CS536 Data Communication and Computer Networks

🅭 Xiyuan Chen

Spring Term, 2024

Information

- No slides, no textbook.
- No curving for the final grade.

Contents

1 Introduction

The lecture notes of this section is lec1 and lec2.

1.1 Components of a computer network

1. host devices (PC, server, laptop)
2. routers & switches (IP router, Ethernet switches, WiFi routers)
    - The global internet has 2 types of routing going on: 1. **Intranet**: routing within a domain. 2. **Internet**: routing between domains.
3. links (wires, fiber, quantum)
    - Confidentiality. We need to encrypt the data.
    - Authentication. We need to make sure the data is from the right source.
    - Integrity. We need to make sure the data is not modified.
    - Bounded by the speed of light. For wireless or wired today, we use eletromagnetic waves. FDM (Frequency Division Multiplexing) → OFDM (Orthogonal Frequency Division Multiplexing)
4. protocals (IP, TCP, UDP, ...). All protocals are part of an OS (in kernel mode). Protocal helps connect different parts of the network. Examples from low- to high-layer:
    - NIC: Network Interface Card. Such as Ethernet card, WALN card, etc. It is read only memory code. **Lower half of the OS**.
    - Device Drivers. **Lower half of the OS**.
    - ARP, RARP. **OS**.
    - IP. **OS**.
    - OSPF, RIP, BGP. OFPF, RIP: within organizations (intra-domain). BGP: global Internet (inter-domain). **OS**.
    - TCP, UDP. **OS**.
    - DNS, HTTP, SMTP, SNMP, SSL. **Application**.
    - SSH, web browser, PHP, P2P, YouTube etc. **Application**.
5. applications (DNS, HTTP, SMTP, SSL, ...)
6. humans and bots (spam, DoS, worm, ...)

> 1, 2 and 3 are **hardware**, 4 and 5 are **software**.

1.2 Communication

- Types of information transmition: **analog** and **digital**.
- In today's networks, the content is digital (bits), but the transmission is analog (eletromagnetic waves) → use analog information to transmit digital information.

Capability of network and end systems:

1. information aabstraction:
    - digital content representatoin: encode/decode information.

- analog rerpesentation and transmission of digital content: analog signals over physical media.

2. information protection:
   - deal with infornation corruption (bits flip). Use BER (Bit Error Rate) to measure the quality of the link.
   - deal with information loss(packet drop at routers and hosts). e.g., culprit: buffer overflow.
   - security. e.g., confidentiality, authentication, integrity, protect from infrustracture attacks such as DoS.
3. performance:
   - fast transmission: throughputs (bps), bottleneck can be software.

     Why 1Gbps Ethernet is not 1Gbps throughputs? TCP is not one-time transmission. TCP is a **reliable** protocal, which means it will make sure the data is delivered. TCP will send a packet, wait for the ACK, and then send the next packet.
   - information latency: physical distance, buffering of messages at routers and hosts. Bad for real-time applications such as video streaming, online gaming, etc.

1.3 Types of networks

1. connectivity:
   - point-to-point
   - multi-access (broadcast)
   - internetwork (network of networks such as Purdue's campus network)
2. medium:
   - wired
   - wireless
3. locaiton:
   - stationary
   - mobile
     - Doppler effect: the frequency of the wave changes when the source or the receiver is moving.
     - Low frequency loses strength but passes through walls. (2.4GHz, 5GHz)

1.3.1 Point-to-point link

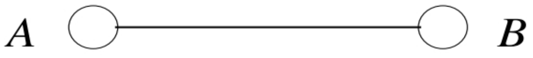

Figure 1: Point-to-point link

- NIC at A, NIC at B
- A and B don't need names in principle.

1.3.2 Multi-access link

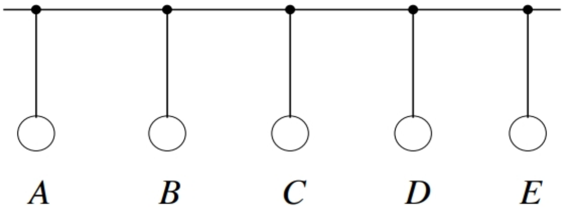

Figure 2: Multi-access link

- sometimes called bus
- names (i.e., addressing) necessary, called local area network (LAN) addresses.
- key issue of multi-access link communication: access control.
  - link is a shared resource.
  - myriad of LAN technologies and protocols.
- denail of service (DoS) attack: receivers need to process a minimum amount of data and analyze metadata to determine if a message is for them. When splashing a lot of messages, the receiver will be overwhelmed.
- Singals may add up to create **superposition**, which makes receivers hard to decode the message.

