GENERAL SIR JOHN KOTELAWALA DEFENCE UNIVERSITY

Communication Networks

ET 3102

https://classroom.google.com/u/1/c/NjUwODgwNjkwNTY3

Classroom > Communication Networks - ET 3102

- Photonic and Laser Engine...
- Next Generation Cellular N...
- Communication Technology
- Communication Theory
- Communication Systems
- Deep Learning
- Machine Learning
- 35th Intake : EE & ET
- Individual Design Project (...
- Random Signals and Proce...

Archived classes

Settings

Stream | Classwork | People | Grades

Class code

nhqhb2c

Announce something to your class

Upcoming

No work due soon

View all

This is where you can talk to your class

Use the stream to share announcements, post assignments, and respond to student questions

Stream settings

10:49 AM

Outline

Overview on ISO/OSI reference model for open systems, packet and distributed systems and Topologies.

Physical and Data Link Layers.

Network (IP) and Transport Layers (TCP/UDP).

Session Layer, Presentation and Application Layer.

Local Area Network and Wide Area Networks.

Submodule Outline

Network (IP) and Transport Layers (TCP/UDP)

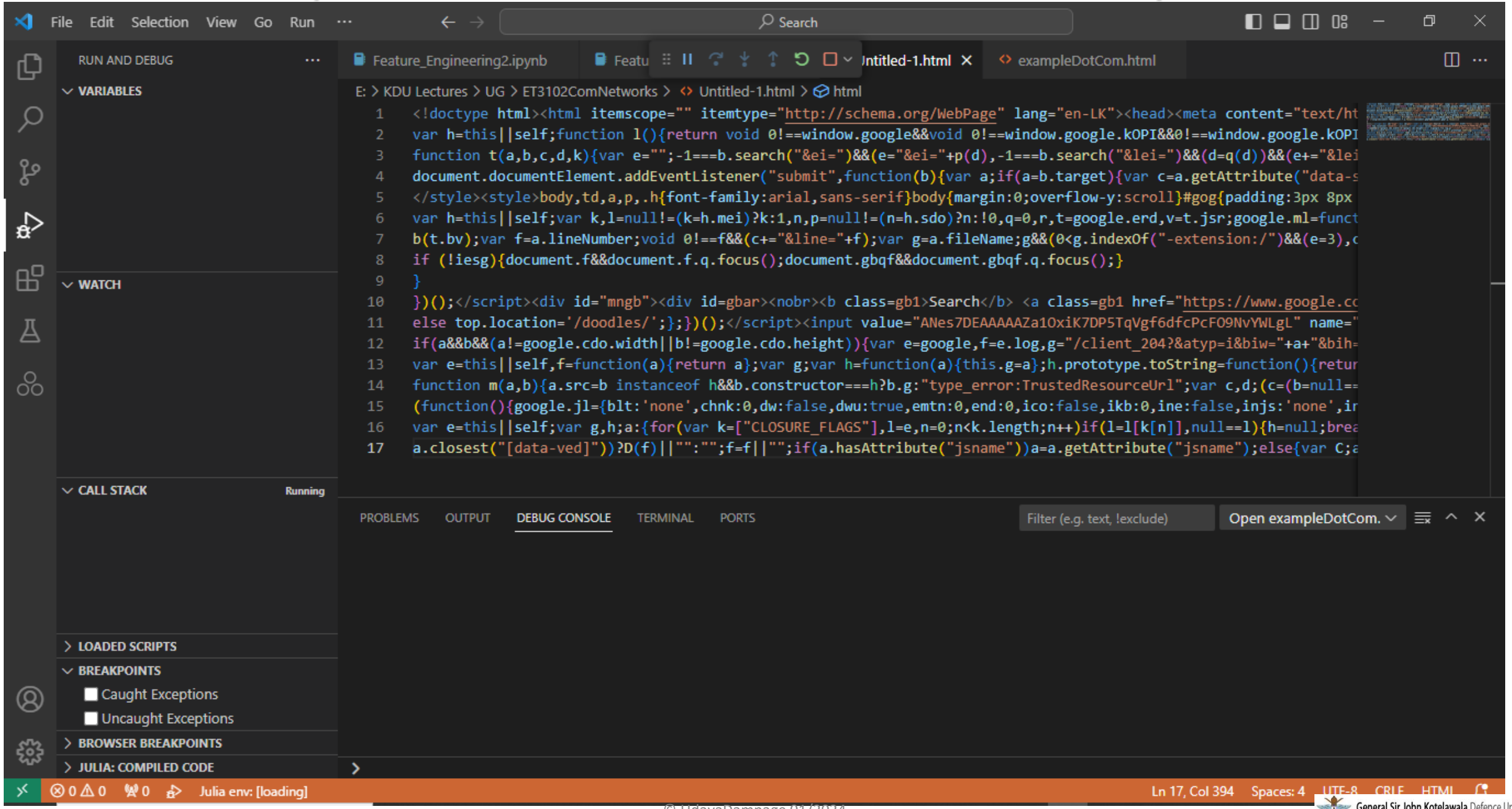
Routing, IP addressing: IPv4 and IPv6, IP sub-networking,

Internet Protocol,

Flow control and congestion control,

Overview of Mobile IP and Mobility management

Software Requirements – VS Code Community Edition



Network (IP) Layer

LAYER 1

- Repeater, hub An interconnection at layer 1 is realized by simply propagating the electrical signal further.
- This may require some signal amplification; a device realizing this is called a repeater.
- The name clarifies that it does nothing but send the signal forward, enabling its propagation to a longer distance.
- If the signal is digital, the repeater may also eliminate distortion effects introduced by the channel.
- Such an operation is called regeneration.
- A regenerative repeater tries to clean the signal from noise before amplifying it (which would result in amplifying the noise as well).
- Sometimes, multiple repeaters are integrated in a single device called hub; the difference between repeater and hub is in the number of interconnected lines, which is two for the former and higher for the latter.
- Actually, a hub does not even need to amplify the signal, the terminology just emphasizes its ability to connecting multiple inputs.
- Repeaters or hubs perform the simplest kind of interconnection.
- These devices are blind to the information content of what they are transmitting (repeating).
- They simply take the electrical signal and send it forward, improving its physical quality.
- Upper layer devices instead use information with higher level of abstraction.

LAYER 2

- Bridge, switch The devices operating on the data link layer are called bridges; a device with the same functionality as a bridge, but with the additional requirement of multiple input capability, is often given a different name: a switch.
- When layer 2 is considered, the requirement of connecting multiple lines is very common.
- Thus, the terms “bridge” and “switch” are often used as synonyms.
- The interconnection realized by a switch involves multiple access, which is no longer regulated by physical (electrical) characteristics of the signal, but rather by the MAC sublayer.
- A switch does not only interpret the bits of a packet, but also its content.
- In practice, the switch extracts the MAC address of the destination, which is contained in the packet, and uses this piece of information to determine how to connect the lines.
- However, bridges and switches cannot realize all kinds of interconnections.
- In particular, they do not have the capability to interconnect all kinds of medium-access protocols because the MAC addressing would be different.
- For example, a network operating on a hybrid wired/wireless physical layer – where some communication lines are cables and others are radio links, is clearly impossible to realize via repeaters, which do not interconnect different physical technologies. Switches can realize an interconnection only between certain kinds of differentMAC sublayers, for example between Ethernet and Fast Ethernet.
- However, to enable an entirely general interface of different medium access mechanisms, we must transfer to the
- network layer.

LAYER 3

- *Router* The purpose of the network layer is to allow communication between different kinds of technologies in a single network construct.
- This is achieved by means of a universal reference system, for example realized through IP addressing.
- The interconnection devices at layer 3 are called *routers*.
- In fact, as the name suggests, routers are in charge of directing the messages from source to destination, an operation called *routing*.
- For this reason, routers they are the places where routing decisions are made.
- Actually, hubs can also sometimes operate some simple routing procedures but these are very rough techniques that do not require interactions at the network layer and especially operate with a specific medium access control (MAC).
- Routers are instead capable of performing much more complex procedures, in an entirely general context.
- Note also that they always connect several lines at once, thus there is no need for a different name for single-input and multiple-input connecting devices.

LAYER 4 and Above

- Gateway Devices realizing connections at layers higher than 3 are often generically denoted as gateways.
- They includes transport gateways, which operate at layer 4 and are able to interconnect parts of the network using a different transport protocol, as well as application gateways, which are able to understand the content of the exchanged data and translate it into a different format.
- In general, the term is used to denote all interconnecting devices that have higher capability than simply managing routing of packets; for example, certain gateways allow the connection end points to be reached more efficiently, or filter the communication to improve security; these functions are sometimes called proxy and firewall.
- Other gateways are able to perform network address translation (NAT).

OSI Protocol Layer Functional Summary

Layer	Name	Functions
7	Application	User level data.
6	Presentation	Standardized data appearance, blocking, text compression.
5	Session	Sessions or logical connections between parts of an application; message sequencing, recovery.
4	Transport	Flow control, end-to-end error detection and correction, priority service.
3	Network	Routing, message blocking into uniformly sized packets.
2	Data Link	Reliable data delivery over physical medium, transmission error recovery, separating packets into uniformly sized frames.
1	Physical	Actual communication across physical medium, individual bit transmission.

NETWORK LAYER ROUTING

- The term “routing” describes the procedures to select paths (also called routes) in a network.
- A common example of routing in everyday life involves the selection of roads when driving towards a destination.
- Information networks require routing decisions to guide the messages through the communication devices to the final destination.
- The routing problem exists even outside the field of telecommunication networks;
- it was identified and studied by mathematicians in general contexts, which has given it a rigorous and theoretically solid basis. However, the strong impulse that the task of finding efficient routes has received in the last decades is motivated by the growth of telecommunication networks.
- The routing problem will be regarded at many levels.

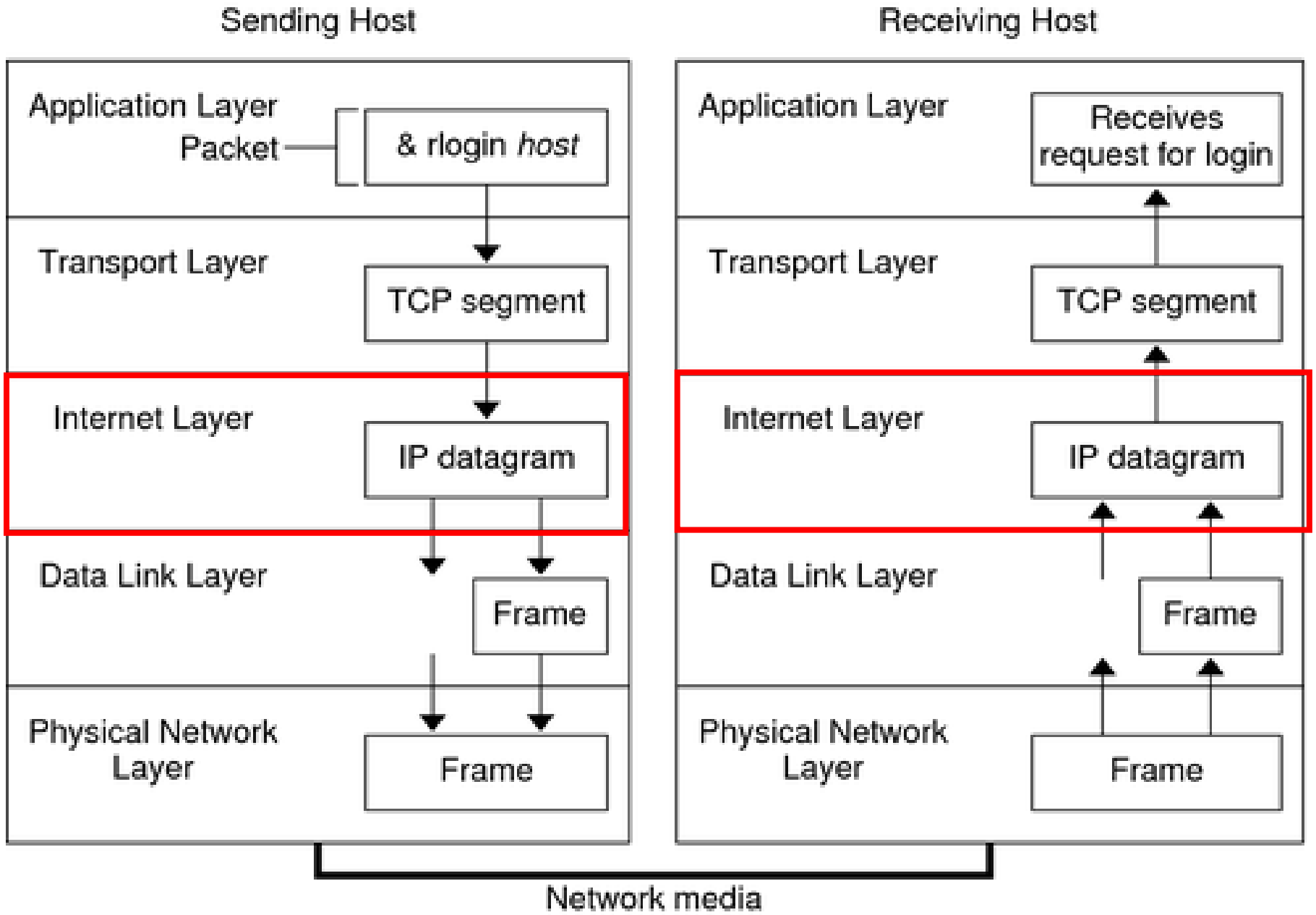
Internet Communication Layers Functional Summary

Layer	Functions	Responsibilities
Application	Prepare messages from user interactions.	User interaction, addressing.
Transport	Convert messages to packets.	Sequencing, reliability (integrity), error correction.
Internet	Convert packets to datagrams.	Flow control, routing.
Physical	Transmit datagrams as individual bits.	Data communication

Internet Communication Layer Protocol Summary

Layer	TCP Protocols	UDP Protocols
Application	HTTP (Hypertext Transfer Protocol): Used for communicating webpages. SMTP (Simple Mail Transfer Protocol): Used for communicating e-mail. FTP (File Transfer Protocol): Used for receiving or sending files Telnet (Terminal Emulation Protocol): Used for performing remote operations as if directly connected to the host from a terminal and others.	SNMP (Simple Network Monitoring Protocol): Used for controlling network devices. Syslog(System Audit Log): Used for entering records in the system log. Time: Used for communication and synchronizing time among network devices and others.
Transport	TCP.	UDP.
Internet	IP.	IP.
Physical	Data Communication.	Data communication.

Network Layer



Routing Algorithms

Network Layer Issues:

- Know about the topology of the communication subnet:
  - Set of all routes
  - Choose appropriate paths
  - avoid overloading
- Still deliver packets when source an destination are in different networks.

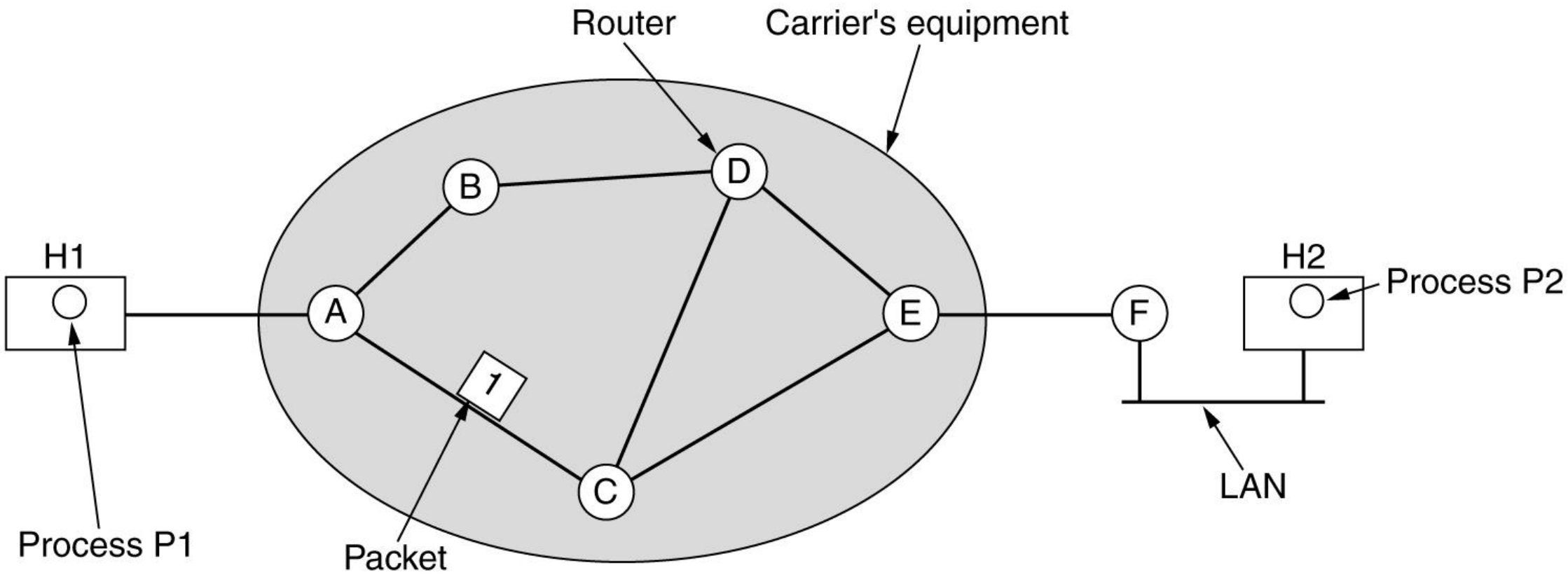
Summary of Topics

- The Problem
- The Dijkstra's Shortest Path Algorithm
- Distance Vector Routing
- Link State Routing
- Hierarchical Routing
- Routing in Ad Hoc Networks

Problem

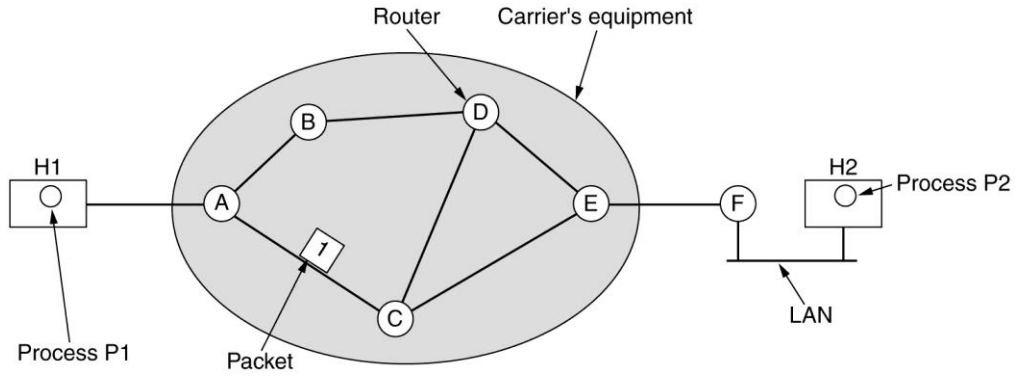
- Store-and-Forward Packet Switching
- Services Provided to the Transport Layer
  - Connectionless Service
  - Connection-Oriented Service

The Problem of Store and Forward Packet Switching



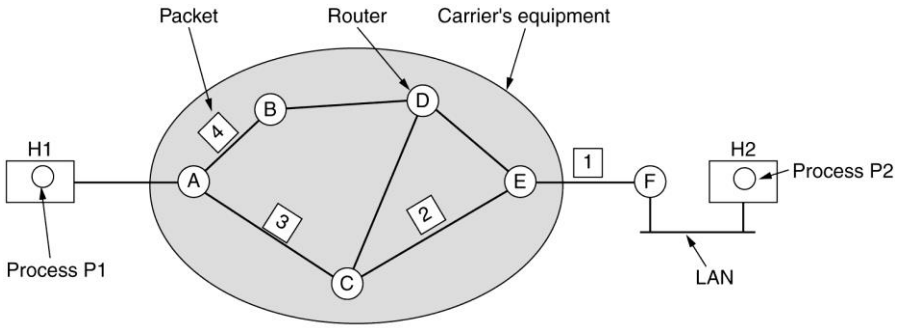
The environment of the network layer protocols.

The Problem of Store and Forward Packet Switching



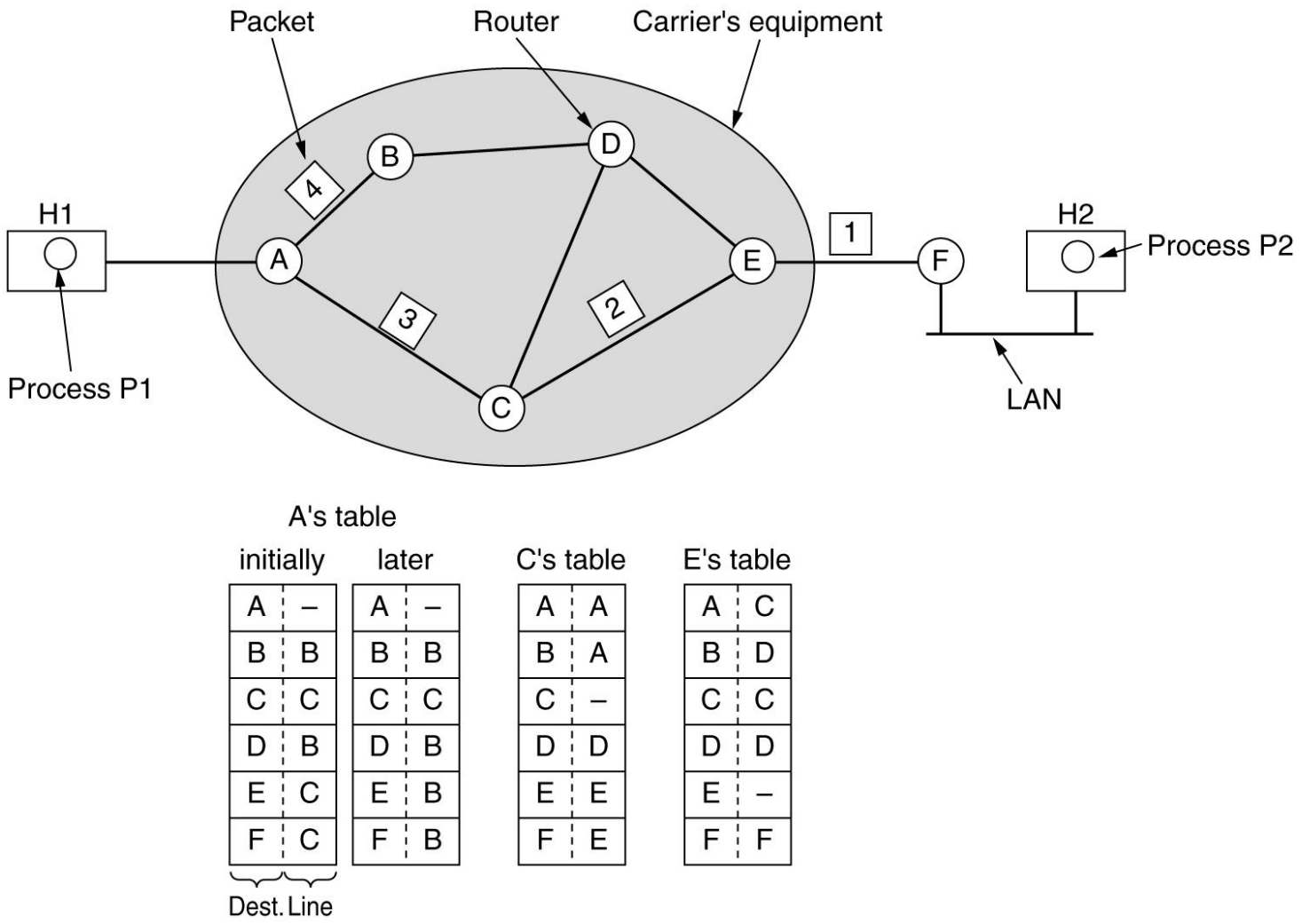
- A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the ISP (e.g., over an ADSL line).
- The packet is stored there until it has fully arrived and the link has finished its processing by verifying the checksum.
- Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered.
- This mechanism is store-and-forward packet switching.

The Problem of Connectionless Service



- If connectionless service is offered, packets are injected into the network individually and routed independently of each other.
- No advance setup is needed. In this context, the packets are frequently called datagrams (in analogy with telegrams) and the network is called a datagram network.
- If connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent.
- This connection is called a VC (Virtual Circuit), in analogy with the physical circuits set up by the (old) telephone system, and the network is called a virtual-circuit network.

