CMSC417

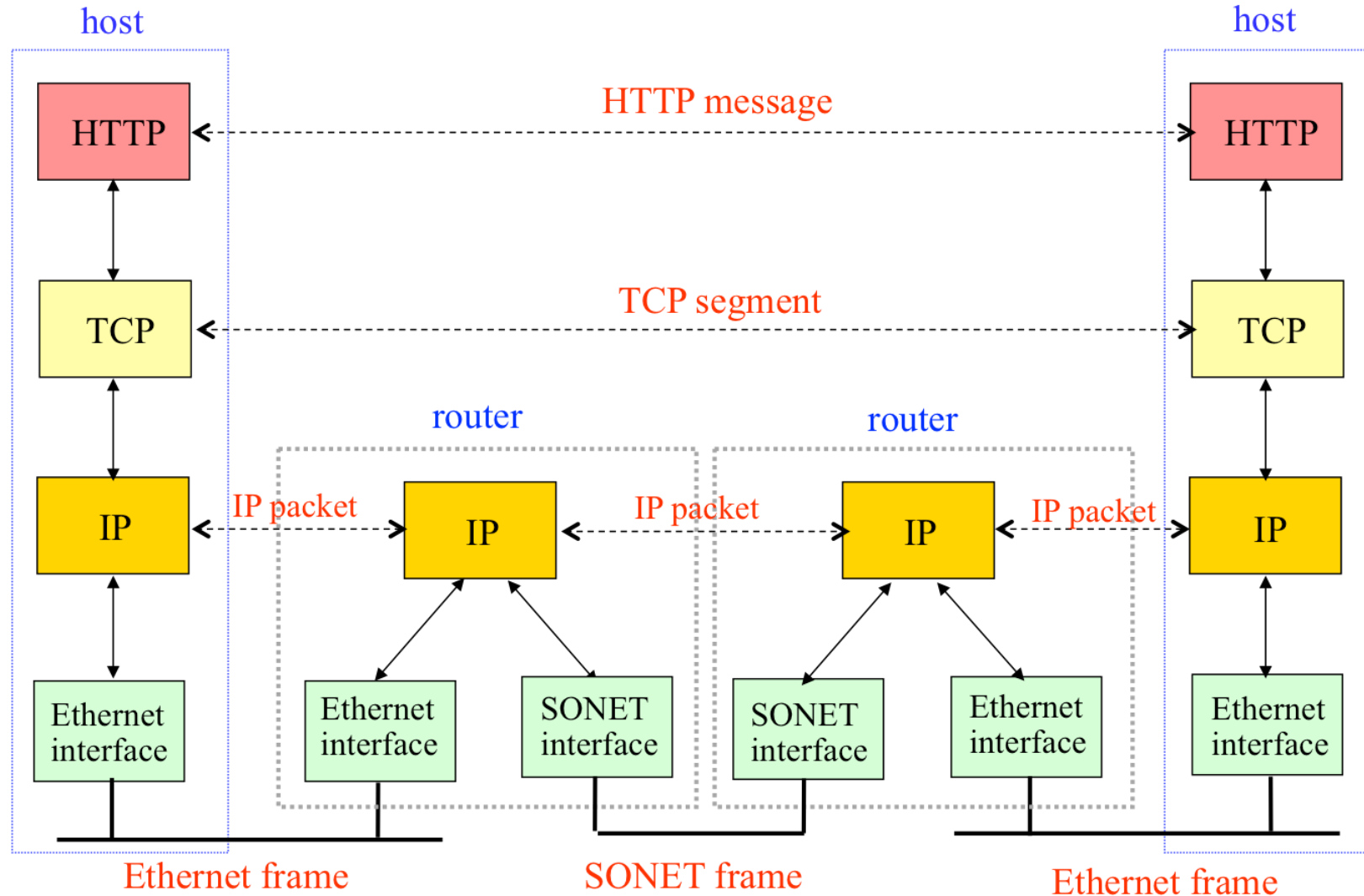# Computer Networks
Prof. Ashok K. Agrawala
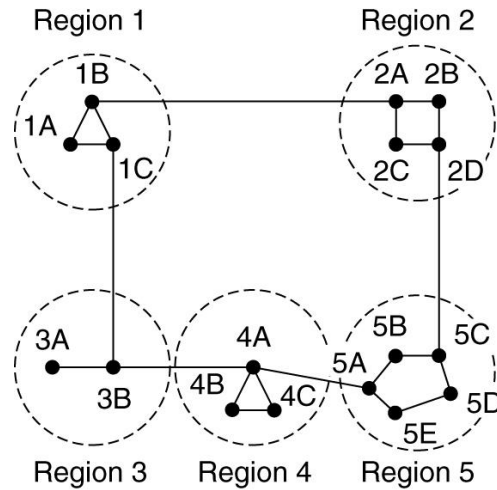
© 2017 Ashok Agrawala

September 25, 2018

Message, Segment, Packet, and Frame

Hierarchical Routing

Region 1 · Region 2 · Region 3 · Region 4 · Region 5

(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

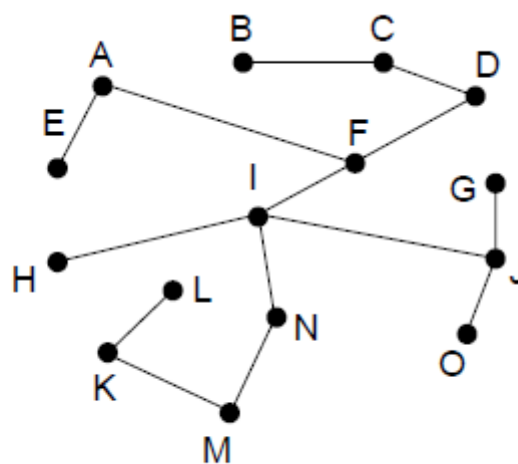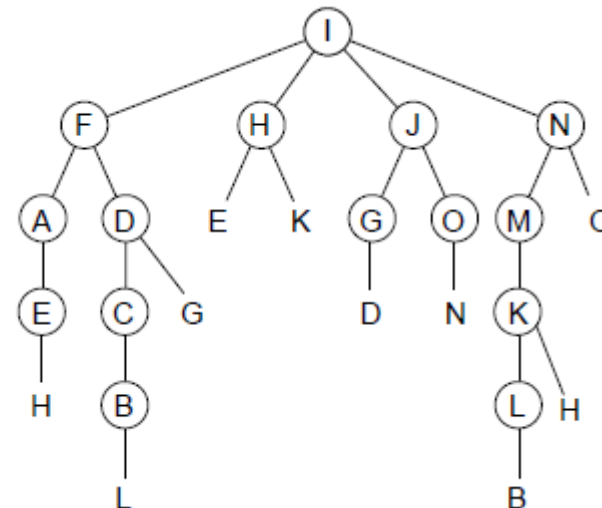| Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Broadcast Routing

