LAN computers connect with Ethernet.

Ethernet is a protocol that defines our frames, speed, how to network cards work, what kind of cabling and connectors we use, what kind of these little hubs we use. Ethernet allows 100 meter runs.

Ethernet says “You can only make your data in discrete chunks of 1500 bytes.”.

You have to broken up your data into zillions of 1500 bytes chunks called a frame. OS is smart, they take the document that you send and takes it apart. Then they puts it back together on the other end.

We uniquely identify every system on the local area network through something called a media access control or MAC address (Physical address / Ethernet address). MAC address is a 48 bit address which is always manifested as 12 hexadecimal characters.

Every network card gets a unique MAC address.

The first 6 characters are OEM ID. So if I'm going to start making network cards I am issued those first six characters from the issuing body of the Internet and then I could spin up all the other ones as much as I want.

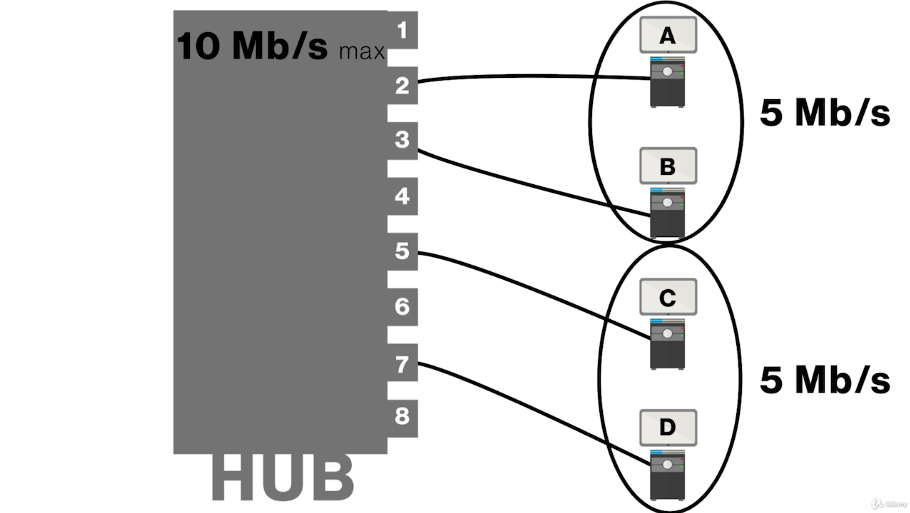
We send in order destination MAC, source MAC, data payload, and FCS (Frame Check Sequence). These four is the Ethernet frame.

FCS is nothing more than a checker so that when data gets over to its destination they can compare FCS value to the data and it gives them a pretty good idea as to whether the data came in good order.

WE ARE TALKING ABOUT LAN (LOCAL AREA NETWORK).

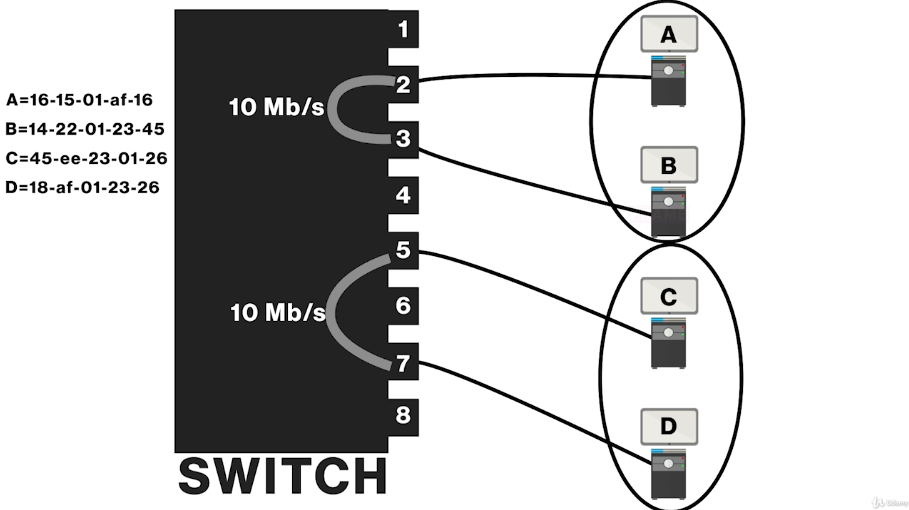
HUB repeats the incoming signal and sends that signal back out to every computer except the sender. Only receiver keeps the coming frame. Other computers will read the MAC address and since they know their MAC address and they look at the destination MAC, they just erase it because it's not for them.

Downside of HUB



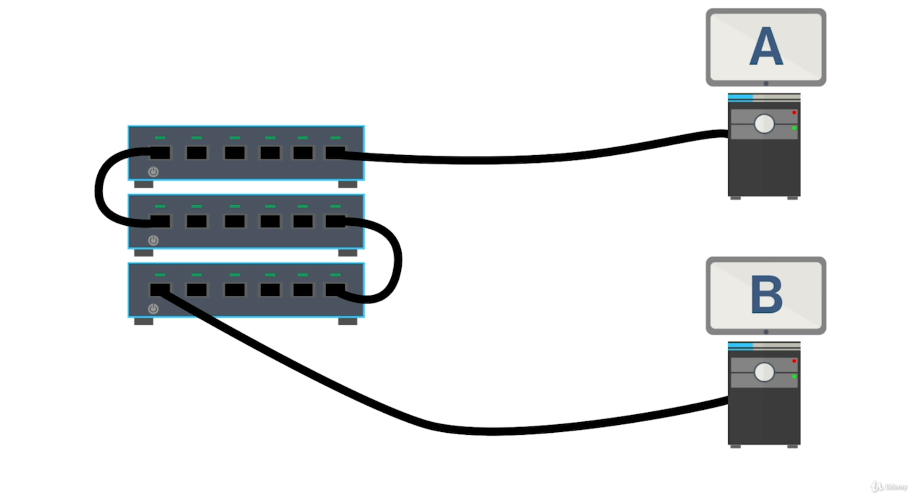
SWITCH collects the MAC addresses and sends the coming data only to intended computer. SWITCH makes a direct physical connection to the intended port. SWITCH provides full bandwidth for all nodes.

Switches watch all inbound frames and learn MAC addresses from them.



Each hexadecimal character represents 4 binary values.

Ethernet standard says you never put more than 1024 computers on a single SWITCH or a bunch of daisy chained SWITCHes.



Left one is daisy chained SWITCHes. They act like 1 single switch.

If you add more computers up to 1024, system becomes overloaded.

Ethernet is not gonna handle too many (millions of) computers.

The concept of a LAN works fantastic for according to Ethernet standards up to 1024 (But in reality 30 to 40 computers is pretty much the standard maximum size for a local area network.).

If we use the term IP address, we need to start making our networks bigger through something called a wide area network (WAN). We interconnect LANs together through WAN.

Routers can differentiate not between just individual computers, but different LANs.

MAC address allows us to get information to different computers within a LAN but we need a different numbering system. Something else that allows us to identify LANs. And that's where we get into what we call logical addressing.

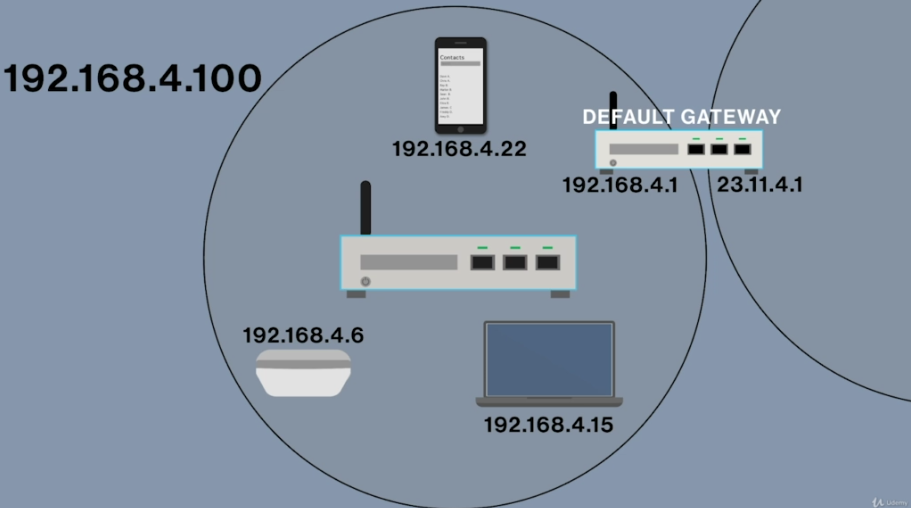
The type of logical addressing we use is IP addressing.

Every device inside your LAN, whether it's wired or wireless, gets a unique address.

If 2 computer want to talk each other at same LAN, they just use their MAC addresses.

If 2 computer want to talk to anybody that doesn't have an address it starts with 192.168.4 (for this example), they have to send it out to this router.

Other side of the gateway router, there is a totally different IP address, because this is a complete different LAN. So there is another LAN at the other side of our router.



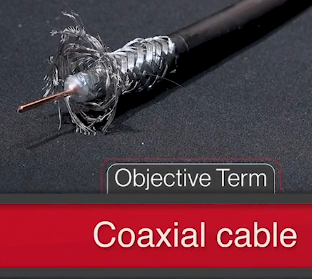
There is a special kind of server that built into the router called DHCP. This automatically gives the IP information that you need.

We pretend the middle white box as a SWITCH.

DOCSIS (used for cable modems) is alternative for Ethernet.

There are lots of different versions of ethernet. They have names like 10BaseT (10 Mbps - Baseband - Twisted pair).

As these different Ethernet standards come along, they need improvements in cabling in order to make sure that they run at their speed that they're capable of.

We use RG ratings at this type of cable.

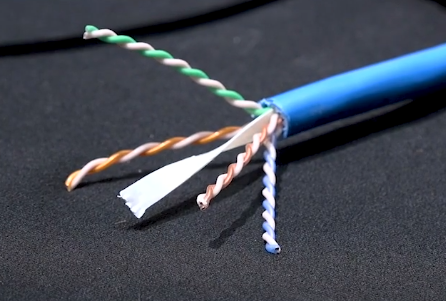
RG-58 : very old

RG-59

RG-6

We use F-type connectors with RG-6. We use BNC connectors with RG-58.

