NICs and MAC Addresses

In our last, and quite lengthy first part, we discussed at length about networks, various ways to connect to one and the various forms a network can take. Now the question still remains as to what parts in a computer, phone, tablet etc. are needed to connect them to a network and the internet. The answer is a **Network Interface Controller** (otherwise known as a NIC).

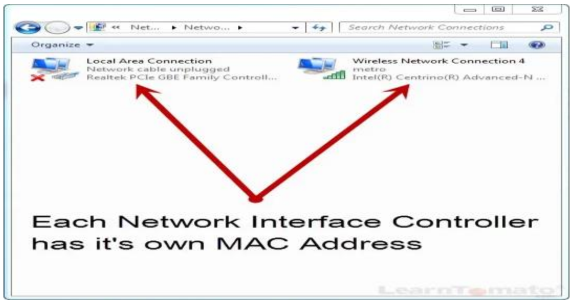
Image source: https://www.reichelt.com/de/en/network-interface-card-pci-10-100-1000-mbit-s-intel-pro-1000gt-p69228.html

A NIC, aka (**network adapter**, **LAN adapter** or **physical network interface…** yes there's a lot of names for this thing) is a computer hardware part that is required to install in a computational device in order to have the device begin communicating with networks. This is the component in your computer that keeps it from being just a simple hunk of metallic parts where you can write word documents. This is the sole component that is responsible for your device reaching out to establish a connection with a network and the internet.

Now another method that helps us to identify our devices on a network is an IP address which was discussed in part one. But how does an IP address work hand-in-hand with a NIC in order for us to connect to any network or the internet? Well first the IP address is given to your computer via a router, but what happens next? The IP address is then statically or dynamically assigned and associated with the NIC by way of using the NIC's MAC Address (Media Access Control).

A MAC Address is the **physical hardware identifier** of the Network Interface Controller. The IP address is only a **logical network address** of the device; meaning that while the IP address can change, a MAC address cannot change at all. A MAC address is always and permanently tied to a network device as it is plastered and embedded physically on the NIC. **Every hardware device that connects to the Internet has a unique identifier known as a MAC address.**

One important question you might ask yourself at this point is how many NICs have a MAC address? Or how many NICs and MAC addresses can I have in my device? On wireless devices such as tablets and smartphones, there is usually only one NIC with one MAC address attached to it. But the case may be different for desktop computers and laptops. For you see, these computers usually have more than just a wireless way to connect to a network or the internet; these devices can include an ethernet port on them allowing them to connect to the internet via a wired connection.



Local Area Connection
Network cable unplugged
Realtek PCIe GBE Family Controll...

Wireless Network Connection 4
metro
Intel(R) Centrino(R) Advanced-N ...

Each Network Interface Controller has it's own MAC Address

Image Source: https://learntomato.flashrouters.com/what-is-a-mac-address-how-to-find-my-mac-address/

So usually for computers with both wired and wireless connecting capabilities, there are NICs for both connection methods and MAC addresses for each of those respective NICs.

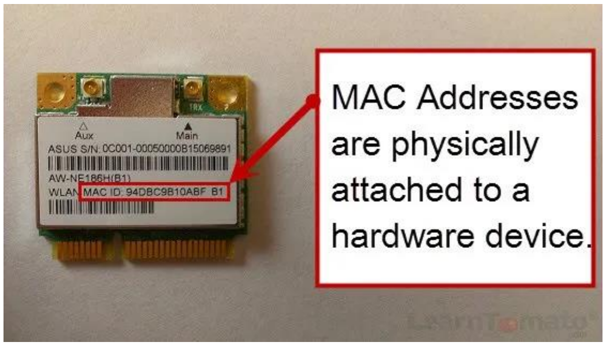

Aux
Main
ASUS S/N: 0C001-00050000B15069891
AW-NE186H(B1)
WLAN MAC ID: 94DBC9B10ABF B1
TRX
MAC Addresses are physically attached to a hardware device.
LearnTomato

