Week 5: Networking Services

POTS and Dial-Up

Dial-up, Modems and Point-to-Point Protocols

- Early networking technologies mostly focused on connecting devices within close physical proximity to each other.
- In the late 1970s, two grad students at Duke University realized they could piggyback off the public telephone network.
  - The public telephone network is known as the **Public Switched Telephone Network (PSTN)**
  - Colloquially called the **Plain Old Telephone Service (POTS)**
- Those two Duke grads built the system known as USENET

Dial-Up

A **dial-up connection** uses POTS for data transfer, and gets its name because the connection is established by actually dialing a phone number.

- Transferring data across a dial-up connection is done through devices called modems.
- **Modem** stands for "modulator/demodulator"
  - It takes data that computers can understand, and turns them into audio wavelengths that can be transmitted over POTS.
- Early modems had very low baud rates.
  - A **baud rate** is a measurement of how many bits can be passed across a phone line in a second.
  - In the 1950s, the average baud rate was 110 bits per second
  - By the days of USENET, the rate had increased to 300 bps
  - And by the time dial-up became a household service in the 1990s, it was 14.4 kbps

Dial-up Internet connectivity is very rare today; but it hasn't gone extinct. Some rural areas use it as the only Internet option.

Broadband Connections

What is broadband?

Broadband is any connectivity technology that isn't dial-up Internet.

- It refers to connections that are always on.
  - They're long-lasting connections that don't need to be established with each use
  - Thus, they're links that are always present.

A single dial-up connection would quickly be oversaturated by just a few users. So businesses began using T-carrier technologies in the 1990s to meet bandwidth needs.

T-carrier technologies were originally invented by AT&T in order to transmit multiple phone calls over a single link.

- These technologies require dedicated lines, which makes them more expensive (and generally only used by businesses).

T-Carrier Technologies

T-carrier technologies were first invented by AT&T in order to provision a system that allowed *lots of phone calls to travel across a single cable*.

- Before then, every individual phone call was made over individual pairs of copper wire.
- Then came *Transmission System 1 (T1)*, the first T-carrier specification
  - With T1, AT&T invented a way to carry up to 24 simultaneous phone calls across a single piece of twisted-pair copper.

        - Years later, this same technology was repurposed for data transfers.
    - Each of the 24 phone channels was capable of transmitting data at 64 kbps;
        - Thus, a single T1 line was capable of transmitting data at 1.544 megabits per second
- Over the years, "T1" has come to mean any twisted-pair copper connection capable of speeds of 1.544 mbps, even if it doesn't strictly follow the original Transmission System 1 specification.

T1 technology originally was only used to connect different telecom company sites to each other; and to connect these companies to other telecom companies.

- But with Internet progression in the 1990s, more businesses adopted T1 lines.
- The T1 line was improved by weaving multiple T1s to act as a single link.
    - So a T3 line is 28 T1s, all multiplexed, achieving a total throughput speed of 44.7 mbps

Digital Subscriber Lines

The twisted-pair copper wires used by telephone lines was capable of transmitting way more data than what was needed for voice-to-voice calls.

By operating at a frequency range that didn't interfere with normal phone calls, a technology known as **digital subscriber line (DSL)** was able to send much more data across the wire than traditional dial-up technologies.

- It also allowed for normal voice phone calls and data transfer to occur at the same time, on the same line.

DSLAM

DSL technologies also use their own modems: **digital subscriber line access multiplexers (DSLAM)**.

- Like dial-up modems, these devices establish data connections across phone lines;
- Unlike dial-up modems, they're usually long-running connections.
    - Generally a connection lasts from the moment the DSLAM is powered on, until the DSLAM is powered off.

Many types of DSL exist, but the two most common are ADSL and SDSL.

- **Asymmetric digital subscriber line (ADSL)** connections feature different speeds for outbound and incoming data.
    - This generally means faster download speeds and slower upload speeds.
- **Symmetric digital subscriber line (SDSL)** features upload and download connections with the same speed.
    - This connection type was originally used by businesses, who hosted servers; but is now common for the home user.
    - SDSL generally has an upper cap of 1.544 mbps (the same as a T1 line).
- Advancements in SDSL led to **high bit-rate digital subscriber lines (HDSL)**, which can transfer above 1.544 mbps.

Cable Broadband

In the 1940s, cable television technologies were developed. The idea was to provide television access to remote towns and rural homes, which were beyond the broadcast range of the era's television towers.

In 1984, Congress passed The Cable Communications Policy Act, which changed everything.

- The act deregulated the cable television business in the United States;
    - This sparked a boom in growth and adoption; and the rest of the world followed suit.
- By the 1990s, cable television infrastructure was on-par with the public telephone system's.
- And cable providers soon became interested in becoming a part of the Internet growth.

Cable companies realized coaxial cables were capable of transmitting much more data than what was required for TV viewing (just like the phone industry realized).

- Cable companies began using frequencies that didn't interfere with TV broadcasts;
    - Cable-based, high-speed Internet was born.
- And this is the technology we refer to when we say **cable broadband**.

Cable Internet access is generally a shared bandwidth technology.

