Chapter5 Network Layer(5)

王昊翔 hxwang@scut.edu.cn

School of Computer Science & Engineering ,SCUT

Communication & Computer Network key-Lab of GD

CCNL 广东省计算机网络重点实验室
Communication & Computer Network Lab of GD

華南理工大學

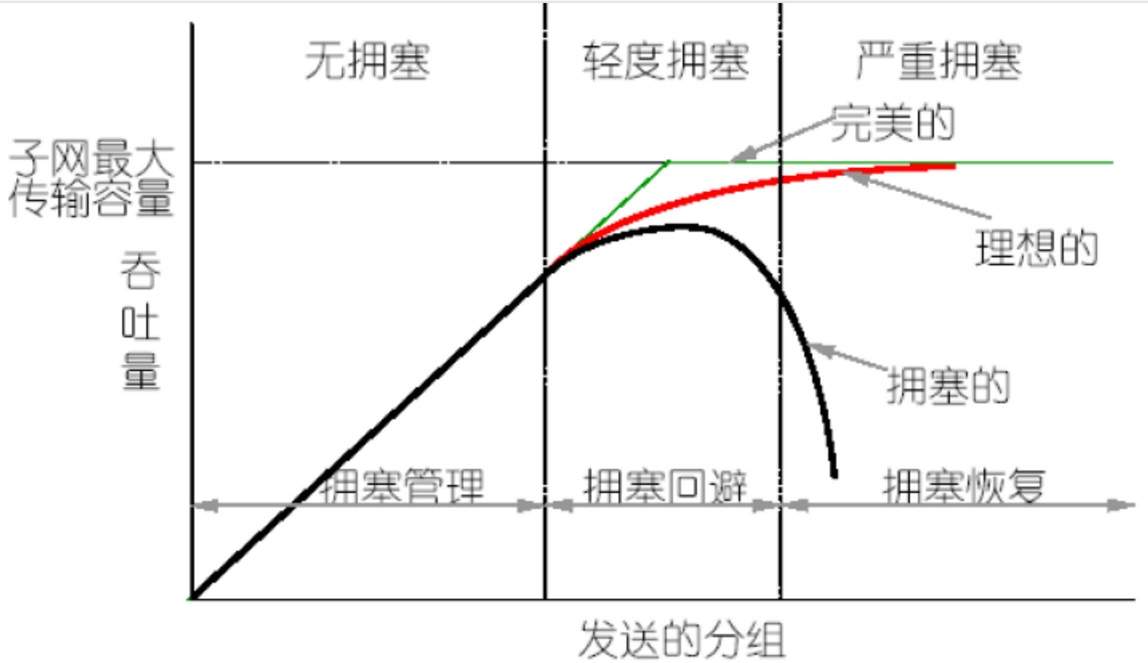
Outline

□ Understanding congestion control

□ Fragmentation

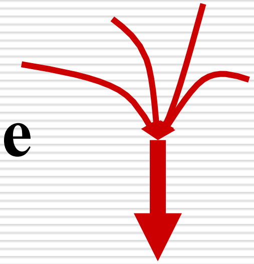
What is congestion?

- □ **Congestion** is a situation in which too **many packets** are present in (a part of) the subnet, performance degrades sharply



Factors Causing Congestion

- □ The input traffic rate exceeds the capacity of the output lines.
  - e.g. Several input lines are forwarded to the same output line.
  - Adding more memory may help up to a point.
  - How about infinite amount of memory?
- □ The processors in routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
- □ Line capacity and processor capability need to be in balance.



Congestion Control vs. Flow Control

- Congestion control
  - It makes sure the subnet is able to carry the offered traffic.
  - It is a global issue involving the behavior of all the hosts, all the routers, the store-and-forwarding processing within the routers, etc.
- Flow control
  - It relates to the point-to-point traffic between a given sender and a given receiver.
  - It makes sure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it.
- A host can get a “slow down” message either because the receiver cannot handle the load or because the network cannot handle it (confused).

