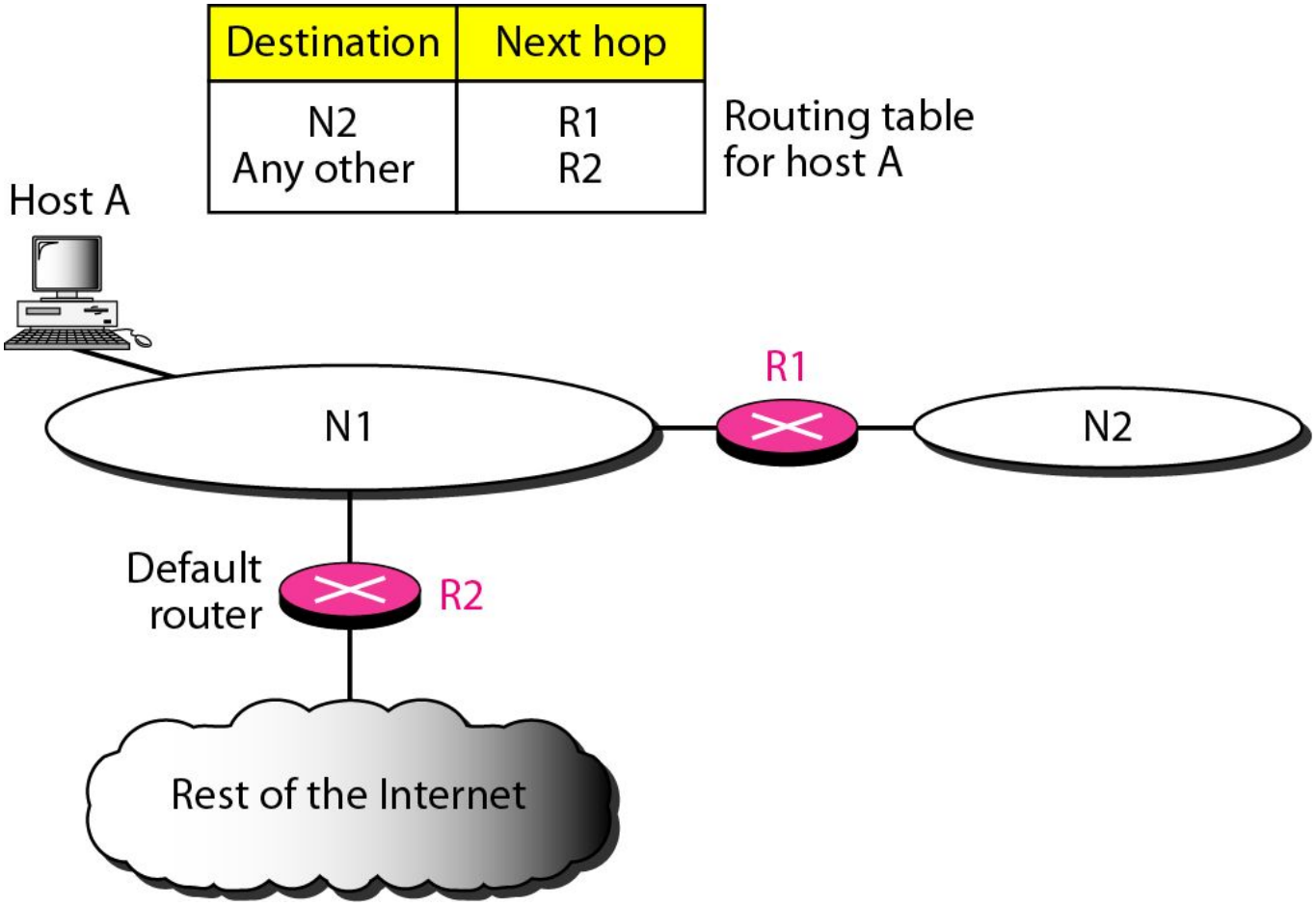
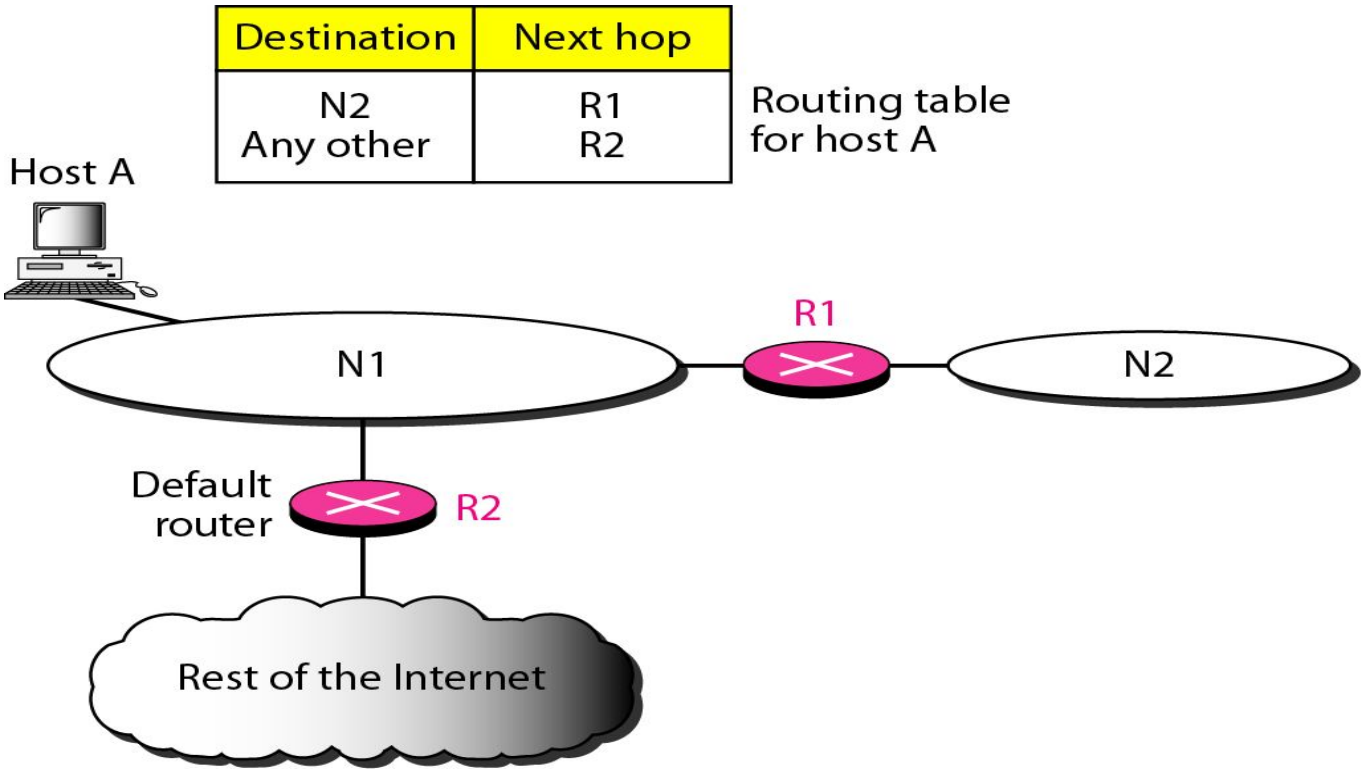


Figure 22.4 *Default method*



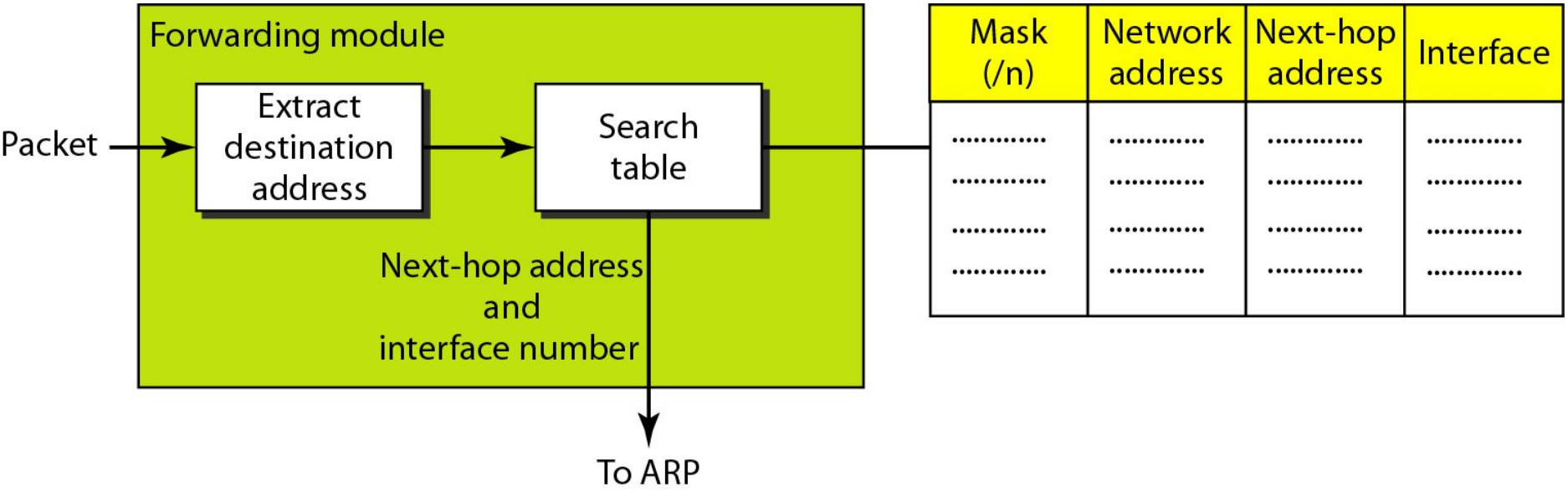
Default method



Host A have one entry called the default(normally defined as network address **(0.0.0.0**).

Forwarding Process

Simplified forwarding module in classless address



Example

Make a routing table for router R1, using the configuration in Figure.

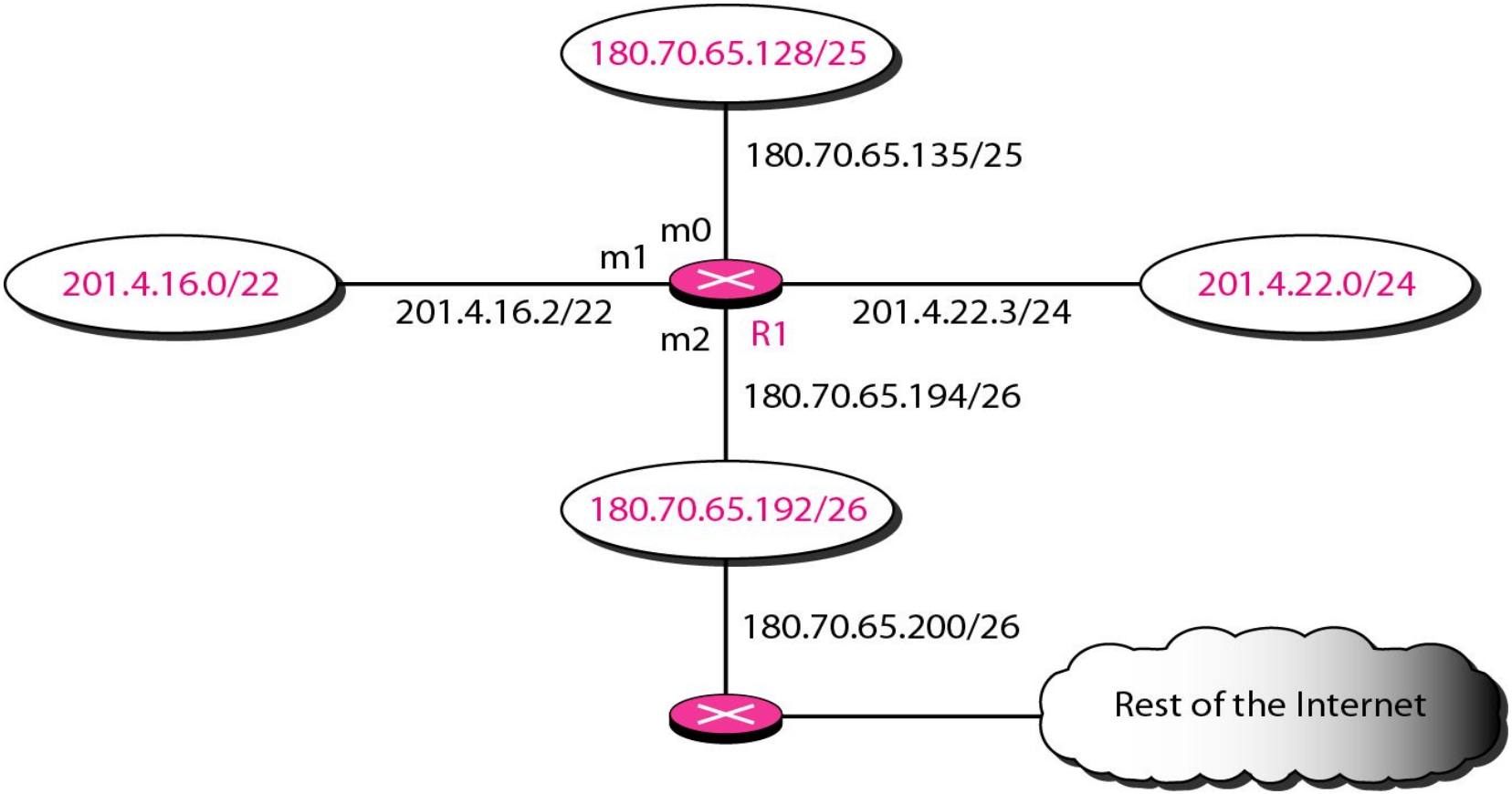


Table ***Routing table for router R1 in Figure***

Mask	*Network Address*	*Next Hop*	*Interface*
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	....	m1
Any	Any	180.70.65.200	m2

Static

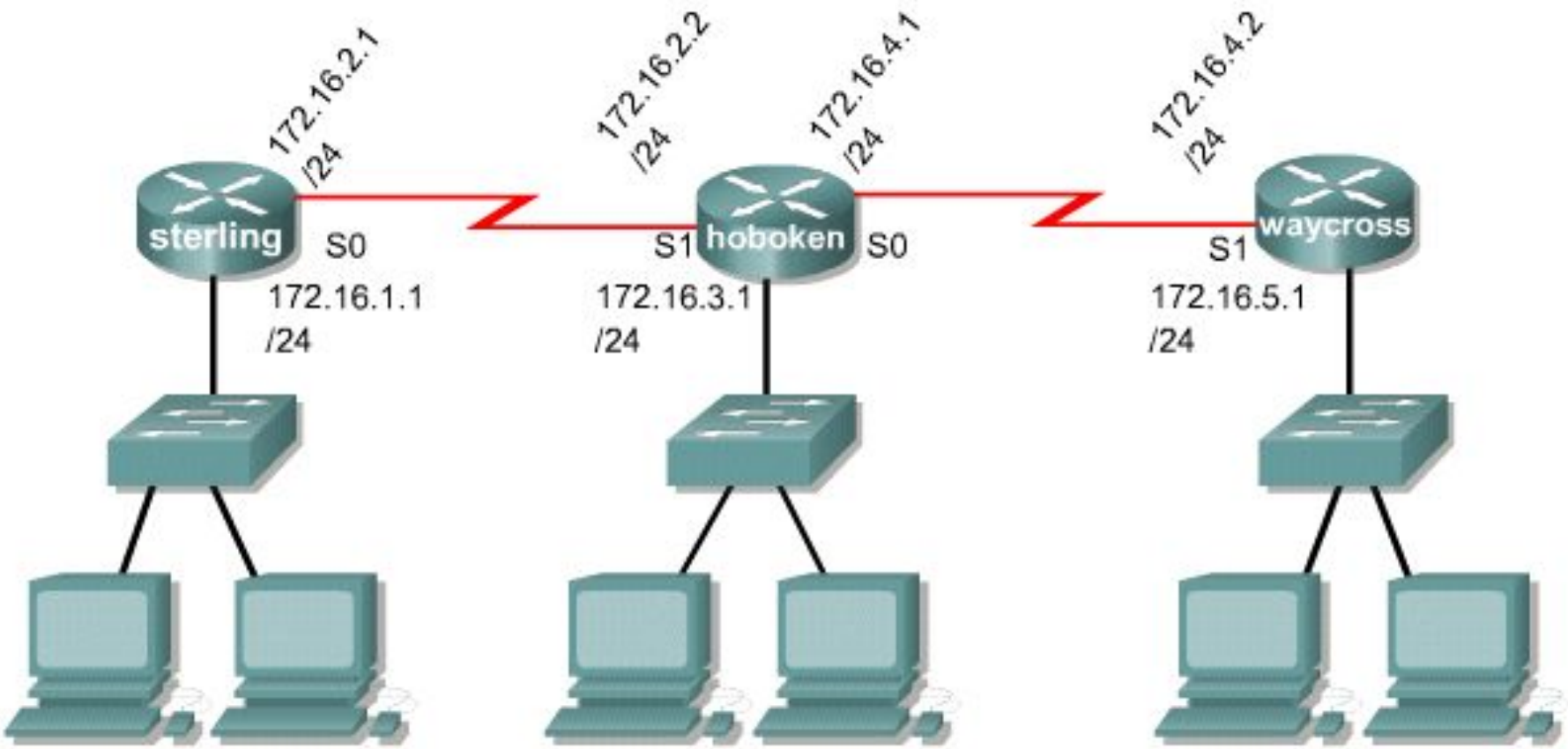
Uses a programmed route that a network administrator enters into the router

Dynamic

Uses a route that a routing protocol adjusts automatically for topology or traffic changes

Static route operation

- Static route operations can be divided into these three parts:
  - Network administrator configures the route
  - Router installs the route in the routing table
  - Packets are routed using the static route
- Since a static route is manually configured, the administrator must configure the static route on the router using the **ip route** command.




```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
                   command  destination   sub mask     gateway
                            network
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
                   command  destination   sub mask     gateway
                            network
```

Verifying static route configuration

- Use the following steps to verify static route configuration:
  - In privileged mode enter the command **show running-config** to view the active configuration.
  - Verify that the static route has been correctly entered.
  - Enter the command **show ip route**.
  - Verify that the route that was configured is in the routing table.

- Advantages of **static routing**
  - —-It can backup multiple interfaces/networks on a router
  - —-Easy to configure
  - —-No extra resources are needed
  - —-More secure
- Disadvantages of **static routing**
  - —-Network changes require manual reconfiguration
  - —-Does not scale well in large topologies

Dynamic Routing Table

- It is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF or BGP.
- Whenever there is a change in the internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers automatically.
- The routers in a big internet need to be updated dynamically for efficient delivery of the IP packets.

Figure ***Common fields in a routing table***

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
.....	.....	.....	.....	.....	.....	.....

Flags

- U(up): U flag indicated the router is up and running.
- G(gateway): G flag means that the destination is in another network.
- H(host-specific): H flag indicates that the entry in the network address is a host specific address.
- D(added by redirection)
- M(Modified by redirection)

Reference count

This field gives the number of users of this route at the moment.

Use

This field shows the number of packets transmitted through this router for the corresponding destination.

