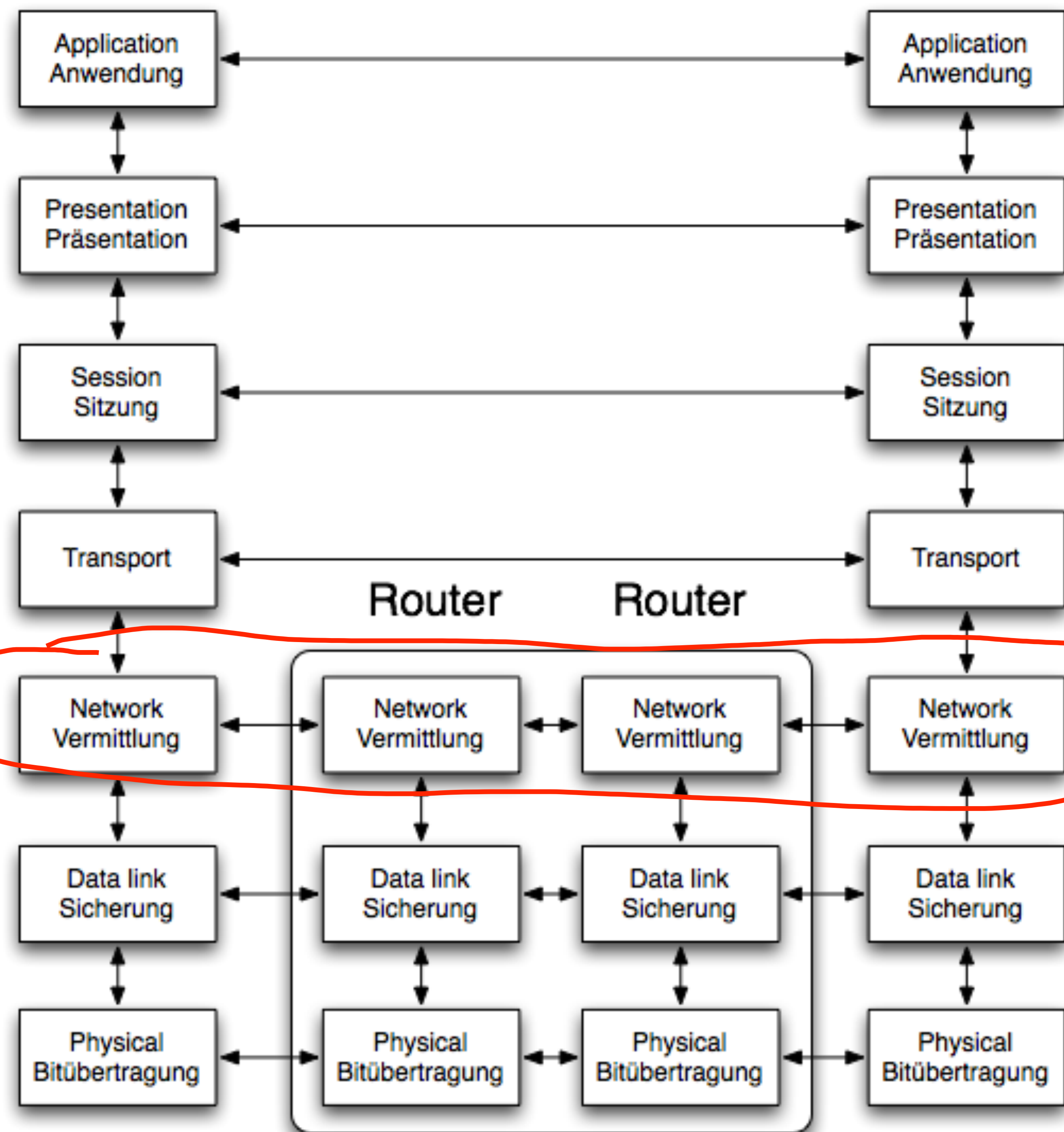
Wireless Sensor Networks
5. Routing

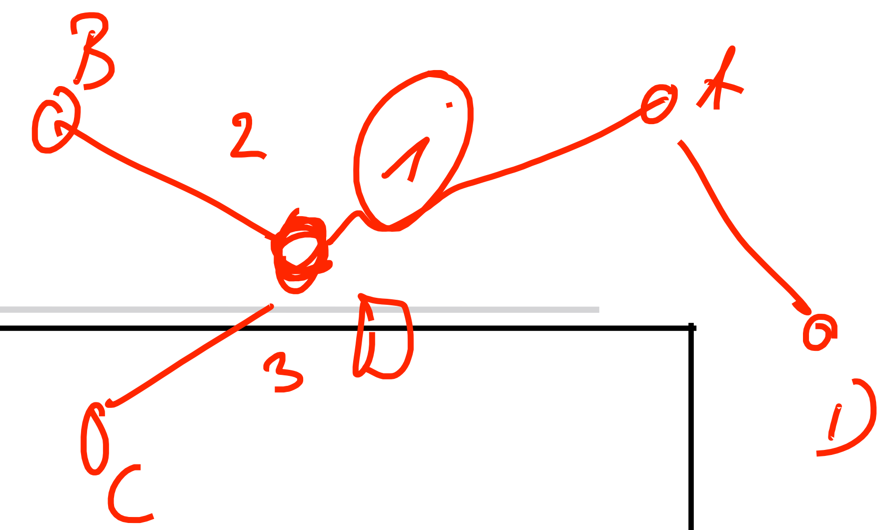
Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg
Version 29.04.2016

ISO/OSI Reference model

- 7. Application
  - Data transmission, e-mail, terminal, remote login
- 6. Presentation
  - System-dependent presentation of the data (EBCDIC / ASCII)
- 5. Session
  - start, end, restart
- 4. Transport
  - Segmentation, congestion
- 3. Network
  - Routing
- 2. Data Link
  - Checksums, flow control
- 1. Physical
  - Mechanics, electrics