Congestion Metrics

1. percentage of all packets discarded for lack of buffer space
2. average queue lengths
3. number of packets that time out and are retransmitted
4. average packet delay
5. standard deviation of packet delay

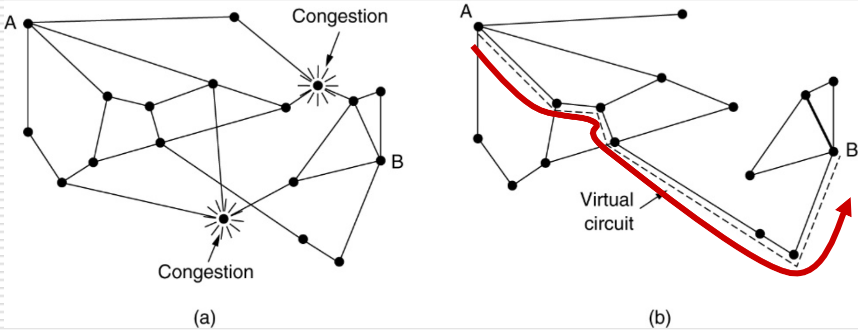
□ Rising numbers indicate growing congestion.

Congestion Information Propagation

- The router detecting the congestion sends a separate warning packet to the traffic source.
- A bit or field can be reserved in each packet. When a router detects a congested state, it fills in the field in all outgoing packets to warn the neighbors.
- Hosts or routers send probe packets out periodically to explicitly ask about congestion and to route traffic around problem areas

Congestion Control In Virt.-circuit Subnets

- Admission control (准入控制，simple but crude)
  - A close loop technique to keep congestion that has already started from getting worse.
  - Basic idea: Once congestion has been signaled, no more virtual circuits are set up until the problem has gone away.
- Alternate Routing（绕过问题区域）
  - Allow new virtual circuits but carefully route all new virtual circuits around problem areas.
- Negotiate an agreement between the host and subnet, so that the subnet can reserve resources along the path when the circuit is set up.（资源预留）
  - volume and shape of the traffic
  - quality of service required
  - other parameters

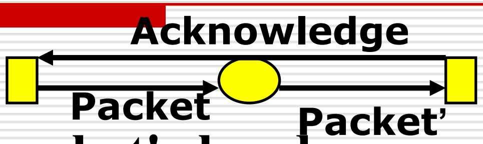


Congestion Control In Datagram Subnets

- □ Each router can monitor the utilization of its output lines and other resources.
- □ Each line is associated with a variable u, whose value (0.0 -1.0) reflects the recent utilization.
- □ Whenever u moves above the threshold, the output line enters a warning state.
- □ Each newly-arriving packet is checked to see if its output line is in warning state.