Figure 22.12 *Autonomous systems*

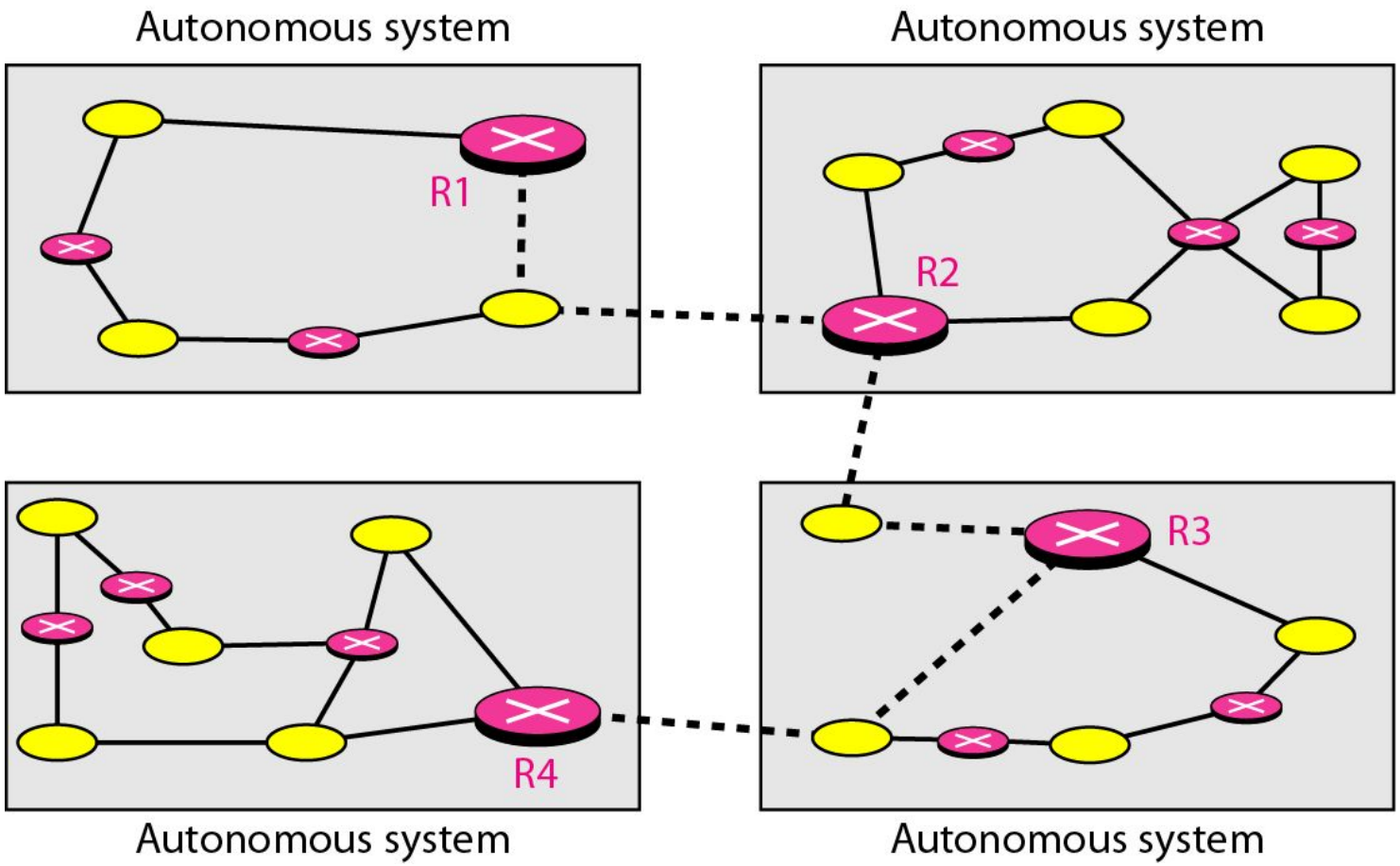
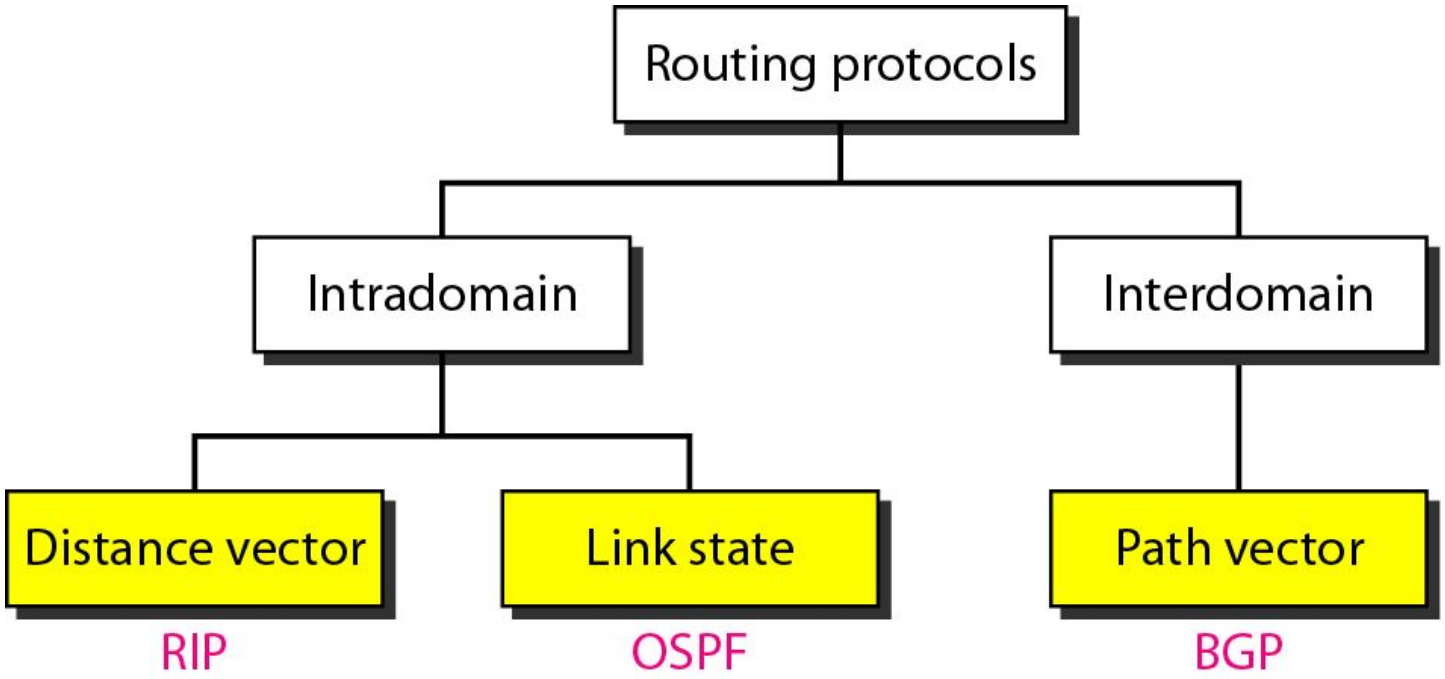


Figure 22.13 *Popular routing protocols*



Distance vector routing

- The least –cost route between any 2 nodes is the route with minimum distance.

- Initialization
- Sharing
- Updating

Figure *Distance vector routing tables*

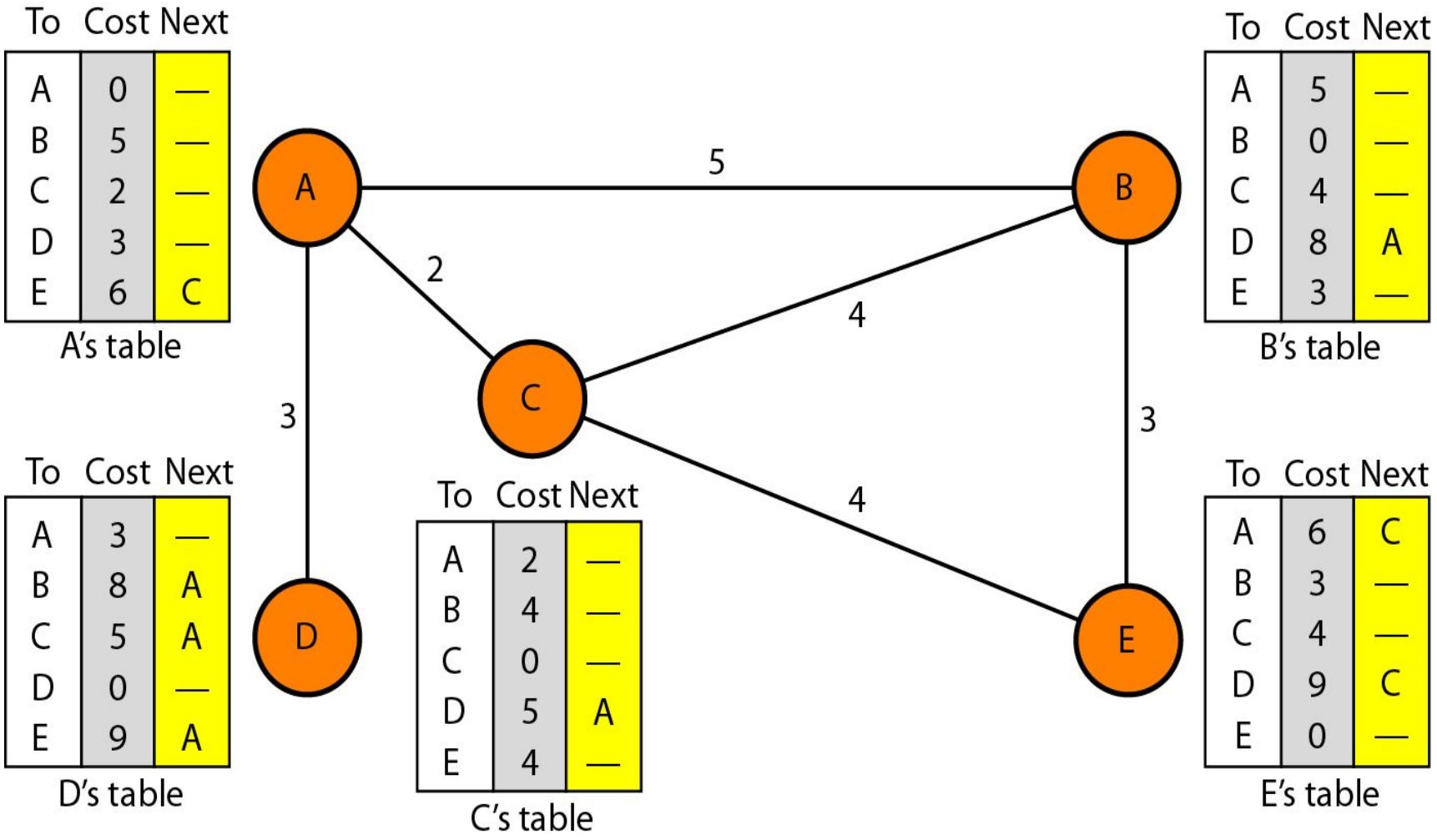
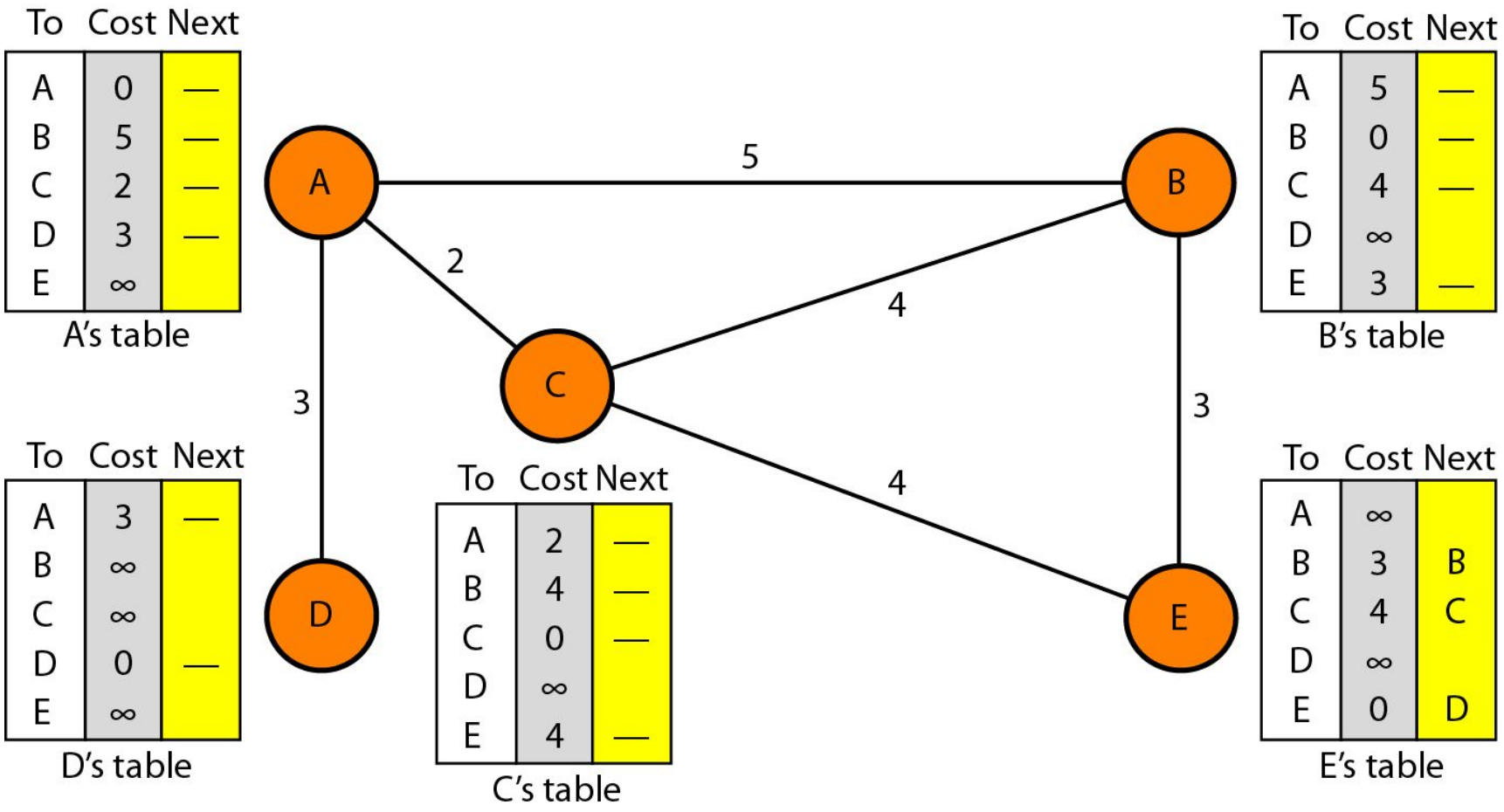


Figure *Initialization of tables in distance vector routing*



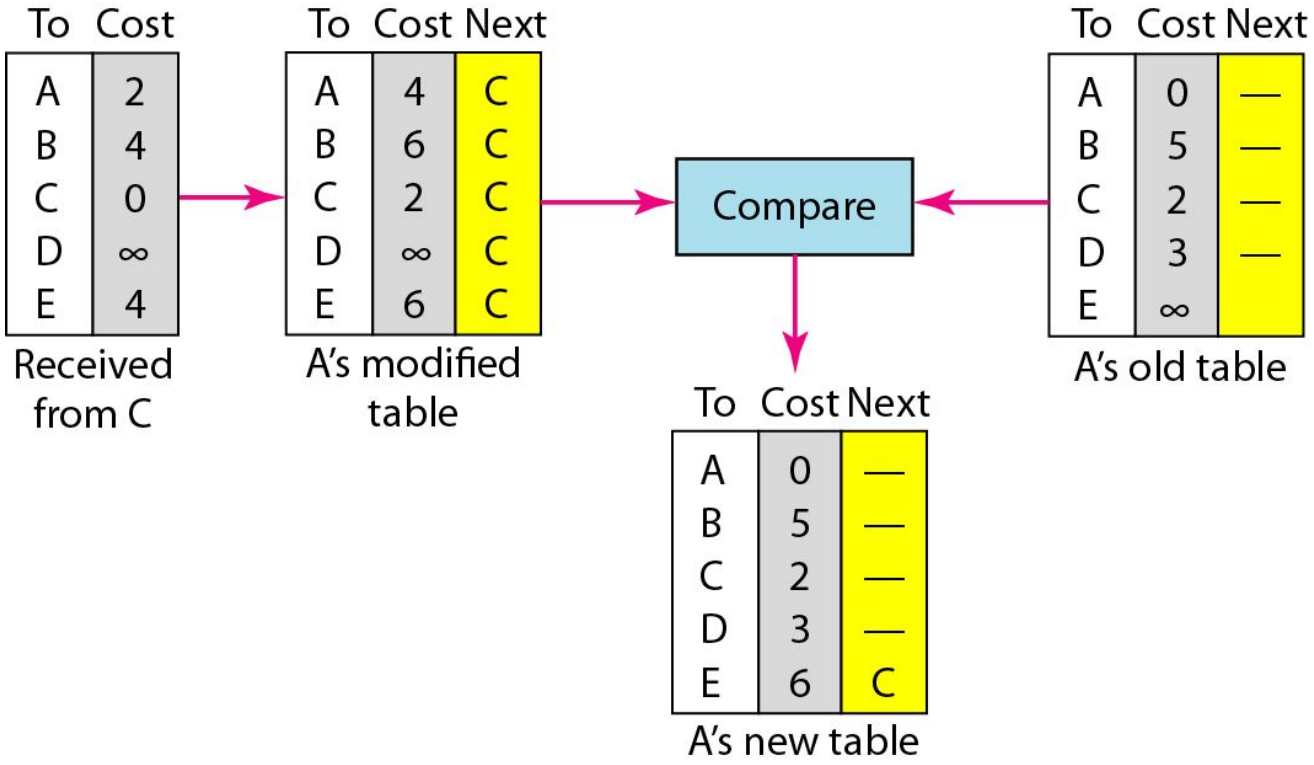
Sharing

In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

Updating

1. The receiving node needs to add the cost between itself and sending node to each value in the 2nd column.
2. The receiving node needs to add the name of the sending node to each row as the 3rd column.
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.