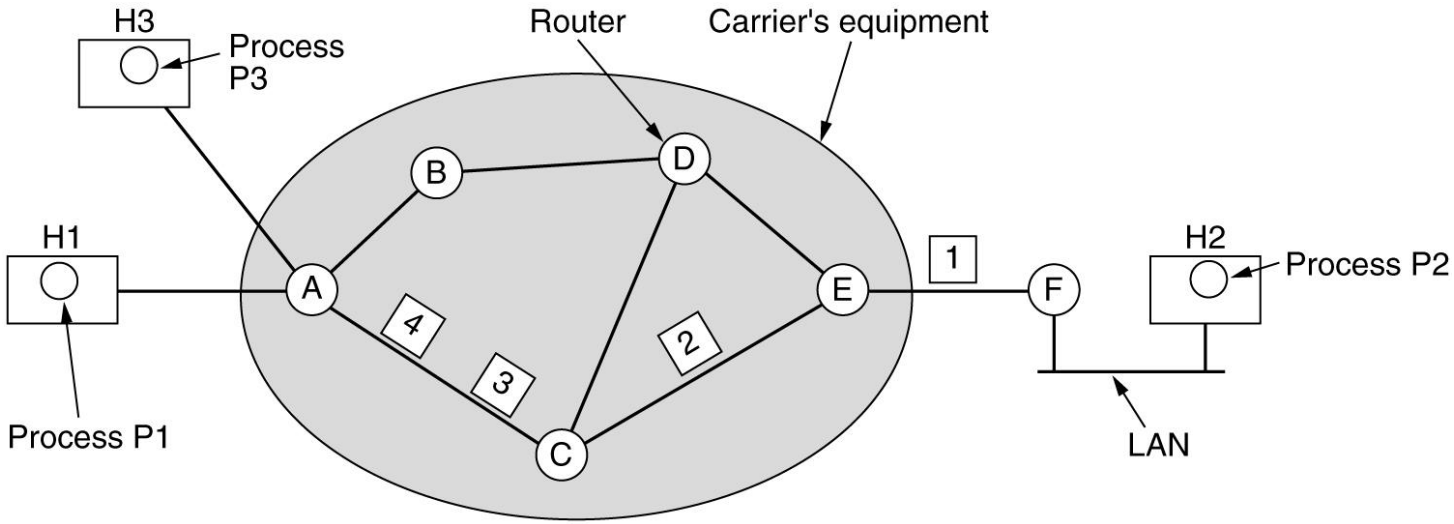
The Problem of Connectionless Service



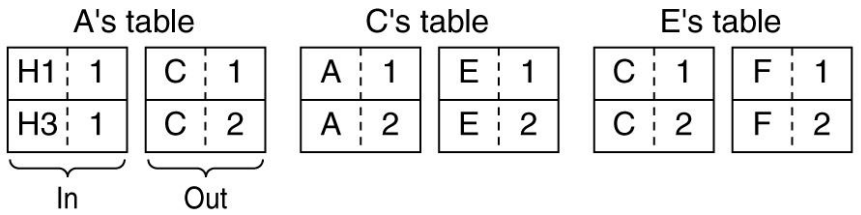
A's table initially		A's table later		C's table		E's table	
A	–	A	–	A	A	A	C
B	B	B	B	B	A	B	D
C	C	C	C	C	–	C	C
D	B	D	B	D	D	D	D
E	C	E	B	E	E	E	–
F	C	F	B	F	E	F	F

Routing within a datagram subnet.

The Problem of Connectionless Service



Label Switching



Connection ID Problem

Routing within a virtual-circuit subnet.

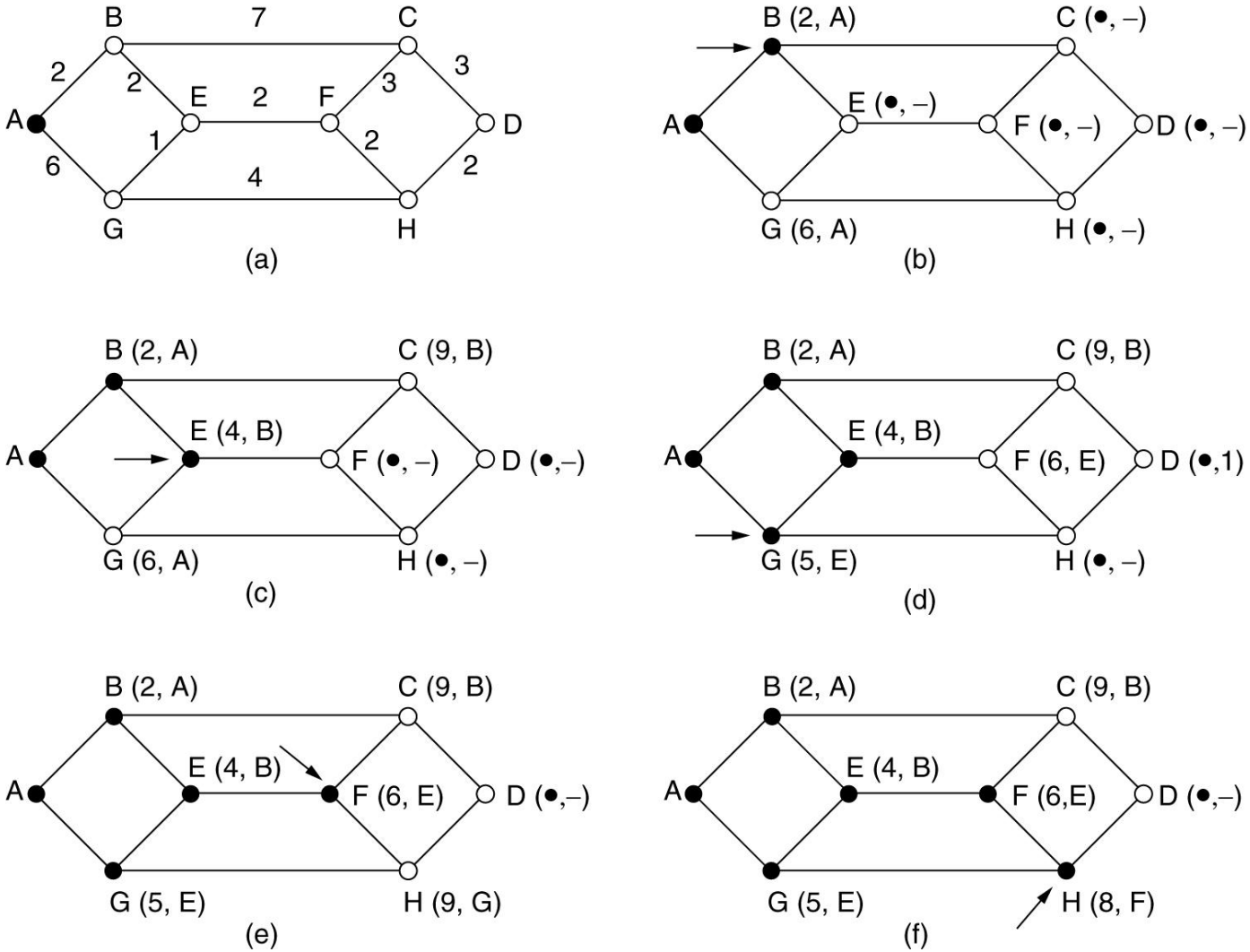
Connectionless VS. Connection-Oriented

Issue	Datagram subnet	Virtual-circuit subnet
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 Possibilities

Shortest Path Algorithm

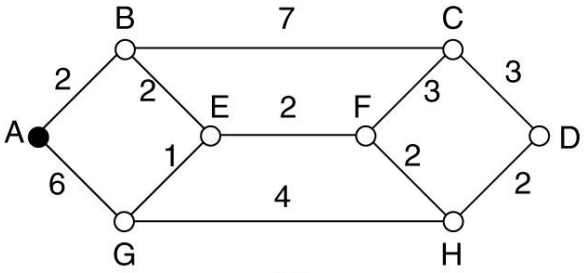
- Each node of the graph representing a router and,
- Each edge of the graph representing a communication line, or link



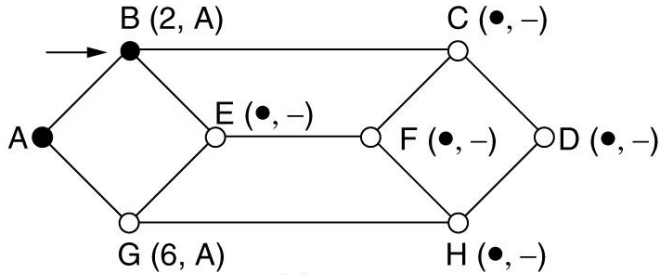
- The first 5 steps used in computing the shortest path from A to D. The arrows indicate the working node.

Shortest Path Algorithm

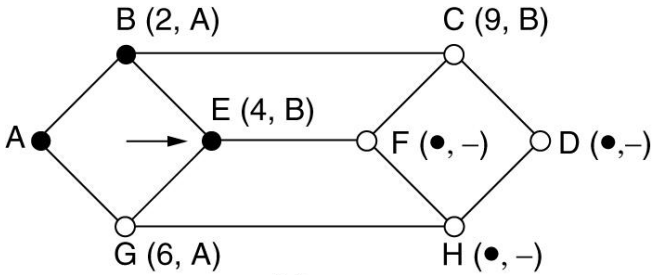
- From the weighted, undirected graph of Fig. (a), where the weights represent, for example, distance, assume that want to find the shortest path from *A* to *D*.
- Start out by marking node A as permanent, indicated by a filled-in circle.
- Then we examine, in turn, each of the nodes adjacent to A (the working node), relabeling each one with the distance to A.



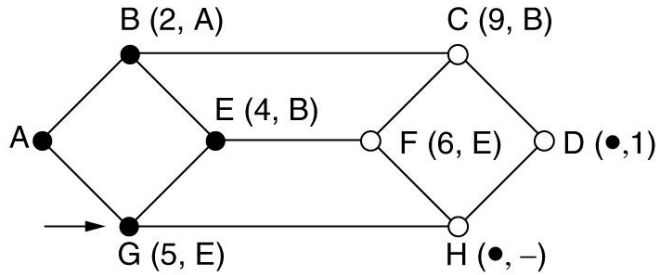
(a)



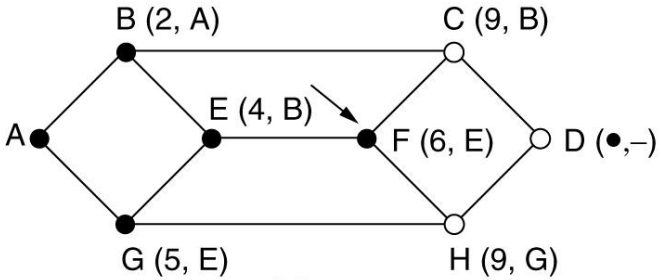
(b)



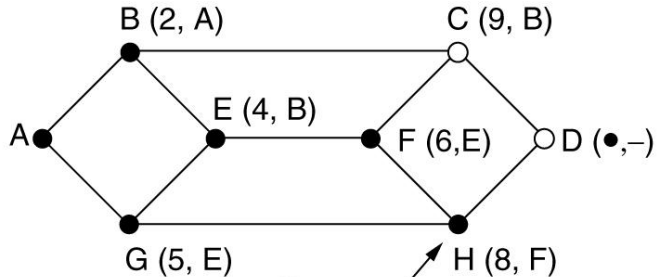
(c)



(d)



(e)

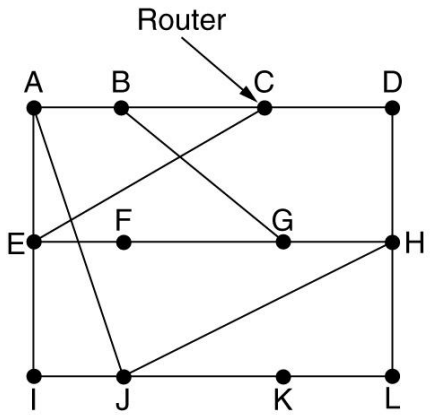


(f)

Distance Vector Routing

- **This** algorithm operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there.
- These tables are updated by exchanging information with the neighbors.

- The distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm and the **Ford-Fulkerson** algorithm, after the researchers who developed it.
- It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP



New estimated delay from J

To	A	I	H	K	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

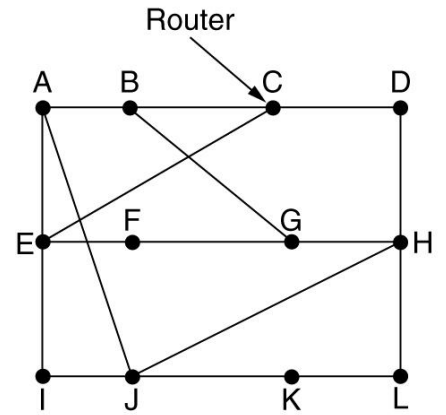
JA delay is 8 | JI delay is 10 | JH delay is 12 | JK delay is 6

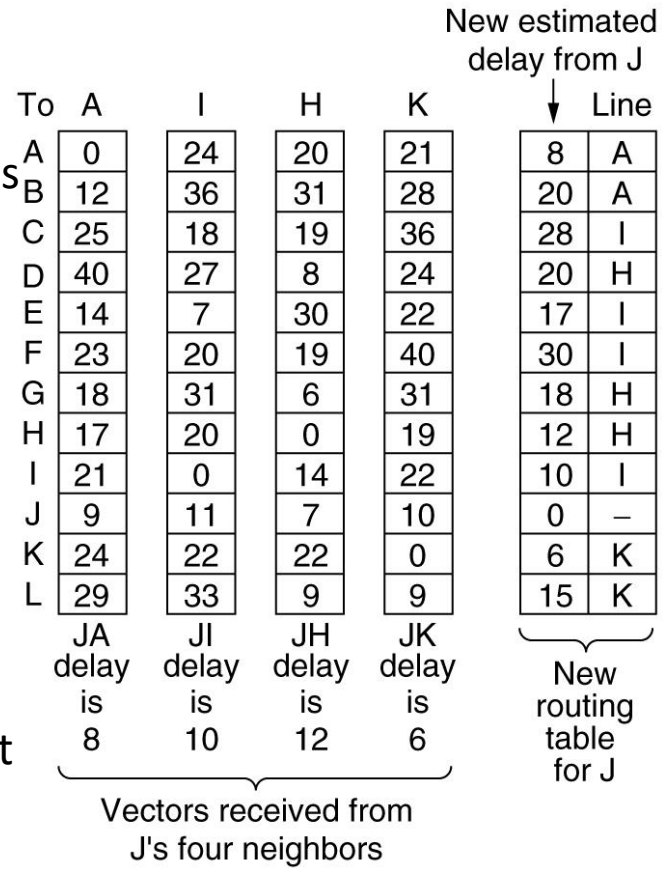
Vectors received from J's four neighbors

New routing table for J

Distance Vector Routing

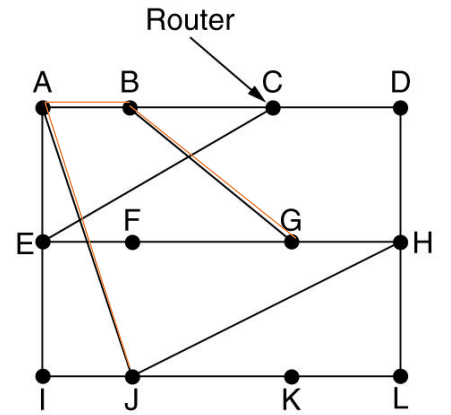
- In distance vector routing, each router maintains a routing table indexed by, and containing one entry for, each router in the subnet.
- This entry contains two parts: the preferred outgoing line to use for that destination and an estimate of the time or distance to that destination.
- The metric used might be number of hops, time delay in milliseconds, total number of packets queued along the path, or something similar.
- The router is assumed to know the ''distance'' to each of its neighbors. If the metric is hops, the distance is just one hop. If the metric is queue length, the router simply examines each queue. If the metric is delay, the router can measure it directly with special ECHO packets that the receiver just timestamps and sends back as fast as it can.





Distance Vector Routing

- As an example, assume that delay is used as a metric and that the router knows the delay to each of its neighbors. Once every T ms each router sends to each neighbor a list of its estimated delays to each destination. It also receives a similar list from each neighbor.



New estimated delay from J

To	A	I	H	K	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

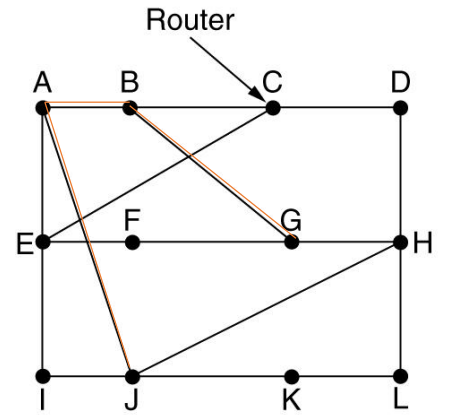
JA delay is 8 | JI delay is 10 | JH delay is 12 | JK delay is 6

Vectors received from J's four neighbors

New routing table for J

Distance Vector Routing - Example

- Find the best path from J to G from the given data ?

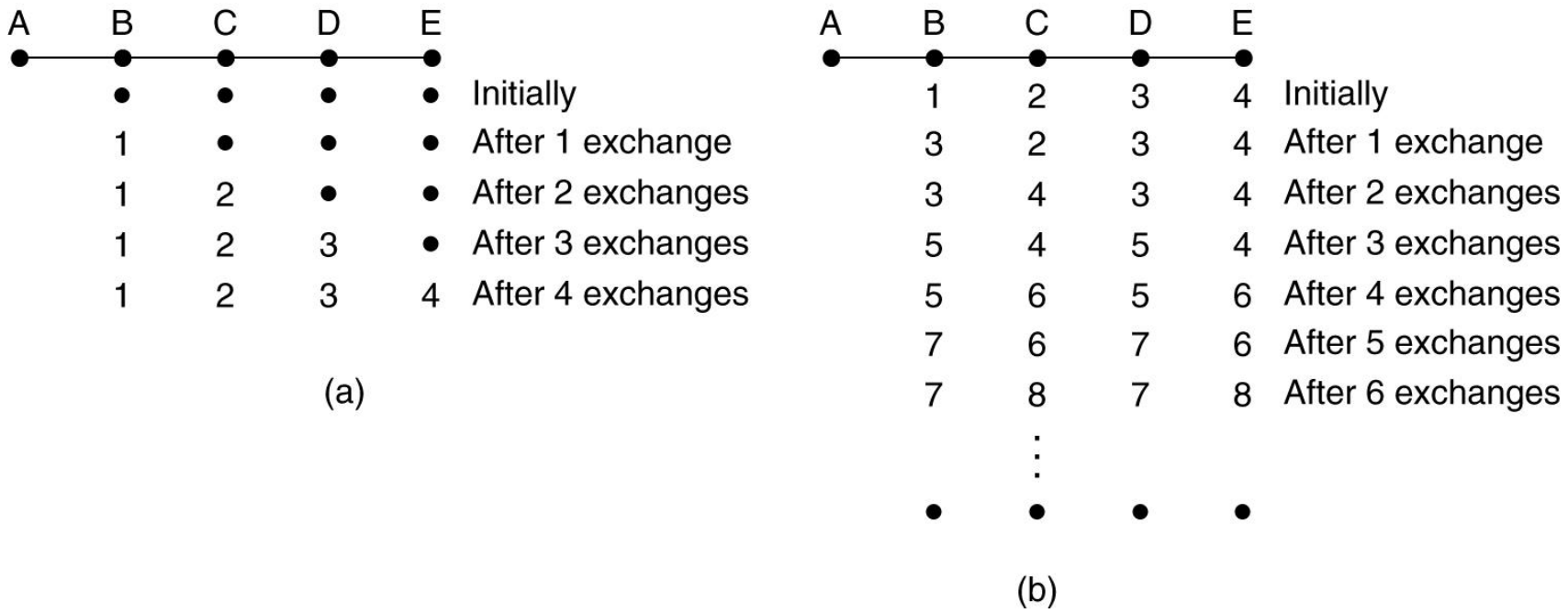


- Consider how J computes its new route to router G. It knows that it can get to A in 8 ms, and A claims to be able to get to G in 18 ms, so J knows it can count on a delay of 26 ms to G if it forwards packets bound for G to A.
- Similarly, it computes the delay to G via I, H, and K as 41 (31 + 10), 18 (6 + 12), and 37 (31 + 6) ms, respectively.
- The best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 ms and that the route to use is via H. The same calculation is performed for all the other destinations, with the new routing table shown in the last column of the figure.

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	New routing table for J	

Vectors received from J's four neighbors

Distance Vector Routing



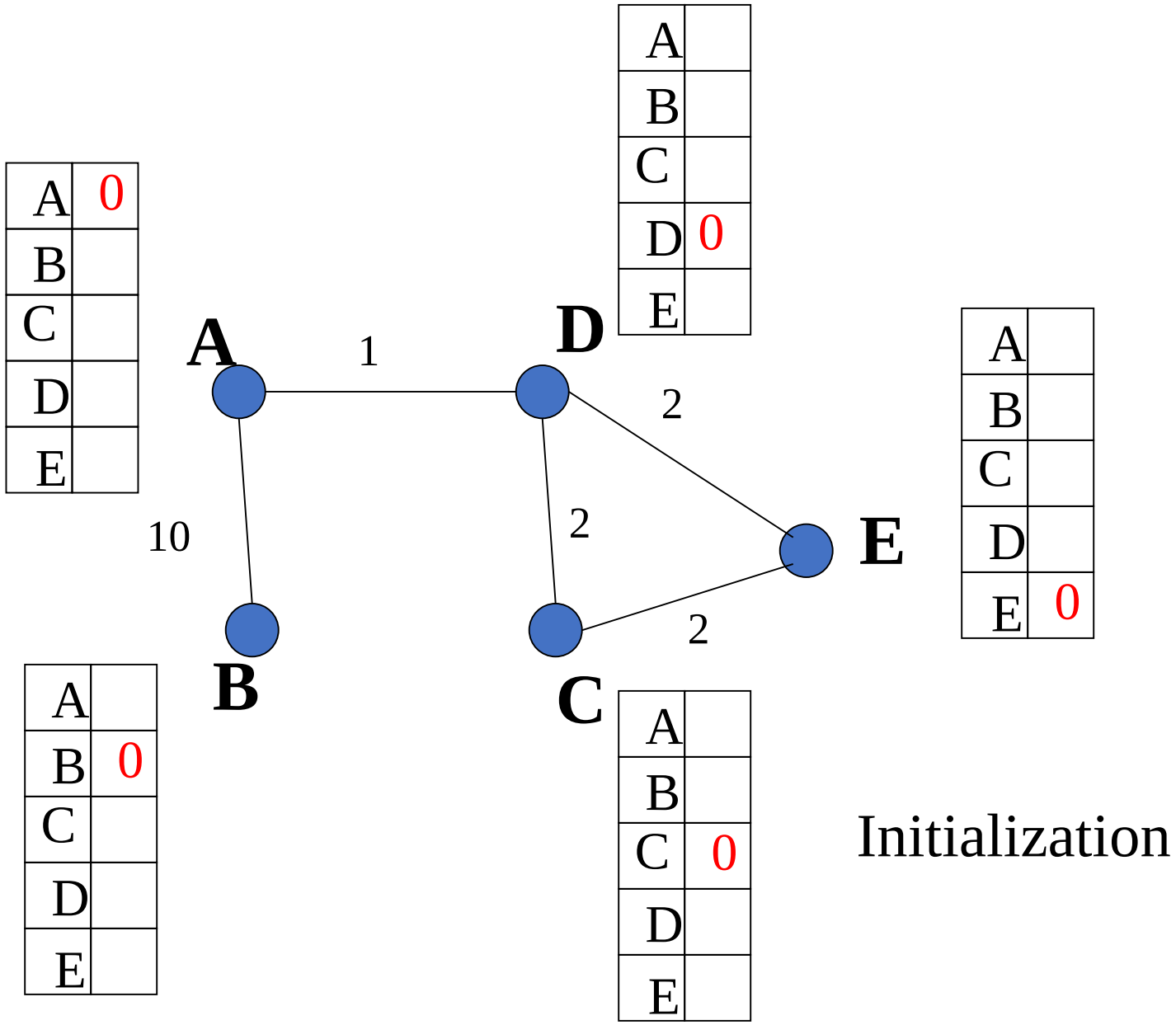
The count-to-infinity problem.

