Computer Communication Networks

Introduction, Communication link, Multiplexing

Dr. Raja Vara Prasad
Assistant Professor
IIIT Sri City

Delays in Packet Switched Networks

- Packets travel from source to destination via intermediate routers/switches.
  - Processing delay
  - Queueing delay
  - Transmission delay
  - Propagation delay
- Nodal delay = Processing delay + Queuing delay + Transmission delay + Propagation delay

Processing Delay

- Time required to examine the packets header
  - Determines where to direct the packet
  - Check for errors
- Order of microseconds

Queuing Delay

- If a router is busy in processing and transmitting a packet, a freshly arrived packet has to wait in queue (buffer) for its turn.
- No queuing delay if the router is idle.
- Queuing delay varies with time and location. In general, it is a random variable.
- Order of microseconds to milliseconds.

Transmission Delay

- Time required to push the packet into the link
- If the length of the packet is L bits and transmission rate of the link is R bps, then

$$\text{Transmission delay} = \frac{L}{R}$$

- Order of microseconds to milliseconds

Propagation Delay

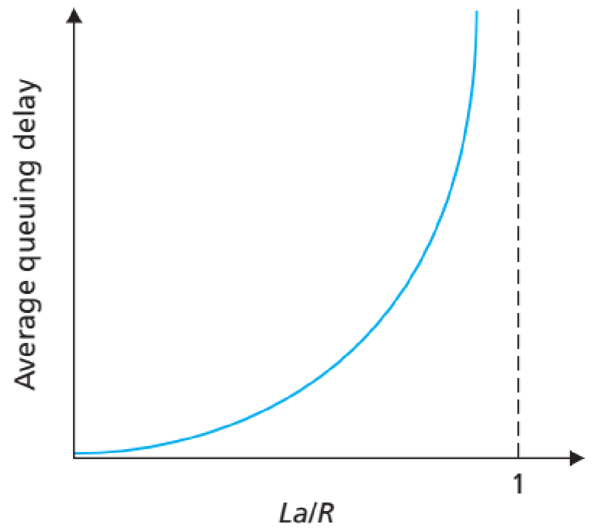
- Time required to propagate from one end of the link to the other end
- The propagation speed depends on the physical link between the routers
- In general, propagation speed s, is in the order of $2 \times 10^8 - 3 \times 10^8 m/s$.
- Propagation speed depends on the distance bewteen the routers, d
- Propagation delay $= \frac{d}{s}$

Traffic Intensity

- Queuing delays are random in nature
- Arrivals to a queue are also random in nature
- Traffic intensity is an indication of queuing delay
- Let a be the average number of packets arriving at a queue
- Each packet is of length L bits adn transmission rate is R bps
- Traffic intensity $= \frac{La}{R}$

Traffic Intensity

- If traffic intensity > 1, the *queuelength* increases to ∞
- It is desirable to have traffic intensity < 1.
- If traffic intensity close to 1, there will be a significant queuing delay



Dependence of average queuing delay on traffic intensity

Throughput

- Suppose Host A is sending data to Host B across a computer network
- Instantaneous throughput is the rate at which Host B is receiving data
- Suppose it takes T seconds to transfer F bits from Host A to Host B, then average throughput $= \frac{F}{T}$ bps.