TWISTED PAIR CABLING

There is no metallic foil in this one so we call this Unshielded Twisted Pair (UTP).

We have 4 twisted pairs in this one.

The reason we put twists in there is that it helps propagate the signal better. If they weren't twisted together the distances we could run individual cables would be much shorter.

In general, this cables run about 100 meters.

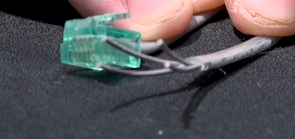
We use CAT (category) ratings for this type of cable. !!!

CAT 5 : 100 Mbps , CAT 5e : 1 Gbps

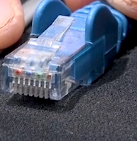
CAT 6 : 1 Gbps (up to 100m) - 10 Gbps (up to 55m) , CAT 6e : 10 Gbps (at 100m segments)

Solid core : Each one of 8 wires is a solid piece of copper. It is not used in environments where frequent bending occurs.

Stranded : Each one of 8 wires is actually stranded. It’s flexible. Because we have stranded in there, we won't break it.

This is telephone cable (UTP) and only has 2 pairs.

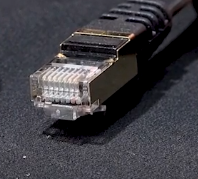
Its connector is RJ-11. It has 4 contacs.



This is RJ-45. It has 8 contacts.

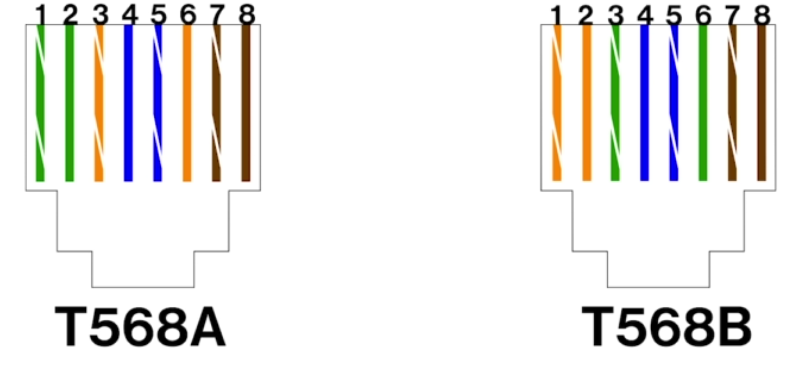
That’s gonna make sense if we have 4 pair twisted pair that’s 8 different wires in there, and this can handle all 8 of those.

The transparent thing at the end is crimp. They also have a CAT rating. You have to match crimp’s and cable’s CAT ratings.



This is Shielded Twisted Pair (STP). It’s still an RJ-45.

All this metallic stuff is shielding and it doesn't just come here on the ends, it runs all the way through the cable and it provides a lot of robust protection.

These 2 different standards for crimps. Each has different order for paired cables.

FIBER OPTIC (FIBER) CABLE

Fiber optic cables don’t use electricity, they use light.

It’s extremely popular when you're talking about like 10 gigabit Ethernet situations or even faster.

There’s 2 different kinds of ways to propagate a light signal.

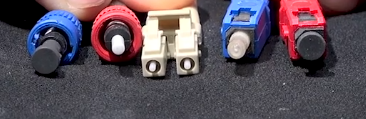
Kind of hair stuff is Kevlar.

Orange is just a protective cover.

White stuff at the right is cladding which actually reflects. There is a tiny (the size of human hair) piece of fiberglass in there that actually propagates a light signal.

This is Multimode kind (uses LED to propagate the signal).

There is another way called Singlemode kind (uses lasers to actually propagate over many many kilometers of distance).



These are connectors and they’re all in pairs because when you're working with fiber optic one single wire generally only sends or receives. So usually when you have a fiber optic connection you plug two of those in one for send and one for receive.

Plenum Ratings : Different types of ratings which are based on plastic cables ability to resist fire.

1. PVC (non-plenum) : Most burnable. Very cheap. You shouldn’t hide it into a plenum (area between a drop ceiling and the actual ceiling that little space where cables go).
2. Riser : Designed for when you’re running cables between floor (vertical). Better than PVC, worse than Plenum.
3. Plenum : Much more resisting to fire.

Straigh-through cabling : Wired the same on each side.

Crossover cabling : T568A on one side T568B on other side. These cable type is actually kind of handy. One of the things you could do with them is you can actually plug two computers directly together, no switch, etc. and they will actually be able to talk to each other most of the time it depends on the network card.

Structered cabling : We want cables in the walls in an organized way that the cables are safe and then we can connect when we need to. This is known as structured cabling.

Main Distribution Fram (MDF) - Intermediate Distribution Frame (IDF) : Structered cabling begins usually in a closet or some kind of room that we will often call the MDF or IDF. It's the closet where the equipment is.

Horizontal runs from wall outlet to patch panel through walls/ceilings.

IP ADDRESS

Every number is an octet and they go from 0 to 255.

4 Billion addresses can be made by IP address.

IP address do 2 things:

1. Identify which LAN you are a part of
2. Give you a unique host ID

The whole idea between taking these numbers and breaking them into four groups with three dots is that we would have Tier 1 of the Internet.

Any address with starting with 1 is experimental, reserved and nobody could use them.

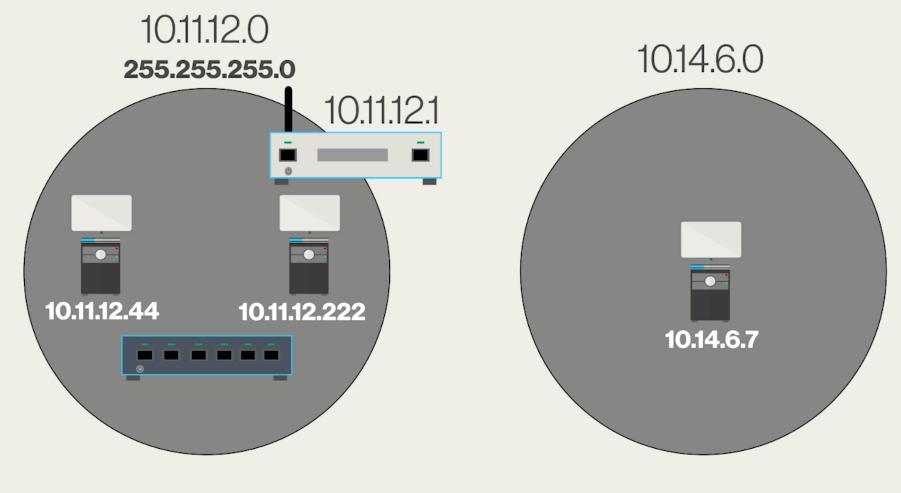
No address can end with 0 or 255.

For example you write 10.11.12.0 ---> This means we are not talking about a computer, we are talking about a network ID. So that’s one of the reasons we can't put a zero on the end of an IP address because it identifies an entire LAN.

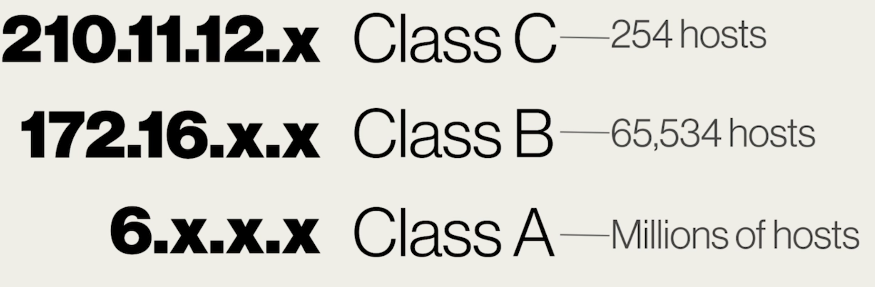
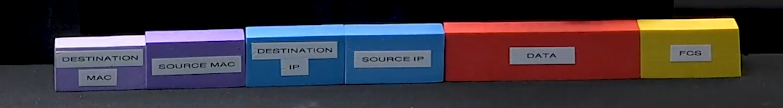
Every OS has a place for us to enter IP address.

If you want a computer to be at the internet, you have to give it 3 things:

1. IP address
2. Subnet mask : only there to let your computer know if it’s a local call or a long distance call. If it is a long distance call, it sends it to the default gateway.
3. Default gateway



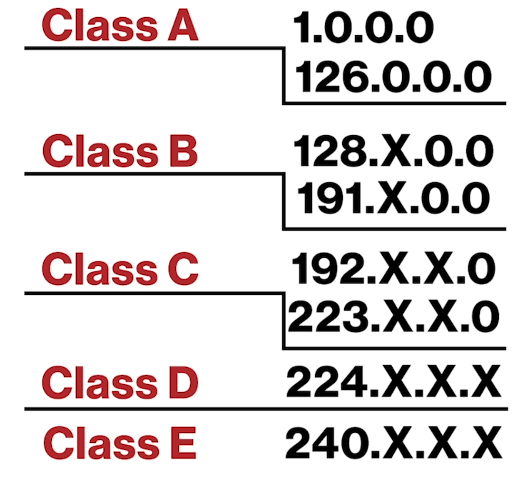
Manuel settings = Static IP address



Class C (majority of subnet masks) -> first 3 is locked Class B -> first 2 is locked Class A -> first one is locked

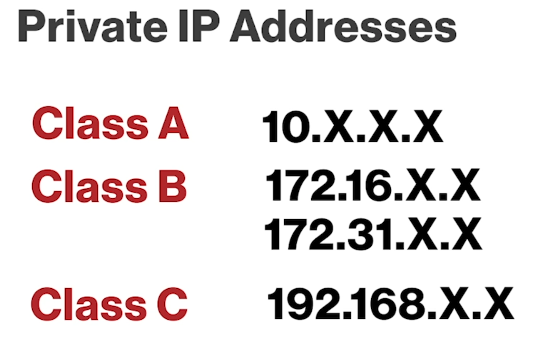
For example your subnet mask is 255.255.255.0 ---> This means that wherever you see 255, numbers have to be the same if you want to send your data to a computer which is in your LAN.

255.255.255.0 ---> Class C. Which means that last 0 is going to be different among the computers in your LAN.

Class D ---> Multicast address. This is actually used in some fairly interesting presentation stuff like one person is doing a video presentation live, a bunch of other people who want to watch that video presentation are temporarily given like a second IP address that starts with 224 just for the duration of the video and then it’s all erased.

Class E ---> Reserved and nobody ever touches it and neither do we.

Private IP address : They're not really connected to the big Internet but they like the TCP/IP protocol and they're gonna go ahead and use it. You are not on the internet with these addresses but you have internet access through the router. There’s 3 sets of those:

You can put anything you want for Xs.

Class B is from 172.16.X.X to 172.31.X.X

If a router sees private IP address, it will simply erase the packet. So they’re kept within private networks only.

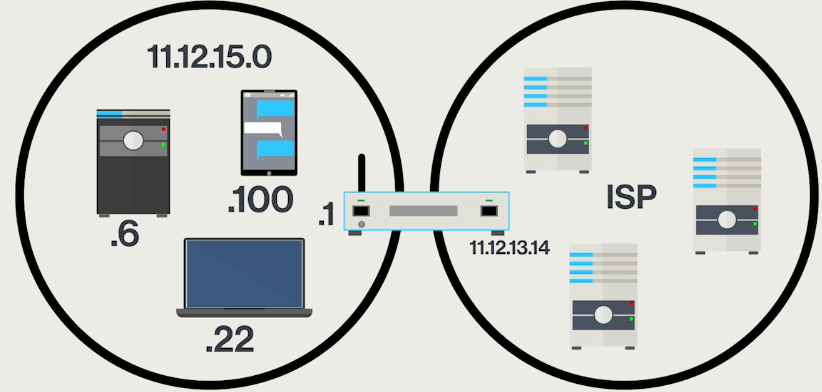
Loopback IP Address : 127.0.0.1 address. It simply refers to your own system. Handy way to test your network card up and running. You can control it with “ping 127.0.0.1” command.

You can control your router with “ping [Router’s IP]” command.

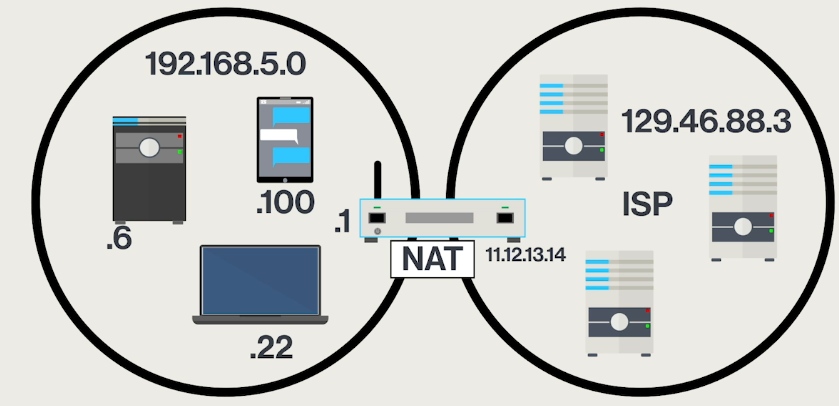
ping -t [Router’s IP] ---> sends more than 4 packets. Infinite number of packets.

NAT (Network Address Translation) : Translates a set of IP addresses to another set of IP addresses. It translates private to public and public to private.

We won’t need NAT or private IP addresses thanks to IPv6. Every device will have its own public IP.



The downside to this is that all of the computers inside your local area network have public, easy to find IP addresses. So we would put these things called firewalls onto our routers. However if somebody could get past the firewall, any computer on your LAN was visible to everythin else. Also this is waste of IP addresses.



For example 192.168.5.6 is trying to talk with 129.46.88.3 (any computer on the internet). Router takes 192.168.5.6 and remove it from the packet and insert its own WAN IP address which is 11.12.13.14 and when the packet comes back, this packet is gonna be addressed to 11.12.13.14 but router will remember that 192.168.5.6 was trying to talk to 129.49.88.3 because router documents all this and as the packet comes back he takes his public address off and puts the private address right back on.

Anything that's inside the LAN is invisible to the Internet. So you can't put web servers or things like that in there.

This slows things down a little bit.

Dynamic Host Configuration Protocol (DHCP) : Dynamic IP addressing. Something in the network will give you IP address, subnet mask, IP of default gateway. We call it DHCP server. Routers usually act as a DHCP server.

Sometimes DHCP servers go down. It doesn’t mean that if you don’t have an DHCP server, you don’t have an IP address. What we have on pretty much all OSs is called the Automatic Private IP Addressing or (APIPA). It is your fallback in case you can't find a DHCP server. You can also get IP addresses and subnet mask manually.

APIPA always give 169.254.X.X address by default (Class B).

You can share folders etc. in your LAN because you all have 169.254.X.X addresses but you can’t get on the internet because your router doesn't use a APIPA, it's got a fixed address on it.

ipconfig /renew ---> Your DHCP server is broke and you have an address given by APIPA. Then DHCP server begins to run again. You should use this command to use proper address for the internet again. This command force a new connection to the DHCP server.

ipconfig /release ---> Disconnect you from the DHCP server.

IPv6 addresses ---> 2001:0000:0000:0001:0000:0000:0000:8a2e

or you can write like this ---> 2001:0:0:1:0:0:0:8a2e There is no leading zeros.

or you can write like this ---> 2001:0:0:1::8a2e Double colon instead of 3 zeros.

IPv6 addresses use a 128 bit addressing scheme and uses a hecadecimal notation.

In the world of IPv4 you only had 1 IP address.

In the world of IPv6 you have minimum of 2 separate IP addresses:

1. Link local address : Always starts with fe80:0000:0000:0000 … last half is automatically generetad by your system itself. Link local address is automatically created when you boot up a computer that’s IPv6 capable. Used for local connections.
2. Global unicast address (Internet address) : Internet address is brought down from your actual router itself. The router will send out a broadcast that says the first half of your address is something and then your computer automatically generates the second half. Used to connect to the internet.

There is something similar to subnet mask at IPv6 called prefix. So the first half is always going to be right where your prefix is. The prefix is simply used to allow us to talk to upstream routers to get our data to the places we needed the very very quickest.

Your web browser is a web client. It's designed to be used by you to query servers to get information.

You have a communication between a web browser and a web server.

Everything on the Internet is a client and a server.

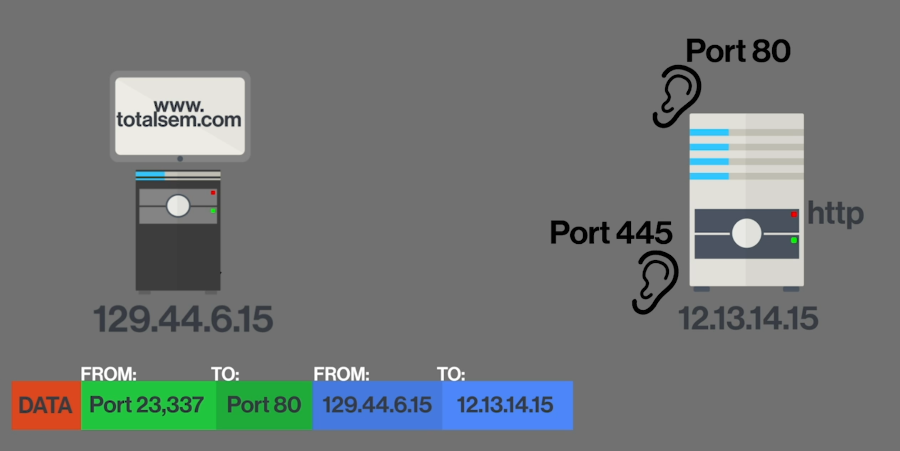
Domain Name System (DNS) : When you type [www.youtube.com](http://www.youtube.com) , it will go out amd get the right IP address.

You may have so many tabs open, you might be having a Skype call, you might be playing a game so your computer needs more than an IP address simply to keep track of this.

For example I can keep going back to same web server and I can have four tabs open and they all work. So we need to add something else to this and this is a port number.

A port number is what gets us to the right application. So the IP address gets you to the computer but the port number gets you to the right application.

Port numbers go from 0 to 65535. You always have source and a destination port number.

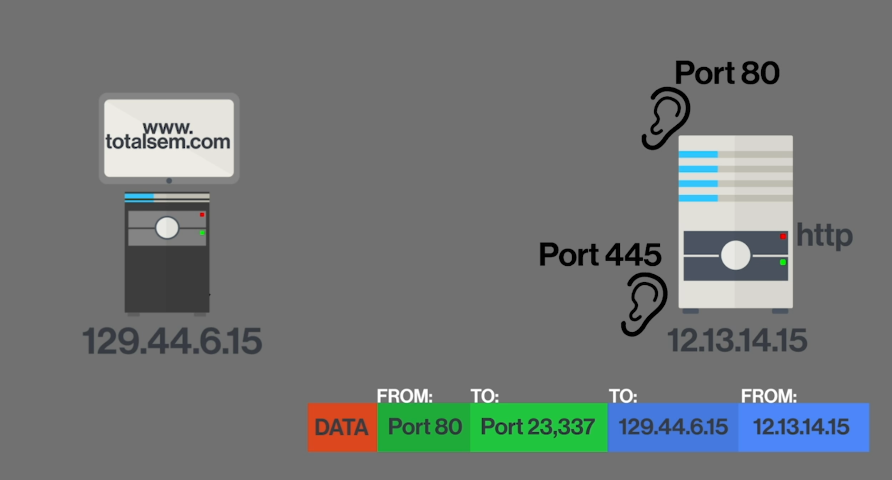


Data is request for a web page.