Distance Vector Routing

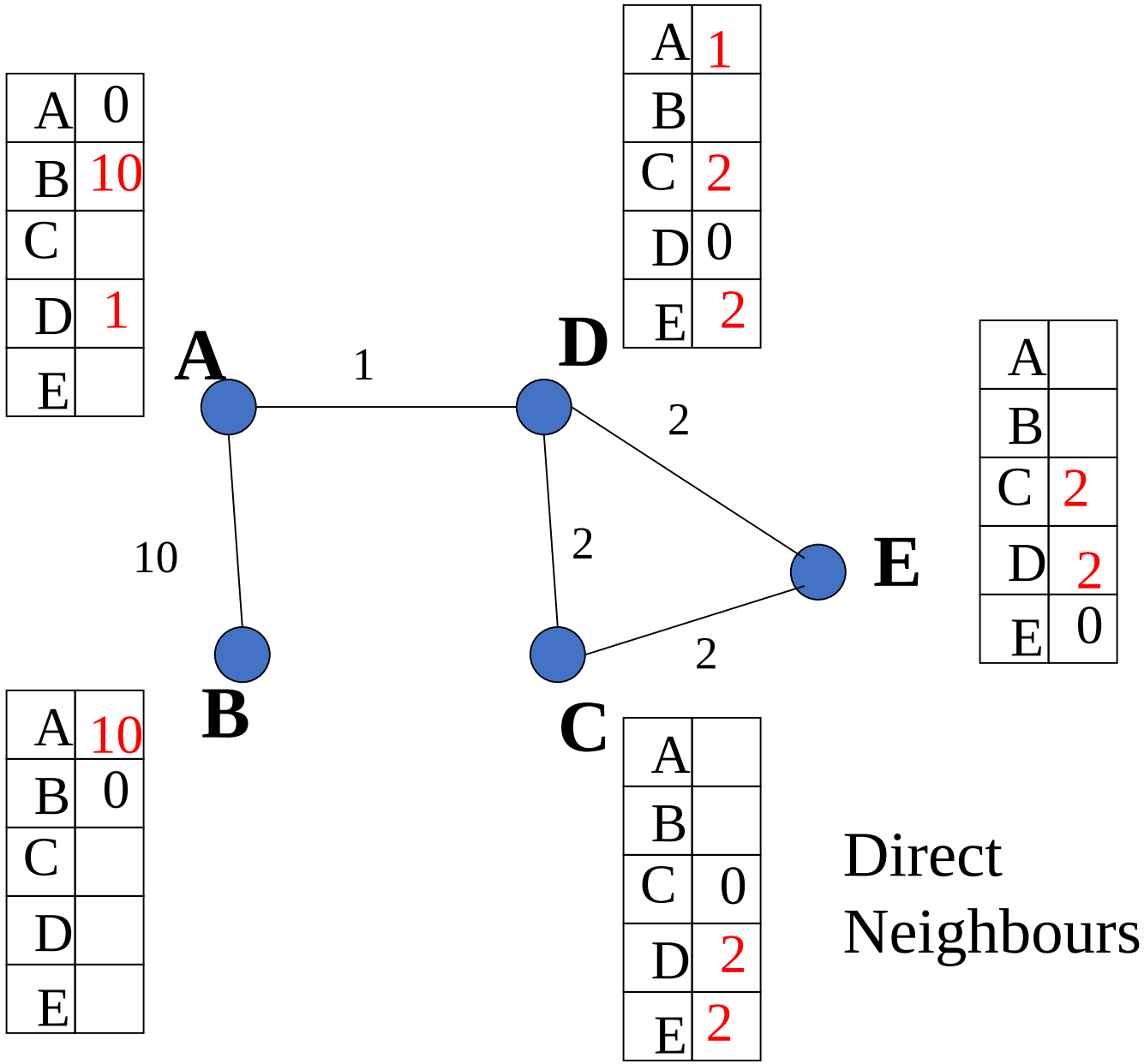
Loop-Breaking Heuristics

- Set infinity to a limited number, e.g. 16.
- Split horizon
- Split horizon with poison reverse

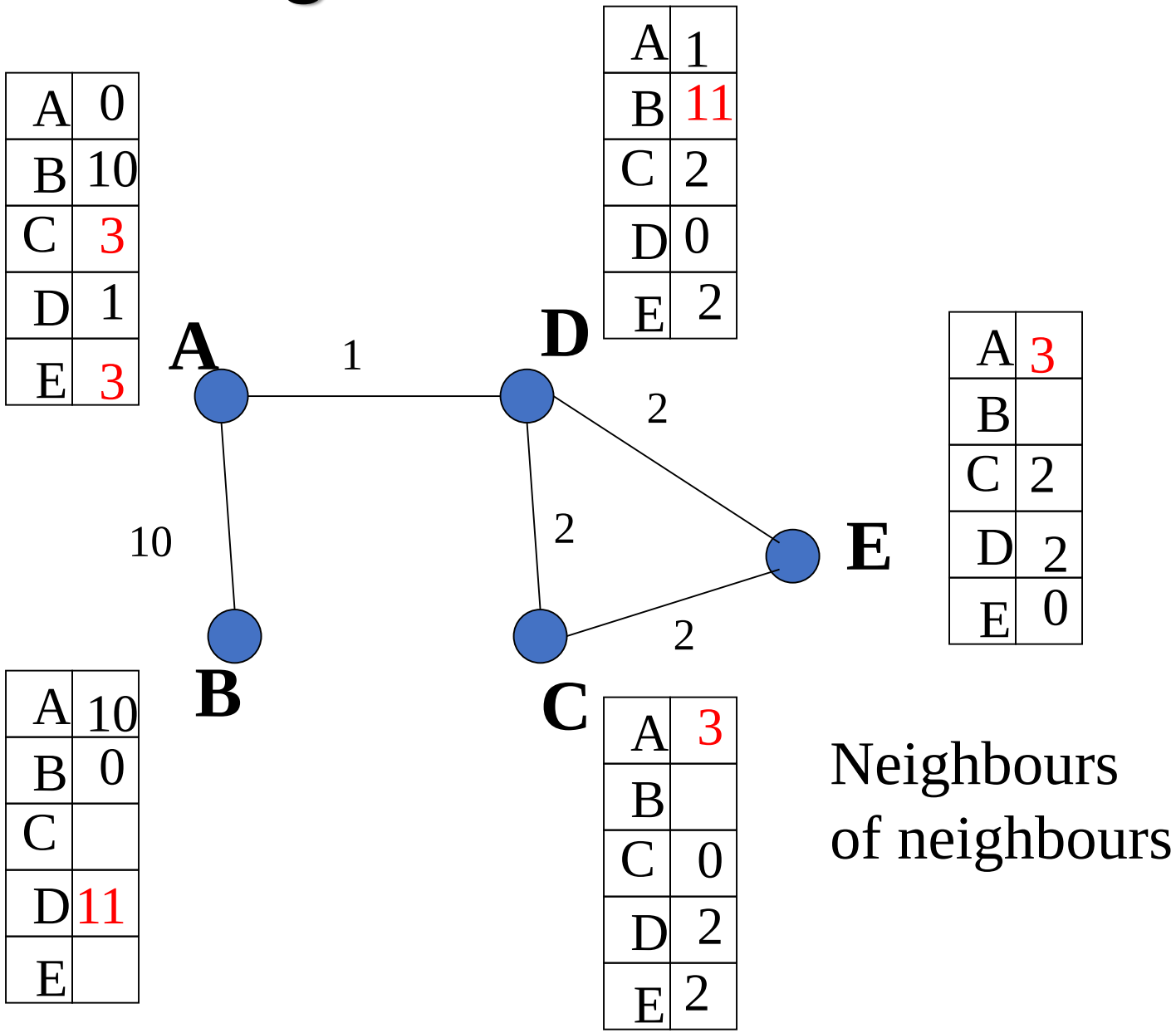
Distance Vector Routing - Example



Distance Vector Routing

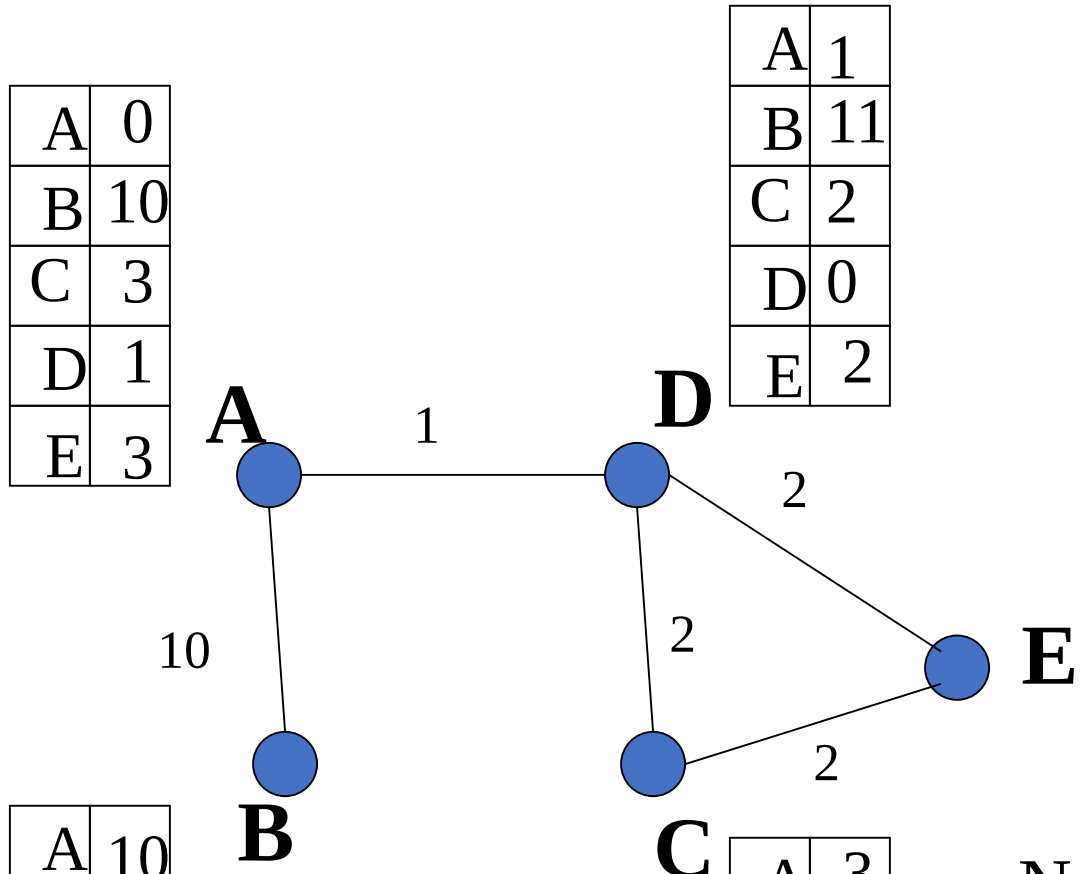


Distance Vector Routing



Neighbours of neighbours

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

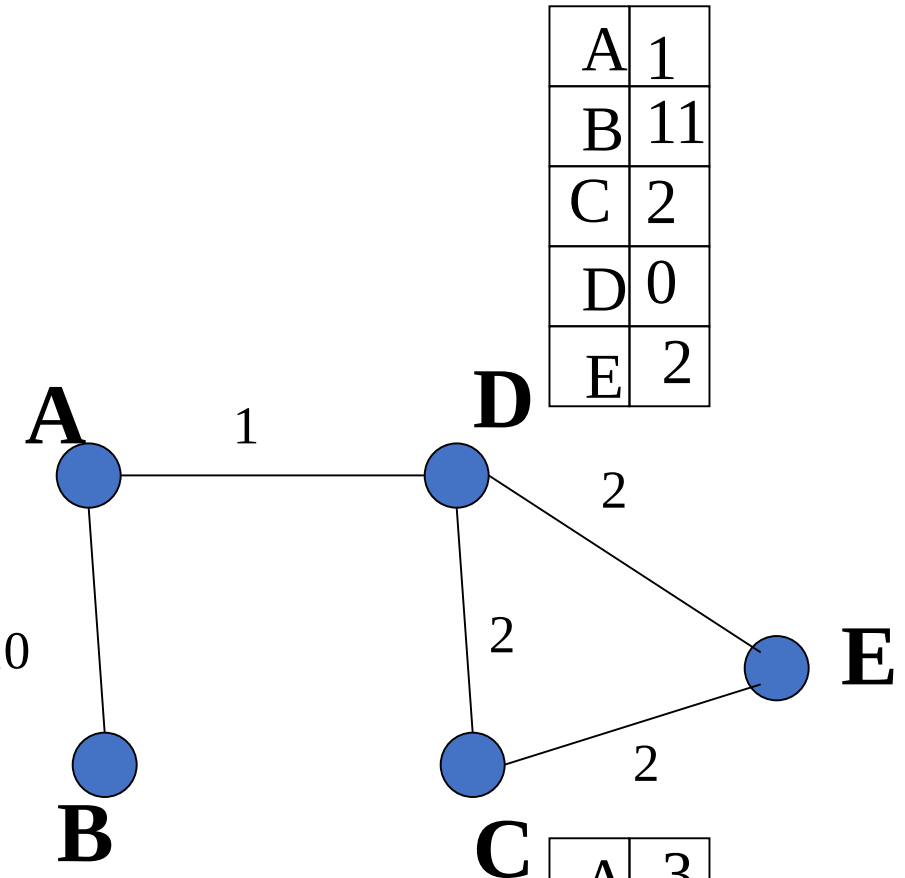
A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Neighbours
of neighbours
of neighbours

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

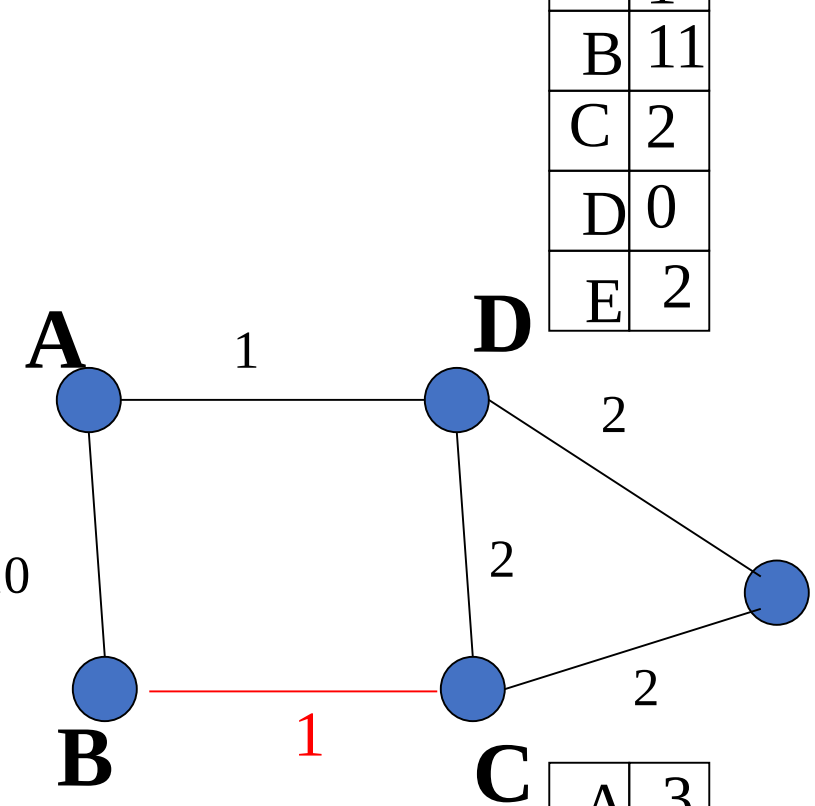
A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Stable convergence

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

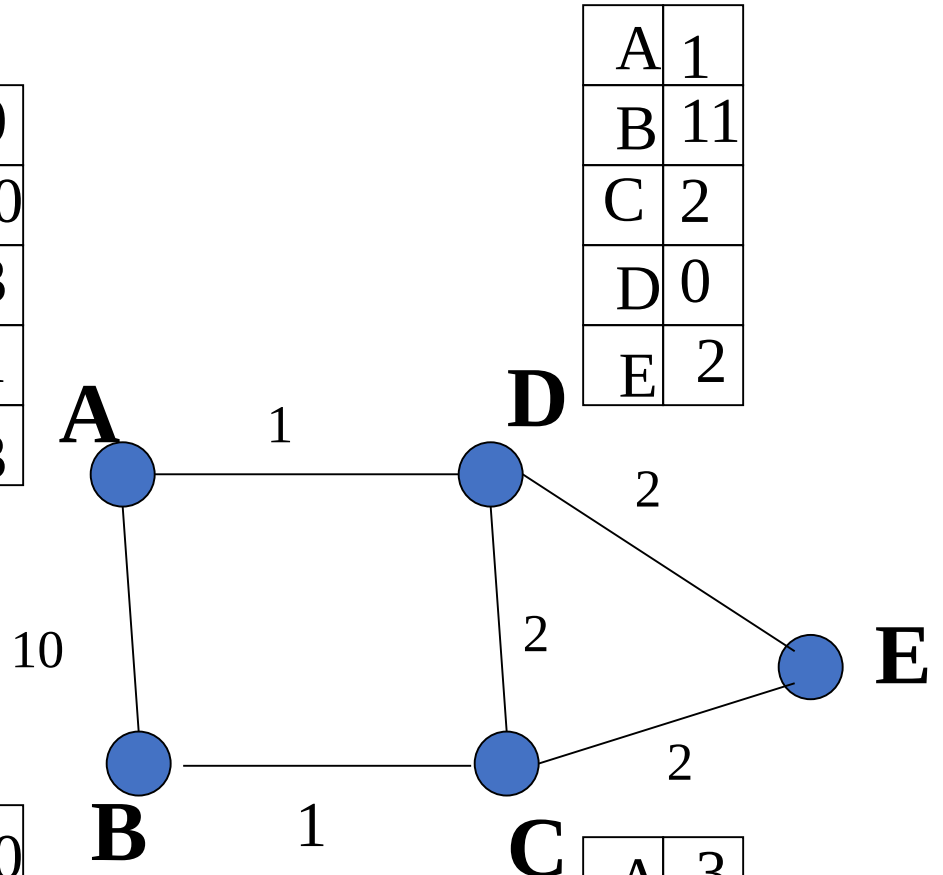
A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Good news:
A new link!

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

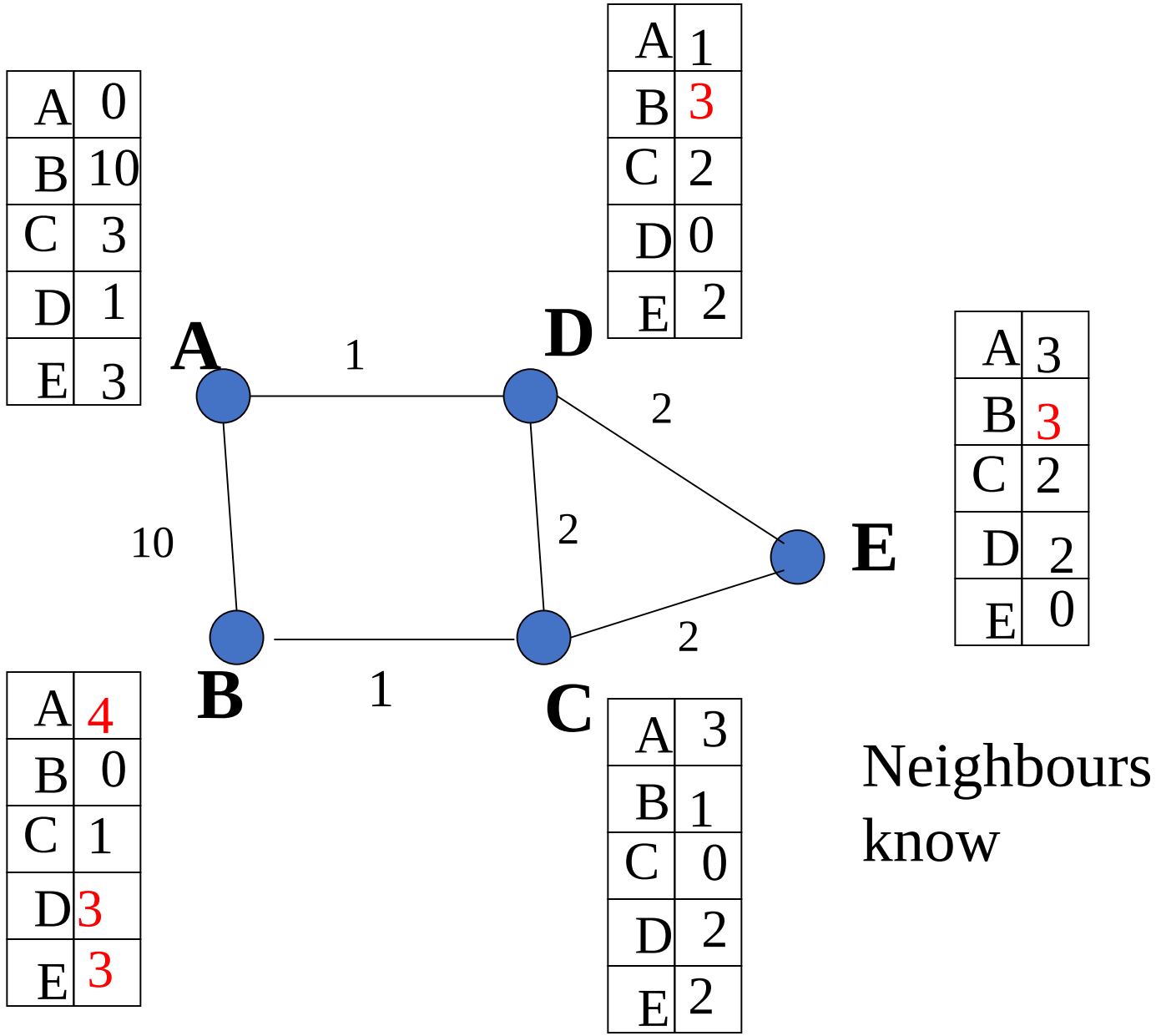
A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	1
D	11
E	13