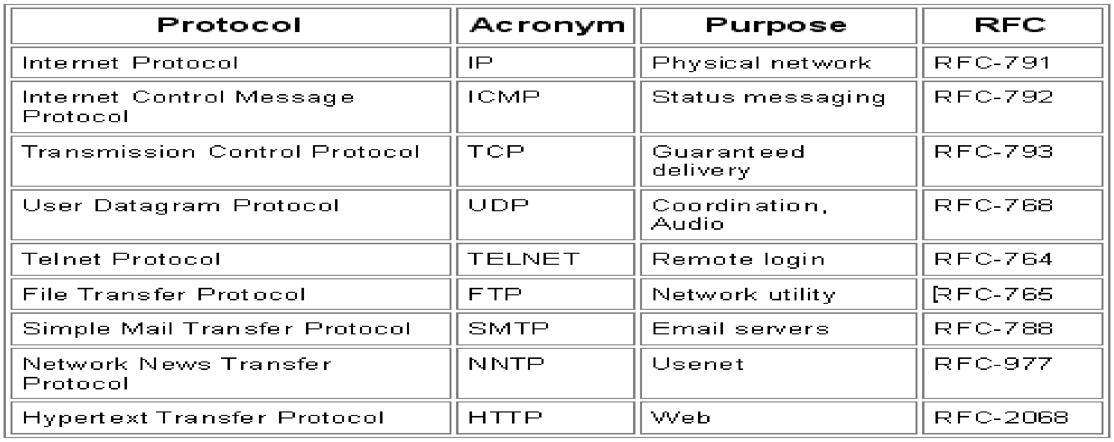
Image source: https://learntomato.flashrouters.com/what-is-a-mac-address-how-to-find-my-mac-address/

Now how does a MAC address work in tandem with an IP address to give you a connection? Well if an IP address is a logical address meant to represent your device on the network, then the MAC address on your device is an address telling your router **where** to send the data. It's almost like going to an auction if you think about it. You want the data from the router and the router is willing to give it to you, as long as your device provides an IP address as proof of who **you** (your device) is and where to send it (the MAC address). It's almost like your router is saying, "I got data for device 192.168.0.32" and your device responds by telling it "Yes I am device 192.168.0.32. Please send that data to my MAC Address. My MAC Address is the following…"

This exchange between a router and device in which a device is trying to acquire data from a router by giving its MAC and IP Address is called an **Address Resolution Protocol (aka ARP).** Now I bet you might be wondering: "what is a protocol?" Well, that leads us into our next discussion topic of Protocols and Ports.

Protocols, Layers & Ports

A "**protocol**" in networking terms, is described by CompTIA as "an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure, or design." Whenever you use your device to use the internet or your currently connected network, your device is using protocols whether you are aware of it or not. An old analogy I used in part one was a bouncer letting you into the club that is what we call "the internet". Well, if the club that you get into is the internet, then protocols are your way of communicating and talking with the people in that gigantic club. You may have different ways of talking to different people at a club and as such your device uses different protocols to get you (the user) what you need from the internet.

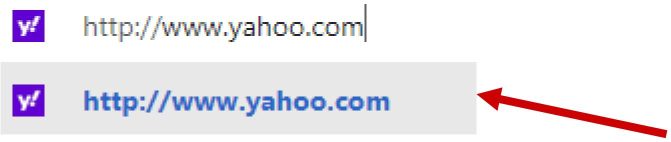


Protocol	Acronym	Purpose	RFC
Internet Protocol	IP	Physical network	RFC-791
Internet Control Message Protocol	ICMP	Status messaging	RFC-792
Transmission Control Protocol	TCP	Guaranteed delivery	RFC-793
User Datagram Protocol	UDP	Coordination, Audio	RFC-768
Telnet Protocol	TELNET	Remote login	RFC-764
File Transfer Protocol	FTP	Network utility	RFC-765
Simple Mail Transfer Protocol	SMTP	Email servers	RFC-788
Network News Transfer Protocol	NNTP	Usenet	RFC-977
Hypertext Transfer Protocol	HTTP	Web	RFC-2068

Image Source: https://medium.com/@sadatnazrul/intro-to-computer-networking-and-internet-protocols-8f03710ca409

There’s a network protocol for almost every action you make with your device when getting the data you want. Even your “**IP**” address that’s used to identify your device on a network stands for “**I**nternet **P**rotocol”.