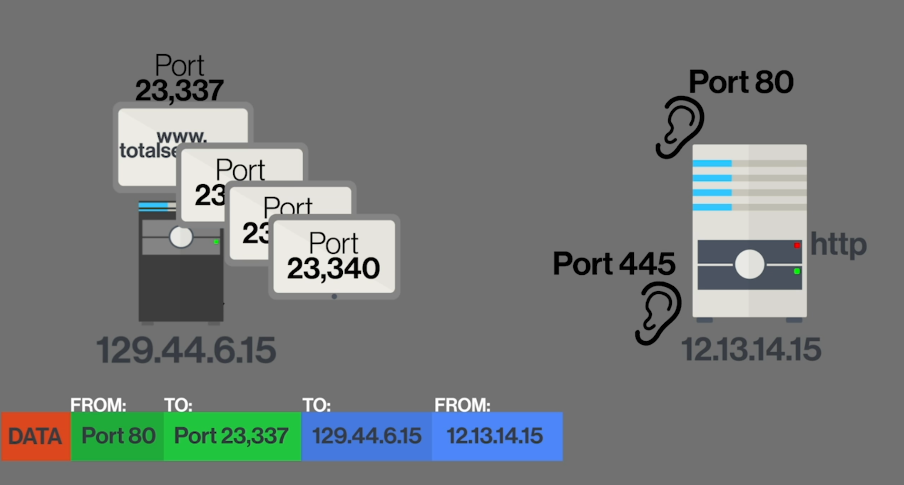
Right box has a web server (HTTP) that listening on port 80.

Same box could be for example Windows File Server and it would be listening on port 445.

So this box can handle both any incoming request for a web page as well as incoming requests to share folders.



Now the data is web page.



When this gets over to my computer I might have 4 or 5 windows open but each one of these windows gets its own port number and this is assigned automatically by the OS.

IP addresses get the data to the right computer but it's the port number that gets into the right application on that computer.

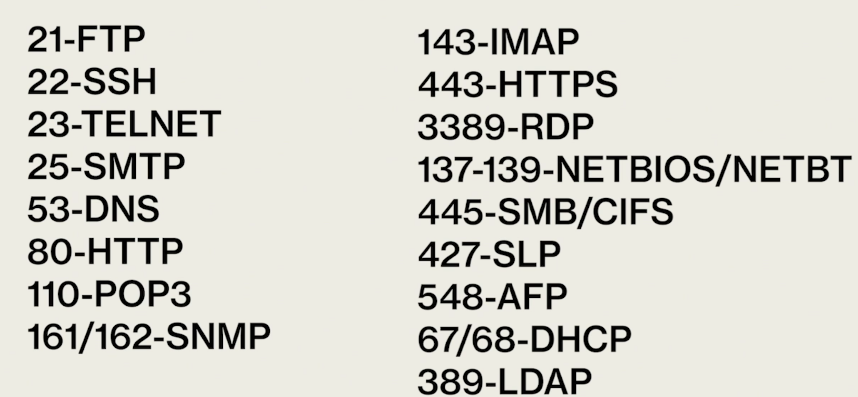
Now our ethernet frames are getting bigger. You also have MAC addresses and FCS.

When you connect to one web page, you don’t do one single connection. One web page might have ads on it, background stuff, it might be running javascript. All of these other thing create their own connection. So just because you open one web page that doesn't mean you're going to get a single connection.

All port numbers from 0 to 1023 are well known ports and these are applications like the web and secure web that are so well-known that nobody else can ever use these port numbers.

All port numbers from 1024 to 49151 are registered ports. For example steam games.

All port numbers from 49152 to 65535 are dynamic/ephemeral ports. Ephemeral port number is assigned by your system, every time it makes a connection to give a return port number for whatever server you might be connecting to.

!!!

A protocol is nothing more than a set of rules that allow different things to work together.

IP only gets addresses to individual devices. So we have lots of other protocols.

TCP/IP (Transmission Control Protocol/Internet Protocol) : 2 different protocols that work together to help get the data between systems. The reason we call it TCP/IP is because almost all the data that we send on the Internet uses the TCP protocol. TCP is connection based protocol which means if I'm a client I'm going to first talk to the server and I'm going to go “hello hello” and I'm going to wait until the server comes back and says “Yes I hear you.”. We create what's known as a handshake and then we start doing whatever we do.

I say hello to ice cream guy, he say hello, we shake hands, maintain eye contact. After that contact, I say whatever I want and ice cream guy gives me what I want. And then we’ll say so long. This is TCP.

UDP (Connectionless protocol) : You just say what you want to the ice cream guy. And And he's just ready and he'll start making what you want without any questions at all. This is UDP.

ICMP (Single packet only) : ICMP is connectionless. ICMP is single packet, never more than one packet. For example ping command, when we just do 1 ping only it is ICMP.

Protocol Data Unit (PDU) : We organize packets by PDUs. Which basically goes for example I’m looking at one of the chunks of data:

This is a PDU.

What part I am interested in?

For example if I'm talking about switches what I'm interested in is MAC addresses and in that case we're going to be talking about this whole thing which we call an complete ethernet frame.

 This is a PDU.

Once we’re in a system, we are interesting this part of the packet. Now we are talking about IP packet.

This is a PDU.

Once we’re actually in our system (computer etc.), then we just interested in this. In this case this could be TCP, UDP or ICMP. We can call this TCP segment or UDP datagram.

DNS has only one job and that is to take fully qualified domain names (FQDN) for example [www.youtube.com](http://www.youtube.com) and the figures out what IP address is associated with that.

FQDNs have a 255 character limit (includes dots).

DNS replaced something called hosts file. It lasted as the primary way to resolve names into the mid 1990s and for the record every computer on earth still has a host file. Back in the old days if you wanted to join the internet you would type in your IP address and give your computer some name and then you would submit that and then every morning at 3:00 a.m. that host file was distributed to every single computer on the Internet.

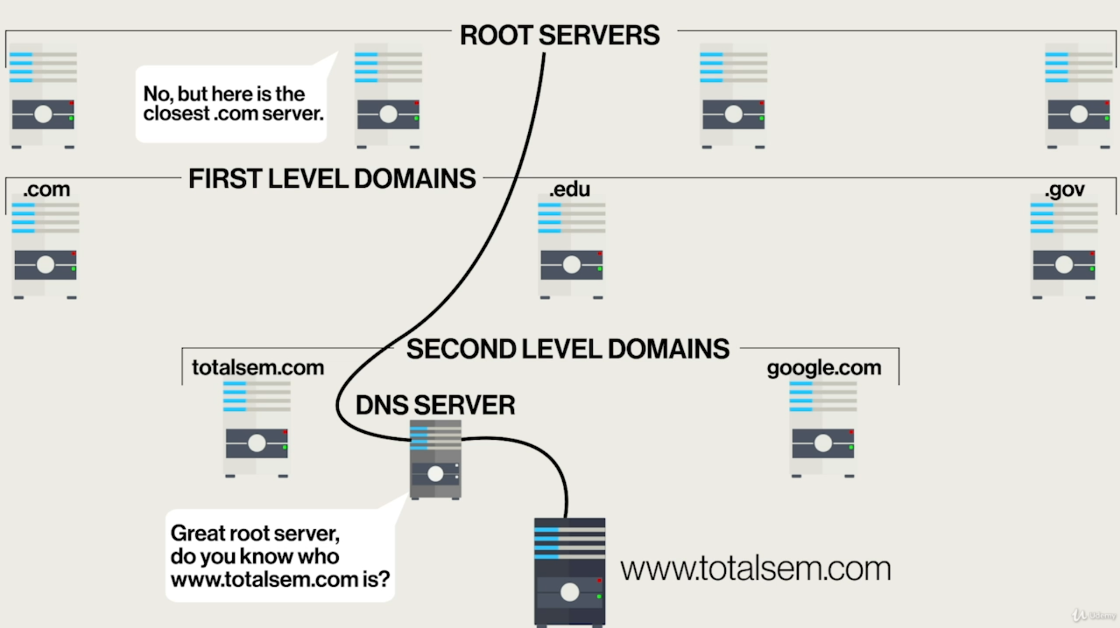
For example we want to go to [www.totelsem.com](http://www.totelsem.com).

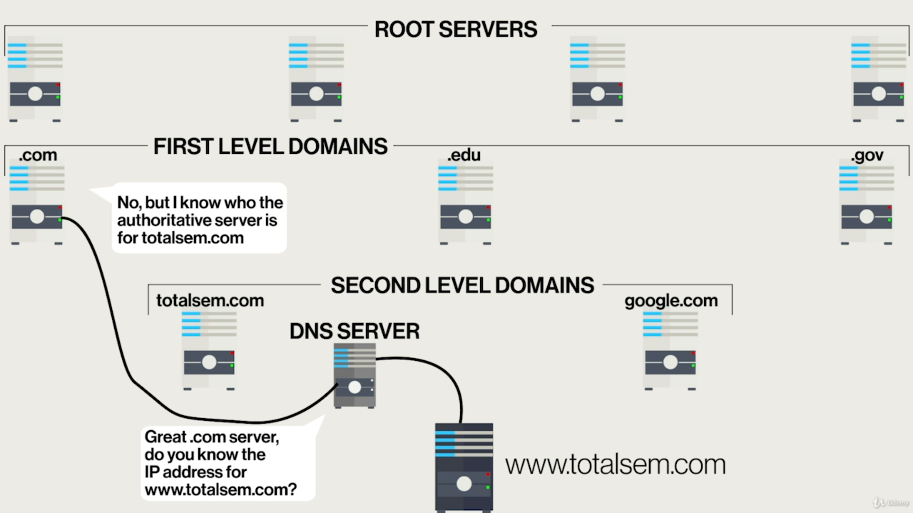
totalsem.com server has this information inside.

