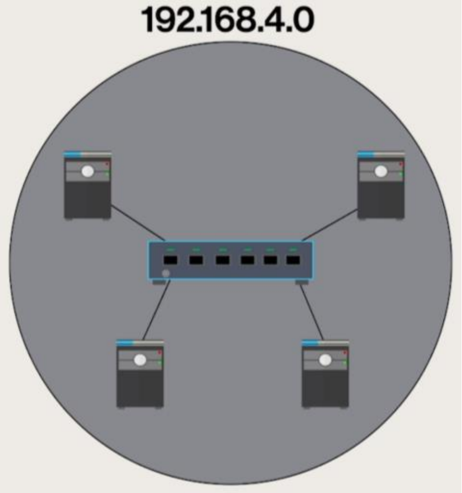
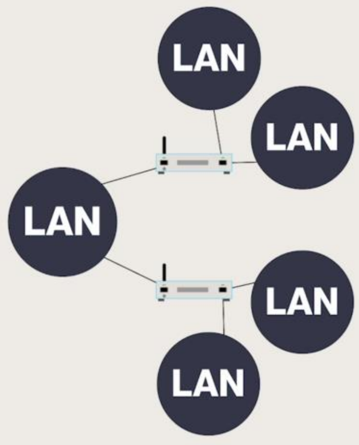
## Beyond the LAN

**- Local area network (LAN) computers share the same network ID**
**- Wide area network (WAN) is 2 or more LANs interconnected by 1 or more routers**
**- A metropolitan area network (MAN) is a WAN that spans a city**
**- Personal area network (PAN) is a point-to-point connection**
**used only in Bluetooth connections**

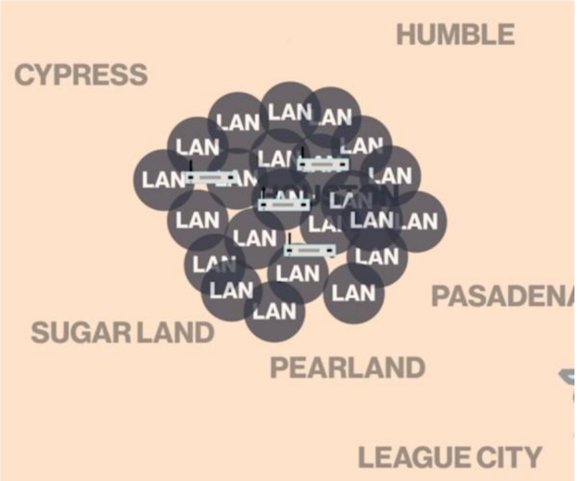


LAN (Local Area Network) - group of computers connected together by a Switch
in a way that they can communicate with each other

All of the computers within this LAN
are going to share an Identical Network ID
In this LAN they're all going to be 192.168.4.0



WAN (Wide Area Network) - 2 or more LAN's connected by 1 or More Routers,
and each LAN having their own unique Network ID



MAN (Metropolitan Area Network) - WAN spread across an entire Town

The Internet - Connect all these towns together, with more Routers,
so it covers the United States, and the Entire World

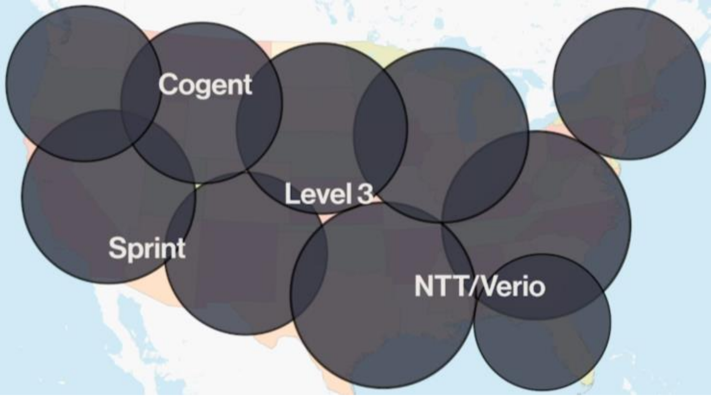
The Internet is the biggest WAN we have!!

PAN (Personal Area Network) - unique to only Bluetooth Networks,
which is a Point-to-Point connection between 2 Bluetooth capable Devices.

## Internet Tiers

**- The Internet is composed of many organizations that connect to each other**
**- Tier 1 are providers that do not pay anyone (peering)**
**- Tier 2 are providers that pay some Tier 13 but also peer with Tier 1 and Tier 2s**
**- Tier 3 providers pay Tier 1 or Tier 2 providers**

Internet is a big WAN, which is technically correct,
but the Internet is broken up into Tiers.



Tier 1 -
Across the US, 10 companies provide the Internet, not really to you & I,
but they provide the Internet to very large customers.

None of them provide complete coverage of the US,
but all 10 companies collectively do cover all of the US.

These companies have to work together! They're competitors!!
They need to create Peering Agreements.

Peering Agreements - Even as competitors, they need to allow each others traffic to go through, and that way together we can cover more of the US.
Other countries handle business the same way as the US.

