Cyber Defense Organization

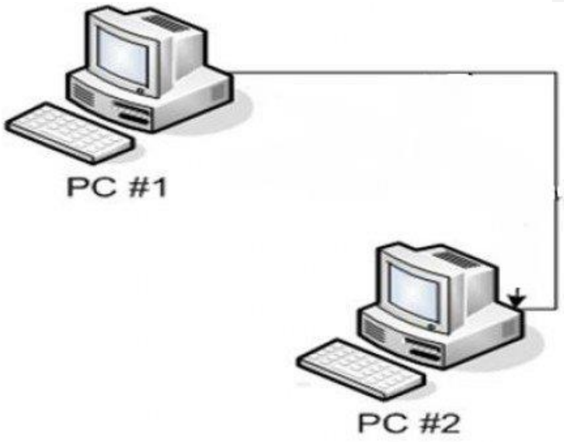
Networking Primer Worksheet - Alec Ridgway 4/14/19

What is a Network?

Before we begin learning all the fancy stuff about networks, we should define what it is first.

Well, simply put, a network is 2+ nodes that can communicate with each other. A node is a device on the network. This could be a computer, a printer, a phone, etc. You could do this with a simple wire connection if you have 2 devices.

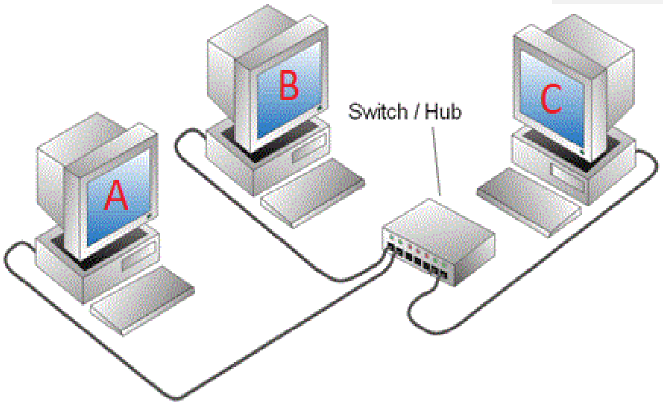
-->
This is technically a network
-->



But what can you do if you need more than 2 nodes? How can we get a line of communication to the 3rd node? This is where Switches, Hubs, and routers come in.

Router v Switch v Hub v

Switches, routers, and hubs all serve similar purposes but have different features that set them apart.



For example, a **switch** is an intermediary device that lets all information be shared across nodes in that network, based off of **MAC addresses "(Media Access Control)"**. A MAC address is a unique hardware identifier that identifies a node on their network.Ex. Node A wants to send info to node B. Within the switch, a MAC address table will be formed and it will check the info for the destination MAC

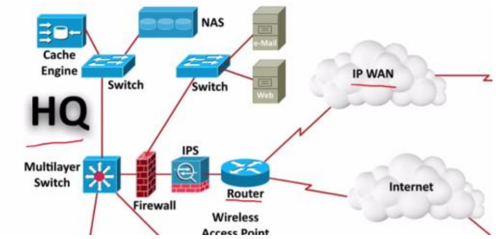
and send the info there.
A MAC address table is like an address book that the switch can refer to when deciding where the information will go.

Fun Fact: switches don’t count as nodes on a network, so they are invisible! (mostly)
Second fun fact: Switches can also use IP addresses as well as MAC addresses to deliver information.
<u>Hubs</u> are all but obsolete at this point, but it is still good to know what they are. They, like switches, are an intermediary device that lets all information be shared across all nodes in that network However unlike a switch, they do not pay attention to MAC addresses which means they send data to everyone regardless of who it was actually meant for. This is done through data replication.
Ex. Node A wants to send info to node B. With a hub, the data from node A will be received, replicated, and sent out to B and C.

