Week 1: Introduction to Networking

Describe how the TCP/IP five layer network model works. Identify basic networking devices. Label each of the five layers in the TCP/IP network model. Describe how the physical layer works. Describe how the data link layer works.

Introduction to Computer Networking

Course Introduction

Protocol: A defined set of standards that computers must follow in order to communicate properly.

Computer networking: The name we've given to the full scope of how computers communicate with each other.

"Networking involves ensuring that computers can hear each other, that they speak protocols other computers can understand, [and] that they repeat messages not fully delivered."

The TCP/IP Five-Layer Network Model

#	Layer Name
5	Application
4	Transport
3	Network
2	Data Link
1	Physical

Physical Layer

- *Represents the physical devices that interconnect computers.*
- Includes specs for networking cables and connectors that join devices
- Also includes specs for how signals are sent over these connections

Data Link Layer

- (Also known as the "network interface", or "network access layer.")
- *Responsible for defining a common way of interpreting these signals so network devices can communicate.*- The data link layer is responsible for getting data across a single link.
- The most common (of many) protocols at the data link layer is Ethernet
  - The **Ethernet** standards also define a protocol responsible for getting data to nodes on the same network or link.

Network Layer

- (Also known as the "Internet layer.")
- *Allows different networks to communicate with each other through devices known as routers.*
- **Internetwork:** A collection of networks connected together through routers
  - The most famous of these is the **Internet**.
- This layer is responsible for getting data delivered across a connection of networks.
- The most common protocol of this layer is **Internet Protocol (IP)**

    - **IP** is the heart of the Internet and most smaller networks around the world
- Network software is usually divided into *client* and *server* categories
    - A single node may run multiple client or server applications

Transport Layer

- *While the network layer delivers data between two individual nodes,* ***the transport layer sorts out which client and server programs are supposed to get that data****.*
    - The network layer is responsible for getting data from one node to another;
    - The transport layer is responsible for ensuring that data gets to the right applications running on those nodes.
- **Transmission Control Protocol (TCP)** is the most common protocol used at this layer
- **User Datagram Protocol (UDP)** is an alternative protocol.

Application Layer

- Many different protocols exist at this layer, and they are all application-specific.
    - HTTP is one such protocol

The TCP/IP Mail Analogy

1. The *physical layer* is the delivery truck and the roads;
2. The *data link layer* is how the delivery trucks get from one intersection to the next, over and over;
3. The *network layer* identifies which roads need to taken to get from address A to address b;
4. The *transport layer* ensures that the delivery driver knows how to knock on your door to tell you that your package has arrived;
5. The *application layer* is the contents of the package itself.

Parting Notes

- The traditional TCP/IP Model only has four layers, as it doesn't differentiate between the physical layer and the data link layer.
    - The fundamental concepts remain the same, however.
- The other well-known model is the **OSI model**, which is taught by network certification by Net+, Cisco, and others.
    - The main difference is the TCP/IP has five layers, whereas OSI has seven
    - The OSI model abstracts the application layer into three layers total

The Basics of Networking Devices

Cables

Cables are what connect different devices to each other, allowing data to be transmitted over them.

- Today's networking cables usually fall into one of two categories:
    i. Copper
    ii. Fiber

Copper

- *Copper* cables are the most common form of networking cable.
    - They're made up of multiple pairs of copper wires inside plastic insulator.
    - These copper wires transmit binary data, using voltage between two ranges.
        - The system receiving the data interprets the voltage changes as binary ones and zeroes.

The most common forms of copper twisted-pair cables are **Cat5**, **Cat5e**, and **Cat6** cables. (Cat is short for "category.")

- The categories have different physical characteristics.
    - But differences in how the twisted pars are arranged inside can drastically alter how quickly data can be transmitted; and how resistant the signals are to outside interference.
- Cat5 has mostly been replaced by Cat5e, because Cat5e's internals reduce **crosstalk**.
- **Crosstalk** is when an electrical pulse on one wire is accidentally detected another wire.
    - This means the receiving end can't understand the data, resulting in a network error.
- Cat5e cables' higher quality specifications make it less likely that data needs to be retransmitted.
- Cat6 cables follow even more strict specification to avoid crosstalk, making those cables more expensive.
    - Cat6 cables can transfer data faster and more reliably than Cat5e cables can.
    - However, due to their internal arrangement, they have a shorter maximum distance when used at higher speeds.