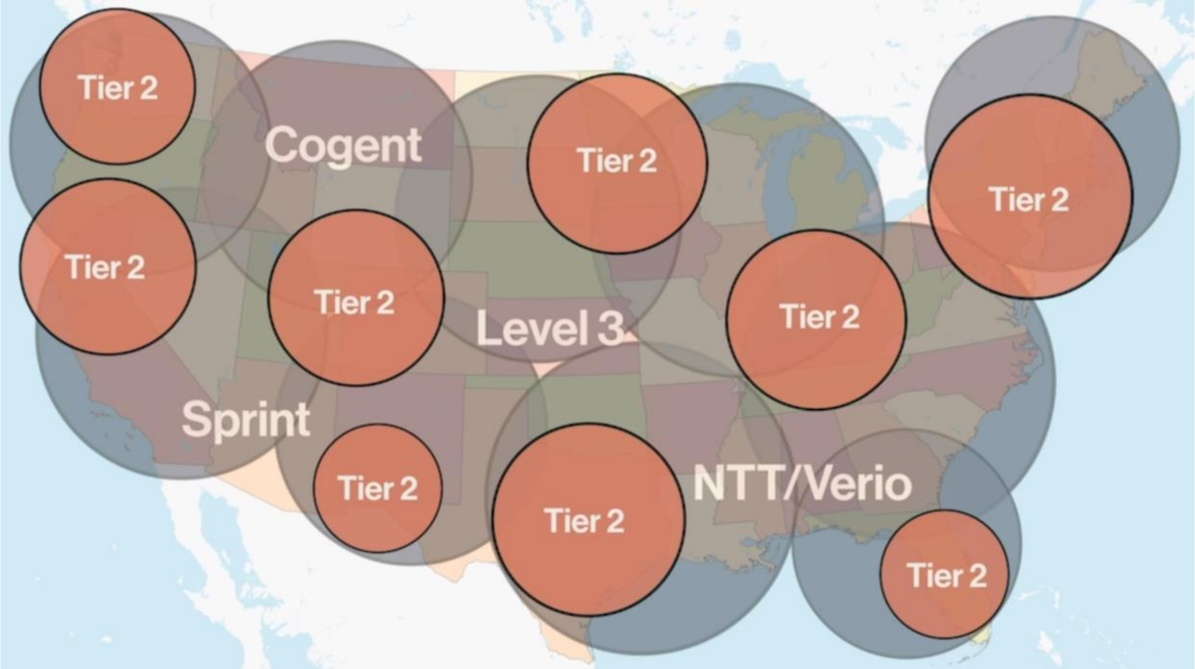
In order to share, they have to interconnect in NOC's

NOC (Network Operation Centers) - Owned by 3rd Parties. Big building with lots of generators (to keep it from losing power because that would be really bad), hurricane, and earthquake proof, and lots of security guards.

Competing companies will build Routers inside these NOC's,
and you run a connection between these 2 sets of Competing Routers,

and that's how we interconnect!!!

Tier 1 doesn't pay for Internet.



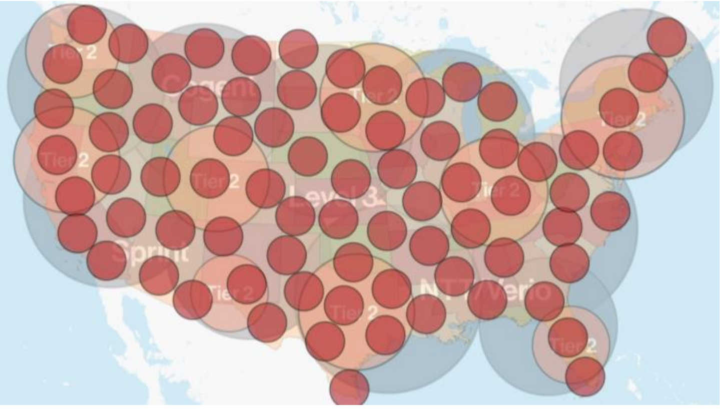
Tier 2 - Not as big as Tier 1 Providers, but they do have a good coverage area!

They have NOT come up with a Peering Agreement with the Tier 1 Providers.

They have to pay for the Internet, just like you & I do.

They do have some Peering Agreements.

They show up to these NOC's just like everyone else does.



Tier 3 - Big Internet Providers (Comcast, AT&T, etc)    No Peering Agreements

Lots of presence all over the place, but they're not interconnected.

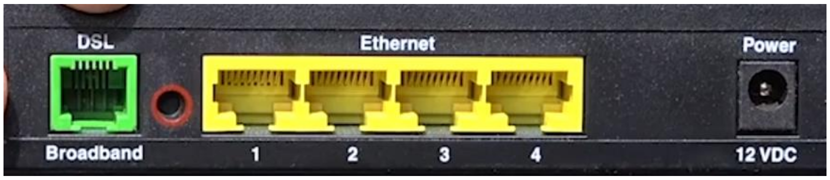
Make money by selling Internet Services to Individuals & Corporations.