- Broadcast sends a packet to all nodes
  - RPF (Reverse Path Forwarding): send broadcast received on the link to the source out all remaining links
  - Alternatively, can build and use sink trees at all nodes
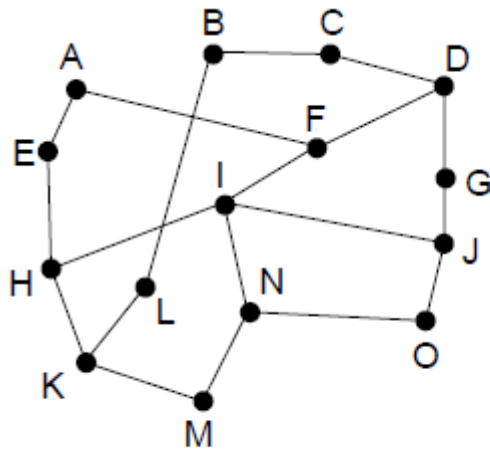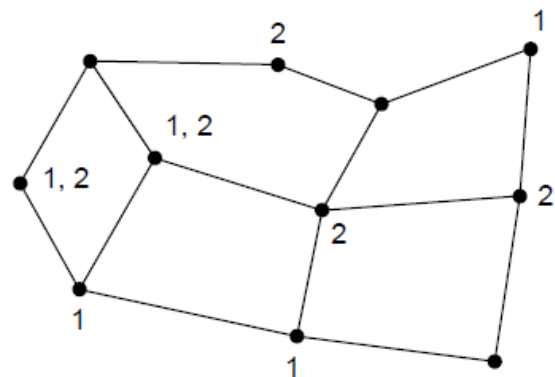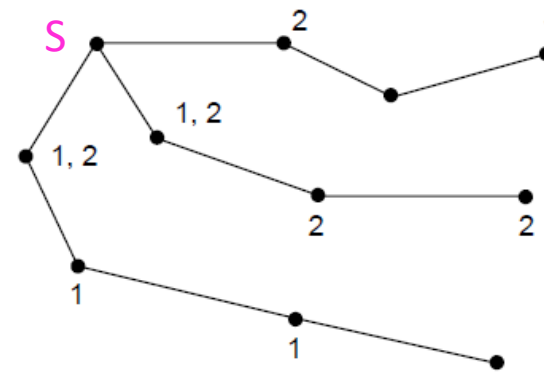

Network

Sink tree for *I* is efficient broadcast

RPF from *I* is larger than sink tree
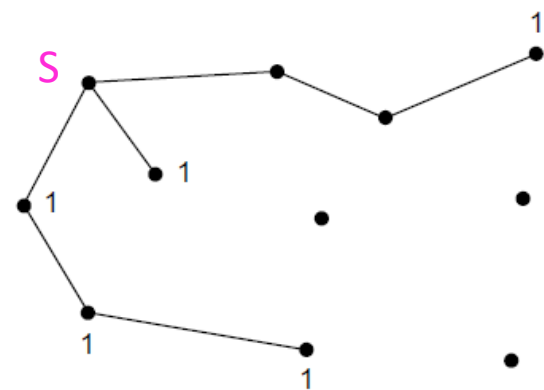
Multicast Routing (1) – Dense Case

- Multicast sends to a subset of the nodes called a group
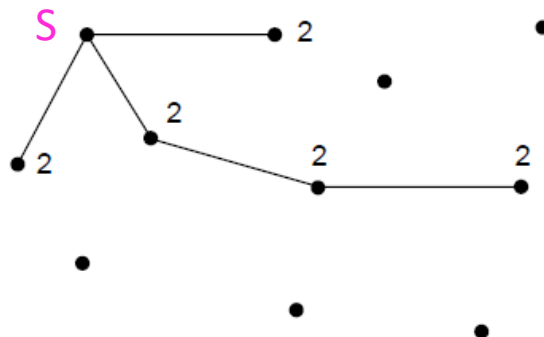 - Uses a different tree for each group and source

Network with groups 1 & 2

Spanning tree from source S

Multicast tree from S to group 1
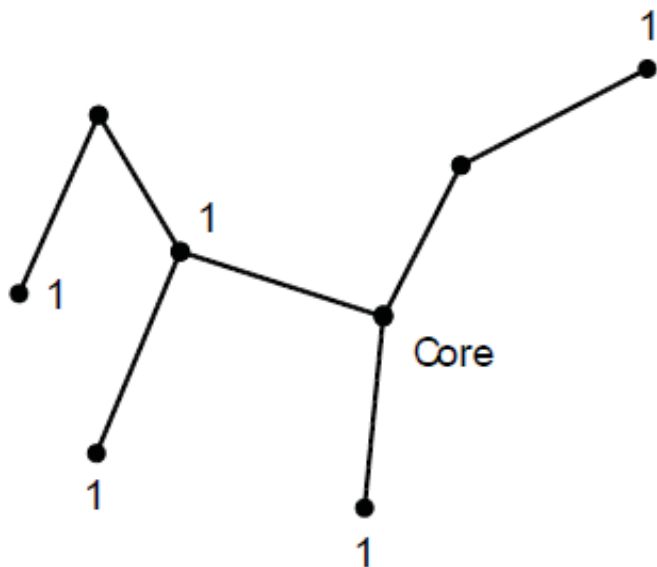
Multicast tree from S to group 2

Multicast Routing (2) – Sparse Case

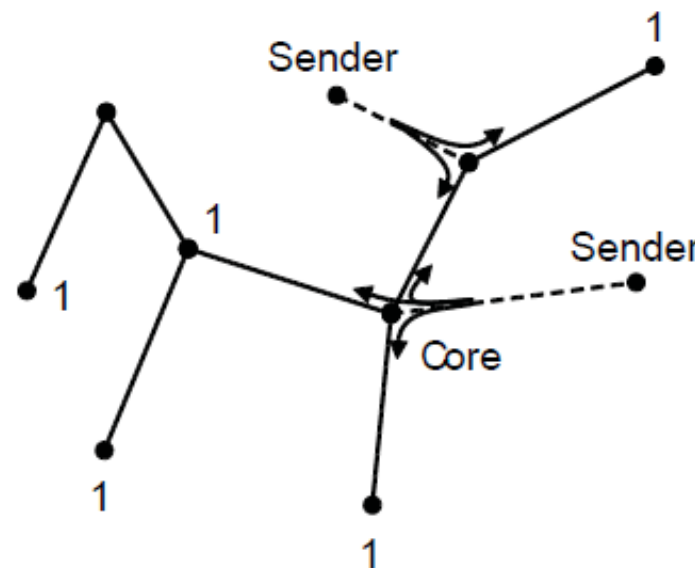- CBT (Core-Based Tree) uses a single tree to multicast
  - Tree is the sink tree from core node to group members
  - Mul
- p 1.