Figure *Updating in distance vector routing*

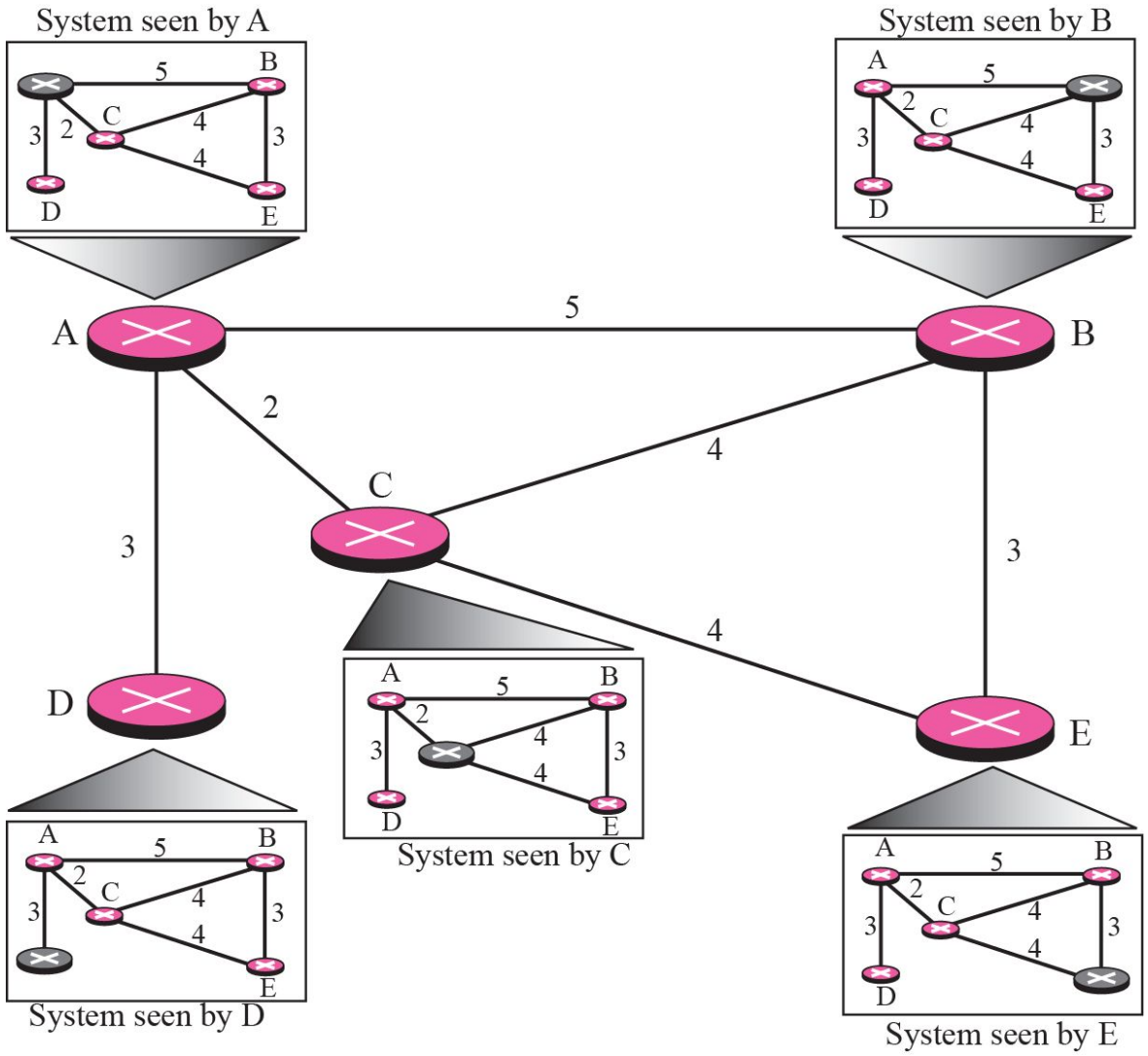


LINK STATE ROUTING

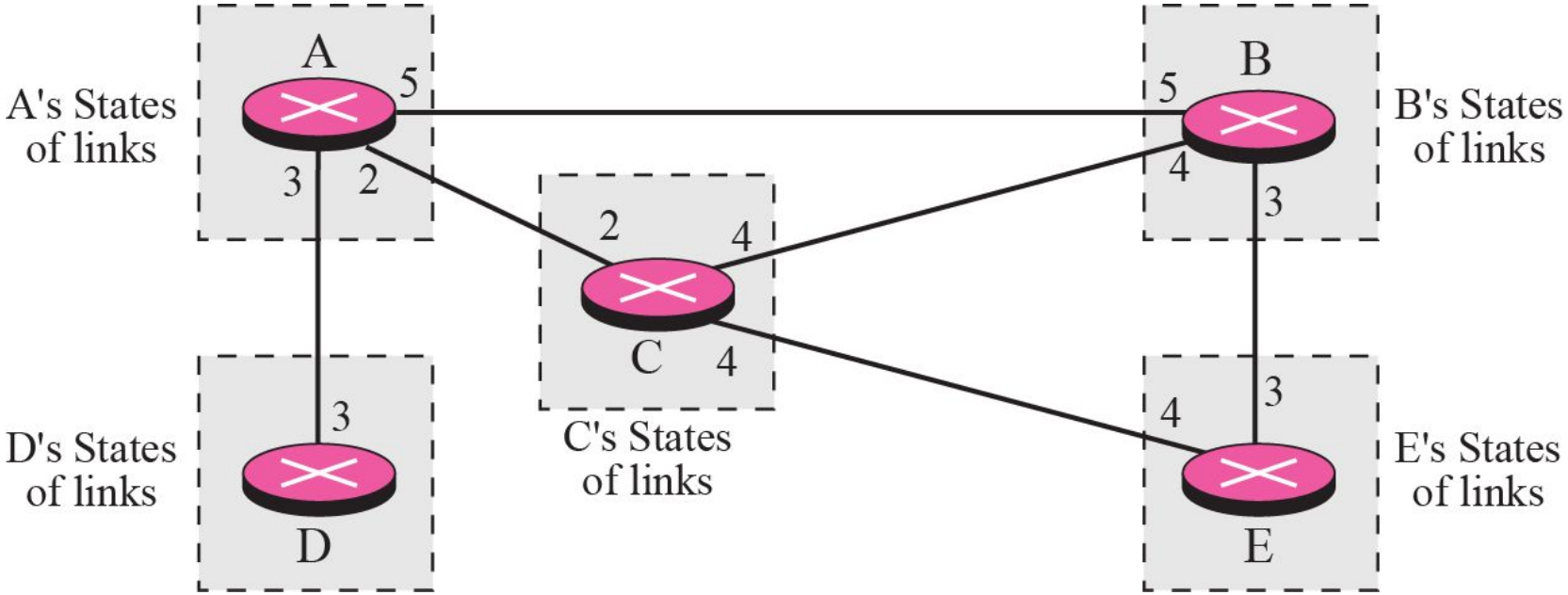
- Link state routing has a different philosophy from that of distance vector routing.
- In link state routing, if each node in the domain has the entire topology of the domain—the list of nodes and links, how they are connected including the

1. Type
2. Cost (metric)
3. The condition of the links (up or down)—the node can use the Dijkstra algorithm to build a routing table.

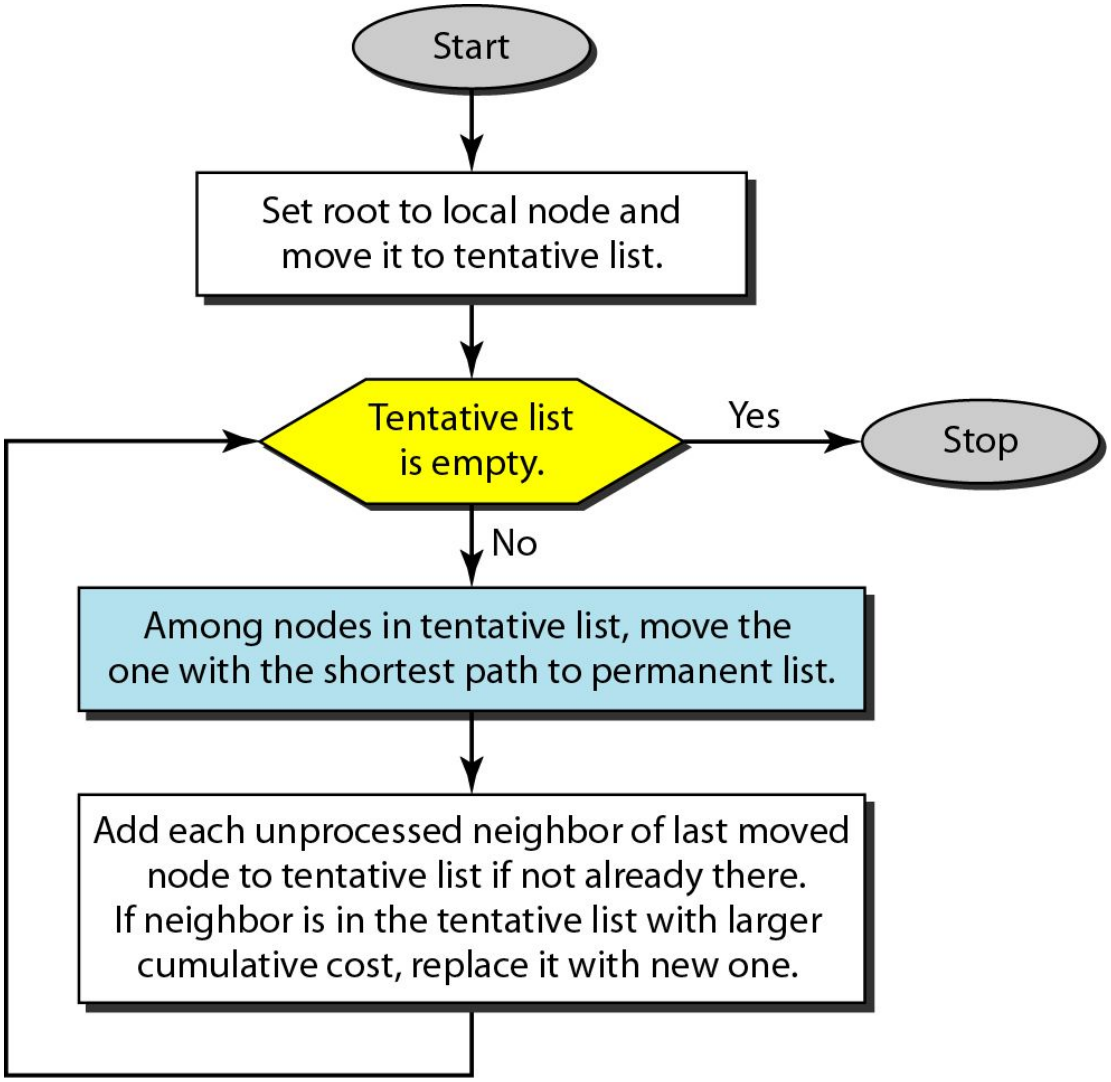
Concept of Link state routing



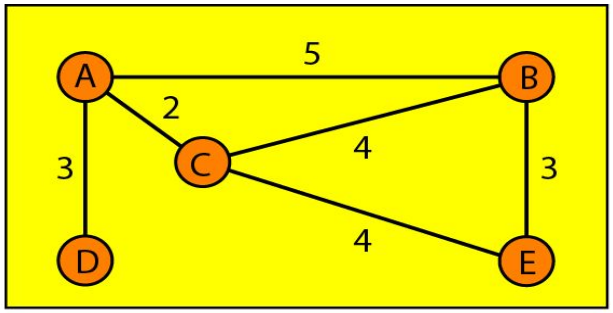
Link state knowledge



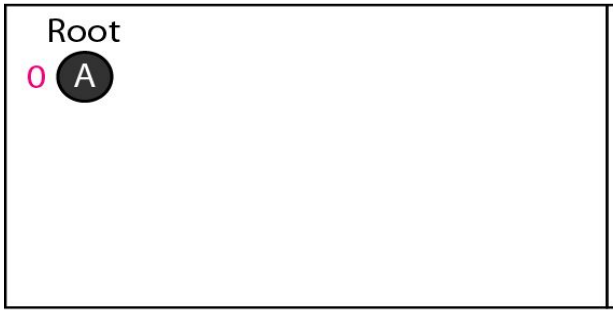
Dijkstra algorithm



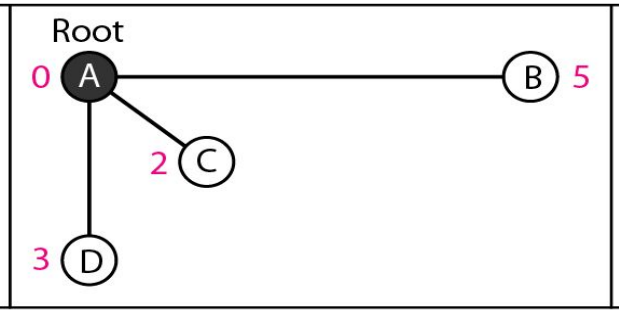
Example of formation of shortest path tree



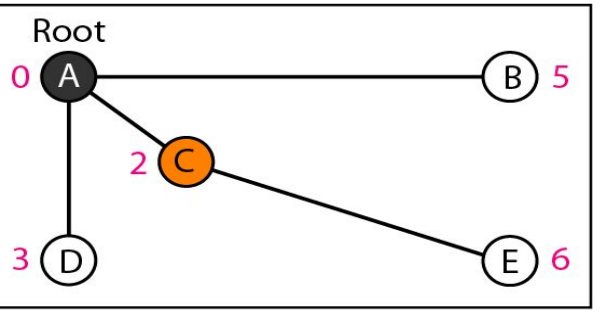
Topology



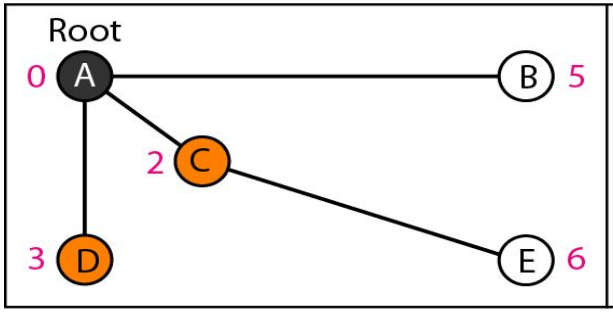
1. Set root to A and move A to tentative list.



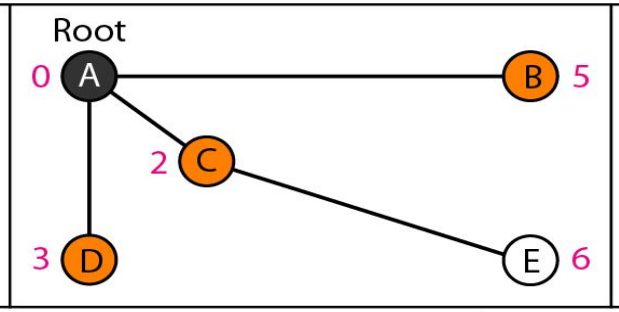
2. Move A to permanent list and add B, C, and D to tentative list.



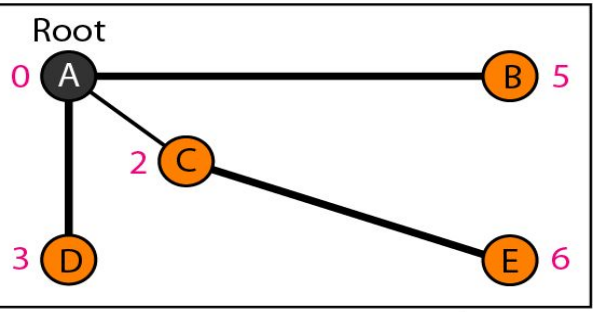
3. Move C to permanent and add E to tentative list.



4. Move D to permanent list.



5. Move B to permanent list.



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

Routing table for node A

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

Building Routing Tables

- Creation of the states of the links by each node, called the link state packets (LSP)
- Distribution of LSPs to every other routers, called flooding (efficiently)
- Formation of a shortest path tree for each node
- Calculation of a routing table based on the shortest path tree

PATH VECTOR ROUTING

- Distance vector and link state routing are both interior routing protocols. They can be used inside an autonomous system.
- Both of these routing protocols become intractable when the domain of operation becomes large.
- Distance vector routing is subject to instability if there is more than a few hops in the domain of operation.
- Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding.
- There is a need for a third routing protocol which we call path vector routing.

- The principle of path vector routing is similar to that of distance vector routing.
- In path vector, we assume that there is one node in each AS that acts on behalf of the entire AS. This is called as speaker node.
- The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs.
- A speaker node advertises the path, not the metric of the nodes, in its AS or other ASs.
- The idea is the same as for DV routing except that only speaker nodes in each AS can communicate with each other

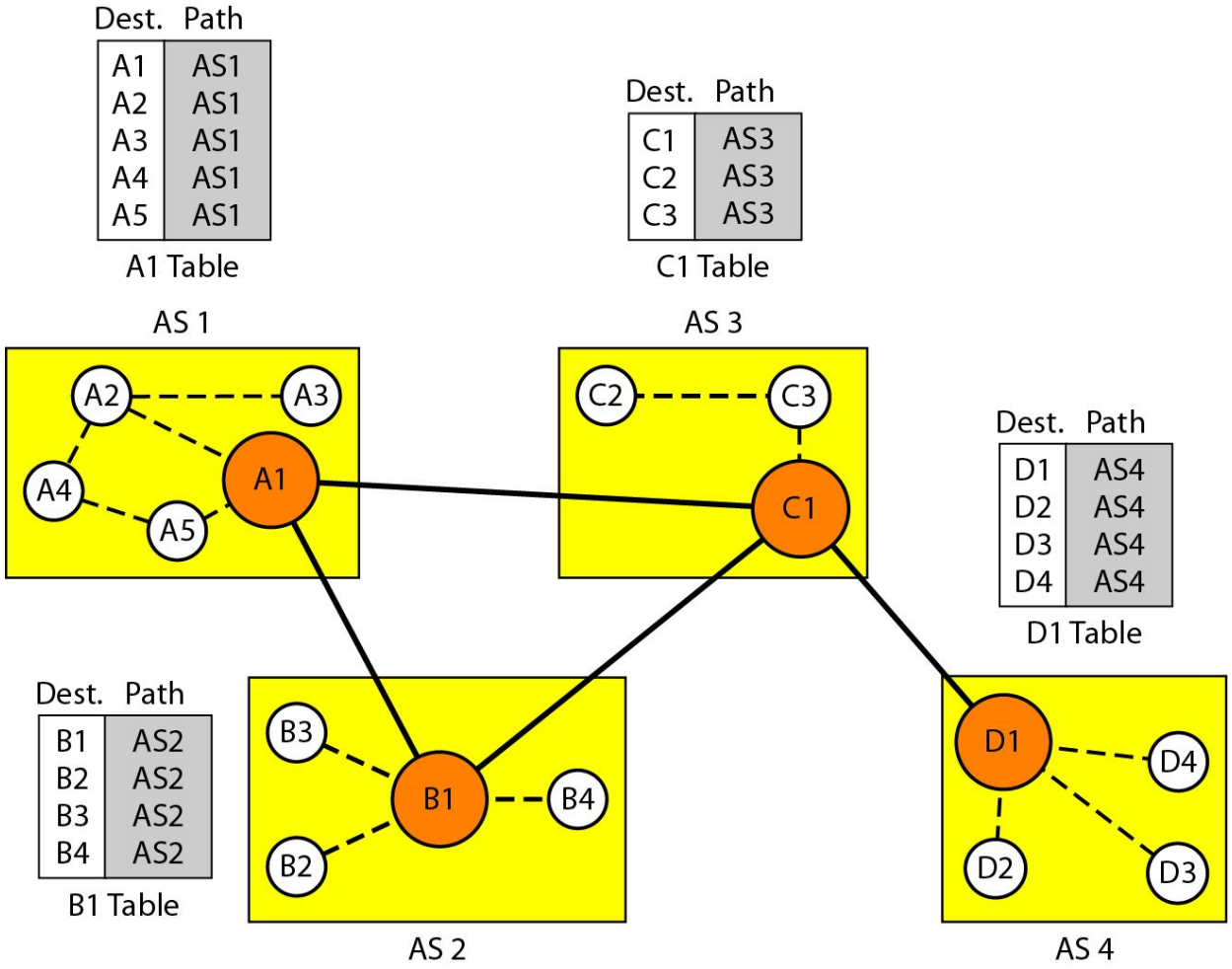
Initialization

- Each speaker node can know only the reachability of nodes inside its AS.
- Node A1 is the speaker node for AS1, B1 for AS2, C1 for AS3 and D1 for AS4.
- Node A1 creates an initial table that shows A1 to A5 are located in AS1 and can be reached through it.
- Node B1 advertises that B1 to B4 are located in AS2 and can be reached through B1. And so on.

