Talking Machines

Machines need to communicate with each other. Though there's plenty a computer can do on its own, there's much more it can't. Browsing the internet, sending and receiving files, and making connections between systems—they all need a way for computers to communicate.

At the same time, a computer can't just accept any information being sent in. Otherwise, our machines would be overrun with malware and viruses. Not all information coming from an outside network is trustworthy, which is why we have firewalls.

So how exactly does this communication work? Let's imagine two computers, A & B. A wants to send over some information to B. The first thing A needs to do, then, is find out B's IP address. A can use B's IP address to make it clear that B is the recipient of this information.

Then, A translates its message into an understandable, universal computer language—based on either TCP or UDP. TCP (short for Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the main sets of rules that governs how messages are formatted and transmitted. They're both very widely used, but for different purposes.

TCP focuses on sending accurate and reliable information. It's great for a lot of places where getting the right information is more important than getting it quickly, such as the World Wide Web, email, and file transfer. It also needs a connection to be made between two systems before information can be sent across it, which helps shield against bad actors.

On the other hand, UDP is extremely important for time-sensitive communication. Though using UDP makes you much more likely to end up with a few lost messages, you'll receive and send your information a lot faster than with TCP. UDP is very common in video and audio streaming, along with lot of fundamental internet applications. UDP also doesn't need a connection to be set up before sending information, which can be both dangerous and useful.

A will choose one of these to send its message to B, and then pass the data along over either a wireless or wired connection.

Harbors at Sea

So what is a port, exactly? The name comes from ports in shipping, where boats load or unload their cargo. They are places where goods arrive from different places or are picked up to be sent off. In computing, and in digital communication, they have a similar purpose.

In computers, though, these ports aren't physical. They're the digital locations where networks connect to each other, created to help computers organize the information they receive. So if A is sending information to B, it'll be sending that message from one of its many ports to one of

B's. The specific ports it chooses to use will vary, but many ports are meant to be used for specific purposes.

For example, ports 80 and 443 match up with HTTP and HTTPS respectively, which are the main ways through which you connect to websites. Ports 20 and 21 are where computers can transfer files through FTP (the file transfer protocol), though it's used less nowadays because it's considered less secure. There are a lot of known vulnerabilities around FTP.

There are a lot of ports, though—65,000+ possible ports, even if not all of them usually used! It's important to not leave unused ports open or unsecured, because that gives attackers the opportunity to make a connection and send in or steal information. Firewalls protect most of these unused ports, preventing external connections and closing ports that aren't used. Only open ports can generally form a connection or receive information. However, these open ports can receive and process information both independently and at the same time. So a very large amount of information can be passed around at a time.

Anonymous Anomymous

One of these ports, FTP port 21, is known to be less secure. There are several well-known ways in which FTP ports can be exposed to attacks, letting curious hackers read logins and steal information while it's being sent. One of these ways is an anonymous login, allowing anyone to login without credentials and sent or retrieve information. This was used for the purposes of letting people get information from public libraries or repositories, but by itself, it's dangerous to keep available and enabled.

FTP is hard to use directly, especially from the command line, but there are several tools than can be used to make this easier. One common tool for networking connections, including FTP, is called WinSCP. With an intuitive interface, it's one of many different tools a cybersecurity professional might keep in their back pocket, ready to intercept attacks or check for any weak points in a system. It can be used for a direct login with a username and password of "anonymous" too, making it simple to either enter a system or to check whether it's secure.

Networking is a complicated topic, with a lot of interesting paths to explore. For more information, check out one of the links below.

To learn more:
https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html#~types-of-networks
https://computersciencewiki.org/index.php/Data_packet
https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/
https://opensource.com/article/18/10/common-network-ports
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml