

Today's Topic: Computer Networks

September 17, 2009

Networking Basics

- In order to understand threats, you need to understand networks. However, these networks are very complex.
- Networking systems are implemented as a series of layers which build on each other.

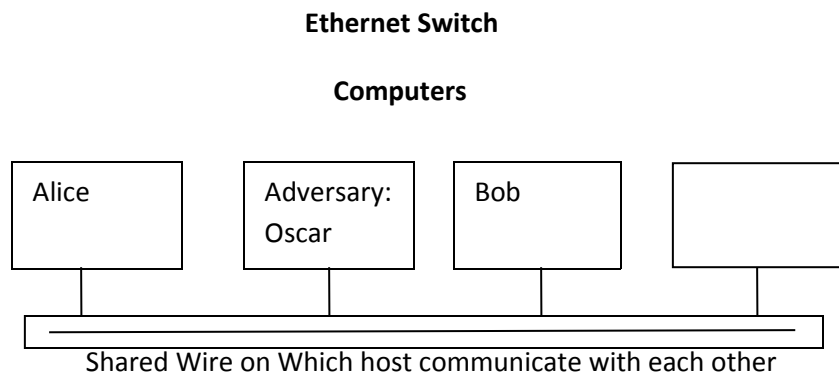
The Lowest level → Physical Level- Physical wires (wires meant in the most abstract sense) that connect one computer to another.

The 2nd level → Data Link Level- governs how information is sent over the wire (Information are bits (1's and 0's))

- *The most popular implementation of networking is Ethernet.*
 - In order for computers to connect to this you need an adaptor which is nowadays is mostly built into computers
 - Switches are used to connect multiple computers to a hub hooked up to a shared wire. This wire enables hosts to communicate with each other.
 - Hosts on a shared wire are a lot like the party lines used when telephones were first introduced. Multiple houses would be connected to a shared telephone wire, each given a distinctive ring so households would know who it's for.
- *Problems can arise from shared Ethernet wires.*
- The first problem is: How can we know whom the message is for?
 - Each Ethernet card has a unique address → a MAC Address
 - MAC = Media Access Control
 - The MAC Address consists of a 48 bit number, represented as 12 digits. The letters are from A-F and the numbers from 1-9.
 - Example: 00 80 C8 DF 26 E3

- When sending out a message, both the source and destination, and the MAC address must be included.
- Frame: Ethernet Message Format

Preamble	Destination MAC	Type	Message Body (Payload)	CRC
-----------------	------------------------	-------------	-------------------------------	------------



Scenario:

- Suppose we have 2 hosts: Alice and Bob
 - Alice wants to send a message to Bob; she sends an Ethernet message
 - In effect, Alice's Ethernet message card broadcasts a message across the network: "This is a message for Bob from Alice: let's meet at 4pm."
 - Bob's Ethernet card picks up the message and relays it to Bob
- Other Ethernet cards pick up the message as well, but ignore it. Why? Because the destination MAC address is different from their own.
- An Adversary is brought into the scenario: Oscar. He would like to read the message between Alice and Bob.
 - Oscar doesn't see the message because his Ethernet card ignored it.

- However; it is possible for Oscar to still see the message because each Ethernet card has a “promiscuous mode.”
 - Promiscuous Mode reports all traffic on the network the user.
 - If Oscars Ethernet card is running in this mode, he can read Alice’s message to Bob.
 - This seems to be a Security Threat: Would it help if makers didn’t let card do this? No. All Oscar needs to do to see the message is print out all the 1’s and 0’s going through the wire.
 - This promiscuous mode also may be useful for administration users for legitimate use.
 - Preventing Oscar from seeing the message is very difficult. The best way to stop him from seeing it is using encryption (This will be covered at a later date).
- ***The 2nd problem that can arise from shared Ethernet cables is: What if there is noise on the line?***

Scenario:

- Ethernet wire passes by a microwave or a strong magnet.
- Some bits occasionally could be corrupted. This could be accidental or intentional.
- What if Oscar tries to corrupt bits?
- A bit anywhere in the message frame could be flipped causing:
 - Bob to get an incorrect message or it is undecipherable.
 - MAC Address could get corrupted.
 - If destination is corrupted it will be delivered to the wrong person: assuming the address it becomes is one someone has. Or most likely, the message will be dropped if no one’s MAC address matched the corrupted destination.
 - If the source is corrupted it will to appear to have come from someone else or from nowhere.

- This Problem needs to be addressed:
 - CRC- Cyclic Redundancy Check → adds a few bits typically to the end of the message. It will contain information that summarizes the entire message.
 - For example: One of the bits might tell you, “Does it contain an even or odd 1’s.”
 - If the message does not have the characteristics the CRC says it should have, then an error occurred in either the message or the CRC. In this case the message will have to be resent. This is an example of trying to prevent errors by building in a bit of redundancy.
 - Real World Examples:
 - Letter: Address and Postal Code
 - Credit Card Numbers: The last digit is derived from the remaining digits in a particular way. Basically, it summarizes the first sets of numbers. This is an Algorithm called the Luhn Algorithm. Web sites apply this in order to ensure the credit card number is correct.
- ***The Third Problem is: Will the entire internet's data flow through my Ethernet card?***
- No.
 - It would be so busy that you wouldn't be able to send messages in or out
 - The entire Internet would come to a halt
 - This problem concerns privacy and also scalability
 - Ethernets have limits → limited to 1024 hosts at the max. Any more than that and you will need to join together smaller networks... (to be continued, this is at a higher level in the network hierarchy)
 - Because of this limitation, you can't see the whole world's data passing through your computer- even in promiscuous mode. Similarly your data isn't seen by every computer on the internet.
- To understand threats from beyond our local network we will need to understand networking at a higher level.
- ...The rest of the Ethernet topic will be continued next class.