Sharing

- A speaker in an AS shares its table with immediate neighbors.
- Node A1 shares its table with B1 and C1.
- Node C1 shares its table with B1 and D1.
- Node B1 shares its table with A1 and C1.
- Node D1 shares its table with C1.

Initial routing tables in path vector routing



Updating

- When a speaker node receives a two column table from a neighbor, it updates its own table by adding the nodes that are not in its routing table and adding its own AS and the AS that sent the table.
- After a while each speaker has a table and knows how to reach node in other Ass.

1. Loop prevention

- The instability of DV routing and the creation of loops can be avoided in PV routing.
- When a router receives a message, it checks to see if its AS is in the path list to the destination.
- If it is, looping is involved and the message is ignored.

Stabilized tables for three autonomous systems

Dest.	Path
A1 … A5	AS1 … AS1
B1 … B4	AS1-AS2 … AS1-AS2
C1 … C3	AS1-AS3 … AS1-AS3
D1 … D4	AS1-AS2-AS4 … AS1-AS2-AS4

A1 Table

Dest.	Path
A1 … A5	AS2-AS1 … AS2-AS1
B1 … B4	AS2 … AS2
C1 … C3	AS2-AS3 … AS2-AS3
D1 … D4	AS2-AS3-AS4 … AS2-AS3-AS4

B1 Table

Dest.	Path
A1 … A5	AS3-AS1 … AS3-AS1
B1 … B4	AS3-AS2 … AS3-AS2
C1 … C3	AS3 … AS3
D1 … D4	AS3-AS4 … AS3-AS4

C1 Table

Dest.	Path
A1 … A5	AS4-AS3-AS1 … AS4-AS3-AS1
B1 … B4	AS4-AS3-AS2 … AS4-AS3-AS2
C1 … C3	AS4-AS3 … AS4-AS3
D1 … D4	AS4 … AS4

D1 Table

2. Policy routing

- When a router receives a message, it can check the path.
- If one of the AS listed in the path is against its policy, it can ignore that path and that destination.
- It does not update its routing table with this path, and it does not send this message to its neighbors.

3. Optimum path

- It cannot include metrics in this route because each AS that is included in the path may use a different criterion for the metric.
- One system may use, RIP which defines hop count as the metric. Another may use OSPF with minimum delay defined as the metric.
- The optimum path is the path that fits the organization.(Eg: AS4 to AS1)
- Other criteria, such as security, safety and reliability can also be applied.

RIP

- The Routing Information Protocol (RIP) is an intra-domain (interior) routing protocol used inside an autonomous system.
- It is a very simple protocol based on distance vector routing which employ the hop count as a routing metric.
- RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
- The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.
- A hop count of 16 is considered an infinite distance and the route is considered unreachable.

RIP version 1

- The original specification of RIP was published in 1988 and uses classful routing.
- The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM).
- This limitation makes it impossible to have different-sized subnets inside of the same network class.
- In other words, all subnets in a network class must have the same size.
- There is also no support for router authentication, making RIP vulnerable to various attacks.

RIPv1 Operation

- RIP defines two types of messages.

1. Request Message
2. Response Message

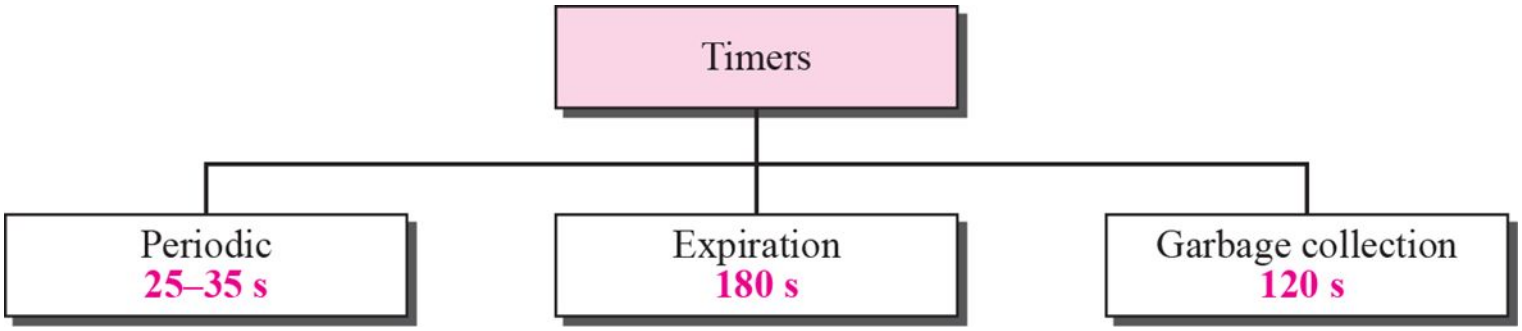
- When a RIP router comes online, it sends a broadcast Request Message on all of its RIP enabled interfaces. All the neighboring routers which receive the Request message respond back with the Response Message containing their Routing table.
- The Response Message is also unnecessarily sent when the Update timer expires. On receiving the Routing table, the router processes each entry of the routing table as per the following rules

- If there are no route entries matching the one received then the route entry is added to the routing table automatically, along with the information about the router from which it received the routing table.

- If there are matching entries but the hop count metric is lower than the one already in its routing table, then the routing table is updated with the new route.

- If there are matching entries but the hop count metric is higher than the one already in its routing table, then the routing entry is updated with hop count of 16 (infinite hop).

RIP Timer



Update Timer(Periodic)

- The update timer controls the interval between two gratuitous Response Messages.
- By default the value is 30 seconds. The response message is broadcast to all its RIP enabled interface.

Invalid Timer(Expiration)

- The invalid timer specifies how long a routing entry can be in

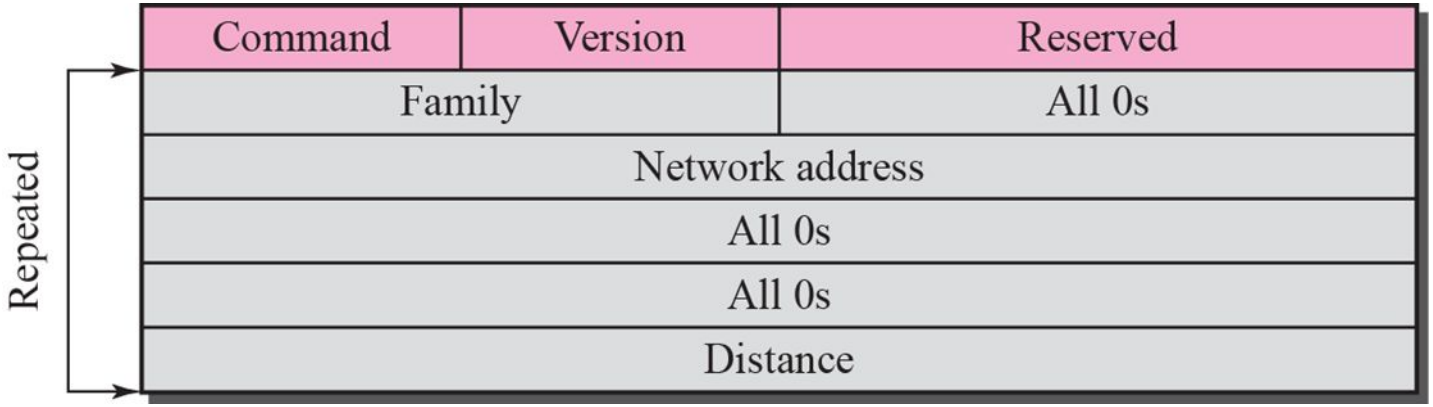
Flush Timer

- The flush timer controls the time between the route is invalidated or marked as unreachable and removal of entry from the routing table.
- By default the value is 240 seconds. This is 60 seconds longer than Invalid timer.
- So for 60 seconds the router will be advertising about this unreachable route to all its neighbors. This timer must be set to a higher value than the invalid timer.

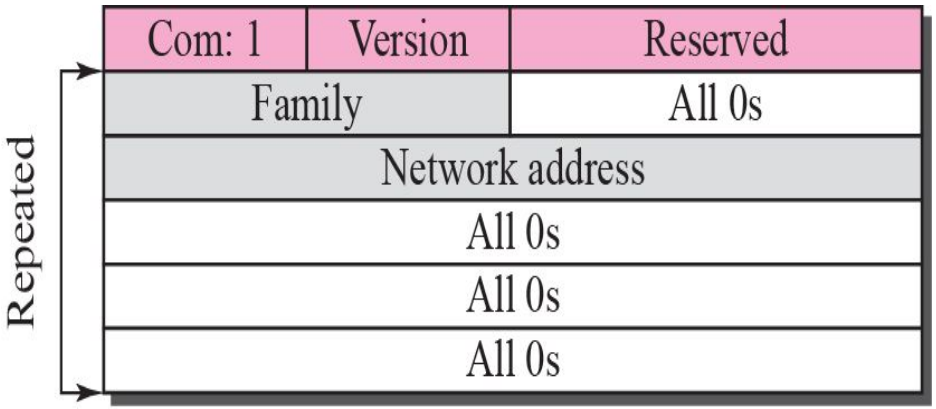
Hold-down Timer

- The hold-down timer is started per route entry, when the hop

RIP message format



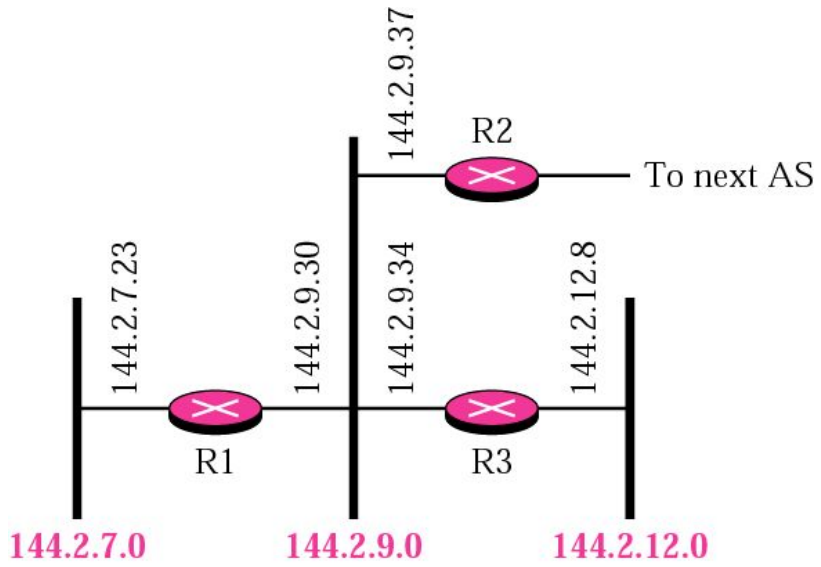
Request messages



a. Request for some

b. Request for all

RIP message example



RIP message

2	1	Reserved	
2		All 0s	
144.2.7.0			Network 144.2.7.0
All 0s			
All 0s			
--			
2		All 0s	
144.2.9.0			Network 144.2.9.0
All 0s			
All 0s			
--			
2		All 0s	
144.2.12.0			Network 144.2.12.0
All 0s			
All 0s			
1			

Limitations

- **The hop count cannot exceed 15, or routes will be dropped.**
- **Most RIP networks are flat. There is no concept of areas or boundaries in RIP networks.**
- **Variable Length Subnet Masks are not supported by RIP version 1 (which is obsolete).**
- **RIP has slow convergence and count to infinity problems.**

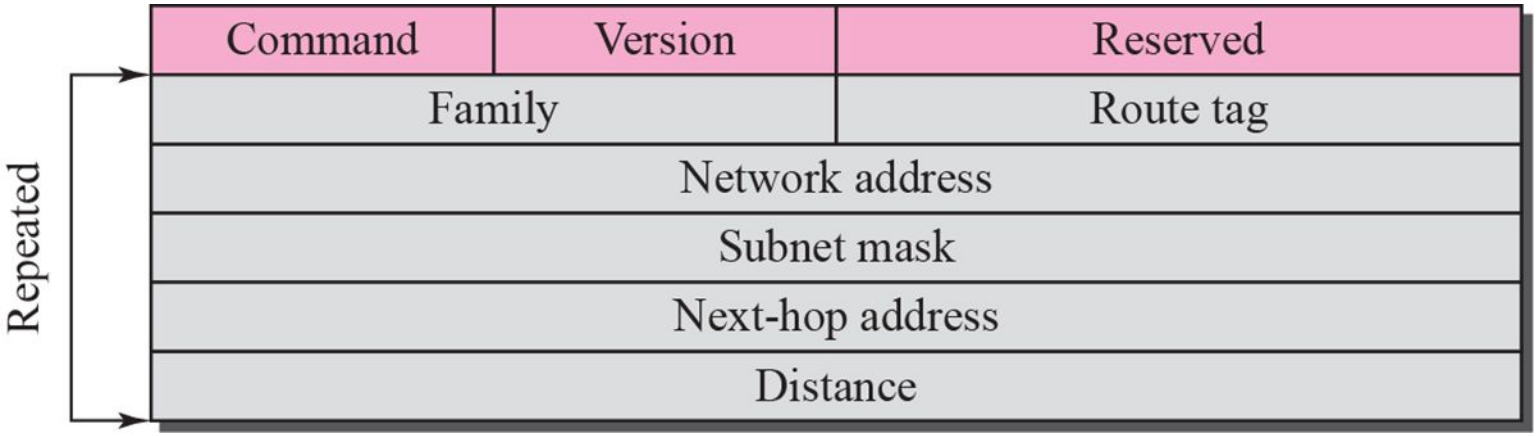
RIP Configuring and Commands

- **ip routing** : enables the router
- **router rip** : you can enter configuration commands to define the RIP process for router
- **network network_address :** Telling the router which networks it should advertise routes for
- **write, write terminal** : Saving configuration & view currently running configuration
- **ping address** : To check and see if the packets are getting routed
- **show ip route** : To view the routers current routing table
- **show ip rip ?** : Gives information about RIP

RIP version 2

- Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993 and last standardized in 1998. It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained.
- In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 *multicasts* the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.

RIP version 2 format



- **Route tags** were also added in RIP version 2. This functionality allows a distinction between routes learned from the RIP protocol and routes learned from other protocols.

Command -- The command field is used to specify the purpose of the datagram.

Version -- The RIP version number. The current version is 2.

Address family identifier -- Indicates what type of address is specified in this particular entry.

Route tag -- Attribute assigned to a route which must be preserved and readvertised with a route. The route tag provides a method of separating internal RIP routes from external RIP routes, which may have been imported from an EGP or another IGP.

IP address -- The destination IP address.

Subnet mask -- Value applied to the IP address to yield the non-host portion of the address. If zero, then no subnet mask has been included for this entry.

Next hop -- Immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded.

Metric -- Represents the total cost of getting a datagram from the host to that destination.

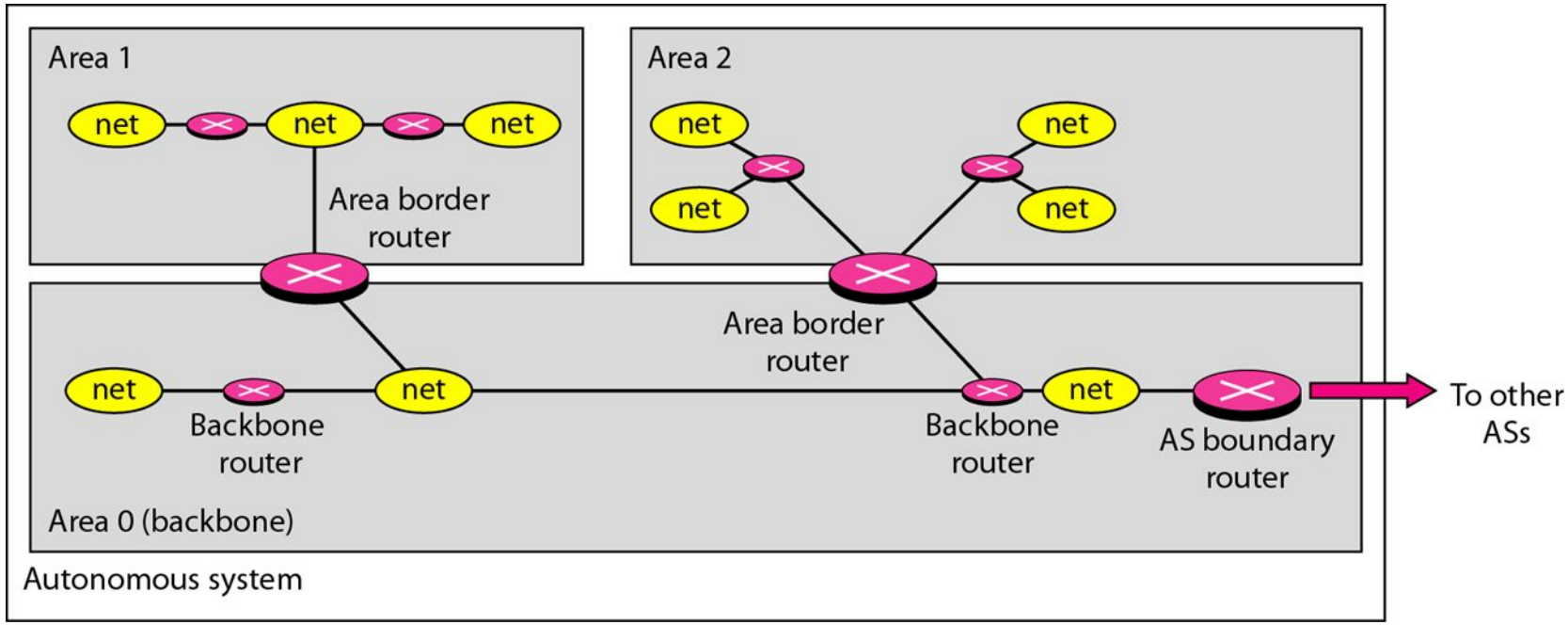
Limitations

- RIP-2 supports generic notion of authentication, but only “password” is defined so far. Still not very secure.
- RIP2 packet size increases as the number of networks increases hence it is not suitable for large networks.
- RIP2 generates more protocol traffic than OSPF, because it propagates routing information by periodically transmitting the entire routing table to neighbor routers
- RIP2 may be slow to adjust for link failures.