Protocols of the Internet

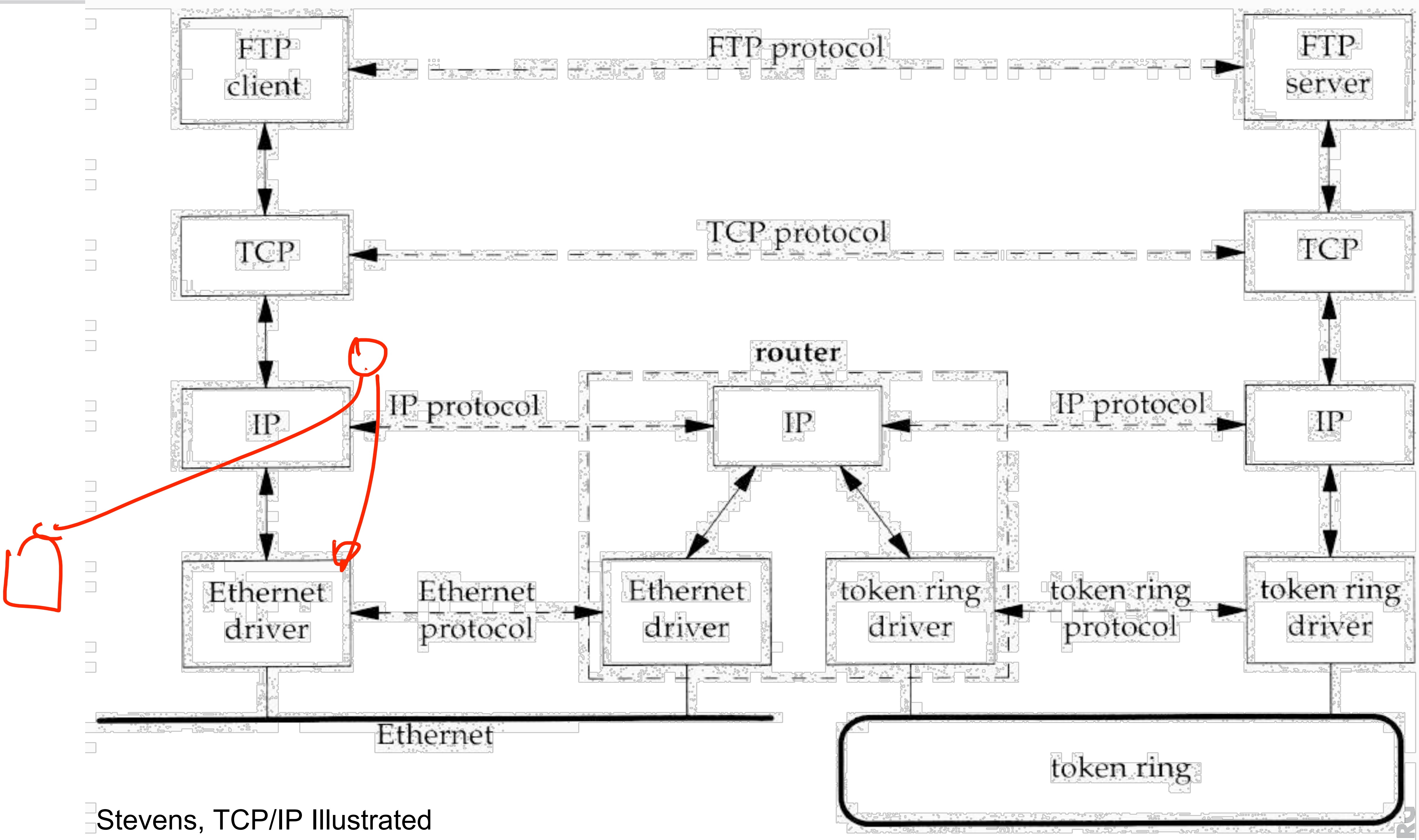


Application	Telnet, FTP, HTTP, SMTP (E-Mail), ...
Transport	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Network	IP **(Internet Protocol)** + ICMP **(Internet Control Message Protocol)** + IGMP **(Internet Group Management Protocol)**
Host-to-Network	LAN **(e.g. Ethernet, Token Ring etc.)**

TCP/IP Layers

- 1. Host-to-Network
  - Not specified, depends on the local network,k e.g. Ethernet, WLAN 802.11, PPP, DSL
- 2. Routing Layer/Network Layer
  (IP - Internet Protocol)
  - Defined packet format and protocol
  - Routing
  - Forwarding
- 3. Transport Layer
  - TCP (Transmission Control Protocol)
    - Reliable, connection-oriented transmission
    - Fragmentation, Flow Control, Multiplexing
  - UDP (User Datagram Protocol)
    - hands packets over to IP
    - unreliable, no flow control
- 4. Application Layer
  - Services such as TELNET, FTP, SMTP, HTTP, NNTP (for DNS), ...

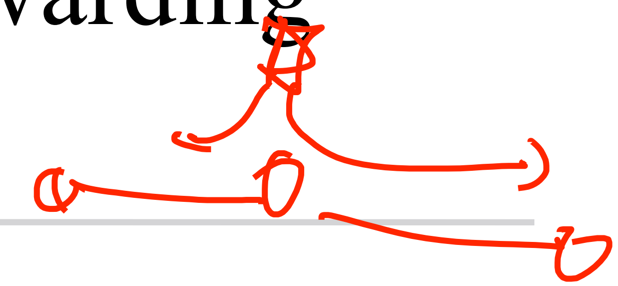
Example: Routing between LANs



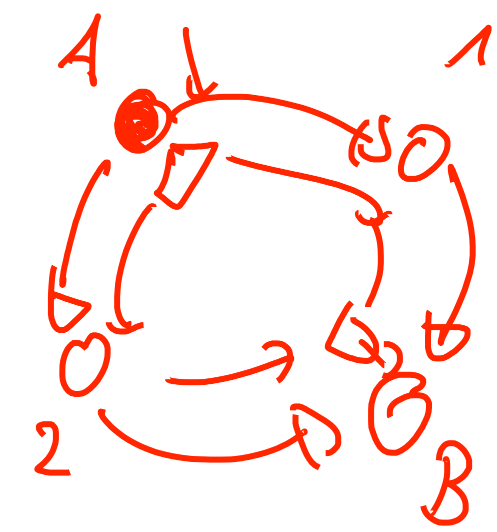
Stevens, TCP/IP Illustrated

CoNe Freiburg

Routing Tables and Packet Forwarding



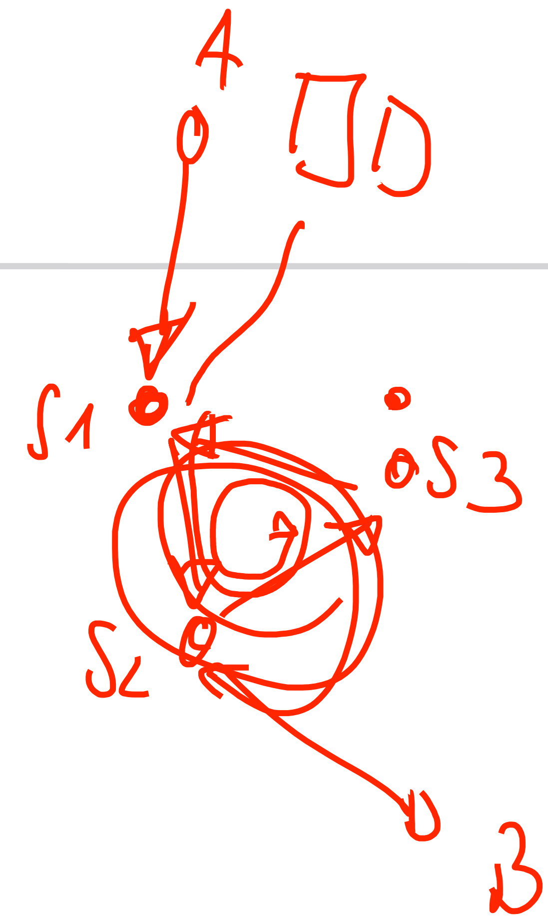
- IP Routing Table
  - contains for each destination the address of the next gateway
  - destination: host computer or sub-network
  - default gateway



- Packet Forwarding
  - IP packet (datagram) contains start IP address and destination IP address
    - if destination = my address then hand over to higher layer
    - if destination in routing table then forward packet to corresponding gateway
    - if destination IP subnet in routing table then forward packet to corresponding gateway
    - otherwise, use the default gateway

UNI FREIBURG

IP Packet Forwarding



- IP -Packet (datagram) contains...
  - TTL (Time-to-Live): Hop count limit
  - Start IP Address
  - Destination IP Address
- Packet Handling
  - Reduce TTL (Time to Live) by 1
  - If TTL ≠ 0 then forward packet according to routing table
  - If TTL = 0 or forwarding error (buffer full etc.):
    - delete packet
    - if packet is not an ICMP Packet then
      - send ICMP Packet with
      - start = current IP Address
      - destination = original start IP Address

Static and Dynamic Routing

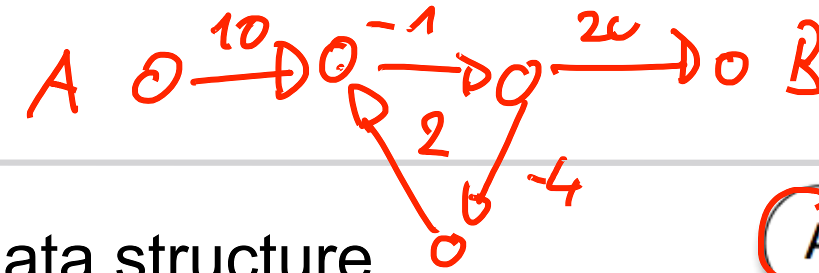
- Static Routing
  - Routing table created manually
  - used in small LANs
- Dynamic Routing
  - Routing table created by Routing Algorithm
  - Centralized, e.g. Link State
    - Router knows the complete network topology
  - Decentralized, e.g. Distance Vector
    - Router knows gateways in its local neighborhood

Intra-AS Routing

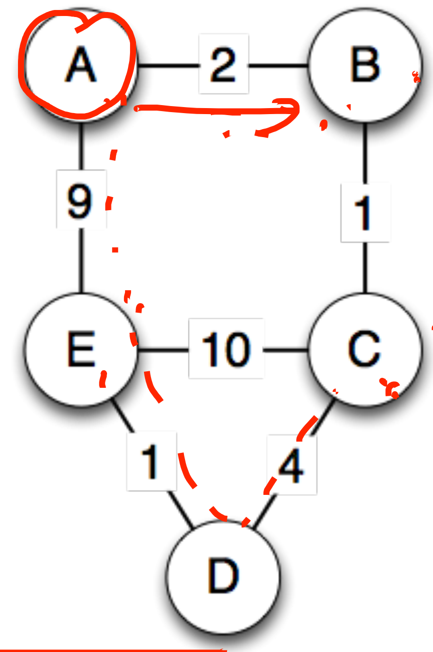
Within an Autonomous System

- Routing Information Protocol (RIP)
  - Distance Vector Algorithmus
  - Metric = hop count
  - exchange of distance vectors (by UDP)
- Interior Gateway Routing Protocol (IGRP)
  - successor of RIP
  - different routing metrics (delay, bandwidth)
- Open Shortest Path First (OSPF)
  - Link State Routing (every router knows the topology)
  - Route calculation by Dijkstra's shortest path algorithm