Throughput

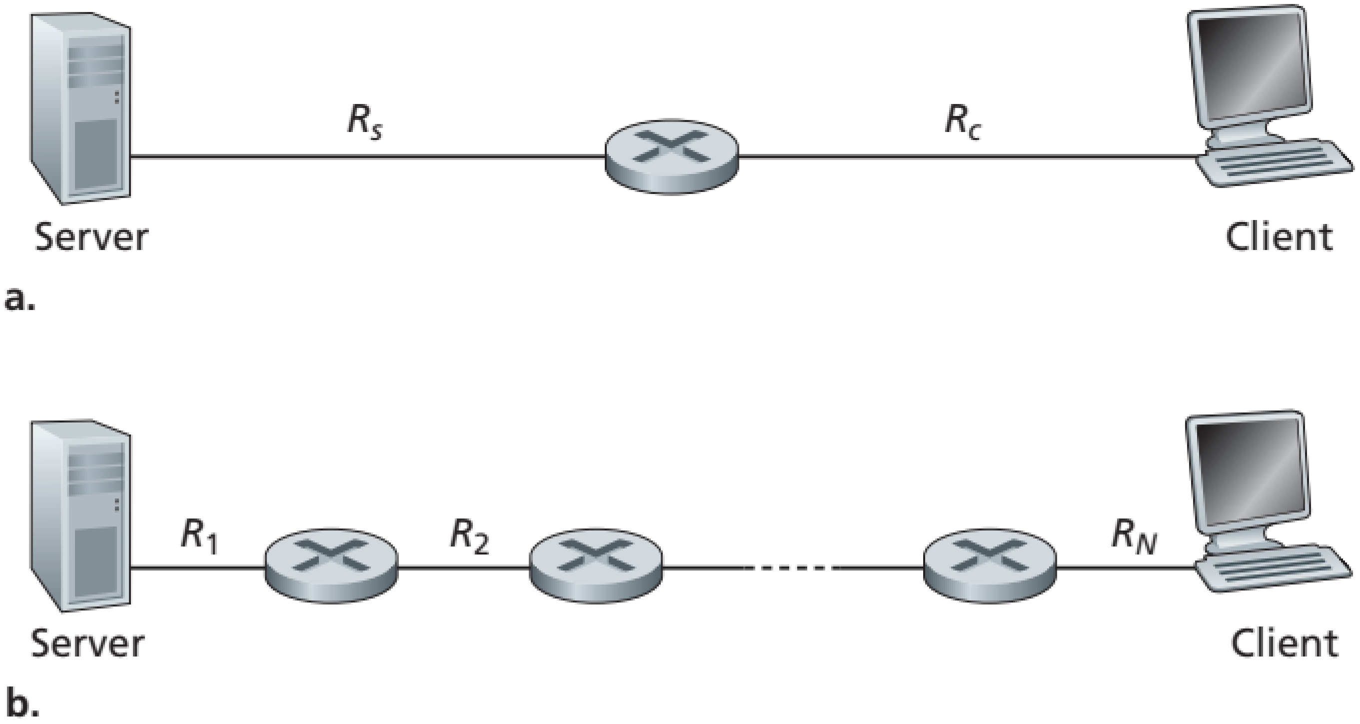


Figure 1.19 ♦ Throughput for a file transfer from server to client

Throughput - Challenges

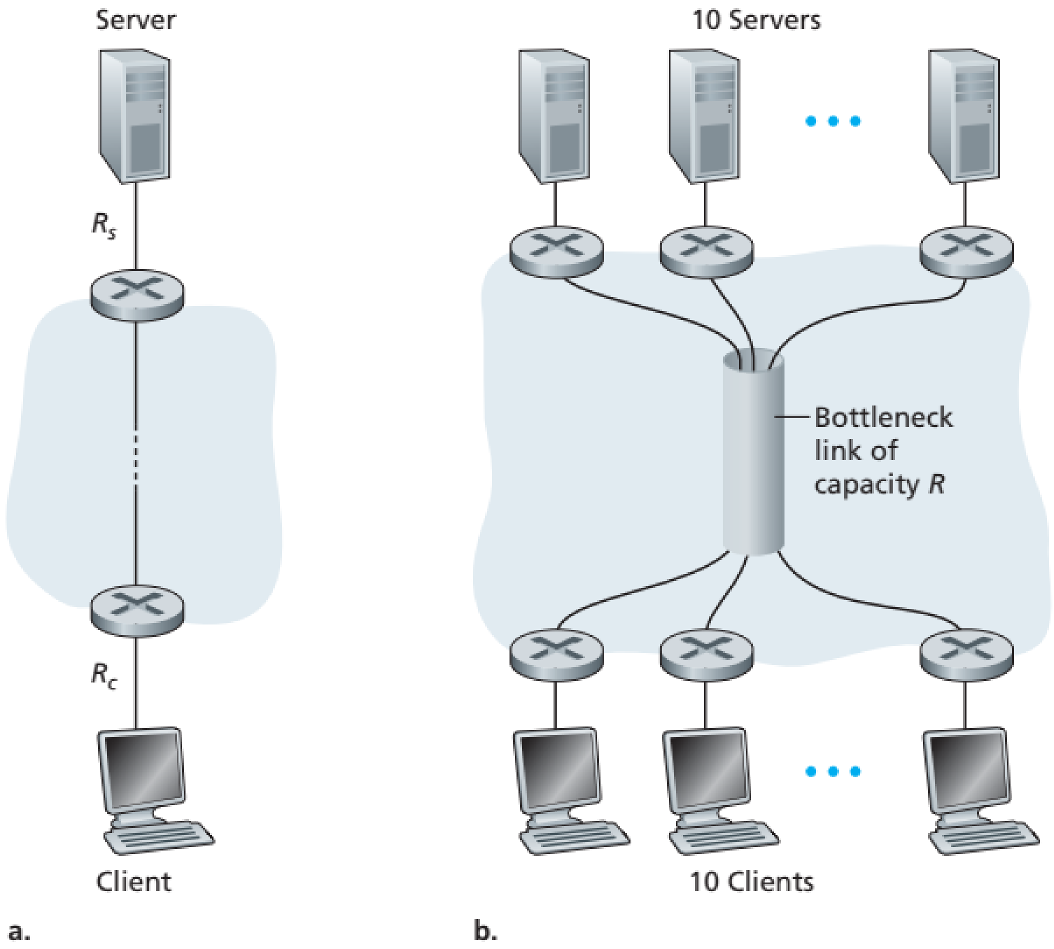


Figure 1.20 ♦ End-to-end throughput: (a) Client downloads a file from server; (b) 10 clients downloading with 10 servers

Case-a:

R, is large—say a hundred times larger than both *Rs* and *Rc*—then the throughput for each download will once again be min{*Rs*, *Rc*}.

Case-b:

Suppose R_s = 2 Mbps, R_c = 1 Mbps, R = 5 Mbps,

- common link divides its transmission rate equally among the 10 downloads.
- Then the bottleneck for each download is no longer in the access network
- instead the shared link in the core, which only provides each download with 500 kbps of throughput.

the end-to-end throughput for each download is now reduced to 500 kbps

Tutorial – Problems

1.Suppose users share a 2 Mbps link. Also suppose each user transmits continuously at 1 Mbps when transmitting, but each user transmits only 20 percent of the time.

a. When circuit switching is used, how many users can be supported?

b. For the remainder of this problem, suppose packet switching is used. Why will there be essentially no queuing delay before the link if two or fewer users transmit at the same time? Why will there be a queuing delay if three users transmit at the same time?

c. Find the probability that a given user is transmitting.

d. Suppose now there are three users. Find the probability that at any given time, all three users are transmitting simultaneously. Find the fraction of time during which the queue grows.

Problem 3

Suppose N packets arrive simultaneously to a link at which no packets are currently being transmitted or queued. Each packet is of length L bits and the link has a transmission rate of R bits/sec. What is the average queueing delay for the N packets ?

Problems

- Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links of rates $R_1 = 500\text{kbps}$, $R_2 = 2\text{Mbps}$, $R_3 = 1\text{Mbps}$.
  - Assuming no other traffic, what is the throughput for the file transfer
  - Suppose the file size is 4 million bytes, how long will it take to transfer the file from A to B?
- How long does it take for a packet of length 1000 bytes to propagate over a link of propagation speed 2.5×10^8 m/s. Length of the link is 2,500 Km and transmission rate is 2Mbps.