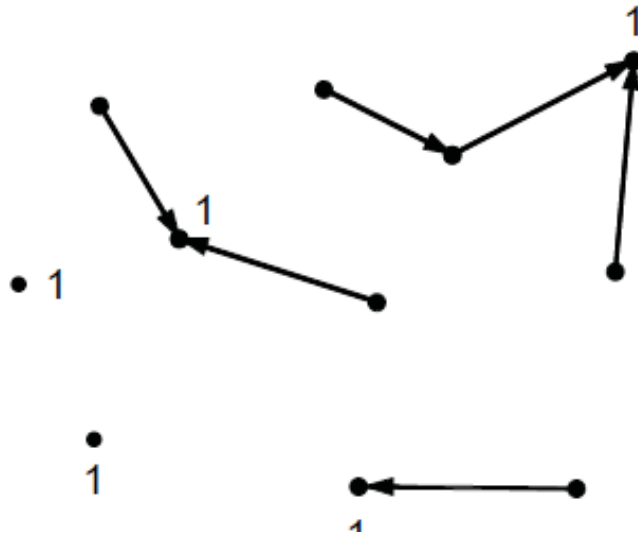
Sink tree from core to group 1

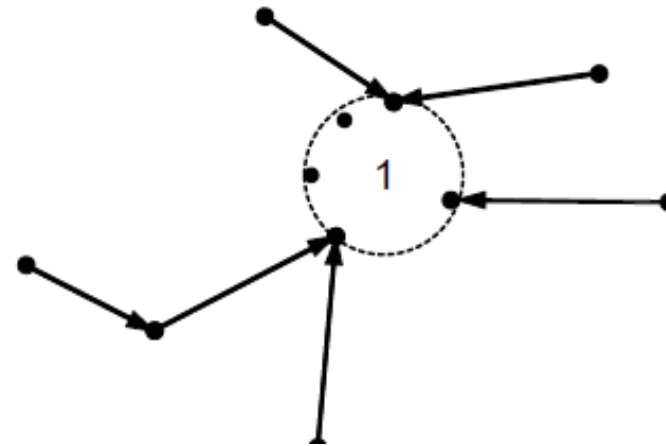Multicast is send to the core then down when it reaches the sink tree

Anycast Routing

Anycast sends a packet to one (nearest) group member

- Falls out of regular routing with a node in many places
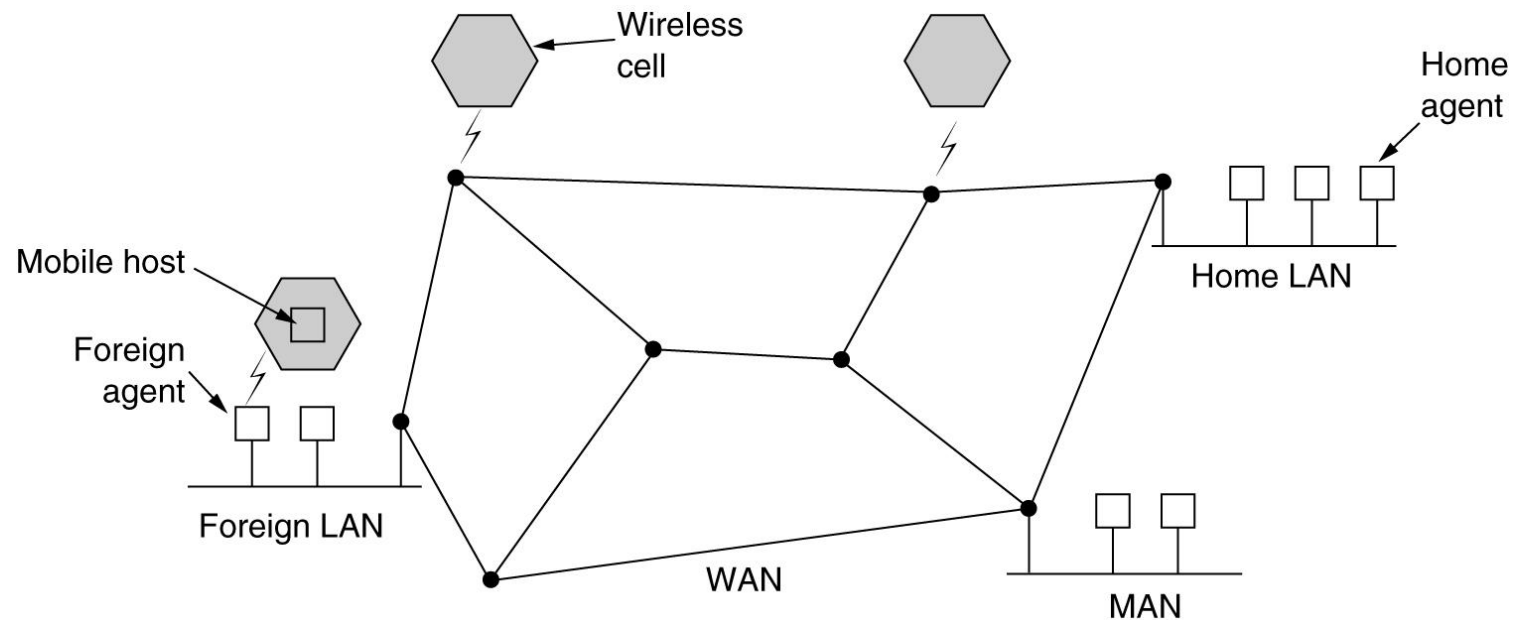

