Introduction

What is a computer network?

Components of a computer network:

- hosts (PCs, laptops, handhelds)
- routers & switches (IP router, Ethernet switch)
- links (wired, wireless)
- protocols (IP, TCP, CSMA/CD, CSMA/CA)
- applications (network services)
- humans and service agents

Hosts, routers & links form the *hardware* side.

Protocols & applications form the *software* side.

Protocols can be viewed as the "glue" that binds everything else together.

A physical network:

Protocol example: low to high

- NIC (network interface card): hardware

  → e.g., Ethernet card, WLAN card
- device driver: part of OS
- ARP, RARP: OS
- IP: OS
- TCP, UDP: OS
- OSPF, BGP, HTTP: application
- web browser, ssh: application

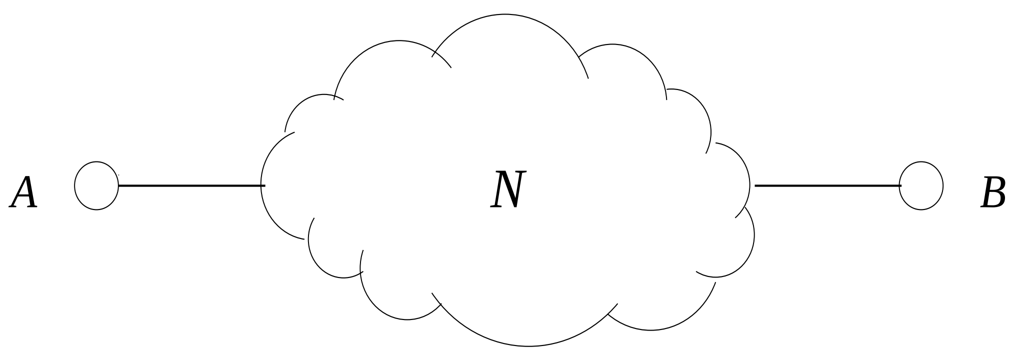
$\longrightarrow$ multi-layered glue

What is the role of protocols?

$\longrightarrow$ facilitate communication or networking

Simplest instance of networking problem:

Given two hosts A, B interconnected by some network N, facilitate communication of information between A & B.



Information abstraction

- representation as objects (e.g., files)
- bytes & bits

  $\longrightarrow$ digital form
- signals over physical media (e.g., electromagnetic waves)

  $\longrightarrow$ analog form

Minimal functionality required of A, B

- encoding of information
- decoding of information

$\longrightarrow$ data representation & a form of translation

Additional functionalities may be required depending on properties of network N

- information corruption

  $\rightarrow 10^{-9}$ for fiber optic cable

  $\rightarrow 10^{-3}$ or higher for wireless
- information loss: packet drop
- information delay: like toll booth, airport
- information security

