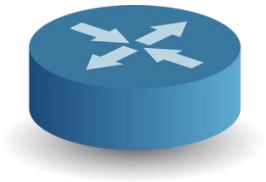
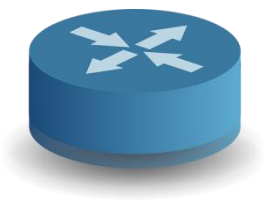


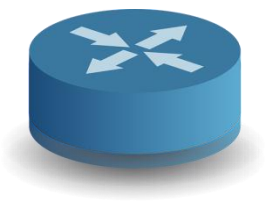
Computer Networks

Dr. Hoda Baraka



Course Learning Outcomes

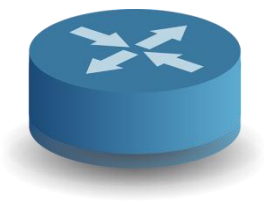
On successful completion of the course, students will be able to:	
1	Explain the concept of packet-switching, circuit switching, and identify and analyze the different types of packet delay in packet-switched networks
2	Describe, analyze and compare a number of network layer, routing protocols
3	Use IP addressing and sub-netting and apply routing algorithms to find shortest paths for network-layer packet delivery



Network Layer

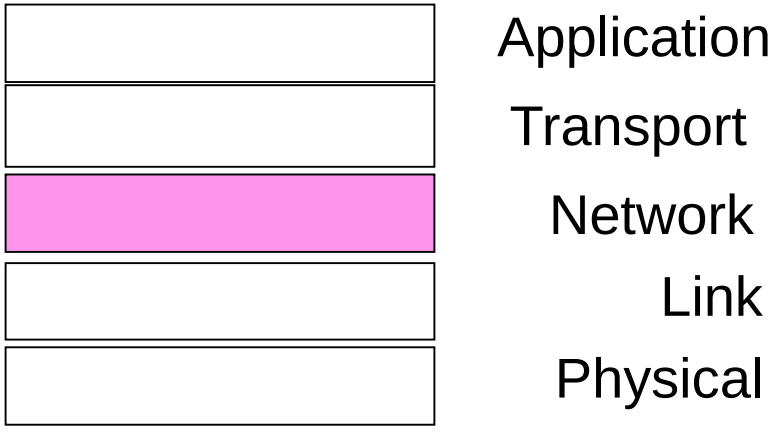
Chapter 5

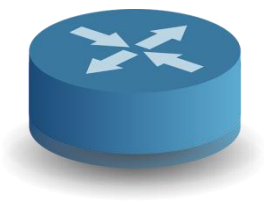
- Design Issues
- Routing Algorithms
- Network Layer of the Internet
- Quality of Service
- Internetworking
- Congestion Control



The Network Layer

Responsible for delivering packets between endpoints over multiple links



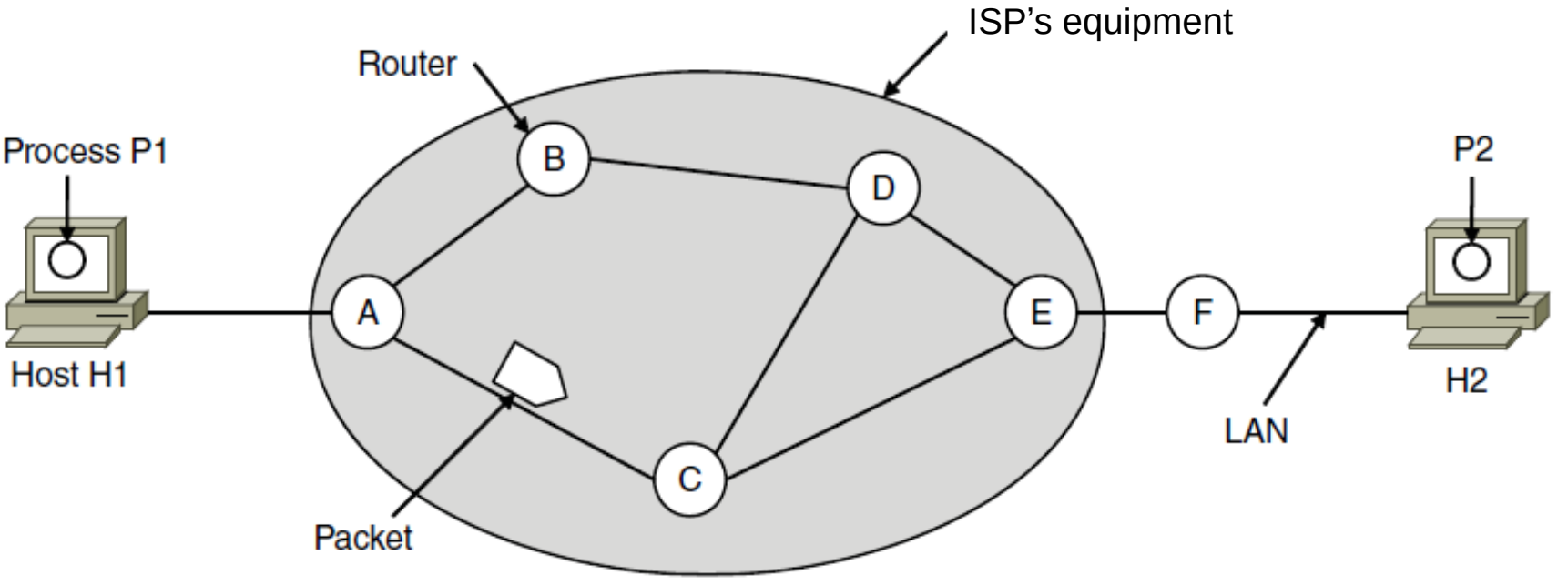


Design Issues

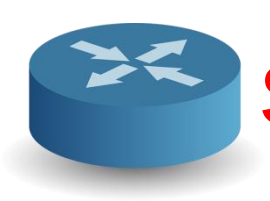
- Store-and-forward packet switching
- Connectionless service – Datagrams
- Connection-oriented service – Virtual Circuits
- Comparison of virtual-circuits and datagrams

Store-and-Forward Packet Switching

Hosts send packets into the network; packets are forwarded by routers



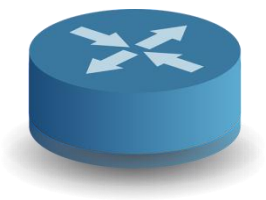
- Idea of how packets moves from source to destination:
  - Source sends packet to nearest router
  - Nearest router forwards to the next router along the path to destination
  - The process continues till destination



Store and Forward Packet Switching

- ***Store-and-forward***: a packet is completely received by a node before it is forwarded to the subsequent node
  - Queuing and congestion control
  - QoS
  - Error correction and detection

- ***Cut-through forwarding***: a node may start to forward a packet before it is completely received



Services Provided to the Transport Layer

- Design Objective of services provided by Network layer
  - Services must be independent of router technology/implementation
  - Transport layer should be shielded from topology and numbering
  - Numbering and addresses presented to upper layer should be uniform and independent of L1 and L2 protocols
- Two different camps
  - Connection oriented
  - Connectionless

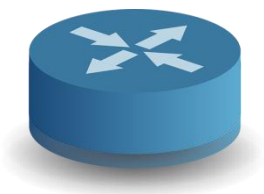
Services Provided to the Transport Layer

Connection oriented

- Backed by telecom (phone) people
- More than 110 years successful experience with worldwide telephone
- L3 should be reliable and provide QoS
- ATM is an obvious example

Connectionless

- Backed by IP people
- 35 years of successful experience
- Subnet is inherently unreliable → hosts should be responsible for reliability
- QoS is getting better and closer to connection oriented
- Many telecom giants are moving towards IP based infrastructure
- IPv4 is an obvious example



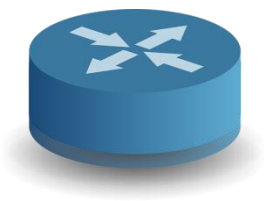
Services Provided to the Transport Layer

Connection Oriented

- Path between source and destination pre-established
- Usually called virtual circuit (**VC**)
- Each L3 segment on the path is sometimes called VC subnet

Connectionless

- No path pre-established
- Each packet is sent and routed independently
- Each packet carries enough information to be correctly forwarded to the destination
- Packet is usually called **datagram** (analogy with telegram)
- Each L3 segment on the path is sometimes called ***"datagram" subnet***

