Work today

- Standards and Web’s relationship to the NJ CS SLS
- Networks - why do we study them?
- Basic Concepts on Networks
- Basic Concepts of Network Security
Exercise 1

Name 5 different computers or devices that you know that connect to the Internet in your environment.
Networks - Gr 3-5 Standard

The Gr 6-8 Standard is a huge leap from the Gr 3-5 standard. In the Gr 3-5 standard, students have to understand basically data is transmitted both wirelessly and with wired communication.

The Gr 6-8 Standard starts to address the actual technology on how a network works.
Why do students need to learn this?

Students need to understand this because, on their person, at any given point in time they are connecting with usually one if not multiple networks.

Consider your average middle schooler: Most have a chromebook and a phone on their person. The chromebook is connecting to the school network and the phone is connecting to the larger telecommunications network. The student may also have a smart watch, smart ring or smart glasses on their person.

If the child has a significant health problem, like a cardiac, neurological, or endocrine challenge like diabetes, they may also be wearing a networked medical assistive device.
Standards we are addressing - Gr 6-8 Networks

<table>
<thead>
<tr>
<th>Core Idea</th>
<th>Performance Expectations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols, packets, and addressing are the key components for reliable</td>
<td>8.1.8.NI.1: Model how information is broken down into smaller pieces, transmitted as addressed packets through multiple devices over networks and the Internet, and</td>
</tr>
<tr>
<td>delivery of information across networks.</td>
<td>reassembled at the destination. • 8.1.8.NI.2: Model the role of protocols in transmitting data across networks and the Internet and how they enable secure and errorless communication.</td>
</tr>
<tr>
<td>The information sent and received across networks can be protected from</td>
<td>8.1.8.IC.1: Compare the trade-offs associated with computing technologies that affect individual’s everyday activities and career options. 8.1.8.IC.2: Describe</td>
</tr>
</tbody>
</table>
Example of Wearable

Wearable are taking the world by storm. Students will need to be able to navigate this world to understand their comfort levels and how to socialize and cope with this world.

Image Source:
Networks - why learn them

There are two major issues at play with network and why students need to learn them:

1. Students need to be able to understand how to connect their devices to the network.
2. Students need to learn how to protect both their data and their devices from any on-line security issues.
Teenagers and the economics of Hacking

● In 2017, families with members under the age of 20 lost $8.7 million in hacking schemes.
● In 2021, families in this same demographic lost $101 million.
● The United States is the primary target for most international hacking.
● New Jersey is in the top 10 states for being targeted in hacking or malicious attacks.

*Source: FBI Internet Crimes Complaint Center
What is a network?

- A connection between two or more computers so that they can share:
  - Data
  - Communication
  - Printing
  - Files
  - Other resources

- A Network is Modeled as:
  - Line represents a connection
  - A Circle (vertex, node) represents a “thing” we are connecting - a computer, a website, etc.
Exercise 2

You have string on the table.

Pretend that each person at the table is a computer. Create a connection between at least two computers using your “Wire” which is the string.

How do you think the computers communicate?
Protocols are the system of rules by which communication happens. Humans have protocols in their communication. Computers use protocols to communicate with each other.
HTTP Protocol
Exercise 3

Pick one person as your message sender, pick one person as your message receiver.

Sender: Write a sentence that is 5 words long - write each word - and only each word - on a index card. Do not tell your receiver what the message is. Shuffle the cards and “send” the cards over your wire to your receiver.

Receiver: Rebuild the message without any help or directions. Check with the sender.
Exercise 3 - Debrief

Questions:

- What do you observe about sending the message?
  - How did you send it across the network?
  - Did you give any vocal directions about how to send the message?
  - Did you give any body language clues about how to send the message?

- What do you observe about receiving the message?
  - Did the cards have any clues about what order the words should have been in?

- Would a little more directions help you in putting the message together?
Exercise 4

Redo this exercise - but pick a sender who speaks a foreign language.

What challenges do we face?
More on Protocols

Protocols define how my hardware connects, how my data is transported - both in routing the data and the “driving directions” for particular data, and the format of the data going over the network.

Anything that goes over a network uses protocols.

Popular Protocols

- SMTP/POP3/IMAP: Email
- SFTP/FTP: Secure File Transfer Protocol
- HTTP(S): Hypertext Transfer Protocol (Secure)
WWW and the Internet - are they the same thing?

NO!!!!

The Internet is the physical network of computing devices - the physical connection and how the physical connections are managed.

The World Web Web is a service that gives us a type of data that is transmitted over the Internet. It is one - albeit very large - service of the internet.

Examples of other services: Email, Instant or Private Messaging, Movie or Music Streaming, File Transfers.