Another example of a network protocol that you may already recognize is the Hypertext Transfer Protocol (aka HTTP or http). If you have used a web browser before you may recognize this protocol when visiting websites on an internet browser like google chrome or internet explorer by having to type “http” into your browser’s search bar before entering the “www.” before the name of a website.



http://www.yahoo.com

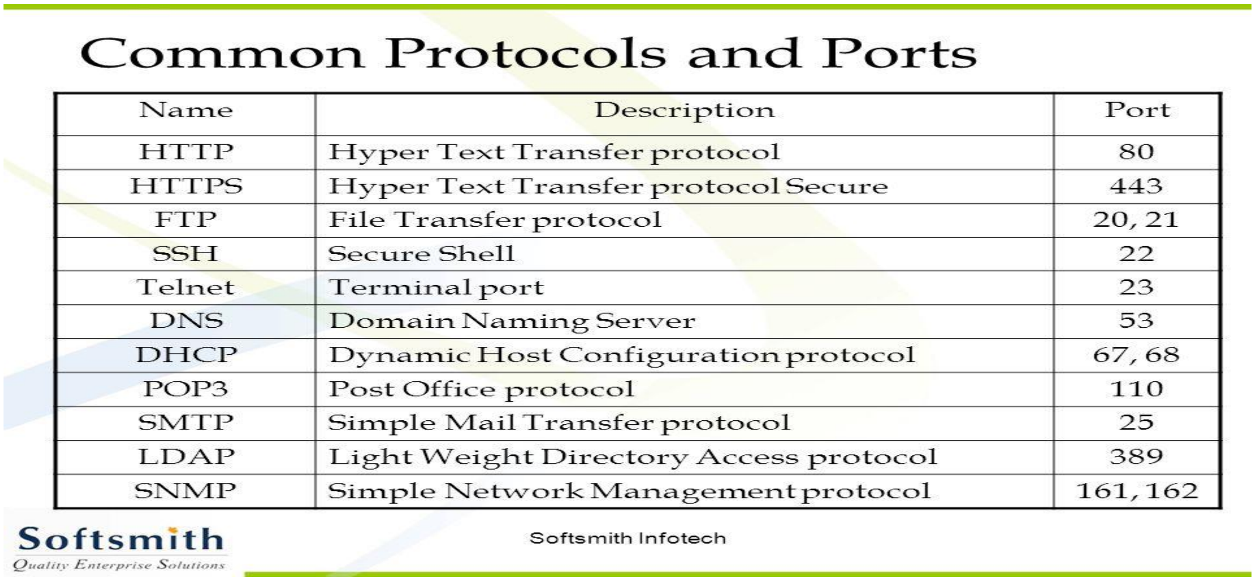
http://www.yahoo.com

The HTTP protocol is known as the protocol that is used by devices to access “distributed, collaborative, hypermedia information systems”. Otherwise known as websites.

Now these network protocols operate and run on different **layers of the network**. Now to save time, I will direct you to this very helpful article written by Syed Sadat Nazrul that describes how network protocols function on these “layers” in any given network. While this reading is not completely required, it will help give you a better and more deeper context and understanding of how these protocols transfer data from your device to others and vice versa using “network layers”.