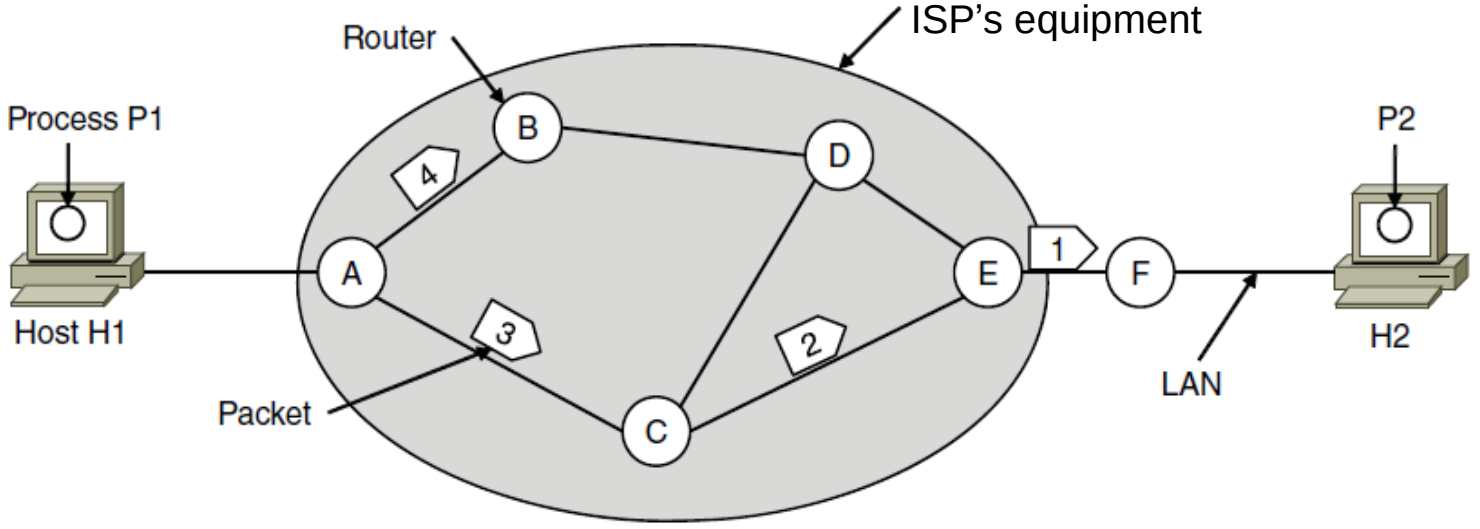


Implementation of Connectionless Service

- A router can only forward a packet to a *directly connected* router
- Each router has a ***routing table***
- In theory, a routing table has enough information to forward a packet to every destination
- A routing table is *dynamic*: It changes due to variations in the network
  - Topology changes (failures and/or introduction of new elements)
  - Congestion
  - Policy and contracts

Connectionless Service – Datagrams

- Packet is forwarded using destination address inside it
- Different packets may take different paths



A's table (initially)

A	
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	
B	B
C	C
D	B
E	D
F	D

C's Table

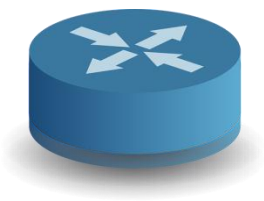
A	A
B	A
C	
D	E
E	E
F	E

E's Table

A	C
B	D
C	C
D	D
E	
F	F

Dest. Line

feh hena ghalta, enta el mfrod el table, ykon bt7ot feh mn 3nd kol location, el mfrod t7ot men el locations elly t2dr tro7lha.
f3nd C, enta el mfrod t7ot A w D w E.

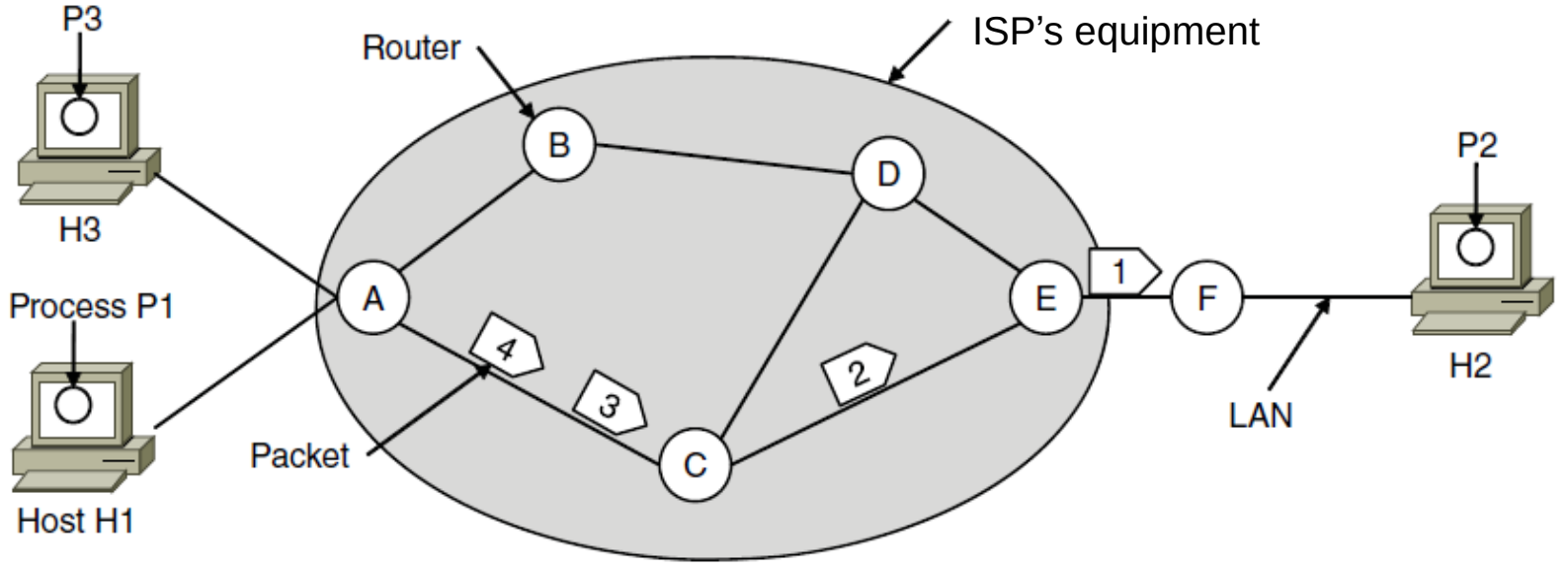


Implementation of Connection-Oriented Service

- A path is established between source and destination prior to sending packets
- A VC is assigned a local connection identifier on each router along the path from the source to the destination
- A connection ID is *unique* only between a *pair* of *consecutive* routers along the VC
- Usually the source and destination are known on every router along the path
- Each packet carries the connection ID when moving from a hop to the next hop

Connection-Oriented – Virtual Circuits

- Packet is forwarded along a virtual circuit using tag inside it
- Virtual circuit (VC) is set up ahead of time



A's table

In: Line	Tag	Line	Tag: Out
H1	1	C	1
H3	1	C	2

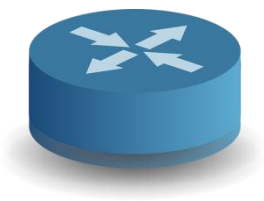
C's Table

A	1	E	1
A	2	E	2

E's Table

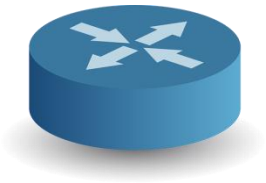
C	1	F	1
C	2	F	2

hwa hean bywdy 3la C, 34an feh algorithm by2olo en C asr3



Comparison of Virtual-Circuits & Datagrams

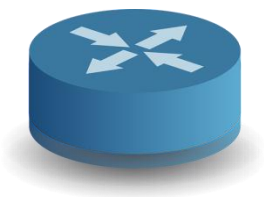
Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC



Routing Algorithms

da aham haga fl chapter da,
enk te3rf ezay tebny el routing table.

- Optimality principle
- Shortest path algorithm
- Flooding
- Distance vector routing
- Link state routing
- Hierarchical routing
- Broadcast routing
- Multicast routing
- Anycast routing
- Routing for mobile hosts
- Routing in ad hoc networks



Terminology

el doc skipped this

Node, vertex: A single router or host

Link, edge, arc: The network connecting two nodes

- LANs are usually modeled as node by itself (in rare cases as full mesh)

Router: A node that whose primary function is to forwarding packets*

- Usually not a data source or sink, although it sends and receives *control* data

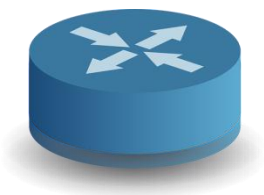
Host: A node whose primary function is a data (payload) source or sink

- A host may forward packets but its primary function is not packet forwarding

A node can have both router and host and router functionality

Hop: A single L3 link between two directly connected nodes

- Usually referred to in the context of routing and forwarding
- *Next-Hop*: The directly connected next node along a path



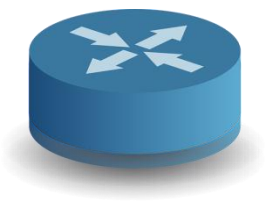
Terminology

el doc skipped this

Routing table: A table contains enough information to forward a packet to all destinations for which the router has at least one path

- Note that, even though a destination is reachable, the routing algorithm may have not found a path (e.g. due to policy or configuration).
- Hence we prefer to have a routing table defined as a table carrying information about ***known*** paths rather than information about reachable destinations

Metric: the weight of the edge or path



Routing Algorithm Desired Properties

el doc skipped this

Correctness*:

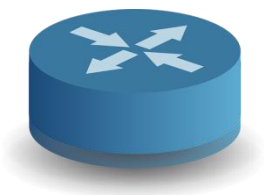
- Need to find a path that leads to destination if one exists or otherwise tell me that no path exists within ***bounded deterministic*** time under practical circumstances

Simplicity:

- Just enough complexity to achieve required functionality

Robustness:

- Routing protocol should be able to adjust for all node and link failures
- System wide failures are *unacceptable*



Routing Algorithm Desired Properties

Stability:

el doc skipped this

- A network must converge to equilibrium under design constraints
- Convergence:
  - A network is said to be converged if every router has a routing table containing a path to each reachable destination
  - A network is said to be converged if all routers have identical topological view of the network

Optimality vs **Fairness**:

- Usually conflicting goals
- All nodes should be able to use the network resources
- Optimality depends on how you define it.
- Example:
  - Maximize utilization and efficiency of network resources
  - Minimize average or maximum queuing delay