Anycast routes to group 1
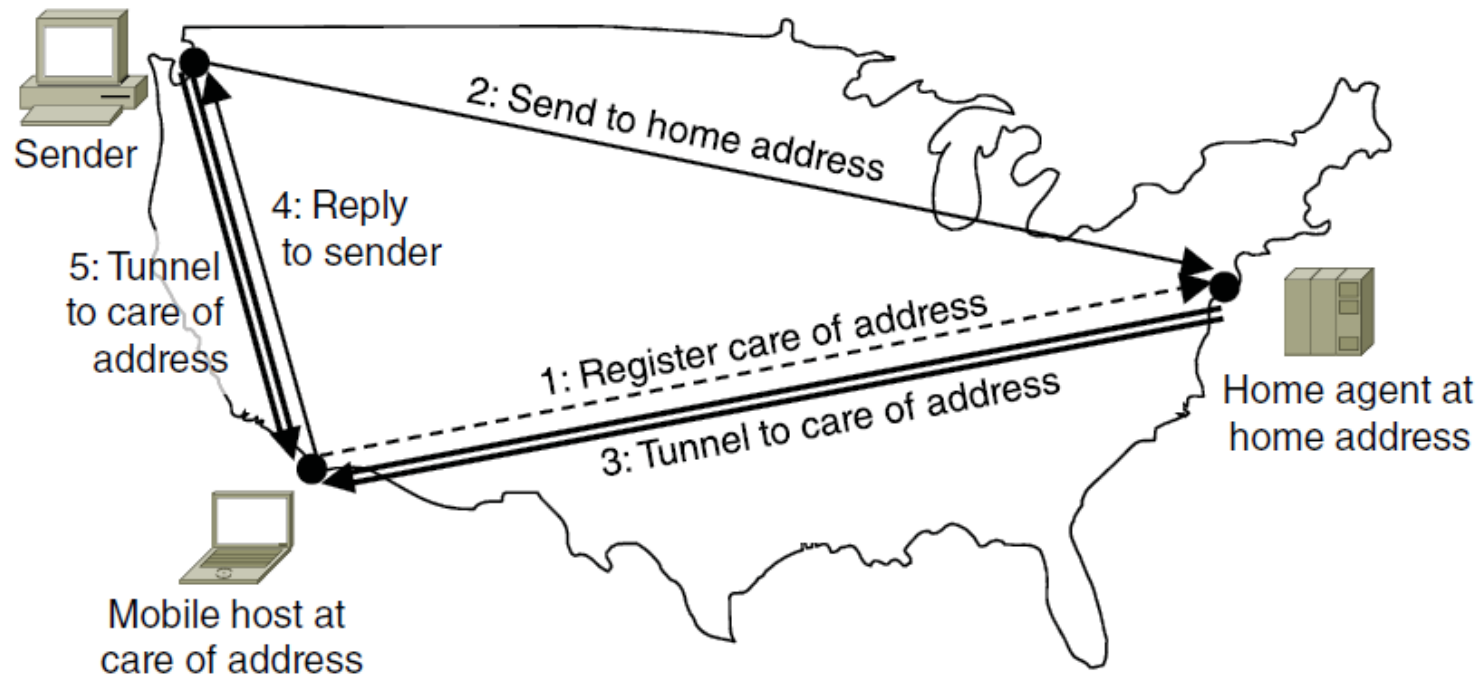
Apparent topology of sink tree to "node" 1

Routing for Mobile Hosts

A WAN to which LANs, MANs, and wireless cells are attached.

Routing for Mobile Hosts

- Mobile hosts can be reached via a home agent
  - Fixed home agent tunnels packets to reach the mobile host; reply can optimize path for subsequent packets
  - No changes to routers or fixed hosts

Routing in Ad Hoc Networks

Possibilities when the routers are mobile:

1. Military vehicles on battlefield.

   - No infrastructure.

2. A fleet of ships at sea.
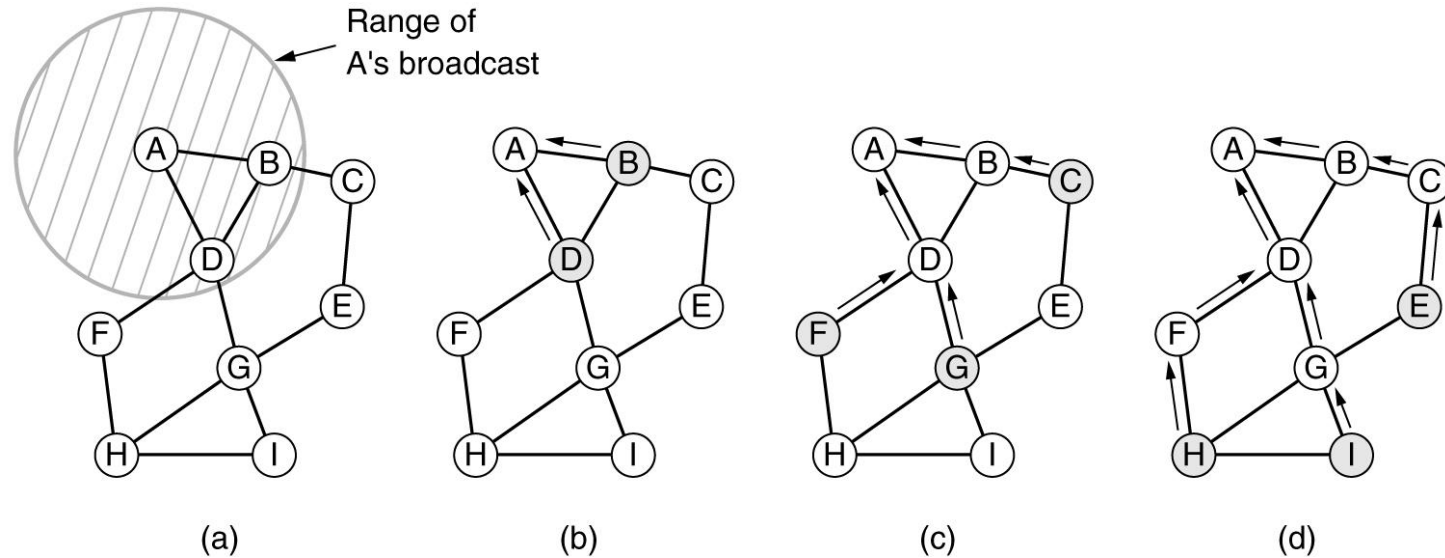
   - All moving all the time

3. Emergency works at earthquake .

   - The infrastructure destroyed.

4. A gathering of people with notebook computers.

   - In an area lacking 802.11.

Route Discovery

(a)   (b)   (c)   (d)

- (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.

Route Discovery (2)

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

Format of a ROUTE REQUEST packet.

Route Discovery (3)

Source address	Destination address	Destination sequence #	Hop count	Lifetime

Format of a ROUTE REPLY packet.

