For today's topic we want to introduce and discuss the key concepts behind computer networks and how computers communicate in cyberspace.

In a broad sense what is a network?
One of the many definitions of a network comes from Merriam Webster and states that a network is an interconnected or interrelated group or system. That is a very broad definition that can be applied to many different things. What separates a computer network from other kinds of networks? Computer networks are made up of general-purpose equipment and are not tuned for a special purpose. For our purposes now we can just say that a network is just a bunch of interconnected computers. The network provides the connectivity between the computers.

To understand what a network is we need to know what networks are composed of?
At this point ask the class to identify what they think are the components of a computer network.

Basically networks are made up of nodes and links.
Nodes are the devices that connect to the network (e.g. computers, laptops, cell phones, etc)
These are also called hosts and can be special purpose hardware like switches
Links are the physical medium that connects the computers
These can be coaxial cable, fiber optic, etc.

In a computer network many nodes are connected in some way (e.g. with wires)

As a side note you can mention to the class the there are several different levels in which connectivity can happen, meaning communication between nodes (also called node-to-node). These can occur at the simplest level of two computers connected together (point-to-point) all the way to switched networks connected through a cloud.

But as the class probably knows there are other mediums that we can use to communicate between nodes, we can have node-to-node communication through a wireless network.

Ask the class if they know how messages are passed across nodes in a wireless network?
Answer: using waves through the air
Without getting into details of network wave propagation you can provide an example to the class by writing a note on a piece of paper and tossing it to a "node" (i.e. student).

This is fine if there is a direct connection or path between the two entities that want to communicate but in today's world that is rarely the case. To transfer a message between two nodes, that message will have to traverse multiple hops. A hop is an intermediary that will pass the message along to its destination. In most cases a message passes through several of these hops on its way to its final destination.

Ask the class to tell you how each hop knows what next hop to send a message to?
Answer is by routing
Wikipedia has a good definition of general routing. It states that routing is the process of selecting paths in a network along which to send a message.

Routing is implemented inside a router. A router knows about multiple nodes. A node may only know of one router.

To get a message to its destination, you might need to go through a router. The router or set of routers will know both you and your destination.

Explain to the class that is like the post office.
When you mail a letter all you want is for the letter to get to its destination, you don't really care how it gets there as long as it does.
The post office will take your letter and send it through their centers, there could be several of these centers that your letter goes through and they could be spread across the country.
Eventually your message will be delivered to the destination.

Sending a message over a computer network is very similar to the post office example above.

When you send a package you know the address to send it to (e.g. 123 Anywhere St.), so how do we determine the address in cyberspace?

As a side note: Another mediums example of addressing that the students can think about is a telephone number. When they make a call to a specific person that person has a unique "address" which they call to get them.

At this point let the class tell you how to determine addresses in cyberspace.

More than likely they are going to say something like a URL (google.com)
If not lead them toward a URL like google.com

Names like google.com and foxnews.com are just aliases and not the actual address, but they are easy for us to remember. Internally these names are converted to IP addresses (e.g. 72.14.213.106).
The underlying protocols used to route messages in cyberspace use these IP addresses to get to the destination through routers.

To get from our easy to remember names to an IP address we use a service called DNS (Domain Name Service). When given a network name an application will ask its DNS server for the corresponding IP address so that the application can begin the routing process of getting a message to its destination. Similarly we look up some ones name in the phone book to get their address.

Like our mailing address, IP addresses are unique. They uniquely identify a node on the network.

There is another address that needs mentioning at this time, MAC address. A MAC (Media Access Control) address is used to uniquely identify the physical device that allows anode to connect to a network (e.g. network card, router)

At this point have the students look up their own MAC and IP addresses.

On Mac and Unix flavors

Open up an xterm window and type 'ifconfig'

On Windows

Open up a DOS prompt and type 'ipconfig /all'

Make sure everyone in the class can find both their MAC and IP addresses before moving on. They can also see this information by looking at their network properties interface.

To further illustrate the concept of hops between sources and destinations wither you run allow the students in concert with you run a trace route to a given address like google.com.