Distance Vector Routing Protocol



- Distance Table data structure
  - Each node has a
    - Line for each possible destination
    - Column for any direct neighbors
- Distributed algorithm
  - each node communicates only with its neighbors
- Asynchronous operation
  - Nodes do not need to exchange information in each round
- Self-terminating
  - exchange unless no update is available

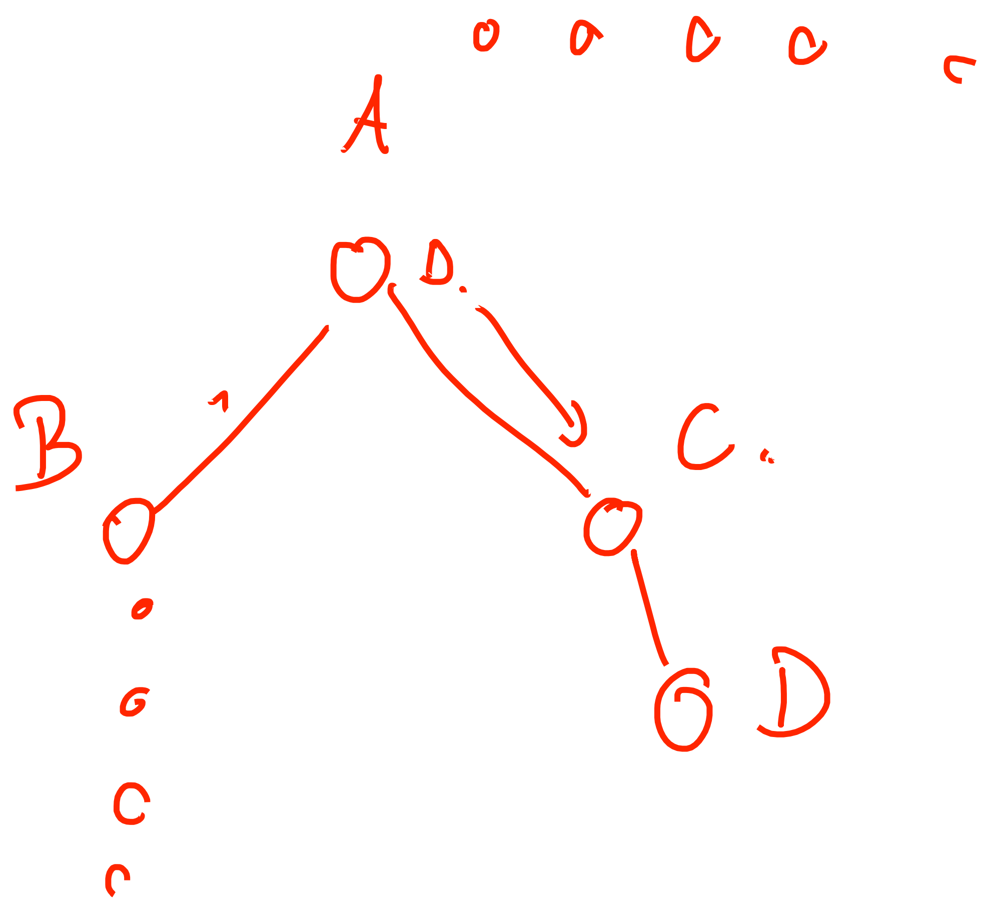


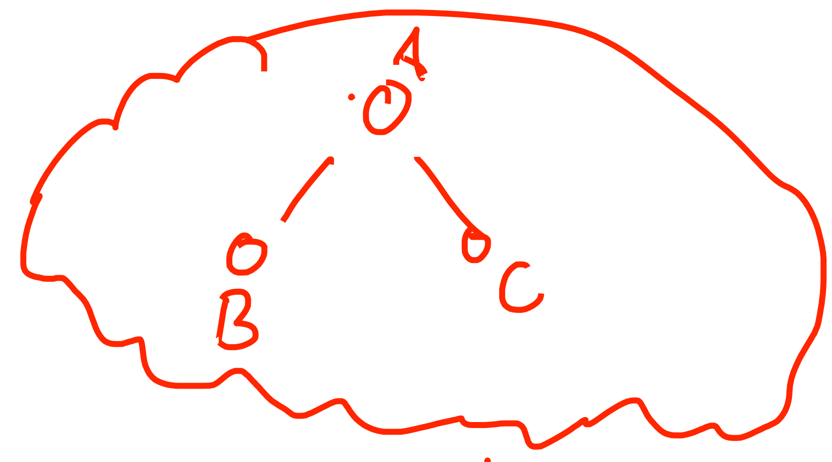
Distance Table for A

		via		Routing Table
from A		B	E	entry
to	B	**2**	15	B
	C	**3**	14	B
	D	**7**	10	B
	E	**8**	9	E

Distance Table for C

		via			Routing Table
from C		B	D	E	entry
to	A	**3**	11	18	B
	B	**1**	9	21	B
	D	6	**4**	11	D
	E	7	**5**	10	D

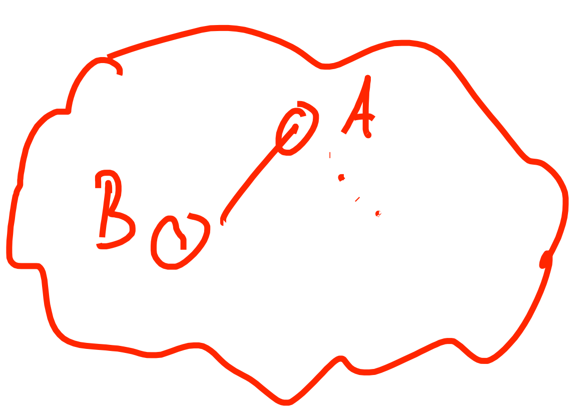




via

A	B	C
to B	1	
C		1

(B) 1
(C) 1



via

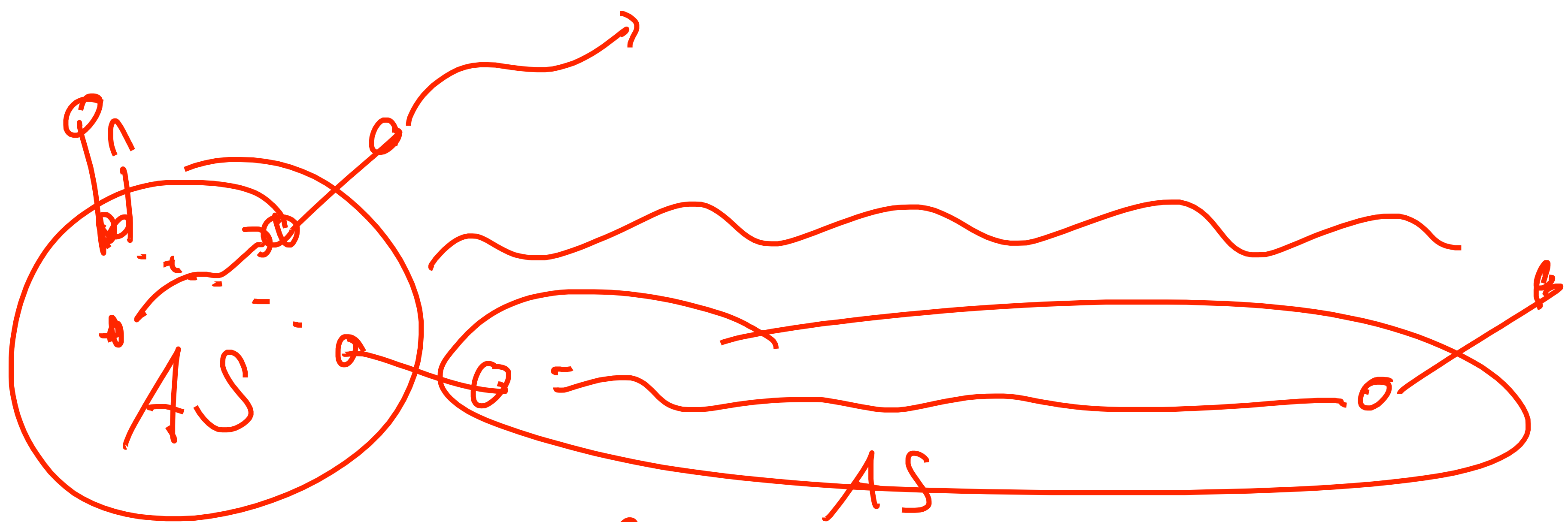
B	A
to A	1
C	2

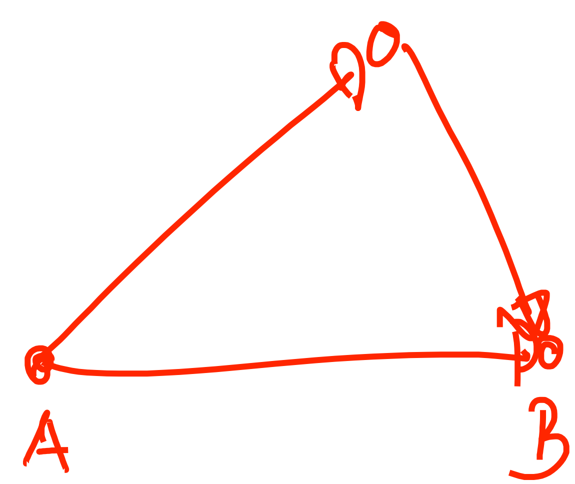
D	C
C	1

→

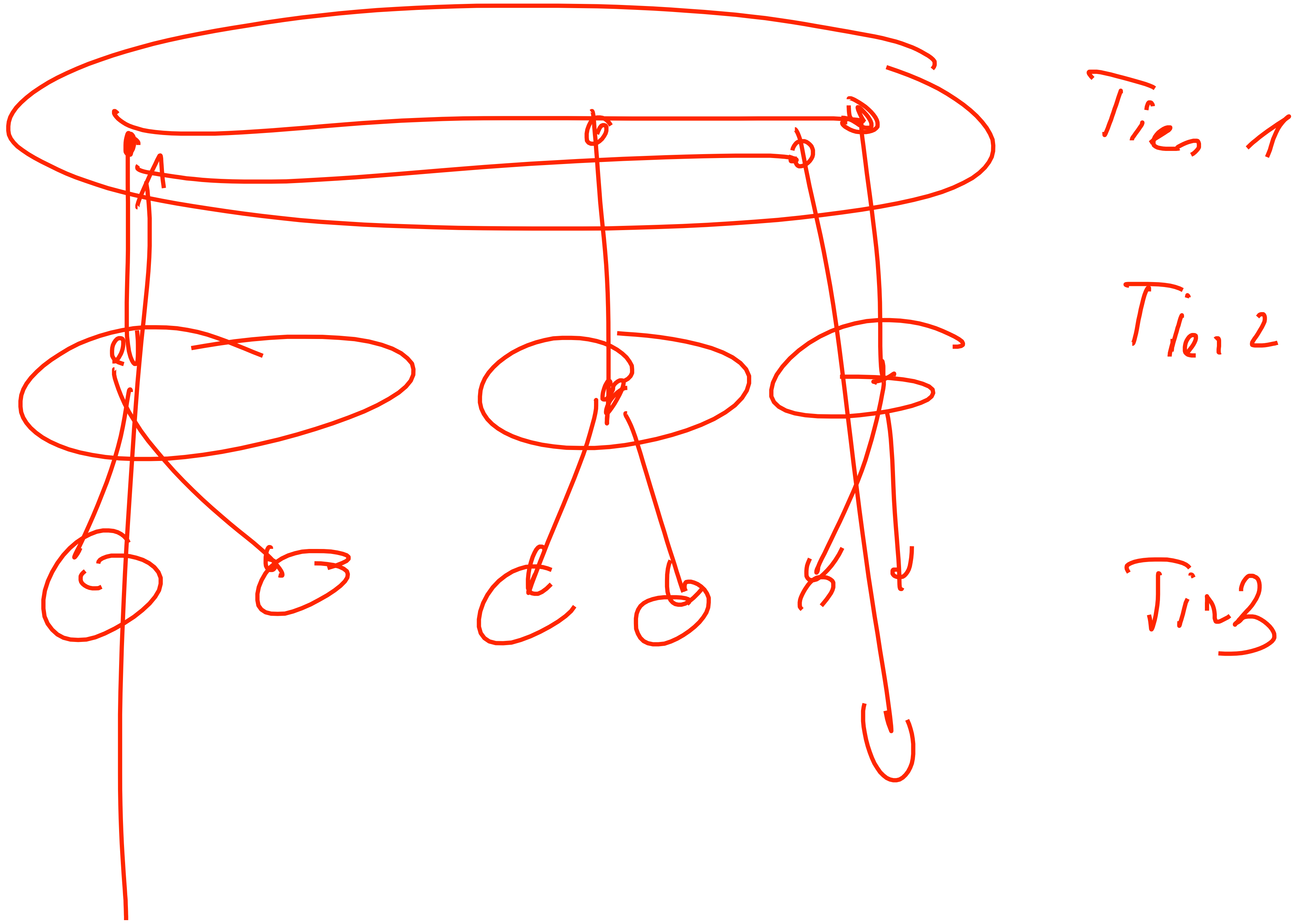
D

Inter - AS

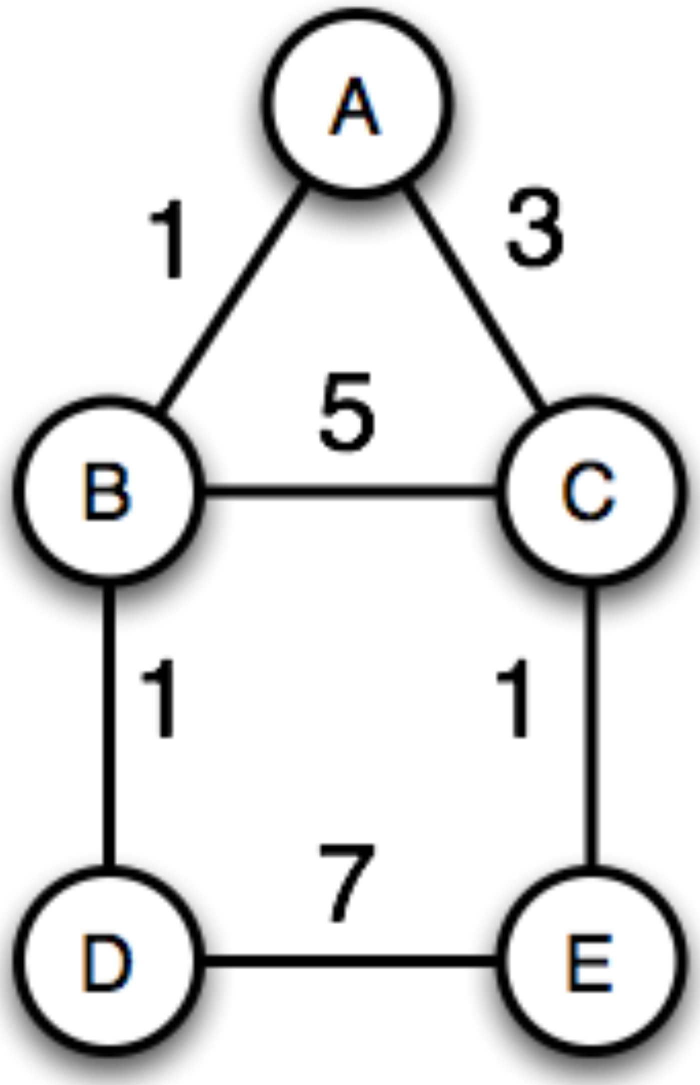




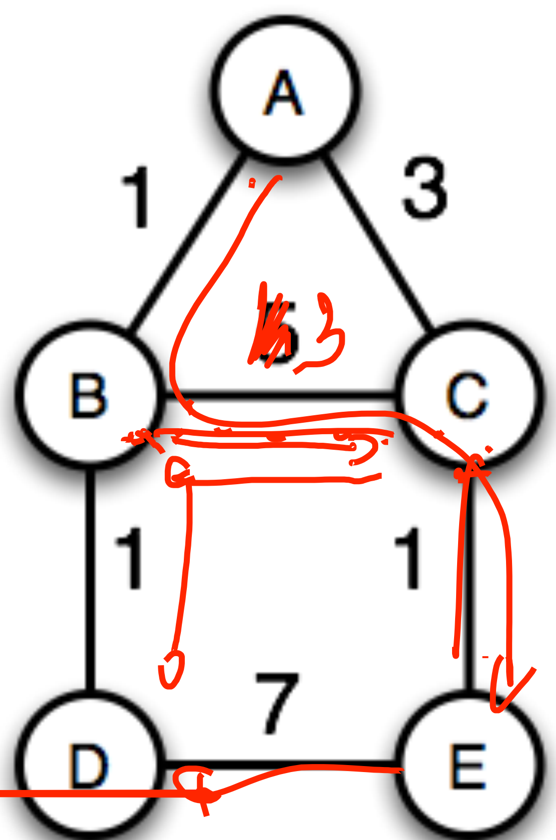
Tier: $l \leftarrow 0$ t_y



Distance Vector Routing Example



from A to	via B	via C	entry
B	**1**	8	**B**
C	6	**3**	**C**
D	**2**	9	**B**
E	7	**4**	**C**