These services work with one another to create a seamless experience, but they are different.
Internet vs WWW

https://www.javatpoint.com/what-is-world-wide-web
A network is the connection between two computational devices. Usually they are “equals”, that is both are computational devices - so a mouse connecting to a computer is usually not considered a network though many now use wireless network connections.

Network can be described (or classified) based on:

- How do we connect (wireless or wired)
- How it is laid out (topology)
- Who owns the network
Basics of Networks - Ring Topology
Exercise 5

At your table, create the ring topology network.

Pick a sender who will send a (new) 5 word message.

Pick a receiver who will receive and put the 5 word message back together again.

- What do you observe about sending the message?
- What do you observe about receiving the message?
- Would a little more directions help you in putting the message together?
- What happens if you remove one link - do you keep the same ability?
Basics of Networks
Basics of Networks - Mesh Topology (every node connected to every other node - used for Peer to Peer Networks)
Exercise 6

At your table, create the ring topology network.

Pick a sender who will send a (new) 5 word message.

Pick a receiver who will receive and put the 5 word message back together again.

- What do you observe about sending the message?
- What do you observe about receiving the message?
- Would a little more directions help you in putting the message together?
- What happens if you remove one link - do you keep the same ability?
- How many links do you need to remove to make a node unreachable?
Basics of Networks
Basics of Networks - Star Topology (used for client/server)
Exercise 7

At your table, create the ring topology network.

Pick a sender who will send a (new) 5 word message.

Pick a receiver who will receive and put the 5 word message back together again.

- What do you observe about sending the message?
- What do you observe about receiving the message?
- Would a little more directions help you in putting the message together?
- What happens if you remove one link - do you keep the same ability?
- How many links do you need to remove to make a node unreachable?
Basics of Networks
How a network is laid out

We call the the way a network is laid out topology.

Wireless Network: Connect to a wireless access point like a router or a repeater or an extender - Need line of sight.

Wired Networks: There is a physical wire that connects devices. There can be a lot of different layouts.
How do we connect - wired vs wireless?

Wireless

Image Credit:
Wireless Network

Wireless Networks need “line of Sight”, that is the radio signal must be able to reach the device.

On a wired network, the signal follows a dedicated path (the wire). On a wireless network, it is broadcast.
An anatomy of a Protocol

A Protocol in general has a header and a body.

- **Header**: The header gives directions about details about the message being sent.
- **Body**: The body has the information that we are trying to transmit.
- **Different protocols break up the messages in different ways.**
TCP/IP Protocol

- The TCP/IP Protocol - created in the late 1960s/ early 1970s as a part of the ARPANET project.
- TCP/IP is based on the idea of a packet.
- Packets: a small piece of data we want to transmit from a sender to a receiver.
- TCP/IP breaks a message into packets, where the header gives directions for routing the message and how to assemble the packets. The body is some small part of the data we want to send.
- TCP: Collects and reassembles packets
- IP: Transmits and routes packets
Exercise 8

As a table, create a scheme for breaking up a sentence that is not by word. For example, every 4 characters (note spaces and punctuation are characters).

Pick any topology that you want.

Sender: Create a message - break it up into packets on your index cards. Only put the characters on it.

Receiver: Try to reassemble the message.

What were the challenges?
Exercise 9

Redo Exercise 8: Now on the opposite side add the following: source, destination, and packet number (1 of x, where x is the number of packets). As a table, create a scheme for breaking up a sentence that is not by word. For example, every 4 characters (note spaces and punctuation are characters.

Pick any topology that you want.

Sender: Create a message - break it up into packets on your index cards. Only put the characters on it.

Receiver: Try to reassemble the message.

Was it easier? Do you think you had more freedom in sending the messages
TCP/IP - anatomy of a packet
Error Correction and Packets

Most Protocols have error correction techniques.

Error Detection Techniques:

**Checksum**: tells the destination how many bits it should receive. When a computer receives a packet, it checks against the checksum that the message is the right size.

**Acknowledgement**: The destination sends back an acknowledgement message to indicate the message is received.

**Retransmission after time out**: The message is retransmitted after a certain amount of time elapses.
Internet Software Layers

- **Application**: Constructs message with address
- **Transport**: Chops message into packets
- **Network**: Handles routing through the Internet
- **Link**: Handles actual transmission of packets
Figure 4.13  The Internet software layers
Figure 4.14 Following a message through the Internet

- **Application**
  - Prepares message and provides destination address
  - Chops message into packets
  - Assigns intermediate address to each packet
  - Transfers packet

- **Transport**
  - Receives message
  - Collects packets and reassembles message

- **Network**
  - At each intermediate stop, the network layer determines the direction in which the packet should be forwarded
  - Detects that packet has reached its final destination

- **Link**
  - Receives packet
Client/Server vs Peer to Peer

Client/Server: a network model or architecture between a client and the server where the client sends a request, and the job of the server is to fulfill whatever the client’s request is. Used for majority of network needs.