They pay for their Internet from Tier 1 & Tier 2

## Broadband Connections

**- Broadband are high speed, always on connections**
**- Digital Subscriber Line (DSL) runs on top of telephone service**
**- Data Over Cable Service Interface Specification (DOCSIS)**
**uses cable connections**
**- Satellites are handy for more remote locations**
**- Many metro areas provide native Ethernet for an ISP**

Broadband Connections - typical way we connect to the internet using
Cable, DSL, sometimes Wireless, sometimes Satellite



DSL (Digital Subscriber Line) - one of the earliest versions of Broadband,
which used telephone lines to give you a Digital Service

DSL Modem (image shown) plus a Router, Switch & WAP
Green Connector (DSL) - Telephone Line Connection (ISP)

The Words displayed on the Device “Wireless Network Key”
indicated to Mike that it’s also a WAP

Modem - only thing that’s a Modem is an old Dial-Up Modem with Dial-Up Connection
We call all of these boxes Modems, even though that’s not what they really are

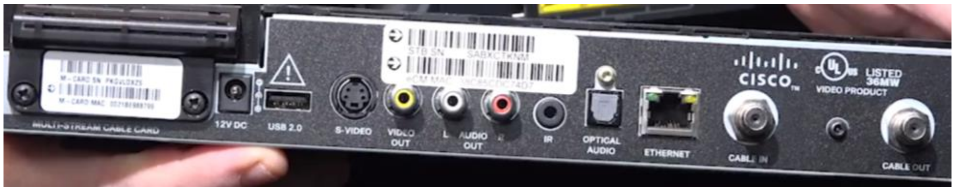
The image show is actually a DSL Terminal Adapter,
but everyone calls it a DSL Modem.

2 Forms of DSL -
Asymmetric DSL (ADSL) - Upload Speed Slower than Download Speed
Upload Speeds - 768 Kbps to 3 Mbps
Download Speeds - 1.5 to 7+ Mbps

Symmetric DSL (SDSL) - Upload & Download are the same Speed

For DSL Configurations,
Network → Internet → IPv4 → Internet Connection Type
Need to change the default Dynamic IP to PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) - allows multiple people to connect to the 1 DSL Modem in your house



Cable -
Cable In - Incoming F-Type Connection
Ethernet - Connects to your Router
Cable Out - just used as a Pass Through to keep a TV running on it

DOCSIS (“doe-sis” - Data Over Cable Service Interface Specification) -
Uses MAC Addresses
Good for using the Internet and watching TV at the same time

Cable Speeds have changed over the years -
Upload/Download Speeds - 1.5/10 Mbps Today 50/100 Mbps
With Optical, we see Cable today in the Gbps

ISP’s will charge $5 per mo for the Cable Modem Box to rent to you
You can buy one for $40 - just do this! Pays for itself in less than a yr

We can Clone the MAC Address from the ISP’s Modem to our bought Modem, which is the only difference between the one we rent and the one we bought.
Clone MAC Address - just manually type this in

Your ISP will ask that you Register your Modem with your ISP (Quick Phone Call)
At that same time, cancel the one that you rented.

Satellite - for anyone that doesn’t live near a Cable or DSL opportunities.

For those out in the country, or on the ocean.

Speeds of 3 Mbps/25 Mbps or better

It also has a Modem.

Latency - sometimes it takes a little longer to initiate the website connection because the Antenna on your roof has to connect to the Satellite that’s 12,000 miles away

Alternative to Satellite -

You can use Special 802.11 setups for your ISP

You can get companies that will get you a Yagi, or a Parabolic Antenna that connects to a Tower.

DSL may need PPPoE
Cable may need a Clone of a MAC Address
In the country, there may be nothing better than Satellite or 802.11

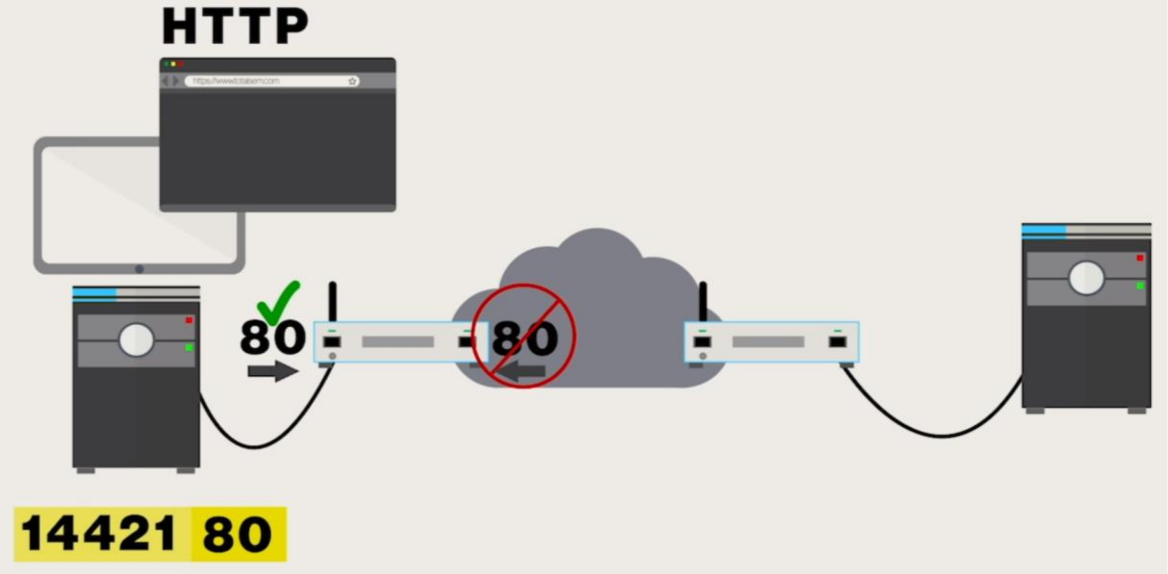
## Firewalls & Servers

**- All Internet connections require a client and a server**
**- One of the primary functions of firewalls is to block ports**
**- Client and server networks use firewalls**
**- Firewalls block ports on an incoming vs. outgoing concept**
**- Servers must not block incoming ports on the ports to which they listen**

What's happening when we make a connection to a Server?

Clients have their Host based Firewall and a Firewall on their Router
Servers have Firewalls too!

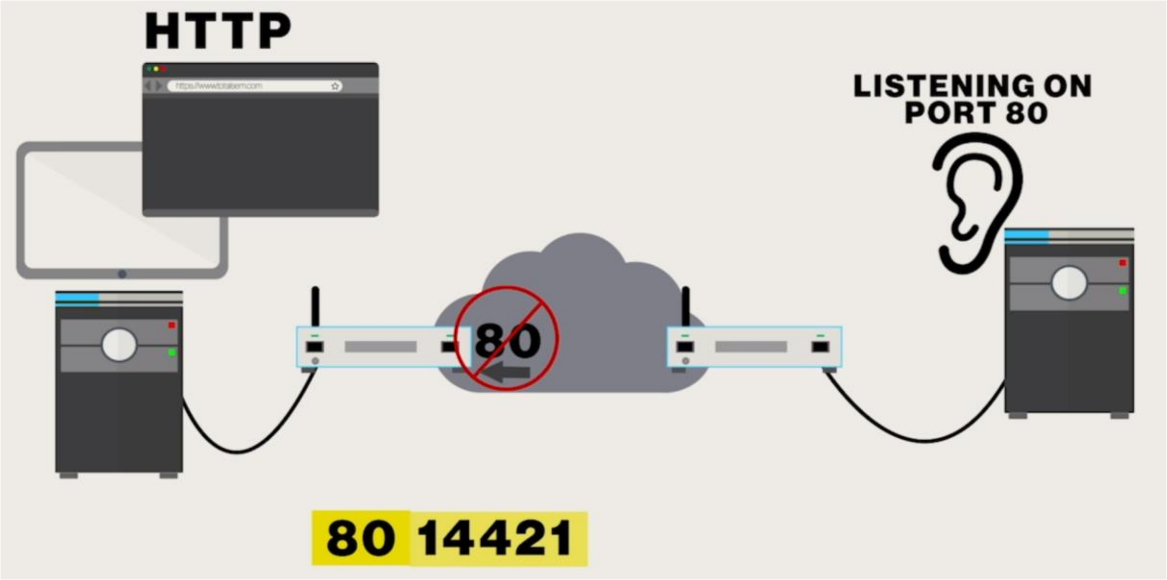
Let's review the idea of an IP Packet as it goes from a Client, to a Server,
and from a Server, to a Client.



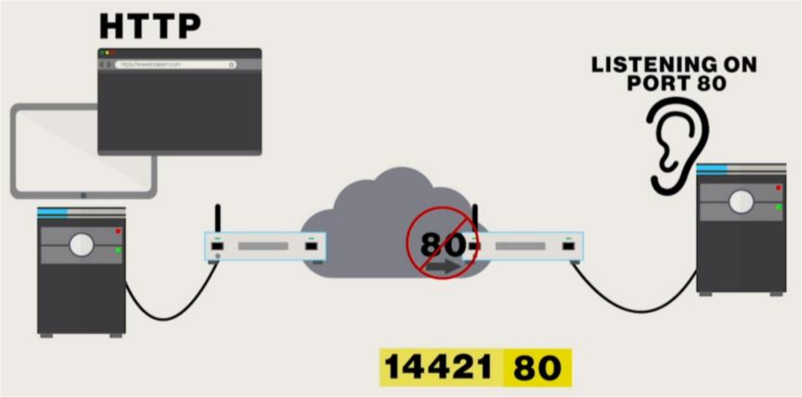
This Client computer is connected to all kinds of Routers, and all types of ISP's into the Internet. The Internet is so complex that we represent it by drawing a Cloud.
The reason it's a Cloud is because we don't care what's going on in there,
we just care about our Server being connected to the Internet.

I want to open up a Webpage on the Server, by first opening up a Web Browser.
We're going to have a Host based Firewall on this system.
Somewhere on the Firewall, it has to say
that All Web Applications go out on Outbound Protocol Port 80 (http),
(there will be another Port Number behind it),
and the Host based Firewall will let this through.

Our Router also has to allow Outgoing Port 80 (most have this by default).
This Router has a Firewall built in that's going to Block Incoming Port 80.



It goes out to the Internet and comes into the Server.
The Server is Listening for Incoming Port 80, and will process that.
When it sends it back, it will swap these 2 Port Numbers (Source & Destination).
Remember, our Router is blocking Port 80.
When it comes back to our Router, it's coming back with a Destination of 14421, so it goes right through our Router.