Route Maintenance

| 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)
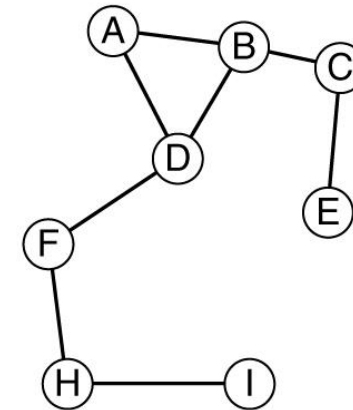
(b)

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

Congestion Control

- General Principles of Congestion Control
- Congestion Prevention Policies
- Congestion Control in Virtual-Circuit Subnets
- Congestion Control in Datagram Subnets
- Load Shedding
- Jitter Control

Congestion
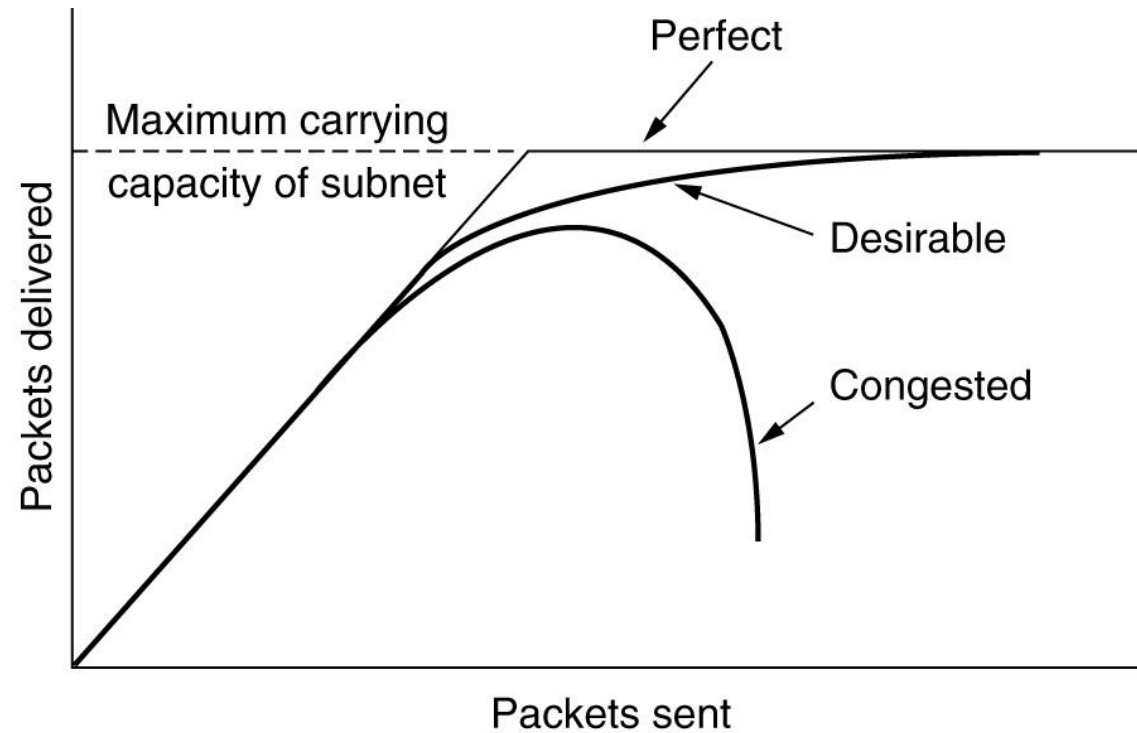
When too much traffic is offered, congestion sets in and performance degrades sharply.
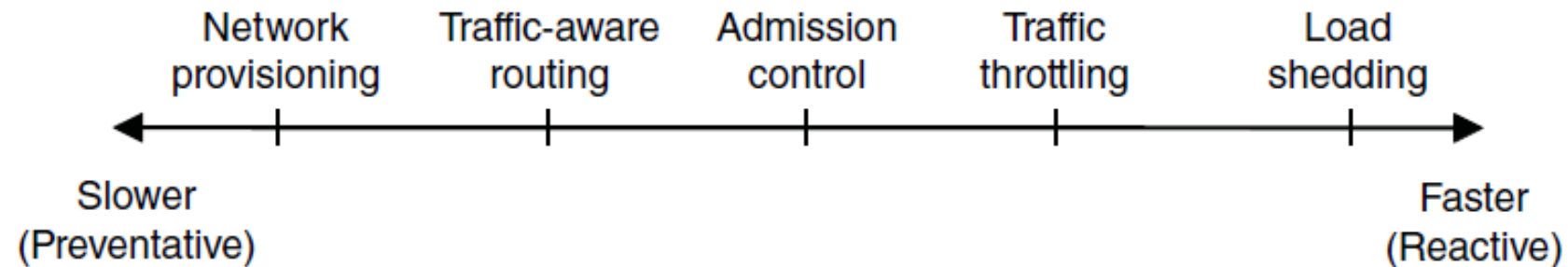
General Principles of Congestion Control

1. Monitor the system .
   - detect when and where congestion occurs.
2. Pass information to where action can be taken.
3. Adjust system operation to correct the problem.

Congestion Control (3) – Approaches

Network must do its best with the offered load
- Different approaches at different timescales
- Nodes should also reduce offered load (Transport)

Network provisioning	Traffic-aware routing	Admission control	Traffic throttling	Load shedding

Slower (Preventative) ←———————————————————→ Faster (Reactive)

Congestion Prevention Policies

| Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Congestion Control in Virtual-Circuit Subnets
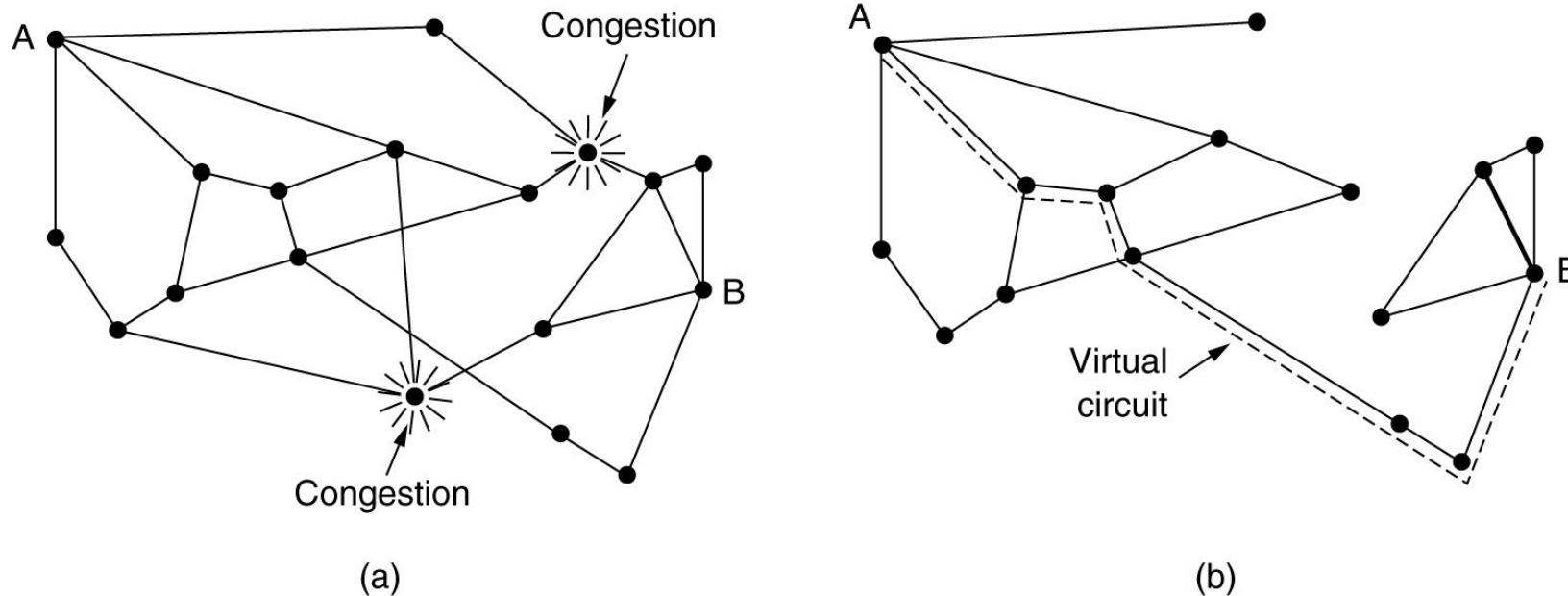
(a) A congested subnet. (b) A redrawn subnet, eliminates congestion and a virtual circuit from A to B.

Traffic-Aware Routing

Choose routes depending on traffic, not just topology
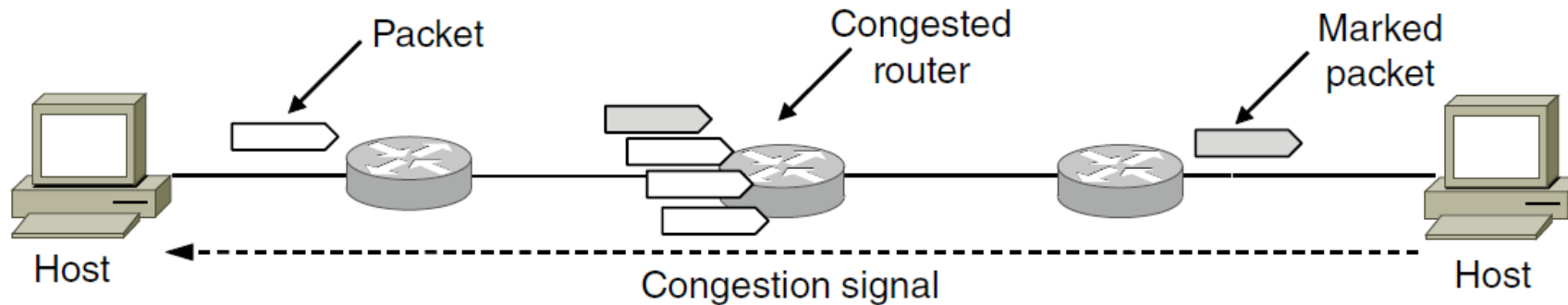
- E.g., use *EI* for West-to-East traffic if *CF* is loaded
- But take care to avoid oscillations
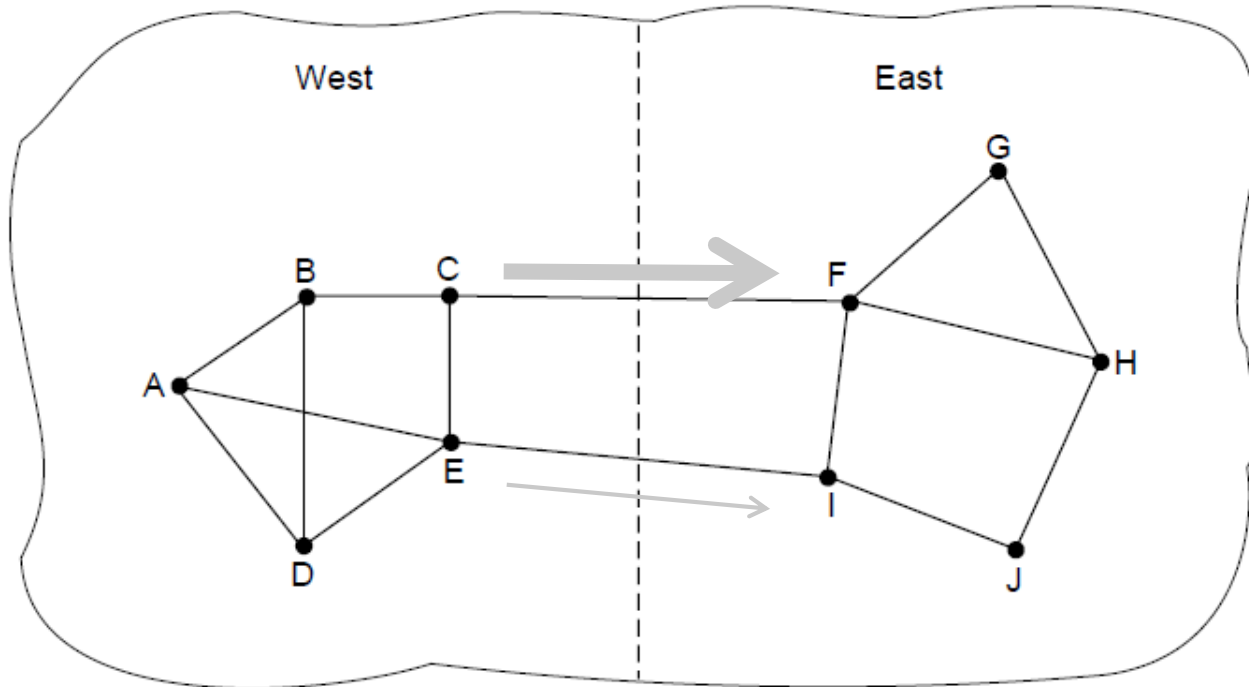
Traffic Throttling