- With DSL or dial-up, the home/business connection goes directly to a **central office (CO)**.
    - A long time ago, COs were actual offices staffed with telephone switchboard operators.
    - COs have since become smaller pieces of automated hardware, that retained the name.
- Technologies connected to COs are guaranteed a certain amount of bandwidth, since it's point-to-point.
- Cable Internet technologies, on the other side, use a shared bandwidth model.
    - Many users share a certain amount of bandwidth until the transmissions reach the ISP's core network.
    - This could be anywhere from a city block to an entire subdivision.

Cable Internet connections are usually managed by a **cable modem**.

- This is a device that sits at the edge of a consumer's network and connects it to the **cable modem termination system (CMTS)**

- The CMTS is what connects many different cable connections to an ISP's core network.

Fiber Connections

- The absolute maximum distance an electrical signal can travel across a copper cable, before it degrades too much and requires a repeater, is thousands of feet.
- Fiber can travel many, many miles before signal degradation, by contrast.

Core Internet networks have used fiber for a long time, due to its high speed and low degradation distance.

- Producing and laying fiber is much more expensive than using copper cables, so fiber was long only used by ISPs or data centers.
- But technology advancements has brought fiber closer and closer to the end user.

FTTX

FTTX stands for **fiber to the X**, where X can be one of many things:

- **Fiber to the neighborhood (FTTN)**
  - Data delivered to a single cabinet that serves a certain amount of the population.
  - From the cabinet, twisted-pair copper or coaxial cables might be used for the last length of distance.
- **Fiber to the building/business/basement (FTTB)**
  - A setup where fiber tech is used for data delivery to an individual building.
  - After that, twisted-pair copper is typically used to actually connect what's inside the building.
- **Fiber to the home (FTTH)**
  - Fiber is actually run to each individual residence in a neighborhood/apartment building.
- **Fiber to the premises (FTTP)**
  - This is another way of referring to FTTH *or* FTTB.

Optical Network Terminator (ONT)

- Instead of a modem, the demarcation point for fiber technologies is known as an **optical network terminator (ONT)**.
- An ONT converts data from protocols the fiber network can understand, to those that more traditional twisted-pair copper networks can understand.

WANs

Wide Area Network Technologies

Wide Area Network (WAN) acts like a single network, but spans across multiple physical locations.

- WAN technologies usually require a special link, contracted through your ISP.
  - The ISP handles sending your data from one site to the other;
  - So it's like all of your computers are in the same physical location.
- WANs work by using a variety of protocols at the data link layer, to transfer data from one site to another.
  - These protocols have much in common with core Internet routing protocols, instead of ethernet protocols.

WAN technologies are great for when you need to transport large amounts of data across lots of sites, because WAN tech is built to be super-fast.

- A business cable or DSL line are cheaper, but just can't handle the load required in these situations.

Example

- Imagine one network of computers on one side of the country; and another network of computers on the other.
- Each of those networks ends at a demarcation point, which is where the ISP's network takes over.
- The area between each demarcation point and the ISP's actual core network is called a **local loop**.
  - This local loop is similar to a T-carrier line, or a high-speed optical connection to the provider's regional office.
- From there it connects out to the ISP's core network and the Internet at large.

Point-to-Point VPNs

Point-to-point VPNs are a popular alternative to WAN technologies.

- With the advent of cloud computing services, the expense of WAN technologies are becoming unnecessary.
- Instead, businesses are turning to point-to-point VPNs, so different sites can still communicate with each other.

A **point-to-point VPN**, also known as a **site-to-site VPN**, establishes a VPN tunnel between two sites.

- It operates much like how traditional VPN setup does;
- But the VPN tunneling logic is handled by network devices at either end, so user don't all have to establish their own connections.

Wireless Networking

- Describe how wireless communication works
- What is the difference between infrastructure networks and ad hoc networks
- How do wireless channels help wireless networks operate
- Wireless security protocol basics

Introduction to Wireless Networking Technologies

Wireless networking is a way to network without wires.

IEEE 802.11 Standards

- The most common specs for how wireless networking devices should communicate are defined by the IEEE 802.11 standards.
  - This set, also called the 802.11 family, make up the set of technologies we call **Wi-Fi**.
- Different 802.11 standards generally use the same protocol, but might operate at different frequency bands.

A **frequency band** is a certain section of the radio spectrum, that's been agreed upon to be used for certain communications.

- EX: North American FM radio operates between 88 and 108 megahertz; this frequency band is called the FM broadcast band.
- Wi-Fi networks most commonly operate at the 2.4 gigahertz and 5 gigahertz bands.

The most common specifications are (in order of adoption):

- 802.11b
- 802.11a
- 802.11g
- 802.11n
- 802.11ac

Naturally, each newer version of the specs is an improvement over the predecessor.

802.11 defines how we operate at both the physical and data link layer.