Think about this. If we have a Port 80 Blocker on the Router going to the Server,
none of our website requests would get fulfilled!
We can't have Port 80 Blocked on a Server!!!
Servers do have their own Firewall built in, just not set to block Port 80!

Router Firewalls serving Public Facing Servers, which are Listening for Port 80,
are not going to block individual Port Numbers,
but they will use Stateful Firewalls.

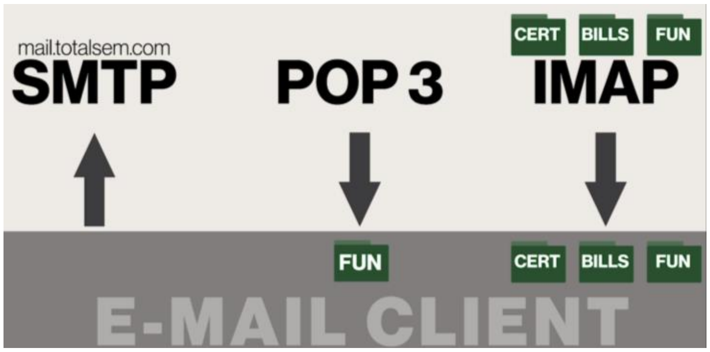
The reason our Routers coming into our House doesn't have Incoming Port 80,
is because we don't have any Web Servers in our LAN!!
We have Web Clients, but no Web Servers.

Our Routers don't worry about Outgoing Port Numbers,
it's only going to be worried about Incoming,
because we don't want people poking around!

## E-Mail

**- E-mail uses Simple Mail Transfer Protocol (SMTP) to send e-mail from a client to an e-mail server**
**- Use Post Office Protocol v3 (POPS) or Internet Message Access Protocol (IMAP) to pull e-mail down from e-mail server**
**- SMTP uses TCP port 25; POPS uses TCP port 110; IMAP uses port 143**
**- Setting up an e-mail account requires knowledge of the IP addresses or DNS name for the different servers**

For Web based tools (Gmail, Yahoo, etc),
you need to configure your Email to be able to Send & Receive Emails.
A lot of these are set as default settings.



SMTP (Simple Main Transfer Protocol) - Port 25
We use this to Send Mail up to a SMTP Server

Now you have a Choice between POP3 or IMAP
Both will bring Email down to the Email Client

POP (Post Office Protocol) - Port 110
Very simplistic, but you need to Set Up all of your own Folders on the Client

IMAP (Internet Message Access Protocol) - Port 143

Stores all of your Folders, and Organization,
so no matter where your Client is it will copy it down.
Today IMAP is very popular

There have been a lot of versions of POP & IMAP over the years

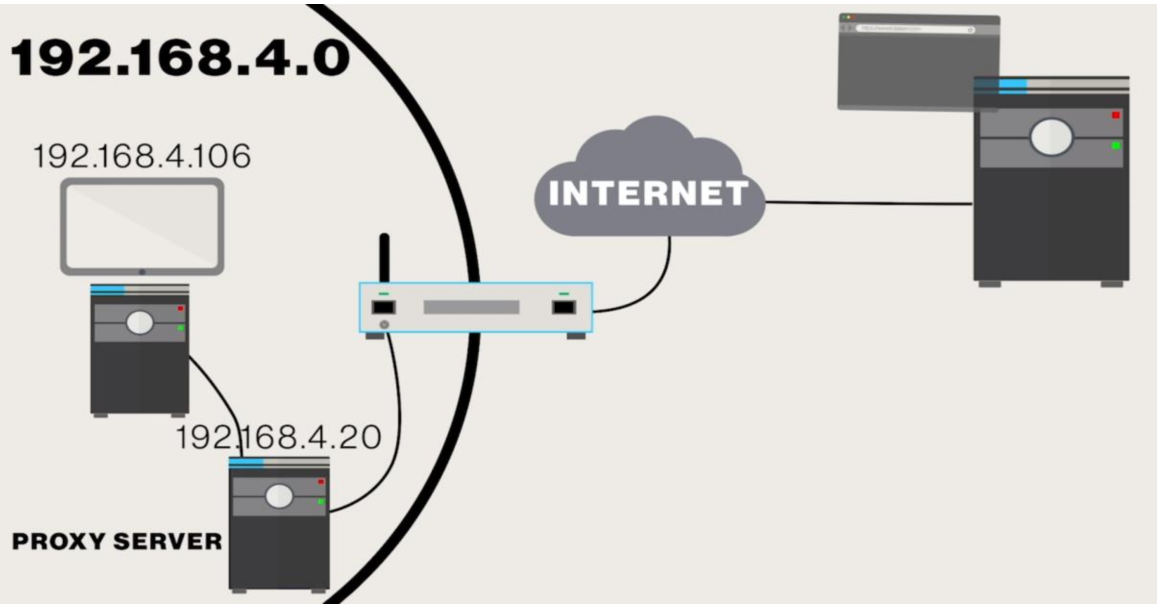
Latest versions are POP3 & IMAP4
Nobody uses the earlier versions. Secure versions of these 3 use Ports like 587

## Proxy Servers

**- A proxy server acts as a go-between (a proxy) between a client and a server**
**- Proxy servers are application-specific (9.9., a Web proxy for HTTP and HTTPS)**
**- Proxy servers provide firewalling, check for malware, ban bad URLs**
**- Applications must know the address of the proxy server**

Most of the time when we're connecting to a Web Server, or an SSH Server, or an FTP Server, etc, it's basically a Direct Connection with nothing in between you & that Server, other than a bunch of Routers, as it gets your Packets between the 2 of us.