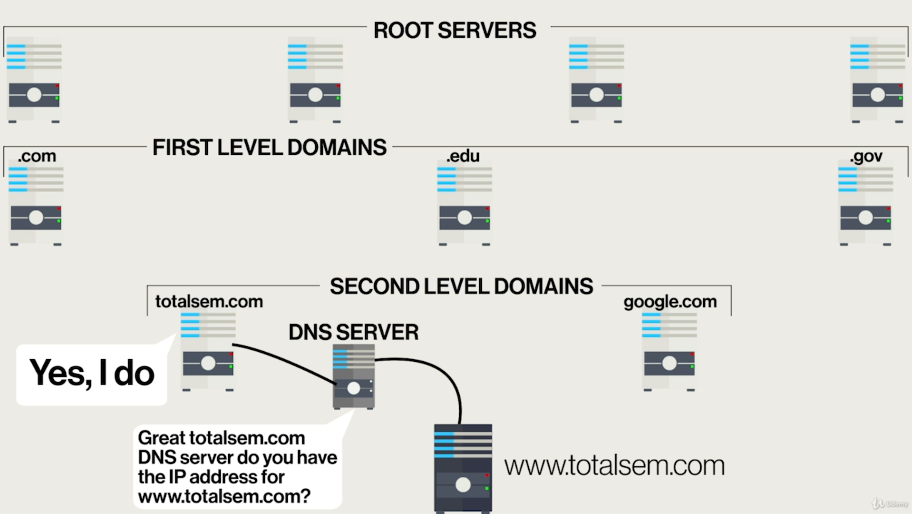
We have DNS server entered into our computers (grey one). It has to be typed in or provided by DHCP.

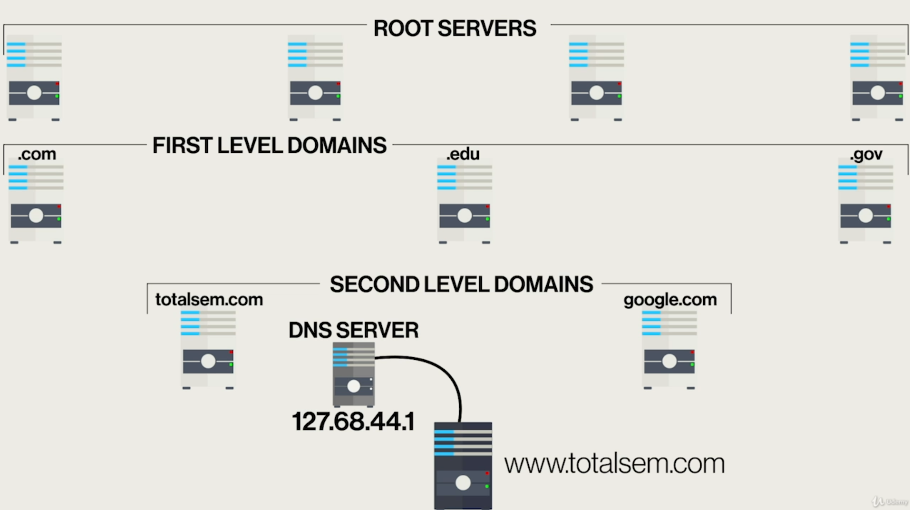
When the moment you hit www.totelsem.com and hit enter on your web browser it will automatically go up to your DNS server and you'll ask the DNS server the simple question “Do you know what the IP address for www.totelsem.com?” . If it doesn’t know, it has a list of all the IP addresses of all the root servers all over the world and it’s gonna pick one based on geography whoever responds fastest.

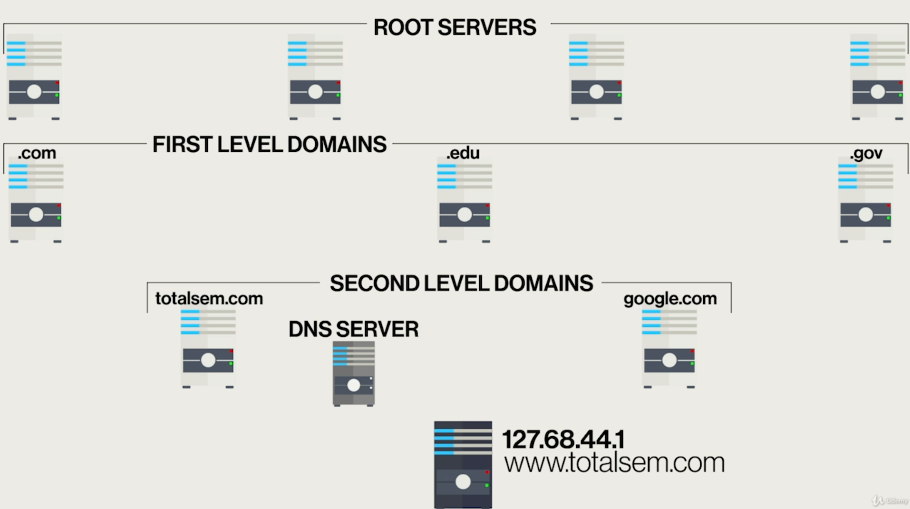
White DNS servers are authoritative.











Then your computer will keep a copy of the IP address of [www.totelsem.com](http://www.totelsem.com) internally in itself. Also your DNS server will keep a copy of that as well. We call it caching.

Somebody else who uses the same DNS server can get the IP address of [www.totelsem.com](http://www.totelsem.com) instantly because DNS server keeps a copy for a certain amount of time.

DNS is provided by your DHCP server.

If sth is wrong with your DNS connections, you can manually configure DNS. You enter 2 DNS servers. One is your local DNS server and other is popular one such 8.8.8.8 or 8.8.4.4. These are come from Google.

nslookup is a tool for DNS solver. It's built into pretty much all operating systems and it's it's a very powerful tool. The problem is that it used to give too much information so most DNS servers have locked down against this tool except for some very basic information.

My goal is simply to say is a particular DNS server a good DNS server. So you can type nslookup at command prompt, it says you the DNS server you’re using. At this point, you can actually talk to the DNS server like “What records are you storing?”. DNS stores lots of different records for example your regular run of the mill record is called A record (Your www and the IP address). Also MX record which is used by mail servers so when you're sending mail it knows how to get to the right spot. Also there’s Cname. If there's more than one name for a particular IP address you can give it different names.

DNS server are not tend to answer so many questions. They don’t answer these 98% of the time.

After type nslookup, you can type any site to the given field. If you don’t get error, your DNS server is good.

You can also type “server 8.8.8.8” to the given field and your DNS server will change.

Microsoft also has a naming scheme for Windows.

Windows naming is designed for LANs.

Netbios/netbt are the names to infer about this naming convention that we use for Windows.

Your Windows has a name. That name is usually set up during the installation itself.

The naming system on Microsoft Windows predates DNS.

All Windows systems will be a member of a domain or a workgroup.

Now if you install a Windows system it will either be a member of a workgroup or it will be a member of a Active Directory Domain.

A workgroup is the most basic type of networking organization there is. It's really just used as an organizational tool. It has no security and has no central administration. It's extremely old fashioned and for small networks it works just fine.

To use domain, we need to have a different kind of computer: a Windows Server System. The type of domain we use today is called an Active Directory Domain. It provides incredible security, substantial central administration. Active Directory Domains are also very powerful.

There is also another thing called homegroup. Microsoft wanted something kind of in between the security and the convenience of work groups. But this is disappeared.

If you have a Windows system, it will be a member of a network organization. At the very least it will be a member of a workgroup. Workgroups are the most basic organization there is. They have no real security as a workgroup. There is no administration as a workgroup. For the folks who just want to share a printer or share a folder, workgroups are fine. Active Directory Domain is gonna require you install a copy of Windows Server, you're going to have to have this up and running. You have to establish the concept of a domain. Then all the computers have to join the domain. It is very powerful very secure but it is expensive and takes a lot of expertise to setup. The concept of a homegroup was sort of automated not quite a domain but a lot better than a work group organization that kind of set all this stuff up for you.

Bottom line is workgroups are what you going to get for defaults.

Active Directory domains are something you're going to pay for through expertise and money.

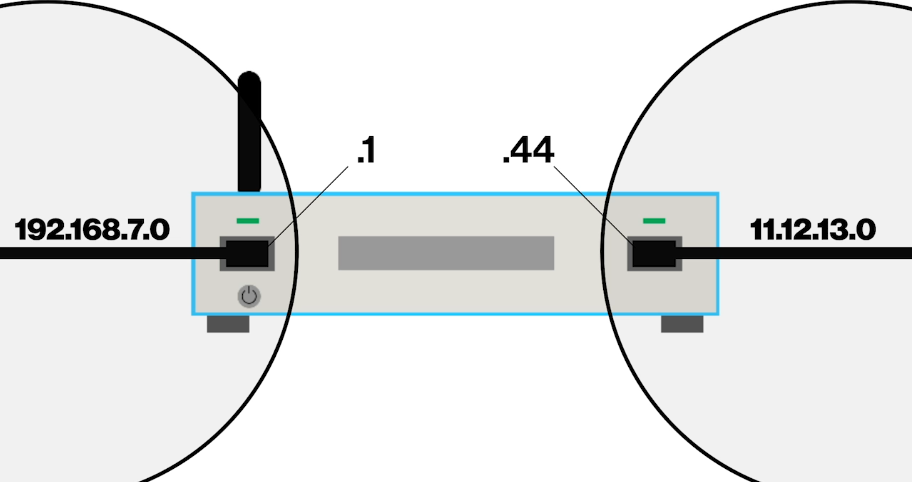
Homegrops are gone.

Router are devices that filter and forward traffic based on IP addresses. We interconnect LANs with routers.

Routers don't care where any packets come from.

Routers have a routing table. Routing table tells the router where to send stuff.





Generally in a router there are switch and access point. All routers don’t have wireless. If you need wireless you get wireless access points, if you need a router you get a router.

Routers don’t care about their connections. You can connect to them using ethernet, you can connect to them using cable modem -DOCSIS-, etc.

There is console port behind the router. It is a serial port using the RS232 language to act as a connection. You can connect your computer to the router via this port and some program such as putty will actually allow you to talk to the router.

SOHO = Small Office/Home Office

SOHO routers are more than a router. They have built in switch and access point.

Routers come with default username and password. You should change them.

If you see APIPA address as your IP address (This means that router is not passing out DHCP), then you should set your IP address manually that matches router’s range.