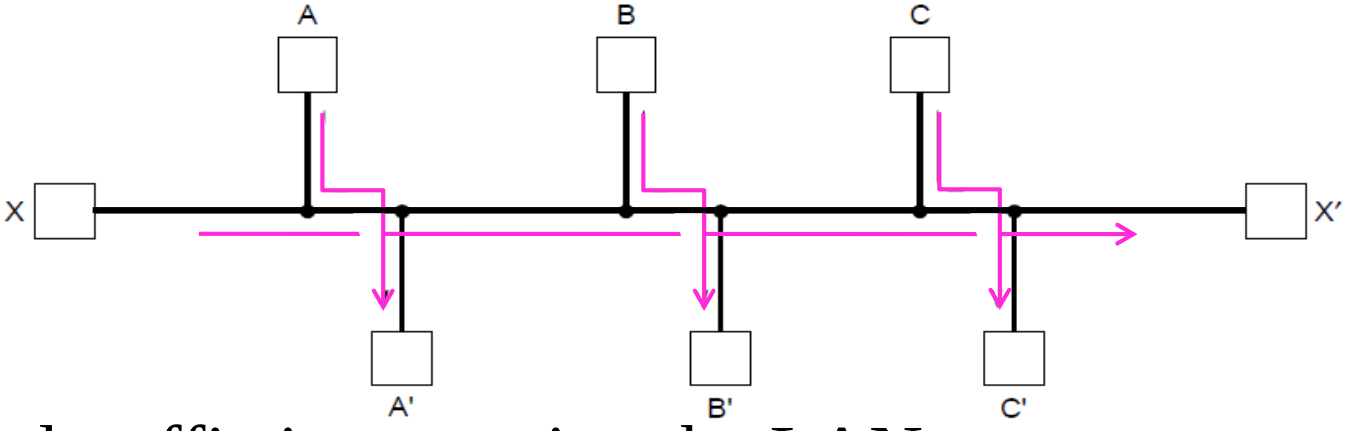
el doc skipped this

Optimality vs Fairness

Conflict between fairness and optimality.

Routing is the process of discovering network paths

- Model the network as a graph of nodes and links
- Decide what to optimize (e.g., fairness vs efficiency)
- Update routes for changes in topology (e.g., failures)

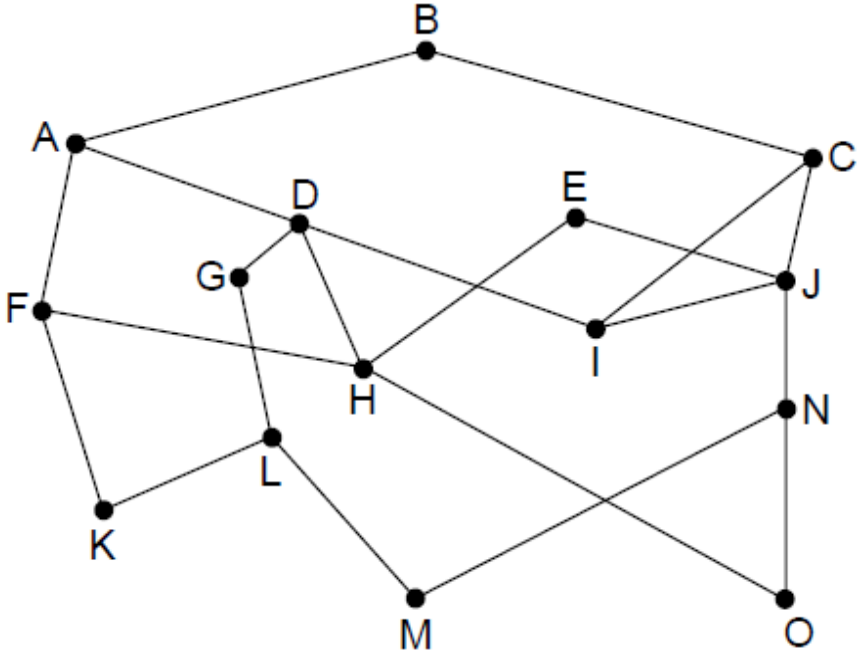


- Vertical traffic is saturating the LAN
- **Optimality (maximize utilization)**:
  - Shutoff packets from X to X` to avoid collision
- **Fairness**:
  - Allow collision to give X→X` a chance

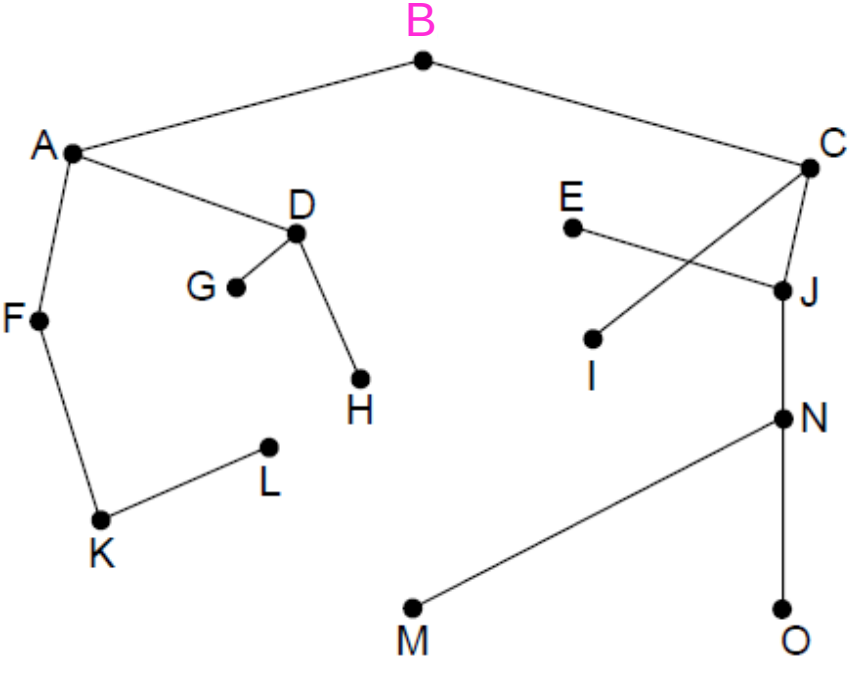
The Optimality Principle

Each portion of a best path is also a best path; the union of them to a router is a tree called the sink tree

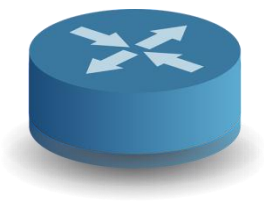
- Best means fewest hops in the example



Network



Sink tree of best paths to router B



Shortest Path Algorithm

Dijkstra's algorithm computes a sink tree on the graph:

- Each link is assigned a non-negative weight/distance
- Shortest path is the one with lowest total weight
- Using weights of 1 gives paths with fewest hops

Algorithm:

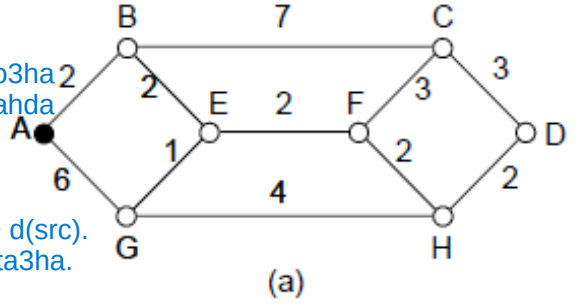
- Start with sink, set distance at other nodes to infinity
- Relax distance to other nodes
- Pick the lowest distance node, add it to sink tree
- Repeat until all nodes are in the sink tree

greedy algorithm

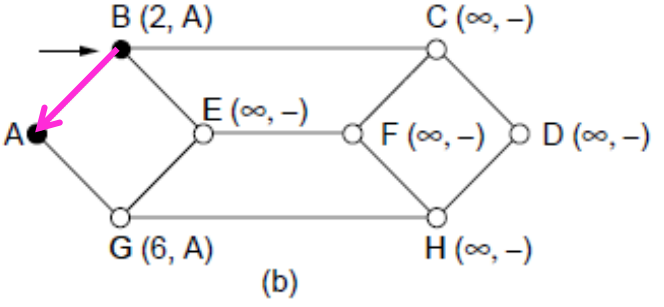
Shortest Path Algorithm

btbd2 3nd node
t3ml relax lel edges bto3ha w b3den ta5ud a2al wahda w tfdl t3ml repeat l7d ama t5ls

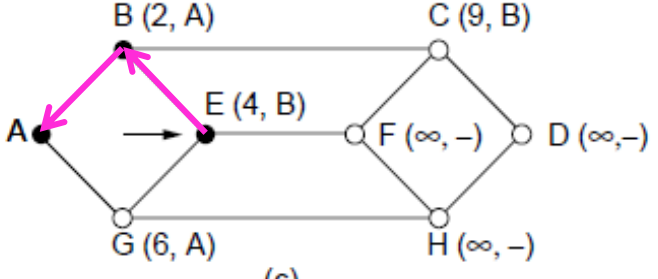
relax -> enk t2ol d(d) + d(src). w t2ol men el parent bta3ha.



