CSC 249
Computer Networks

Chapter 1, Introduction
Sections 1.5 to end

January 31, 2008

Chapter 1: Introduction

Overview:

- What is the Internet?
- What is a protocol?

- The network edge: hosts, access net, physical media
- The network core: packet/circuit switching, Internet structure
- Performance: loss, delay, throughput
- **Protocol layers**, service models
- Security

Course Overview

- Fundamental Question:
  - How is data transferred through the Internet?
  - How is our natural language communication transmitted shared, binary-based media?
- Principles to develop
  - Reliable data transfer
  - Fast & error-free data transfer
  - Security and privacy safeguards
- Implementation
  - Network layer model
    - Application → Transport → Network → Link → Physical… layers

Networking Principles

- Reliable communication over an unreliable network
  - Congestion and flow control
- Interconnecting heterogeneous networks
- Finding the best path through the networks
- Sharing a multi-access channel
- Identifying devices → addresses
- Security
- Privacy & privacy rights

Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

Nodal delay: The life of a packet

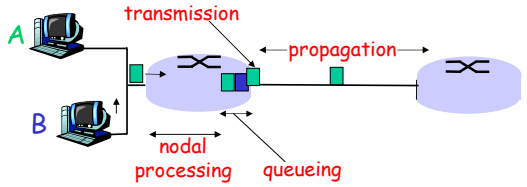
- A packet arrives at a router, and...

1. The header is read to determine where to send the packet next, and perhaps perform error checking of the bits transmitted =
2. If other packets got there first and are waiting in the output buffer, there is:
3. The rate at which the router can unload the bits onto the physical link =
4. The time to travel from one router to the next router =

Which of these delays are constant and which are variable?

Four sources of packet delay

- 1. nodal processing:
  - check bit errors
  - determine output link
- 2. queueing
  - time waiting at output link for transmission
  - depends on congestion level of router

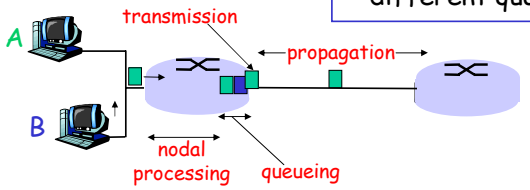


Delay in packet-switched networks

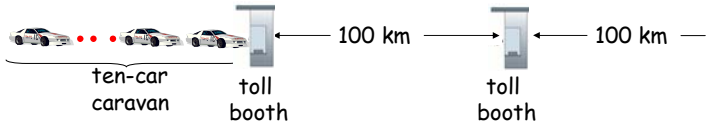
3. Transmission delay:
- R=link bandwidth (bps)
- L=packet length (bits)
- time to send bits into link = L/R

4. Propagation delay:
- d = length of physical link
- s = propagation speed in medium (~2×10^8 m/sec)
- propagation delay = d/s

Note: s and R are *very* different quantities!



Caravan analogy (more)



- Cars now "propagate" at 1000 km/hr
- Toll booth now takes 1 min to service a car
- Q: Will cars arrive to 2nd booth before all cars serviced at 1st booth?

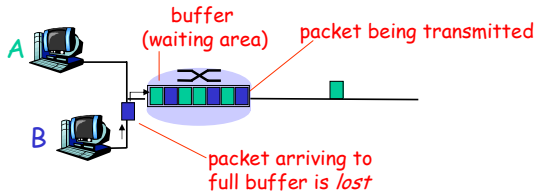
Nodal delay

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

- d_{proc} = processing delay
  - typically a few microsecs or less
- d_{queue} = queuing delay
  - depends on congestion
- d_{trans} = transmission delay
  - = L/R, significant for low-speed links
- d_{prop} = propagation delay
  - a few microsecs to hundreds of msecs

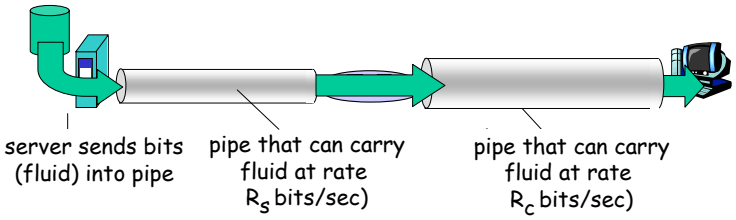
Queuing Delay & Packet Loss

- A queue (aka buffer) preceding a link has finite capacity
- A packet arriving to a full queue is dropped (aka lost)
- A lost packet may be retransmitted by the previous node, by the source end system, or not at all



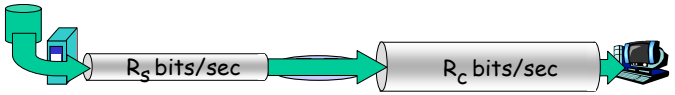
Throughput: End-to-End Measure

- *Throughput:* rate (bits/time unit) at which bits transferred between sender/receiver
  - *instantaneous:* rate at given point in time
  - *average:* rate over long(er) period of time

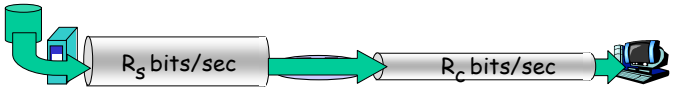


Throughput (more)

- $R_s < R_c$ What is average end-end throughput?



- $R_s > R_c$ What is average end-end throughput?

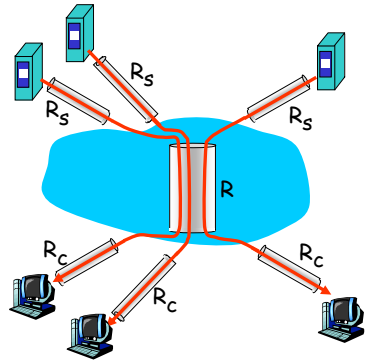


bottleneck link

link on end-end path that constrains end-end throughput

Throughput: Internet scenario

- per-connection end-end throughput: $\min(R_c, R_s, R/10)$
- in practice: R_c or R_s is often bottleneck



10 connections (fairly) share backbone bottleneck link R bits/sec

Chapter 1: roadmap

1.1 What *is* the Internet?
1.2 Network edge
- end systems, access networks, links

1.3 Network core
- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks
1.5 Protocol layers, service models
→ Tangent into News Story
1.6 Networks under attack: security

Discussion: Proposed Federal Law

- NSA would have right to eavesdrop on all internet traffic passing through the USA
  - email, Google searches, file transfers
- Objective is to protect federal government computers and systems

- Issues
  - Security vs. privacy
  - What would it take to implement this??
  - more…?

Questions

- How might this be implemented?
  - Messages broken down into packets
  - Packets from different messages are interleaved
  - Crytography?
  - Resources to watch everything?!
- Will it help with security?
- Will it threaten privacy (too much)?

- Think about this when playing with Wireshark
  - Our freeware packet sniffer

Chapter 1: roadmap

1.1 What *is* the Internet?
1.2 Network edge
- end systems, access networks, links

1.3 Network core
- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks
1.5 Protocol layers, service models
1.6 Networks under attack: security

Protocol "Layers"

Networks are complex

- There are many components:
  - applications
  - hosts
  - protocols
  - routers
  - links of various media
- A complex system is defined as a system of systems

Why layering?

Dealing with complex systems:

- Defining an explicit structure highlights the relationship between the complex system's pieces
- Modularization eases maintenance & updating of the system
  - change of implementation of layer's service transparent to rest of system
  - e.g., an internal change in one layer doesn't affect the rest of the system,
  - Much as an internal change in a method/function does not affect the rest of a program

Why layering: Other Systems

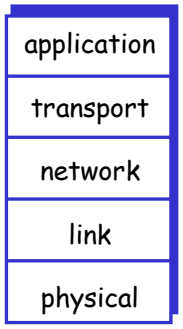
- A building
  - Frame and siding
  - Electrical system
  - Plumbing
  - Heating and air conditioning…
- A car
  - Steering
  - Brakes…

Internet Layers: The Protocol Stack

- Each layer
  - provides a service to the layer above, relying on services provided by layer below
  - appears to communicate directly with the same layer at the other "host"

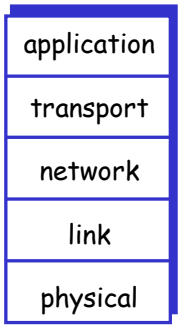
Internet Layers: The Protocol Stack

- application: supporting network applications
  - FTP, SMTP, HTTP
- transport: process-process data transfer
  - TCP, UDP
- network: routing of datagrams from source to destination
  - IP, routing protocols
- link: data transfer between neighboring network elements
  - PPP, Ethernet
- physical: bits "on the wire"



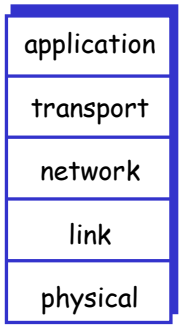
Internet Layers: Services (first glimpse)

- application:
- transport:
- network:
- link:
- physical:

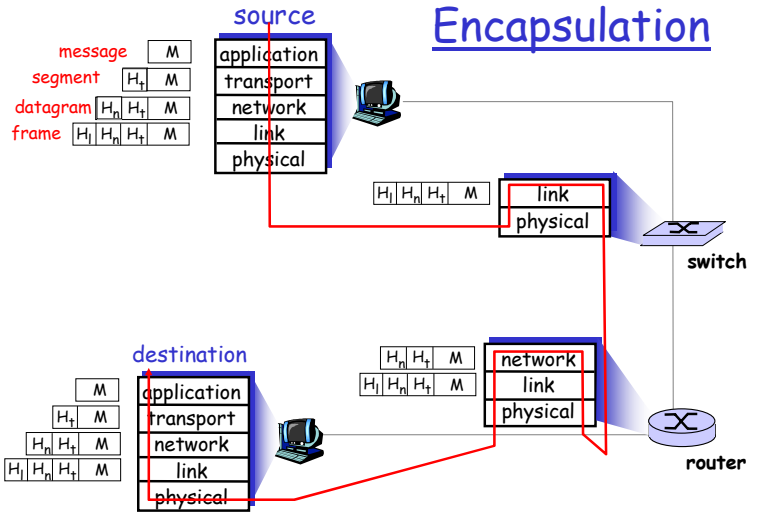


Internet Layers: Communication between…

- application:
  - users, applications
- transport:
  - processes, "ports"
- network:
  - routers, hosts
- link:
  - one device to the next
- (physical)



Encapsulation



Layering Discussion Questions

- What is an application-layer message? A transport-layer segment? A network-layer datagram? A link-layer frame?
  - What are the differences between each?
- Which layers in the Internet protocol stack does a router process? A link-layer switch? A host?

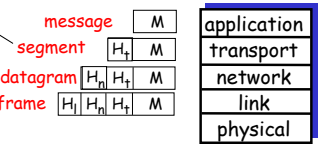
Encapsulation

Possible Header Information

Process (port) identification, end-to-end error checking

Source and destination IP addresses

Individual link error checking



Chapter 1: roadmap

1.1 What *is* the Internet?

1.2 Network edge

- end systems, access networks, links

1.3 Network core

- circuit switching, packet switching, network structure

1.4 Delay, loss and throughput in packet-switched networks

1.5 Protocol layers, service models

1.6 Networks under attack: security

Network Security

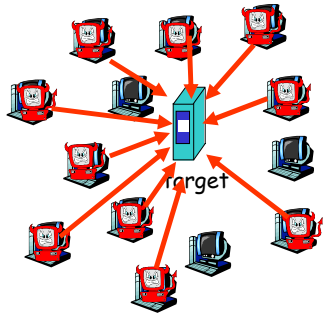
- Attacks on Internet infrastructure:
  - infecting/attacking hosts: malware, spyware, worms, unauthorized access
  - denial of service: deny access to resources (servers, link bandwidth)
- Internet not originally designed with (much) security in mind
  - Internet protocol designers playing "catch-up"
  - Security considerations in all layers

Denial of service attacks

- attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network (see malware)
3. send packets toward target from compromised hosts

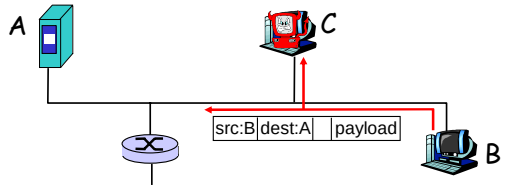
→ Queuing delay & packet loss



Sniff, modify, delete your packets

Packet sniffing:

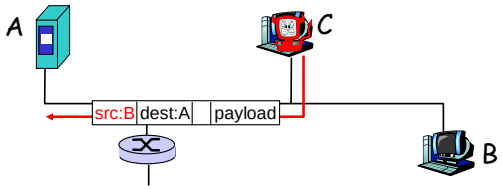
- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- Wireshark software used for end-of-chapter labs is a (free) packet-sniffer

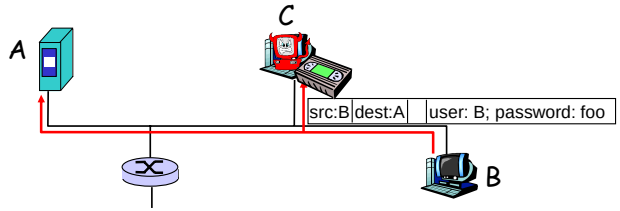
Masquerade as you

- *IP spoofing:* send packet with false source address



Masquerade as you

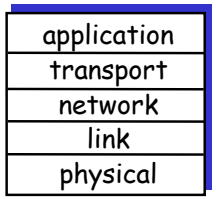
- *IP spoofing:* send packet with false source address
- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view



Security Discussion Question

- What is the difference between a virus, a worm and a Trojan horse?

Recap: Layering Summary



- Services?
- Responsibilities?
- Protocols?
- Communications between _____?
- Header information?
- Implemented on which network devices?

Summary

- Sources of packet delay
- Internet layering model
  - Definition of layers
  - Services provided by each layer
- Security attacks

Next Class

- Third Class
  - Wireshark
  - Install on your own computer and startup
  - Bring questions to class!!
- Tuesday we will start Chapter 2