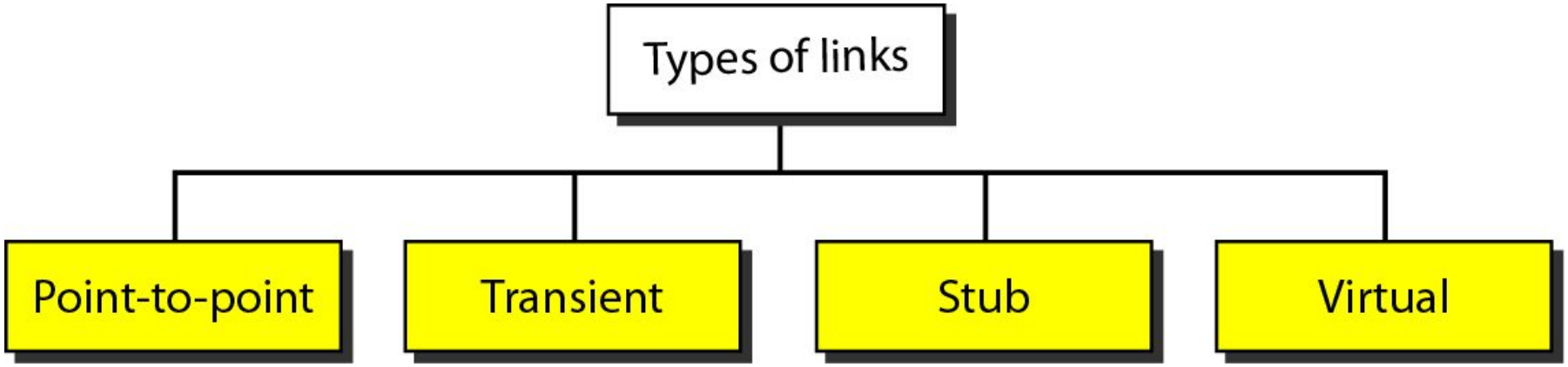
OSPF

- The Open Shortest Path First (OSPF) protocol is an intra-domain routing protocol based on link state routing

Areas in an autonomous system

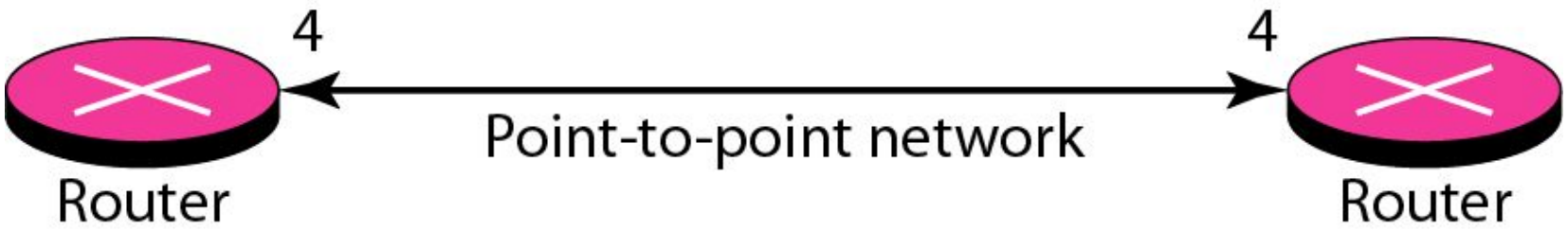


Types of links



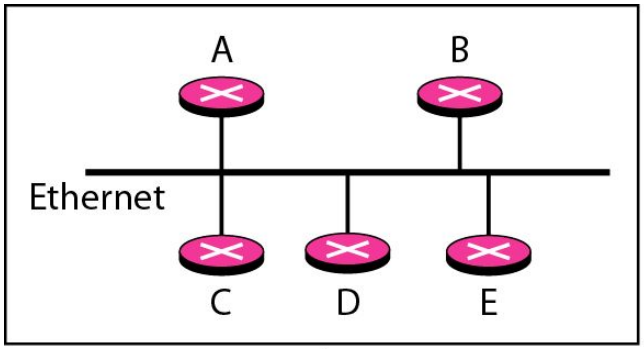
Point-to-point link

It connects two routers without any other host or router

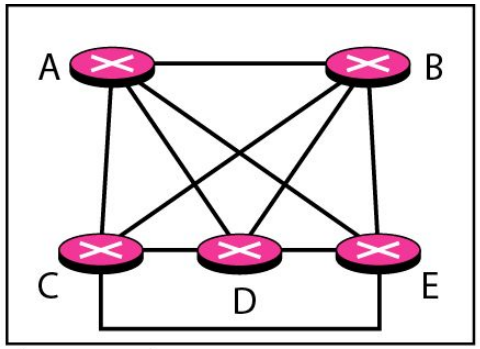


Transient link

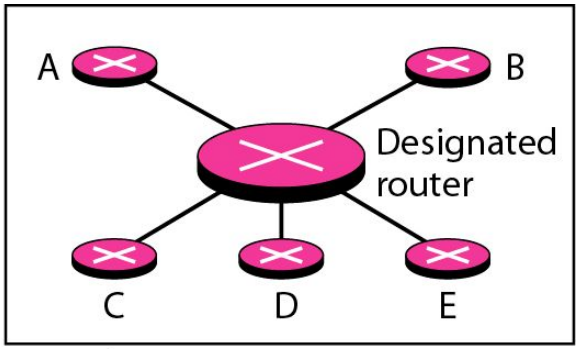
It is a network with several routers attached to it.



a. Transient network



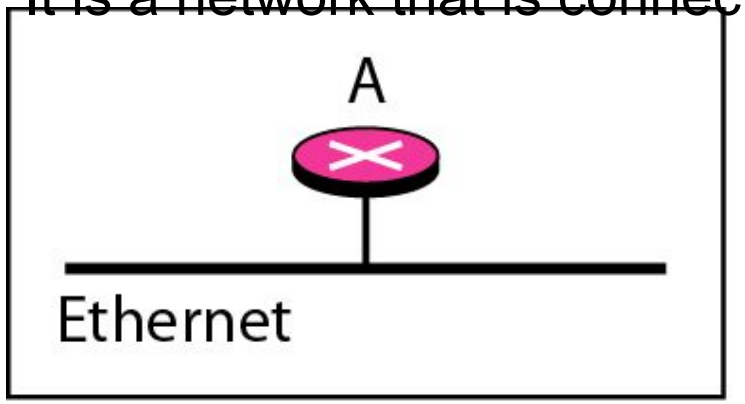
b. Unrealistic representation



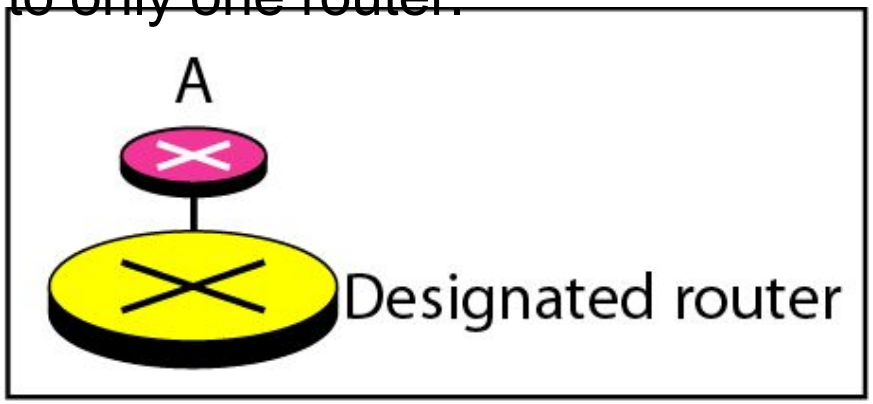
c. Realistic representation

Stub link

It is a network that is connected to only one router.



a. Stub network



b. Representation

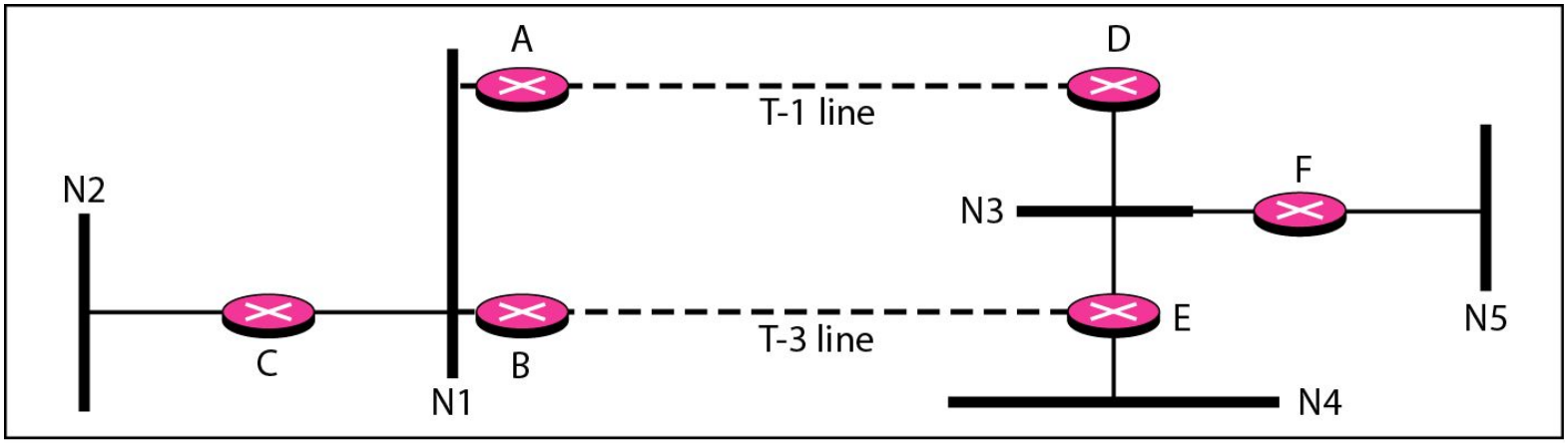
Virtual link

- When the link between two routers is broken, the administration may create a virtual link between them.

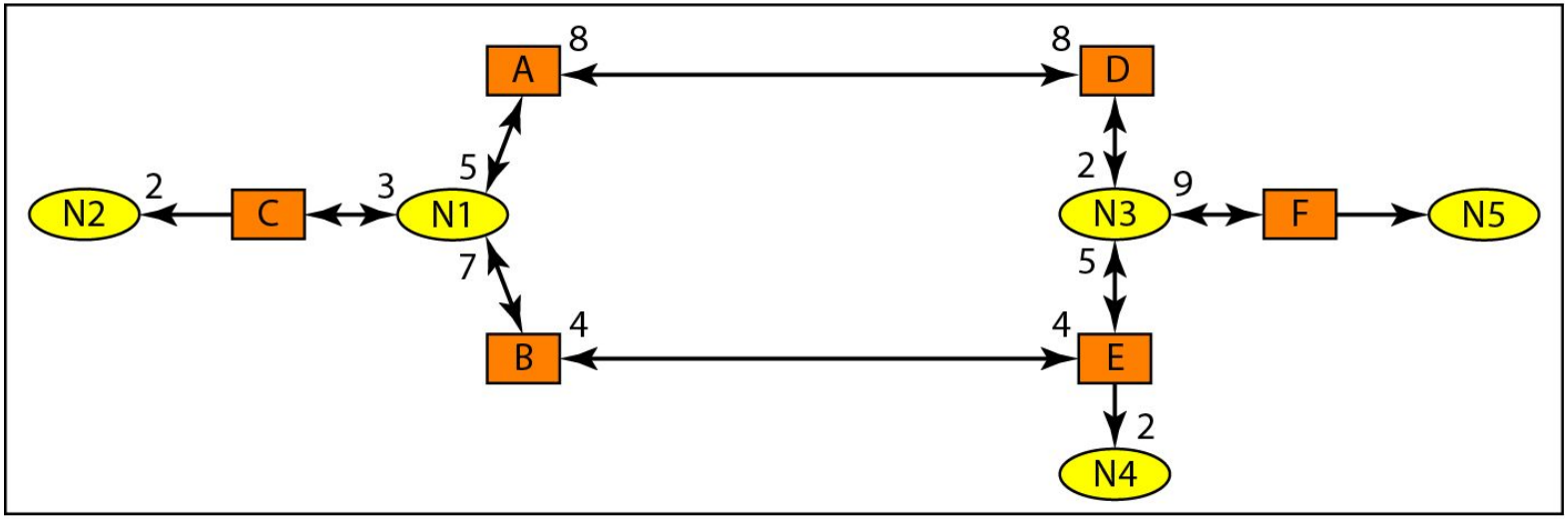
Table 11.5 *Link Types, Link Identification, and Link Data*

Link Type	*Link Identification*	*Link Data*
Type 1: Point-to-point	Address of neighbor router	Interface number
Type 2: Transient	Address of designated router	Router address
Type 3: Stub	Network address	Network mask
Type 4: Virtual	Address of neighbor router	Router address

Example of an AS and its graphical representation in OSPF

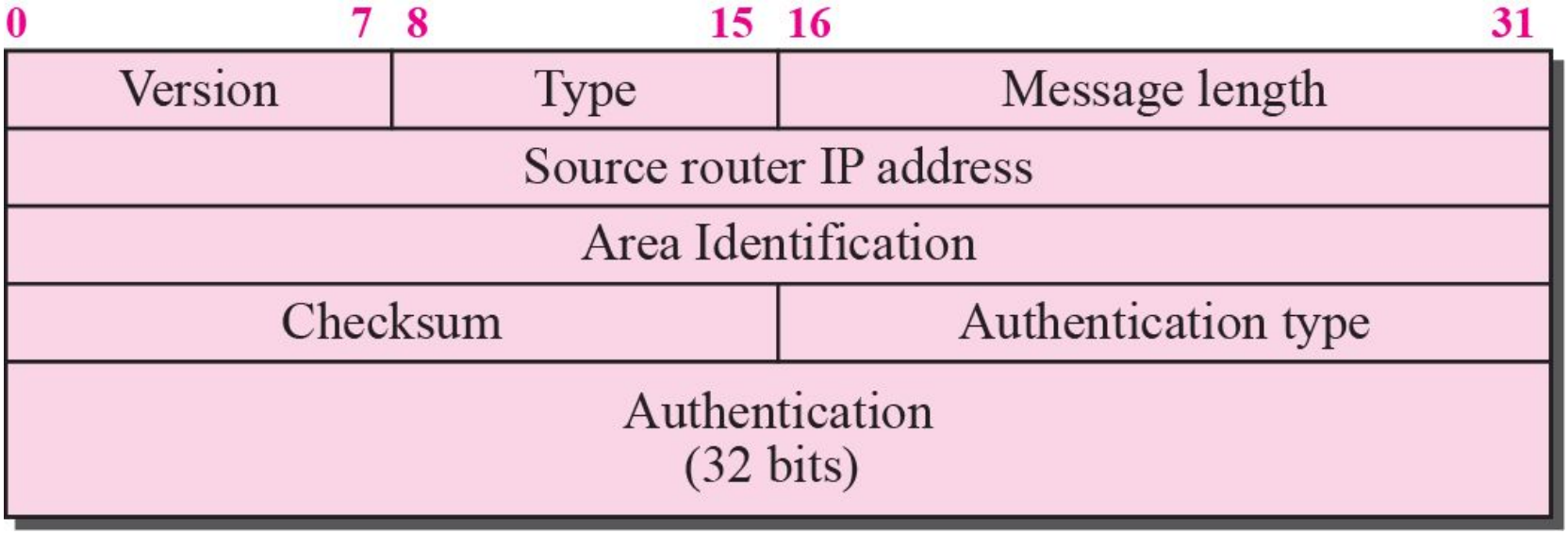


a. Autonomous system

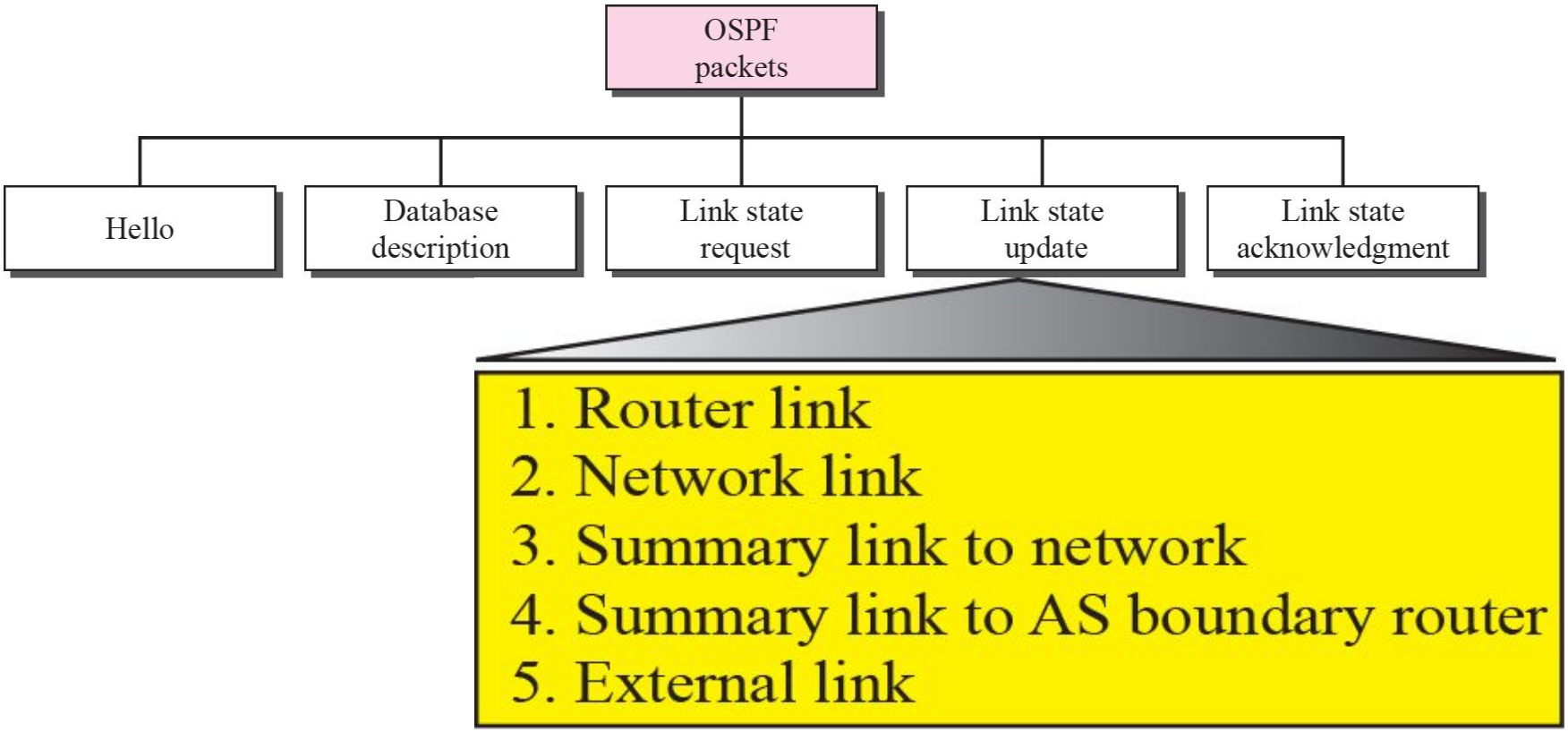


b. Graphical representation

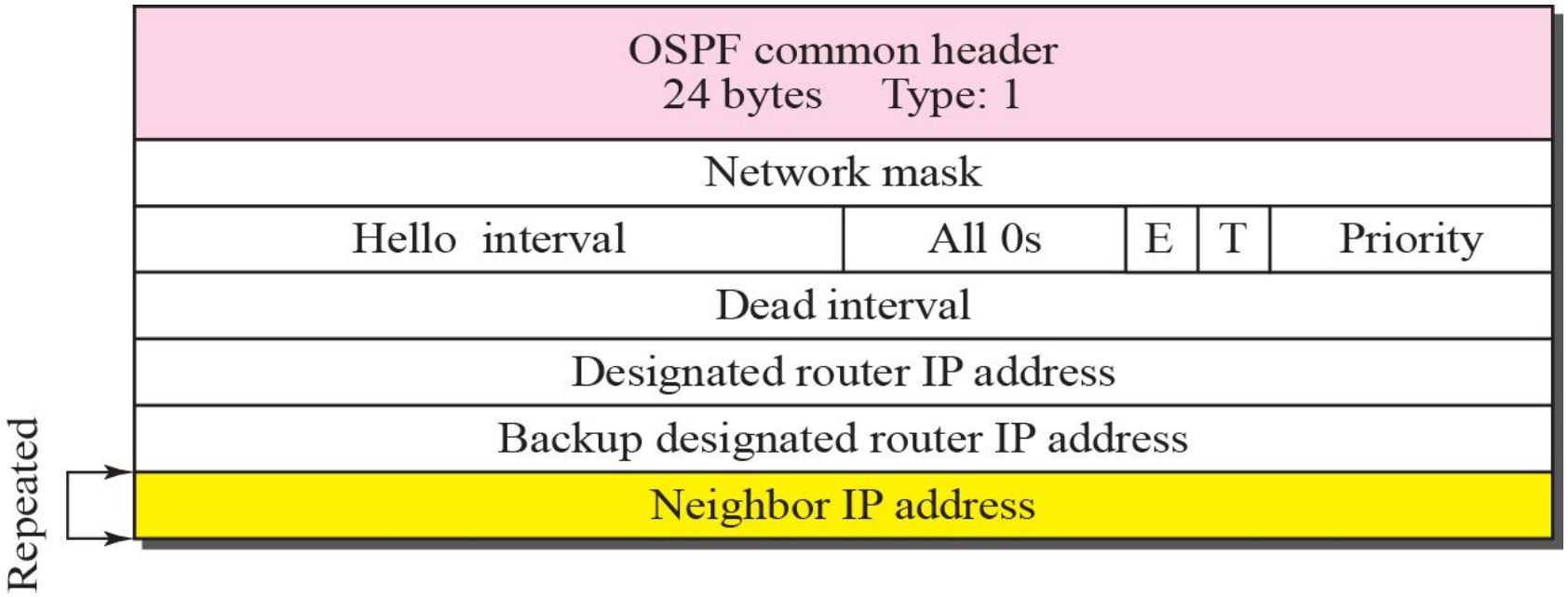
OSPF common header



Types of OSPF packet



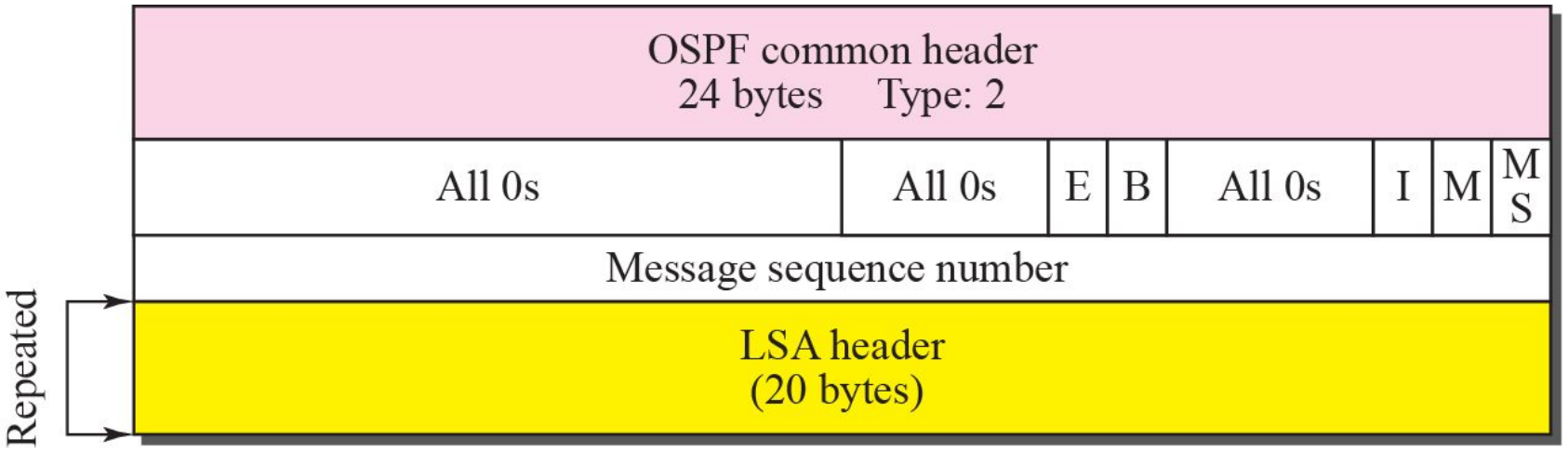
Hello packet



OSPF uses the hello message to create neighborhood relationship and to test the reachability of neighbors.

This is the first step in link state routing. Before a router can flood all of the other routers with information about its neighbors, it must first greet it neighbors.

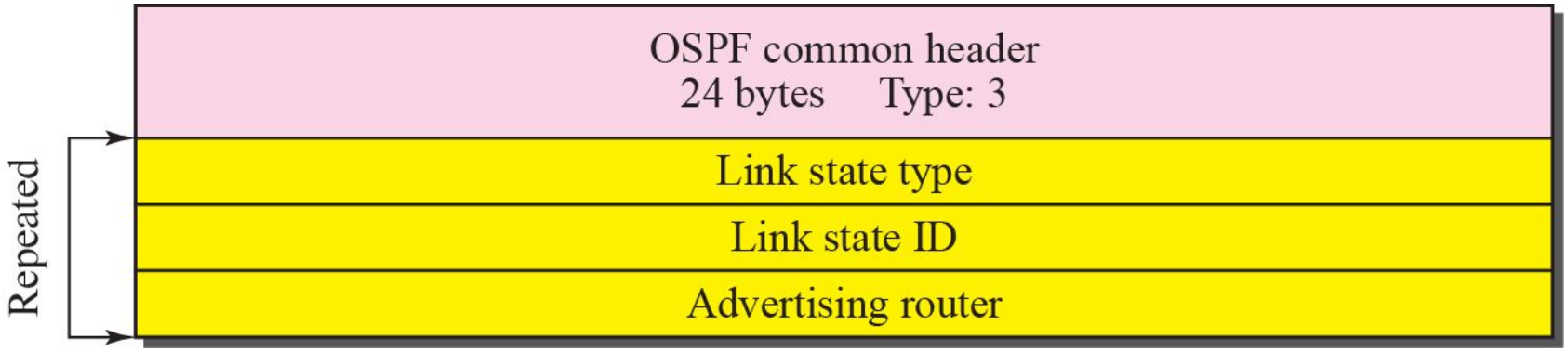
Database description packet



When a router is connected to the system for the first time or after a failure, it needs the complete link state database immediately. Therefore, it sends hello packets to greet its neighbors. If this is the first time that the neighbors hear from the router, they send a database description message.

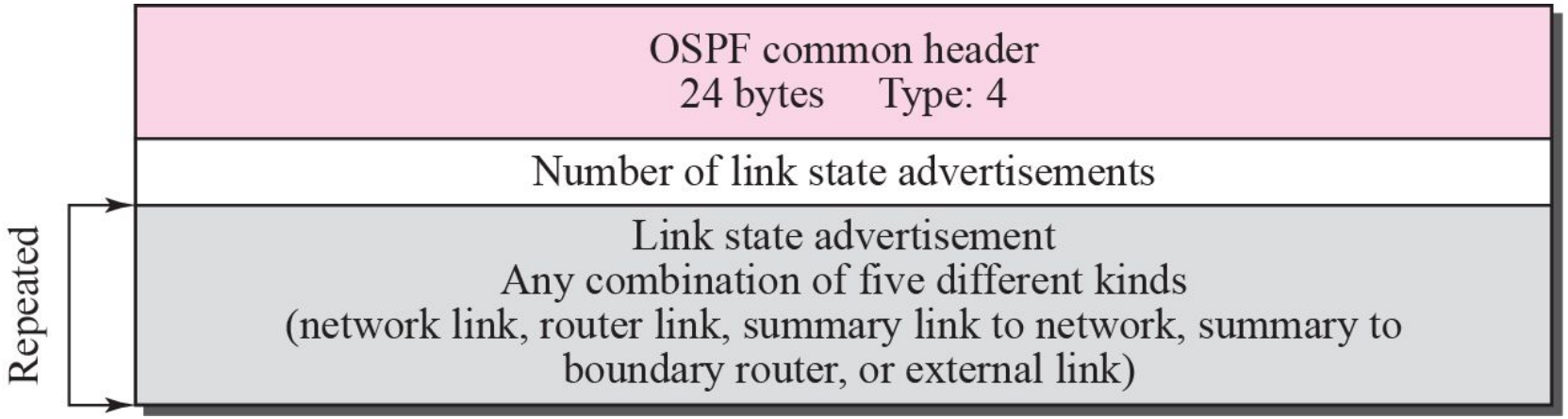
The database description packet does not contain complete database information; it only gives an outline, the title of each lines in the database.

Link state request packet

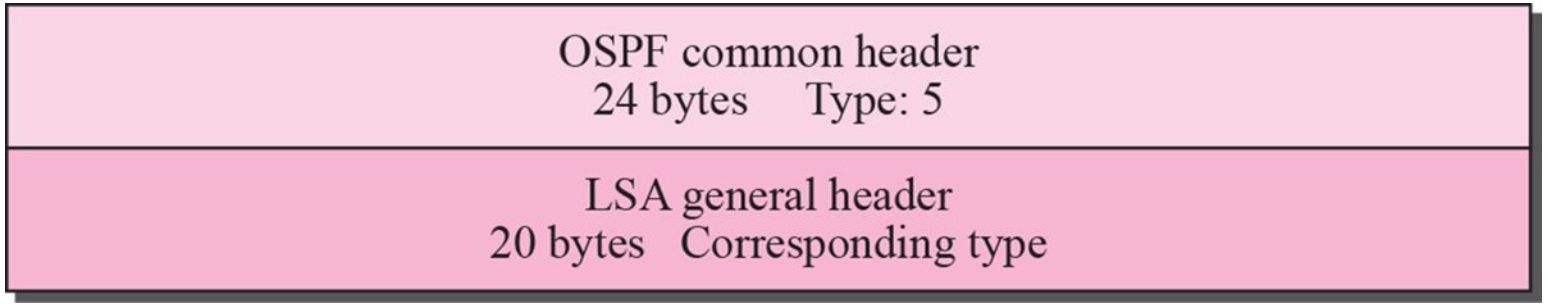


Link state type	Link state ID
Router link	IP address of the router
Network link	IP address of the designated router
Summary link to network	Address of the network
Summary link to AS boundary	IP address of the boundary router
External link	Address of the network

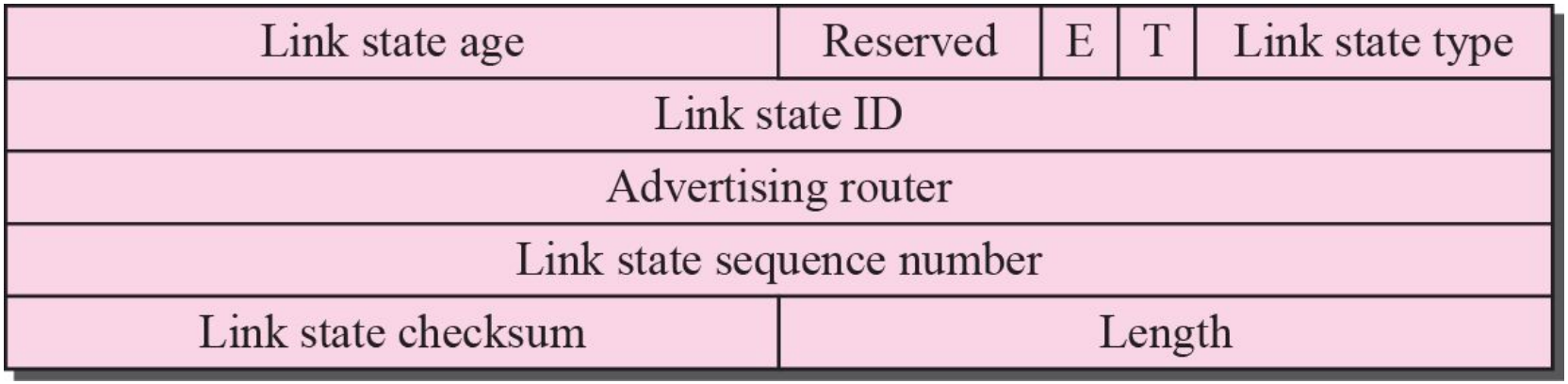
Link state update packet



Link state acknowledgment packet



LSA general header



LSA General Header

- Link state age
  - When a router creates the message, the value of this field is 0
  - When each successive router forwards this message, it estimates the transit time and adds it to the cumulative value of this field
- E flag
  - If this flag is set to 1, it means the area is a stub area (an area that is connected to the backbone area by only one path
- T flag
  - If this flag is set to 1, it means the router can handle multiple types of services
- Advertising router
  - The IP address of the router advertising this message
- Link state sequence number
  - A sequence number assigned to each link state update message

EIGRP

- “Enhanced” Interior Gateway Routing Protocol
- Cisco proprietary, released in 1994
- Developed from the older IGRP (classful)
- EIGRP is classless, supports VLSM, CIDR
- EIGRP is an *advanced distance-vector* routing protocol that relies on features commonly associated with link-state protocols. (sometimes called a *hybrid routing protocol*).

- **RIP, IGRP, EIGRP**
- RIP is a typical distance vector routing protocol enhancements for better performance using hop count as metric, max 15.
- IGRP was introduced to have a better metric and not be restricted to 15 hops. It is a typical distance vector routing protocol, and classful.
- EIGRP was introduced to be classless and with.

IGRP

- Bellman-Ford algorithm
- Ages out routing entries
- Sends periodic updates
- Keeps best routes only
- Slow convergence with holddown timers

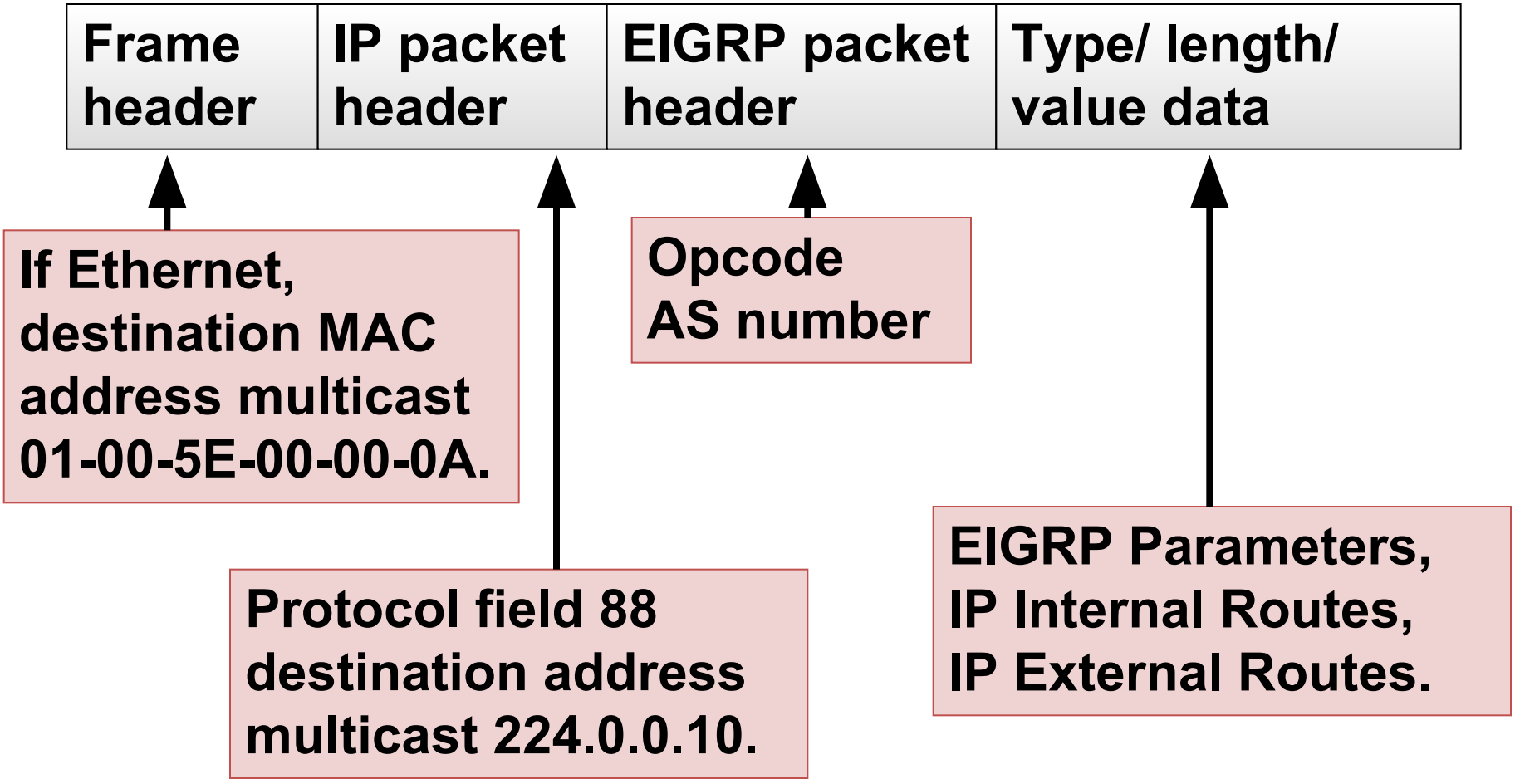
EIGRP

- Diffusing Update Algorithm (DUAL)
- Does not age out entries
- No periodic updates
- Keeps backup routes
- Faster convergence, no holddown timers

IGRP and EIGRP: A migration path

IGRP	EIGRP
Classful Routing Protocol	Classless Routing Protocol • VLSM, CIDR
bandwidth = (10,000,000/*bandwidth kbps*) delay = *delay*/10 24 bit metric for bandwidth and delay	bandwidth = (10,000,000/*bandwidth kbps*) * 256 delay = (*delay*/10) * 256 32 bit metric for bandwidth and delay
Maximum Hop Count = 255	Maximum Hop Count = 224
No differentiation between internal and external routes.	Outside routes (redistributed) are tagged as external routes.
Automatic redistribution between IGRP and EIGRP as long as “AS” numbers are the same.	

Encapsulation



EIGRP packet header

EIGRP packet header

- Opcode specifies packet type:
  Update, Query, Reply, Hello
- Autonomous system (AS) number specifies the EIGRP process. Several can run at the same time.
- Other fields allow for reliability if needed.