Almost all routers are DHCP clients to whoever they’re upstream to. Whoever is upstream is giving them an IP address, a default gateway, a subnet mask, and also DNS information.

Quality of Service (QoS) : Toolset which allows you to meter how much bandwidth things get. You can give a certain IP address more bandwidth than others, you can give a certain MAC address more or less bandwidth than others, you can assert certain ports to have more or less bandwidth than others.

Universal Plug and Play (UPnP) : A tool that makes your device a little bit noisy and it announces itself to the world. It will show up in your networking and things like that a little bit easier than if you were to just count on windows to do it by itself.

For Windows, you’ve got Link Layer Discovery Protocol (LLDP) which is on by default.

UPnP and LLDP help with network device identification.

Simple Network Management Protocol (SNMP) : Tool that goes way beyond simple discovery. It's a powerful tool that's used by network administrators to not only know that for example there's a switch there, but to be able to see how much bandwidth is going through the switch to. Not only know that there's a router out there but to have an idea of what is the router filtering right now. Simply it enables querying of network devices.

VLAN (Virtual LAN) : VLAN takes one physical switch and electronically turns it into two or more switches. It literally separates the LAN. In this way, I can keep my VoIP phones on their own separate network (Phones can’t talk with other devices that are connected to switch outside of the VLAN ports.) without having to buy an extra switch.

Switches uses MAC addresses. They don’t have IP addresses. So what we're going to do is we're gonna give this switch an IP address, not because the switch needs an IP address but because it gives us a way to get to the switch so we can configure it. This is Managed Switch.

Port security : I can tell to switch that “Whatever computers that are plugged into you right now, memorise those MAC addresses and if anybody else other than the MAC addresses that are on here right now try to plug in, just turn the port off, disable the port or send me a note saying ‘There's a unauthorized MAC address.’ or something like that to let me know that there are devices that shouldn't be playing on this switch trying to come in.”.

Rogue DHCP server : Occurs when you expect an IP address like 192.168.4.sth and you get an IP address like 192.168.7.sth. You've got a trace and find whatever box is doing that.

WIRELESS

IEEE 802.11 Standard : Primary way all of our wireless stuff talk.

Wireless Access Point (WAP) : A bridge between an ethernet network and a wireless 802.11 network.

If you have a wireless access point or 2 or 3 or 4, we are in what's known as infrastructure mode.

You also need wireless network card or USB type device.

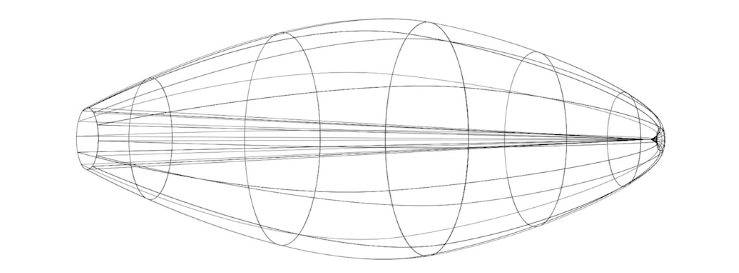
In laptops, antenna for the wireless network card is actually in the monitor.

All tablets, smartphones have 802.11 network cards built into them and the antenna is the entire case.

Service Set Identifier (SSID) : Name of the wireless network. Your network card will connect to it through its client software.

That was infrastructure mode. There is also another mode called ad hoc mode. With this mode there is no access point. You just have bunch of network interface cards. Your computer act like a wireless access point.

There are 4 types of antennas:

1. Omni-directional : Looks like a stick. Like antennas on automobiles. Radiation pattern looks like a big fuzzy ball. The more power you put to the antenna the larger this fuzzy ball gets.
2. Dipole : Looks like a stick. 2 omni-directional antennas are pointing exactly opposite of each. You get a big flat circular signal which is absolutely perfect. Don’t propagate the signal to upwards or downwards.
3. Patch : Looks flat square. Radiation signal is a big fuzzy ball but only half of one.
4. Highly directional : Yagi antenna and parabolic antenna. Really good for long distances. It’s radiation pattern looks like this: 

Original 802.11 standard defined a networking speed of about 1 Mbps.

We extend the standard to support newer technologies, faster speeds, able to support more systems that type of thing.

802.11 is based on the unlicensed industrial, scientific, and medical (ISM) radios bands. Bands are 2.4 GHz band and 5 GHz band.

Band : Range of radio frequencies.

2.4 GHz band : 2.412 - 2.4884 GHz

So we've got this whole range of frequencies to work with so different wireless access points can use different ranges. So we don't stop on each other.

Channels : In 802.11 2.4 GHz band, there are really 14 different channels and each channel takes a different piece of this band. And the idea is is that you can tune your wireless access point to use one channel while your neighbour or sth uses a different channel. So we don’t stomp on each other.

For 2.4 GHz band in Europe, there are 13 channels; in US, there are 11 channels; in Japan, there are 14 channels.

5 GHz band : 5.150 - 5.875 GHz



Inside the WAP, there is a radio and this radio is either 2.4 GHz radio or 5 GHz radio.

EXTENSIONS TO 802.11

If you've got 802.11g you are automatically backward compatible with 802.11b. Because radio frequencies are same.

802.11n is backward compatible with anyone of the extensions.

MIMO (Multiple in/Multiple out) : It allows a single wireless access point to use multiple antennas to change its radiation signal in such a way that it almost kind of zeroes in on a device. You just make sure you have an 802.11n wireless nic and you have an 802.11n wireless access point and you get the MIMO.

802.11ac : It can split the channels. It is fast. It improves the concept of MIMO that we saw on 802.11n and creates multi-user MIMO. Instead of just having one client that we can kind of zoom in at a time it can zoom in on multiple clients at a time simply depending on the number of radios it has put in it.

They say Wi-Fi 4 for 802.11n,

They say Wi-Fi 5 for 802.11ac.

You can have more than 1 SSID for one router.

Profiles store the SSIDs and their passwords.

Wireless Mesh Network (WMN) : It's basically ad hoc mode. Mesh networks have a base station and beacon devices that connect to the base station. Mesh networks use their own encryption. Mesh networks are universally easy to configure.

Alternatives for 802.11

RFID (Radio Frequency Identification) : RFID manifests as a tiny little sticker. This sticker is actually a radio and it stores usually a few hundred bits of information not a lot although there are some versions of RFID that store more. Radios activated by the energy of the scanning device.

RFID requires some kind of reader to activate the RFID tag which then will send data back to the reader itself.

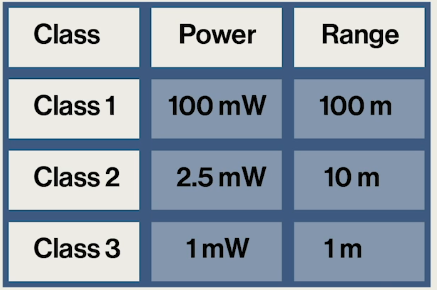
These readers use radio frequency energy to power up stickers. Then the stickers have enough energy to transmit back. So whatever information they have will be transmitted back to the reader and you get whatever you need.

For example if a trash can is empty or not, toothpastes all of these use RFID.

We don’t see RFID much except for Near Field Communication (NFC).

For example you have a laser printer and this printer is tap to print. All smartphones have RFID reader in them that does NFC. NFC is RFID. So we see these types of NFCs for all kinds of tap to sth. For example tap to pay.

Bluetooth : From a signal level, it looks a lot like 802.11 but it has some very big differeneces. Bluetooth is designed to connect to only 2 devices together one time. This called as personal area network (PAN).



PAN is unique only to Bluetooth network. It's a direct point to point connection between 2 bluetooth capable devices.

LAN is connection of computers in an area with a switch. All computers have same network ID (e.g. 192.168.4.0).

WAN is connection of LANs with one or more routers. Each one of LANs has unique network ID.

MAN (Metropolitan Area Network) is spread of WANs out across an entire town or sth.

The Internet is connection of these different towns with more routers so that it covers whole world. So the internet is the biggest WAN.

Internet is broken up into Tiers.

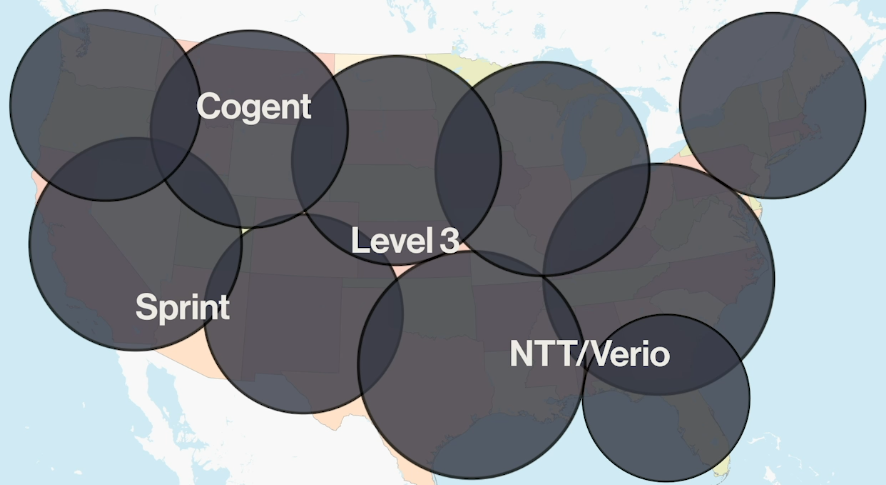
TIER 1

Around the US, there are around 10 different companies that provide internet to very large customers. None of these companies provide complete coverage of the US. However between these 10, they cover the entire US. They have to work together to cover. These people are actually competitors but they have to work together because nobody can cover the United States completely.

So these different companies creates peering agreements. It goes like this : “I hate you and you hate me. However let's go ahead and allow each other to let each other's traffic go through and that way together we can cover more of the US.”

They have to have place where they interconnect. There are very protected places called Network Operation Centers (NOCs). The idea behind these places is that they're owned by third parties. Then competing companies will come in and then they will build routers inside these NOCs and you then run a connection between these two sets of routers and that’s how we interconnect.

