Congestion

- When number of packets sent is within subnet carrying capacity, all are delivered
- As traffic increases, packet loss happens
- At very high traffic, performance collapses
- Both transport and network layers share responsibility of handling congestion
- Network layer is directly affected
- In that chapter, we look at network aspect
**Goodput:** rate at which *useful* packets are delivered by the network.

**How Congestions Happens**

- Incoming packets from multiple inputs need to go to same output line; queue builds up
- If insufficient memory, packets lost
- Adding memory helps to some point
- Even with $\infty$ memory, congestion gets worse
  - delayed packets timeout, retransmitted
  - duplicates increase load
- Congestion collapse: load exceeds capacity
How Congestions Happens

- Slow processors
  - CPU slow in doing bookkeeping tasks
  - queues build up
- Low bandwidth lines
  - can’t forward packets same as arriving speeds
- Mismatch between system parts
  - upgrading some parts only shifts bottleneck

Congestion VS Flow Control

- Congestion control
  - make sure subnet is able to carry offered traffic
  - global, involve behavior of all hosts
  - all factors that diminish carrying capacity
- Flow control
  - traffic between a given sender & given receiver
  - ensure fast sender not overwhelm slow receiver
  - involve feedback from receiver to sender
Example: Congestion VS Flow Control

- Flow control
  - fiber optic network with 1000 Gbps
  - S. Computer try to transfer file to a PC @ 1 Gbps
  - no congestion
  - flow control needed to slow SC

- Congestion control
  - network with 1 Mbps lines, 1000 computers
  - half of them trying to transfer @ 100 kbps
  - no overpowering problem
  - but total traffic exceed network capacity

General Principles of Congestion Control

- Can be viewed as a Control Theory problem

- Open Loop: solve problem by good design
  - attempt to prevent congestion from happening
  - after system is running, no corrections made

- Closed Loop: concept of feedback loop
  - monitor system to detect congestion
  - pass information to where action is taken
  - adjust system operation to correct problem
General Principles of Congestion Control

- Monitoring system
  - % of discarded packets for lack of buffer space
  - number of packets timeout & retransmitted
  - average delay

- Passing information
  - send packet to sources announcing problem
  - bit field in outgoing packets to warn neighbors
  - routers send probe to ask about congestion

Adjusting system
- routers expected to take appropriate action
- timing is very important
- too quick: system will oscillate wildly
- too slow: react too sluggishly to be useful
- possible actions

- Open loop
  - act at source
  - act at destination

- Closed loop
  - explicit feedback
  - implicit feedback
Congestion Prevention Policies

- Retransmission policy
  - fast retransmit, go back N add heavier load than
  - using slow retransmit, selective repeat

- Acknowledgement policy
  - immediate ACK for each packet increases load
  - save, piggyback onto reverse traffic
  - however, timeout causes retransmission

- Virtual circuit or datagram?
  - most congestion control alg require VC
Congestion Prevention Policies

- Routing algorithm
  - good algorithm helps spread traffic on all lines
- Packet lifetime
  - how long packet lives before being discarded
  - too long: lost packets cause congestion
  - too short: timeout quickly, retransmissions
- Timeout determination
  - harder, end-to-end is unpredictable
  - too short: unnecessary retransmissions
  - too long: slow response time

Congestion Control in Virtual-Circuit Subnets

- Admission Control
  - once there’s congestion, no more VCs setup
  - in telephone: no dial tone
- Alternative approach
  - allow but carefully route new VCs
Congestion Control in Datagram Subnets

- Routers monitor utilization of output lines
- Assign utilization variable for each out line
  - $u$: recent line utilizations $0 < u < 1$
  - $u_{new} = a u_{old} + (1 - a)f$ updated periodically
  - $f$: instantaneous utilization (0 or 1)
  - $a$: constant $0 < a < 1$, how fast router forgets recent history
- If $u >$ threshold enter warning state
- At new packet arrival, check state of out line

The Warning Bit
- special bit in packet header
- router in warning state set bit on out packets
- dest copies bit on next ACK packet, send back
- source cut back on traffic
- monitor fraction of warning ACKs, adjust rate
Congestion Control in Datagram Subnets

- Choke Packets
  - instead of indirect warning bit algorithm
  - tell source directly
  - send choke packet back to source
  - original packet is tagged, so will not generate another choke packet, then forwarded as usual

- Hop-by-hop choke packets
  - affect every hop it passes through
  - provide quick relief at the point of congestion

**a)** A choke packet that affects only the source

**b)** A choke packet that affects each hop it passes through
Load Shedding

- When other methods fail
- Throw excess packets away
- Term taken from electricity
  - blacking certain areas to save entire grid
  - on hot summer days with high demand
- Choosing packets to discard
  - random, may cause retransmissions
  - priority-based, required coop from senders

Load Shedding

- Random Early Detection (RED)
  - drop packets before situation become hopeless
  - routers maintain average queue length
  - if exceeds threshold, line said to be congested
  - router can’t tell which source most trouble
  - pick packet randomly from congested queue
- TCP responds to lost packets by slowing
  - in wired networks, loss is result of congestion
  - form of indirect feedback
  - in wireless networks, cannot be used
Jitter Control

- For some applications audio, video stream
  - increased delay is not a problem
  - as long as it is constant
- Jitter: variation in delay
- Var bet 20-30 ms unacceptable for sound
- If 99% packets 24.5-25.5 ms might be OK

[Diagram of Jitter Control]

(a) High Jitter
(b) Low Jitter
Jitter Control

- Calculate average time
- Each hop check how close to schedule
  - speed up slow packets
  - slow down fast packets
- For video-on-demand
  - buffering, play from buffer instead of real-time
- For real-time videoconferencing
  - buffering delay unacceptable