Now with these many protocols running at the same time on your device, you may be wondering how your computer, phone or tablet is able to keep track of all these incoming and outgoing signals being transmitted using these protocols. The answer is that your device keeps track of these protocols by assigning a numbered value to each one. This is called a **network “port”** (not to be confused with a **physical port** that’s on your device such as a USB Port for example). According to TechTarget, a network port is described as “ …a software-defined number associated to a network protocol that receives or transmits communication for a specific service.” So for each network protocol that exists and is being used by your device, there’s a port number associated with that protocol.

Now there are a lot of network ports that your device can use; in fact there are upwards of 65,535 network ports that any device can use. However, the most common protocols have reserved ports that they run on.



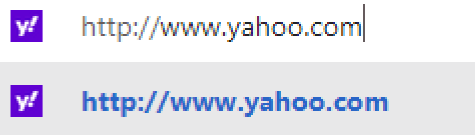
Common Protocols and Ports

Name	Description	Port
HTTP	Hyper Text Transfer protocol	80
HTTPS	Hyper Text Transfer protocol Secure	443
FTP	File Transfer protocol	20, 21
SSH	Secure Shell	22
Telnet	Terminal port	23
DNS	Domain Naming Server	53
DHCP	Dynamic Host Configuration protocol	67, 68
POP3	Post Office protocol	110
SMTP	Simple Mail Transfer protocol	25
LDAP	Light Weight Directory Access protocol	389
SNMP	Simple Network Management protocol	161, 162

Image Source: https://slideplayer.com/slide/6198981/

Let's go back to talking about our good ol HTTP for this example. On your device, when you are using the internet to use yahoo.com which is accessed by your device using HTTP, your device will retrieve yahoo.com via port 80 and display it for you to use on your device. And any other service or website that runs on HTTP will be retrieved by a server and shown on your device using HTTP. Now, you may notice that there is another similar protocol to HTTP that runs on a different port; this being HTTPS (Hypertext Transfer Protocol Secure) on port 443. This protocol operates the same way as HTTP by retrieving websites for you to access and use however you please but the only difference is that websites that are retrieved and sent to you using HTTPS are sent to you more securely by encrypting your internet traffic. Meaning that any website you visit that runs on HTTPS will not be easily known by bots, hackers that might be snooping or listening in on your internet traffic. To demonstrate this, let's look back at our yahoo.com example from earlier.

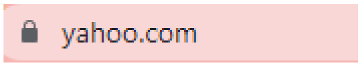
Http is typed into a chrome search bar to access yahoo.com. But after pressing enter to search for it,



http://www.yahoo.com

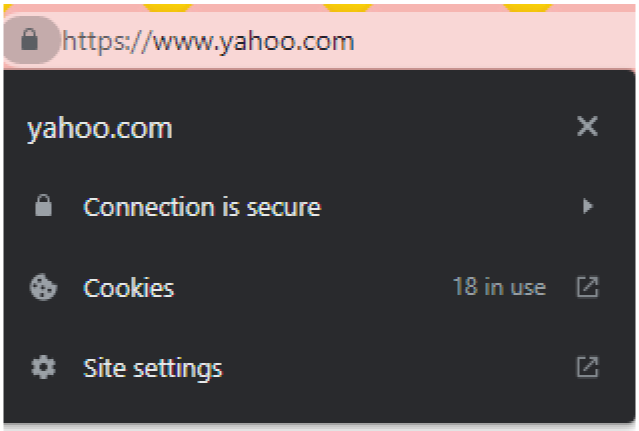
http://www.yahoo.com

Yahoo.com appears! But wait, in the chrome search bar, I see a lock icon right next to "yahoo.com" let me click on it to see what happens.



yahoo.com

When I click on the lock icon in my chrome search bar, this tiny window mentions that my "connection is secure". This is a clear indication that I was shown Yahoo.com and that it was retrieved to be shown on my computer using HTTPS on port 443. How you may ask? I will show you how.