Network N connecting two or more nodes can be

- point-to-point links
- multi-access links
- internetworks

$\longrightarrow$ physical vs. logical topology

$\longrightarrow$ e.g., peer-to-peer, VPN

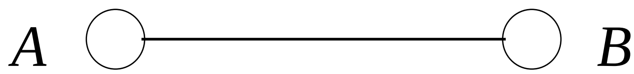
Network medium may be

- wired
- wireless

Node (e.g., hosts, routers) may be

- stationary
- mobile

Point-to-point links

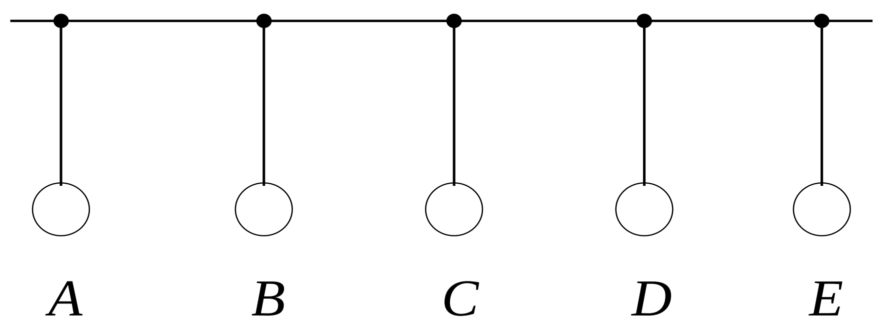


- various "cables"
- line of sight wireless communication

  → directional antennas
- no addressing necessary

  → special case

Multi-access links



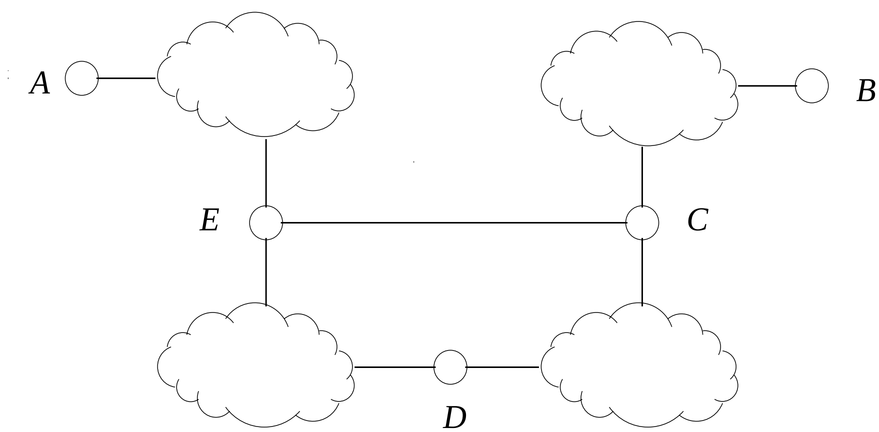
- bus (e.g., old Ethernet)
- wireless media

  → omni-directional antennas
- broadcast mode (physical; not logical)

  → listen to everything: promiscuous mode
- access control: i.e., bus arbitration

  → resolve contention and recover from interference
- addressing necessary

Internetwork



- recursive definition

  $\longrightarrow$ point-to-point and multi-access: internetwork

  $\longrightarrow$ composition of one or more internetworks
- addressing necessary
- path selection between sender/receiver: routing
- how much to send: congestion control
- protocol translation: internetworking
- location management: e.g., Mobile IP

LAN (local area network) vs. WAN (wide area network) distinction:

- LAN: point-to-point, multi-access
- WAN: internetwork

$\longrightarrow$ geographical distinction is secondary

$\longrightarrow$ often go hand-in-hand

$\longrightarrow$ counter example?

Myriad of different LAN technologies co-existing in a WAN. For example:

- Fast Ethernet (100 Mbps)
- Gigabit Ethernet (1000 Mbps)
- WLAN (54 or 11 Mbps)
- FDDI (Fiber Distributed Data Interface)
- wireless Ethernet (11 Mbps, 54 Mbps)
- SONET
- ATM
- modem/DSL

$\longrightarrow$ WAN is a collection of LANs

Each LAN, in general, speaks a different language.

$\longrightarrow$ message format

$\longrightarrow$ procedural differences

Internetworking solves this problem by translating everything to IP ...

$\longrightarrow$ technical definition of **I**nternet

But:

$\longrightarrow$ IP is not necessary

$\longrightarrow$ e.g., large systems of layer 2 switches

$\longrightarrow$ trend: L2 (70s & 80s) $\rightarrow$ IP (90s) $\rightarrow$ L2 (Y2K+)

$\longrightarrow$ IP remains central glue

Remark on addresses (aka names):

Communicating entities are *processes* residing on nodes A and B running some operating system.

Thus an *address* must also identify which process a message is destined for on a host.

$\longrightarrow$ e.g., port number abstraction

Key Issues

<u>Fault-tolerance</u>

The larger the network, the more things can go wrong.

E.g.: link/node failures, message corruption, software bugs

$\longrightarrow$ managing downtime: tier-1 providers

$\longrightarrow$ 99.999%

Two types of failures:

- independent
- correlated

In a network system with n components, assume a component fails with independent probability p

$\longrightarrow$ expected number of failures: $n \cdot p$

$\longrightarrow$ probability of no failures: $(1-p)^n$

$\longrightarrow$ probability of k simulaneous failures: p^k

Thus correlated failures have miniscule probability.