Although, there can be something in between
that we'd want to be there like a Proxy Server.



We're in a Network, with a Network ID 192.168.4.0

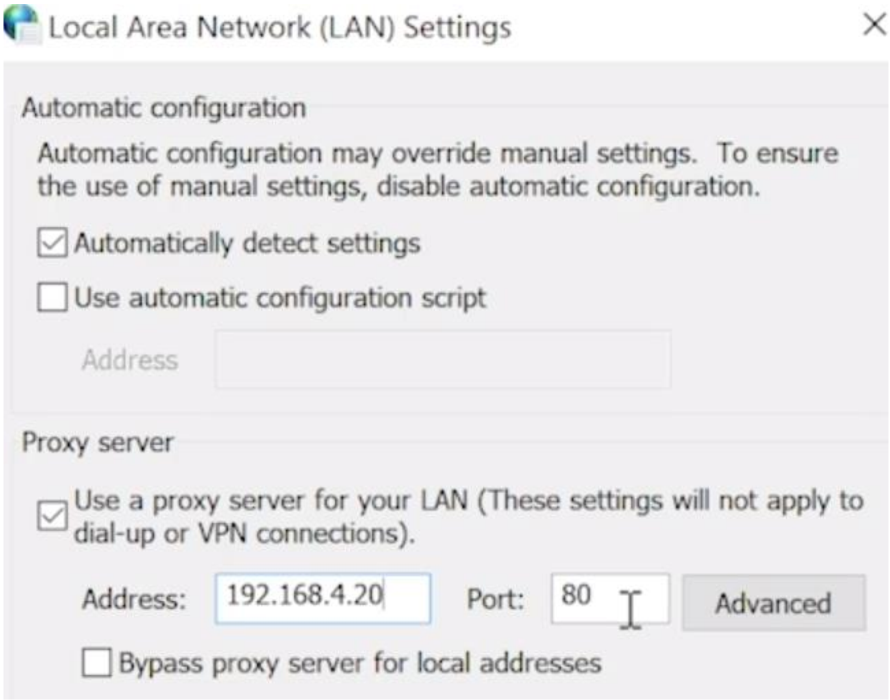
We'd send our Packet → Proxy Server → Router → Web → Web Server

Proxy Server - can be used as a filter for places you shouldn’t be going to.
Instead of having the Firewall store all of this info, we can put it on the Proxy Server.
We can have it filter for your information.

When a Packet comes back to your computer, it goes Router → Proxy Server → You
This can block anything we don’t want coming through to you.

Very popular in schools.

Proxy Servers are Application Specific
If you want to Proxy web pages, you need to go into your Web Browsers,
and make some changes.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.4.20 Port: 80 Advanced

□ Bypass proxy server for local addresses

Control Panel → Internet Options → Connections → LAN Settings

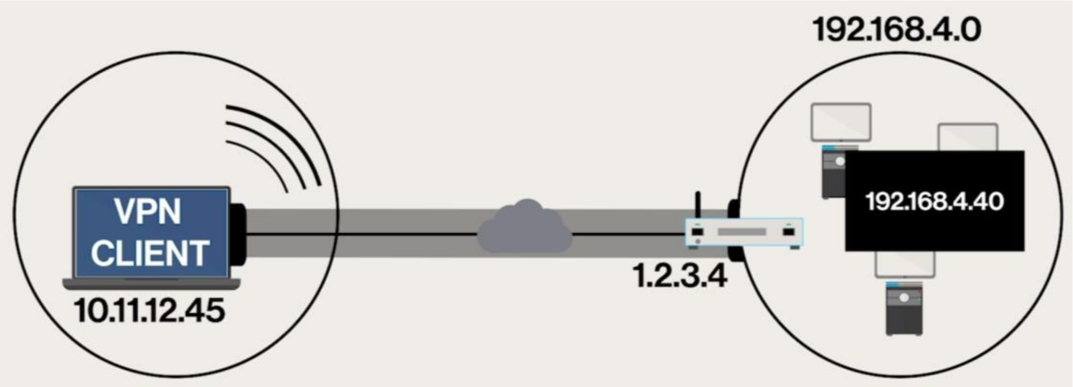
You have to select the checkbox for using a Proxy Server,
and you have to type in the IP Address of the Proxy Server.
Port 80 is set as a default.

Proxy Servers can do Caching, which is nice for frequently used web pages.
If there’s a site that's constantly changing, these Servers are very smart.
They’ll Cache all the static aspects of the site, and grab anything that changes.