https://www.yahoo.com

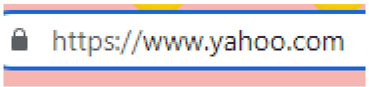
yahoo.com

Connection is secure

Cookies 18 in use

Site settings

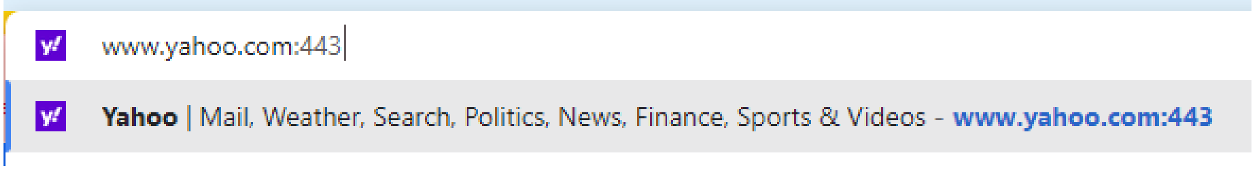
When I double click on the chrome search bar, as if to type something in, I see the true web URL of yahoo.com. It looks like HTTPS was retrieved using HTTPS instead of HTTP.



https://www.yahoo.com

A good sign of knowing immediately if the website you are visiting is using HTTP or HTTPS is to just remember that websites that were retrieved using HTTPS have a lock icon next to the website's URL in the search bar.

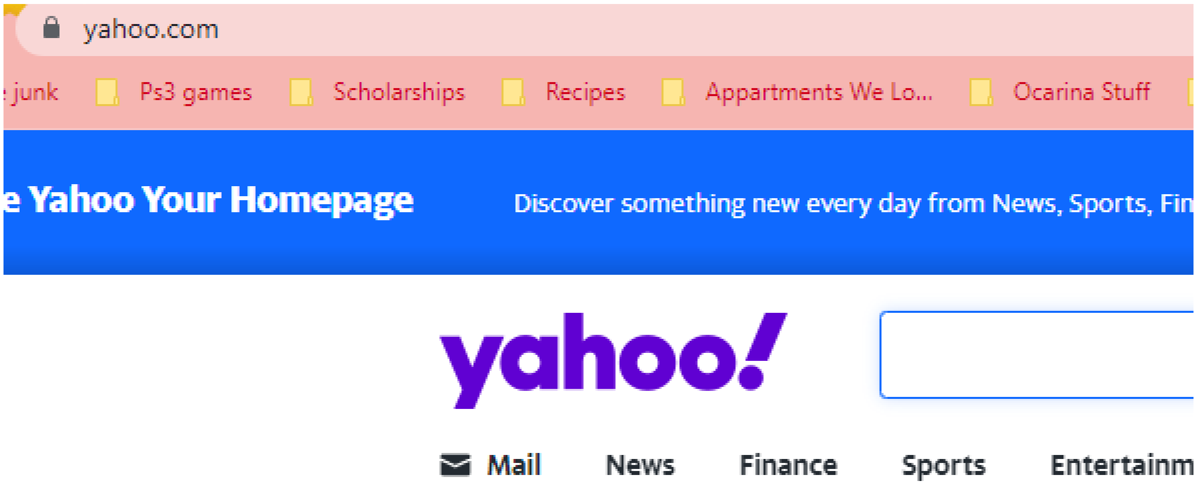
Another good way to REALLY tell that the website is being retrieved and sent to your device using HTTPS (aka port 443) is typing the website you want to visit in the search bar such as "www.yahoo.com" and while you could leave it as just that, you can add on ":443" at the end. In this example below, I did just that, and after I pressed the Enter button….



www.yahoo.com:443

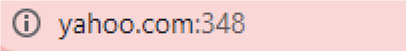
Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos - **www.yahoo.com:443**

Yahoo.com loaded and came up exactly like how it usually does!