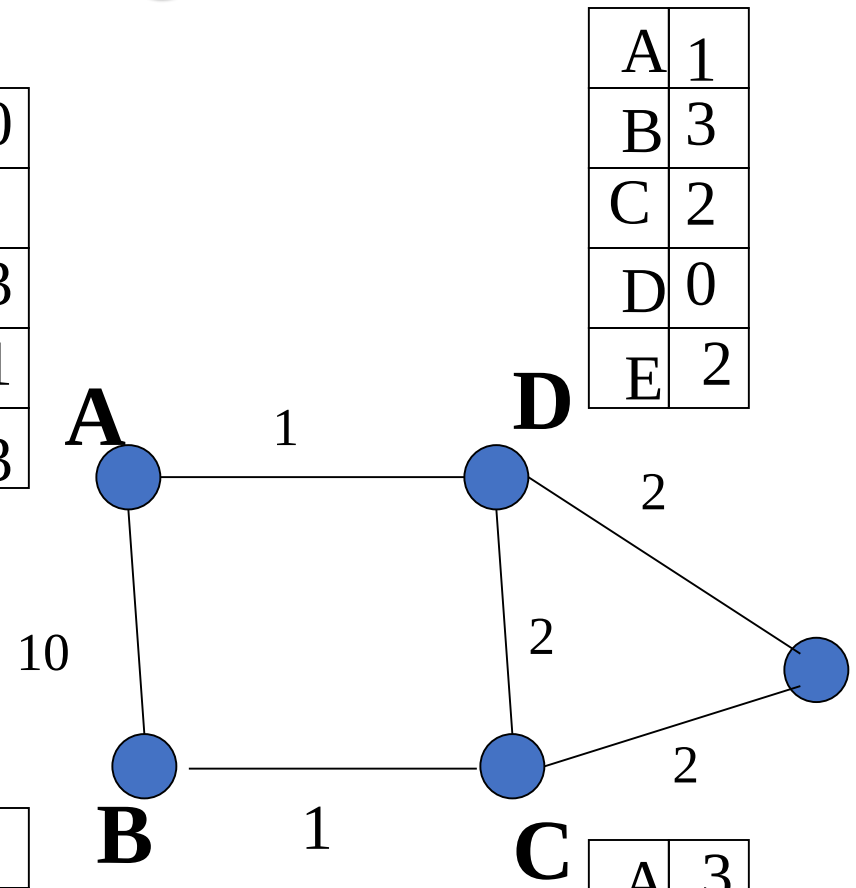
A	3
B	1
C	0
D	2
E	2

Direct endpoints know

Distance Vector Routing



Distance Vector Routing



A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2

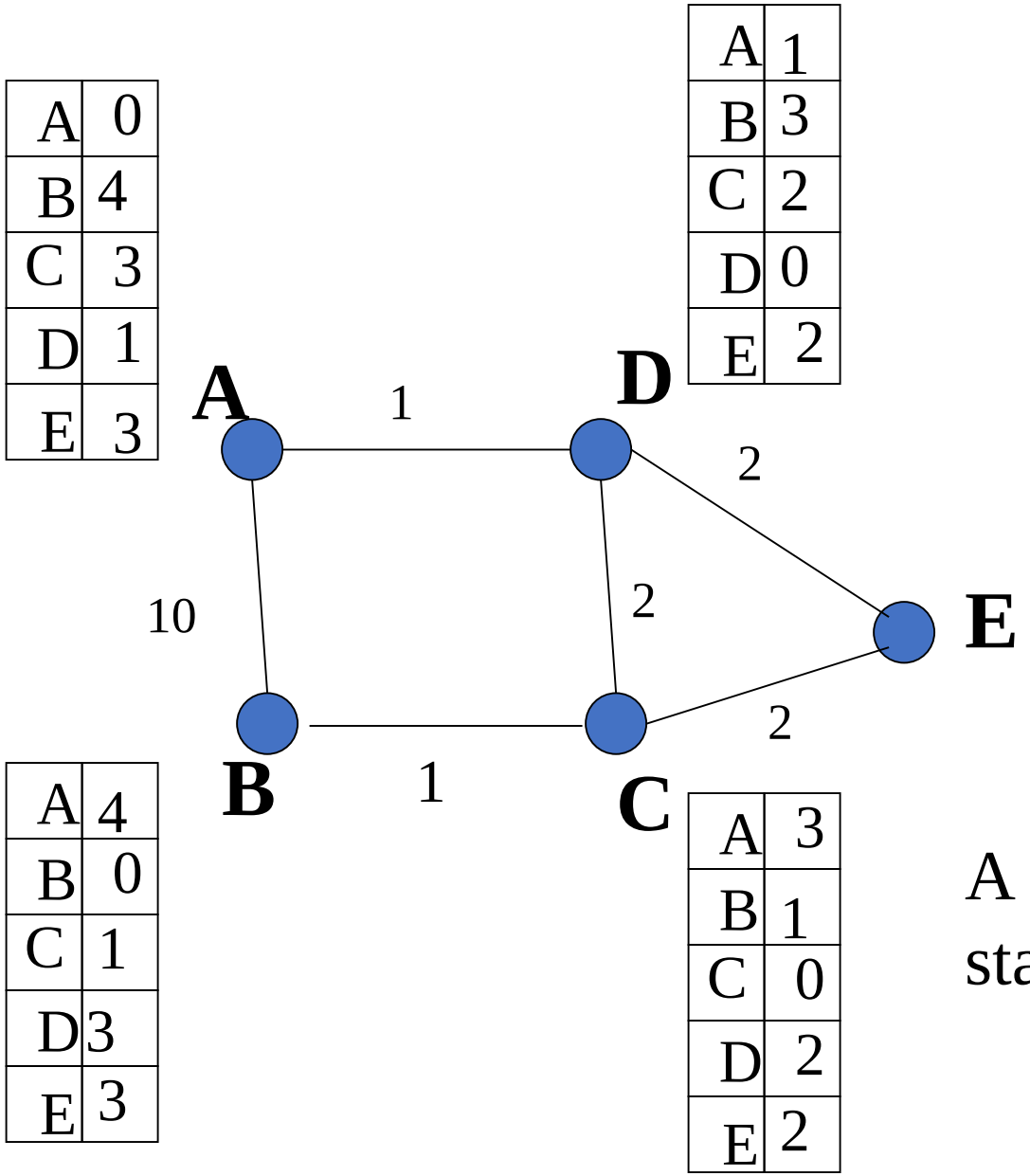
A	3
B	3
C	2
D	2
E	0

A	4
B	0
C	1
D	3
E	3

A	3
B	1
C	0
D	2
E	2

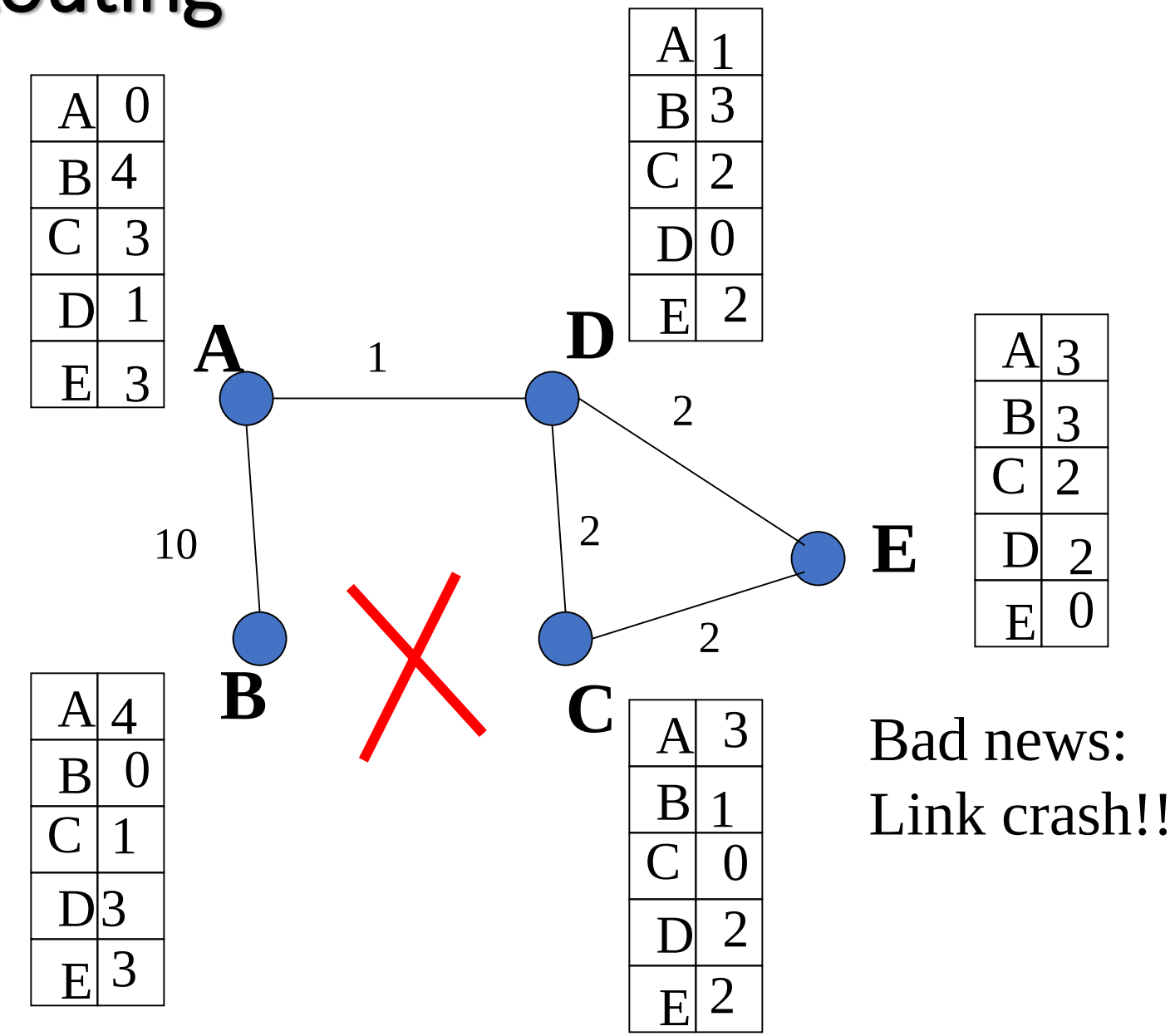
Neighbours of neighbours know

Distance Vector Routing



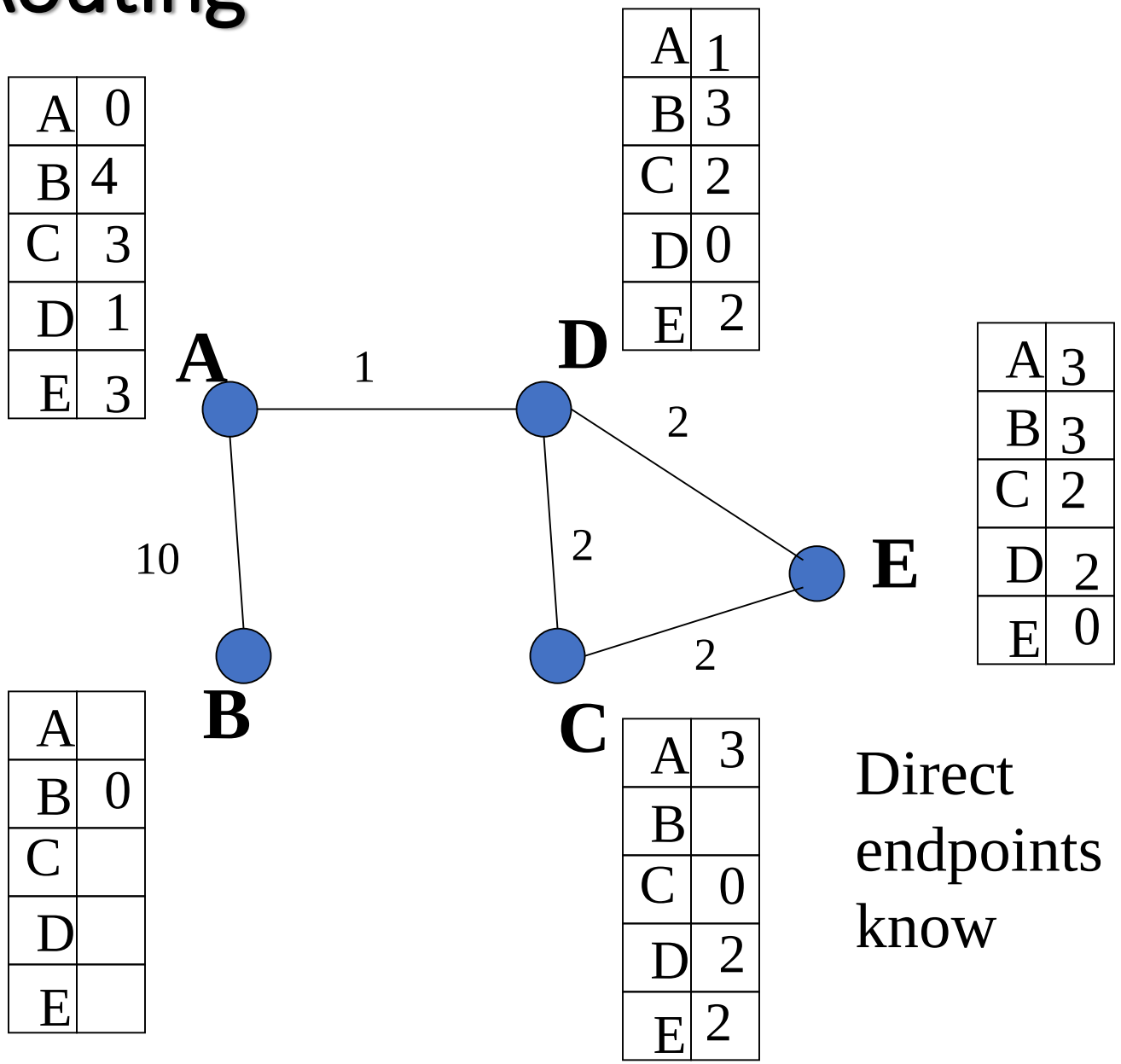
A happy and stable network

Distance Vector Routing



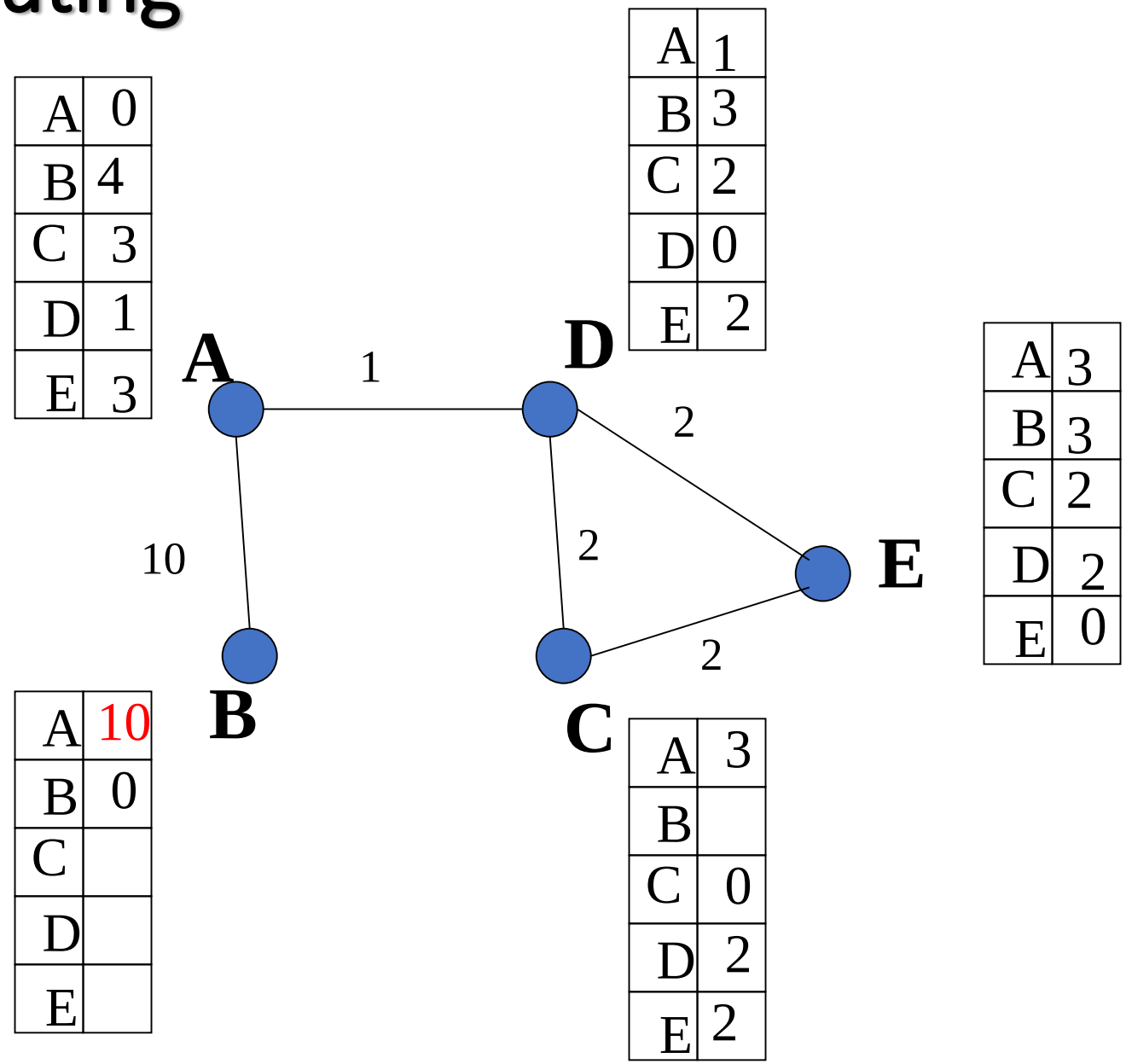
Bad news:
Link crash!!

Distance Vector Routing



Direct endpoints know

Distance Vector Routing



A	0
B	4
C	3
D	1
E	3

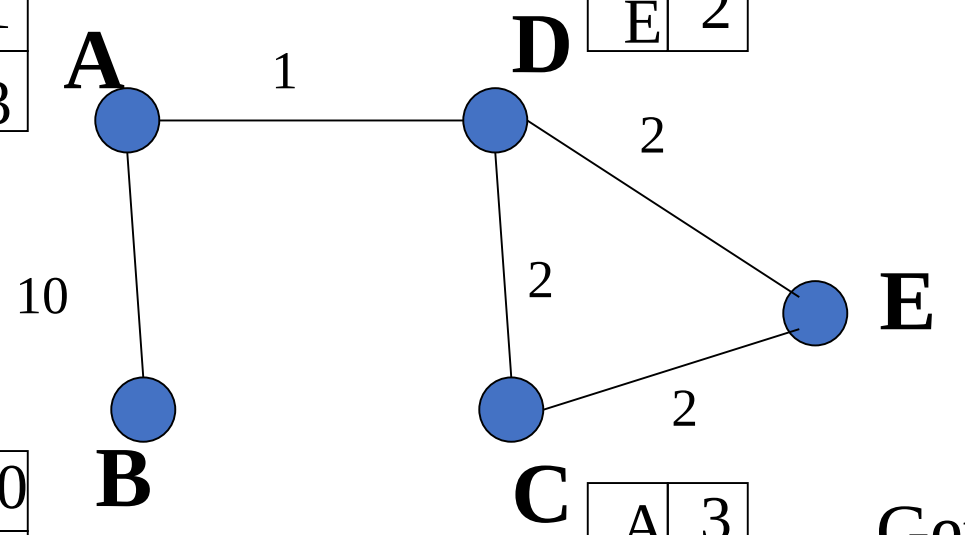
A	1
B	3
C	2
D	0
E	2

A	3
B	3
C	2
D	2
E	0

A	10
B	0
C	
D	
E	

A	3
B	
C	0
D	2
E	2

Distance Vector Routing



A	0
B	4
C	3
D	1
E	3

A	1
B	3
C	2
D	0
E	2

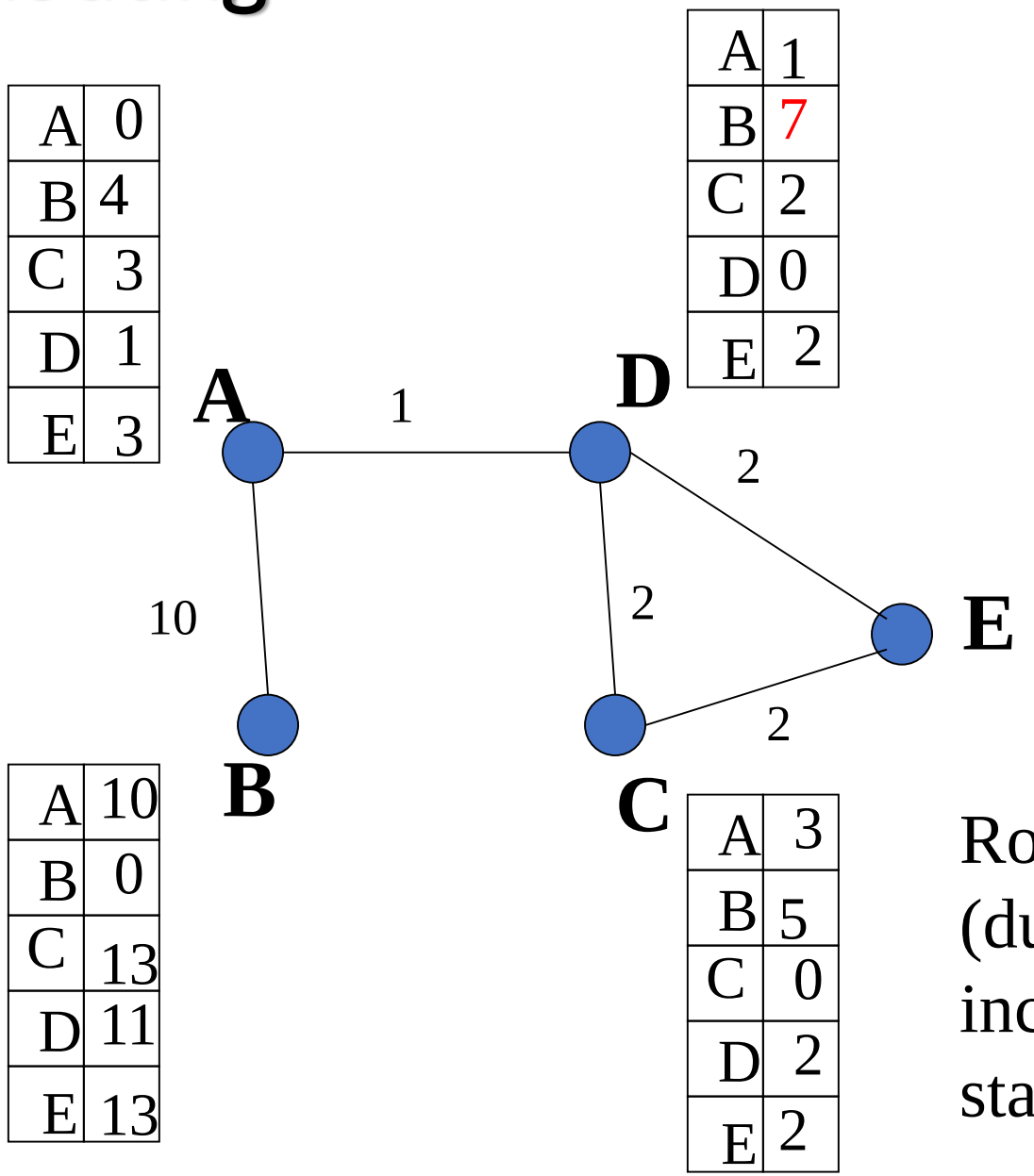
A	3
B	3
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	5
C	0
D	2
E	2

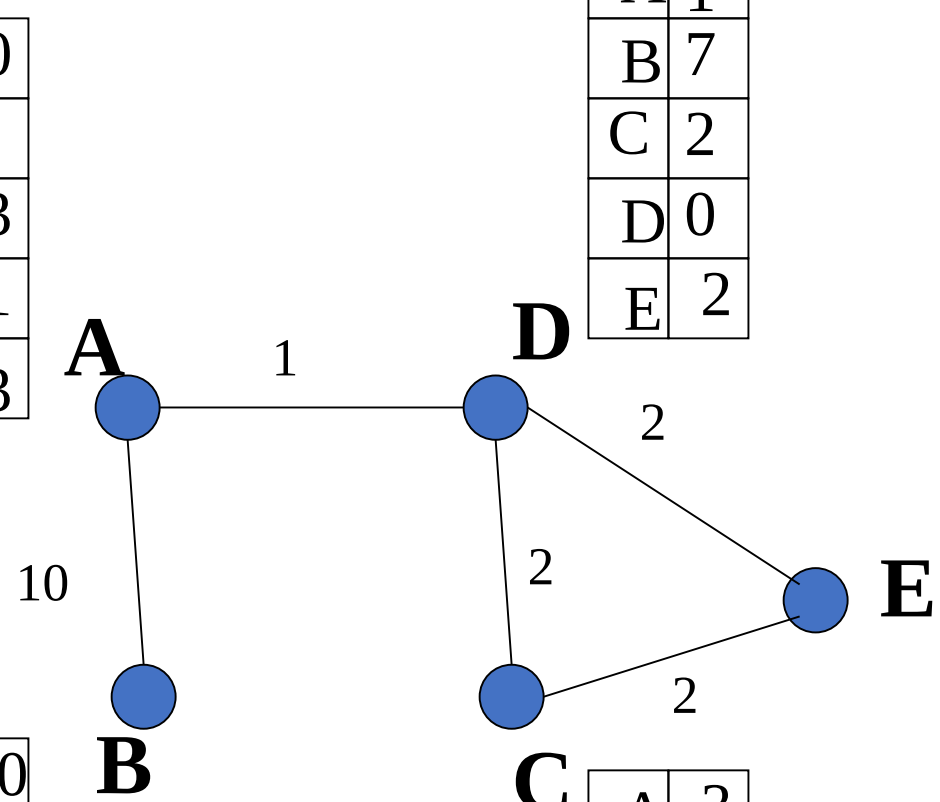
Get help from neighbours

Distance Vector Routing



Routing loop (due to inconsistent state info)

Distance Vector Routing



A	0
B	8
C	3
D	1
E	3

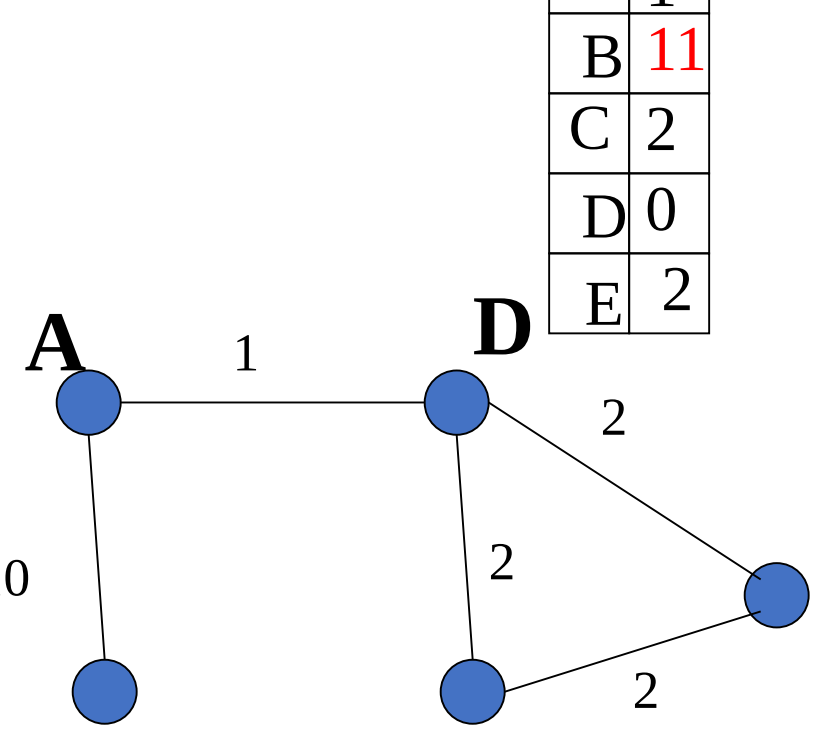
A	1
B	7
C	2
D	0
E	2

A	3
B	7
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	9
C	0
D	2
E	2

Distance Vector Routing



A	0
B	8
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

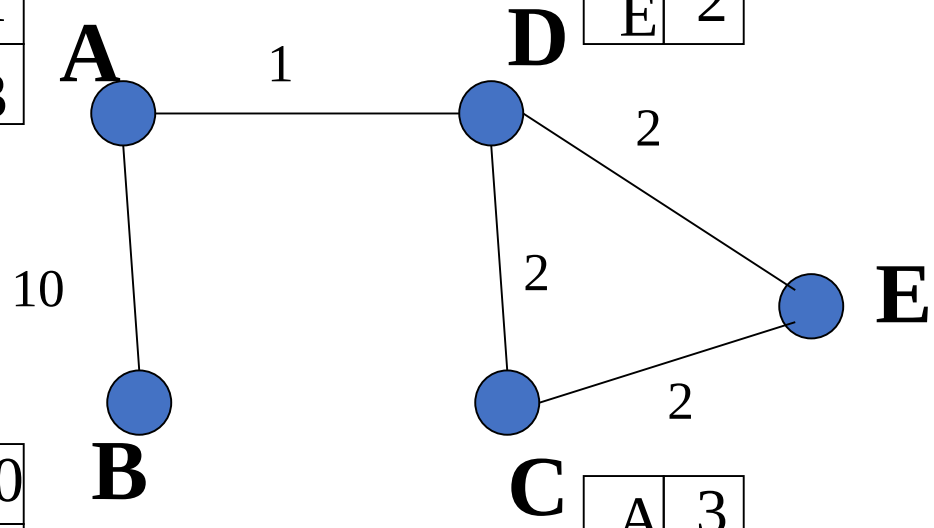
A	3
B	11
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	9
C	0
D	2
E	2

Counting to infinity…

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

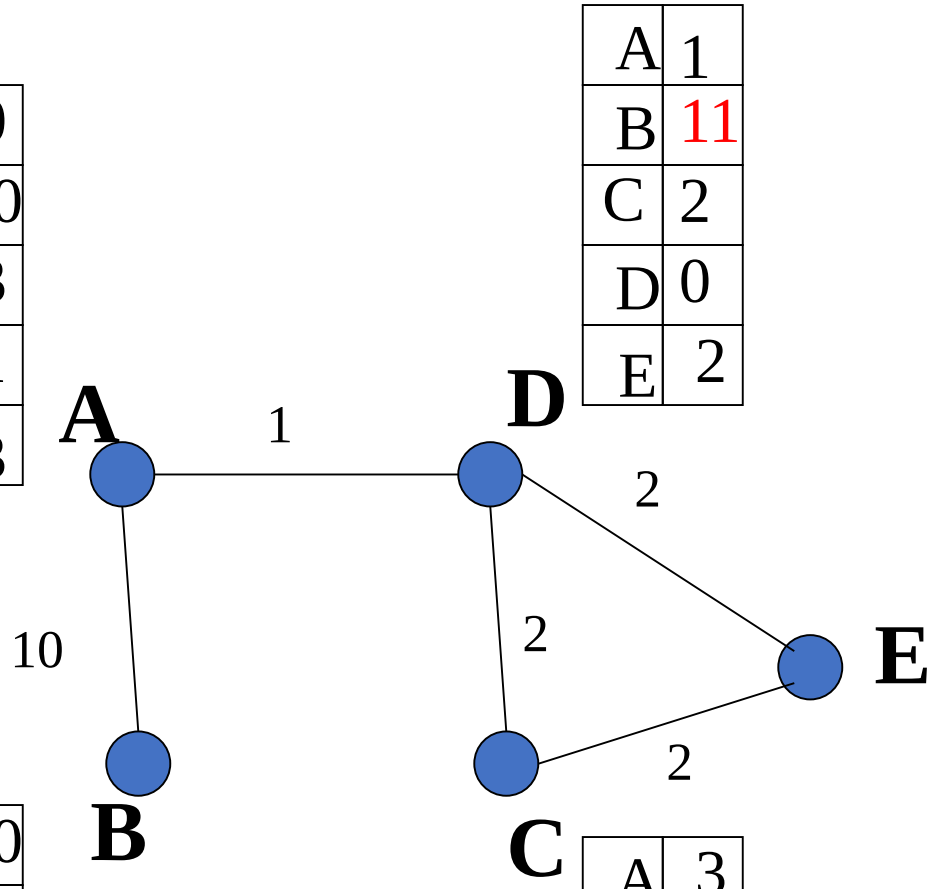
A	1
B	11
C	2
D	0
E	2

A	3
B	11
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

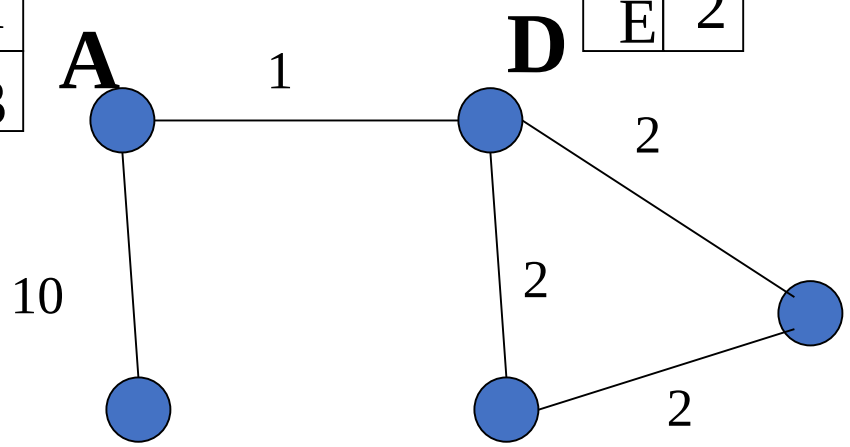
A	1
B	11
C	2
D	0
E	2

A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Distance Vector Routing



A	0
B	10
C	3
D	1
E	3

A	1
B	11
C	2
D	0
E	2

A	3
B	13
C	2
D	2
E	0

A	10
B	0
C	13
D	11
E	13

A	3
B	13
C	0
D	2
E	2

Stability again

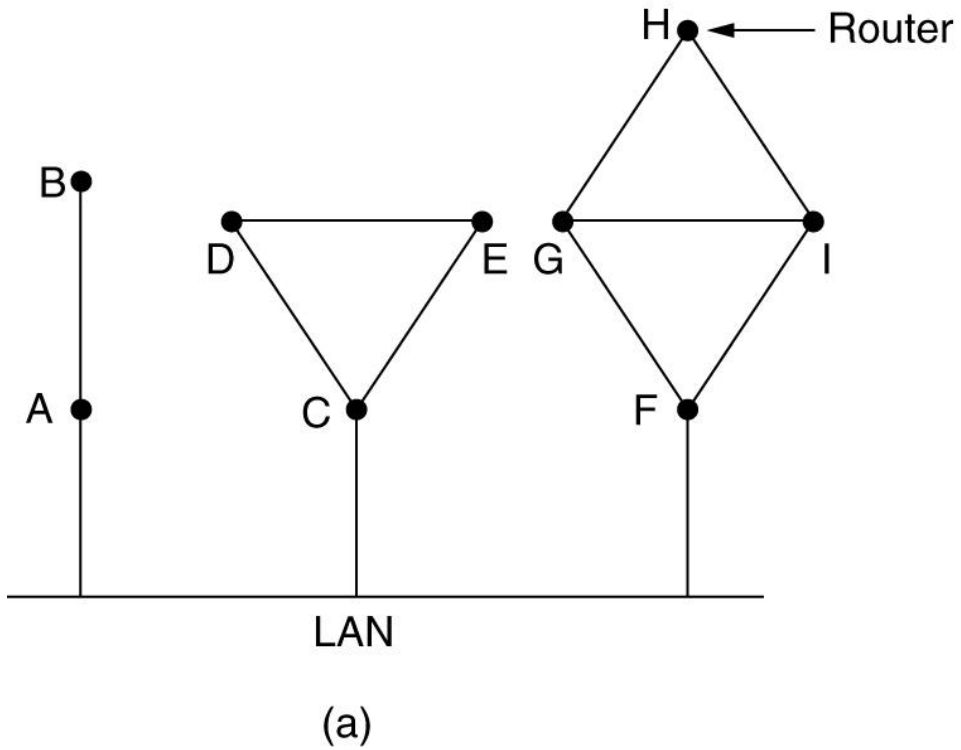
Link State Routing

Each router must do the following:

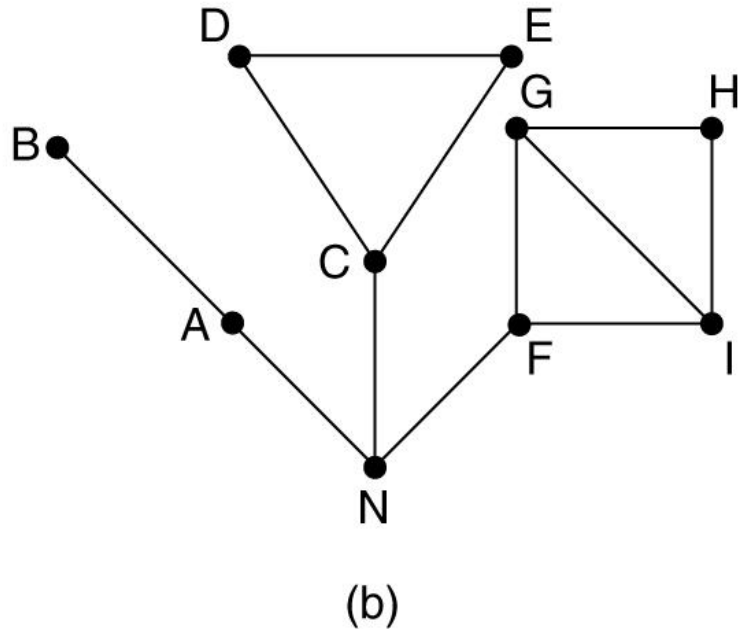
- Discover its neighbors, learn their network address.
- Measure the delay or cost to each of its neighbors.
- Construct a packet telling all it has just learned.
- Send this packet to all other routers.
- Compute the shortest path to every other router.

Link State Routing

Learning about the Neighbors



(a) Nine routers and a LAN.

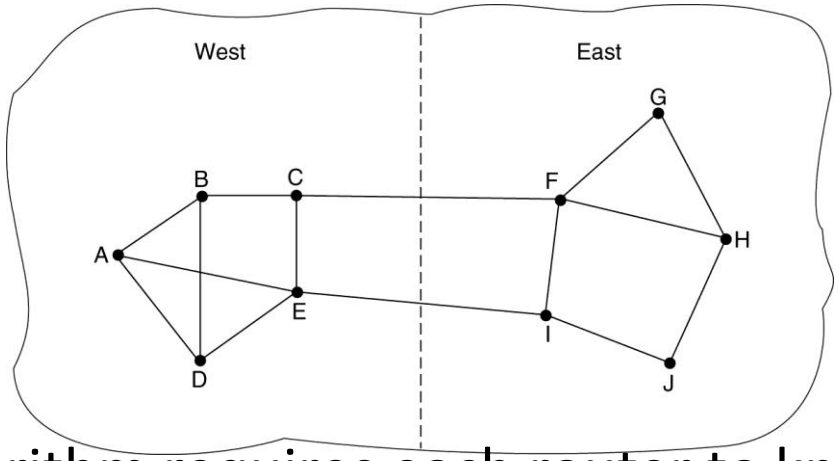


(b) A graph model of (a).

Link State Routing

Measuring Line Cost

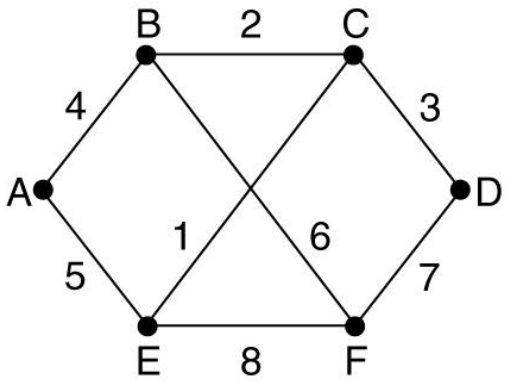
- A subnet in which the East and West parts are connected by two lines.



- The link state routing algorithm requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors.
- The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.
- By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.

Link State Routing

Building Link State Packets



(a)

(a) A subnet.

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

(b)

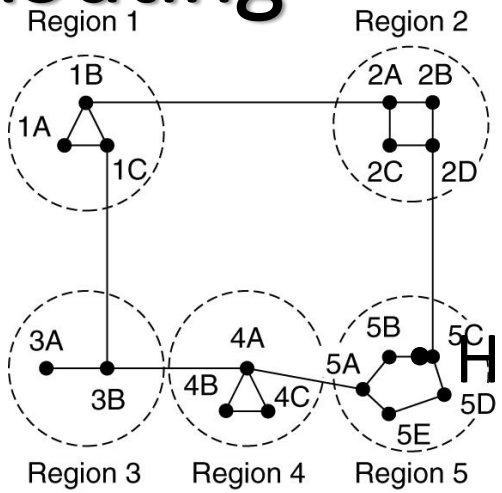
(b) The link state packets for this subnet.

Distributing the Link State Packets

- The packet buffer for router B in the previous slide.

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	

Hierarchical Routing



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Hierarchical routing.

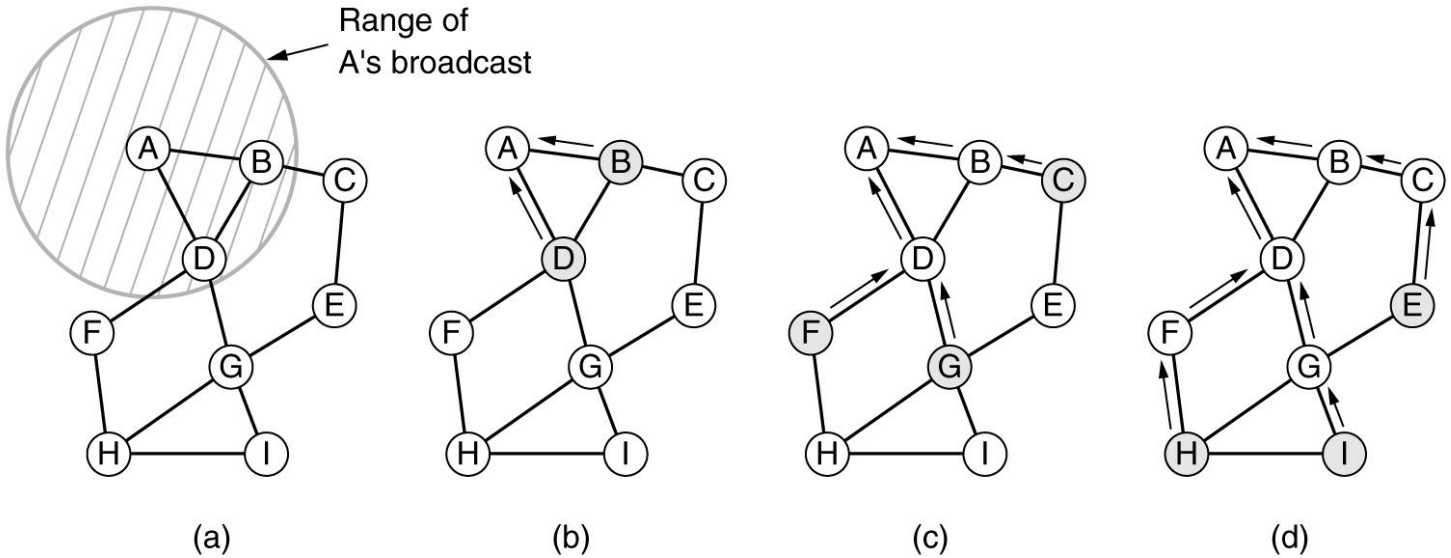
- At a certain point the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically, as it is in the telephone network.
- When hierarchical routing is used, the routers are divided into what we will call regions, with each router knowing all the details about how to route packets to destinations within its own region, but knowing nothing about the internal structure of other regions.
- When different networks are interconnected, it is natural to regard each one as a separate region in order to free the routers in one network from having to know the topological structure of the other ones.

Routing in Ad Hoc Networks

- Possibilities when the routers are mobile:
- Military vehicles on battlefield.
  - No infrastructure.
- A fleet of ships at sea.
  - All moving all the time
- Emergency works at earthquake .
  - The infrastructure destroyed.
- A gathering of people with notebook computers.
  - In an area lacking 802.11.

Routing in Ad Hoc Networks

Route Discovery



- (a) Range of A's broadcast.
- (b) After B and D have received A's broadcast.
- (c) After C, F, and G have received A's broadcast.
- (d) After E, H, and I have received A's broadcast.
- Shaded nodes are new recipients. Arrows show possible reverse routes.

Routing in Ad Hoc Networks

Route Discovery

Source address	Request ID	Destination address	Source sequence #	Dest. sequence #	Hop count

- Format of a ROUTE REQUEST packet.

Routing in Ad Hoc Networks

Route Discovery

Source address	Destination address	Destination sequence #	Hop count	Lifetime

- Format of a ROUTE REPLY packet.

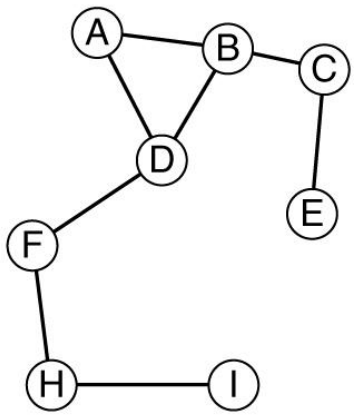
Routing in Ad Hoc Networks

Route Maintenance

- (a) D's routing table before G goes down.
- (b) The graph after G has gone down.

Dest.	Next hop	Distance	Active neighbors	Other fields
A	A	1	F, G	
B	B	1	F, G	
C	B	2	F	
E	G	2		
F	F	1	A, B	
G	G	1	A, B	
H	F	2	A, B	
I	G	2	A, B	

(a)



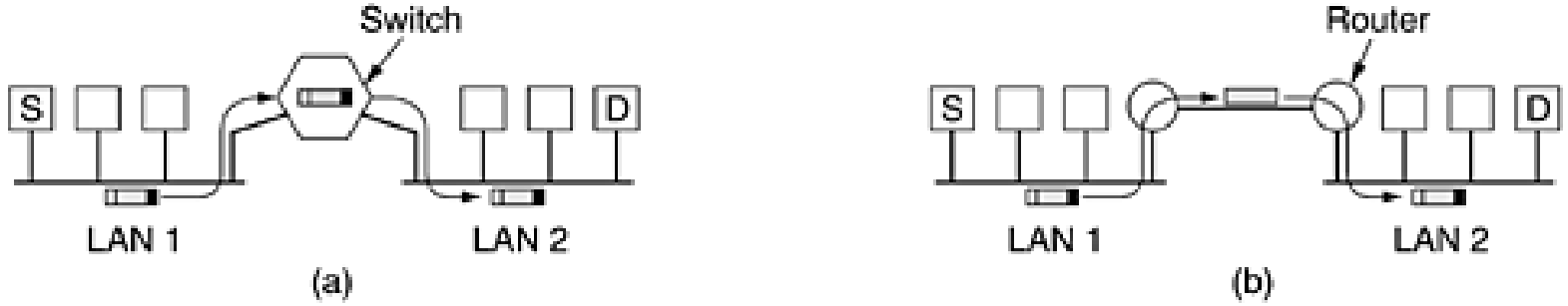
(b)

Internet Routing Protocols

Sub Module Summary

- The IP Protocol
- IP Addresses
- Internet Control Protocols (ICMP, ARP, RARP, BOOTP, and DHCP)
- Intra-Autonomous System Routing: RIP and OSPF
- Inter-Autonomous System Routing: BGP

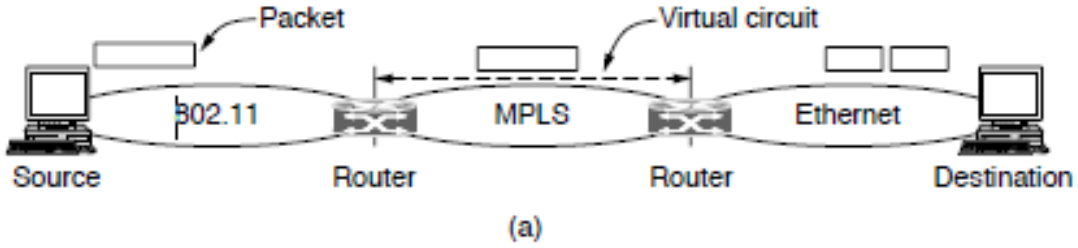
When Networks are connected – Example 1



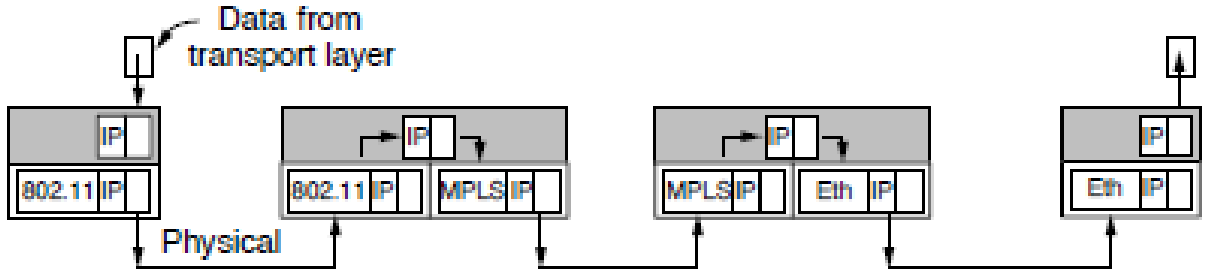
- In Fig. (a), the source machine, S, wants to send a packet to the destination machine, D. These machines are on different Ethernets, connected by a switch. S encapsulates the packet in a frame and sends it on its way. The frame arrives at the switch, which then determines that the frame has to go to LAN 2 by looking at its MAC address. The switch just removes the frame from LAN 1 and deposits it on LAN 2.

- Consider the same situation (b) but with the two Ethernets connected by a pair of routers instead of a switch. The routers are connected by a point-to-point line, possibly a leased line thousands of kilometers long. Now the frame is picked up by the router and the packet removed from the frame's data field. The router examines the address in the packet (e.g., an IP address) and looks up this address in its routing table. Based on this address, it decides to send the packet to the remote router, potentially encapsulated in a different kind of frame, depending on the line protocol. At the far end, the packet is put into the data field of an Ethernet frame and deposited onto LAN 2.

When Networks are connected - Example 2



(a)

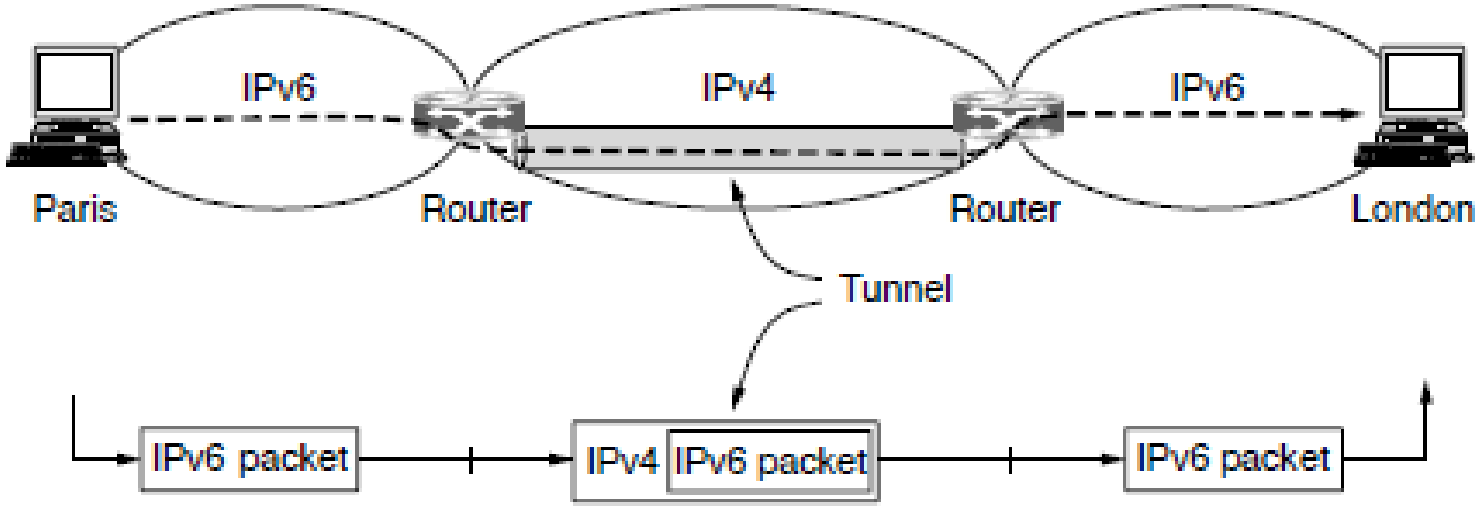


(b)

- An internet comprised of 802.11, MPLS, and Ethernet networks is shown in Fig. (a). Suppose that the source machine on the 802.11 network wants to send a packet to the destination machine on the Ethernet network. Since these technologies are different, and they are further separated by another kind of network (MPLS), some added processing is needed at the boundaries between the networks.

- Because different networks may, in general, have different forms of addressing, the packet carries a network layer address that can identify any host across the three networks. The first boundary the packet reaches is when it transitions from an 802.11 network to an MPLS network. Remember, 802.11 provides a connectionless service, but MPLS provides a connection-oriented service. This means that a virtual circuit must be set up to cross that network. Once the packet has traveled along the virtual circuit, it will reach the Ethernet network. At this boundary, the packet may be too large to be carried, since 802.11 can work with larger frames than Ethernet. To handle this problem, the packet is divided into fragments, and each fragment is sent separately. When the fragments reach the destination, they are reassembled. Then the packet has completed its journey.

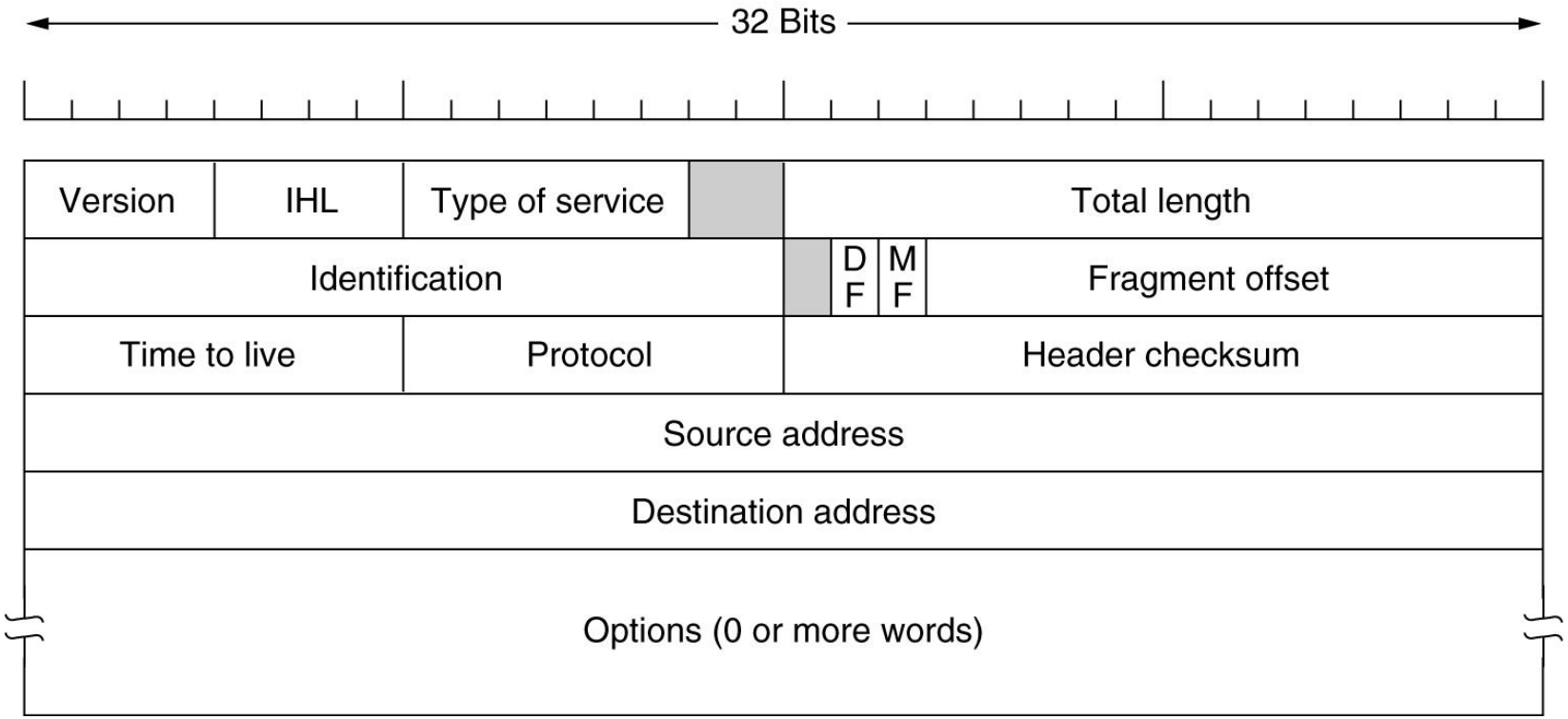
When Networks are connected - Example 3



- The solution to this problem is a technique called tunneling.
- To send an IP packet to a host in the London office, a host in the Paris office constructs the packet containing an IPv6 address in London, and sends it to the multiprotocol router that connects the Paris IPv6 network to the IPv4 Internet.
- When this router gets the IPv6 packet, it encapsulates the packet with an IPv4 header addressed to the IPv4 side of the multiprotocol router that connects to the London IPv6 network.
- That is, the router puts a (IPv6) packet inside a (IPv4) packet. When this wrapped packet arrives, the London router removes the original IPv6 packet and sends it onward to the destination host.

IP Protocol

- The IPv4 (Internet Protocol) header.