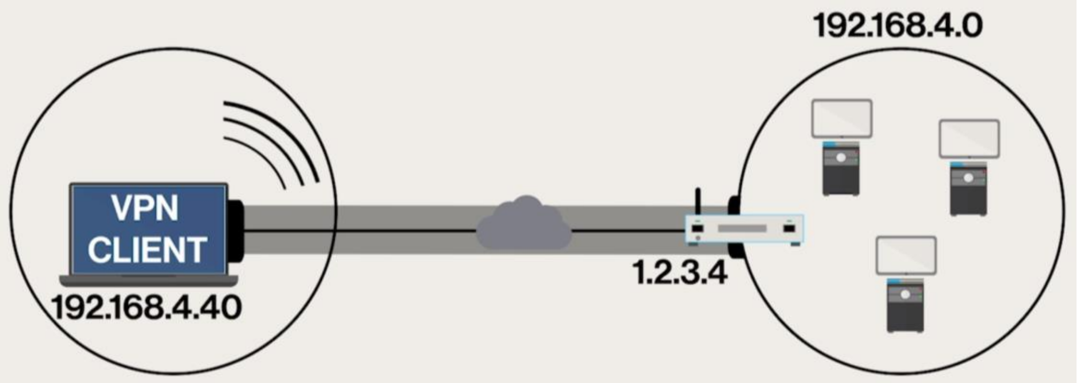
## Virtual Private Networks (VPN’s)

**- Virtual Private Networks (VPNs) use the Internet**
**to create a private connection to a remote network**
**- VPN client program connects to a VPN server at the remote network**
**- VPN client needs to know IP address of the VPN server to make the connection**

Virtual Private Networking (VPN) - we’re taking The Internet,
and turning it into a (fake) Virtual Private Network.
This enables us to see & use the devices we have in our normal LAN
when we’re not in the office!



With our Wireless we can have a VPN Client software installed on our Laptop,
which acts as a direct connection between our Laptop
and the WAN side of the Router back at the Office.



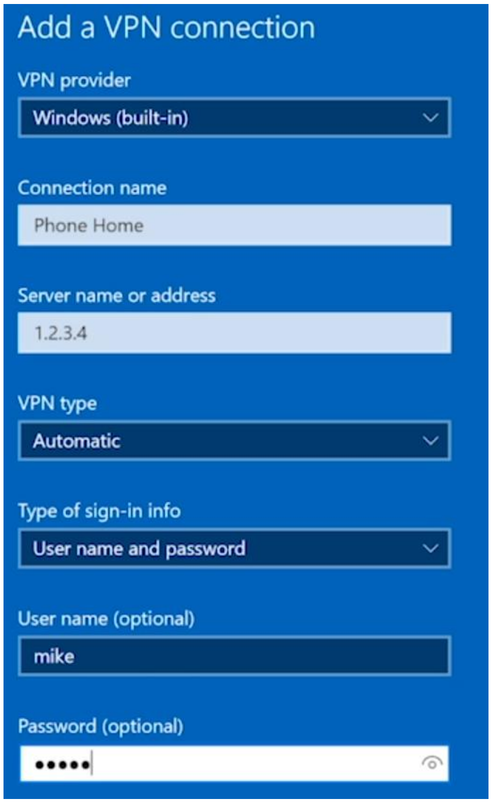
We need to tell the VPN Client software the IP Address of the WAN side of the Router. The Router lets you into the Network, and the DHCP Server gives you an IP Address. Now we have another connection that has the same address as if I was a DHCP Client on my Network!

This is a VPN Tunnel that makes this connection
To do this, we’d need a VPN Client, and a Router, or a dedicated box,
which acts as the VPN EndPoint in your LAN.
Most people buy a special Router with the VPN EndPoint software built into the Router
What we have to worry about is how we connect to our Router.

We need to set up a VPN Client. There's a limited one that's built into Windows.

There are lots of ways to make VPN's that have Protocol Names like
PPTP, L2TP, IPsec
For a lot of these we're going to need a 3rd Party tool

If you get a Cisco VPN Router, they'll give you software to make the VPN Client



Add a VPN connection

VPN provider
Windows (built-in)

Connection name
Phone Home

Server name or address
1.2.3.4

VPN type
Automatic

Type of sign-in info
User name and password

User name (optional)
mike

Password (optional)
•••••

For the software that came with Windows -
Right Click Start Button → Network Connections → VPN → Add a VPN Connection

When you save this, it manifests as a New Network Card!

Split Tunneling -
If you're using a Web Browser to go to a website, if you're on VPN, your Packet is sent
Your Computer → Internet → Office → Internet → Office → Internet → Your Computer

## Internet of Things (IoT)

**- Internet of Things (IoT) means giving Internet capability to devices not traditionally associated with the Internet**
**- The most common IoT connections are 802.11, Zigbee, and Z-Wave**
**- IoT requires a hub to link to the IoT devices**
**- Google Home, Amazon Alexa, and Apple Siri add voice capabilities to IoT**

IoT (Internet of Things) - refers to things that we'd never imagined would have internet connection (Light Bulbs, Refrigerators, Doorbells, Garage Door Openers, etc)

Light Bulb in Mike's hand has a Microprocessor, Address, API (to do certain things)

These need to be Wireless and 802.11 is the method we talk to these things

Zigbee - designed for Home Automation Runs on the 2.4 GHz Band
Doesn't need a lot of Bandwidth,
because we're just trying to tell something to Turn On/Off

Z-Wave - 900 MHz Band Used to be used for Portable Phones

For IoT, you need a Hub (Philips Hub, Google Home, etc
Act as Primary Hub for the IoT in our Homes

These Hubs need to be configured

These Home Automation tools become even more fun with Voice tools!

