0. Contents

1. Layer 1 : Physical

Layer 1, the Physical Layer

This layer deals with the hardware of networks such as cabling. It defines the mechanical and electrical standards of interface devices and the types of cables used to transmit digital signals (e.g. optical fiber, coaxial cable, wireless, etc.).

The major protocols used by this layer include Bluetooth, PON, OTN, DSL, IEEE.802.11, IEEE.802.3, L431 and TIA 449.

Latency is the term used to describe the total time it takes a data packet to travel from one node to another. This is often measured in milliseconds (ms). The greater the latency, or "lag," the higher this number will be.

Availability refers to how long the network stays up and operational without interruption, and how quickly it can recover should it go down.

Bandwidth refers to the maximum amount of data that can be transmitted over a medium in a given time.

Throughput refers to the actual amount of data that is transmitted over a medium in a given time.

1.1. Telephony

A TCP/IP network transmits data to the desired recipient using packet switching. To accomplish this, each packet of information has a source and destination address. A router is responsible for analyzing the packet header information and directing the packet based on pre-configured tables.

Frame Relay Line

ATM (Asynchronus Transfer Mode)

MPLS (Multiprotocol Label Switching)

CSU / DSU : converts LAN data to WAN data

Patch Panel

110 Block

1.1.1. SONET

SONET : Synchronus optical Networking. These are the optical equivalents of T1 lines and are called OC-Lines. The signal types (basically just the frame type) used in these lines is called STS. Each consequtive line is essentially a mutiple of 52 making the following table a lot easier to remember.

OC-1 : 51.85 Mbps : STS-1 OC-3 : 155.52 Mbps : STS-3 OC-12 : 622.08 Mbps : STS-12 OC-24 : 1.244 Gbps : STS-24 OC-48 : 2.488 Gbps : STS-48 OC-192 :

9.955 Gbps : STS-192 OC-256 : 13.22 Gbps : STS-256 OC-768 : 39.82 Gbps : STS-768

DWDM

1.1.2. Trunk Lines

analog signal

digital signal

fdm (frequency division multiplexing) : Origianl telephone systems used frequency division multiplexing , today they use time division multiplexing.

tdm (time division multiplexing)

DS0 Signal

DS1 Signal : A DS1 Signal is 24 DS0 signals all going down the same wire.

DS3 Signal :

T1 Cable Line : 24 channels , 1.544 Mbps T3 Cable Line : 672 Channels , 44.736 Mbps E1 Cable Line : 32 , 2.048 Mbps E3 Cable Line : 512 , 34.368 Mbps

T1 Crossover

PSTN (Public Switched Telephone Network)

Dial-Up : Provided by telephone lines. To connect to the internet , you would get a connection line through your dial-up ISP. This means that the ISP would give you a telephone number , username and password. You call this telephone number from your modem through your computer. Dial-up uses the PPP protocol. Be careful when thinking about the timeline though , cause dial-up refers to the phone line which came about decades before dial-up networking.

BPL (Broadband over power line) : This is basically a technology that uses power lines to deliver internet in addition to electricity. Not very successful in terms of implementation and is rare to find. The main problem was the huge amount of interference due to electricity while running on the same line. This was in addition to the danger of having to make patches and stuff cause the wire was carrying not only a signal but also live current.

1.1.3. ISDN

ISDN (Integrated Service Digital Network) : Came up before dial-up networking and provided either 64Kbps or 128 Kbps speeds. These used ISDN phones , and you would also get a ISDN adapter that you would plug into to be able to get connected.

1.1.4. PBX

1.1.5. VoIP

RTP STRP RDP Kubernetes

RTP : udp 5004 / udp 5005 RTSP SIP : tcp 5060 / 5061 H.323 : tcp 1720 MGCP : 2427 / 2727 , Media Gateway Control Protocol

1.2. 802.3 : Ethernet

POE : Power over Ethernet . Back in the day you would need to give WAPs two seperate sets of input. One would be the ethernet input , the other would be power input so that the device had electricity to function. Today we can provide power over the ethernet cable itself. This is called POE. This is used in difficult to power areas. It is commonly used with phones, wireless access points and cameras. The power is usually comming directly from the switch that the ethernet cable is plugged into. This is called an endspan. If the switch does not provide power , then a power injector is installed in the middle. This type of connection is called a Midspan.