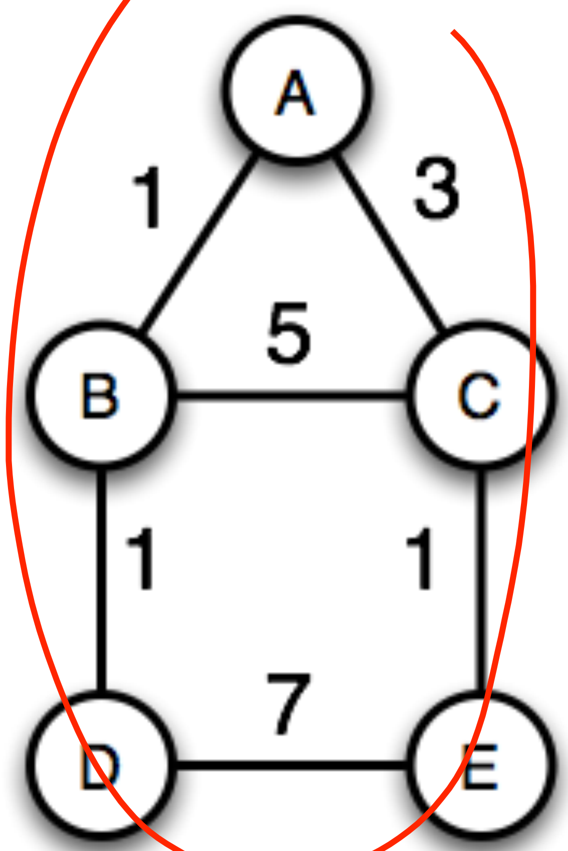
from A to	via B	via C	entry
B	1	-	B
C	-	3	C
D	-	-	-
E	-	-	-

from B to	via A	via C	via D	entry
A	1	-	-	A
C	-	3	-	C
D	-	-	1	C
E	-	-	8	D

from C to	via A	via B	via E	entry
A	3	-	-	A
B	-	5	-	B
D	-	-	8	E
E	-	-	1	E

from B to	via			Entry
	A	C	D	
A	1	-	-	A
C	-	5	-	C
D	-	-	1	D
E	-	-	8	D

from C to	via			Entry
	A	B	E	
A	3	-	-	A
B	-	5	-	B
D	-	-	8	E
E	-	-	1	E

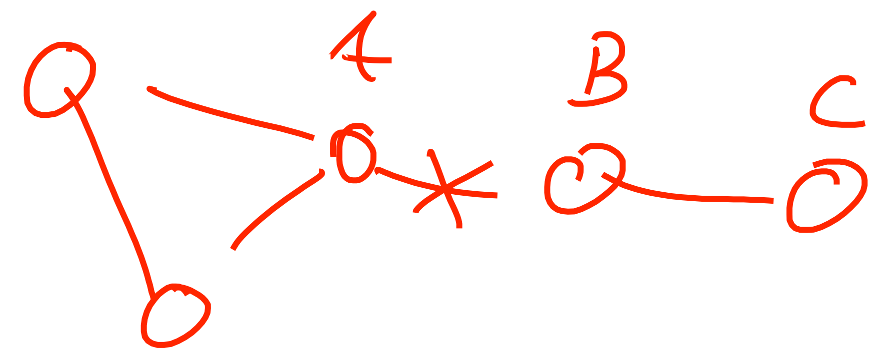


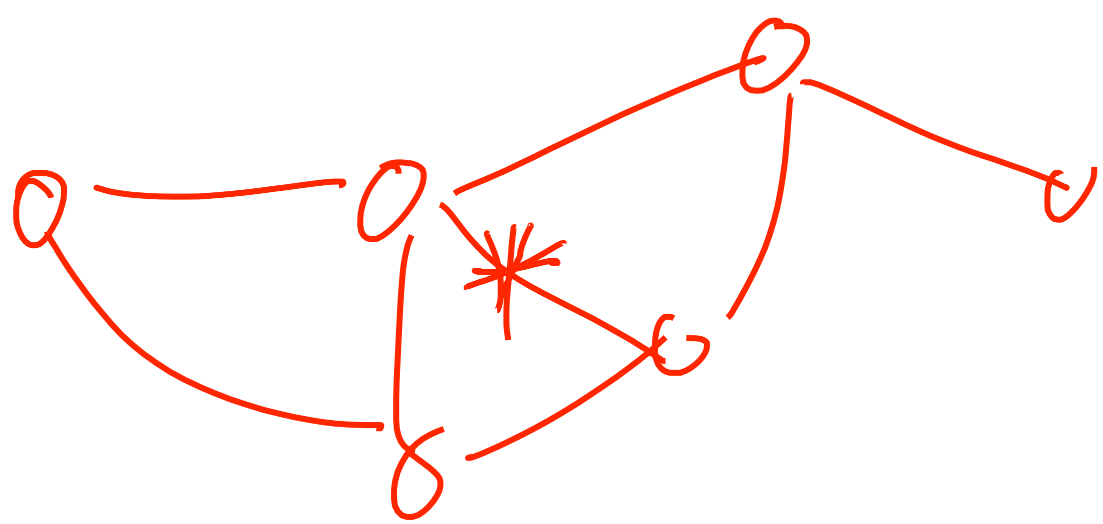
from B to	via			Entry
	A	C	D	
A	1	8	-	A
C	-	5	-	C
D	-	13	1	D
E	-	6	8	C

from C to	via			Entry
	A	B	E	
A	3	6	-	A
B	-	5	-	B
D	-	6	8	B
E	-	13	1	E

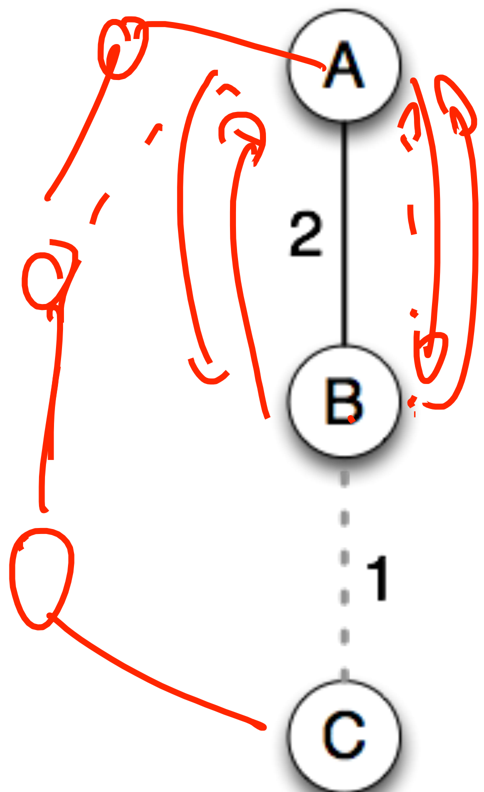
"Count to Infinity" - Problem

- Good news travels fast
  - A new connection is quickly at hand
- Bad news travels slowly
  - Connection fails
  - Neighbors increase their distance mutally
  - "Count to Infinity" Problem