(a)

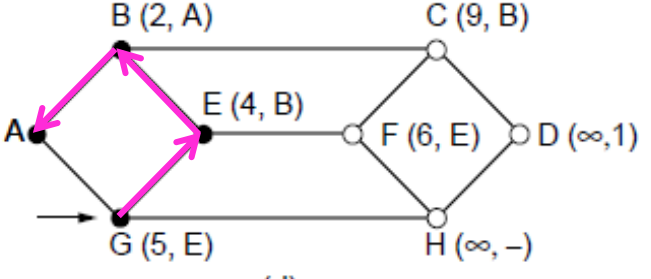


(b)

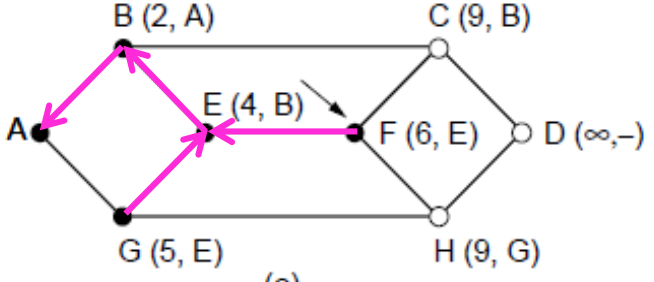


(c)

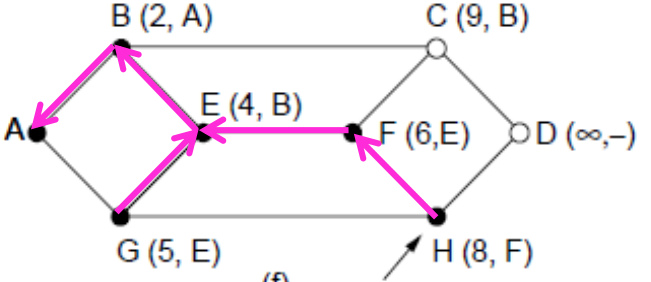
bno2f lama n3ml visit l kol el nodes.



(d)

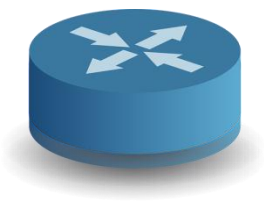


(e)



(f)

A network and first five steps in computing the shortest paths from A to D. Pink arrows show the sink tree so far.



Shortest Path Algorithm

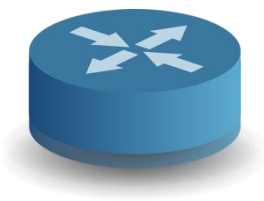
. . .

```
for (p = &state[0]; p < &state[n]; p++) {        /* initialize state */
      p->predecessor = –1;
      p->length = INFINITY;
      p->label = tentative;
}
state[t].length = 0;  state[t].label = perman
k = t;
do {
      for (i = 0; i < n; i++)                    /* this graph has n nodes */
            if (dist[k][i] != 0 && state[i].label == tentative) {
                  if (state[k].length + dist[k][i] < state[i].length) {
                        state[i].predecessor = k;
                        state[i].length = state[k].length + dist[k][i];
                  }
            }
```

. . .

Start with the sink, all other nodes are unreachable

Relaxation step. Lower distance to nodes linked to newest member of the sink tree

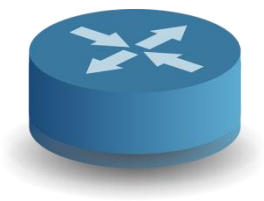


Shortest Path Algorithm (4)

. . .

```
    k = 0; min = INFINITY;
    for (i = 0; i < n; i++)
        if (state[i].label == tentative && state[i].length < min) {
            min = state[i].length;
            k = i;
        }
    state[k].label = permanent;
} while (k != s);
```

Find the lowest distance, add it to the sink tree, and repeat until done



Routing Protocol

A routing protocol specifies 2 main items

- How to distribute information about the topology
- How to use the information to compute paths

Other information

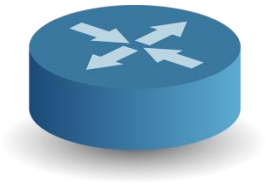
- How to compute metrics
- How to interpret metrics

Two commonly used paradigms

- Distance Vector
- Link state

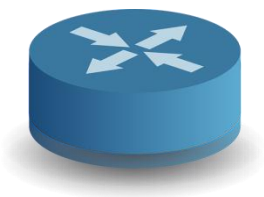
Routing to *multiple destinations* is different

- Multicast
- Broadcast



Flooding

- A simple method to send a packet to all network nodes
- Each node floods a new packet received on an incoming link by sending it out all of the other links
- Nodes need to keep track of flooded packets to stop the flood; even using a hop limit can blow up exponentially



by3mlo routing ezay?

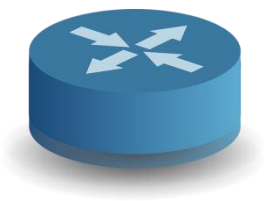
Flooding

enta ka router, el hadaf bta3k enk t3rf enta httl3 3la anhy link 34an tewsl lel destination.

dayman awl 7aga fe 7l ay moshkela, enk t3ml 7l ghaby msh m7tag enk tfkr feh.

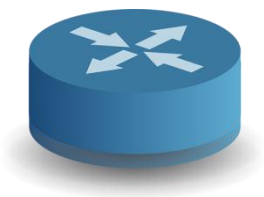
fa el flooding enk tb3t 3la kol el links nfs el package, fa da hydmnlk enk htsl aked, bs da msh a7sn 7aga 34an el efficiency bt3to msh kwsya.

- Not a routing protocol, i.e. it does **not** specify how to compute paths
  - it is a *way of* ***forwarding*** **packets**
- Incoming packet is *replicated* to *all outgoing* interfaces *except* incoming interface
- Lead to possible infinite duplication of packets
- **How to limit packet duplication:**
  - Limit Number of hops on each packets
  - Keep track of which packet has been forwarded and don't forward it again (used in LSA flooding, later)- link state advertising
  - Selective flooding: Only flood out of interface *approximately* towards the destination.
    - Problem: How to find "*approximate*" interfaces
  - Use RPF flooding (to be mentioned later) – reverse path forwarding



Flooding

- Disadvantages
  - Waste of resources
  - Possible loops, although there are ways to avoid them
  - **Not Practical for *most cases***
- Advantages
  - Extremely robust → always finds a path if one exists
  - Military applications



Flooding

- Where Flooding is used?
  - In MANETs – mobile adhoc networks
    - Used as for initial packets to discover and compute paths in on demand routing
  - Multicast mode → *PIM-DM**
    - PIM-DM does what is called "***RPF (reverse path forwarding) flooding***"
    - Flood to *multicast-enabled* interfaces only if the packet arrives on the **RPF interface (***What is an RPF interface?***)**
    - Do **not** flood on the *incoming interface*
  - To distribute link state updates and other information in link state routing protocols

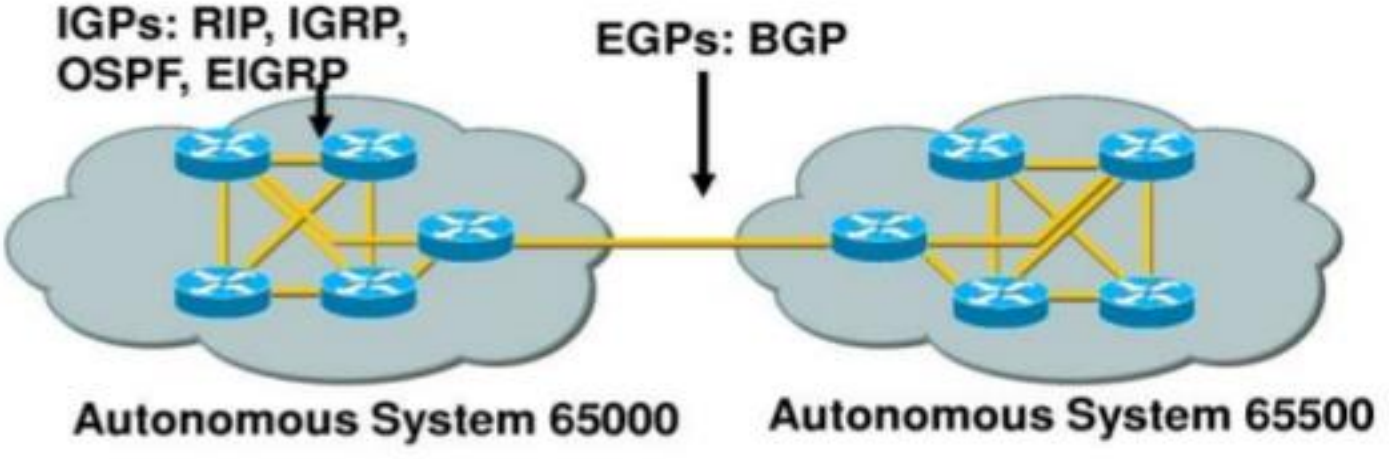
*Cisco PIM-DIM: Protocol Independent Multicast- Dense mode

Interior/Exterior Gateways

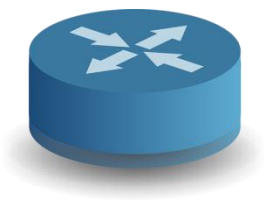
Border gateway Protocol - BGP

Internetworking - Module 13

BGP is the only actively used EGP on the Internet



IGP: Interior Gateway Protocol
EGP: Exterior Gateway Protocol



Distance Vector Routing

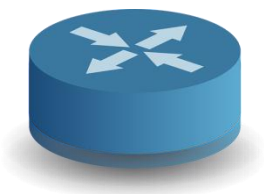
da awl tare2a fakro feha 34an ye3mlo routing.