All of these are Tier 1 which are working together.

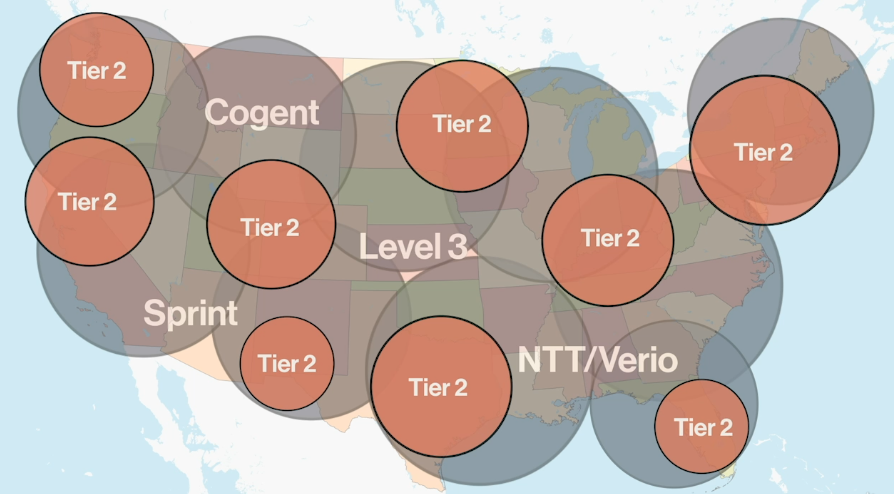


TIER 2

Tier 2s have not come up with a peering agreement with the Tier 1 providers. In essence, they have to pay for their internet just like you do. However they do have some period agreements with some folks.

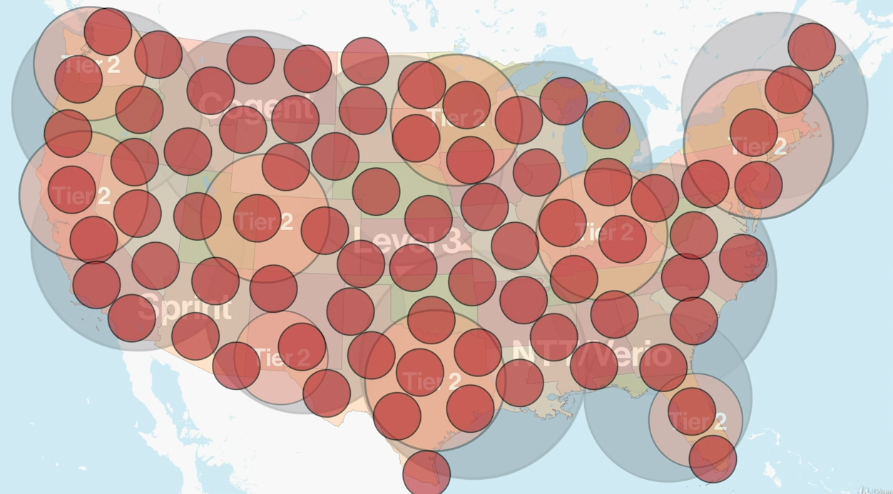
If you don't pay for anything you are Tier 1, if you pay for a few people in a few places but otherwise you are period with others you're Tier 2.

Tier 2s show up at these NOCs just as anybody else does but they're not quite as big.



TIER 3

These are big Internet Service Providers. They are not totally interconnected. They make their money by selling Internet services to individuals and corporations. They almost have no period agreements and they're going up to the Tier 2 and Tier 1 and they're paying for their internet. Comcast, AT&T are examples. Tier 3 pretty much pay for everything they got.



And then at the bottom of the food chain of the internet are people like you.

Somebody who's a Tier 2 today could be a Tier 3 tomorrow or vice versa.

Dial up : Dial up (best known as Plain Old Telephone Service (POTS) or Public Switched Telephone Network (PSTN)) is the old school telephones. 56 Kbps max. Use modems. Modems convert analog POTS to digital COM port connections. Modems connect to other modems using a phone number.

Comport : How Windows recognizes different serial ports.

ISDN : ISDN was the first time that we started to move into the digital world. Doesn’t use modems. Uses something called terminal adapters. 64-128 Kbps.

You are gonna use broadband connection to use the internet.

Broadband connections are typical way we connect. Cables, DSL, wireless, satellite…

Broadbands are high speed, always on connection.

Digital Subscriber Line (DSL) : It piggybacked on top of telephone lines to give you a digital service. You could still have a regular telephone on that line but it added more signal that was a digital signal.

Asymmetric DSL (ADSL) : Means that your upload speed was much slower than your download speed.

Symmetric DSL (SDSL) : Means that your upload speed and download speed are same.

Point-to-Point Protocol Over Ethernet (PPPoE) : When people first started using broadband, we thought we were going to do it like dial up where you had a modem in your computer and you connected and if you wanted 2 computers to connect to the Internet in your house, they had a dial another phone number. But with broadband people started using routers for the first time. So what we would do is that we'd end up putting four or five or six people on one intricate internet connection.

Cable : Uses a protocol called DOCSIS (Data Over Cable Service Interface Specification). DOCSIS is pretty similar to ethernet. It has MAC addresses etc.

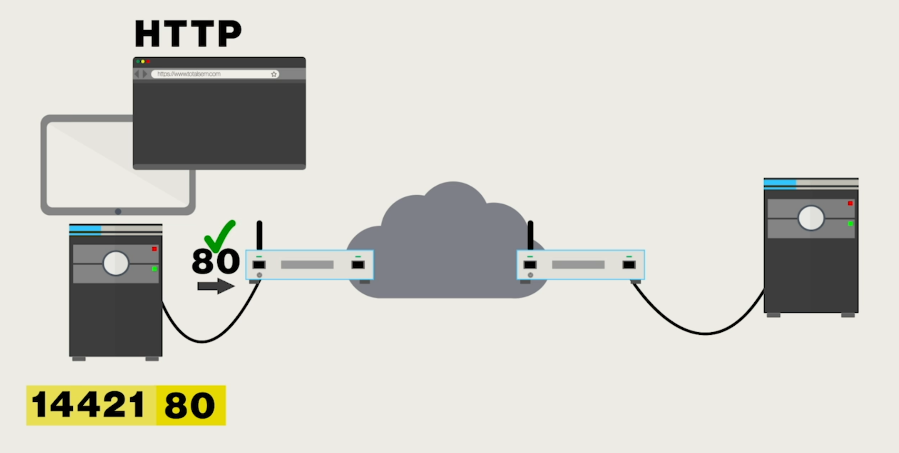
Satellite : The only downside to satellite is that it gets what we call latency.

You can use special 802.11 setups for your ISP.

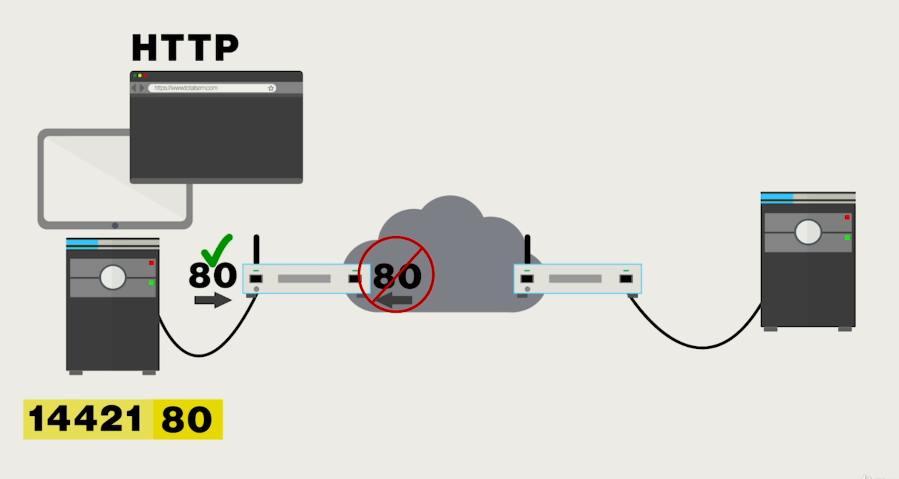
Many metro areas provide native Ethernet for ISP.

Firstly, any outbound going out on port 80 has to be allowed by host based firewall.

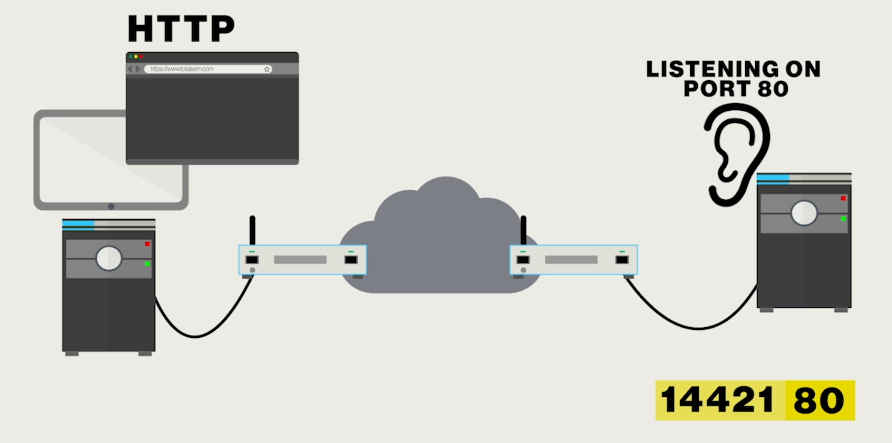
Secondly, our router’s firewall has to allow outgoing port 80. Most routers, certainly all SOHO routers allow outbound port 80 by default.