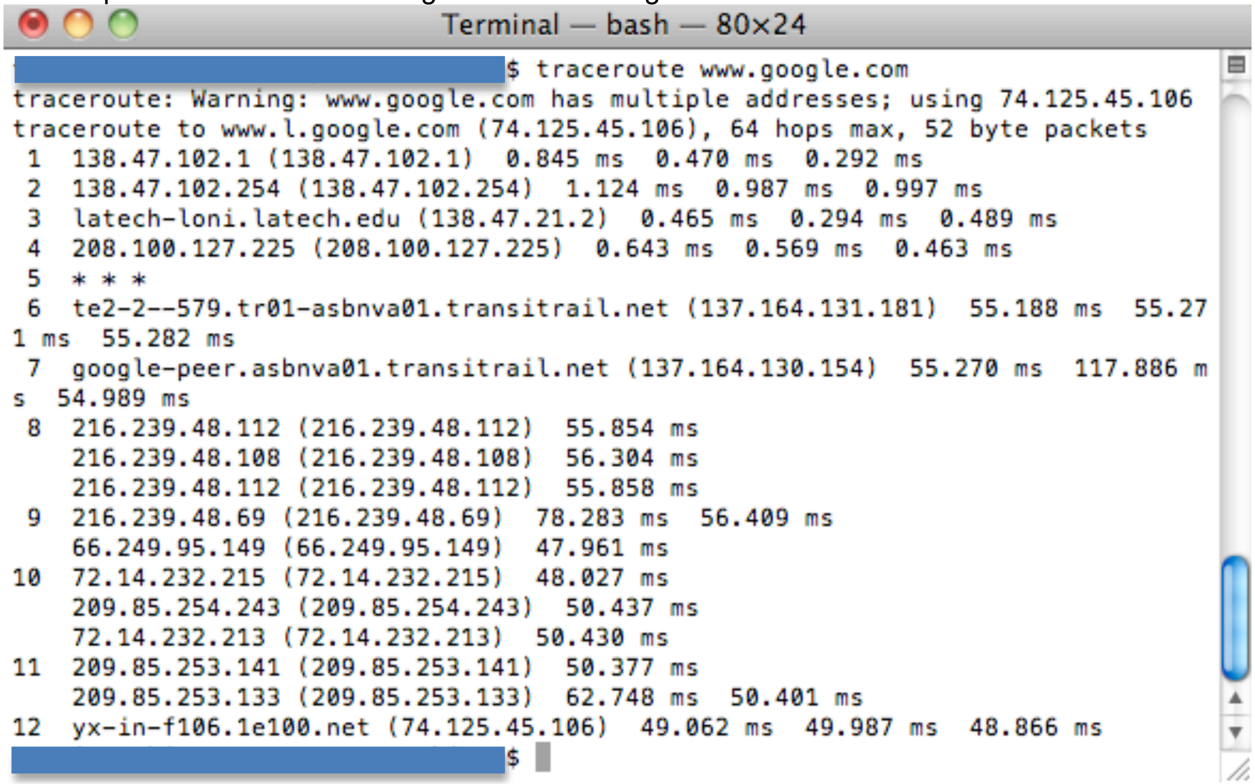
On Mac and Unix flavors

Open up an xterm window and type 'traceroute www.google.com'

On Windows

Open up a DOS prompt and type 'tracert www.google.com'

The response will look something like the following:



```
[redacted]$ traceroute www.google.com
traceroute: Warning: www.google.com has multiple addresses; using 74.125.45.106
traceroute to www.l.google.com (74.125.45.106), 64 hops max, 52 byte packets
 1  138.47.102.1 (138.47.102.1)  0.845 ms  0.470 ms  0.292 ms
 2  138.47.102.254 (138.47.102.254)  1.124 ms  0.987 ms  0.997 ms
 3  latech-loni.latech.edu (138.47.21.2)  0.465 ms  0.294 ms  0.489 ms
 4  208.100.127.225 (208.100.127.225)  0.643 ms  0.569 ms  0.463 ms
 5  * * *
 6  te2-2--579.tr01-asbnva01.transitrail.net (137.164.131.181)  55.188 ms  55.27
1 ms  55.282 ms
 7  google-peer.asbnva01.transitrail.net (137.164.130.154)  55.270 ms  117.886 m
s  54.989 ms
 8  216.239.48.112 (216.239.48.112)  55.854 ms
    216.239.48.108 (216.239.48.108)  56.304 ms
    216.239.48.112 (216.239.48.112)  55.858 ms
 9  216.239.48.69 (216.239.48.69)  78.283 ms  56.409 ms
    66.249.95.149 (66.249.95.149)  47.961 ms
10  72.14.232.215 (72.14.232.215)  48.027 ms
    209.85.254.243 (209.85.254.243)  50.437 ms
    72.14.232.213 (72.14.232.213)  50.430 ms
11  209.85.253.141 (209.85.253.141)  50.377 ms
    209.85.253.133 (209.85.253.133)  62.748 ms  50.401 ms
12  yx-in-f106.1e100.net (74.125.45.106)  49.062 ms  49.987 ms  48.866 ms
[redacted]$
```

We have discussed how a node is identified through its address, now let’s look at how a message actually is passed from the source to its destination

Messages are passed across a network in packages called packets. You may want to ask the class if they know what the packages are called before telling them.

If you have a long message you want to send to a friend, this message would be split up into smaller pieces called packets. Each packet contains a part of the message along with an ordering. This ordering allows for the message to be sent out of order and still be easily put back in order at the destination. This ordering along with other information like the source and destination addresses is included in what is called a packet header. The packet header contains all the information necessary for a intermediary hop to pass the message along toward its destination.

As an in class exercise let’s create a student network and pass a message.
To create this network the students will be our nodes and we can use ropes as our “connections”. Have the class stand up and you can randomly select a few to be our routers. Then pass out ropes to the “routers”; they will hold one end of the ropes and hand the other end to randomly selected classmates (these could and should also be other “routers”). This will create our “network”.

At this point develop a message and write it on multiple index cards, be sure to number the index cards to maintain ordering. These will be our packets. Also select a source and a destination that are not our “routers”. Have a source send the message to a destination by placing the packets on a keychain hook or carabineer hook and then on the rope. Slide the hooks down the rope to the next hop. At each hop or router that student will make a decision as to which rope to select to continue sending the packet along. Make sure that the packets go through multiple routers to get to the destination. The individual packets can also take different paths to the destination. Once all the packets have arrived at the destination, the receiver can reorder them and make sense of the message.

An extension of this would be to assign some students as DNS servers. So the sender would have to "ask" (send a message and wait for a response) the DNS server for the address of the destination before sending the packets to it.

To add something interesting to the mix at the end.
Have the students send another message as before. This time as the packets are traversing the ropes you reach in and intercept a packet and replace it with something else. This would be something called a man-in-the-middle attack. We will go in more detail about this later but it gives the students a very nice visual to remember.