Commented [1]: Info I was using for this:
https://helpdeskgeek.com/networking/router-vs-switch-vs-hub-vs-modem-vs-gateway/
Will work on more tomorrow

-Alec

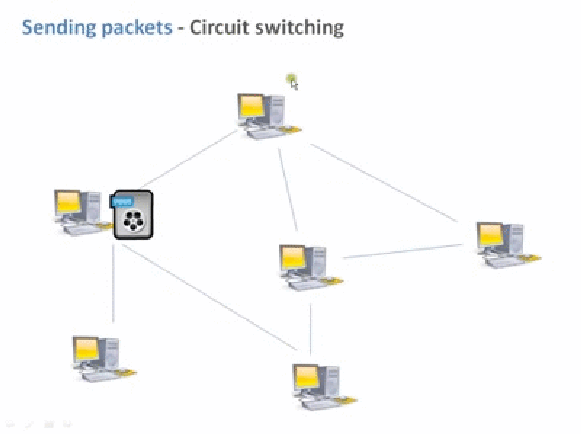
<u>Routers</u> are what most of you will be familiar with. They help connect the network together, like a switch. The Router acts like a more advanced switch, using IP address vs MAC. This allows it to communicate with devices outside of the network and route them to the correct destination.



Packets/ Encapsulation/ IP protocols

Encap and osi here

The Info that I was talking about earlier are called **<u>Packets</u>**. Packets are parts of data sent over the internet. For example, if you have an image of family and you want to send it to your grandma across the country. When you hit send on that email, the image is taken apart into small pieces to be sent easier over the internet. The packets then are reassembled in the correct order once they arrive at your grandma’s computer.



Sending packets over the internet is done in many different ways, these are called internet protocols, such as TCP/IP, UDP, FTP. There are many more and we will get into them later but for now, we need to know that there are different ways to send packets over the internet. If we want to swap from one protocol to another, we would need to **encapsulate** the packet. This is done to let the packets continue across the network.

Hey, guess what… it's later so that means we'll talk about the different **internet protocols.** There are a lot of them but let's focus on what a protocol is and a few important ones. A protocol is a set of rules and standards that basically define a language that devices can use to communicate. Some of the more important ones are..

Media Access Control (MAC) - Media access control is a communications protocol that is used to distinguish specific devices. This is given to the device when it is created, and makes it unique from all other devices out there. You'll most likely hear this when people are talking about MAC addresses.

Commented [2]: MAC is not really a protocol as much as it is a unique identifier hard coded into the hardware.

Internet Protocol (IP) - IP addresses are uniquely given to devices on Networks. There is a lot to unpack with this one, so we'll talk about it in its own section.

Internet Control Message Protocol (ICMP) - ICMP packets are transmitted when a packet of a different kind meets some kind of a problem. Basically, they are used as a feedback mechanism for network communications.

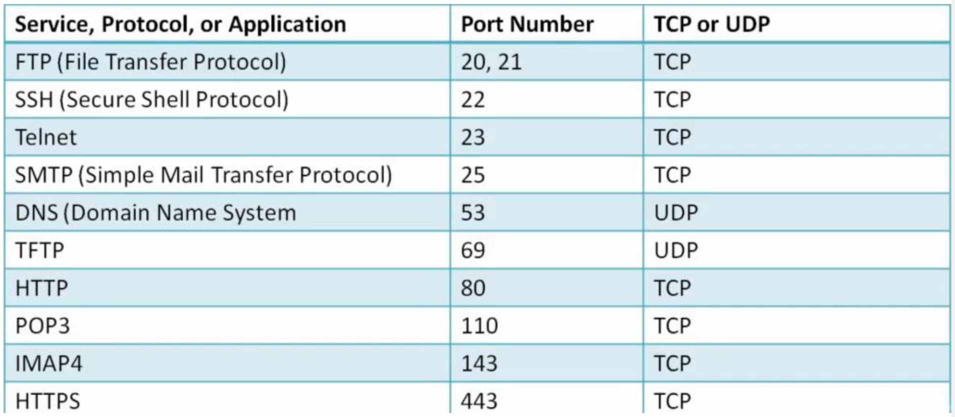
These are some important ones, tho there are more. I can't give a description of each just to save space, but I would definitely check out the ones listed here.

What is a port?