Actions When In Warning State

- The Warning Bit（警告位）

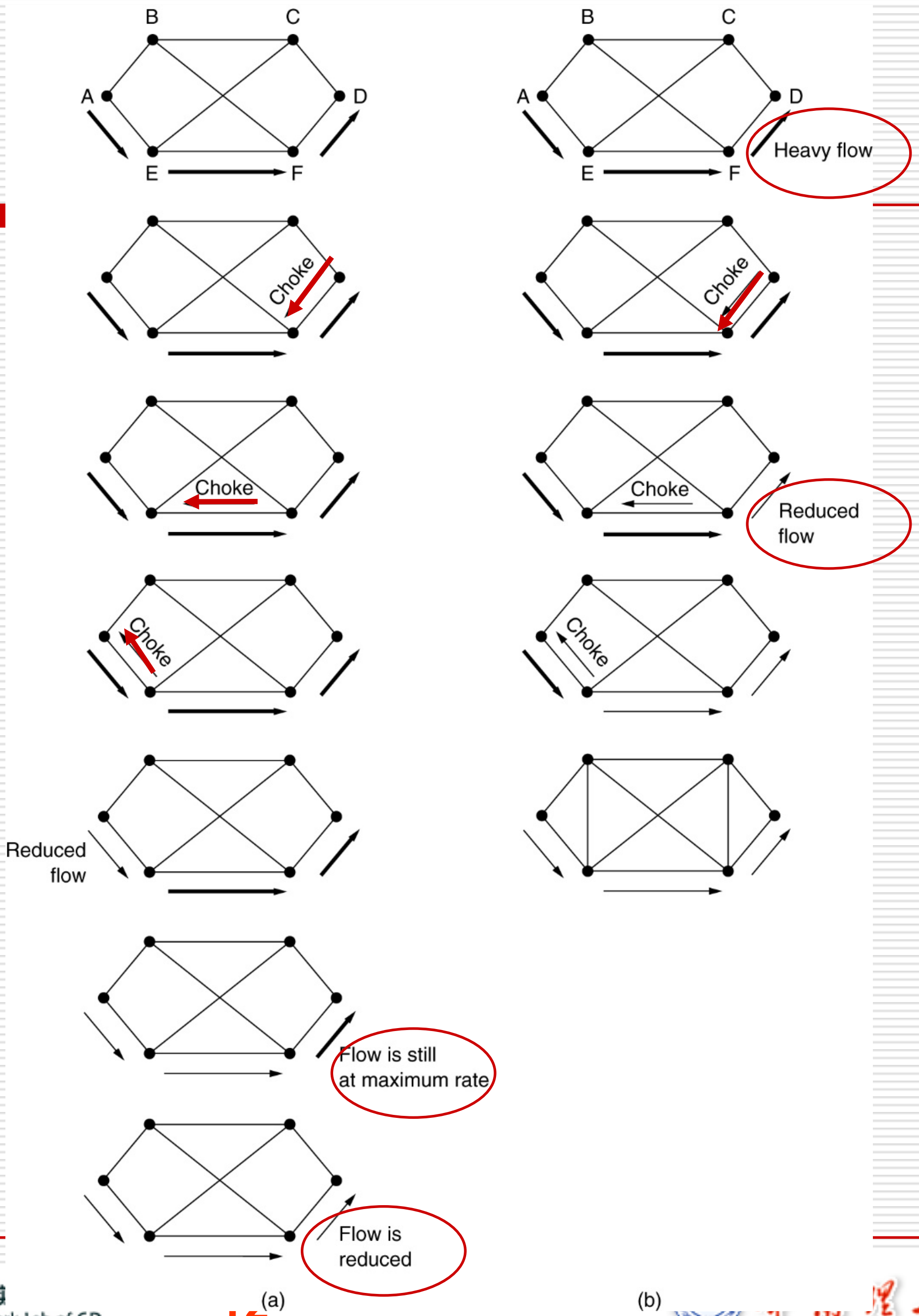


  - A special bit is set in the packet's header.
  - the bit is copied into the next acknowledgement sent back to the source.
  - The source monitored the fraction of acknowledgements with the bit set and adjusted its transmission rate accordingly.
- Choke Packets（抑制分组）
  - The router sends a choke packet back to the source host, giving it the destination found in the packet.
  - When the source host gets the choke packet, it is required to reduce the traffic to the destination by certain percent.
  - The host should ignore choke packets referring to the same destination for a fixed time interval
  - If no choke packets arrive during the listening period, the host may increase the flow again.

Actions When In Warning State (cont'd)

- Hop-by-Hop Choke Packets（逐跳抑制分组）
  - At high speeds or over long distances, sending a choke packet to the source hosts does not work well because the reaction is so slow.
  - An alternative approach is to have the choke packet take effect at every hop it passes through.
  - The net effect of this hop-by-hop scheme is to provide quick relief at the point of congestion at the price of using up more buffers upstream.

Two Choke


B
C
A
D
E
F
B
C
A
D
E
F
Heavy flow
Choke
Choke
Choke
Choke
Reduced flow
Choke
Choke
Reduced flow
Flow is still at maximum rate
Flow is reduced
(a)
(b)

Fragmentation

- Each network imposes some maximum size on its packets.
  - Hardware (e.g., the width of a TDM transmission slot)
  - Operating system (e.g., all buffers are 512 bytes)
  - Protocols (e.g., the number of bits in the packet length field)
  - Compliance with some (inter) national standard
  - Desire to reduce error induced retransmissions to some level
  - Desire to prevent one packet from occupying the channel too long
- The network designers are not free to choose any maximum packet size they wish.
- Maximum payloads range from 48 bytes (ATM cells) to 65,515 bytes (IP packets), although the payload size in higher layers is often larger.