Fiber

- Fiber is short for *fiber optic cables*.
- **Fiber cables** contain individual optical fibers, which are tiny tubes made out of glass about the width of a human hair.
    - These tubes of glass transport beams of light.
    - Unlike the voltage of copper cables, fiber cables use pulses of light to transmit binary data.
- You're more likely to encounter fiber cables at data centers than you are in offices or residences.

The advantages of fiber optic cables:

- Aren't effected by electromagnetic interference like copper wires are.
- Generally transport data quicker.
- Can transport data over much longer distances than copper, without suffering potential data loss.

However, fiber cables are much more expensive and fragile than copper cables.

Hubs and Switches

- **Hub:** A physical layer device that allows for connections from many computers at once.
    - Hubs allow all computers to talk to each other, resulting in a lot of noise and creating a collision domain.
    - A **collision domain** is a network segment where only one device can communicate at a time.
        - If multiple systems try sending data at the same time, the electrical pulses sent across the cable can interfere with each other.
        - It causes systems to have to wait for a "quiet period" before they try resending the data.
    - Because of this, hubs are rare and mostly a historical artifact today.

Instead, the more common way of connecting many computers today is a network switch (originally known as a *switching hub*)

- A **switch** is very similar to a hub; but while a hub is a layer one (physical layer) device, a switch is a layer two (data link layer) device.
    - Thus, a switch acts like a postmaster at a mail center:
        - Inspecting the contents of ethernet protocol data;
        - Determining which system the data is intended for;
        - And sending the data to only that particular system.

Switches drastically reduce (or totally eliminate) the problem of collision domains on a network; resulting in fewer re-transmissions and higher overall throughput.

Routers

Hubs and switches are the primary devices used to connect computers on a single network, usually referred to as a *LAN*, or *local area network*.

But if you want to send or receive data to computers on other networks, you need a router.

Routers

A **router** is a device that knows how to forward data between independent networks.

- While a hub is a layer one device, and a switch is a layer two device, a router is a layer three (network layer) device.
- Routers inspect IP data to determine where to send things, like how switches inspect ethernet data to determine where to send things.

The purpose of most routers is to forward traffic coming from the home or office LAN, and forward it to the Internet service provider (ISP).

- Once traffic is at the ISP, a more complex router known as a *core router* takes over.
- **Core ISP routers** are the backbone of the Internet.
    - They are directly responsible for how data is sent and received across the Internet every day.
    - Not only do core routers handle way more traffic than home routers, but they also make significantly more complex decisions about where to sent traffic.
    - They also usually have many different connections to many other routers.

Routers share data

- Routers share data with each other via a protocol known as the **border gateway protocol (BGP)**.
    - The BGP lets them learn about the most optimal paths to forward traffic.
    - When you open a web browser and load a web page, the traffic between computers and the web servers could have traveled over dozens of different routers.

In summary, routers are the global guides to getting Internet traffic to the right places.

- A *server* is as something that provides data to something requesting that data.

- The thing receiving the data, is referred to as a *client*.
- Not just nodes can be servers or clients--individual computer programs running on the same node can be servers and clients to each other, too.
- Most devices are not purely servers or clients--almost all nodes are both at some point in time.
    - EX: An email server is referred to as a *server*, despite it itself being a client to a DNS server.
        - Why?
        - Because its primary purpose is to serve data to clients.
    - Another example is a desktop occasionally acts as a server, while its primary purpose is to act as a client so the computer user can perform tasks.
- Regardless, in most network topographies, each node is primarily either a server or client.

In summary

"[A] server is anything that can provide data to a client, but we also use the words to refer to the primary purpose of various nodes on our network."

The Physical Layer

Moving Bits Across the Wire

- *"The physical layer consists of devices and means of transmitting bits across computer networks."*
- A **bit** is the smallest representation fo data that a computer can understand; a one or a zero.
    - These ones and zeroes sent across networks are what make up the frames and packets of data in networking.
    - Copper network cables constantly carry an electrical charge
    - Bits travel across this network in a process called modulation
    - **Modulation** is a way of varying the voltage of this charge using across the cable
- Modulation, as applied to computer networking, is more specifically known as *line coding*
    - Line coding allows devices on either end of a link to understand whether an electrical charge is a one or a zero.