So there are 2 major distinctions between ports. Hardware ports and Software ports. Software is where the meat of this all is, but to quickly mention. Hardware ports are physical access points, like where you plug stuff into. This is important terminology that people will throw around so it's good to know.

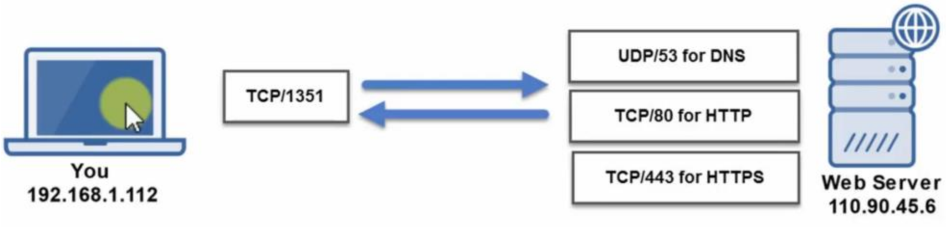
Software ports are the important stuff to know. These ports allow your computer to multitask. If you have multiple things going, such as email, FTP, and an internet browser, and they all want to communicate with your IP address rather than have them all wait in line they each have their own channel of communication. These ports also help the computer determine what type of packet it is receiving, because each of the TCP/IP networking services have their own port. This also helps out the firewall because they filter traffic by ports.

All of the well known ports, which are networking services with their own designated port, all have ports less than 1024



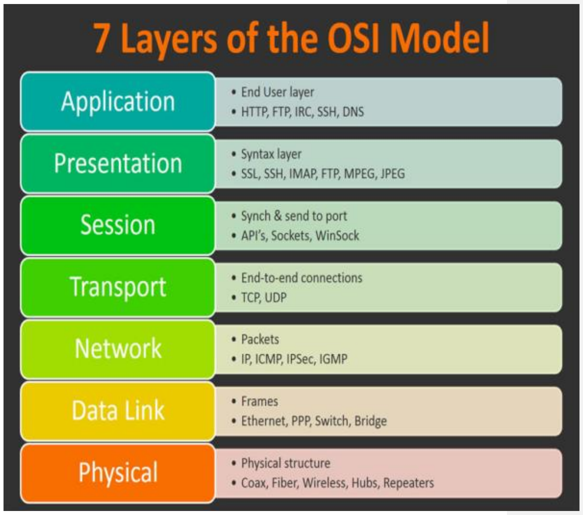
Service, Protocol, or Application	Port Number	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System	53	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP4	143	TCP
HTTPS	443	TCP

The way that your computer uses these ports is that you initialize your communication with a random high number port. As you can see below, the home computer is listening in on port 1351 and the web server is listening in on port 53, 60, and 443. When you send out a DNS request, the web server gets your request on port 53, then sends it back when completed to your IP address on port 1351.



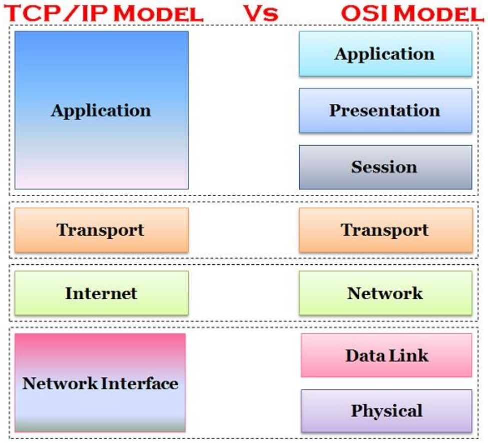
Networking Models

There are two kinds of models people have for networks, the OSI model and the TCP/IP model. We'll talk about the OSI model first, then the TCP/IP since there is some overlap there.



OSI breaks networks down into 7 layers, as seen on the right. Each layer is responsible for different types of traffic and items. There is some overlap between layers, though not much. Things to note about OSI is that the last few layers, session - application, tend to get grouped together into one layer. A lot of the time applications end up doing the jobs listed in layers 5 and 6, and this is becoming more common practice as things are being developed. As a result, the OSI is more of a theoretical model that is still important to know. People use this model to communicate. For example, a layer three issue is most likely an issue with a router. There are also such a thing as a layer 2 (MAC address) and layer 3 (IP address) switch.

The **TCP/IP** model is a more practical model. It breaks things up into 4 categories vs 7. This, along with the fact that you read the TCP/IP model top down instead of bottom up (like with OSI) means that the model ends up being more tangible. The OSI model is also referred to when making network architecture where TCP/IP is for client-server communications.



https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html use this link for more info.

IP/Subnetting

IP addresses and subnets are critical in forming the network. They allow nodes on the network to communicate to a specific node. The best way to imagine IP/Subnet is like house numbers and towns. The IP addresses are the house numbers and the subnet is what town they are in.

In more technical speak **IP Addresses** are a temporary address that is given to a node on a network. This allows data to be packaged and addressed which means that the data is able to communicate to the desired computer. IP addresses are 4 bytes which will be important for discussing subnet masks.

Subnets are ways to segment your network. These are a prefixed range of numbers that can be allowed for those IP addresses. For example, if we have the first 3 bytes dedicated to the subnet and the 4th one to the network, the subnet mask would look like this.
255.255.255.0

Whenever a number is a 0, that means it belongs to the host, so that is what actually differentiates the computers in that network segment.

Example ip addresses.
192.168.30.5 with a subnet of 255.255.255.0

This means that the first 3 sections are dedicated to the subnet and the last is for the host.
So 192.168.30.5 might be Bob’s computer in accounting and 192.168.30.6 would be Karen’s. If you wanted to look at HR there IP might look like 192.168.40.x.

IPV4 vs IPV6 and ABC Classes

So IPV4 and IPV6 accomplish the same tasks, with the most notable difference being that IPV6 has more possible addresses. To understand why it is significant that IPV6 has more possibilities we'll need a quick history lesson.

Back when IP addresses were initially being handed out, there were only a select few places that could have them, mostly colleges and research institutes. Each organization that wanted IP addresses were put into classes, class A received the widest range of IP addresses, where class C received the least. 16 million hosts on each of 127 networks and 254 hosts on 2 million networks, respectively.

Commented [3]: Do we want to talk about private vs public IP

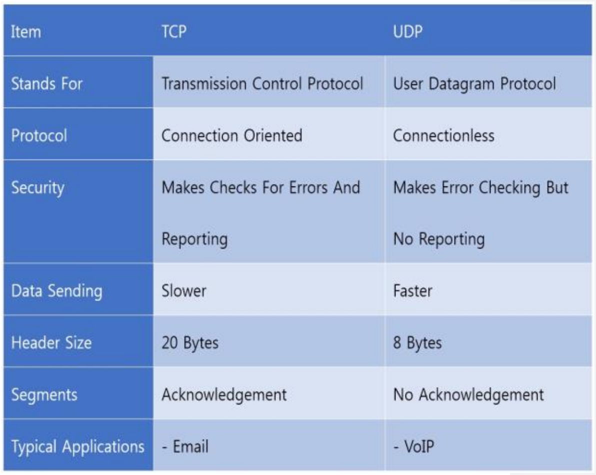
Commented [4]: I think we probably should, since this is just going to be a glossary of info

When the classes were first implemented, no one predicted the explosive growth of the internet. So today there is a shortage of IPV4 addresses. IPV6 was made to solve this issue, and has been slowly replacing IPV4.

TCP v UDP (Connection Oriented v connectionless)

TCP (Transmission control protocol) and UDP(User datagram protocol) are another two important protocols in the IP suite. They both deal with packet sending, they just do it in different ways

In essence, **TCP** communicates with the server and establishes a reliable connection. It prioritizes accuracy over speed. It does this by sending SYN packets to the server to start sending information. After the other computer sends a SYN packet followed by an ACK packet, your computer sends data TCP numbers the packets so they are displayed in order If a packet is not received your computer will get a notification and send the packet again. This is called the three way handshake.