Metric Calculation (Review)

Both EIGRP and IGRP use the following metric calculation:

metric = [K1 * bandwidth + (K2 * bandwidth)/(256 - load)+(K3 * delay)]* [K5/(reliability + K4)]

The following are the default constant values:

K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0

When K4 and K5 are 0, the [K5/reliability + K4)] portion of the equation is not factored in to the metric. Therefore, with the default constant values, the metric equation is as follows:

metric = bandwidth + delay

IGRP and EIGRP, which scales the value of 256, use the following equations to determined the values used in the metric calculation:

bandwidth for IGRP = (10000000/bandwidth)
bandwidth for EIGRP = (10000000/bandwidth)*256
delay for IGRP = delay/10
delay for EIGRP = delay/10*256

EIGRP

bandwidth is in kbps

- k1 for bandwidth
- k2 for load
- k3 for delay
- k4 and k5 for Reliability

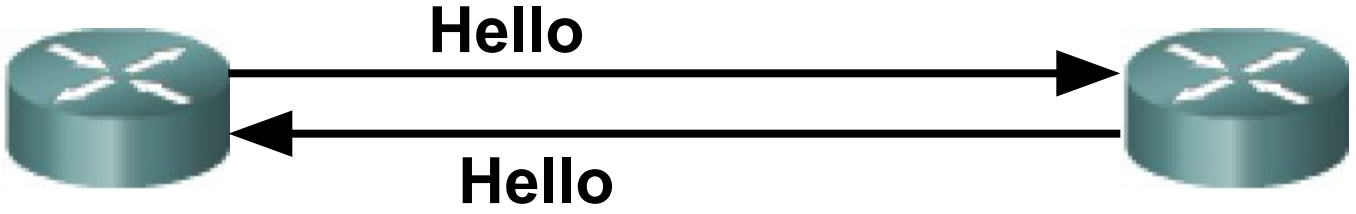
```
Router(config-router)# metric
   weights tos k1 k2 k3 k4 k5
```

Features of EIGRP

- **Classless** Routing Protocol (VLSM, CIDR)
- **Faster convergence** times and improved scalability
- **Rapid Convergence and Better handling of routing loops – (DUAL)** (coming)
- **Efficient Use of Bandwidth**
  - **Partial, bounded updates**: Incremental updates only to the routers that need them.
  - **Minimal bandwidth consumption**: Uses Hello packets and EIGRP packets by default use no more that 50% of link's bandwidth EIGRP packets.
- **PDM (Protocol Dependent Module)**
  - Keeps EIGRP is modular
  - Different PDMs can be added to EIGRP as new routed protocols are enhanced or developed: IPv4, IPv6, IPX, and AppleTalk

Hello packets

- Used by EIGRP to discover neighbours
- Used to form adjacencies with neighbours.
- Multicasts
- Unreliable delivery



Update packets

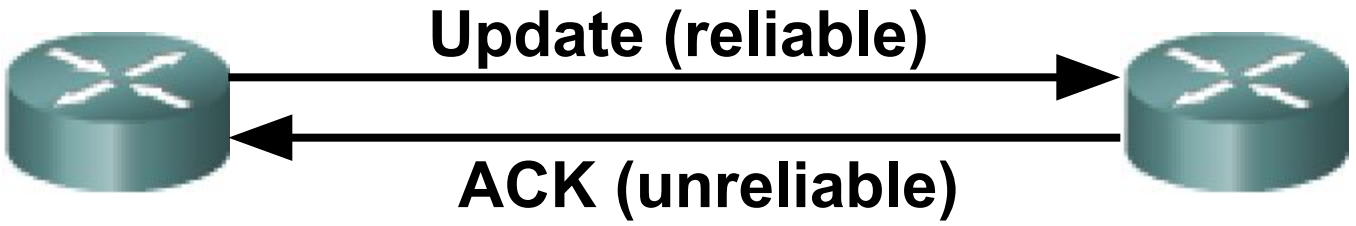
- Used to propagate routing information.
- No periodic updates.
- Sent only when necessary.
- Include only required information
- Sent only to those routers that require it.
- Reliable delivery.
- Multicast if to several routers, unicast if to one router.

Update packets

- EIGRP updates are sent only when a route changes.
- EIGRP updates are **partial**. They include only information about the changed route.
- EIGRP updates are **bounded**. They go only to routers that are affected by the change.
- This keeps updates small and saves bandwidth.

Acknowledgement (ACK) packets

- Sent when reliable delivery is used by RTP.
- Sent in response to update packets.
- Unreliable delivery
- Unicast

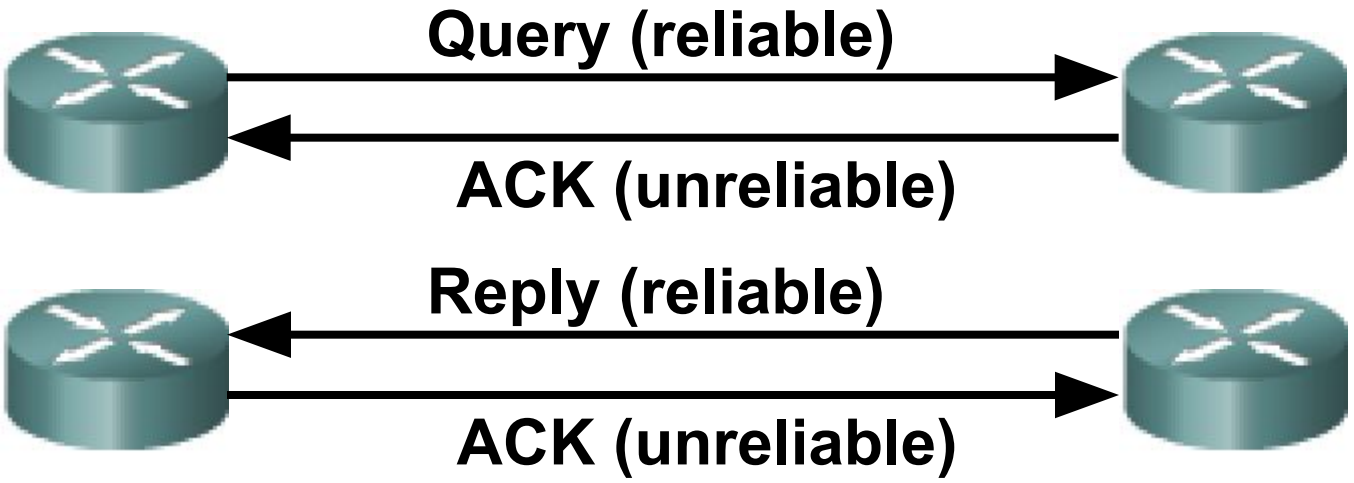


Query packet

- Used when searching for a network
- E.g. a route goes down. Is there another route?
- Uses reliable delivery so requires ACK
- Multicast or unicast
- All neighbours must reply

Reply packet

- Sent in response to a query from a neighbour.
- Sent reliably so requires ACK.
- Unicast



Summary of message types

	Unicast	Multicast	Either
Reliable	Reply		Update Query
Unreliable	ACK	Hello	

EIGRP Terminology

- **Neighbor table** – Each EIGRP router maintains a neighbor table that lists adjacent routers. This table is comparable to the adjacency database used by OSPF. There is a neighbor table for each protocol that EIGRP supports.

- **Topology table** – Every EIGRP router maintains a topology table for each configured network protocol. This table includes route entries for all destinations that the router has learned. All learned routes to a destination are maintained in the topology table.

- **Routing table** – EIGRP chooses the best routes to a destination from the topology table and places these routes in the routing table. Each EIGRP router maintains a routing table for each network protocol.

- **Successor** – A successor is a route selected as the primary route to use to reach a destination. Successors are the entries kept in the routing table. Multiple successors for a destination can be retained in the routing table.

- **Feasible successor** – A feasible successor is a backup route. These routes are selected at the same time the successors are identified, but are kept in the topology table. Multiple feasible successors for a destination can be retained in the topology table.

Neighbor Table

- Whenever a new neighbor is discovered, the address of that neighbor and the interface used to reach it are recorded in a new neighbor table entry.

```
RouterC#show ip eigrp neighbors
IP-EIGRP neighbors for process 44
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   192.168.0.1     Se0           11 00:03:09 1138  5000  0  6
1   192.168.1.2     Et0           12 00:34:46    4   200  0  4
```

Neighbor Table

```
RouterC#show ip eigrp neighbors
IP-EIGRP neighbors for process 44
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   192.168.0.1     Se0           11 00:03:09 1138   5000  0  6
1   192.168.1.2     Et0           12 00:34:46    4    200  0  4
```

- *Neighbor address* The network-layer address of the neighbor router(s).
- *Queue count* The number of packets waiting in queue to be sent. If this value is constantly higher than zero, then there may be a congestion problem at the router. A zero means that there are no EIGRP packets in the queue.

Neighbor Table

```
RouterC#show ip eigrp neighbors
IP-EIGRP neighbors for process 44
H   Address         Interface   Hold Uptime   SRTT   RTO  Q  Seq
                                (sec)         (ms)       Cnt Num
0   192.168.0.1     Se0           11 00:03:09 1138   5000  0  6
1   192.168.1.2     Et0           12 00:34:46    4    200  0  4
```

- *Smooth Round Trip Timer (SRTT)* The average time it takes to send and receive packets from a neighbor.
  - This timer is used to determine the retransmit interval (RTO)

- *Hold Time* The interval to wait without receiving anything from a neighbor before considering the link unavailable.
  - Originally, the expected packet was a hello packet, but in current Cisco IOS software releases, any EIGRP packets received after the first hello will reset the timer.

Topology Table

- EIGRP uses its **topology table** to store all the information it needs to calculate a set of distances and vectors to all reachable destinations.

```
RouterB#show ip eigrp topology
IP-EIGRP Topology Table for process 44
Codes: P - Passive, A - Active, U - Update, Q - Query, R -
   Reply, r - Reply status
P 206.202.17.0/24, 1 successors, FD is 2195456
         via 206.202.16.1 (2195456/2169856), Ethernet0
P 206.202.18.0/24, 2 successors, FD is 2198016
         via 192.168.0.2 (2198016/284160), Serial0
         via 206.202.16.1 (2198016/2172416), Ethernet0
```

Topology Table

```
RTX#sh ip eigrp top 204.100.50.0
IP-EIGRP topology entry for 204.100.50.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD
   is 2297856
  Routing Descriptor Blocks:
  10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 192.168.1.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

FD/RD

IP Routing Table

- EIGRP chooses the best routes (that is, successor) to a destination from the topology table and places these routes in the routing table.
- Each EIGRP router maintains a topology table for each network protocol.
- EIGRP displays both internal EIGRP routes and external EIGRP routes.

```
RouterB#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
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
   default U - per-user static route
Gateway of last resort is not set
C    10.1.1.0 is directly connected, Serial0
D    172.16.0.0 [90/2681856] via 10.1.1.0, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1, 00:00:04, Serial0
```

IP Routing Table

- The routing table contains the routes installed by DUAL as the best loop-free paths to a given destination.
- EIGRP will maintain **up to four routes** per destination.
- These routes can be of **equal, or unequal cost** (if using the **variance** command). (later)