Congested routers signal hosts to slow down traffic

- ECN (Explicit Congestion Notification) marks packets and receiver returns signal to sender
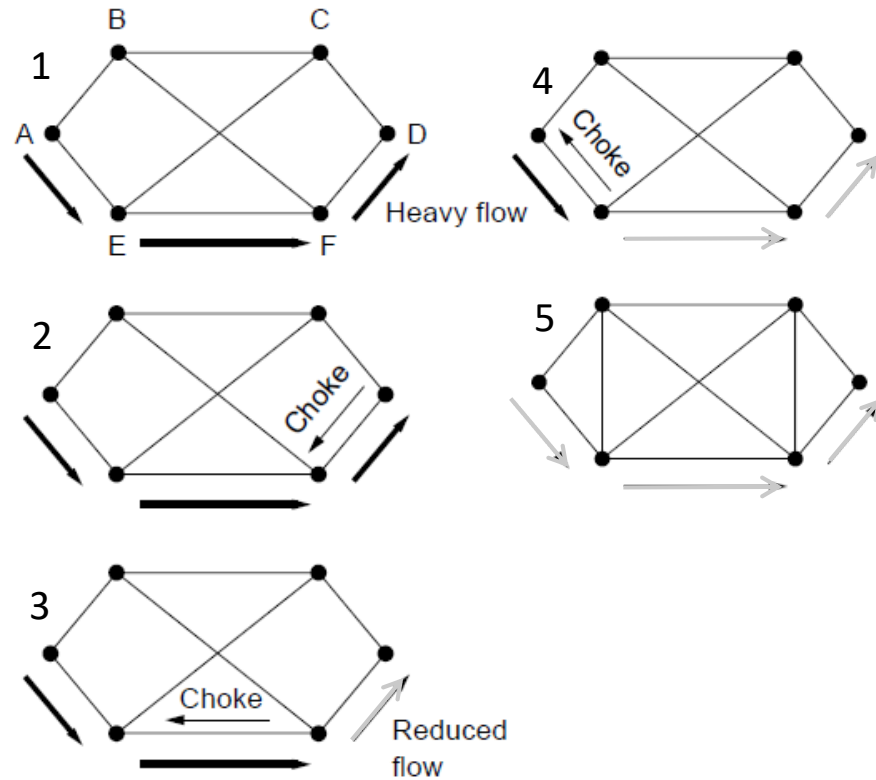
Load Shedding (1)

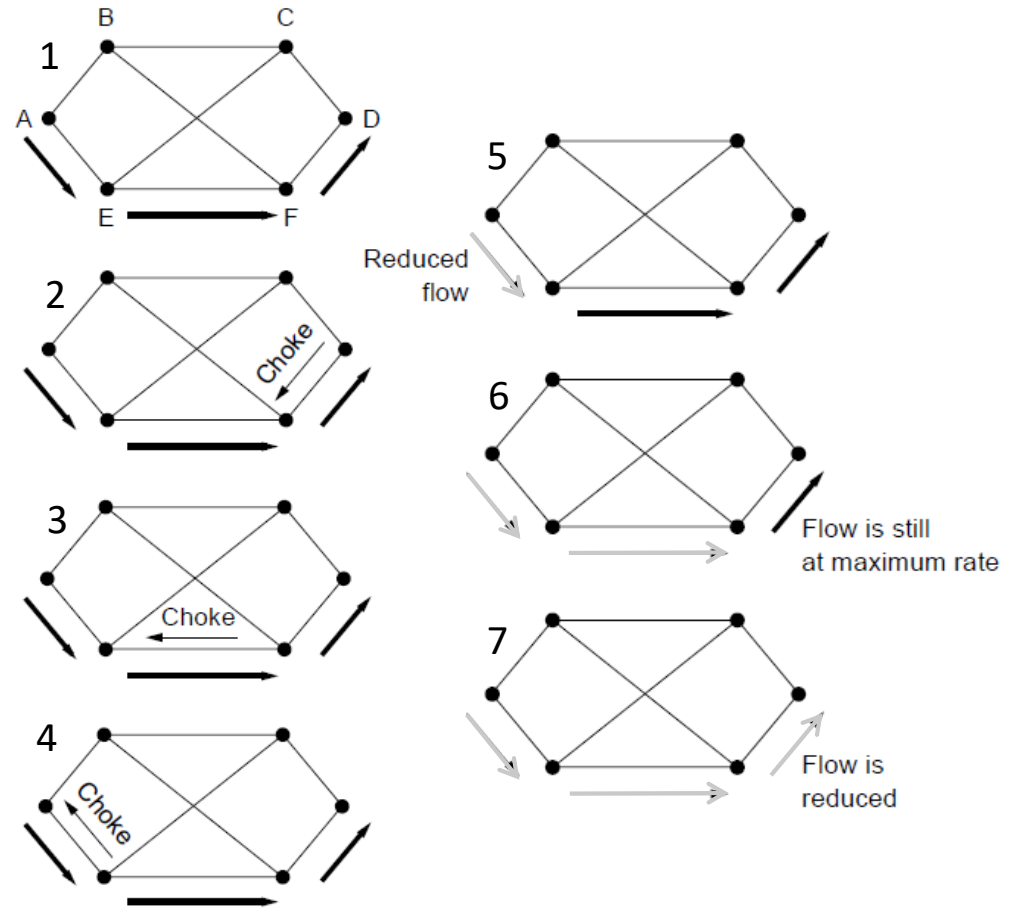When all else fails, network will drop packets (shed load)