## Troubleshooting Internet Connections

**- Network troubleshooting, check physical connectivity first**
**- Run ipconfig /al| from the CLI to get a ton of network information**
**- Run traceroute/tracert to test Internet connectivity (before you have problems)**
**- Run ping to test connection between two systems (plus DNS)**

Understand how Networks work
Go with a couple of rules that always work for Mike!

Rule 1 - Don’t let the Physical get you down
If you think there’s a problem with your Physical Network,
always check that first!!

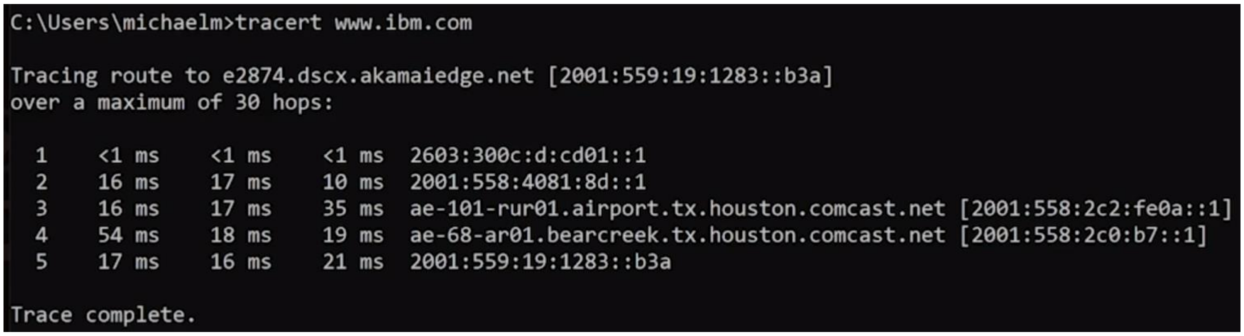
Check your Link Lights
Look at the Lower Right Corner (Windows Notification Area)
or Upper Right Corner on a Linux or Mac
and check for connection

Know your Network! (ipconfig /all)
Network ID Router DNS Server
These are MUST knows even before a problem!!!!
Write them down!

Know your Internet Connectivity!
A lot of places will have 2 or 3 Routers before we get out to the Internet.

Traceroute - run it when everything is good, so you know
what it’s supposed to look like, then if something’s bad,
you can deal with it

Windows: tracert Linux/Mac: traceroute



```
C:\Users\michaelm>tracert www.ibm.com

Tracing route to e2874.dscx.akamaiedge.net [2001:559:19:1283::b3a]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2603:300c:d:cd01::1
  2    16 ms    17 ms    10 ms  2001:558:4081:8d::1
  3    16 ms    17 ms    35 ms  ae-101-rur01.airport.tx.houston.comcast.net [2001:558:2c2:fe0a::1]
  4    54 ms    18 ms    19 ms  ae-68-ar01.bearcreek.tx.houston.comcast.net [2001:558:2c0:b7::1]
  5    17 ms    16 ms    21 ms  2001:559:19:1283::b3a

Trace complete.
```

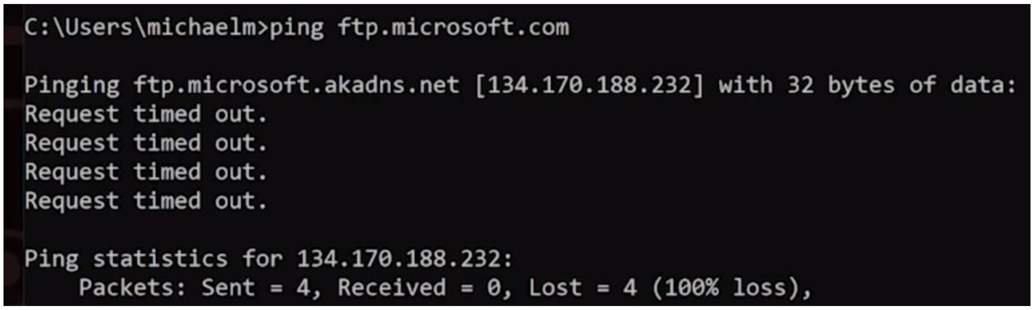
tracert www.ibm.com
1st IPv6 - Internal Router
2nd IPv6 - Default Gateway (Router)
Followed by other connections

Know all of your Routers to get out to the Internet!

Asterisk are Routers that are designed not to respond back
and will show Request timed out.
This is ok!! All we want to know are the Routers to go Out to the Internet

If the Internet goes down, and it’s one of your Routers,
then it’s your problem!

Ping - Ping your Router Amazing tool when used properly!!
ping 192.168.4.1
If you get a reply, you automatically know you have a good IP Address
and you know the Router is responding, so it’s probably up and running.



```
C:\Users\michaelm>ping ftp.microsoft.com

Pinging ftp.microsoft.akadns.net [134.170.188.232] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 134.170.188.232:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ping ftp.microsoft.com ping www.ibm.com
We get timed out. But, we also get a IP Address!!!
This is the Best way to see if your DNS Server is Working!

Mike fixes 95% of Network Problems with Ping, TraceRT, and ipconfig