"Count to Infinity" - Problem



from A	via B	Routing Table entry
to B	2	B
C	3	B

from B	via A	via C	Routing Table entry
to A	2	-	A
C	5	-	A

from A	via B	Routing Table entry
to B	2	B
C	7	B

from B	via A	via C	Routing Table entry
to A	2	-	A
C	5	-	A

from A	via B	Routing Table entry
to B	2	B
C	7	B

from B	via A	via C	Routing Table entry
to A	2	-	A
C	9	-	A

Path-Vector

BGP

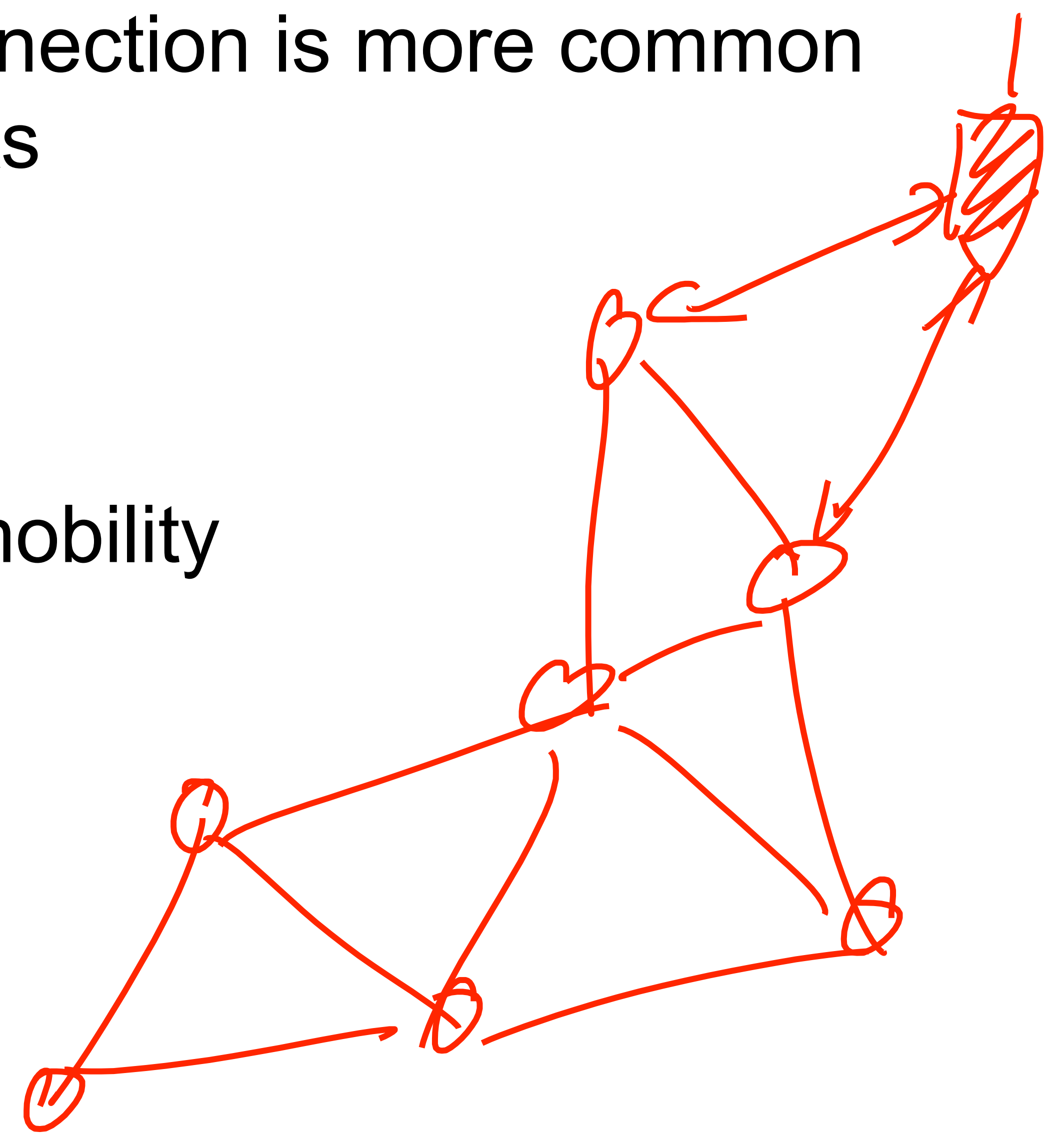
Border Gateway Protocol

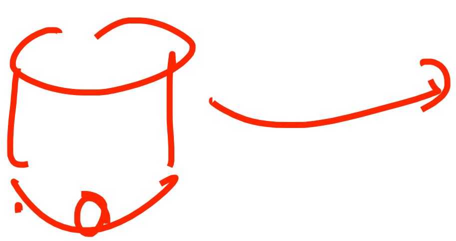
Link-State Protocol

- Link state routers
  - exchange information using Link State Packets (LSP)
  - each node uses shortest path algorithm to compute the routing table
- LSP contains
  - ID of the node generating the packet
  - Cost of this node to any direct neighbors
  - Sequence-no. (SEQNO)
  - TTL field for that field (time to live)
- Reliable flooding (Reliable Flooding)
  - current LSP of each node are stored
  - Forward of LSP to all neighbors
    - except to be node where it has been received from
  - Periodically creation of new LSPs
    - with increasing SEQNO
  - Decrement TTL when LSPs are forwarded

Characteristics of routing in mobile ad hoc networks

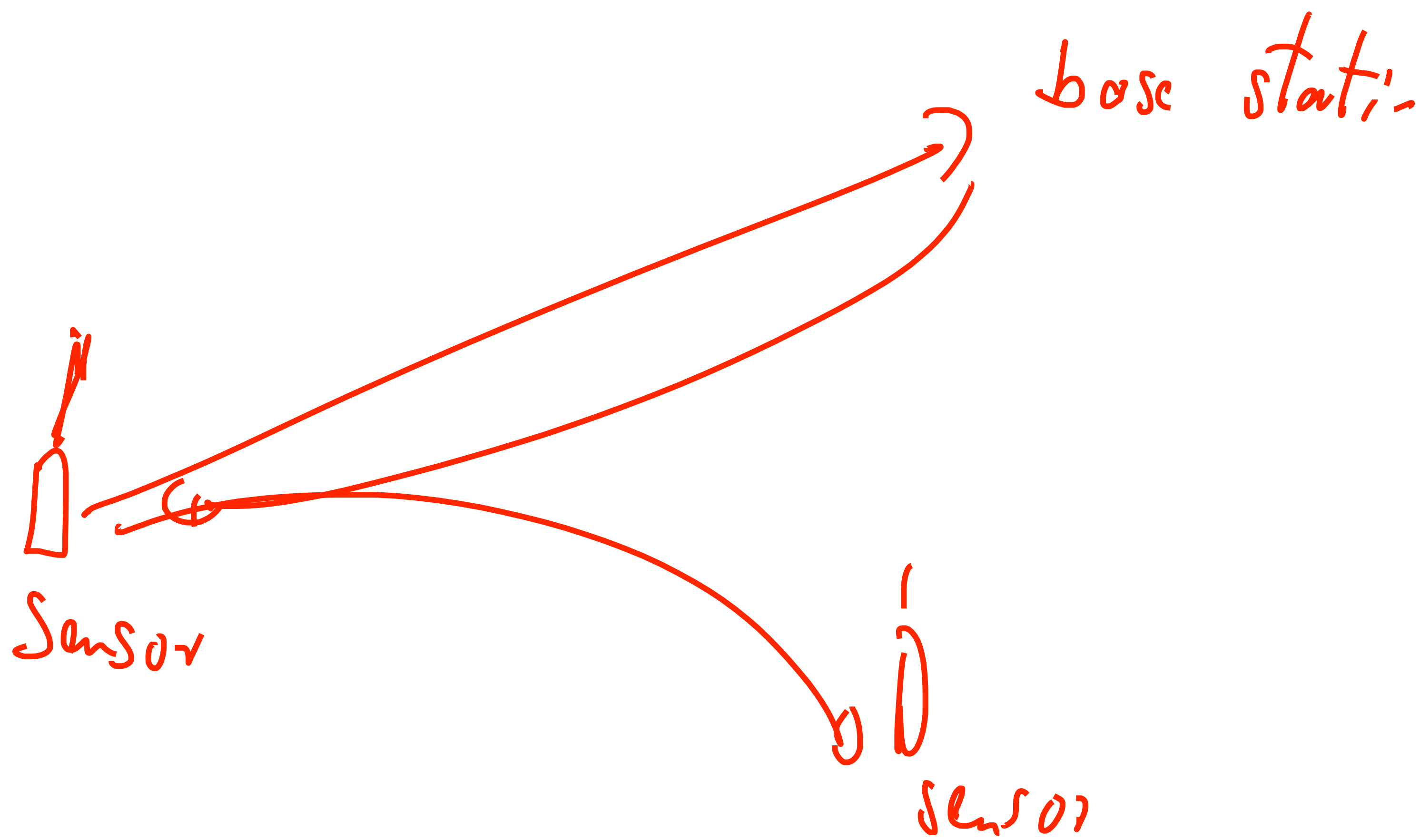
- Movement of participants
  - Reconnecting and loss of connection is more common than in other wireless networks
  - Especially at high speed
- Other performance criteria
  - Route stability in the face of mobility
  - energy consumption





Unicast Routing

- Variety of protocols
  - Adaptations and new developments
- No protocol dominates the other in all situations
  - Solution: Adaptive protocols?