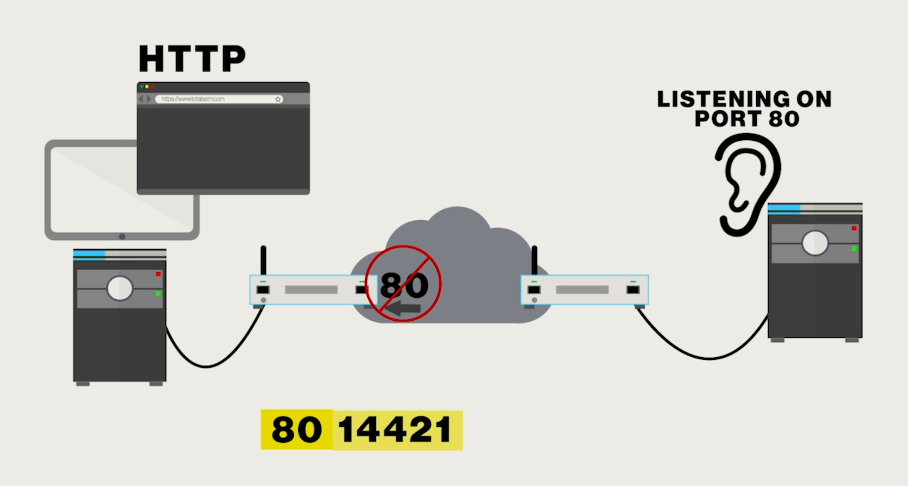
Firewall is also gonna block incoming port 80.



Server is listening for incoming port 80 and it’s gonna process that. When it sends it back, it’s gonna swap incoming outgoing port numbers. So now the destination port number is going to be 14421 and then the source port becomes 80.



Firewall is not gonna block us because our destination port is not 80. Our destination is 14421.

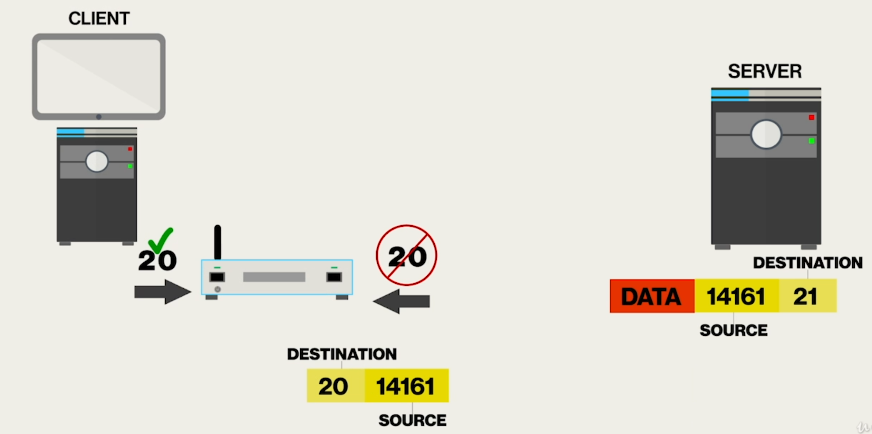


All servers have firewalls. Anything that a server is listening on whatever that port number is, it has to be left open. For example Above server’s firewall can’t block port 80.

FTP (File Transfer Protocol) : Protocol like HTTP. Old way to move files around on the Internet. FTP is used to transfer files from one system to another. Uses port 21. Every web browser on earth is an FTP client. FTP was early cloud storage. FTP uses passive and active mode. Active mode is much faster.

In passive mode, you send your data with destination (21) and source port (e.g. 14161) and server swapped these port numbers and sends it back to you.

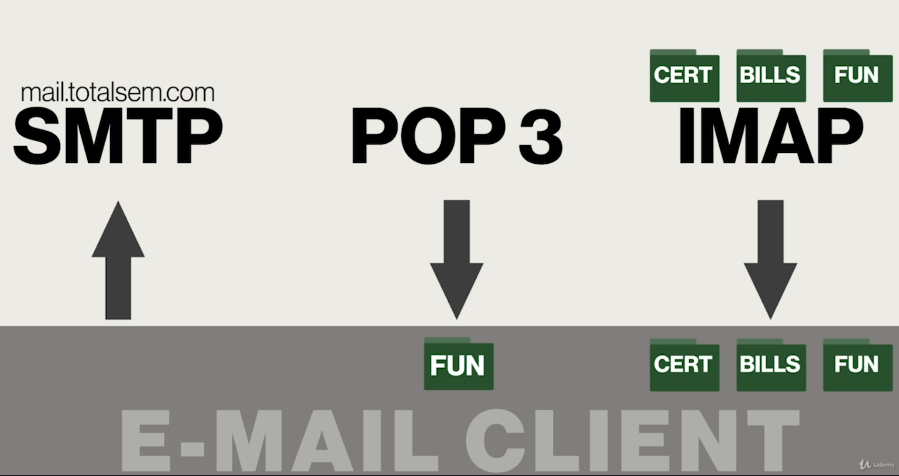
In active mode, you send your data with destination (21) and source port (e.g. 14161) but server will start sending back communications on port 20 as a destination port. That’s a problem. Router will block this. You initiated on port 21, not port 20.



In order to deal with this, every router on earth has something called port triggering and it’s pretty much just for FTP. We say “If somebody says sth out on port 21, you need to allow incoming port 20s.”.

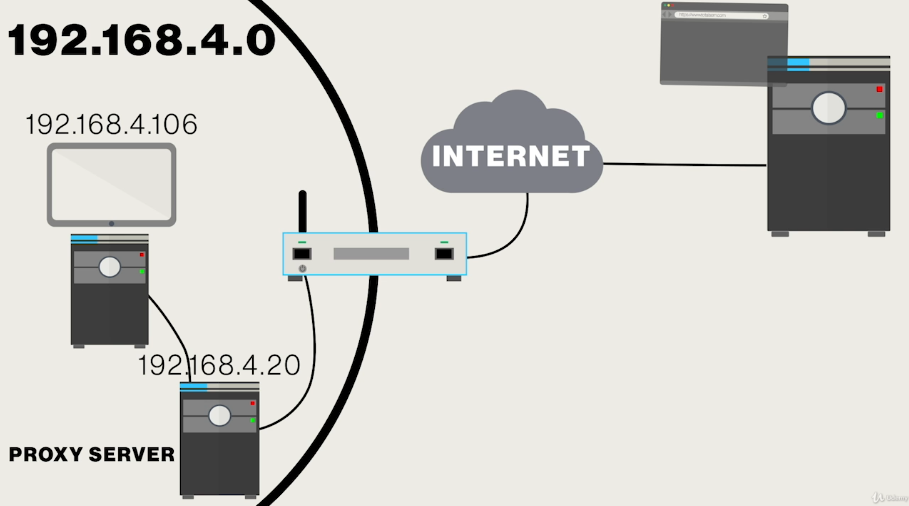
3 different protocols for email:

1. Simple Mail Transfer Protocol (SMTP) - Port 25 : SMTP is the protocol that we use to send our mail up to an SMTP server. So you have to configure an SMTP server and they usually have interesting names like mail.totalsem.com or sth like that. SMTP is used to send email from a client to an email server.
2. Post Office Protocol (POP) - Port 110 : Brings email down to your email client. You have to setup all your own folders on the client itself.
3. Internet Message Access Protocol (IMAP) - Port 143 : Brings email down to your email client. Stores all of your folders and all of your organization so that no matter where your client is, it will simply copy that down.



Latest verrsions is POP 3 and IMAP 4. No one use IMAP 2 or POP 2 or etc.

These protocols also have secure versions which have completely different port numbers.



Anything that's to the web, instead of going directly out to the router it's going to go through the proxy server and then out the router.

Why would we do sth like this :

* I could have in that proxy server a list of places you shouldn't be going to. Instead of just making my firewall store all this stuff, I could put it on this proxy server.
* I could have it to filter for my or incoming information.

Proxy servers are extremely popular in like schools and things like that to protect kids from going to places they shouldn't go.

I got to tell my web browser that whenever it fires up, don’t just go to the router, we need to go to the proxy server instead.

Proxy servers are application specific. If you want to proxy web pages you've got to go into your web applications (your web browsers) and make some changes.

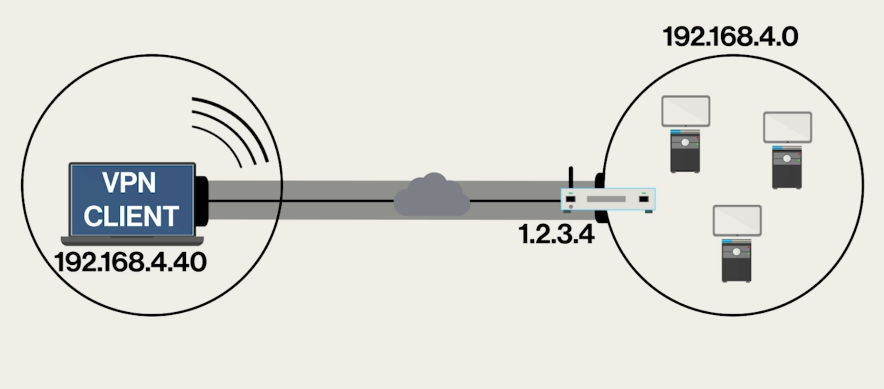
Web browser is actually a lot of different clients. It is a HTTP client, it is a HTTPS client, it is a FTP client…

The nice part about a proxy server is not only does it filter out things we're not really happy about, but it also has some real benefits:

* Proxy servers can do caching. If I've got web pages that everybody goes to a lot, a lot of times I'll just set up a proxy server just because everybody can very quickly get to that web page.

Virtual Private Network (VPN) : What we're doing is we're taking the Internet and turning it into a fake, virtual private network. For example if you are at airport, it seems like you are connected to your switch at home, and you got an IP address just like you are at home. You can see all the shared resources on your LAN just like you are sitting at your desk.

VPN client is a special software. It’s gonna make a direct connection between your laptop and the WAN side of your router at home. You know WAN side IP of your router because it never changes, it’s static. You give this IP to the VPN client.



This is VPN tunnel that makes this connection.

IoT device has microprocessor, address to it can be talked to, API.

How can we talk with IoT devices:

* 802.11
* Zigbee : used exclusively for IoT. It's designed for home automation. Runs at 2.4 GHz band. It doesn't have a lot of bandwidth because it doesn't need it.
* Z-wave : Runs at 900 MHz band.

You have to have some kind of hub to link to the IoT devices.