1.3.3 Internetwork

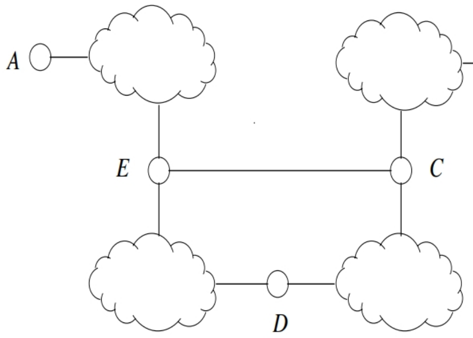

Figure 3: Internetwork

- recursive definition: network of networks.
- everything is the composition of point-to-point links and multi-access links.
- additional complications:
  - 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. IPv4: 32 bits, IPv6: 128 bits.
  - protocol translation: LANs speak different languages (e.g., Ethernet and WLAN). We call hosts that are able to do more than one network connection and IP address **multi-homed**.

- location management: mobility. e.g., handoff of mobile host among multiple networks.

1.4 LAN vs WAN

- LAN (Local Area Network): point-to-point links and multi-access links.
- WAN Wide Area Network: internetwork. **WAN is a network of LANs.**

Setellite, GPS, Starlink, printer to PC are all point-to-point links, thus they are all LANs. Communication between east coast and Europe is through cables under the ocean, thus it is still a LAN. (if we ignore repeaters during the transmission here.)

When we talk about conenctions within Purdue campus which involves hundreds of routers, switches and devices, it is WAN.

Takeaway: LAN and WAN are not about the size of the network, but the type of the network. If the connection is a large network of LANs, it is WAN. And when connecting 2 LANs, we need some intermediary who speaks both languages of the 2 lines being connected.

1.5 Port

When we commnunicate between devices, each device has an OS. When we try to send data, we are not sending it to OS (in most cases, except pinging), but to a **process** (or **thread**). How do we know which process to send to?

Attempt: use process ID. But process ID is **not predictable**. We cannot assign PID manually to a new process.

Solution: use (IP address, **port number**) pair. Port is a number that is predictable. We can assign a port number to a process. When we send data, we send it to a port number. The OS will know which process to send to.

1.6 Network Design & Performance

1.6.1 Emphasis of lightweight network core

The priciple nowadays is to **keep the hardware simple** and **put the complexity in software**. We push heavyweight stuff toward the edge.

> ATM: Asynchronous Transfer Mode. It is a circuit-switched network. It is a smart router designed in the 80s. It handles some of the jobs for packets. But IP ended up winning the competition.

The network is kept very small, we call it an **end-to-end paradigm**.

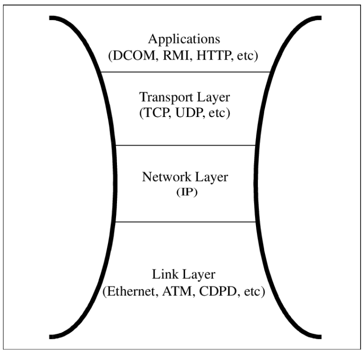

Figure 4: Hour-glass Design of Network

1.6.2 Performace yardsticks

- **Bandwidth** in bps (bits per second). We **ignore** protocol overhead in this metric.
- **Throughputs** in bps. Protocol overhead is included. In practice, app and user space OS overhead causes further slow-down.
- **Latency** in msec (milliseconds).
  - signal speed limit: speed of light.
  - processing and buffering delay: time to process a packet, time to wait in a queue.
- **Jitter** in msec: variation in latency. Average delay small but max delay large. Jitter is bad for real-time applications.

A single bit cannot go faster (bound by reality world and physics). The only way we can increase the speed is to **increase the number of bits** we send at a time (increase the **bandwidth**. i.e., bits packed into 1 second).

Internet traffic is **bursty**. e.g., real-time video streaming.

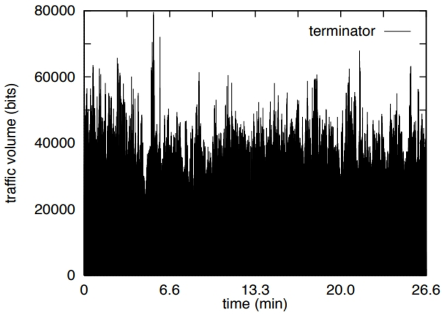

Figure 5: Bursty Internet Traffic Diagram

2 Fundamentals of Data Transmission