802.3af , PoE : 15.4 watts 802.3at , PoE+ : 30 watts

EOP : ethernet over power is the reverse of POE. This allows us to extend our ethernet network using the power cables that we already have in our homes. This is also called PLC (Power line communication). These types of connections can deliver 500 Mbps. Commonly only devices that are not traditionally connected to the internet use these connections. An example is electric cars, which can charge and be connected to the internet through EOP.

1.3. 802.11 : Wireless

802.11 is a IEEE Protocol that uses radio waves to transfer network information between different individual wireless nodes.

Wireless Bridge : A normal bridge is one that joins two networks so that they can work together as one larger network. A Wireless bridge does the same with wireless networks. There can be more than one type of wireless bridge however :

- Wi-Fi to Ethernet Bridge : Usually WAP to Ethernet
- Wi-Fi to Wi-Fi : Joins two wireless networks usually to increase coverage. - Bluetooth to Wi-fi Bridge : Allows connecting to Wi-Fi through bluetooth.

Wi-Fi Repeater Mode is a variation on bridging. Rather than connect seperate netowrks in a way that allows devices in each one to communicate with each other, repeater mode extends the wireless signal of one network to longer distances.

Wireless Range Extenders basically work as Wi-Fi Repeaters.

SSID (Service Set Identifier) : Each WAP has a word or a phrase that is used to help wireless devices identify and connect to the WAP. These words / phrases are called SSIDs and are typically broadcasted to whoever wants to attempt to connect to them.

BSSID (Basic Service Set Identifier) ESSID (Ex-

tended Service Set Identifier)

Infrastructure Mode

Ad Hoc Mode

Wireless Bands : A band is a range of frequencies across the electromagnetic spectrum. Basically the electromagnetic spectrum (radio , micro, infrared , visiable , ultravoilet , x-rays , gamma rays) is first chopped up according to wavelength. Then within each wavelenth people decide to further break up the spectrum into smaller ranges called bands. So different technologies with different ranges , power needs , applications etc ... will use different bands in different wavelengths throughout the EM Spectrum.

Wireless Channel : Which in turn are broken again into smaller units called channels.So channels are individual , smaller sections of the overall frequency band used by a wireless network. The width of the these channels is usually measure in MHz and is called the channel width. Channel also have something called a channel buffer , which is a empty frequency space put around channels widths in a band since radiowaves are imperfect and we want to allow for some fluctuations without overlap. Each channel is marked using the center of the channel width. As an example if we have a channel in the 2.4Ghz band going from 2.4Ghz to 2.42Ghz , with channel width 22MHz , we have channel midpoints : 2.412 , 2.437 , 2.462. These 3 channels in the 2.4 band are called channels 1 , 3 and 7. These are the conly channels we can have without overlap.

ISM Bands : All 802.11 networks are designed to run in the industrial , scientific and medical bands. These are portions of the radio spectrum that are reserved internationally for telecommunication communication purposes. Although for 802.11 these days we will primarily only deal with 2 bands : 2.4/5.0GHz. This means that these 2.4Ghz and 5.0Ghz are the starting points for the bands that these technologies use. So the 2.4Ghz band will use 2.40Ghz to roughly 2.5Ghz as its band range and within this band we will have multiple channels specified in MHz. Disributing the number and size of a channel usually depends on the regulatory commitee in specific countries.