Distance vector is a distributed routing algorithm

- Shortest path computation is split across nodes

Algorithm:

- Each node knows distance of links to its neighbors
- Each node advertises vector of lowest known distances **to all neighbors**
- Each node uses received vectors to update its own table
- Repeat periodically



Distance Vector Routing

- Sometimes called distributed **Bellman-Ford** routing algorithm
- Basis for one of the earliest routing protocols → **RIP (Routing Information Protocol)**
- Data Structures
  - Router maintains a table of best path(s) to every destination (**vector**) :
    - next-hop(s) to get there
    - Metric to every destination: A.K.A distance, and hence the term *distance vector*.
  - The table is modified based on information *from* ***directly connected neighbors*** only
  - Router knows the metric to each of its neighbors
  - Metric can be anything (delay, hop count,…, etc.)
  - Metric is assumed to be *additive* (more complex metric aggregation are used in BGP)

BGP : Border Gateway Protocol

Distance Vector Routing

Basic Idea

- Routers X and Y are neighbors
- Metric from router Y to X is m_{YX}
- *Periodically*, router X advertises its metric, $x(i)$, to destination i to its neighbor Y
- Metric of router Y to destination i is

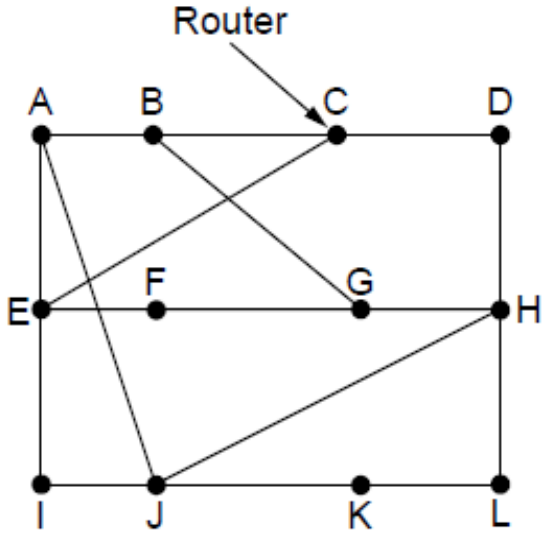
  $y(i)=x(i)+m_{YX}$
- If $y(i)$ is the minimum metric to destination i, then the best path to i is specified as:
  - Metric to destination i is $y(i)= x(i)+m_{YX}$
  - Next-hop to destination i is X

Formally, for a given node y and the destination node i,

- $y(i) = min_{x \in adj[y]} \{x(i)+m_{YX}\}$
- $Next\text{-}hop(i) = argmin_{x \in adj[y]} \{x(i)+m_{YX}\}$
- If there is more than one minimum path
  - Tie breaking is applied (depends on the protocol, configuration, or implementation)
  - ECMP (Equal-cost multi-path routing) is applied: I.e. more than one path is used to the same destination

Distance Vector Routing

kol node, by2ol ana mn 3ndy le ba2y el nodes m7tag msafat ad a.



Network

tb eshm3na khadha el A I H K ?
34an dol el nodes elly mtwsla bl J.
fa hwa byst2bl el gdawl bta3thom, w y3ml ping

To	A	I	H	K	New estimated delay from J Line
A	0	24	20	21	8 A
B	12	36	31	28	20 A
C	25	18	19	36	28 I
D	40	27	8	24	20 H
E	14	7	30	22	17 I
F	23	20	19	40	30 I
G	18	31	6	31	18 H
H	17	20	0	19	12 H
I	21	0	14	22	10 I
J	9	11	7	10	0 –
K	24	22	22	0	6 K
L	29	33	9	9	15 K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	

Vectors received at J from Neighbors A, I, H and K

New vector for J

fhwa keda hy3ml 4 pings, behom ye3rf JA, JI ... dol el delays el 7a2e2ya elly hwa edr yewslhom.

34an nbny el table. hngm3 el values elly gyaly fl tables + el delay bt3ty.

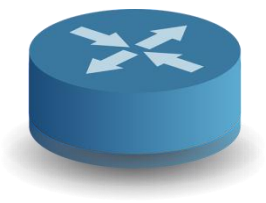
dayman bnb3t 2 columns, el destination, wl delay.

flw mn 3nd el J 3auz aro7 lel B, el options bt3ty btb2a

(A ->12 + 8)
(I -> 36 + 10)
(H -> 31 + 12)
(K -> 28 + 6)
---
now we need to select the minimum,
fa keda ht2ol enk a7sn tre2 ta5du hwa el A, l2no minimum path.

ay router byb3t el destination, w byb3t gambha el delay.

ana ka router msh muhtam el msg weslt ezay, lakn ana mohtm eny a3rf hya weslt fe ad a.

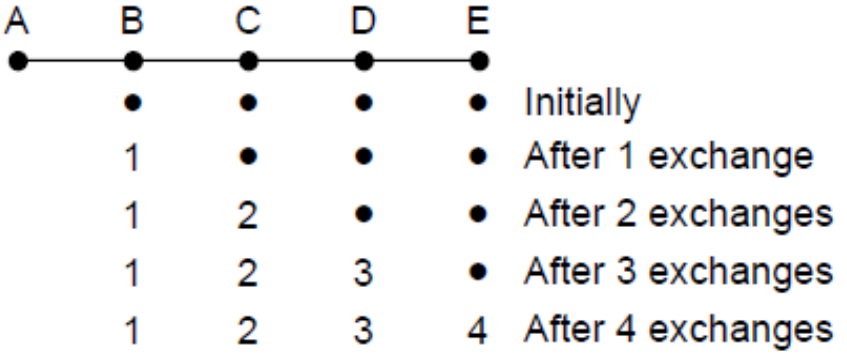


Distance Vector Routing
The Count-to-Infinity Problem

de mushkela nategt en ana mogrd bab3t el msafa elly ba5udha mn gher ma a2ol ana wsltlha ezay.

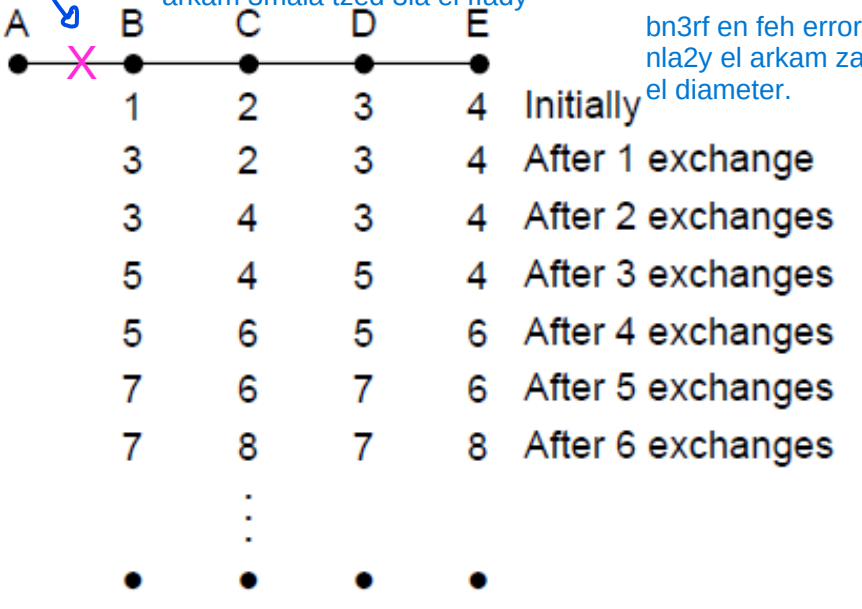
Failures can cause Distance Vector protocol to "count to infinity" while seeking a path to an unreachable node

el cut da 7asal b3d ma na kont banet el table awl mara, fa el cable hena et2t3, fa ana el B lama tegy t3ml ping le A, msh htrod 3leha, fa hyrg3lha inf, lakn lama teb3t l C, C ht2olha ana bawsl lel A fe 2, fa hya ht2ol khlas tlama ana bro7 lel C, fe 1, w C bta5ud 2, yeb2a ana me7tag 3, lakn fl 72e2a ana msh bwsl aslum, w lama hro7 3nd C, hlaa2y nfs el klam, fa hla2y el arkam 3mala tzed 3la el ffady



Good news of a path to *A* spreads quickly

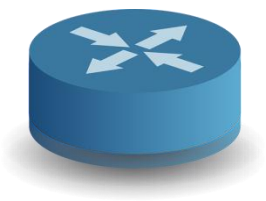
this link is cut.



bn3rf en feh error, lama nla2y el arkam zadet 3n el diameter.

Bad news of no path to *A* travels slowly

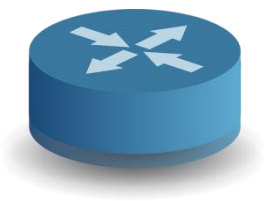
Bad news travel slowly



Distance Vector

- Advantages
  - Simplicity: Simple implementation and computation
  - Plug and play: No need for extensive network design and configuration
- Disadvantages
  - Slow because of count-to-infinity
  - Slow even *without* count-to-infinity:
    - » Path calculation happens serially
    - » Need to periodically send almost the entire routing table to the neighbors
      - Unless updates are sent reliably (Such as TCP in case of BGP)
  - May not converge on large highly dynamic networks
- RIP and RIPv2 are the most common examples
- BGP can be considered a variation of distance vector

el router dol kol wazefthom el asasya enhom u8sno el table bta3 el istances nem el routers w b3ha. toul el w2t by3mlo update lel routing tables.



