Introduction

What is a computer network?

Components of a computer network:

- host devices (PCs, servers, laptops, handhelds)
- routers & switches (IP router, Ethernet switch, WiFi routers)
- links (wired, wireless, quantum)
- protocols (IP, TCP, UDP, CSMA/CA, OSPF, BGP)
- applications (DNS, HTTP, SMTP, SNMP, SSL)
- humans and bots (spam, DoS, worm)

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

Protocols & applications form the *software* side.

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

Protocol example: from low- to high-layer

- NIC (network interface card): firmware

  $\rightarrow$ e.g., Ethernet card, WLAN card, CDMA or TDMA air interface (cellular)

  $\rightarrow$ mainly ROM code

- device driver: part of OS

  $\rightarrow$ fast and slow interrupt handlers

- ARP, RARP: OS

  $\rightarrow$ NICs have two names (e.g., 48 vs. 32 bits): translation

- IP: OS

  $\rightarrow$ software glue of global Internet

- OSPF, RIP, BGP: routing protocols above IP

  → OFPF, RIP: within organizations (intra-domain)

  → router OS (e.g., IOS)

  → BGP: global Internet (inter-domain)

- TCP, UDP: OS

  → TCP: files (text, image, video)

  → UDP: multimedia streaming

- DNS, HTTP, SMTP, SNMP, SSL: application layer

- ssh, web browser, php, P2P (BitTorrent), YouTube, Netflix, Facebook, Twitter, CDNs, bots: application layer

What layers are relevant?

- 1970s: lower layers and hardware
- 1980s: both lower and higher layers
- 1990s: higher layers
- today: both lower and higher layers, and hardware

→ driving force: ubiquitous wireless networks

→ driving force: data centers, streaming services

→ boundary between telephony and data networks is gone

→ myriad devices: Internet of Things (IoT)

Example: Digital TV and freed-up UHF spectra

→ sub-GHz spectra reuse (e.g., 300–700 MHz) for data networking

Example: Short-distance services

→ RFID for electronic payments, tolls, inventory control, home security

→ getting rid of wires

Example: CAN (controller area network) bus and vehicle networks

→ specialized network control

→ increasingly relevant: self-driving vehicles

→ connected to GPS, cellular, IP networks

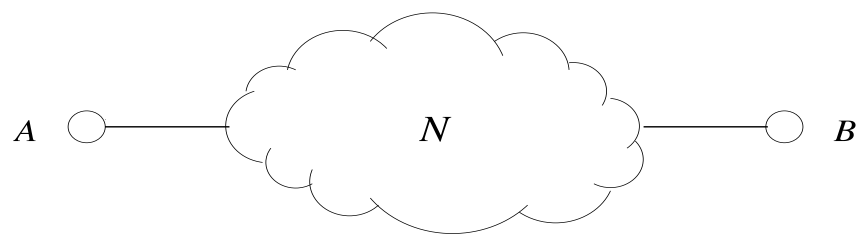
Computer networks enable communication

Simplest instance of communication:

- Two hosts A, B connected by some network N.
- Transmit information between A and B.

  → information: analog or digital

  → simplest case: single bit



Norm in today's networks: content is digital (i.e., bits) but transmission is analog (i.e., electromagnetic waves).

→ use analog information to transmit digital information

Network N can take several forms

$\longrightarrow$ building block: communication link

- point-to-point link: dedicated, direct link between A and B

  $\rightarrow$ e.g., single wire, line-of-sight antennae

- broadcast link: what A sends can be heard by all (not just B)

  $\rightarrow$ multicast: logical (not physical)

- internetwork: network of networks

  $\rightarrow$ e.g., Purdue's campus network, tier-1 AT&T's intranet, global IP Internet

What capabilities must A, B, and N have?

One: information abstraction

- digital content representation: encode/decode information
  - → from little/big endian to message format: header, payload, trailer
  - → app payload: file, streaming media, protocol interaction
- analog representation and transmission of digital content
  - → analog signals over physical media (e.g., copper, fiber, wireless)
  - → digital tranmission using square waves has specific roles

Two: information protection

- Deal with information corruption: bit flip

  → bit error rate (BER)

  → e.g., ballpark 10^{-9} for fiber optic cable, 10^{-6} for wireless

- Deal with information loss: packet drop at routers and hosts

  → culprit: buffer overflow

  → subject of resource provisioning, scheduling

- Security

  → protect against eavesdropping: confidentiality

  → protect against ID theft: authentication

  → protect against tampering: integrity

  → protect against infrastructure attack: intrusion detection/prevention, denial of service (DoS) attacks

Three: performance

$\longrightarrow$ focus: software overhead and limitations

- file transmission should be fast: bottleneck can be hardware and software

  $\rightarrow$ throughput (bps): 10 Gbps hardware link does not mean 10 Gbps throughput

  $\rightarrow$ affected by overhead and algorithms/protocols

  $\rightarrow$ data compression: source coding

- latency or delay (msec): physical distance/speed-of-light (SOL) imposes fundamental limit

  $\rightarrow$ affected by buffering of messages at routers and device operating systems

  $\rightarrow$ bad for video/audio streaming, voice, interactive games

Features of a network N:

Connectivity:

- point-to-point link
- multi-access link
- internetwork

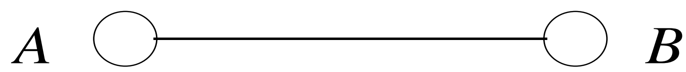
Physical medium:

- wired
- wireless

Location:

- stationary
- mobile

Point-to-point link



- NICs (network interface cards) at A and B
- wired: physical wire connecting two NICs

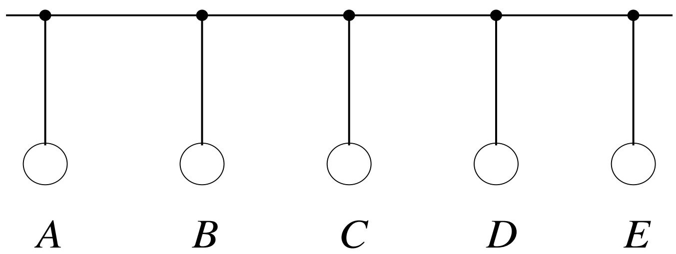
  → various cables: copper and fiber of different grades
- wireless:

  → line-of-sight (LOS) antennae at the NICs: directional

  → e.g., roof-top building-to-building, infrared TV remote, 60 GHz networks
- A and B don't need names

  → at least in principle

Multi-access link



- classical bus (e.g., old Ethernet)

  → broadcast to every reachable device

- wireless media with omni-directional antennas

  → e.g., wireless LANs

- wireless media with semi-directional antennas

  → e.g., GPS satellites, cellular tower

  → signal casts a cone

- names (i.e., addressing) necessary

  → "From" and "To"

  → called local area network (LAN) addresses

- key issue of multi-access link communication: access control

  → link is a shared resource

  → how to share?

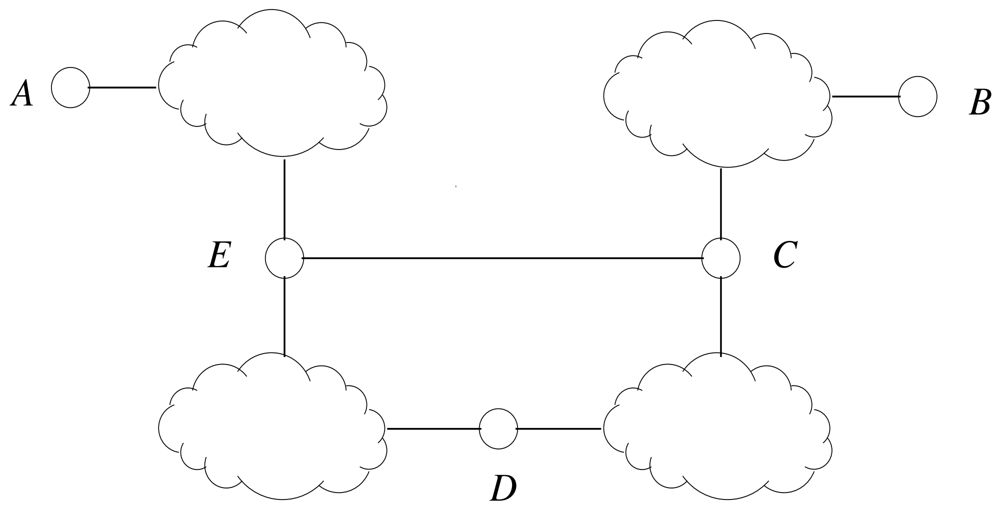
  → simultaneous transmission possible?

  → myriad of LAN technologies and protocols

  → e.g., WiFi, Bluetooth, RFID, Ethernet, OFDMA, CAN

  → much of LAN technology and protocols revolve around this issue

Internetwork



- recursive definition

  → point-to-point and multi-access are networks

  → network of networks: internetwork

- ultimately networks reduce to

  → point-to-point and multi-access links

  → everything else: composition

Complications introduced by internetworks:

- New names beyond LAN addresses

  → in principle, LAN addresses are unique and suffice

  → in practice, new names (i.e., network addresses) bring benefits despite overhead

  → dominant: IP, in particular, IPv4 and IPv6

- Protocol translation

  → LANs speak different languages (e.g., Ethernet and WLAN)

  → internetworking overhead

- Path selection between sender/receiver

  → routing: within and across organizations

  → e.g., routing within Purdue, routing from Purdue to one of its service providers

- How fast to send on a long path

  → links with different speeds and traffic

  → affects feedback control

  → how to coordinate sender/receiver to achieve fast speeds: congestion control

- Location management

  → e.g., moving from 1st floor in LWSN to 2nd floor, moving from LWSN to WANG, commuting on a bullet train

  → handoff of mobile host among multiple networks

  → LAN handoff, IP handoff (Mobile IP)

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

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

→ geographic proximity is secondary (albeit often goes hand-in-hand)

→ counter examples?

Naming: LAN and IP addresses are insufficient.

Typically communicating entities are apps running as processes in a host/router operating systems (e.g., Linux, Windows, IOS).

→ IP specifies NIC of host/server/router: no process identification

→ device with with multiple NICs may have multiple IP addresses: multi-homed

To identify a process to whom a message is destined:

→ use 16-bit port number supported by operating systems

→ why not use process IDs?

→ typical address: (IP address, port number) pair

→ note: IP address must eventually be translated to LAN address

→ port numbers borrowed for IP address extension: IP address depletion problem

Sometimes port number not needed.

Identifiers needed at the organization level

→ autonomous system number (ASN)

→ e.g., ASN 17 for Purdue, Netflix AS40027, AT&T AS7018

→ basis for global (inter-domain) routing

→ IP addresses are associated with autonomous systems

→ policy issues