P6. This elementary problem begins to explore propagation delay and transmission delay, two central concepts in data networking. Consider two hosts, A and B, connected by a single link of rate R bps. Suppose that the two hosts are separated by m meters, and suppose the propagation speed along the link is s meters/sec. Host A is to send a packet of size L bits to Host B.

a. Express the propagation delay, d_{prop}, in terms of m and s.

b. Determine the transmission time of the packet, d_{trans}, in terms of L and R.

c. Ignoring processing and queuing delays, obtain an expression for the end-to-end delay.

d. Suppose Host A begins to transmit the packet at time $t = 0$. At time $t = d_{trans}$, where is the last bit of the packet?

e. Suppose d_{prop} is greater than d_{trans}. At time $t = d_{trans}$, where is the first bit of the packet?

f. Suppose d_{prop} is less than d_{trans}. At time $t = d_{trans}$, where is the first bit of the packet?

g. Suppose $s = 2.5 \cdot 10^8$, $L = 120$ bits, and $R = 56$ kbps. Find the distance m so that d_{prop} equals d_{trans}.

P12. A packet switch receives a packet and determines the outbound link to which the packet should be forwarded. When the packet arrives, one other packet is halfway done being transmitted on this outbound link and four other packets are waiting to be transmitted. Packets are transmitted in order of arrival. Suppose all packets are 1,500 bytes and the link rate is 2 Mbps. What is the queuing delay for the packet? More generally, what is the queuing delay when all packets have length L, the transmission rate is R, x bits of the currently-being-transmitted packet have been transmitted, and n packets are already in the queue?

Traceroute

- program that can run in any Internet host
- When the user specifies a destination hostname, the program in the source host sends multiple, special packets toward that destination
- packets work their way toward the destination, they pass through a series of routers
- router receives one of these special packets, it sends back to the source a short message that contains the name and address of the router
- source will send *N* special packets into the network, with each packet addressed to the ultimate destination
- source records the time that elapses between when it sends a packet and when it receives the corresponding return message
- the source can reconstruct the route taken by packets flowing from source to destination, and the source can determine the round-trip delays to all the intervening routers

```
1 cs-gw (128.119.240.254) 1.009 ms 0.899 ms 0.993 ms
2 128.119.3.154 (128.119.3.154) 0.931 ms 0.441 ms 0.651 ms
3 border4-rt-gi-1-3.gw.umass.edu (128.119.2.194) 1.032 ms 0.484 ms 0.451 ms
4 acr1-ge-2-1-0.Boston.cw.net (208.172.51.129) 10.006 ms 8.150 ms 8.460 ms
5 agr4-loopback.NewYork.cw.net (206.24.194.104) 12.272 ms 14.344 ms 13.267 ms
6 acr2-loopback.NewYork.cw.net (206.24.194.62) 13.225 ms 12.292 ms 12.148 ms
7 pos10-2.core2.NewYork1.Level3.net (209.244.160.133) 12.218 ms 11.823 ms 11.793 ms
8 gige9-1-52.hsipaccess1.NewYork1.Level3.net (64.159.17.39) 13.081 ms 11.556 ms 13.297 ms
9 p0-0.polyu.bbnplanet.net (4.25.109.122) 12.716 ms 13.052 ms 12.786 ms
10 cis.poly.edu (128.238.32.126) 14.080 ms 13.035 ms 12.802 ms
```

Networks Under Attack

- "attempt to wreak havoc in our daily lives by damaging our Internet-connected computers, violating our privacy, and rendering inoperable the Internet services on which we depend"

malicious stuff—collectively known as **malware**—that can enter and infect devices

- deleting our files.
- installing spyware that collects our private information, such as social security numbers, passwords, and keystrokes
- sends this over the Internet back to attacker

compromised host may also be enrolled in a network of thousands of similarly compromised devices, collectively known as a **botnet**

✓ **self-replicating**

✓ **Viruses** are malware that require some form of user interaction to infect the user's device

✓ **Worms** are malware that can enter a device without any explicit user interaction

Networks Under Attack

Denial-of-service (DoS) attacks:

- renders a network, host, or other piece of infrastructure unusable by legitimate users
- *Vulnerability attack:* sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. The service can stop or, worse, the host can crash.
- *Bandwidth flooding:* sends a deluge of packets to the targeted host, so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.
- *Connection flooding.* The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host stops accepting legitimate connections due to the bogus connections.