Twisted Pair Cabling and Duplexing

- The most common cabling type for connecting computer devices is known as *twisted pair cable*.
    - Named because it contains pairs of copper wires that are twisted together.
    - The pair of wires act as a single conduit for information.
    - Being twisted helps protect against electromagnetic interference and crosstalk from other networks.
- Twisted pair cables allow for duplex communication.
    - **Duplex communication** is the concept that information can flow in both directions across the table.
    - This is contrast to **simplex communication**, which is unidirectional.
        - Simplex communication: Baby monitor (only one way) = Duplex communication: Phone (two way)
- Networking cables ensure duplex communication is possible by reserving one or two pairs for communicating in one direction.
    - Then, they use the other pairs for communicating in the *other* direction.
- Both devices communicating at the exact same time is called **full-duplex**.
- **Half-duplex** is what happens when there are network connection problems;
    - Communication is still *possible* in each direction;
    - But only one device can be communicating at a time.

Network Ports and Patch Panels

The final part of the physical layer process are the endpoints of network links.

- Twisted pair cables terminate with a plug, which takes the individual internal wires and exposes them.
- The most common plug is the **Registered Jack 45 (RJ45)**.
- Network ports are generally directly attached to devices that make up a computer network.
    - Switches would have many network ports; whereas a server or desktop would only have one or two.

Most network ports have two small LED lights: The link LED, and the activity LED

- The link LED will be lit when a cable is properly connected to two devices that are both powered on.
- The activity LED will flash when data is actively transmitted across the cable.

A **patch panel** is a device containing many network ports, but it does no other work.

- It's just a container for the endpoints of many runs of cable.
- Patch panels in turn run cables to switches or routers, to provide network access.

The Data Link layer

Ethernet and MAC Addresses

Despite widespread consumer adoption of Wi-Fi, traditional cable networks still make up the bulk of networking in businesses and data centers.

- **Ethernet** is the protocol most widely used to send data across individual links.
- Ethernet and the data link layer allow software at higher levels of the stack to send and receive data.
- The primary purpose of the data link layer is to do the handle interpreting the hardware and physical layers, for the higher layers.
    - By dumping this responsibility on the data link layer, the Internet, transport and application layers can all operate the same no matter how the device they're running on is connected.
- Ethernet was first invented in 1980, and published/standardized in 1983.
    - It's largely the same today as it was back then.
    - Ethernet came about because switches or switchable hubs hadn't yet been invented.
        - This meant basically all devices on a network shared a single collision domain (where only one device can speak at a time).
- Ethernet solved the unintelligible results of single collision domains by introducing *carrier sense multiple access with collision detection* (CSMA/CD).
    - **CSMA/CD** is used to determine when the communications channels are clear and when the device is free to transmit data.
        - With CSMA/CD, computers can detect data collision, then will wait a moment before trying to send data again.
- When a network segment is a collision domain, it means that all devices on that segment receive all communication across the entire segment.
    - This means we need a way to identify which node the transmission was actually meant for.
    - This is where something known as a *media access control address* (or MAC address) comes into play.
- A **MAC address** is a globally unique identifier attached to an individual network interface.
    - It's a 48-bit number normally represented by six groupings of two hexadecimal numbers.
- **Hexadecimal** is a way to represent numbers using 16 digits (like how binary uses 2 digits)
    - Hexadecimal (or *hex*) represents the numbers 10 through 15 by the letters A through F, respectively.
- Another way to reference each group of numbers in a MAC address is an octet.
    - In computer networking, an **octet** is any number that can be represented by 8 bits.
    - Two hexadecimal digits can represent the same numbers that 8 bits can.
- MAC addresses are globally unique because a 48-bit number has literally hundreds of trillions of possible values.
- The first three octets of a MAC address are the **organizationally unique identifier (OUI)**
    - These are assigned to individual hardware manufacturers by the Institute of Electrical and Electronics Engineers (IEEE).
    - Hence, you can always identify the manufacturer of a network interface purely by its MAC address.
- The last three octets can be assigned any way, so long as they remain globally unique.

"***Ethernet** uses **MAC** addresses to ensure that the data it sends has both an address for the machine that sent the transmission; as well as the one the transmission was intended for.*"

- Thus, even on a single collision domain, each node on the network knows when traffic is intended for it.