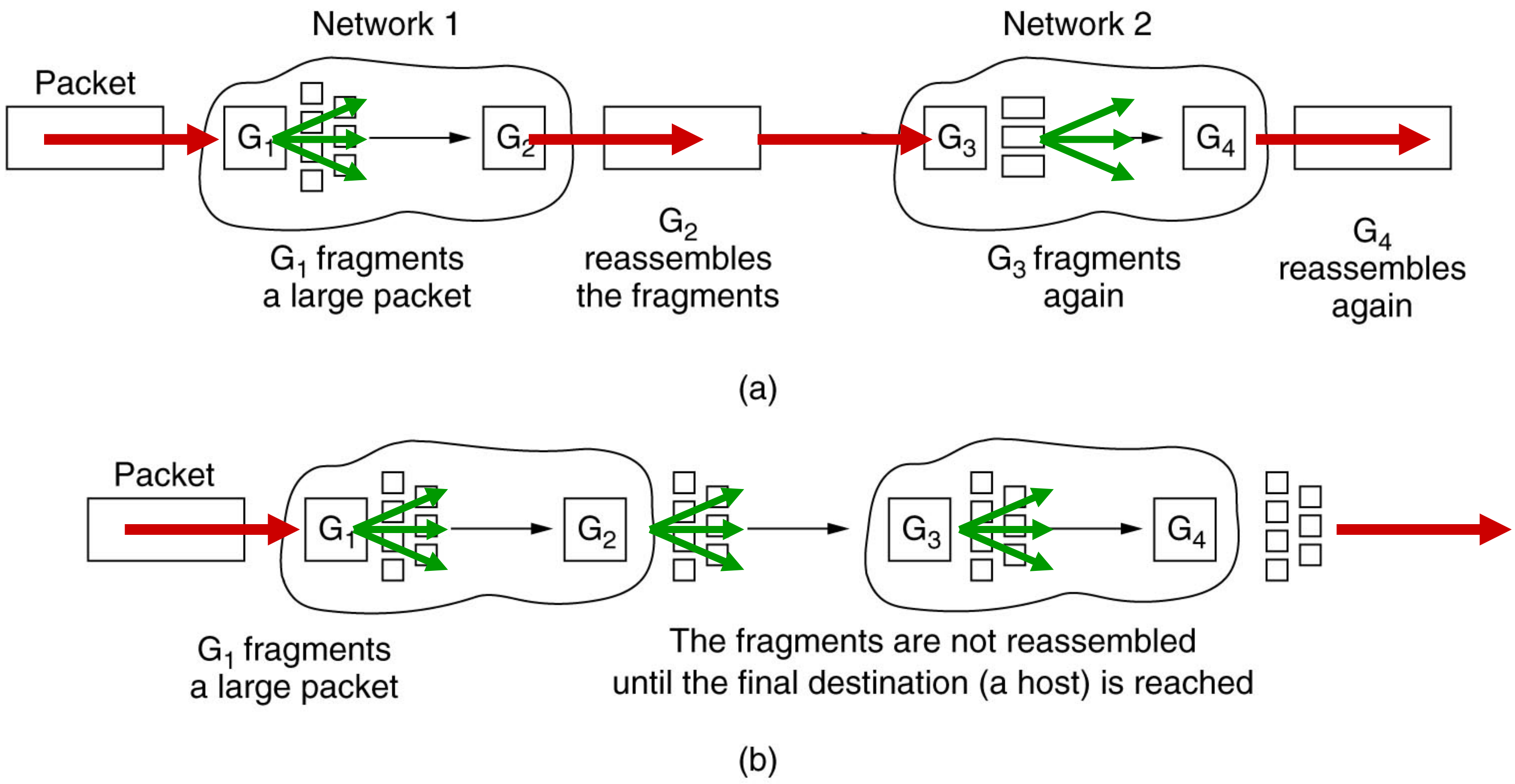
Fragmentation (cont'd)

- If one network allows only 48 byte packets while another network allows 65515 byte packets, then it is difficult to get the large packet over the network that only allows smaller packets.
- How can this be done? – Fragmentation (分段)
  - Fragmentation is the process of breaking up a packet into several smaller packets to send over a network.
  - The problem isn't breaking up the packet to send it, but putting the packet back together on the other end.
  - There are two different types of fragmentation – transparent and non-transparent.

Fragmentation (cont'd)

- □ Transparent fragmentation tries to make the fragmentation invisible to any other network on the route by reconstruction the packet each time it leaves a network.
- □ Non-transparent fragmentation results in all of the fragmented packets traveling through multiple networks to get to the destination, leaving the destination to put them back together.

Fragmentation (cont’d)


Network 1
Network 2
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
G_2 reassembles the fragments
G_3 fragments again
G_4 reassembles again
(a)
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
The fragments are not reassembled until the final destination (a host) is reached
(b)

Fragmentation - Problems

- Transparent fragmentation
  - The exit gateway must know when it has received all the pieces.
  - All packets must exit via the same gateway.
  - The overhead required to repeatedly reassemble and then refragment a large packet is big.
- Non-transparent fragmentation
  - It requires every host to be able to do reassembly.
  - The total overhead increases because each fragment must have a header.

A Method of Numbering the Fragments

□ Define an elementary fragment size small enough to pass through every network.