802.11 Frames

An 802.11 frame has several fields:

- First is the **frame control field**, a 16-bit field divided into sub-fields, used to describe how the frame itself should be processed.
  - Which version of 802.11 was used, etc.
- Next is the **duration field**
  - It specifies how long the total frame is, so the receiver knows how long it should listen to the transmission.
- Then come four 6-bit long **address fields**:
  - Source address field (the MAC address of the sending device)
  - Intended network destination (on the network)
  - Receiving address (the MAC address of the access point that should receive the frame)
  - Transmitter address (the MAC address of whatever has just transmitted the frame)
    - Often, the destination and receiver addresses may be the same; and the source and transmitter addresses are also often the same.
- Between the third and fourth address field is the **sequence control field*
  - A 16-bit long field containing the sequence number used to keep track of ordering the frames.
- Then comes the **data payload** section
  - Which has all of the data of the protocols further up the stack.
- Finally comes the **frame check sequence** field
  - It contains a checksum for a cyclical redundancy check, just like how Ethernet does it.

Alphabet Soup

Networks that operate on the 5Ghz band are almost always faster, but have less of a range.

Most 2.4Ghz networks are slightly slower and more susceptible to interference, but cover a larger area.

Wireless Network Configurations

There are a few main ways a wireless network can be configured:

- Ad-hoc networks
  - Where nodes all speak directly to each other
- Wireless LANs (WLANs)
  - Where one or more acmes points act as a bridge between a wireless and a wired network
- Mesh networks

- A hybrid of ad-hoc and WLAN

Ad-hoc networks

- The simplest of the three
- No real supporting network infrastructure
- Every device involved with the network communicates with every other device within range, and all nodes help pass along messages

Wireless LANs (WLANs)

- The most common type of wireless network in the business world
- Consists of one ore more access points, which act as bridges between the wireless and wired networks.
- The wired network operates as a normal LAN;
  - Wireless devices communicate with access points;
  - Then they forward traffic to the gateway router, where everything proceeds as normal.

Mesh networks

- Similar to ad-hoc networks, since lots of the devices communicate with each other wirelessly (forming a *mesh*)
- Most mesh networks are made of only wireless access points, still connected to a wired network
- This kind of network lets you deploy more access points to the mesh, without having to run a cable to each of them
- This setup allows for increasing the performance and range of a wireless network.

Wireless Channels

Channels are individual, smaller sections of the overall frequency band used by a wireless network.

- Channels are important because they address collision domains.
  - Remember that a **collision domain** is any one network segment where one computer can interrupt another.
- Switches are devices that solve the problem of collision domains, on wired networks.
  - But wireless networks don't have switches.
- Channels help fix this problem, to a certain extent.

Radio waves are imprecise things, so you need some buffers around what exact frequencies a transmission might actually arrive on.

- Some channels overlap, but some are far enough apart so they won't interfere with each other at all.
- Most wireless networking equipment today can auto-sense what channels are most congested.
  - Some access points will only perform this analysis on startup;
  - Others will dynamically change their channel as needed

The key point of channels is avoid collision domains wherever you can. Optimize wireless network deployments, and make sure both your own access points and those of neighboring businesses overlap channels as little as possible.

Wireless Security

Wireless networking lacks the physical security measures of wired networking. In theory, anyone can intercept any wireless transmission. Enter WEP.

Wired Equivalent Privacy (WEP) is an encryption technology that provides a very low level of privacy.

- WEP is only as safe as sending unencrypted data over a wired connection.
- The WEP standard is a weak encryption algorithm, at only 40 bits for its keys.
- WEP was quickly replaced by WPA.

Wi-Fi Protected Access (WPA) was an improvement over WEP.

- WPA uses a 128-bit key, making it more difficult to crack

WPA2 is today's wireless networking security standard.

- It uses a 256-bit key

Another way to help secure wireless networks is through MAC filtering.

MAC filtering configures access points to only allow for connections from a specific set of MAC addresses, belonging to trusted devices.

Cellular Networking

Cellular networking--also called mobile networking--is becoming a predominant wireless networking method.

Cellular networks have much in common with 802.11 networks, featuring many specifications.

Just like Wi-Fi, cellular networks operate over radio waves, with specific frequency bands specifically reserved for cellular transmissions.

But what's different is cellular transmission frequencies can travel over longer distances more easily, usually over many miles.

Cellular networks are built around the concept of *cells*.

- Each cell is assigned a specific frequency band for use.
- Neighboring cells are set up to use bands that don't overlap
  - (Like how an optimal WLAN is setup with multiple access points.)
- A good way to think of cell towers that broadcast and receive transmissions is as *access points*
- Cellular networks aren't reserved for only phones
  - Tablets, laptops, and even automobiles feature cellular antennas.

Mobile Device Networks

Mobile devices use wireless networks to communicate with the Internet and other devices. This can include:

- Cellular networks
- Wi-Fi
- Bluetooth
- Internet of Things network protocols

Mobile devices tend to use *non-metered connections* when available, to save on expenses.

Bluetooth Pairing

- Mobile devices connect to their peripherals using short-range wireless networks.
- The most common of these is called **Bluetooth**.
- This connection is called *pairing* the devices:
  - The two devices exchange information (sometimes a PIN or password) so they can remember each other.
  - From then on, the devices will automatically connect to each other when they're both powers on and in range.
  - Pairing can sometimes fail, and may require making the device forget the peripheral so it can be paired again.

Questions for review

Keywords

Concepts