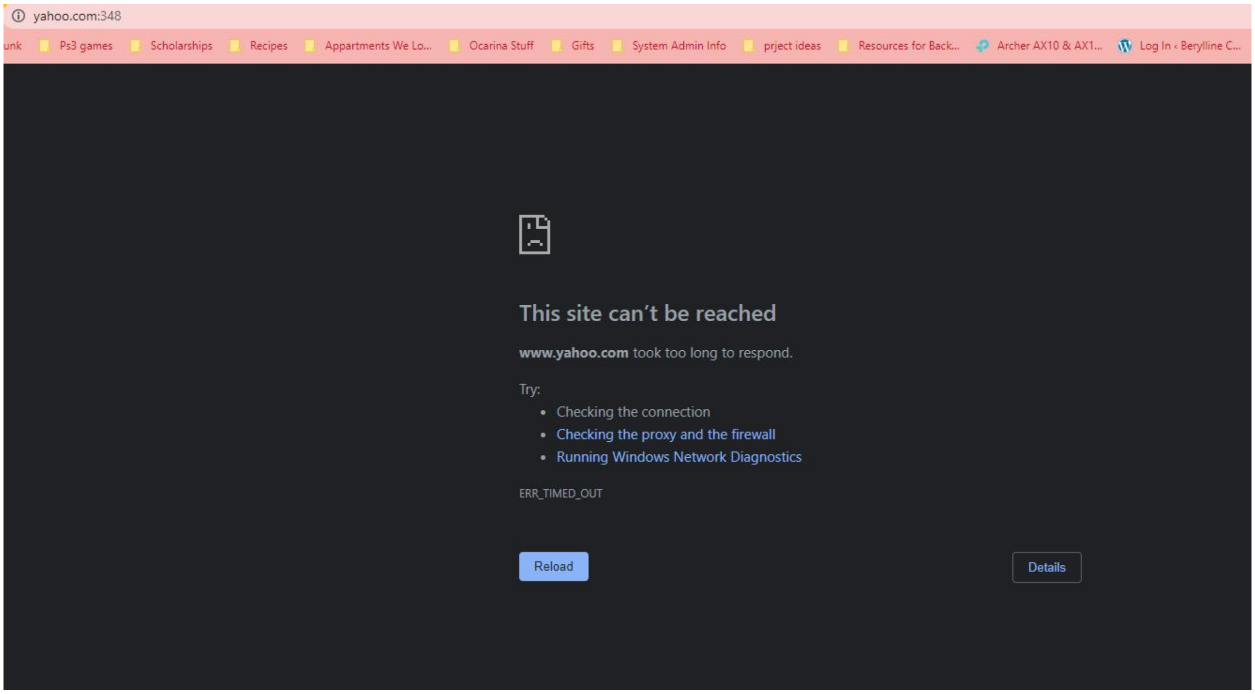
yahoo.com

Now if I type in some random, unused port number at the end such as "www.yahoo.com:348" …



yahoo.com:348

Yahoo.com will not load since I am trying to retrieve yahoo.com, a website, using a port that has no protocol that can retrieve it.



yahoo.com:348

This site can't be reached

www.yahoo.com took too long to respond.

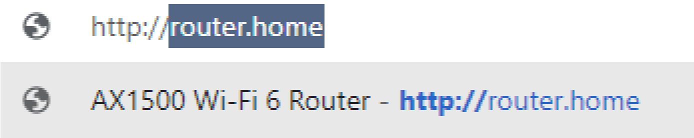
Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_TIMED_OUT

Now as for HTTP, it is still a protocol that is used today to retrieve websites using your browser, but not nearly as much as HTTPS since it does not ensure security/encryption.