Peer-to-Peer (P2P): a network is created when two or more PCs are connected and share resources without going through a separate server computer. Used for gaming and smaller activities. BitTorrent - a protocol for sharing large files - has been used for sharing movies and other large media. Facebook, Twitter and US Government use it internally.
Network Security

8.1.8.NI.3: Explain how network security depends on a combination of hardware, software, and practices that control access to data and systems.

• 8.1.8.NI.4: Explain how new security measures have been created in response to key malware events.
Network Security and Hardware

**Hardware Firewall**: a physical device that enforces a network boundary. Can be used to filter certain websites (i.e., your school probably has a firewall that prevents certain websites from being accessed by students).

All network links cross over this hardware allowing for the analysis of the incoming and outgoing traffic.

**Access Control**: Only allowing access to certain systems from certain physical locations.

**Proxy server**: An intermediary server that retrieves data from an Internet source, such as a webpage, on behalf of a user.
HOW A FIREWALL WORKS

Image courtesy https://drsoft.com
Ways to violate Hardware Security

- **Manufacturer “Backdoors”**
  - Used as a means to administer a network device, usually set with a default username / password.

- **Eavesdropping, Intercepting Network Packets**
  - Unsecured messages, files, logon information, etc. can be intercepted as it is sent over the internet - especially public wifi, hotspots, etc. Packet sniffing software can be used at payment terminals.

- **Redirecting Traffic**
  - Routers usually come with a built-in firewall. A hacker could configure this firewall to direct traffic to a destination of their choosing, in the same way we might use it to prevent access to certain websites.

- **DOS / DDOS Attack**
  - One or more computers used to flood a network with packets and slow down traffic.
Network Security and Software

● **Computer anti-virus**
  ○ Software that can detect and eliminate computer viruses and malware
  ○ Often runs independently and continuously in background

● **Internet protection**
  ○ Most modern web browsers detect potential malware and will block and warn before going to a potentially malicious website

● **Threat monitoring**
  ○ Can include monitoring network traffic to detect and block potential attacks
  ○ Software firewall (built into computer) provides a line of defense, checking incoming and outgoing network traffic to your computer
Ways to violate Software Security

**Malware:** Broad consensus among antivirus software that program is malicious or obtained from flagged sources. Umbrella term for malicious software

**Viruses:** a type of malware designed to alter the way a computer operates, or cause harm to the computer system by inserting its own code into those programs

**Worms:** a standalone malware computer program that replicates itself in order to spread to other computers via a network

**Rootkits:** a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software

**Backdoor:** a typically covert method of bypassing normal authentication or encryption in a computer, product, or embedded device. Often manufacturer installed, and exploited by a hacker
Network Security and Practices

Passwords

- Unique sequences of characters. The longer the string with diverse characters the better.
- Hashing passwords: putting a password through a hashing algorithm (bcrypt, SHA, etc) to turn plaintext into an unintelligible series of numbers and letters.
- Salting passwords: a technique to protect passwords stored in databases by adding a string of 32 or more characters and then hashing them
- Encrypting passwords: Encryption scrambles your password so it’s unreadable and/or unusable by hackers.

Biometrics: unique physical characteristics, such as fingerprints, that can be used for automated recognition.

Multifactor Authentication: an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN.
Ways to violate Practices Security

How to get around passwords:
● Brute force attack
● Social Engineering
  ○ Phishing
  ○ Keylogger
  ○ Malware

How to get around biometrics:
● Fingerprints easy to hack - graphite and white paper, tape, high resolution pictures
● High resolution image of the eye
● Social Engineering

How to get around multifactor authentication (2fa or mfa):
● Simjacking - hacking your simcard
● Malware can get around MFA
● Text messages can be intercepted and they are not encrypted
● Social Engineering
Key Responses to Network Security

● **Improved firewall rules**
  ○ When a network suffers any kind of malicious attack, security experts will often analyze firewall rules and update / modify them to protect against new attacks and vulnerabilities

● **Software patches**
  ○ When a security vulnerability is exploited in a malicious way, the vendor will update the software to protect against the vulnerability. For example, there was a major security flaw in Apple’s macOS High Sierra that allowed anyone to gain administrator access to any individual mac computer with the operating system. Apple released a “patch”, or a software update, to prevent this from occurring and protect against potential threats

● **Segregating the network**
  ○ Segregating a network involves identifying devices on the network that contain sensitive information, and separating them from the general network. For example, at a school a server containing budget information would not reside in the same part of a network as student devices accessing the internet