```
RouterB#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
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
   default U - per-user static route
Gateway of last resort is not set
C    10.1.1.0 is directly connected, Serial0
D    172.16.0.0 [90/2681856] via 10.1.1.0, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1, 00:00:04, Serial0
```

EIGRP Technologies

Four key technologies set EIGRP apart from IGRP

- Neighbor discovery and recovery
- Reliable Transport Protocol
- DUAL finite-state machine
- Protocol-specific modules

Hello Intervals and Default Hold Times

Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mbps or less	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mbps	T1, Ethernet	5 seconds	15 seconds

- ***Hello Time*** The interval of Hello Packets
- ***Hold Time*** The interval to wait without receiving anything from a neighbor before considering the link unavailable.

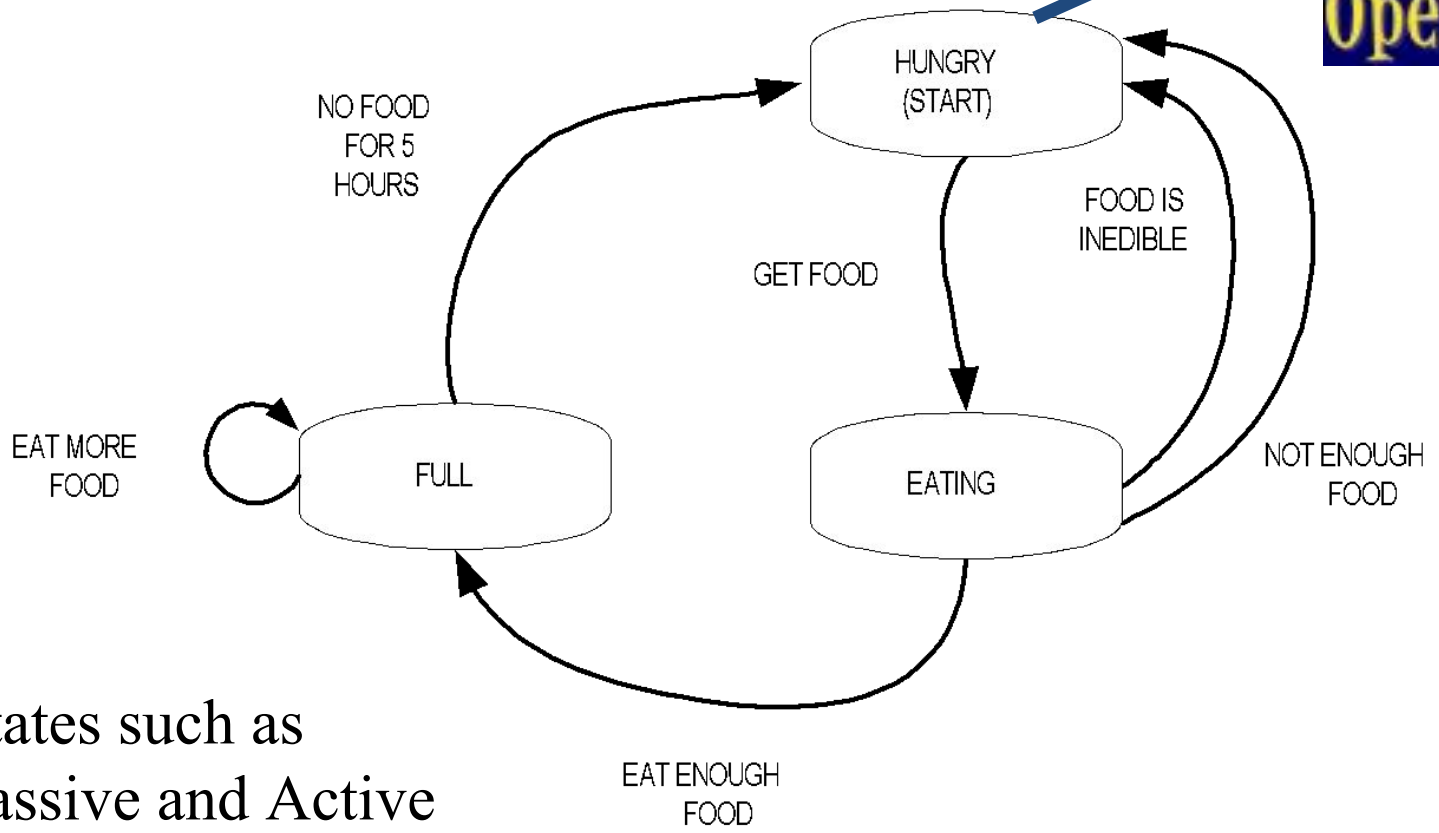
DUAL FSM

- The centerpiece of EIGRP is DUAL, the EIGRP route-calculation engine.
  - The full name of this technology is DUAL **finite state machine (FSM)**.
  - This engine contains all the logic used to calculate and compare routes in an EIGRP network.

What is FSM?

- An FSM is an abstract machine, not a mechanical device with moving parts.
- FSMs define a set of possible states something can go through, what events causes those states, and what events result from those states.
- Designers use FSMs to describe how a device, computer program, or routing algorithm will react to a set of input events.

FSM Example



States such as Passive and Active trigger Certain Events

DUAL FSM

- DUAL selects alternate routes quickly by using the information in the EIGRP tables.
- If a link goes down, DUAL looks for a feasible successor in its neighbor and topology tables.
- A **successor** is a neighboring router that is currently being used for packet forwarding, provides the least-cost route to the destination, and is not part of a routing loop.
- **Feasible successors** provide the next lowest-cost path without introducing routing loops.
  - Feasible successor routes can be used in case the existing route fails; packets to the destination network are immediately forwarded to the feasible successor, which at that point, is promoted to the status of successor.
- Selects a best loop-free path to a destination, the next hop being known as the **successor**.
- All other routers to the same destination, that also meet the **feasible condition**, meaning they are also loop-free (later), become **feasible successors**, or back-up routes.
- **debug eigrp fsm**

What if the successor fails?

Feasible Successor exists:

- If current successor route fails, feasible successor becomes the current successor, i.e. the current route.
- Routing of packets continue with little delay.

No Feasible Successor exists:

- This may be because the Reported Distance is greater than the Feasible Distance.
- Before this route can be installed, it must be placed in the ***active state*** and recomputed.
- Routing of packets continue but with more of a delay.

BGP

Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.

Types of AS:

1. Stub AS
   - A stub AS has only one connection to another AS.
   - The interdomain data traffic in a stub AS can be either created or terminated in the AS.
   - The host in the AS can send/Receive data traffic/coming form other ASs.
   - Data traffic cannot pass through a stub AS. A stub AS is either a source or a sink.

2. Multihomed AS

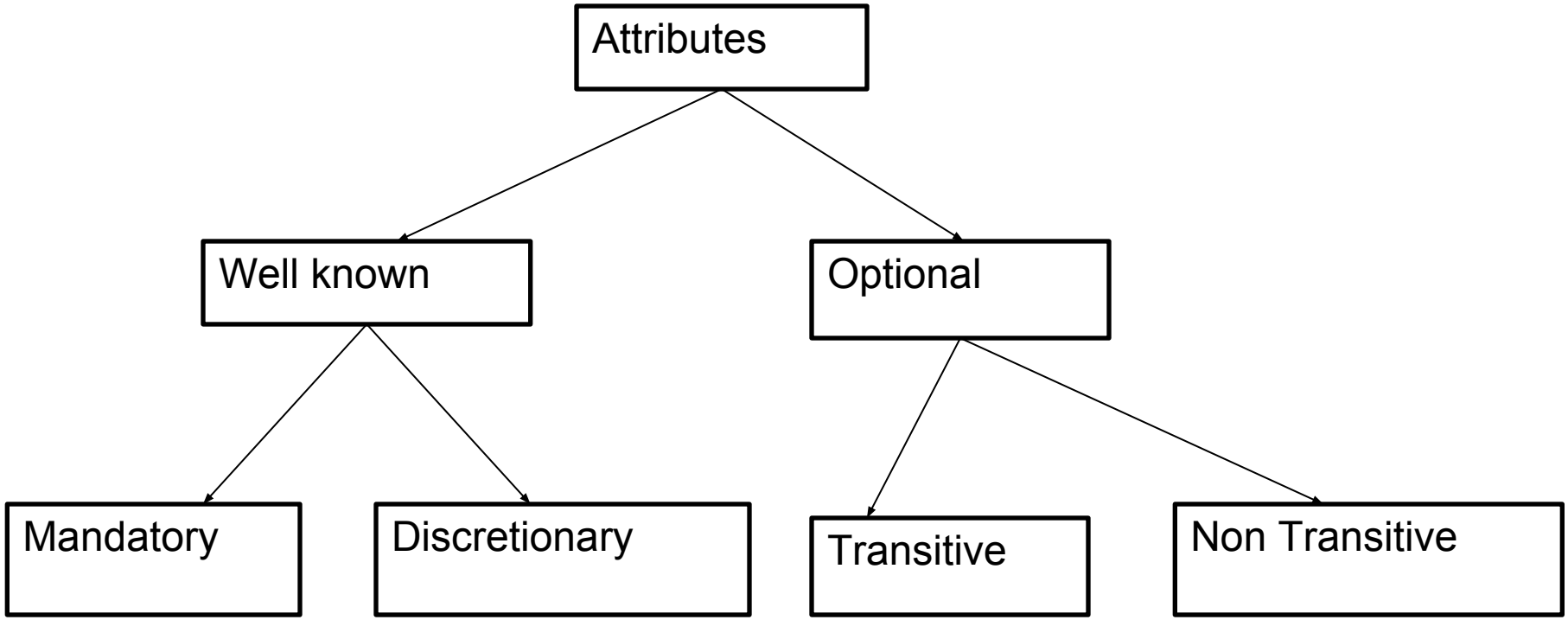
- It has more than one connection to other ASs, but it is still only a source or a sink.
- It can send/receive data traffic from/to more than one AS.
- It does not allow data coming from one AS and going to another AS to pass through.

3. Transit AS

- It allows transient traffic.

Path attributes

- The path was presented as a list of attributes. Each attribute give some information about the path.
- The list of attributes helps the receiving router make a more informed decision when applying its policy.


Attributes
Well known
Optional
Mandatory
Discretionary
Transitive
Non Transitive

- **Well Known-** one that every BGP router must recognize.
- **Optional-** one that needs not be recognized by every router.
- **Well known mandatory-** one that must appear in the description of a route.
- **Well known Discretionary-** one that must be recognized by each router.
- **Optional Transitive –** one that must be passed to the next router by the router that has not implemented this attribute
- **Optional Non Transitive –** one that must be discarded if the receiving router has not implemented.

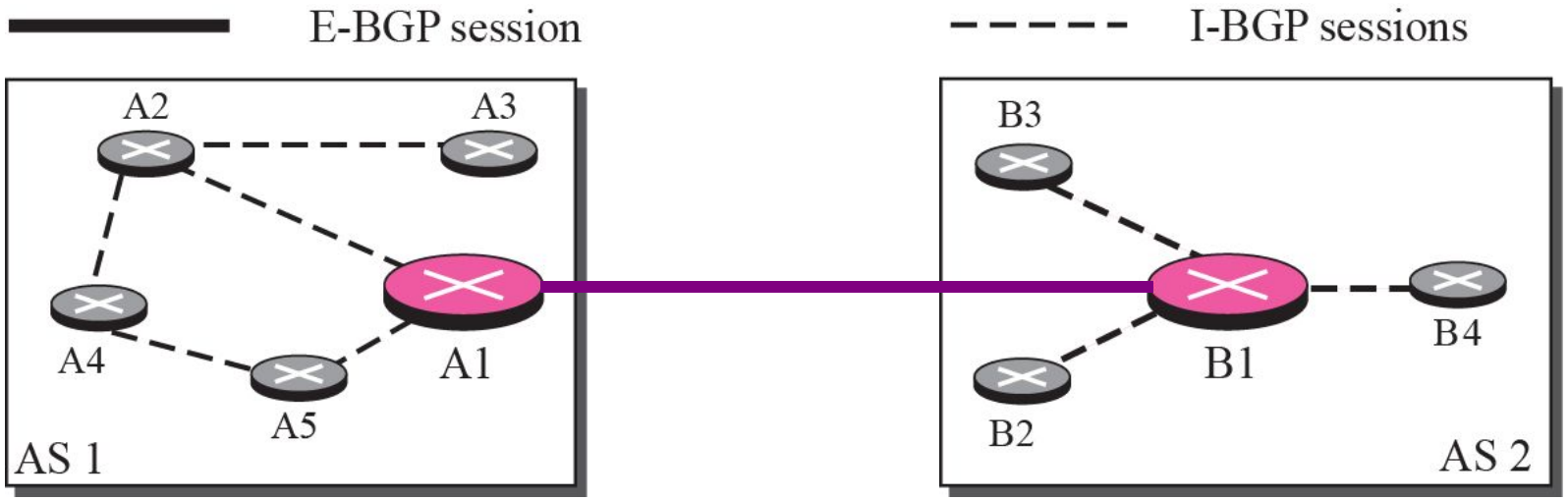
BGP Sessions

- 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.
- When a TCP connection is created for BGP, it can last for a long time, until something unusual happens.
- For this reason, BGP sessions are sometimes referred to as semi permanent connections.

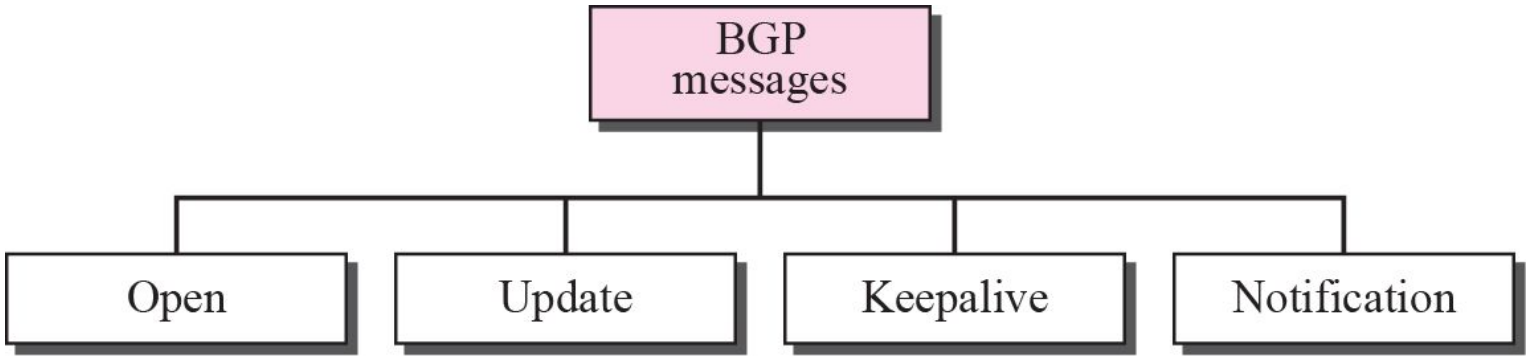
External and Internal BGP

- If we want to be precise, 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 IBGP session is used to exchange routing information between two routers inside an autonomous system.
- The session established between AS1 and AS2 is an E-BGP session. The two speaker routers exchange information they know about networks in the Internet.
- However, these two routers need to collect information from other routers in the autonomous systems. This is done using I-BGP sessions.

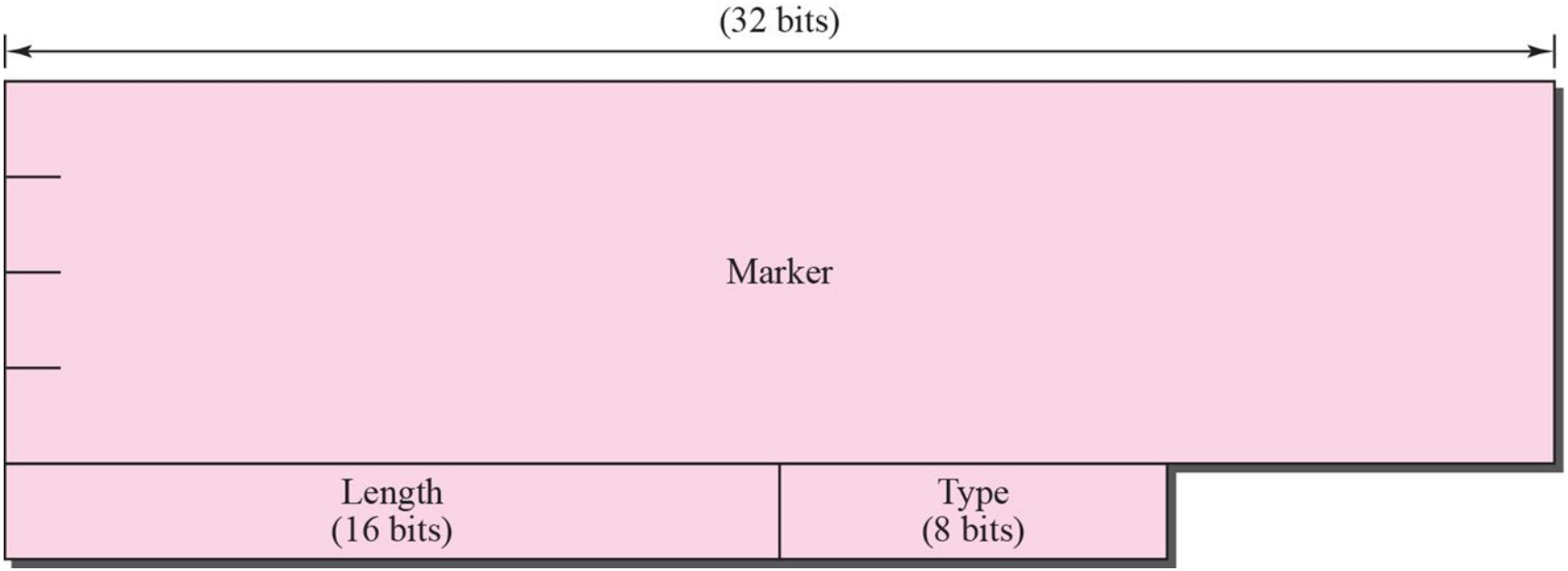
Internal and external BGP sessions



Types of BGP messages



BGP packet header



Packet Format

- All BGP packets share the same common header.
- The fields of this header are as follows:

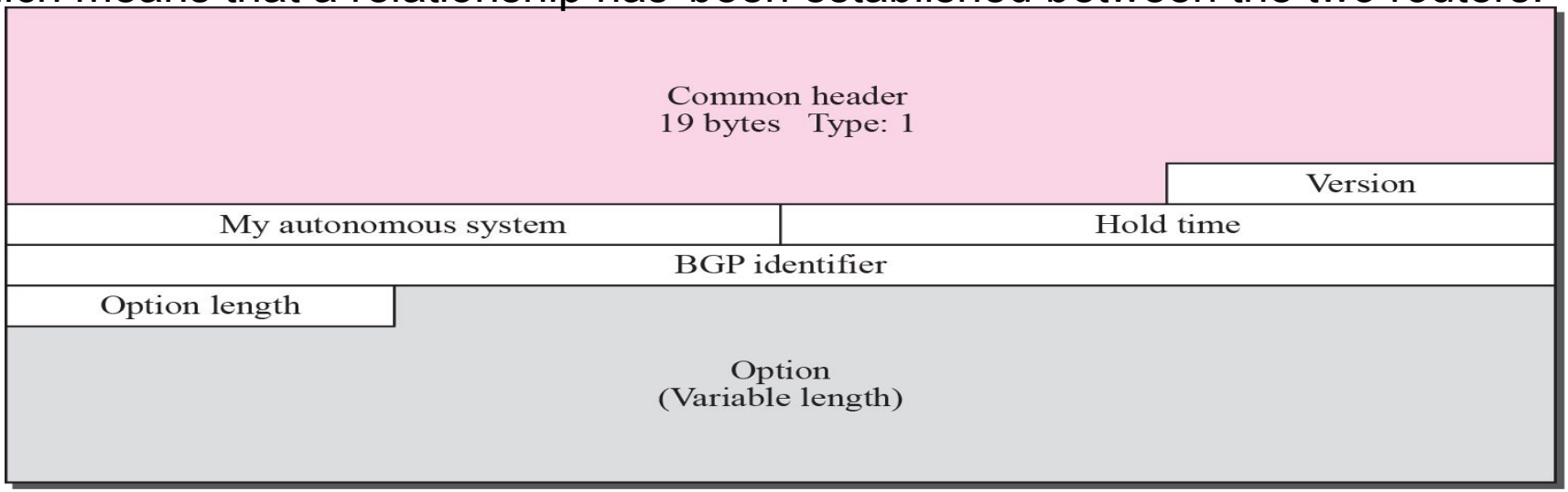
❑ **Marker.** The 16-byte marker field is reserved for authentication.

❑ **Length**. This 2-byte field defines the length of the total message including the header.

❑ **Type.** This 1-byte field defines the type of the packet.

Open message

To create a neighborhood relationship, a router running BGP opens a TCP connection with a neighbor and sends an open message. If the neighbor accepts the neighborhood relationship, it responds with a keepalive message, which means that a relationship has been established between the two routers.



- **Hold time.** This 2-byte field defines the maximum number of seconds that can elapse until one of the parties receives a keepalive or update message from the other. If a router does not receive one of these messages during the hold time period, it considers the other party dead.

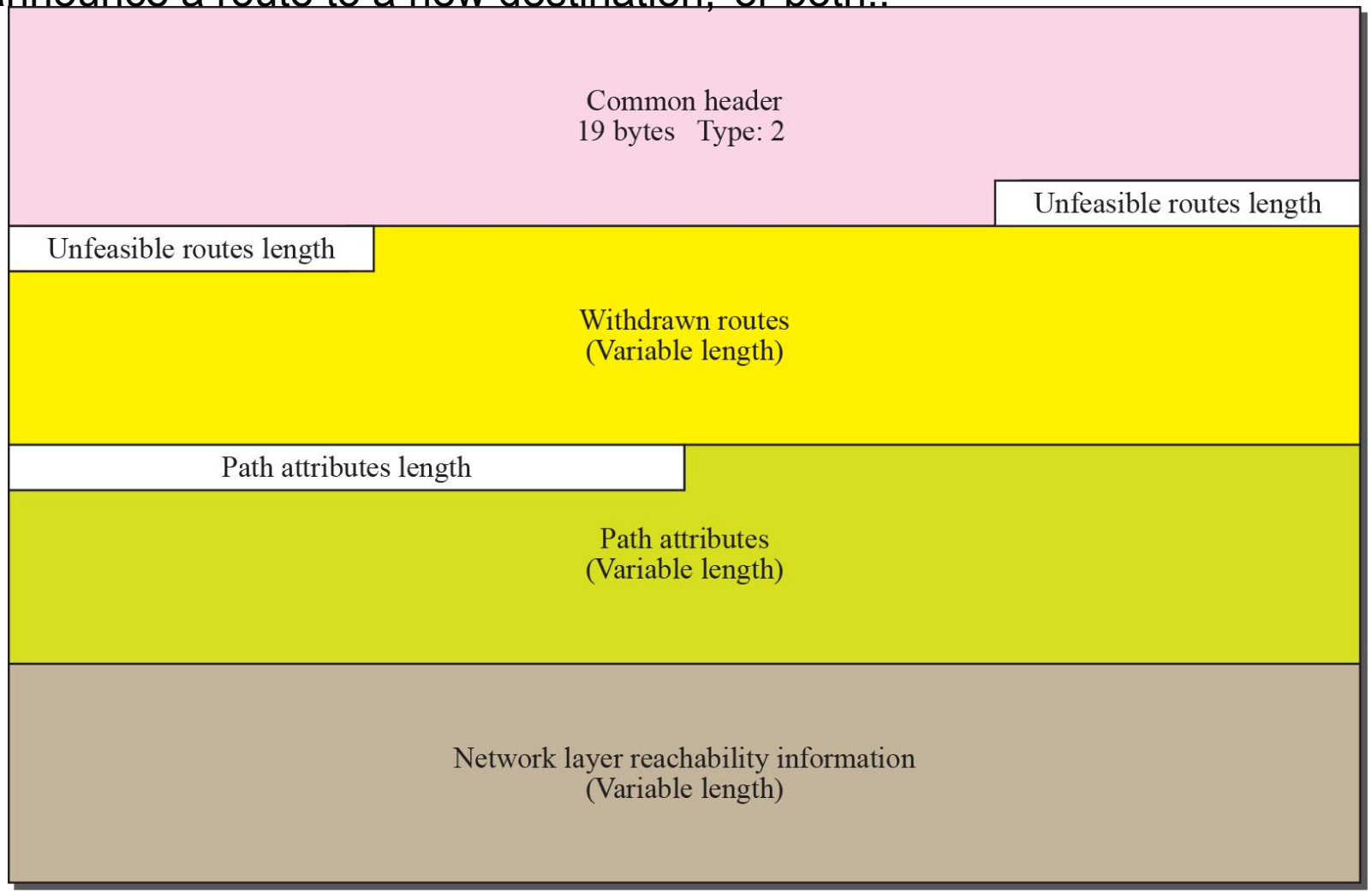
BGP identifier. This 4-byte field defines the router that sends the open message. The router usually uses one of its IP addresses (because it is unique) for this purpose.

Option length. The open message may contain some option parameters. In this case, this 1-byte field defines the length of the total option parameters. If there are no option parameters, the value of this field is zero.

Option parameters. If the value of the option parameter length is not zero, it means that there are some option parameters. Each option parameter itself has two subfields: the length of the parameter and the parameter value. The only option parameter defined so far is authentication.

Update message

The update message is the heart of the BGP protocol. It is used by a router to withdraw destinations that have been advertised previously, announce a route to a new destination, or both..



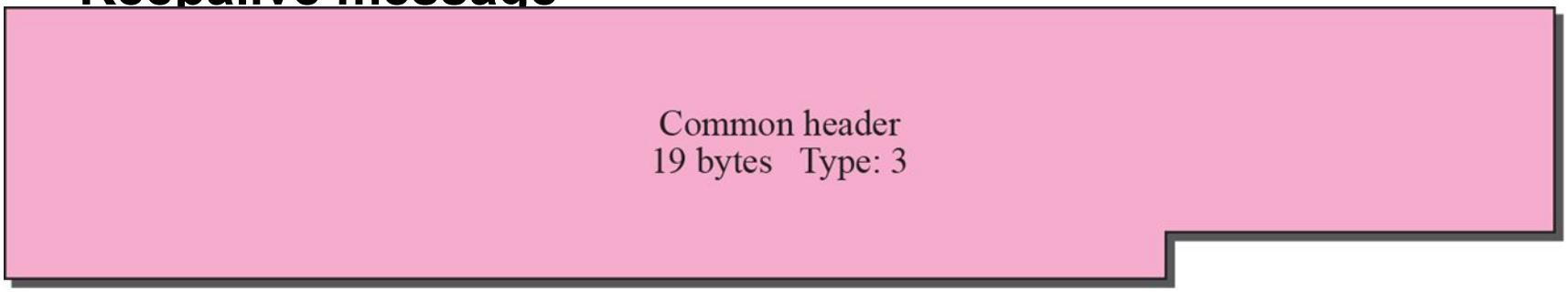
Unfeasible routes length. This 2-byte field defines the length of the next field.

Withdrawn routes. This field lists all the routes that must be deleted from the previously advertised list.

Path attributes length. This 2-byte field defines the length of the next field.

Network layer reachability information (NLRI). This field defines the network that is actually advertised by this message. It has a length field and an IP address prefix. The length defines the number of bits in the prefix. The prefix defines the common part of the network address

Keepalive message



Notification message

A notification message is sent by a router whenever an error condition is detected or a router wants to close the connection