Link State Routing

w2fna hena.

Link state is an alternative to distance vector

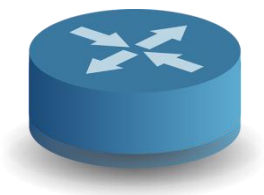
- More computation but simpler dynamics
- Widely used in the Internet (OSPF, ISIS)

Algorithm:

- Each node floods information about its neighbors (learnt using HELLO and ECHO packets) in LSPs (Link State Packets); all nodes learn the full network graph

- Each node runs Dijkstra's algorithm to compute the path to take for each destination

- Type of Link State packets: LSRequest, LSUpdate, LSAck



Link State Routing

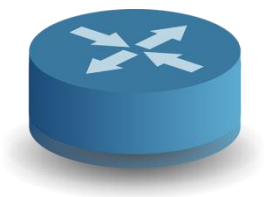
Basic Idea:

- Each router must do the following:

  1. Discover its neighbors, learn their network address.
  2. Measure the metric (delay, cost,…, etc.) to each of its neighbors.
  3. Construct a packet telling all it has just learned.
  4. Send this packet to all other routers (**flood**) (not just direct neighbors).
  5. Each router independently and in parallel computes the shortest path to every other router.

- In theory, shortest path algorithm can be anything. However Dijkstra's is almost always applied

- Each router must have a *network wide* unique identifier



Learning about the Neighbors

Hello Packets

- Neighbors exchange special packets called “hello” to enable dynamic discovery of neighbors and maintain neighbor relationships
- Hello packets are locally multicasted or broadcast on a LAN to routers participating in the routing protocol

Hello packets are exchanged periodically

Hold down/ Dead time:

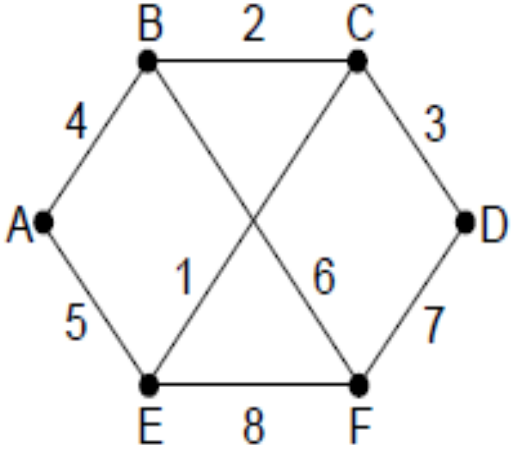
- Time until a neighbor is declared non-existing
  - More than the hello period
  - Usually 3 times the hello period

Hello packet can include other info, e.g.

- Router-ID
- Area ID
- Method of calculating metric
- Security and authentication information (option)

Link State Routing– LSPs

LSP (Link State Packet) for a node lists neighbors and weights of links to reach them



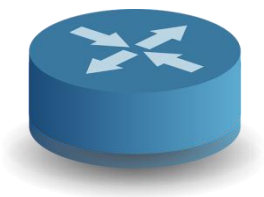
Network

Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

LSP for each node

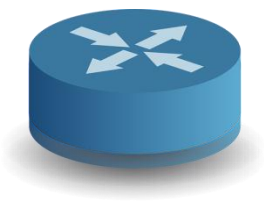
- Header of each LSP
  - Router ID: Unique identifier of the advertising router
  - Age: How long should **other routers** keep the information in this LS packet, Usually measured in seconds
  - Sequence: incremented for every LSP



Distributing the Link State Packets: AGE

Age can be used to solve the 3 basic flooding problems (how?)

1. Sequence number wrapping:
   - when the sequence number wraps, router LSA will be assumed obsolete and hence ignored
   - Thus age will not be refreshed
   - Eventually the router entry will expire and its LS will be accepted once again
   - Most routing protocol use 32 bits, so wrapping is unlikely
2. Router crash and reset its sequence number to zero
   - Same as above
3. Sequence number corruption
   - Same as above



Distributing the Link State Packets
Refinements

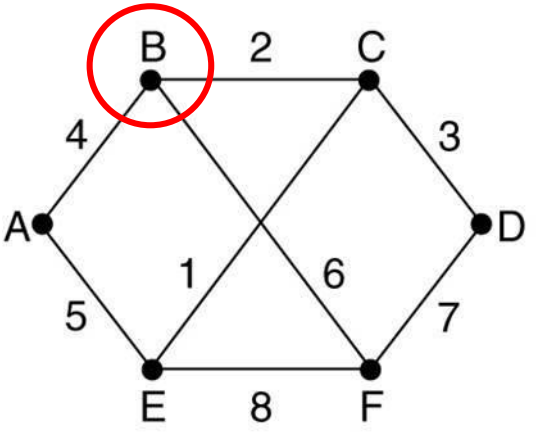
- ACK a flooded packet to guard against link errors
  - ACK even if the packet is duplicate
  - If ACK is expected and node does not ACK, neighbor may re-flood*
- Do not flood a received LSP immediately
  - Hold it in a holding area
  - If duplicate is received from a different interface do not flood on the second interface
  - If multiple LSPs from the same source received, send the latest (the one with largest seq)
  - When a line is idle, scan holding area for ACKs to be sent or LSPs to be flooded

Distributing the Link State Packets

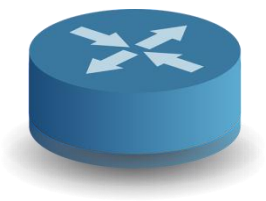
Example LSA buffer for node **B**

- Assume each row correspond to LSPs just arrived from a router but **not** yet processed
- Assume we do not flood LSPs immediately
- LSP from A arrived from A only
  - ACK to A
  - Flood to C,F
- LSP from E received twice (from A and F)
  - ACK to A and F
  - Flood to C only

htegy fl emt7an/



Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

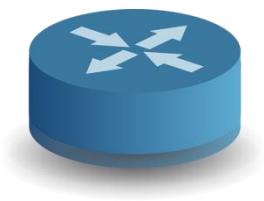


Link State Routing – Reliable Flooding

Seq. number and age are used for reliable flooding

- New LSPs are acknowledged on the lines they are received and sent on all other lines
- Example shows the LSP database at router B

			Send flags			ACK flags			
Source	Seq.	Age	A	C	F	A	C	F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

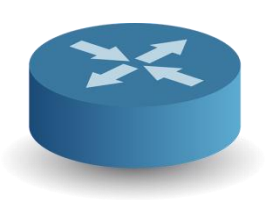


Computing Routes

- Each router has a full view of the network
  - Use Dijkstra to compute shortest path to each destination
- Scaling problems
  - Router with *n* neighbors in a network with average *k* links → *O(kn)* memory
  - Dijkstra is computationally intensive → problem in large networks
  - Configuration and implementation bugs can cause very hard to debug problems
- Advantages of Link state protocols
  - All routers compute routes in parallel → faster to converge
  - Better for larger networks
- Disadvantages
  - Complex implementation
  - Computationally intensive
  - Not a plug-and-play protocol → need to have good network design
- Bottom Line
  - Link State are better protocol and used in almost all large ISPs

Common Link State Protocols

- OSPF (Open Shortest Path First) for Internal Gateway Protocol (IGP)
- IS-IS (Intermediate System to Intermediate System)
  - Initially designed for DECnet and adopted by ISO
  - Interior Gateway Protocol (IGP)
  - Link attribute are usually info that routers can used to compute routes
  - Hence it can be used for IP, IPX, apple Talk,…,etc
  - Simpler implementation and configuration than OSPF



BGP— Exterior Routing Protocol

BGP (Border Gateway Protocol) computes routes across interconnected, autonomous networks

- Key role is to respect networks' policy constraints

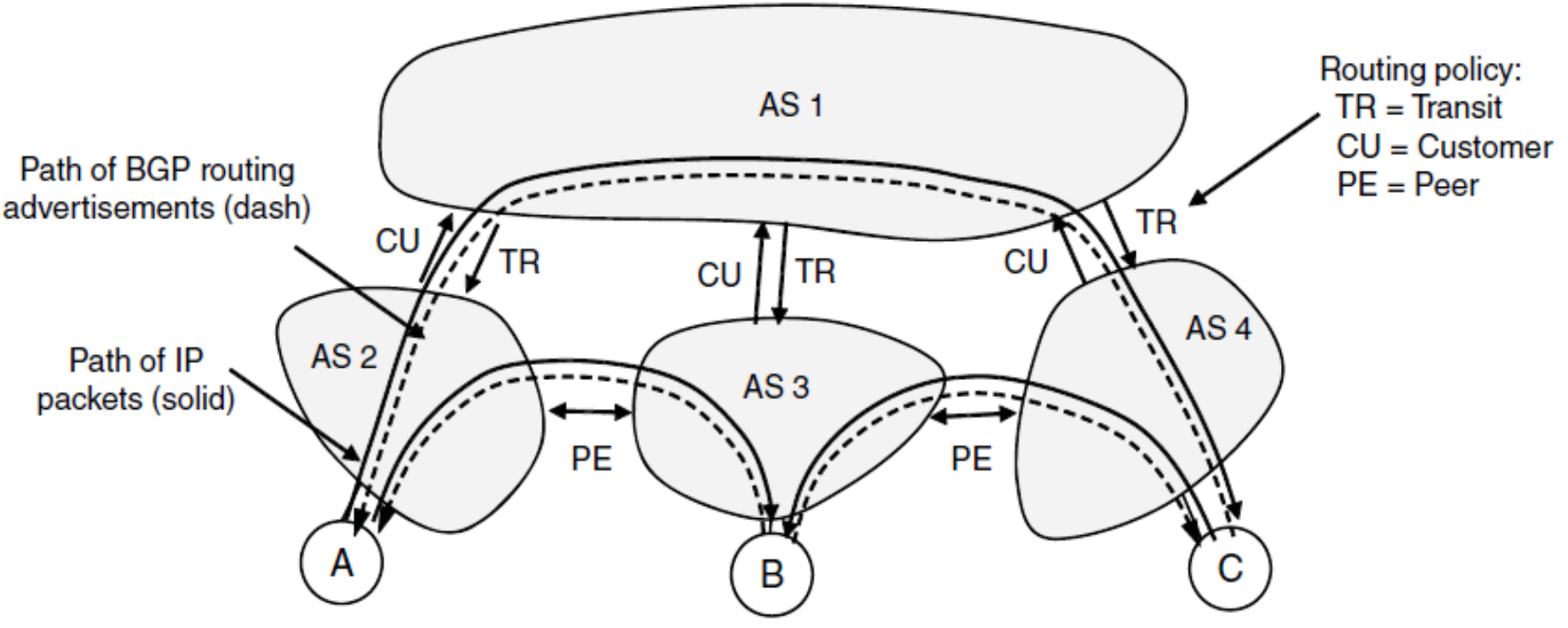
Example policy constraints:

- No commercial traffic for educational network
- Never put Iraq on route starting at Pentagon
- Choose cheaper network
- Choose better performing network
- Don't go from Apple to Google to Apple

BGP— Exterior Routing Protocol (2)

Common policy distinction is transit vs. peering:

- Transit carries traffic for pay; peers for mutual benefit
- AS1 carries AS2↔AS4 (Transit)



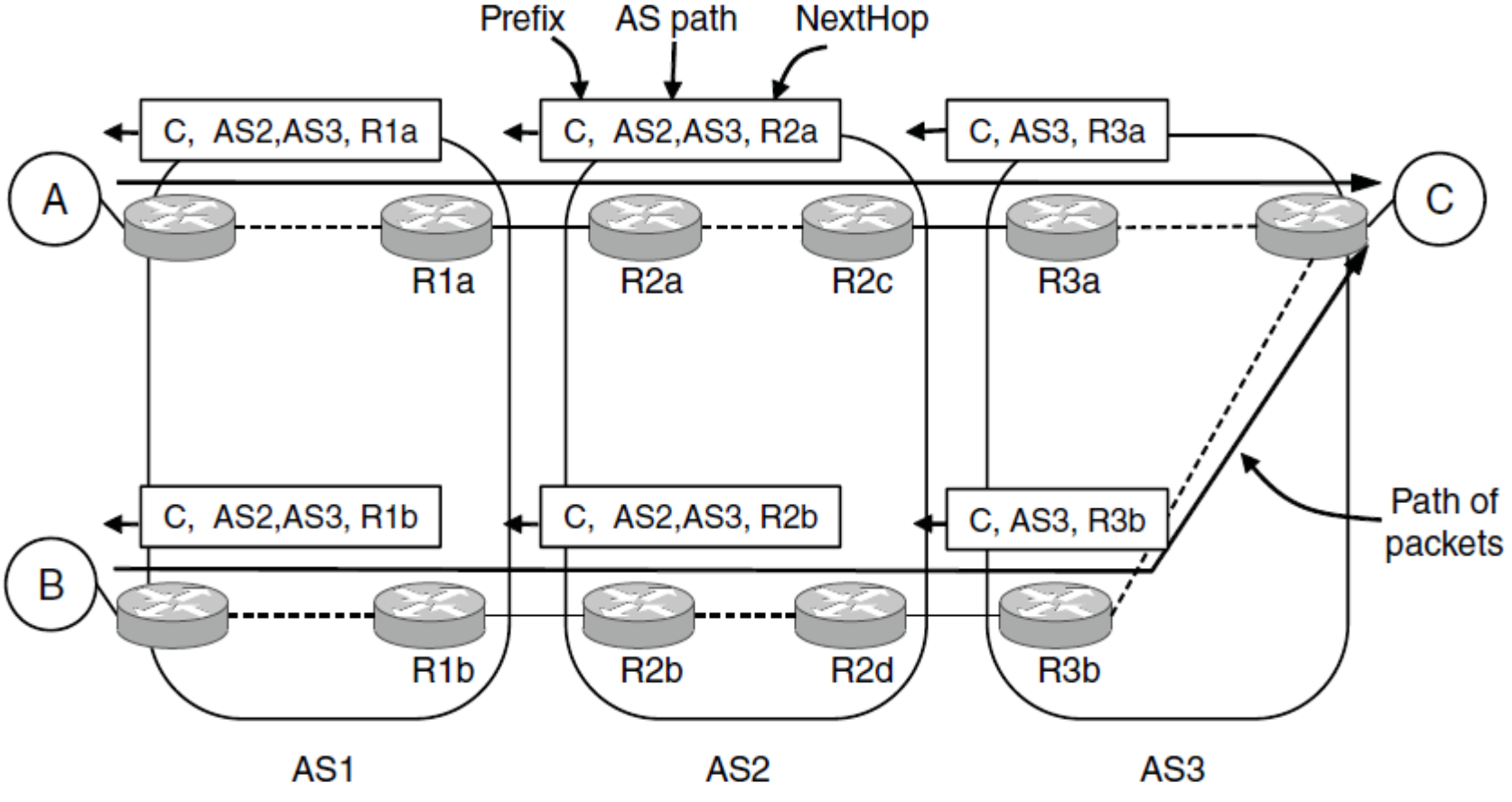
BGP— Exterior Routing Protocol

Path Vector Protocol

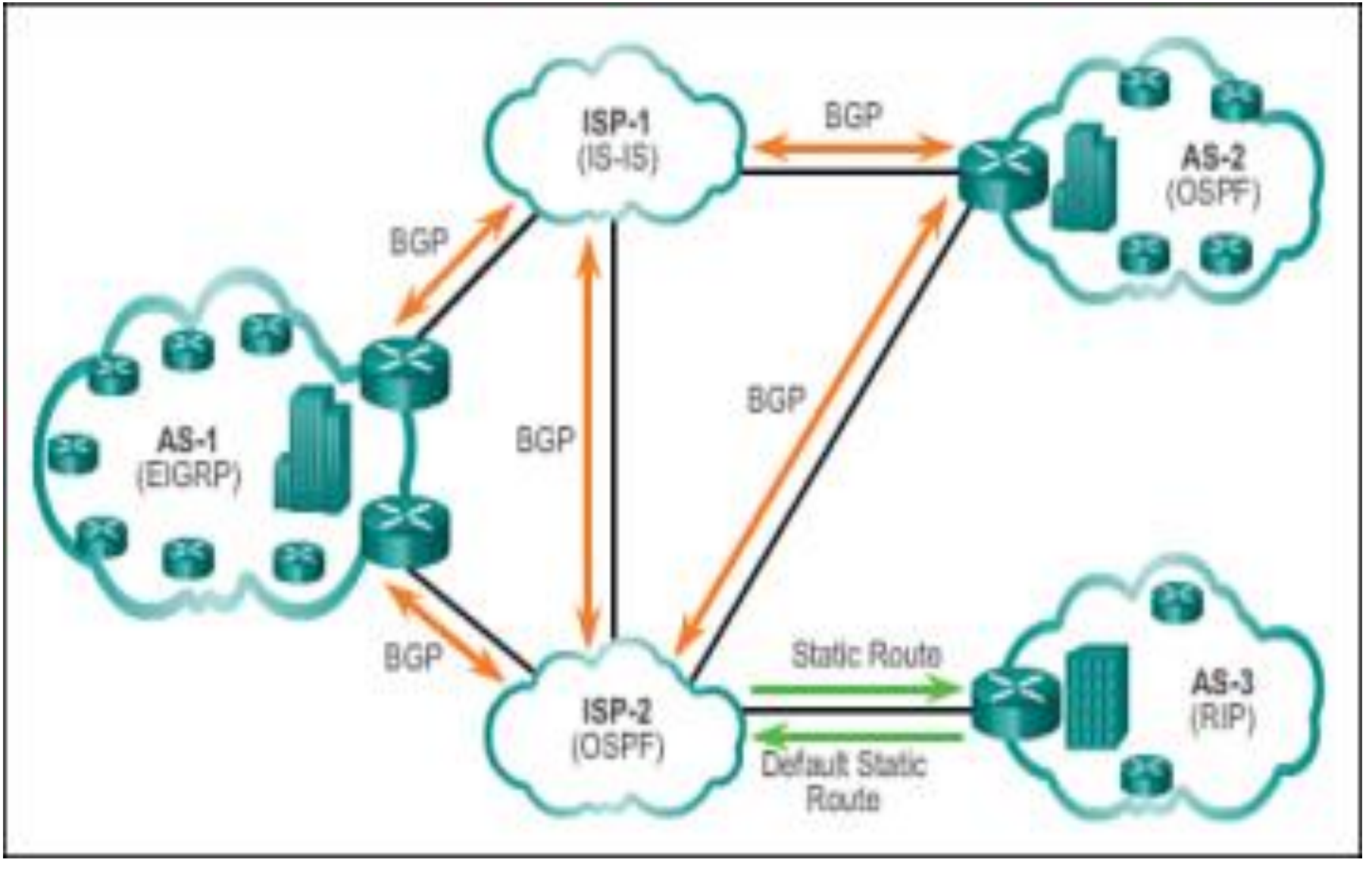
etlob mn hany yeshr7lk el slide de tany

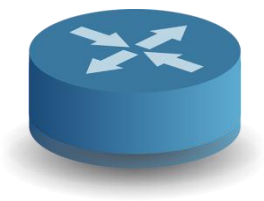
BGP propagates messages along policy-compliant routes

- Message has prefix, AS path (to detect loops) and next-hop IP (to send over the local network)



Example Scenario for Routing Protocols





Example Scenario

There are five individual autonomous systems in the scenario:

ISP-1: This is an AS and it uses IS-IS as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

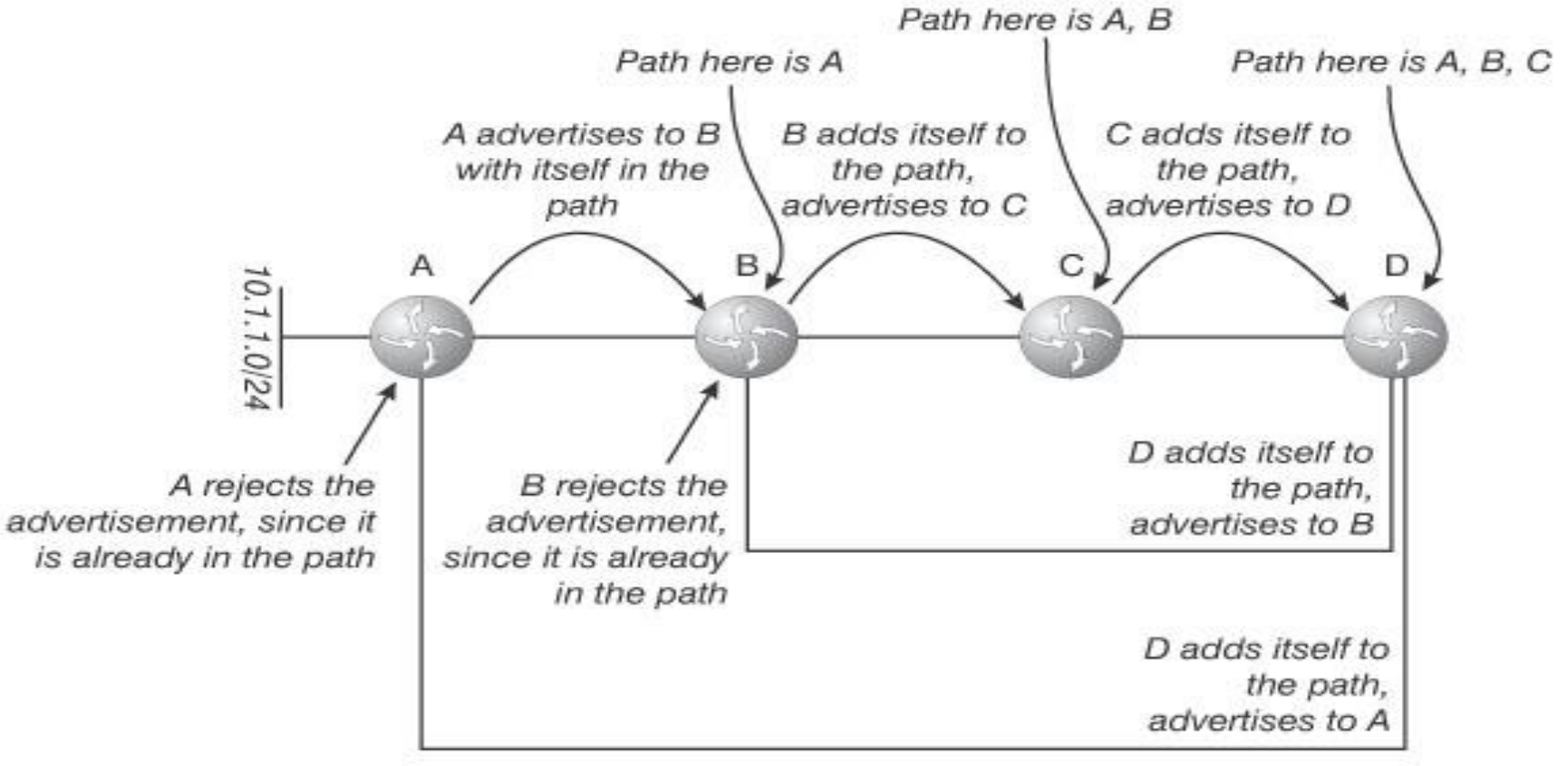
ISP-2: This is an AS and it uses OSPF as the IGP. It interconnects with other autonomous systems and service providers using BGP to explicitly control how traffic is routed.

AS-1: This is a large organization and it uses EIGRP as the IGP. Because it is multihomed (i.e., connects to two different service providers), it uses BGP to explicitly control how traffic enters and leaves the AS.

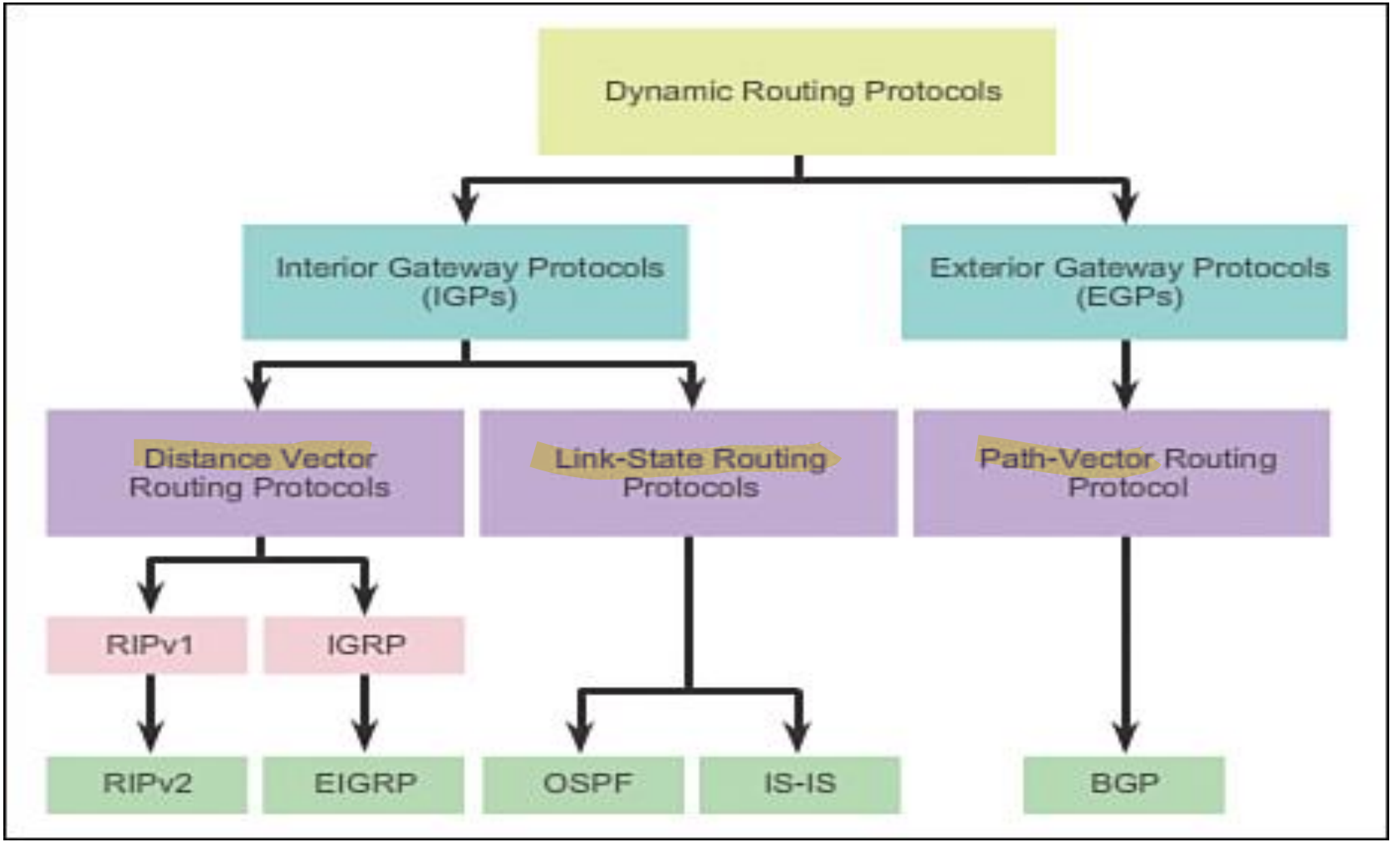
AS-2: This is a medium-sized organization and it uses OSPF as the IGP. It is also multihomed; therefore, it uses BGP to explicitly control how traffic enters and leaves the AS.

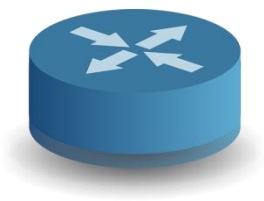
AS-3: This is a small organization with older routers within the AS; it uses RIP as the IGP. BGP is not required because it is single-homed (i.e., connects to one service provider). Instead, static routing is implemented between the AS and the service provider.

BGP: Path Vector Routing



Dynamic Routing Protocols





Assignment

- Difference between IGP, EGP
- Difference between OSPF, IS_IS, RIP, EIGRP, BGP

EIGRP: Enhanced Interior Gateway Routing **Protocol**