Can be done end-to-end or link-by-link

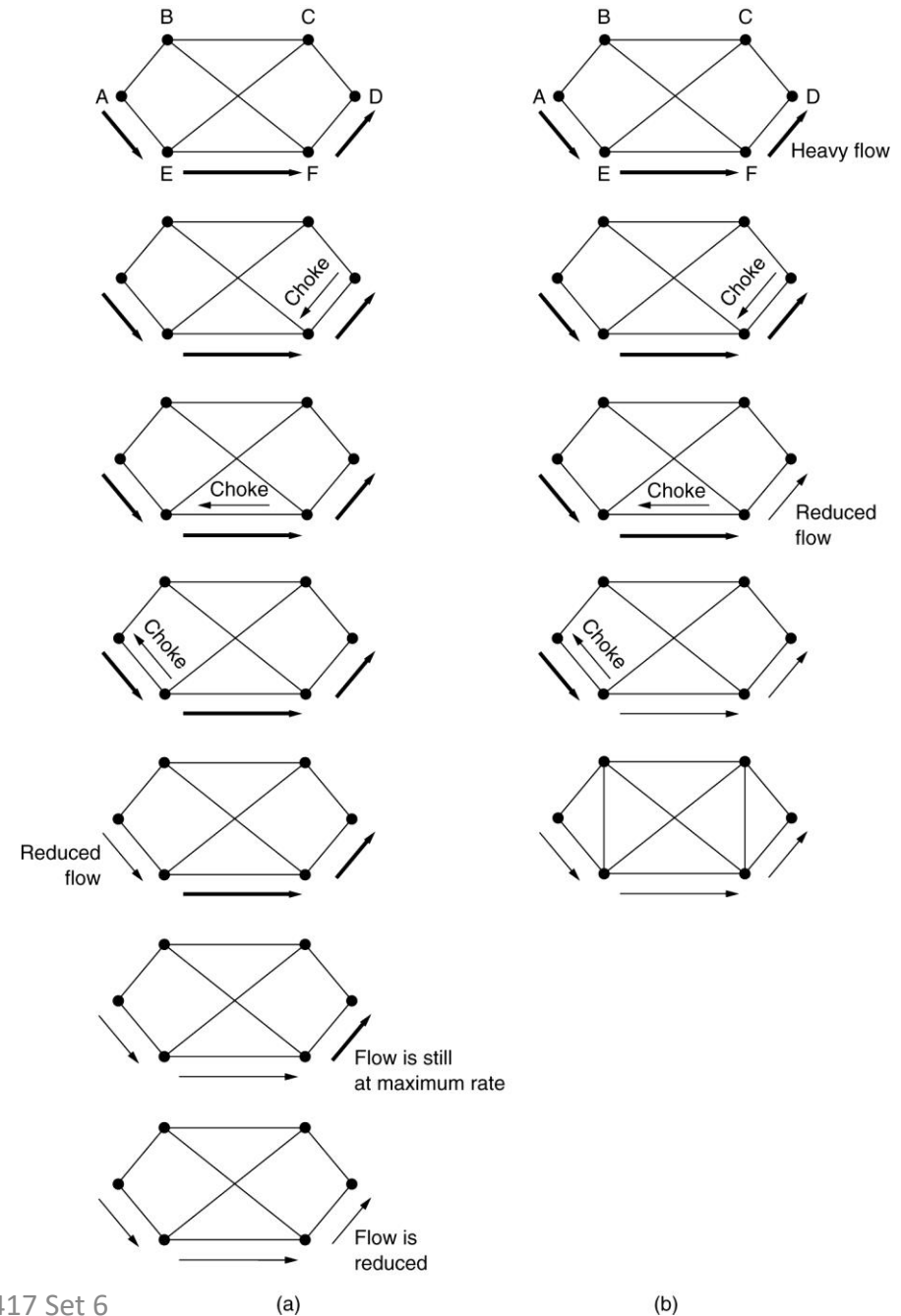Link-by-link (right) produces rapid relief

Load Shedding (2)

End-to-end (right) takes longer to have an effect, but can better target the cause of congestion
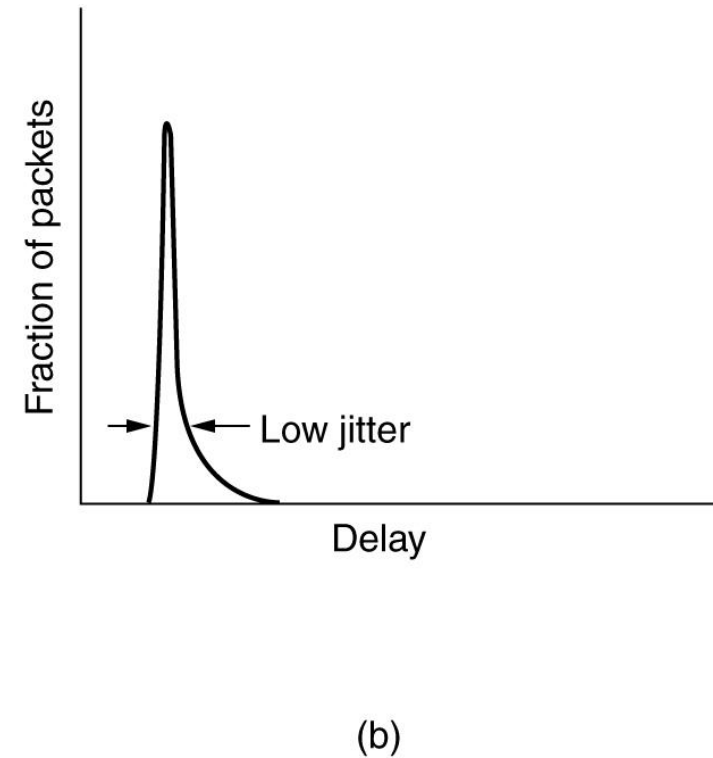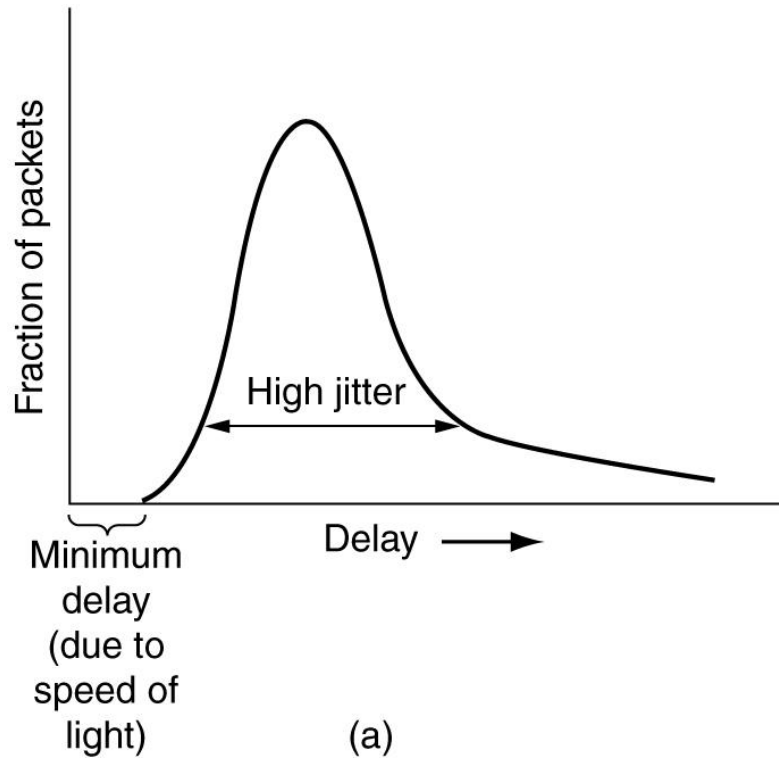
Hop-by-Hop Choke Packets

(a) A choke packet that affects only the source.

(b) A choke packet that affects each hop it passes through.

CMSC417 Set 6 (a) (b)

Jitter Control

(a) High jitter.   (b) Low jitter.