- **Distributed DoS (DDoS)** attack: leveraging botnets with thousands of comprised hosts; much harder to detect and defend against than a DoS attack from a single host.

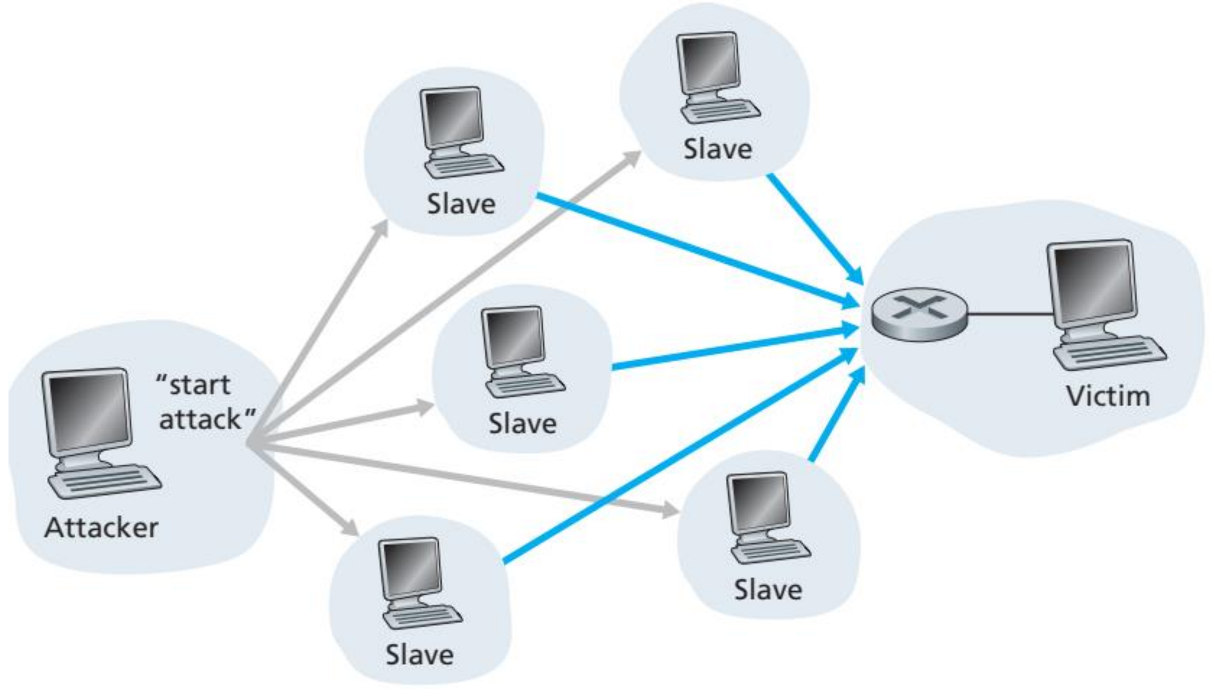
Networks Under Attack

Distributed DoS (DDoS) attack: leveraging botnets with thousands of comprised hosts

- much harder to detect and defend against than a DoS attack from a single host.

Packet Sniffers:

- placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted



- packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages.
- Sniffed packets can then be analyzed offline for sensitive information
- Wireshark: a packet sniffer
- packet sniffers are passive—do not inject packets into the channel—difficult to detect
- defenses against packet sniffing involve cryptography