Unicast, Multicast, and Broadcast

- At the Ethernet level, you look at a special bit in the destination MAC address, to determine the type of transmission.

Unicast

If the least significant bit in the first octet of a destination address is set to zero, it means that Ethernet frame is intended for only the destination address.

- A **unicast** transmission is always meant for just one receiving address.
  - One device transmitting data to one other device.

Multicast

If the least significant bit in the first octet of a destination address is set to one, it means you're dealing with a multicast frame.

- A **multicast** frame is similarly set to all devices on the local network signal.
- What's different is that it will be accepted or discarded by each device depending on criteria aside from their own hardware MAC address.
  - Network interfaces can be configured to accept lists of configured multicast addresses for these sort of communication.

Broadcast

An Ethernet broadcast is sent to every single device on a LAN.

- This is accomplished by using a special destination known as a broadcast address.
  - The Ethernet broadcast address is all Fs.
- Ethernet broadcasts are used so that devices can learn more about each other.

Dissecting an Ethernet Frame

- A **data packet** is an all-encompassing term that represents any single set of binary data being sent across a network link.
  - Data packets at the Ethernet level are known as Ethernet frames.
- An **Ethernet frame** is a highly structured collection of information presented in a specific order.
  - It allows network interfaces at the physical layer to convert a string of bits into meaningful data (or vice versa).

Anatomy of an Ethernet Frame

- The first part of an Ethernet frame is known as the preamble.
  - A **preamble** is 8 bytes (or 64 bits long) and can itself be split into two sections.
  - The first seven bytes are a series of alternating ones and zeros.
    - These act partially as a buffer between frames and can also be used by the network interfaces to synchronize internal clocks they use, to regulate the speed at which they send data.
  - This last byte in the preamble is known as the **start frame delimiter (SFD)**.
    - This signals to a receiving device that the preamble is over and that the actual frame contents will now follow.
- Immediately following the start frame delimiter, comes the **destination MAC address**.
  - This is the hardware address of the intended recipient.
- Which is then followed by the source MAC address--where the frame originated from.
  - *(Don't forget that each MAC address is 48 bits or 6 bytes long.)*
- The next part of an Ethernet frame is called the **EtherType field***.
  - It's 16 bits long and used to describe the protocol of the contents of the frame.

Instead of the EtherType field, you could also find a **VLAN header**.

- A VLAN header indicates that the frame itself is a VLAN frame.
- If a VLAN header is present, the EtherType field follows it.
- VLAN stands for virtual LAN.
  - It allows you to have multiple logical LANs operating on the same physical equipment.
  - VLAN tags will only be delivered out of a switch configured to relay that specific tag.
    - This allows a single network to operate like multiple LANs
    - Like IP phones operating on one VLAN, and desktops operating on another.

After this, you find the data payload of an Ethernet frame.

- A **payload** in networking terms, is the actual data being transported (which is everything that isn't a header).
  - The data payload of traditional Ethernet frames ranges from 46 to 1500 bytes long.
- The payload contains all of the data from the higher layers (like IP, transport, and application) that's actually being transmitted.

Following this is the **frame check sequence**.

- This is a 4-byte (or 32-bit) number that represents a checksum value for the entire frame.
  - The **checksum value** is calculated by performing what's known as a *cyclical redundancy check* against the frame.
- A **cyclical redundancy check (CRC)** is an important concept for data integrity, used across all computing (not just network transmissions).
  - It's basically a specified calculation that the sender computes, and logs.
  - The recipient then performs the calculation, and compares it against the sender's log.
  - If the calculation doesn't exactly match, the data is inferred to be corrupted or lost during transmission.
    - It's then up to a protocol at a higher layer to decide if that data should be retransmitted.
    - *(Ethernet itself only reports on data integrity. It doesn't perform data recovery.)*

Questions for review

Keywords

▶ What is a node?

▶ What is a client?

▶ What is a server?

▶ What is the most common form of cable?

▶ What is collision domain?

▶ What is a switch?

▶ What is UDP?

▶ How many octets are there in a MAC address?

Concepts

▶ Why did hubs fall out of favor?

▶ What's the difference between a hub and a switch?

▶ What's the purpose of the Data Link layer?