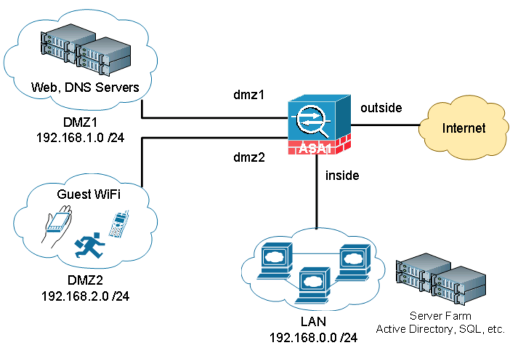


Item	TCP	UDP
Stands For	Transmission Control Protocol	User Datagram Protocol
Protocol	Connection Oriented	Connectionless
Security	Makes Checks For Errors And Reporting	Makes Error Checking But No Reporting
Data Sending	Slower	Faster
Header Size	20 Bytes	8 Bytes
Segments	Acknowledgement	No Acknowledgement
Typical Applications	- Email	- VoIP

UDP is more of a raw stream of data. A UDP request is much faster but also slopper than TCP. if a packet gets dropped with a UDP request you can't request for it to be sent again, like with TCP. Because of how sloppy UDP is, it is used in scenarios where reliability isn't as necessary as speed. So if you send an image over the internet, some of the pixels will be lost but the human eye isn't going to notice a couple, even 100 pixels missing from the picture.

As you can see in the chart and based on what you’ve read above, UDP is connectionless, which means you can just send info out to the receiver. Even if the receiver isn’t taking data at this time. TCP establishes a connection with a handshake. It sends out its request packets to see if it can receive data and if the answer is yes then the data will be transmitted.

LAN v WAN v DMZ



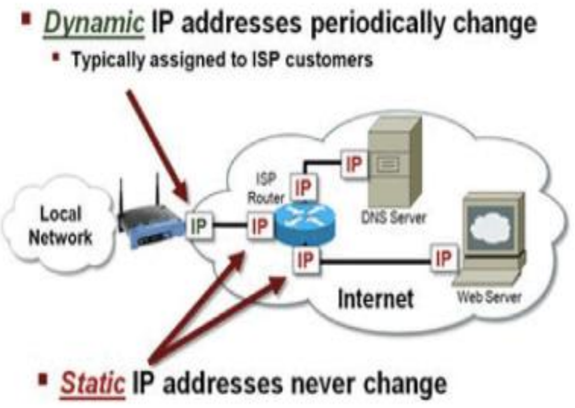
LAN (Local area network), WAN (Wide area network) and DMZ(demilitarized zone) are all terms used when describing network topologies. The topology is a way of visualizing the network and everything on it.

The **LAN** is the network of machines that are all locally connected, in one area. Think of a LAN as your house.This is done through ethernet cables and switches/routers. This is a very basic concept but core to all competitions and businesses.

WANs are networks connected across multiple locations, geographically. So if you had a remote office you were linked to, then that would be considered a WAN. These are usually connected through VPNs over the internet. This establishes a secure and private connection over the internet. The internet as a whole could also be considered a WAN.

The **DMZ** is a portion of the network that is cut off from the rest of it. This is between a WAN and LAN. This is what the internet and the general public will be interacting with. This is like a buffer zone to help keep the LAN secure.

Static vs Dynamic IP addresses

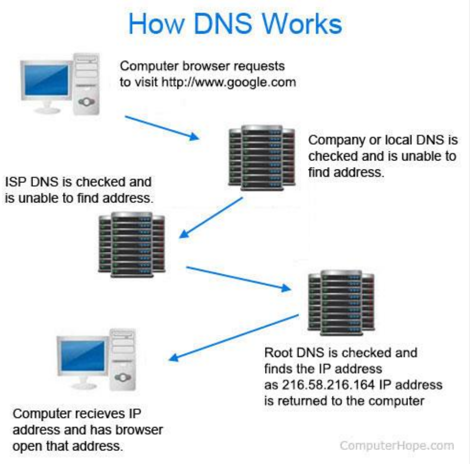

Dynamic IP addresses periodically change
Typically assigned to ISP customers
Local Network
IP
ISP Router
IP
IP
IP
DNS Server
IP
IP
Internet
Web Server
Static IP addresses never change

Static and Dynamic IP addresses are the two ways to break up IP addresses. Each has their own uses and benefits/cons.