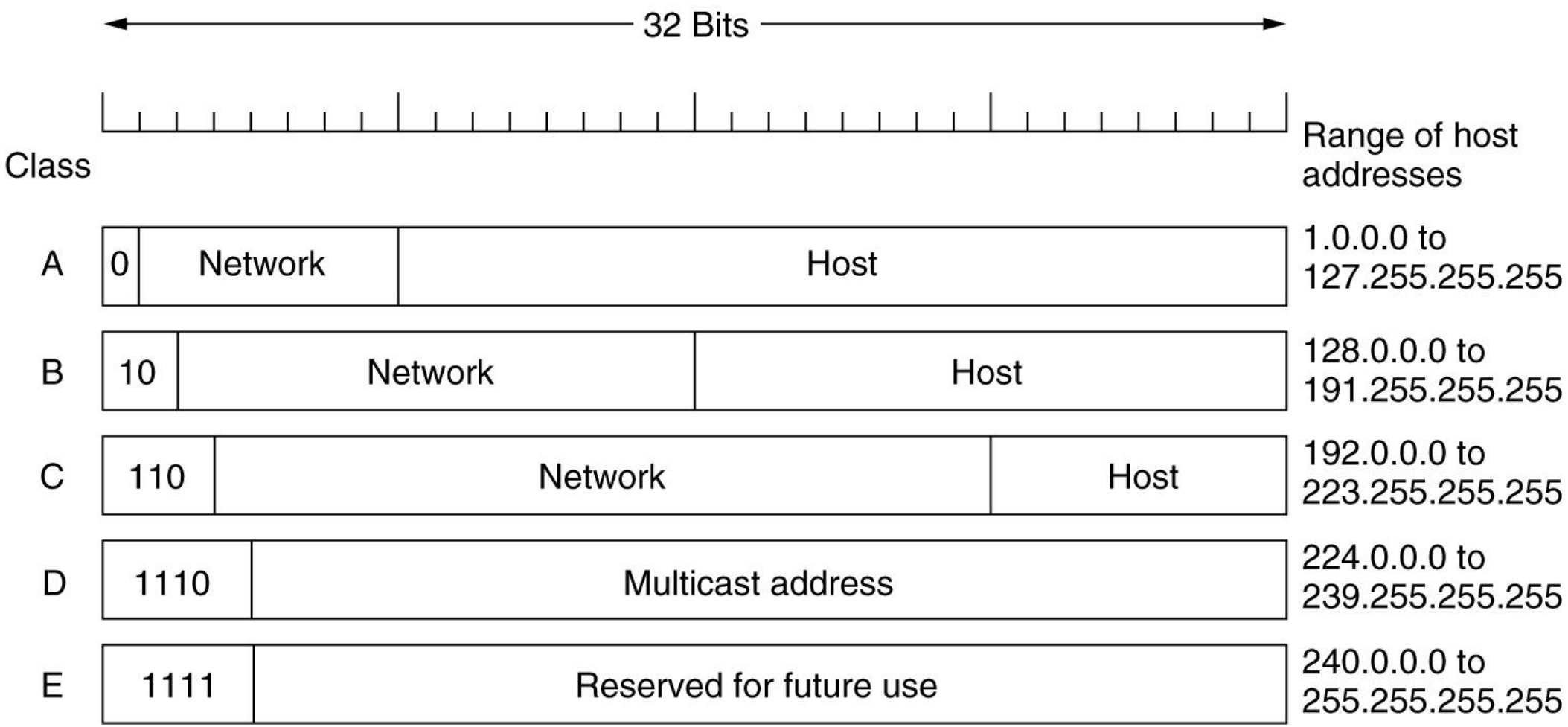


IP Protocol

- Some of the IP options.

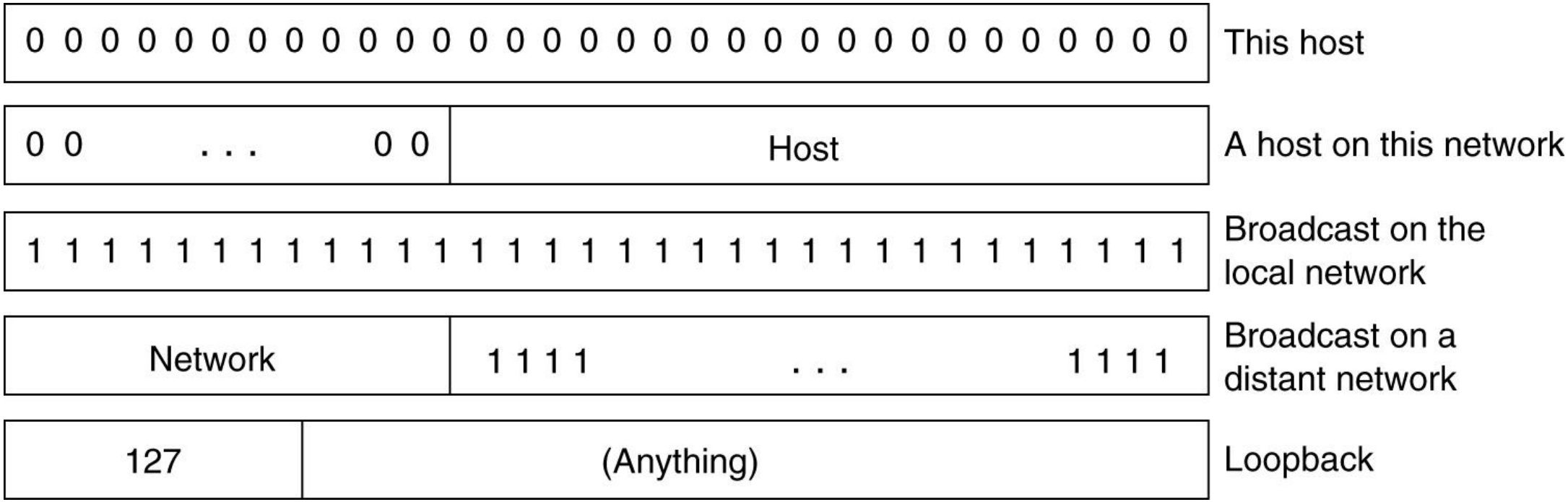
Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

IP Addresses



- IP address formats.

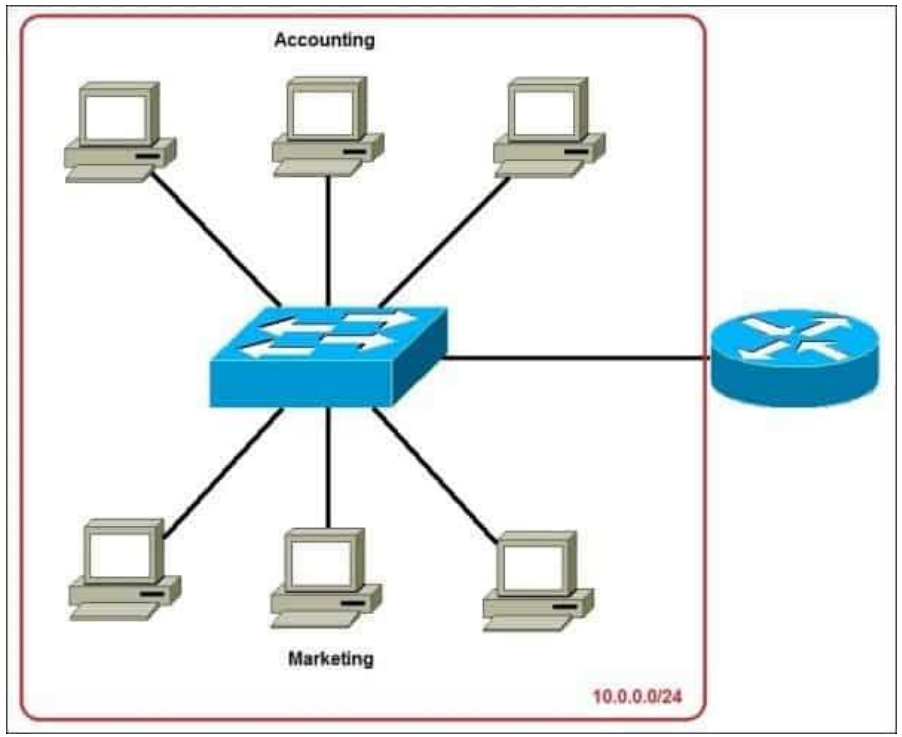
IP Addresses

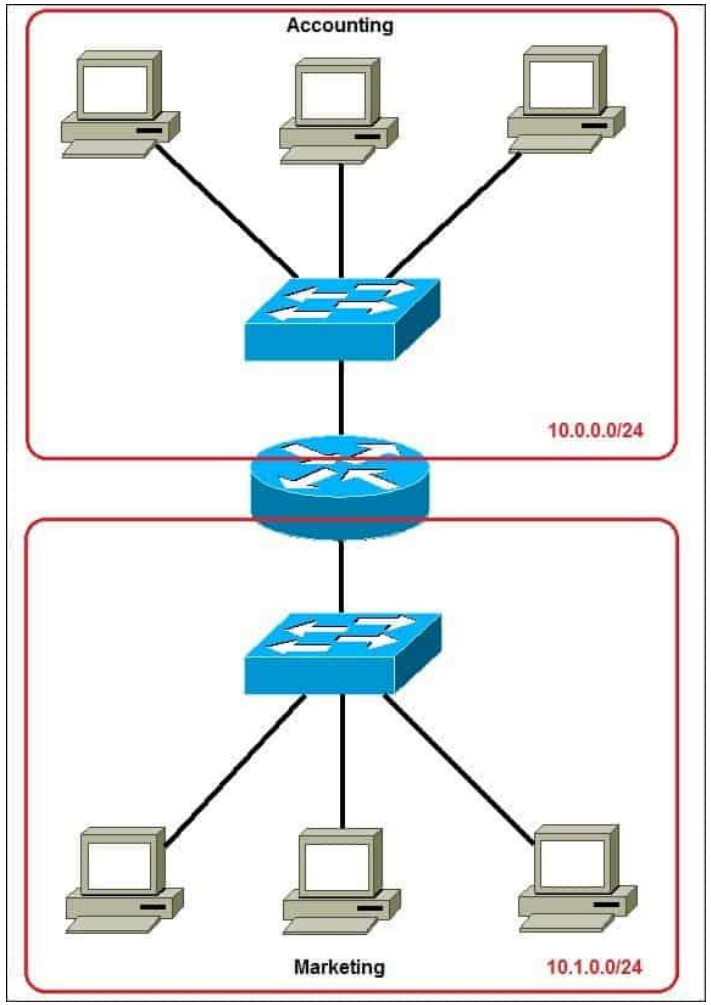


- Special IP addresses.

Subnets

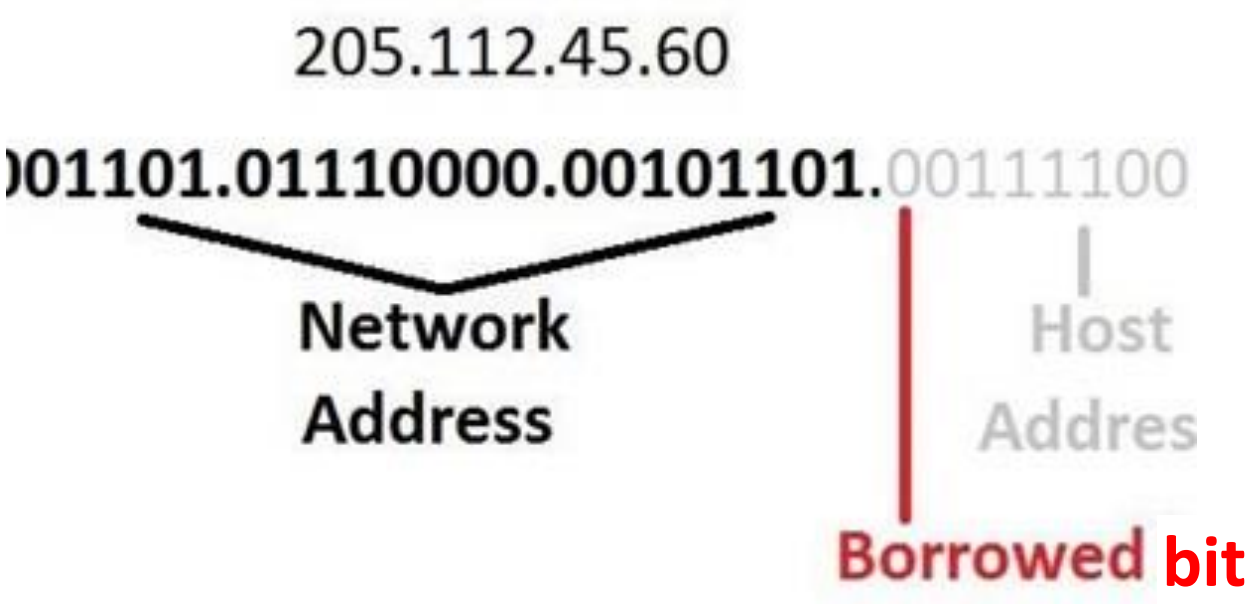
Subnets





- Subnetting is the practice of dividing a network into two or more smaller networks.
- It increases routing efficiency, enhances the security of the network, and reduces the size of the broadcast domain.

Subnets



- In the above diagram, there is a subnet mask for a Class C address. The subnet mask is 255.255.255.128 which, when translated into bits, indicates which bits of the host part of the address will be used to determine the subnet number.

- An example of an IP address with a borrowed bit pointed out

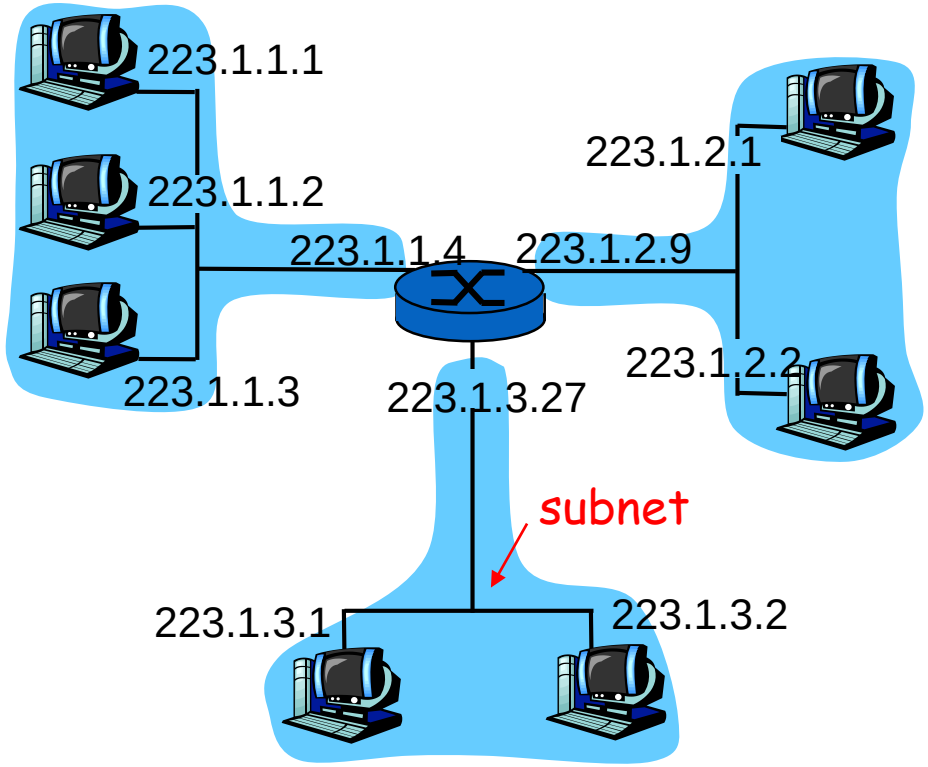
- More bits borrowed means fewer individually addressable hosts that can be on the network. Sometimes, all the combinations and permutations can be confusing, so here are some tables of subnet possibilities..

Subnets

Class bits	Subnet Mask	Effective Subnets	Effective Hosts	Number of Subnet Mask bits
1	255.255.128.0	2	32766	/17
2	255.255.192.0	4	16382	/18
3	255.255.224.0	8	8190	/19
4	255.255.240.0	16	4094	/20
5	255.255.248.0	32	2046	/21
6	255.255.252.0	64	1022	/22
7	255.255.254.0	128	510	/23
8	255.255.255.0	256	254	/24
9	255.255.255.128	512	126	/25
10	255.255.255.192	1024	62	/26
11	255.255.255.224	2048	30	/27
12	255.255.255.240	4096	14	/28
13	255.255.255.248	8192	6	/29
14	255.255.255.252	16384	2	/30
15	255.255.255.254	32768	2	/31

Subnets

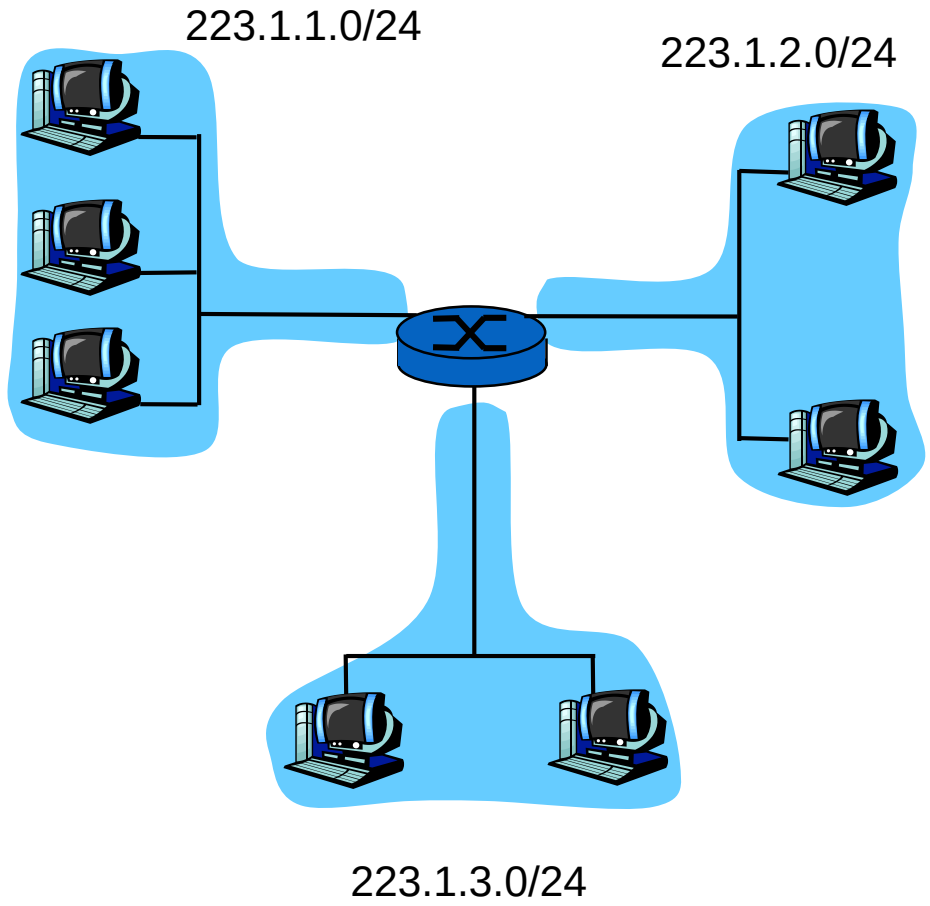
- IP address:
  - subnet part (high order bits)
  - host part (low order bits)
- *What's a subnet ?*
  - device interfaces with same subnet part of IP address
  - can physically reach each other without intervening router



network consisting of 3 subnets

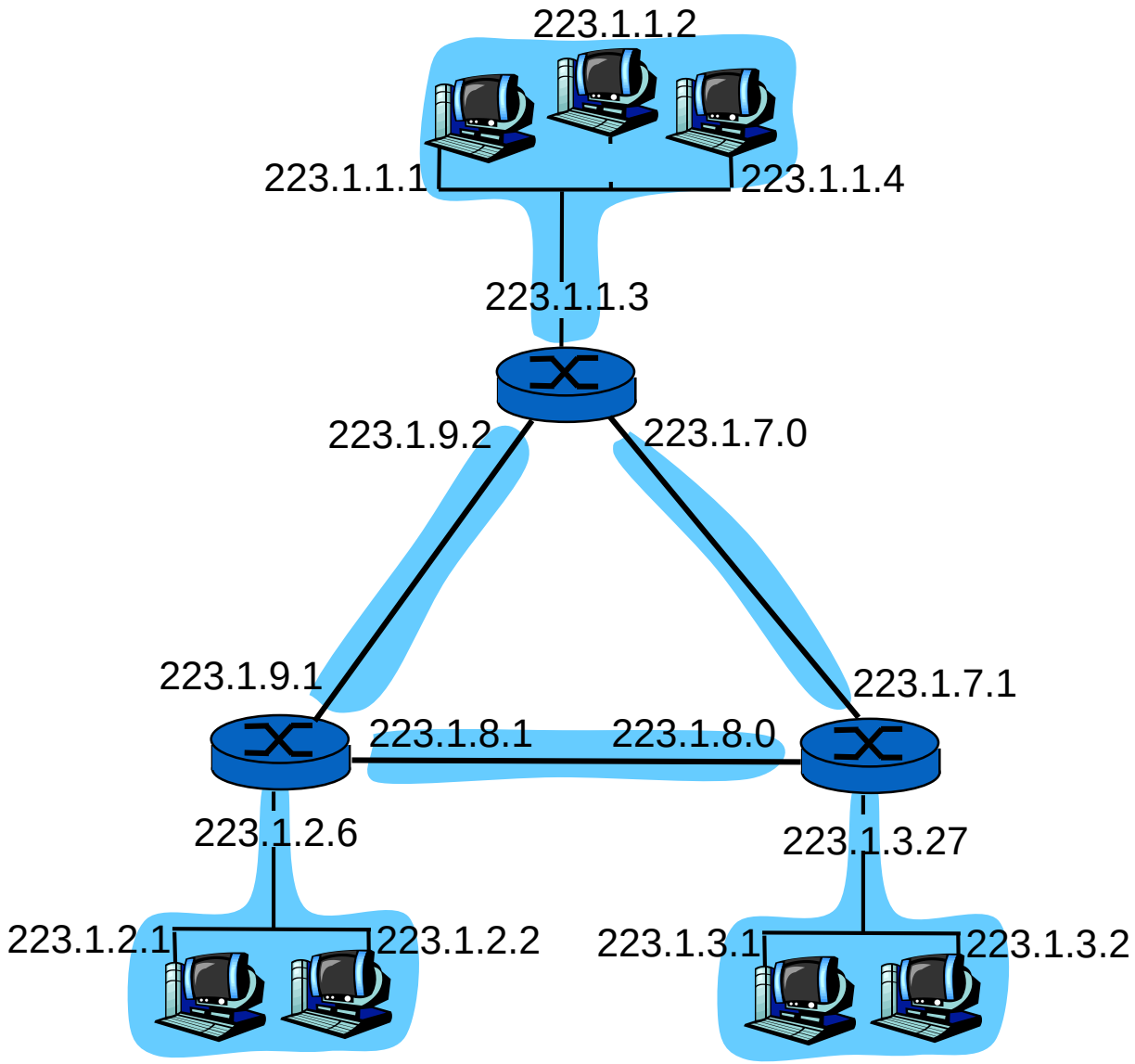
Subnets

- Recipe
- To determine the subnets, detach each interface from its host or router, creating islands of isolated networks. Each isolated network is called a subnet.

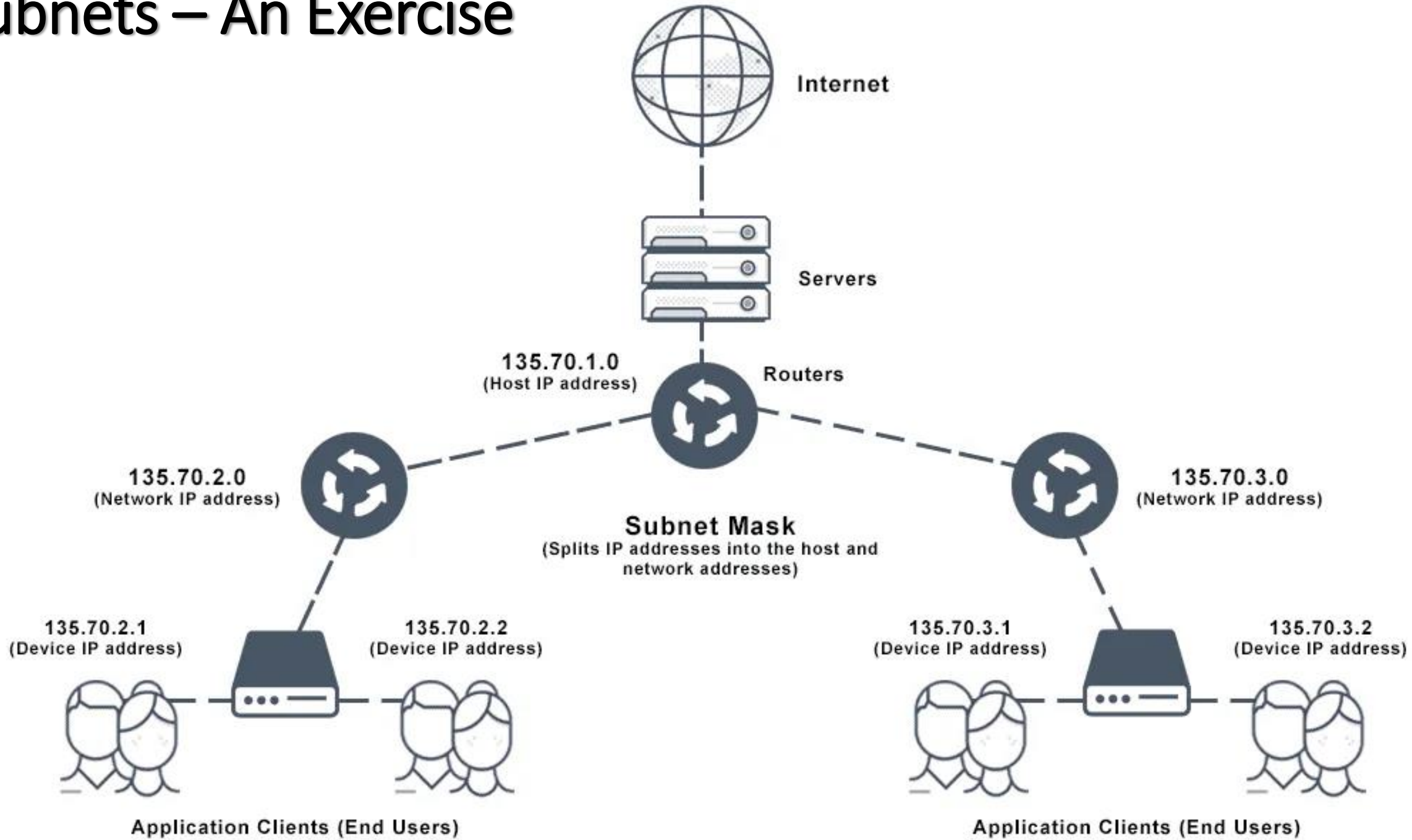


Subnet mask: /24

Subnets



Subnets – An Exercise



Subnets – An Exercise

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

- Select a number from row 1 which is equal to or just greater than the number of subnets required. We choose 4.
- Select the whole column i.e. Subnets-4, Host-64, Mask-/26. We choose 4 subnets, each of which will have 64 host IDs including networking ID and broadcasting ID, and /26 is the subnet mask for all of these subnets.