CSMA / CA : When we try to get two machines to communicate with each other using wireless radio waves , we very quickly will run into a problem. The problem being that what if multiple devices are talking on the same channel. This causes interference , and is very similar to the early days of the ethernet where the NICs would detect collisions on the wired networks before we had switches. The wireless solution to this is called Carrier Sense Multiple Access Collision Avoidance or CSMA / CA. Do not confuse this with CSMA / CD which is the wired ethernet equivalent. CSMA will basically only allow communications between a client and a server to take place as long as the coast is clear. This ensures that there are never any collisions because they avoid each other and do not even try to communicate until a channel is open and free.

DSSS (Digital-sequence spread-spectrum) :

OFDM (Orthogonal frquency-division multiplexing)

Wireless Controller : When we have several WAPs working together , we do not want to go and configure each one individually. In this case we use a device called a wireless controller which allows us to configure all of the WAPs at the same time by propogating out the changes to all the devices.

1.3.1. Antennas

Omni Antenna

Dipole Antenna

Directional Antenna / Yagi Antenna

Parabolic Antenna

SMA Connector

Antenna Gain : Measured in dBi

1.3.2. 802.11 Coverage

Reflection : This is when the radio waves are bounding off the surface and travelling in roughly the opposite direction of what they came in. If we have rooms / offices behind materials like metal walls , then the radio waves will get strondly reflected by the wall and it would be difficult for them to connect.

Refraction : In opposition to reflection , refraction bends the radio waves only a little bit such that their trajectory changes. Certain materials like glass walls can cause the radio waves to bend in another direction than the one in which they were intially intended to travel. This can be used to our advantage however.

Absorbtion : Biggest problem that most people have to face is absorbtion. The radio waves are just straight up absorbed by the material and not reflected or refracted. This is most often the problem with thick concrete walls.

Attenuation : The radio waves weakening over a certain distance is called attenuation.

Interference , reflections , and absobtion are all environmental issues that can affect the signal. Another thing to keep in mind is the bandwidth and to use channels with the least amount of congestion.

Jitter : Choppy / Laggy overall performance as a result of the frames on the wireless network arriving at different speeds. This can be bcause one frame was on a wave that got reflected , another frame was on a wave that got refracted / absorbed etc ....

SNR Ratio / Signal-to-Noise Ratio :

Mesh Networks :

1.3.3. Wireless Access Points

802.11a	54Mbps	5.0GHz	20MHz	OFDM	
802.11b	11Mbps	2.4GHz	22MHz	DSSS	
802.11g	54Mbps	2.4GHz	20MHz	OFDM	
802.11n	108 - 300Mbps	2.4/5.0GHz	20MHz/40MHz	OFDM	MIMO
802.11ac	1Gbps +	5.0GHz	160MHz	OFDM	MU-MIMO

Figure 1: 802.11 Extension Evolution

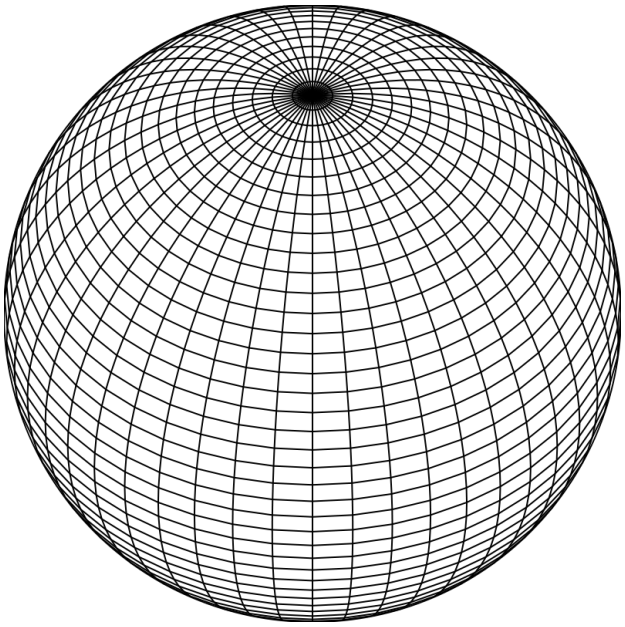

Figure 2: Omnipole Antenna Pattern.

