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
  - e.g., Ethernet card, WLAN card, CDMA or TDMA air interface (cellular)
  - mainly ROM code
- device driver: part of OS
  - fast and slow interrupt handlers
- ARP, RARP: OS
  - NICs have two names (e.g., 48 vs. 32 bits): translation
- IP: OS
  - software glue of global Internet
• OSPF, RIP, BGP: routing protocols above IP
  → OSPF, 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, Facebook, Twitter, 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: wireless networks
  → primacy of mobile devices
  → boundary between telephony and data networks is gone
  → ubiquitous Internet of Things (IoT)
Example: Digital TV and freed-up UHF spectra
→ 300–700 MHz frequency targeted for data networking (e.g., super WiFi)

Example: Short-distance services
→ RFID for electronic payments, tolls, inventory control
→ Bluetooth streaming
→ getting rid of wires (e.g., wireless USB, wireless battery charging)

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

- **point-to-point link**: dedicated, direct link between $A$ and $B$
  
  $\rightarrow$ e.g., single wire, line-of-sight antenna

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

- **internetwork**: network of networks
  
  $\rightarrow$ e.g., Purdue’s campus network, 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)
  - once upon a time (80s): transmission using square waves was popular
Two: information protection

• deal with information corruption: bits flip
  \[ \rightarrow \text{bit error rate (BER)} \]
  \[ \rightarrow e.g., 10^{-9} \text{ for fiber optic cable, } 10^{-6} \text{ or higher for wireless} \]

• deal with information loss: packet drop at routers and hosts
  \[ \rightarrow \text{culprit: buffer overflow} \]

• security
  \[ \rightarrow \text{protect against eavesdropping: confidentiality} \]
  \[ \rightarrow \text{protect against ID theft: authentication} \]
  \[ \rightarrow \text{protect against tampering: integrity} \]
  \[ \rightarrow \text{protect against infrastructure attack: denial of service (DoS), intrusion} \]
Three: performance

- file transmission should be fast: bottleneck can be software

  \[\rightarrow \text{throughput (bps)}\]

  \[\rightarrow \text{e.g., 1 Gbps hardware link does not mean 1 Gbps throughput}\]

  \[\rightarrow \text{Why not? What does TCP do? Are there faster methods?}\]

- information latency: time (msec)

  \[\rightarrow \text{physical distance: speed-of-light (SOL)}\]

  \[\rightarrow \text{buffering of messages at routers and host operating systems}\]

  \[\rightarrow \text{bad for video/audio streaming, voice, interactive games}\]
Types of network $N$:

connectivity:
- point-to-point link
- multi-access link
- internetwork

physical medium:
- wired
- wireless

location:
- stationary
- mobile
*Point-to-point link*

\[ A \quad \text{---} \quad B \]

- NIC at \( A \), NIC at \( B \)
- wired: physical wire connecting two NICs
  \( \rightarrow \) various cables: copper, fiber of different quality
- wireless:
  \( \rightarrow \) line-of-sight (LOS) antenna at two NICs: directional
  \( \rightarrow \) e.g., roof-top building-to-building, infrared TV remote, 60 GHz networks
- \( A \) and \( B \) don’t need names
  \( \rightarrow \) at least in principle
Multi-access link

- sometimes called bus (e.g., old Ethernet)
- wireless media with omni-directional antennas
  → e.g., wireless LANs
- wireless media with semi-directional antennas
  → e.g., GPS satellites, cellular tower antenna
  → signal casts a cone
  → broadcast (everyone) or multicast (subgroup)
- 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?

→ myriad of LAN technologies and protocols

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

→ much of LAN technology and protocols revolves 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 is their composition
Additional 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
  → 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)