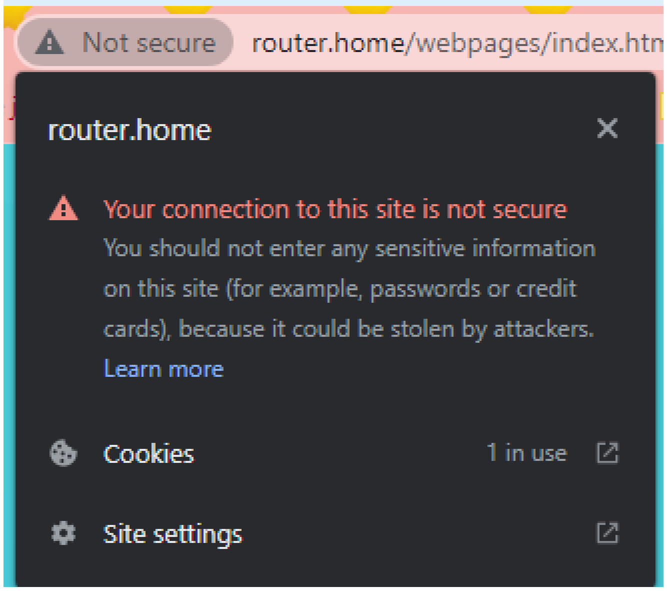
Any sites that were retrieved using port 80 (aka HTTP)…..



http://router.home

AX1500 Wi-Fi 6 Router - **http://**router.home

This will have a website showing up like normal. However, since HTTP is being used and not HTTPS, no secure lock icon will appear next to the website's URL in your web browser search bar. Instead of that, when using HTTP to retrieve a website, this "Not secure" icon will show up.



Not secure router.home/webpages/index.htm

router.home

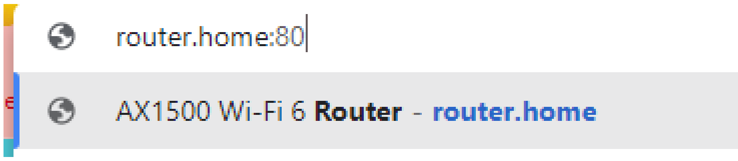
Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Cookies 1 in use

Site settings

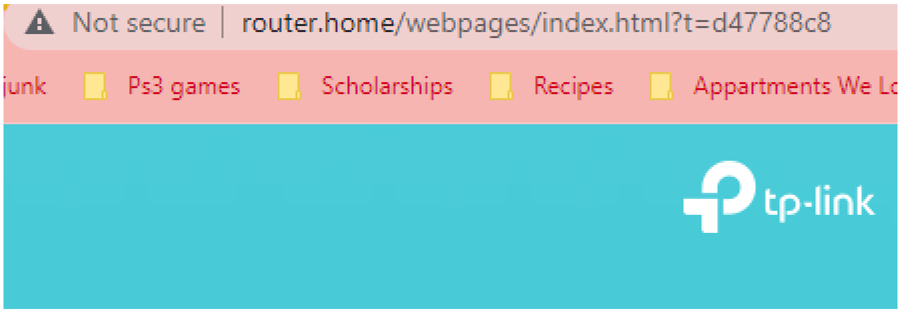
And to make doubly sure that this website is using HTTP, I will enter the port number ":80" at the end of the website to see if it will load and show up normally.



router.home:80

AX1500 Wi-Fi 6 **Router** - **router.home**

And it looks like this website is loading normally even after searching for it by specifying the port number "80" at the end of this website's URL.



Not secure | router.home/webpages/index.html?t=d47788c8

Firewalls

Our next topic of discussion is about firewalls. Now even if you don't know much about computers, you may have heard the term "firewall" be used before in conversation when someone is talking about the safety of your computer or your network. That is because firewalls are one of the most essential tools at our disposal to keeping both our devices and our network safe from the greater bigger landscape of the internet. I encourage you all to watch this short 6 minute video on Youtube made by PowerCert Animated Videos that details what a firewall is, how it works, how it protects your device and network and all of the different types of firewalls there are. It is a short and concise video that includes terms that we have previously learned in this Introductory series of articles.

In part three, we will go over what we’ve all been waiting for. VPNs! And most of the common threats and attacks that anyone ANYONE can encounter when browsing the internet.