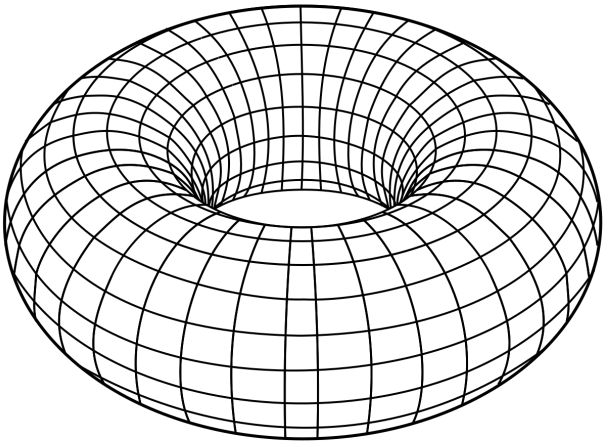

Figure 3: Dipole Antenna Pattern.

WAP : A hub for wireless devices (where we would use a switch / normal hub for wired connections) , usually has incoming data from ethernet that is transformed into wireless data by a router ? The router then sends this data to the WAP , which then sends the data wirelessly to your computer. Wireless access points are usually used by large companies / universities etc... to enusre theat there is coverage everywhere. You can achieve the same result using routers everywhere instead of wireless access points , but the problem with this setup is manageability. This is becuase if there are any settings that need changing then , you would have to log into every single router individually to make that change. Whereas if you have multiple WAPs and one router the entire thing is treated as one single subnet as opposed to multiple different subnets , so we would need to make only one change. Another difference between a router and a WAP is that routers can take both wired and wireless connections , whereas a WAP can take only wireless connections. This is because routers have a built in ethernet switch. Routers also have a firewall , whereas WAPs do not have a firewall. Routers also have a built in DHCP service, which dynamically assigns IP addresses to devices that are connected to that router. Routers also have a WAN port , where the cable from the modem will go. This gives the router an internet connection which is then passed on to the other devices. Whereas a WAP only has an ethernet port and no WAN port.

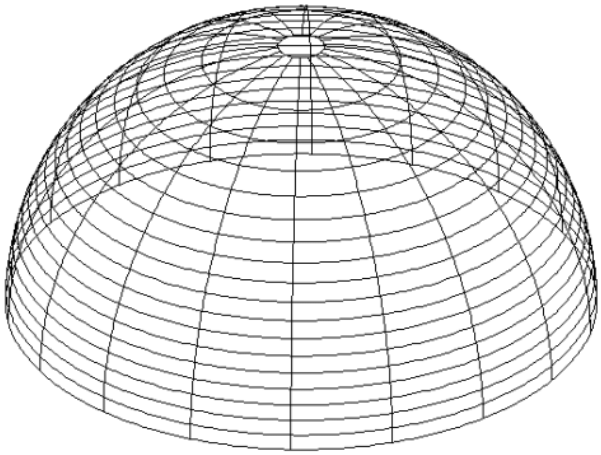

Figure 4: Patch Antenna Pattern.

Strictly speaking, access points are a L2 device. Their primary function is to bridge 802.11 WLAN traffic to 802.3 Ethernet traffic.

However, in the real world, enterprise wireless vendors often push more functionality to either the AP itself and/or tie them into a controller, with the end result that they often incorporate functionality from higher layers as well.

yes, an AP (or any bridge) needs to keep track of which interface any individual device is connected. In general (and simply), they work on the principle of frames destined to an associated station gets forwarded out the wireless interface and any other frames get forwarded

out the wired interface (or sent to the controller).

1.3.4. WEP

- WEP (Wired Equivalent Privacy)—this is an older standard. WEP is flawed and you would only select this if compatibility with legacy devices and software is imperative.