Static IP addresses are usually assigned to LAN devices. These devices will never change their IP address unless you do it. They are also used for websites, so that you can always always go there. The mapping of website names like Google, to their IP address 8.8.8.8 is done through a DNS (Domain name server) server.

Dynamic IP addresses are temporary IP addresses that change and are being constantly assigned and reassigned. Let's look at an example to explain this best. You walk into a restaurant and want to connect to their Wifi. When you enter the password to get the Wifi, you have just joined that network. So that devices on that network can talk to you, and so that you can talk out to the internet, you are given a temporary IP address. This is done through a DHCP (dynamic host configuration protocol) server.

DNS (Domain name server)


How DNS Works
Computer browser requests to visit http://www.google.com
Company or local DNS is checked and is unable to find address.
ISP DNS is checked and is unable to find address.
Root DNS is checked and finds the IP address as 216.58.216.164 IP address is returned to the computer
Computer recieves IP address and has browser open that address.
ComputerHope.com

DNS servers are vital to how we use the internet today. Without them we would need to memorize all of the IP addresses of the websites that we wanted to visit. DNS maps IP addresses to names that we can easily remember. Google has two public DNS servers, 8.8.8.8 and 8.8.4.4 their primary and secondary respectively. DNS servers are usually set up with primary and secondary servers, in case the first one fails or is unable to find your request.

DNS servers are often subject to attack due to their importance. rDNS lookup or reverse DNS resolution is a common attack. rDNS is a legitimate method used by DNS servers to confirm what the domain name attached to an IP address it. However, this can be used to trick a DNS server into sending you to the wrong place. They could make it so when you type google.com into the search bar, it doesn’t bring you to 8.8.8.8 but instead a spoofed version of google.com. This could be used to gain access to your login credentials or to steal your ID, depending on what site is being spoofed.

DHCP (dynamic host configuration protocol)

DHCP is responsible for dynamically assigning IP addresses to devices on the network. DHCP is needed in today’s world in order to manage a network. It automates what is a relatively simple, but lengthy process by handing out IP addresses, subnet masks, default gateways, and a DNS server. If you had to assign this all by hand, everytime a device enters or leaves your network, you would lose your mind trying to keep everything unique and the same.

The scope of the DHCP service defines the range of IP addresses it can give out. This is done by setting a starting and ending IP address, which can be adjusted to whatever the network needs. When an IP address is given out, it is done so on a lease. This is to prevent any addresses being held up by computers that leave the network.

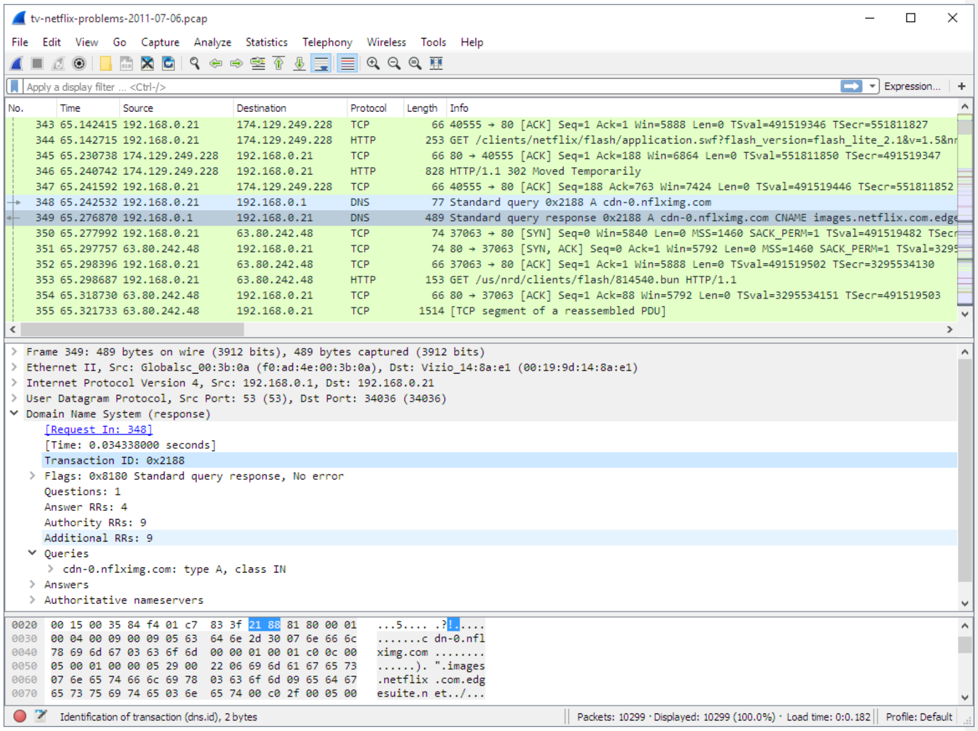
If you need to set up a static IP address, you can create a reservation list within the DHCP server. This is usually done on servers.