$\longrightarrow$ exponentially small in k

In reality, failures are not independent.

$\longrightarrow$ e.g., power outage, natural disasters

We have:

$\longrightarrow$ Murphy's Law

- issue of reliable communication
- reliable network services

  $\rightarrow$ main principle: redundancy
- Examples:
  - routing of messages: alternate/back-up routes
  - domain name servers: duplication
  - transmission by space probes: forward error correction (FEC)

    $\rightarrow$ also used for multimedia traffic

Network security

Features:

- confidentiality: encryption
- integrity: message has not been tampered
- authentication: sender really is who she claims to be

$\longrightarrow$ "CIA"

$\longrightarrow$ foundation: cryptography

$\longrightarrow$ end-to-end

$\longrightarrow$ networking problem?

Modern security vulnerabilities:

- denial of service (DoS) attack

  $\longrightarrow$ e.g., SYN flooding

- distributed DoS (DDoS) attack

  $\longrightarrow$ e.g., commercial, personal, infrastructure

- worm attacks: e.g., CodeRed, Blaster, ...

  $\longrightarrow$ buffer overflow: mainly bugs in MS DLLs

- spam mail (security issue?)

- with fault-tolerance impacts QoS (quality of service)

  $\rightarrow$ Aug. 04: US broadband deployment exceeds dial-up

- security: trade-off with overhead

  $\rightarrow$ what is the desired operating point?

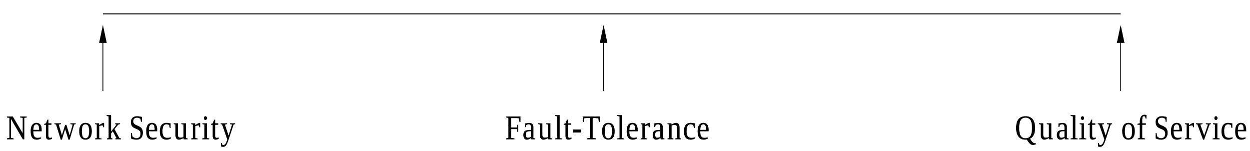
  $\rightarrow$ too much $\Rightarrow$ too slow

  $\rightarrow$ too little $\Rightarrow$ too vulnerable

For example: secure routing (S-BGP)

$\longrightarrow$ "BBN vs. Cisco"

Big picture:



$\longrightarrow$ points in the same spectrum

$\longrightarrow$ malicious (Byzantine) vs. non-malicious

$\longrightarrow$ availability

$\longrightarrow$ service assurances

Performance

Issues:

- excessive traffic can cause congestion (analogous to highways)
- traffic volume exhibits large fluctuations

  $\rightarrow$ burstiness
- multimedia traffic is voluminous (even for single user)
- ubiquitous access

  $\rightarrow$ wired/wireless Internet

Potential for bottleneck development

$\longrightarrow$ spontaneous or persistent

$\longrightarrow$ similar consequences as failures

Different applications require different levels of service quality.

Challenges:

$\longrightarrow$ how to provide customized QoS

$\longrightarrow$ many users and applications: scalability

$\longrightarrow$ must interoperate with legacy Internet

Current state:

- overprovisioning

  $\rightarrow$ "throw bandwidth at the problem"

  $\rightarrow$ tier-1 ISPs use sophisticated traffic engineering

- still no Internet QoS

  $\rightarrow$ changing with VoIP and content deployment

- not economic

  $\rightarrow$ few tier-1 providers make money

Data networking, telephony, and content convergence

⟶ Y2K+ trend

- VoIP (Voice-over-IP): wired world

  → traditional TDM-based telephony system is entirely separate network

  → economic factors are dictating convergence

  → from KaZaA to Skype

- cellular voice networks: 2G, 2.5G, 3G

  → what is 4G?

  → telcos/cellular providers are concerned

  → take-over by WLAN + IP?

  → strategy: active participation

- peer-to-peer: rampant content dissemination

  → from audio to movies

  → content providers need to get into the action

  → do not want to get into the action

$6 question:

$\longrightarrow$ what will the wireless/wireline future hold?

Mixture of high bandwidth/low bandwidth networks, wireline/wireless, . . .