Subnets – An Exercise

Original networkID:
192.168.4.0/24

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Network ID	Subnet Mask	Host ID Range	# of Usable Host	Broadcast ID

Network IDs

- Let's find the first network ID which is always the original network ID, i.e. 192.168.4.0
- The second network ID can be obtained by simply adding 64 (the number of hosts) to the first network ID, 192.168.4.64
- Similarly, third network ID becomes 192.168.4.128 and fourth network ID becomes 192.168.4.192

Subnet Mask

- The subnet mask becomes /26 as per the column we selected.

Subnets - – An Exercise

Network ID	Subnet Mask	Host ID Range	# of Usable Host	Broadcast ID
192.168.4.0	/26	192.168.4.1-192.168.4.62	62	192.168.4.63
192.168.4.64	/26	192.168.4.65-192.168.4.126	62	192.168.4.127
192.168.4.128	/26	192.168.4.129-192.168.4.190	62	192.168.4.191
192.168.4.192	/26	192.168.4.193-192.168.4.254	62	192.168.4.255

Number of usable Host IDs

- As per the selected column, the number of hosts becomes 64, however, the first and last host IDs are reserved for network ID and broadcast ID. Thus, the net usable IDs come down to 64–2 = 62 for all the subnets.

Broadcast ID

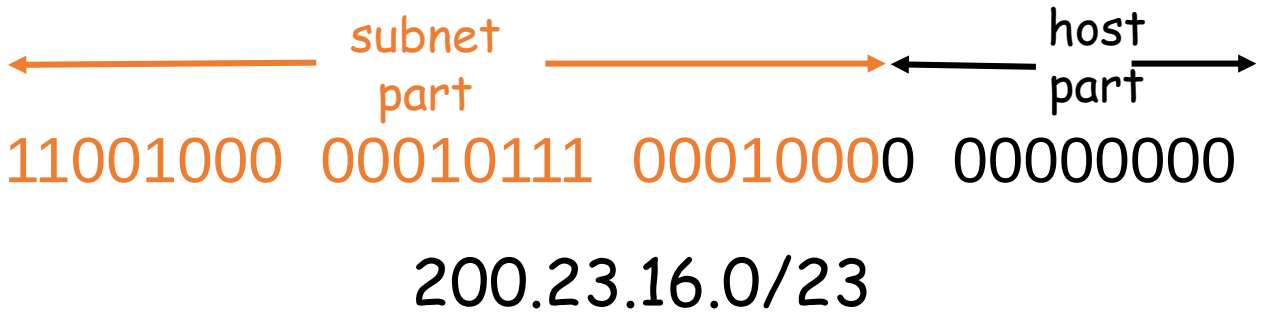
- Since, the last host ID is reserved for broadcast ID, the broadcast ID for first subnet becomes 192.168.4.63 the broadcast ID for second subnet becomes 192.168.4.127 the broadcast ID for third subnet becomes 192.168.4.191 the broadcast ID for fourth subnet becomes 192.168.4.255

Host ID range

- The range of host IDs refers to the host IDs between the network ID and the broadcast ID in a subnet.

IP addressing: CIDR

- CIDR: Classless InterDomain Routing
  - subnet portion of address of arbitrary length
  - address format: a.b.c.d/x, where x is # bits in subnet portion of address



IP Addresses

IP addresses: how to get one?

- Q: How does *host* get IP address?

- hard-coded by system admin in a file
  - Wintel: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config
- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - “plug-and-play”
-

IP Addresses

IP addresses: how to get one?

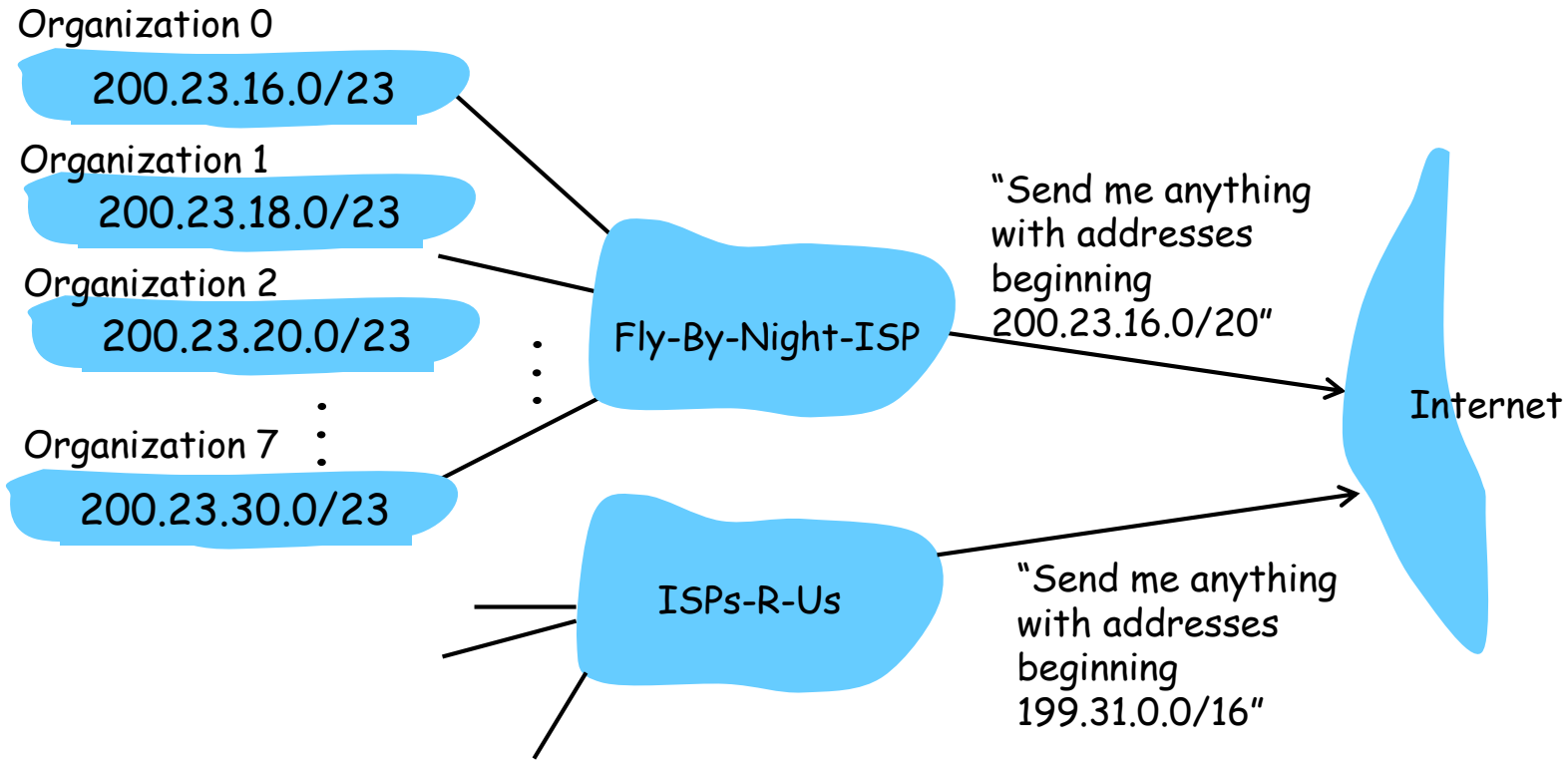
- Q: How does *network* get subnet part of IP addr?
- A: gets allocated portion of its provider ISP's address space

ISP's block	11001000 00010111 00010000	00000000	200.23.16.0/20
Organization 0	11001000 00010111 00010000	00000000	200.23.16.0/23
Organization 1	11001000 00010111 00010010	00000000	200.23.18.0/23
Organization 2	11001000 00010111 00010100	00000000	200.23.20.0/23
...	.....	....	....
Organization 7	11001000 00010111 00011110	00000000	200.23.30.0/23

IP Addresses

Hierarchical addressing

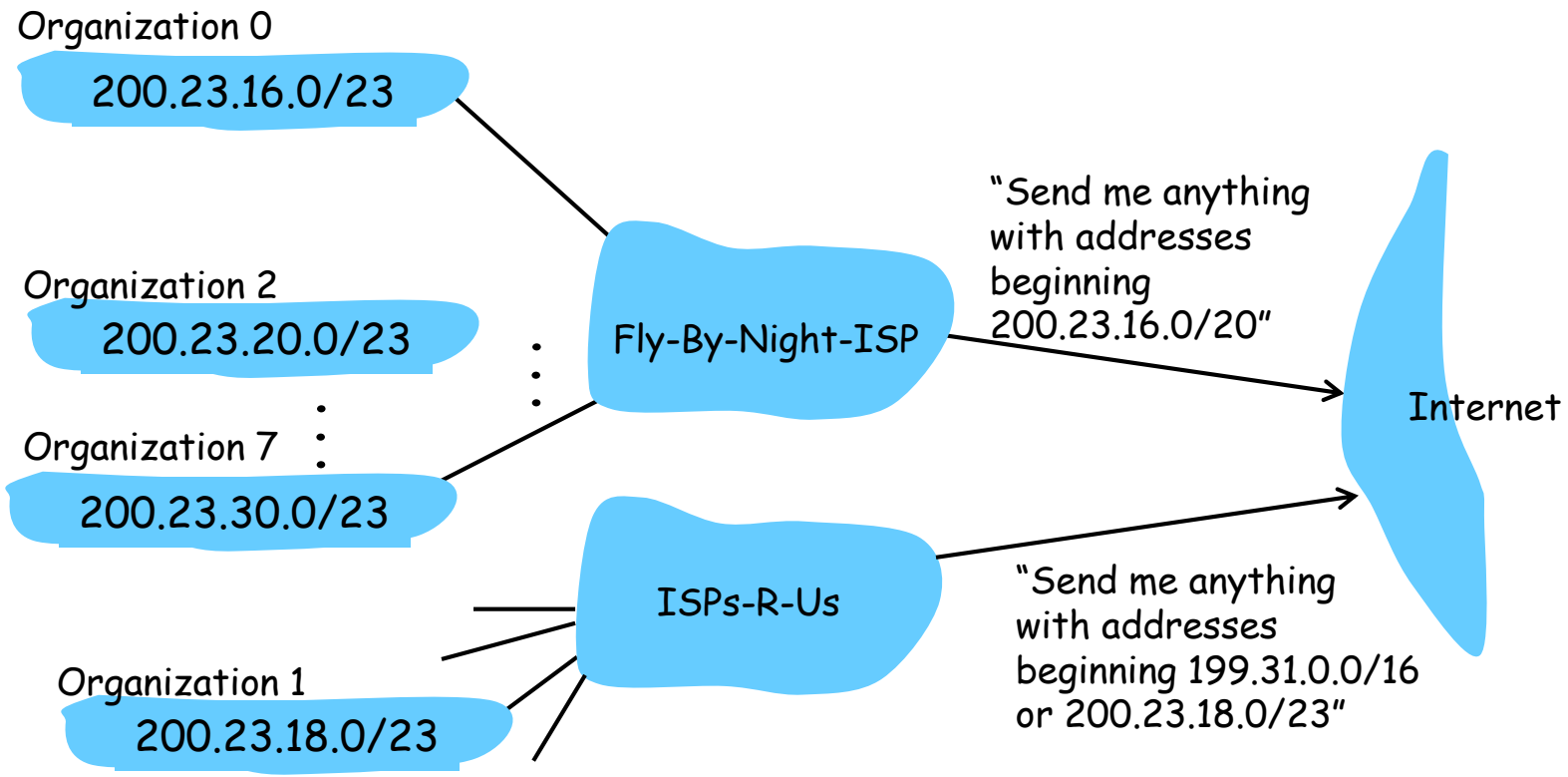
Hierarchical addressing allows efficient advertisement of routing information:



IP Addresses

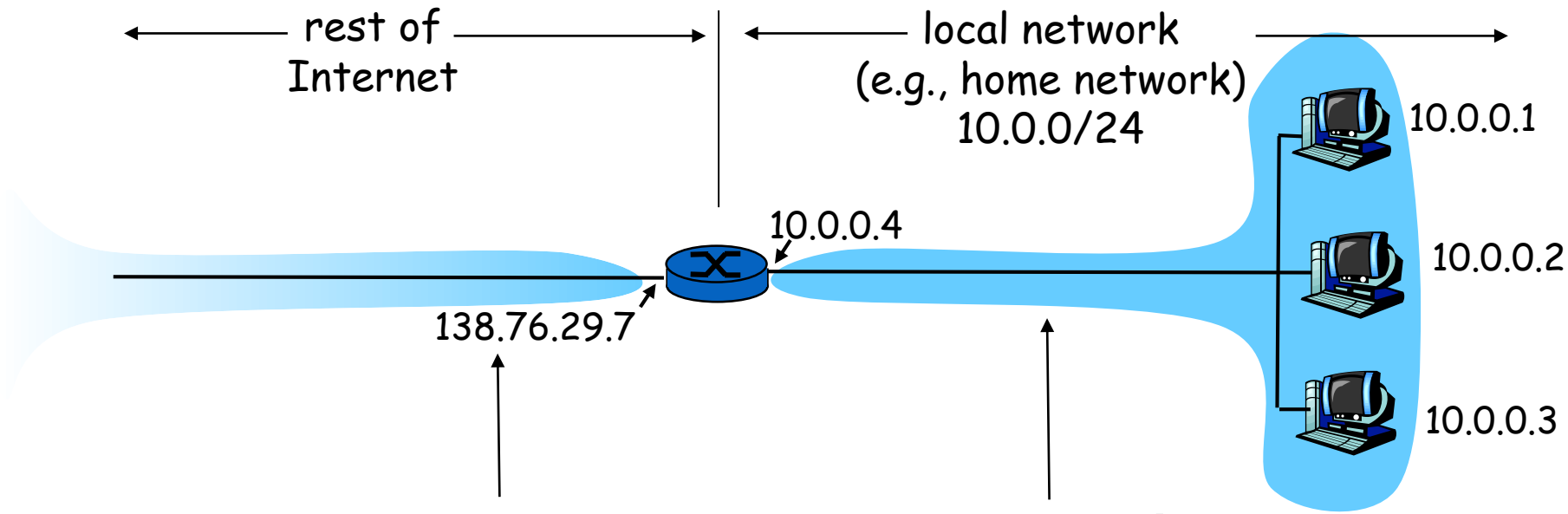
Hierarchical addressing

ISPs-R-Us has a more specific route to Organization 1



IP Addresses

NAT (Network Address Translation)



All datagrams *leaving* local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

IP Addresses: NAT

- Motivation: local network uses just one IP address as far as outside world is concerned:
  - no need to be allocated range of addresses from ISP: - just one IP address is used for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).

IP Addresses: NAT

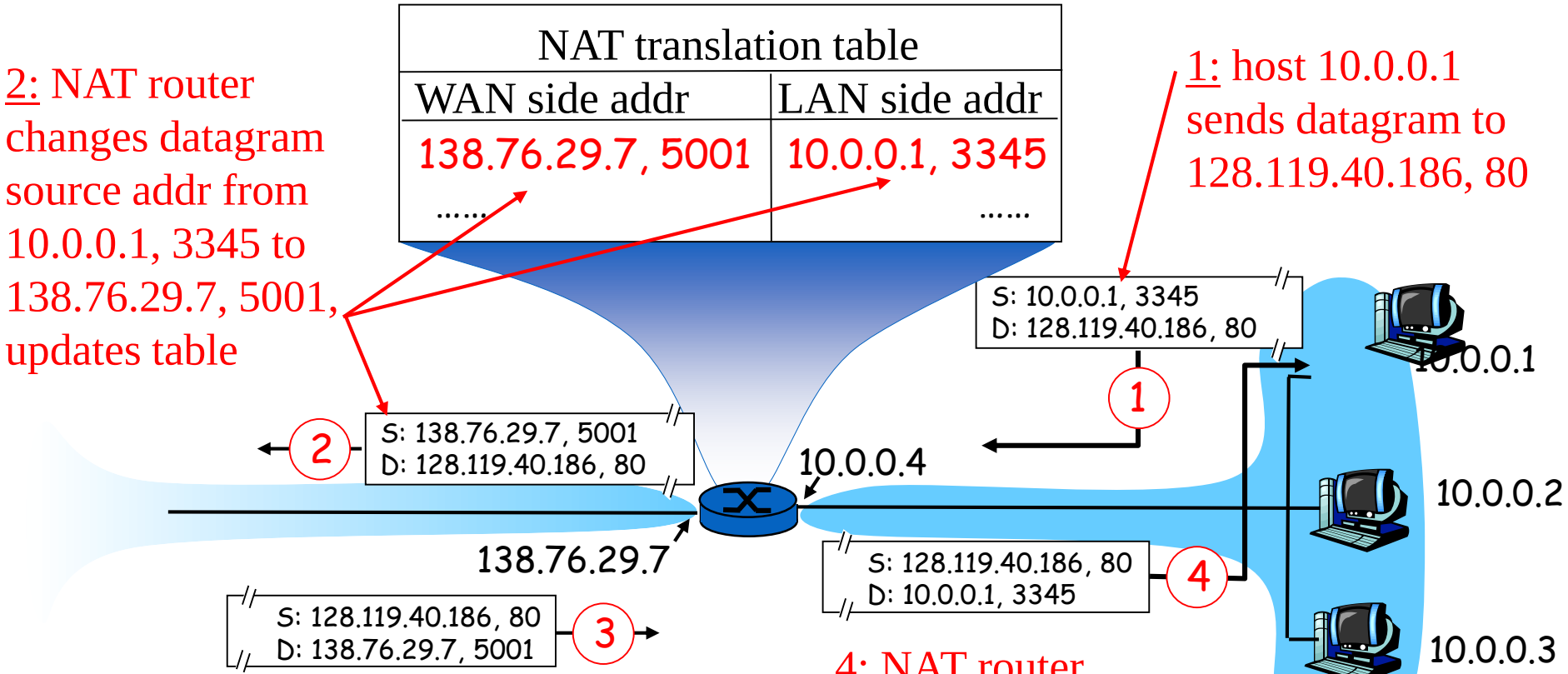
- Implementation: NAT router must:
  - *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)

    . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr.

  - *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair
  - *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

IP Addresses

IP Addresses: NAT



IP Addresses

NAT

- 16-bit port-number field:
  - 60,000 simultaneous connections with a single LAN-side address!
- NAT is controversial:
  - routers should only process up to layer 3
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, eg, P2P applications
  - address shortage should instead be solved by IPv6

Internet Control Message Protocol

ICMP

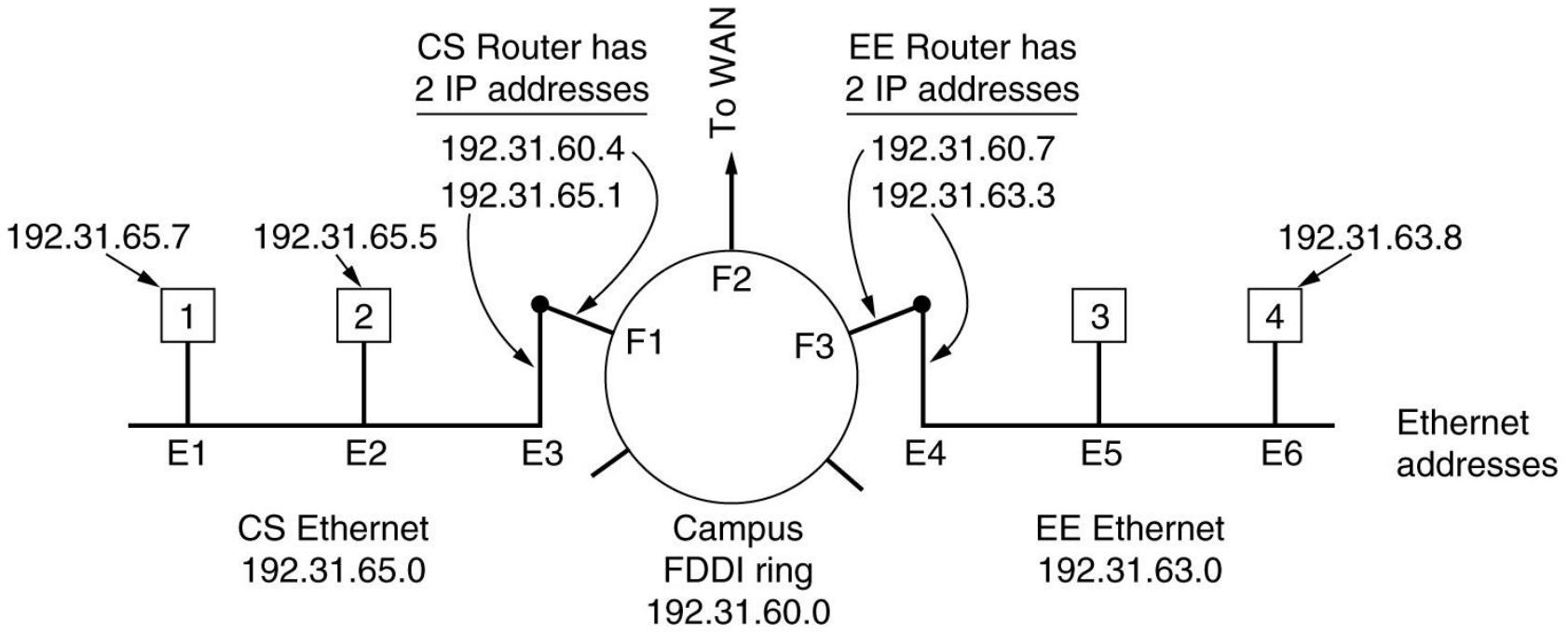
- The principal ICMP message types.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

The Address Resolution Protocol

ARP

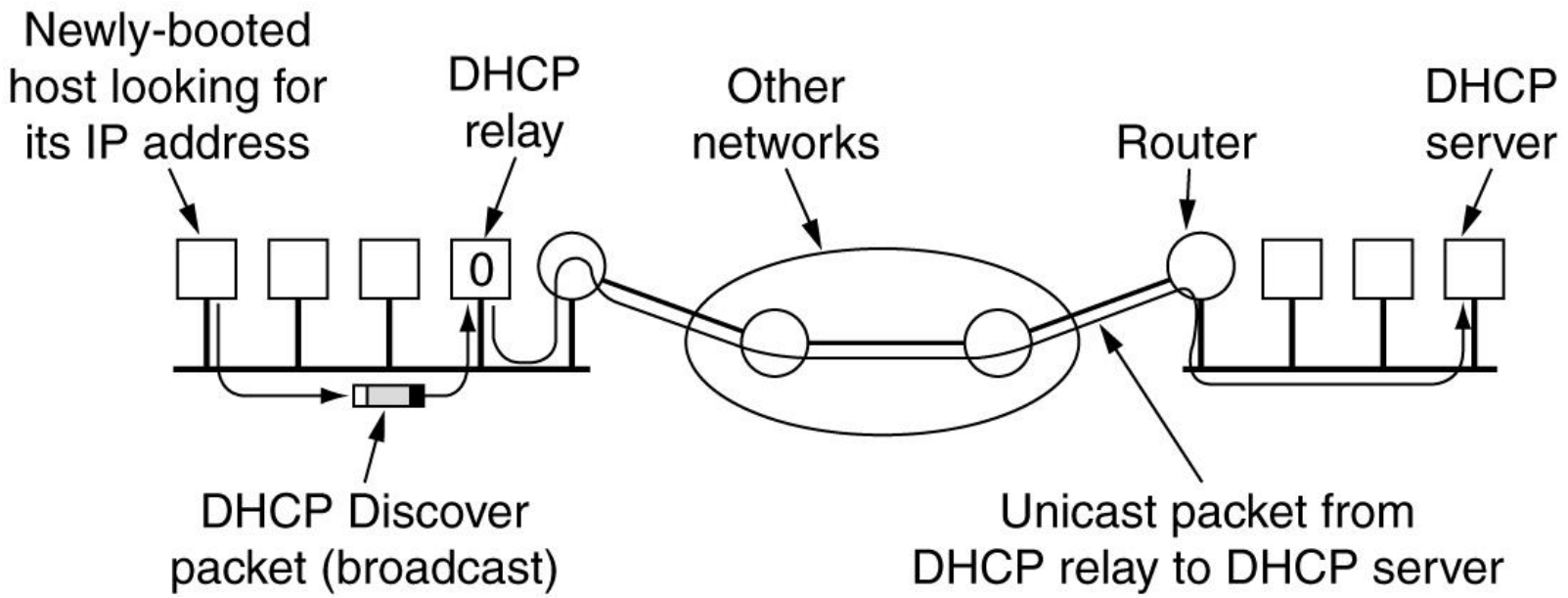
- Three interconnected /24 networks: two Ethernets and an FDDI ring.



Dynamic Host Configuration Protocol

DHCP

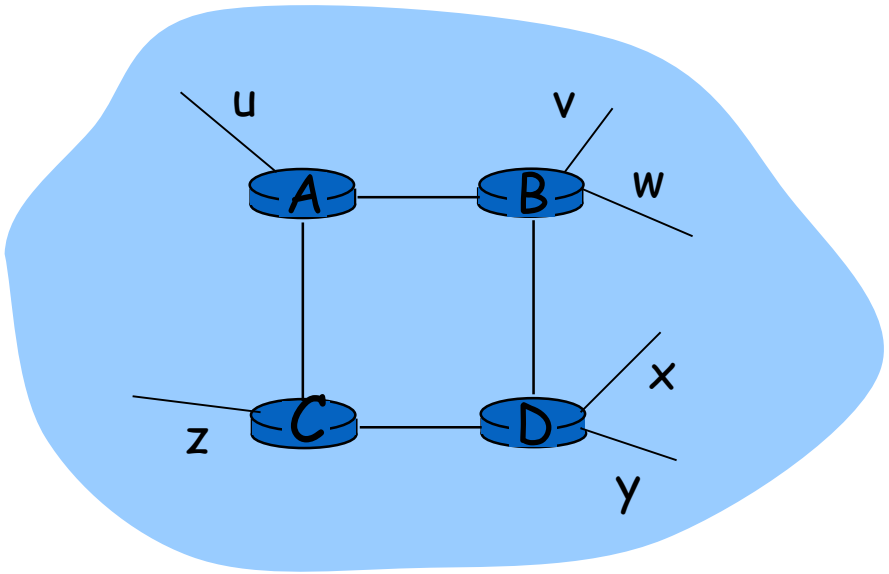
- Operation of DHCP.



Routing Information Protocol

RIP (Routing Information Protocol)

- Distance vector algorithm
- Included in BSD-UNIX Distribution in 1982
- Distance metric: # of hops (max = 15 hops)



From router A to subsets:

destination	hops
u	1
v	2
w	2
x	3
y	3
z	2

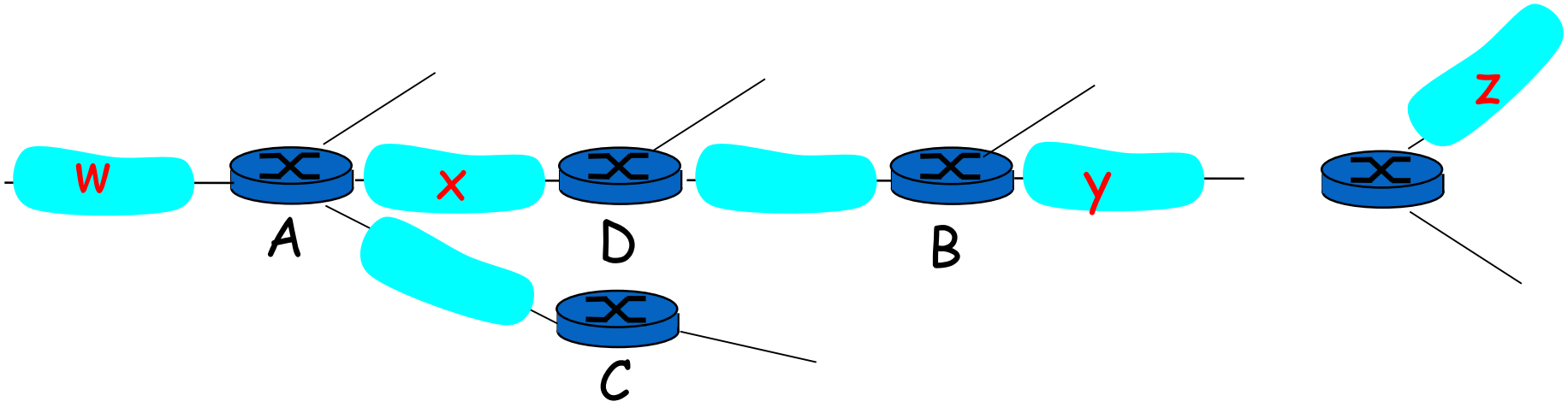
Routing Information Protocol

RIP : advertisements

- Distance vectors: exchanged among neighbors every 30 sec via Response Message (also called advertisement)
- Each advertisement: list of up to 25 destination nets within AS

Routing Information Protocol

RIP : Example



Destination Network	Next Router	Num. of hops to dest.
w	A	2
y	B	2
z	B	7
x	--	1
….	….	….

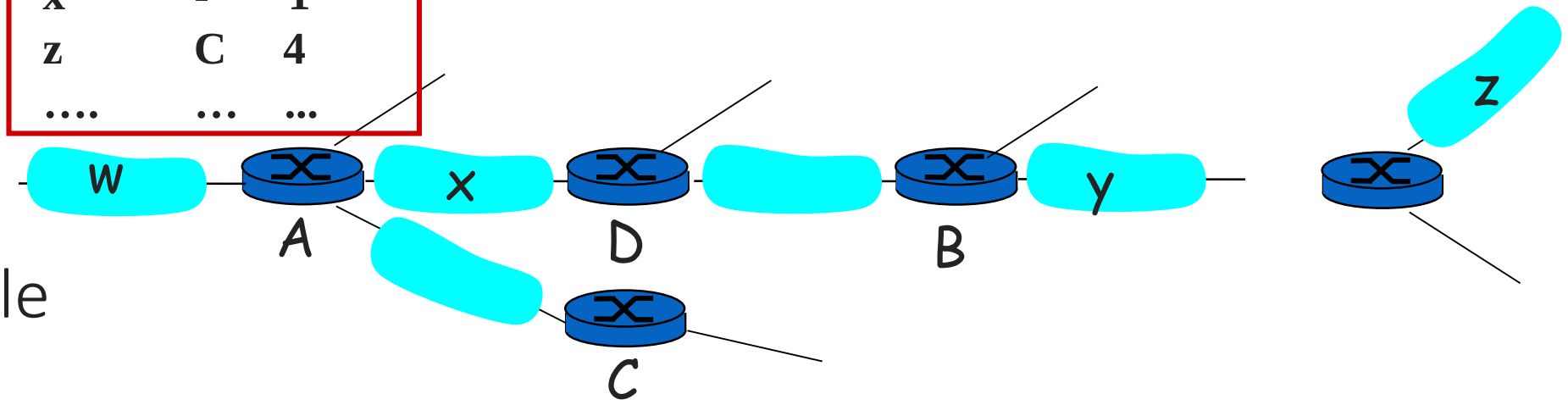
Routing table in D

Routing Information Protocol

RIP : Example

Dest	Next	hops
w	-	1
x	-	1
z	C	4
….	…	…

Advertisement from A to D



Destination Network	Next Router	Num. of hops to dest.
w	A	2
y	B	2
z	~~B~~ A	~~7~~ 5
x	--	1
….	….	….

Routing table in D

Routing Information Protocol

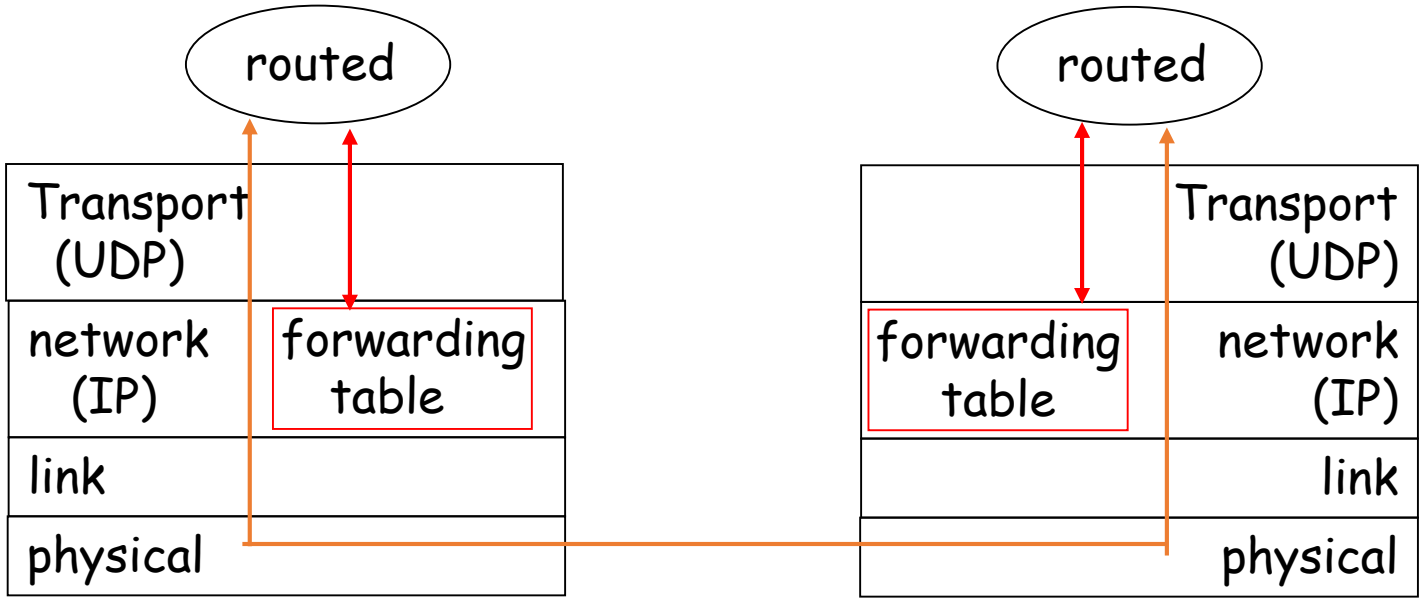
RIP : Link Failure and Recovery

- If no advertisement heard after 180 sec --> neighbor/link declared dead
  - routes via neighbor invalidated
  - new advertisements sent to neighbors
  - neighbors in turn send out new advertisements (if tables changed)
  - link failure info quickly propagates to entire net
  - poison reverse used to prevent ping-pong loops (infinite distance = 16 hops)

Routing Information Protocol

RIP : Table processing

- RIP routing tables managed by **application-level** process called route-d (daemon)
- advertisements sent in UDP packets, periodically repeated



Open Shortest Path First

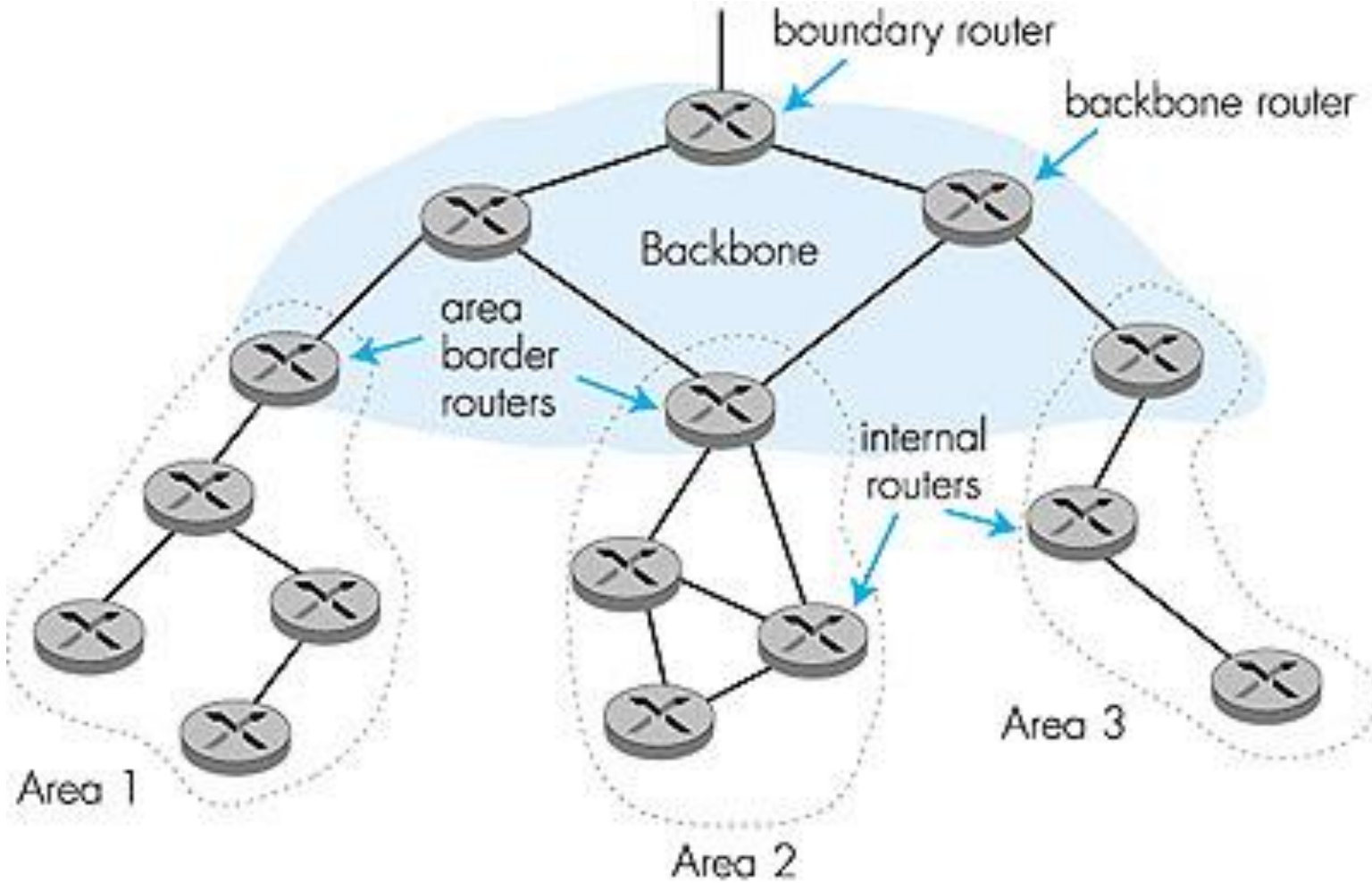
OSPF

- "open": publicly available
- Uses Link State algorithm
  - LS packet dissemination
  - Topology map at each node
  - Route computation using Dijkstra's algorithm

- OSPF advertisement carries one entry per neighbor router
- Advertisements disseminated to entire AS (via flooding)
  - Carried in OSPF messages directly over IP (rather than TCP or UDP

Open Shortest Path First

Hierarchical OSPF



Open Shortest Path First

Hierarchical OSPF

- Two-level hierarchy: local area, backbone.
  - Link-state advertisements only in area
  - each nodes has detailed area topology; only know direction (shortest path) to nets in other areas.
- **Area border routers:** "summarize" distances to nets in own area, advertise to other Area Border routers.
- **Backbone routers:** run OSPF routing limited to backbone.
- **Boundary routers:** connect to other AS's.

Border Gateway Protocol

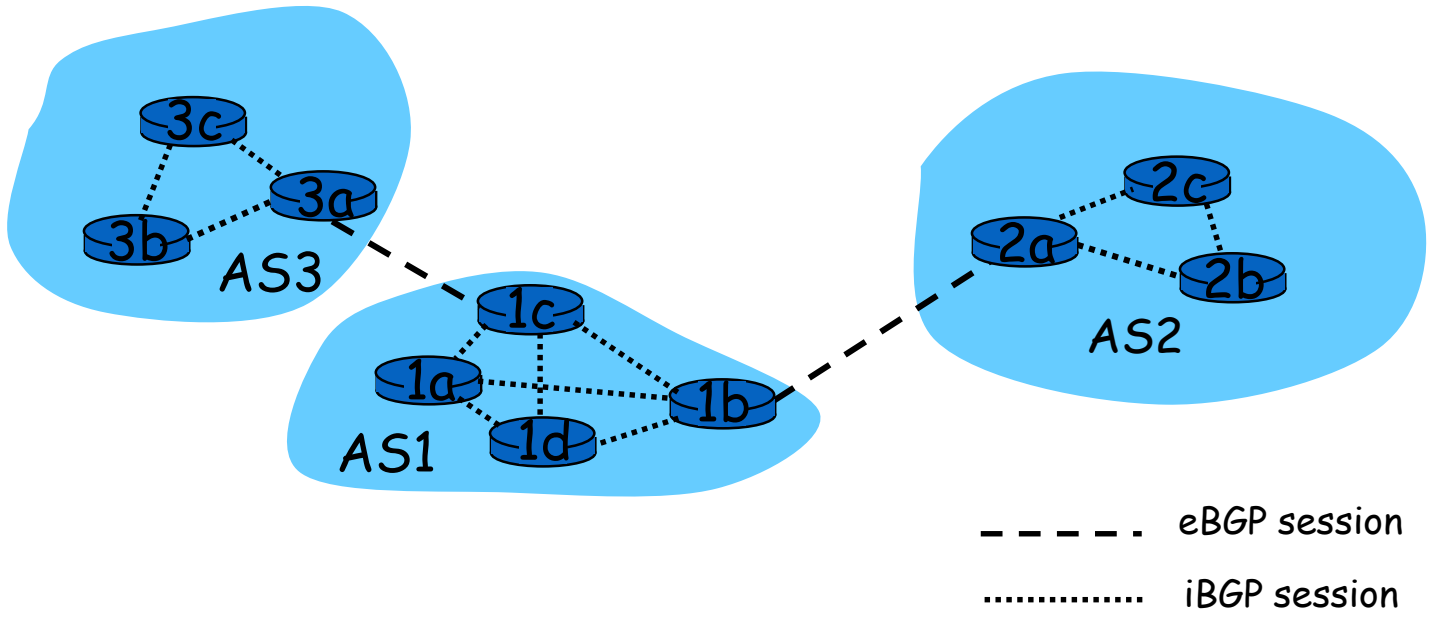
BGP

- BGP (Border Gateway Protocol): *the* de facto standard
- BGP provides each AS a means to:
  - Obtain subnet reachability information from neighboring ASs.
  - Propagate the reachability information to all routers internal to the AS.
  - Determine "good" routes to subnets based on reachability information and policy.
- Allows a subnet to advertise its existence to rest of the Internet: *"I am here"*

Border Gateway Protocol

BGP : basics

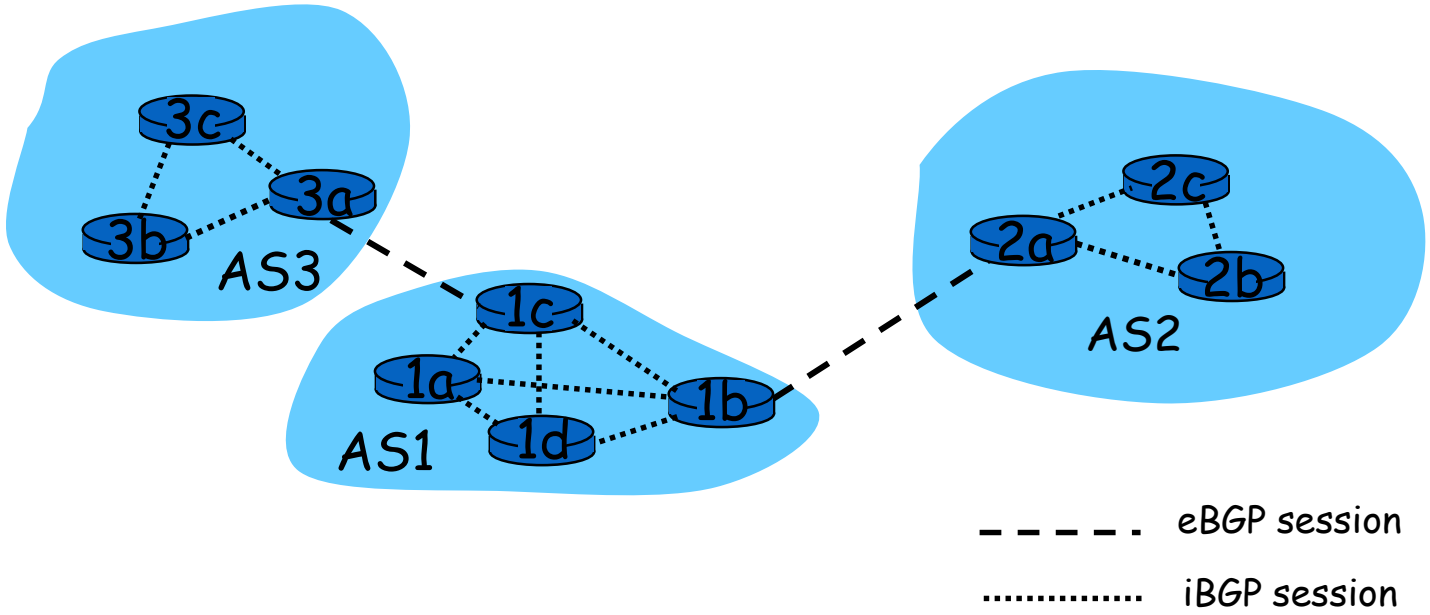
- Pairs of routers (BGP peers) exchange routing info over semi-permanent TCP connections: BGP sessions
- Note that BGP sessions do not correspond to physical links.
- When AS2 advertises a prefix to AS1, AS2 is *promising* it will forward any datagrams destined to that prefix towards the prefix.
    - AS2 can aggregate prefixes in its advertisement



EE

BGP : Distributing reachability info

- With eBGP session between 3a and 1c, AS3 sends prefix reachability info to AS1.
- 1c can then use iBGP do distribute this new prefix reach info to all routers in AS1.
- 1b can then re-advertise the new reach info to AS2 over the 1b-to-2a eBGP session.
- When router learns about a new prefix, it creates an entry for the prefix in its forwarding table.



BGP : Path attributes & BGP routes

- When advertising a prefix, advert includes BGP attributes.
  - prefix + attributes = “route”
- Two important attributes:
  - AS-PATH: contains the ASs through which the advert for the prefix passed: AS 67 AS 17
  - NEXT-HOP: Indicates the specific internal-AS router to next-hop AS. (There may be multiple links from current AS to next-hop-AS.)
- When gateway router receives route advert, uses import policy to accept/decline.

BGP : route selection

- Router may learn about more than 1 route to some prefix. Router must select route.
- Elimination rules:
  1. Local preference value attribute: policy decision
  2. Shortest AS-PATH
  3. Closest NEXT-HOP router: hot potato routing
  4. Additional criteria

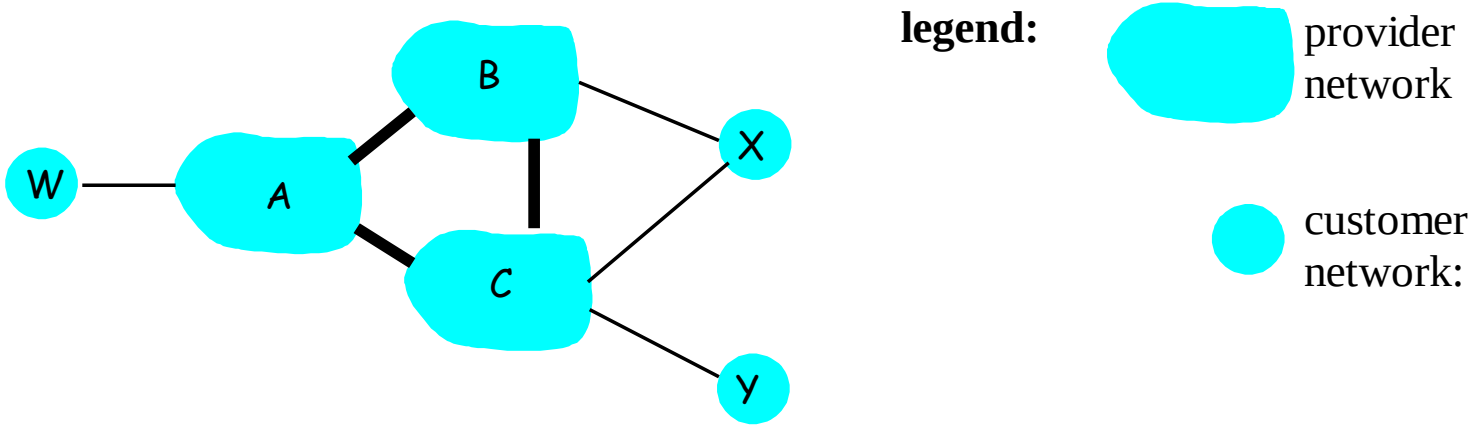
Border Gateway Protocol

BGP : messages

- BGP messages exchanged using TCP.
- BGP messages:
  - OPEN: opens TCP connection to peer and authenticates sender
  - UPDATE: advertises new path (or withdraws old)
  - KEEPALIVE keeps connection alive in absence of UPDATES; also ACKs OPEN request
  - NOTIFICATION: reports errors in previous msg; also used to close connection

Border Gateway Protocol

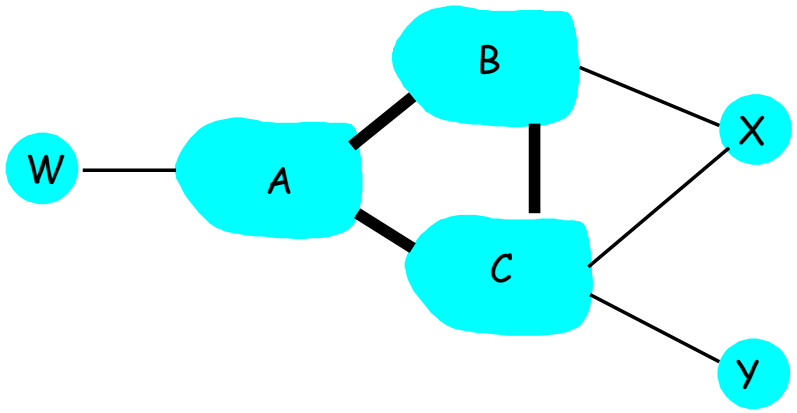
BGP : routing policy

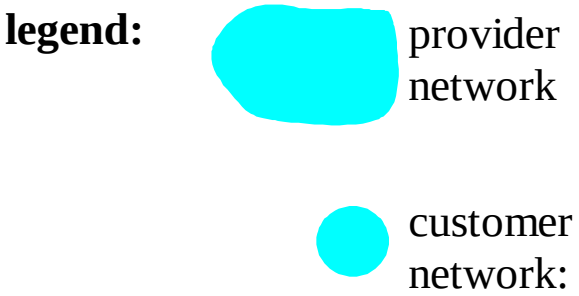


- A,B,C are provider networks
- X,W,Y are customer (of provider networks)
- X is dual-homed: attached to two networks
  - X does not want to route from B via X to C
  - .. so X will not advertise to B a route to C

Border Gateway Protocol

BGP : routing policy





- A advertises to B the path AW
- B advertises to X the path BAW
- Should B advertise to C the path BAW?
  - No way! B gets no “revenue” for routing CBAW since neither W nor C are B’s customers
  - B wants to force C to route to w via A
  - B wants to route *only* to/from its customers!

References

1. Nevio Benvenuto and Michele Zorzi, (2011). Principles of Communications Networks and Systems, John Wiley.

2. Thomas Robertazzi, (2011). Basics of Computer Networking (Springer Briefs in Electrical and Computer Engineering), Springer.

3. Andrew S. Tanenbaum and David J. Wetherall. 2010. Computer Networks (5th. ed.). Prentice Hall Press, USA.

4. https://study-ccna.com


©udayadamnage

Exercise One