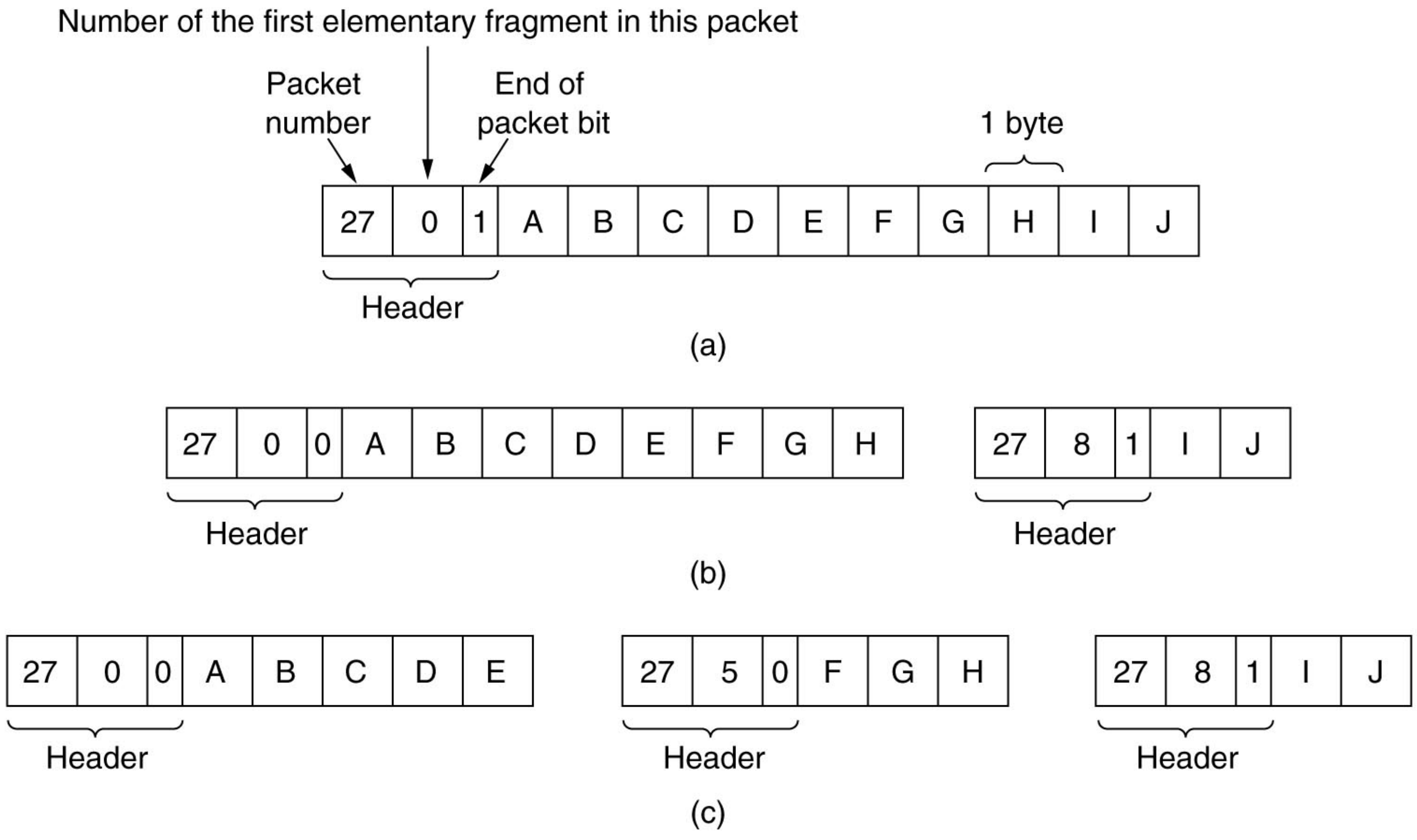
□ When the original packet is fragmented, all the pieces are equal to the elementary fragment size except the last one (shortter).

□ An internet packet may contain several elementary fragments.

□ The internet packet header must provide

1. the original packet number
2. the number of the first elementary fragment contained in the internet packet, and
3. a bit indicating whether the last elementary fragment in the internet packet is the last one of the original packet.

A Fragmentation Example


Number of the first elementary fragment in this packet
Packet number
End of packet bit
1 byte
27 | 0 | 1 | A | B | C | D | E | F | G | H | I | J
Header
27 | 0 | 0 | A | B | C | D | E | F | G | H
Header
27 | 8 | 1 | I | J
Header
27 | 0 | 0 | A | B | C | D | E
Header
27 | 5 | 0 | F | G | H
Header
27 | 8 | 1 | I | J
Header

(a)

(b)

(c)

Summary

- Congestion control
- Fragment

Thank you all !