Routing in MANETs

- Routing
  - Determination of message paths
  - Transport of data
- Protocol types
  - proactive
    - Routing tables with updates
  - reactive
    - repairm of message paths only when necessary
  - hybrid
    - combination of proactive and reactive

Routing Protocols

- **Proactive**
  - Routes are **demand independent**
  - Standard Link-State und Distance-Vector Protocols
    - Destination Sequenced Distance Vector (**DSDV**)
    - Optimized Link State Routing (**OLSR**)

- **Reactive**
  - Route are determined when needed
    - Dynamic Source Routing (**DSR**)
    - Ad hoc On-demand Distance Vector (**AODV**)
    - Dynamic MANET On-demand Routing Protocol
    - Temporally Ordered Routing Algorithm (**TORA**)

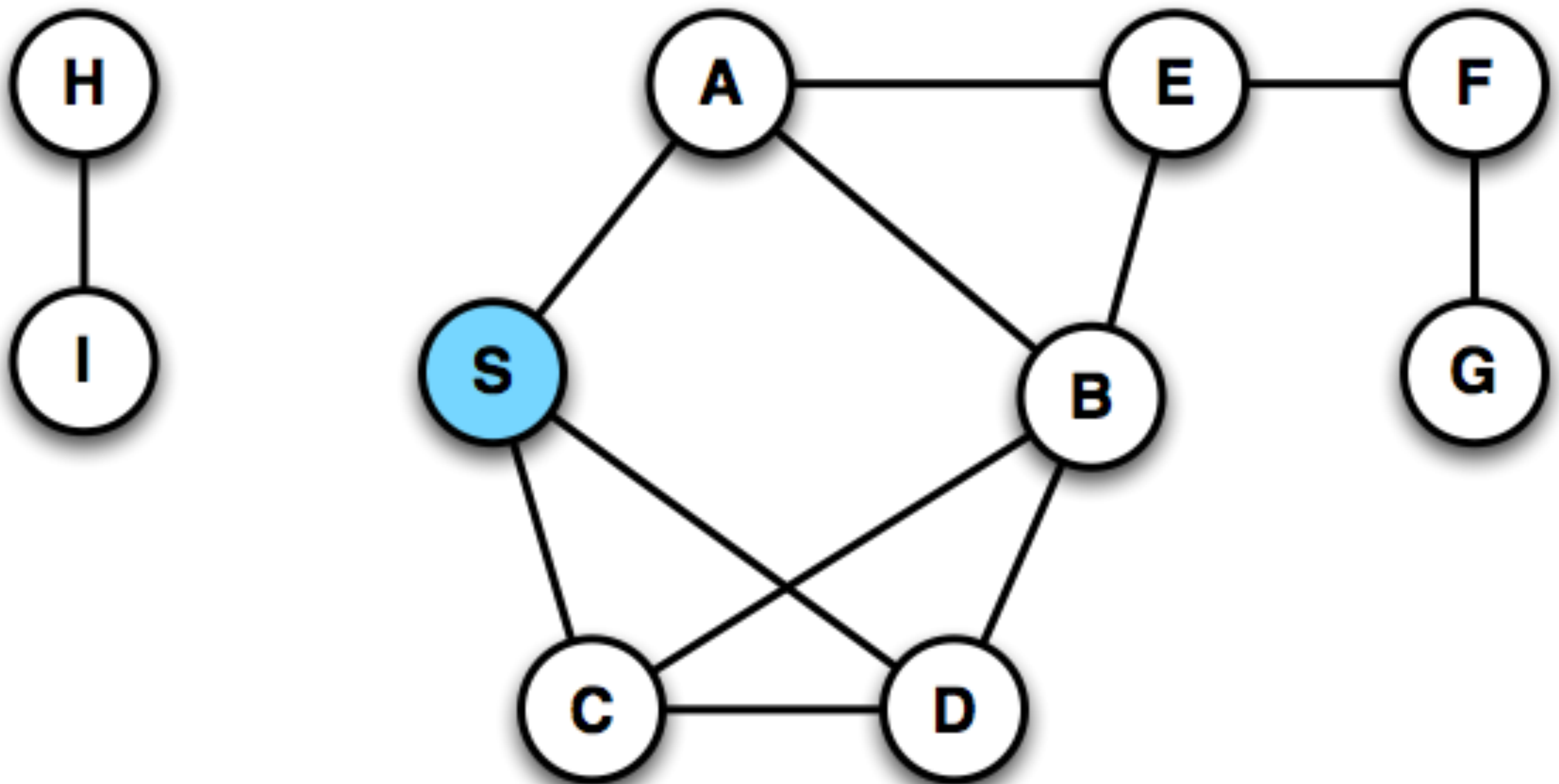
- **Hybrid**
  - combination of reactive und proactive
    - Zone Routing Protocol (**ZRP**)
    - Greedy Perimeter Stateless Routing (**GPSR**)

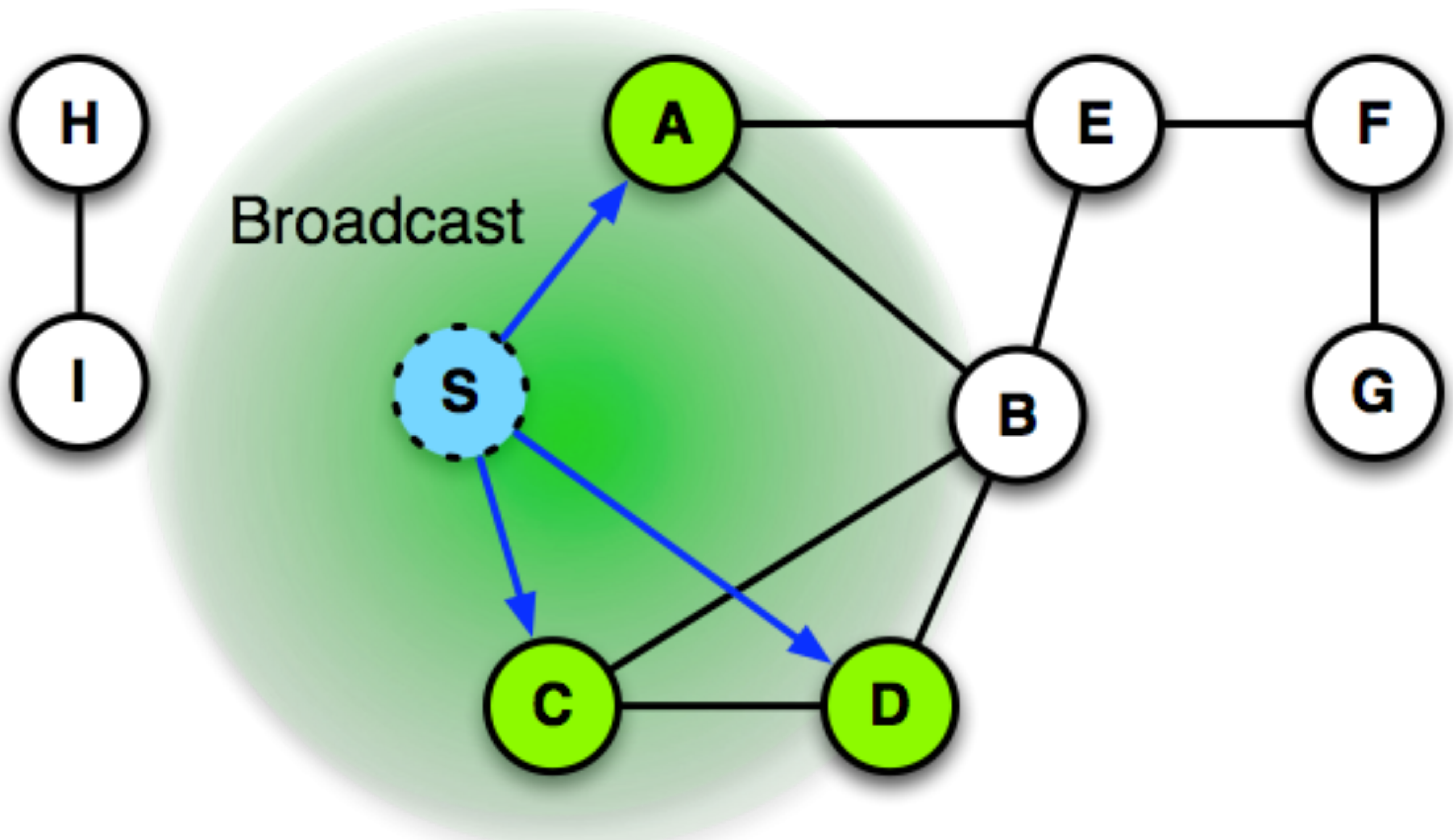
Trade-Off

- Latency because of route discovery
  - Proactive protocols are faster
  - Reactive protocols need to find routes
- Overhead of Route discovery and maintenance
  - Reactive protocols have smaller overhead (number of messages)
  - Proactive protocols may have larger complexity
- Traffic-Pattern and mobility
  - decides which type of protocol is more efficient

