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)
- network protocols (OFDM, CSMA, IP, UDP, TCP, OSPF, BGP)
- application layer protocols (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 comprise the "glue" that binds all components together

Protocol examples: from low- to high-layer

- NIC (network interface card): firmware
  - → e.g., Ethernet card, WLAN card, Bluetooth, OFDMA air interface (cellular)
  - → "ROM" code
- device driver: part of OS
  - → interfaces with hardware and firmware
  - → fast and slow interrupt handlers
- ARP, RARP: OS
  - → NICs have multiple names (e.g., 48-bit hardware address vs. 32- or 64-bit IP address): translation
- IP: OS
  - → software glue of Internet
  - → global IP internetwork

- 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 forces:

$\rightarrow$ ubiquitous wireless networks

$\rightarrow$ real-time and streaming multimedia

$\rightarrow$ data centers

Boundary between telephony and data networks is gone.

Myriad devices: Internet of Things (IoT).

Computer networks enable communication

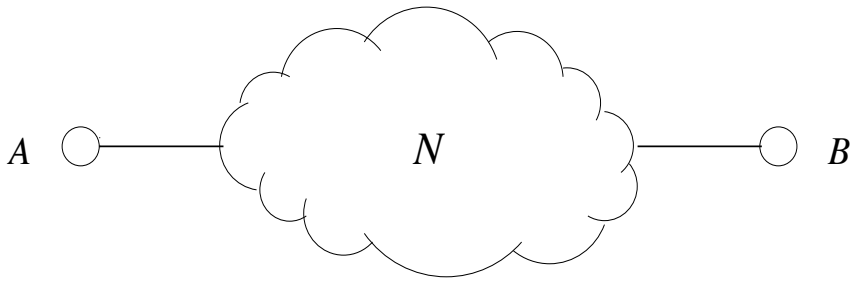
Simplest instance of communication:

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

  $\rightarrow$ information: digital

  $\rightarrow$ note: analog information (e.g., audio) is converted into bits

  $\rightarrow$ simplest case: a single bit



Norm in today's networks:

- content is digital
- transmission is analog

→ analog transmission: electromagnetic waves

→ both wired and wireless media

Important to understand how bits are transmitted using analog transmission.

→ underlying principles

→ dominant technology: OFDM

Network N can take several forms

$\longrightarrow$ building block: communication link

$\longrightarrow$ link: wired, wireless

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

  $\rightarrow$ copper/fiber wire between two NICs

  $\rightarrow$ line-of-sight antennae between two NICs

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

- internetwork: network of networks

  $\rightarrow$ starting with point-to-point and broadcast links

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

What capabilities must A, B, and N have?

Information abstraction

- digital content representation: encode/decode information
  - → how to organize bits, bytes
  - → from little/big endian to message format: header, trailer, payload
  - → payload type: file, streaming media, control
- analog transmission of digital content
  - → analog signals over physical media
  - → digital tranmission using square waves has its use

Information protection

- information corruption: bit flip
  - → bit error rate (BER)
  - → e.g., ballpark 10^{-9} for fiber optic cable, 10^{-6} for wireless
- information loss: packet drop at routers and hosts
  - → culprit: buffer overflow
  - → subject of resource provisioning, scheduling
- security
  - → eavesdropping: confidentiality
  - → ID verification: authentication
  - → tampering: integrity
  - → infrastructure attack: intrusion detection/prevention, denial of service (DoS) attacks

Performance

→ focus: software overhead and speed

→ beyond correctness

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

  → throughput (bps): 10 Gbps hardware link does not mean 10 Gbps throughput

  → various software related issues

- latency or delay (msec)

  → physical distance/speed-of-light (SOL) imposes fundamental limit

  → buffering of messages at routers and host systems

  → bad for video/audio streaming, voice, interactive games

Features of a network N:

Connectivity:

- point-to-point link
- multi-access (i.e., broadcast) link
- internetwork

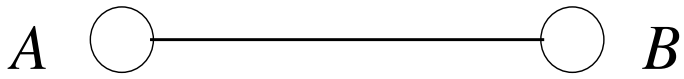
Physical medium:

- wired
- wireless

Location:

- stationary
- mobile

Point-to-point link



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

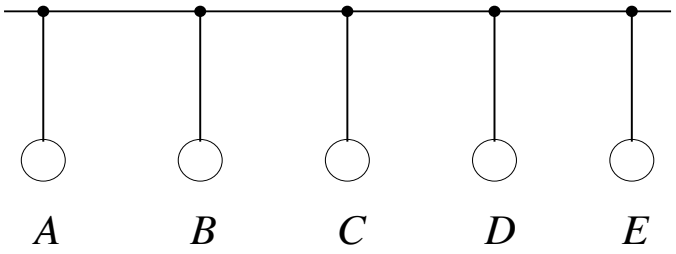
  → various cables: copper and fiber of different grades
- wireless:

  → 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

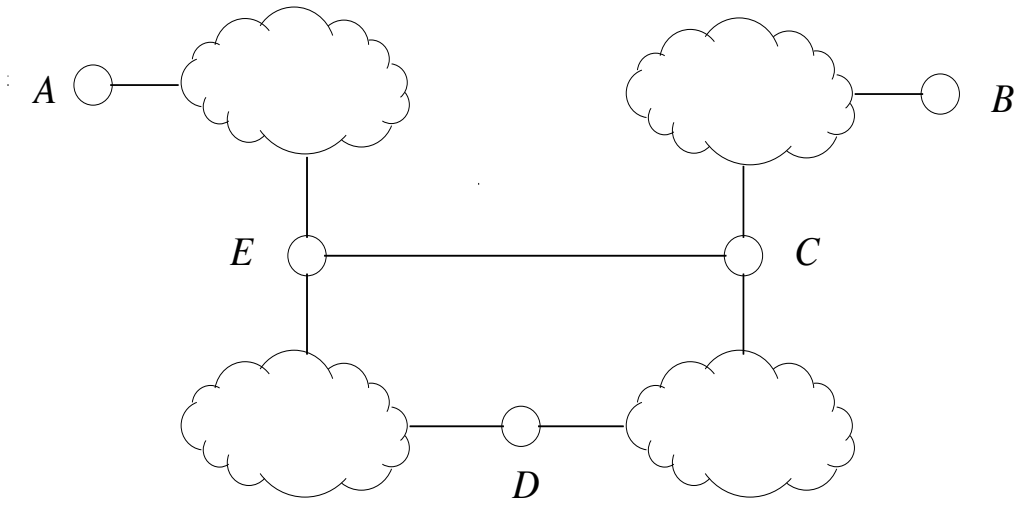
  → how to share?

  → simultaneous transmission possible?

  → myriad of LAN technologies and protocols

  → e.g., WiFi, Bluetooth, RFID, Ethernet, 5G, CAN

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
- 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
  - → going as fast as possible may cause accidents
  - → 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 HAAS, commuting on a bullet train
  - → handoff of mobile host among multiple networks

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 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?

→ default address: <IP address, port number> pair

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

→ ultimately: boils down to bits sent across LANs

Names/identifiers needed at the organizational level

→ autonomous system number (ASN)

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

→ used for global (inter-domain) routing

→ IP addresses are assigned to autonomous systems

→ global Internet: packets passed between autonomous systems