ARP (address resolution protocol)

The ARP maps IP and MAC addresses together. This is used in LAN networks so that the two devices can communicate. The IP address just directs devices to each other on networks and the MAC is the identifying number. The information of IP/ MAC address combo is stored in the ARP cache. Within this, you can see a list of the IP addresses, physical addresses, and the type. The type is either dynamic of static, which functions identically to the static/dynamic IP addresses mentioned above.

Wireshark

Wireshark is a tool that you can use to look at network traffic. It analyzes packets and displays all the information in them in a human readable form.



```
No.  Time      Source          Destination     Protocol Length Info
 343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
 344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
 345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
 346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
 347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
 348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
 349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
 350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
 351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
 352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
 353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
 354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
 355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes || Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 || Profile: Default

This is what a standard Wireshark capture looks like. All Wireshark does is display the information, and it will not act upon it, that is up to the user.

Here is the download link: https://www.wireshark.org/

Cisco Packet tracer

Steps to download

1. Go here https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer
2. Sign up
3. Go to email and verify account (fakenamegernerator.com)
4. Click download link
    a. Most likely the 64 bit for windows
5. Open the zip file you just downloaded
6. Run installation executable
7. Log into the app
8. Click allow for the firewall stuff

What does Cisco Packet tracer do?

It allows you to emulate a network topology, aka build a network virtually so you don’t need to buy all the hardware.

To make a simple network, click the routers icon in bottom left (should be checked by default) and click the 1841 router, then click to place it on screen.

The numbers denote different routers, each is a different make/ model with different perks to each.

Next choose end devices, from where routers was before, and place down two PCs.

After placing down the PCs, go to connections in the same area. Select the copper copper cross-over and click on a PC. Once done, click on the fast ethernet for that PC and connect it to there, then do the same with the router (if its PC 0, then Ethernet 0 on the router).

Once this is done for both PC 0 and PC 1, congrats you've just set up a physical network. But now we need to configure it. Go to the router and click on it and head over to the CLI tab (command line interface).

If they accidentally press ctrl +c it will exit easy set up mode, they then need to delete router and make a new one, as well as redoing all the connections.

Ok so at this point, I need to check with Liam to see how we want to do this. Because you have the option here of entering a command line where you can set up and configure the router or a nice walk through.
Try using the GUI instead of the command line
https://www.youtube.com/watch?v=VqMeJ-WH4E0&t=8s

You select networking devices in the bottom left hand corner

Introduce packet tracer, then the stuff below

Add switch, add 2 computers, set IP addresses on computers to 10.0.0.1/.2, default subnet mask, go into sim mode, open up a PC, then do ping on the other IP address, and boom, you have your demonstration.

Maybe explain what the ping command is

Explain what an IP is, default gateway, subnet, DNS/ DHCP

Introduce packet tracer, then the stuff below