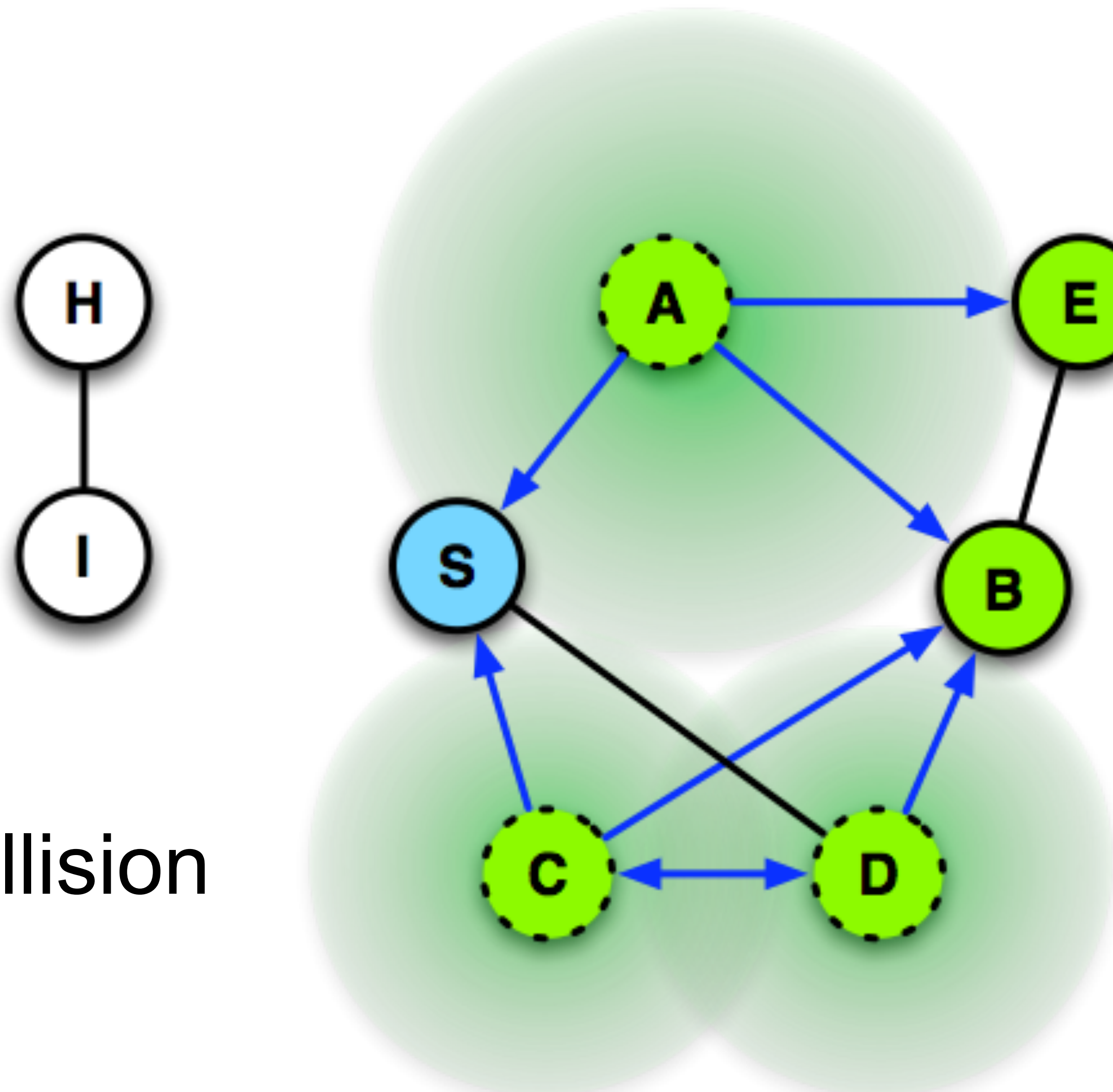
Flooding

- Algorithm
  - Sender S broadcasts data packet to all neighbors
  - Each node receiving a new packet
    - broadcasts this packet
    - if it is not the receiver
- Sequence numbers
  - identifies messages to prevent duplicates
- Packet always reaches the target
  - if possible


H
I
A
E
F
S
B
G
C
D

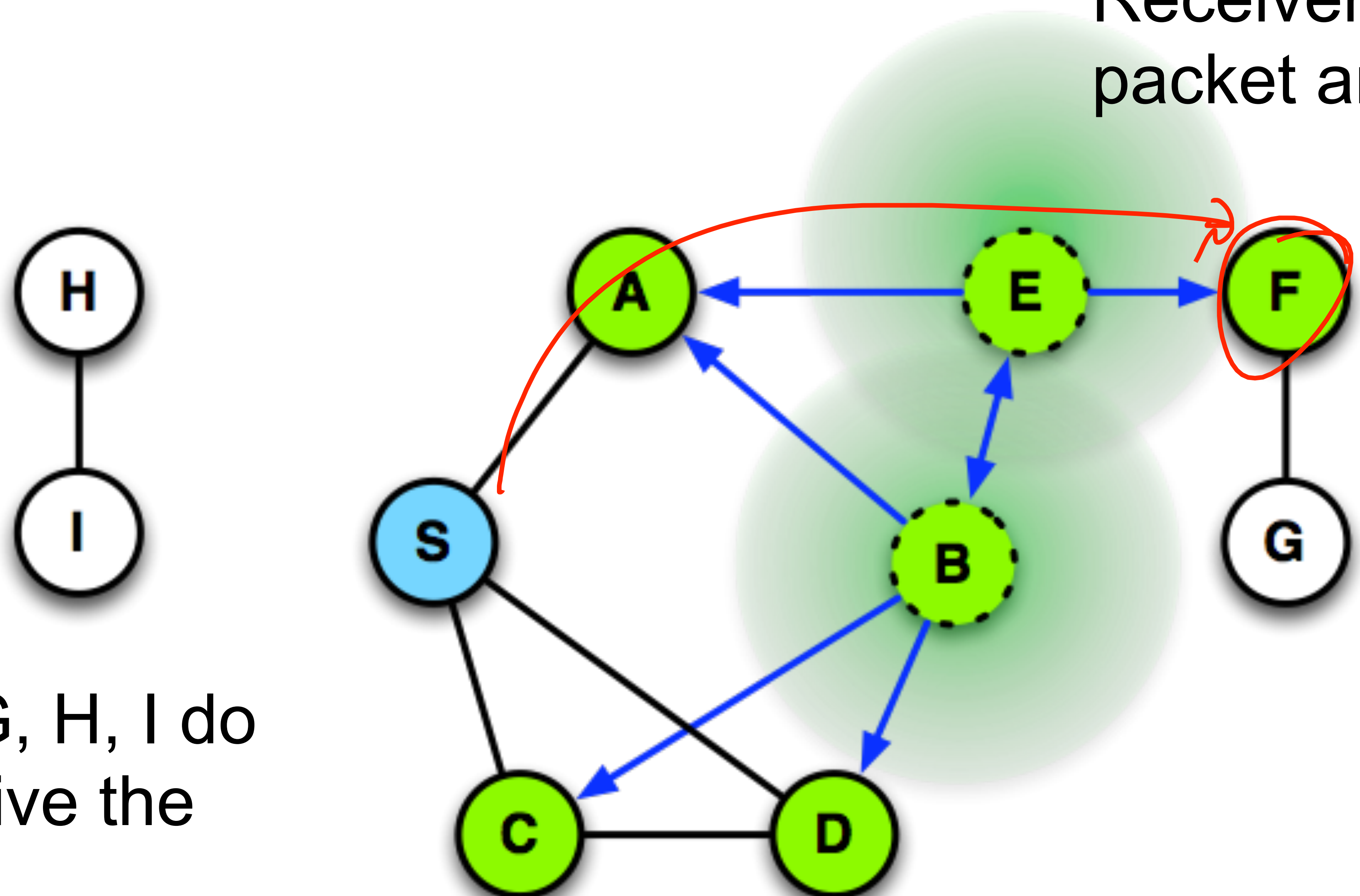


Packet for Receiver F



Possible collision
at B

Receiver F gets packet and stops



Nodes G, H, I do not receive the packet

Flooding

- Advantage
  - simple and robust
  - the best approach for short packet lengths, small number of participants in highly mobile networks with light traffic
- Disadvantage
  - High overhead
  - Broadcasting is unreliable
    - lack of acknowledgements
    - hidden, exposed terminals lead to data loss or delay