TKIP

WEP (Wired Equivalent Privacy) : Developed in 1999 , it was the first wireless security protocol , and as the name implies the creators intended to have the same degree of security as we could achieve in a wired network. That fell flat pretty quickly because it was found that the encryption key that WEP used was sent in the clear.

Initialization Vector

1.3.5. WPS

Wi-Fi Protected Setup (WPS) allows the router to use an auto-generated SSID and encryption key, and for these to be communicated to the client without the user having to enter them manually.

WPS (Wifi Protected Setup) : This usually manifests iteself in the form of a button on some wireless device (printer , game controller , etc . . .) and it allows for push button configuration of a wireless network connectivity. All you have to do is hit the WPS button on the target device , then within about 60 seconds hit the WPS button on your router / WAP , and the two devices will configure themselves to work together using WPA2-AES. Pretty much every device nowdays is WPS-enabled. Anothed connection method is the pin number. Every WPS device that has a PIN number that you can type into your computer to connect. The problem is that WPS is vulnerable to a number of hacks including a straightforward brute force and should be turned off wherever possible.

1.3.6. WPA

- Wi-Fi Protected Access (WPA)—this fixes most of the security problems with WEP. WPA uses the same weak RC4 (Rivest Cipher) cipher as WEP but adds a mechanism called the Temporal Key Integrity Protocol (TKIP) to make it stronger.

- WPA2—this implements the 802.11i WLAN security standard. The main difference to WPA is the use of the AES (Advanced Encryption Standard) cipher for encryption. AES is much stronger than RC4/TKIP. The only reason not to use WPA2 is if it is not supported by devices on the network. In many cases, devices that can support WPA can be made compatible with WPA2 with a firmware or driver upgrade.

Wi-Fi Protected Access (WPA) does not automatically generate an SSID and encryption keys. It uses the same weak cipher as the outdated Wired Equivalent Privacy (WEP), but adds a mechanism called the Temporal Key Integrity Protocol (TKIP) to make it stronger.

Temporal Key Integrity Protocol (TKIP) is part of the WPA standard and is not a wireless protocol in itself.

Advanced Encryption Standard (AES) is a cipher for encryption. AES is part of the WPA2 standard, but not a wireless protocol in itself.

WPA + TKIP (Temporal Key Integrity Protocol) : When eveyone knew that WEP was trash people started rabbling. They wanted a better security protocol to use in wireless networks so the internet guys said no problem , we got. We got this new and shiny 802.11i standard that will fix all your problems. When is out ? I like 4 years. If you are cisco or netgear or some other company that is providing 802.11 services now , you are not going to sit and wait around half a decade for this fix. So they invented WPA. This protocol had better encryption than WEP using TKIP (Temporary Key Intergrity Protocol). TKIP dynamically changes its keys as it is being used.

WPA + AES (WPA2) : While the internet guys were still busy working away at 802.11i , the industry released WPA2. This protocol used even stronger encryption than WPA. This was done using a stronger encryption standard called CCMP-AES (or just AES for short). This encryption method was so strong that even the U.S government adopted it and was using it for sensitive government data.

WPA-Mixed Mode : Some routers today allow both WPA and WPA2 to work together. Which means that we will be using TKIP and AES encryption. The only reason to use this is for compatability purposes where some older devices still might not be using only WPA2.

WPA-PSK (Pre Shared Key)

CCMP-AES

802.11i

1.3.7. EAP / 802.1X

EAP : Enables Flexible authentication. EAP-PSK (Pre-Shared Key) PEAP (Protected Extensible Authentication Protocol) EAP-MD5 EAP-TLS EAP-TTLS

1.3.8. Access Control Lists (ACL)

MAC Filter : You can filter devices based on their MAC addresess. This is done using a form of an access control list similar to what you would use in a firewall.

1.3.9. Users

Rogue AP / Evil Twin : When someone plugs in an additional unauthorized WAP to our wired network it is called an evil twin or a rogue AP. This can happen for a number of reasons. Bob over in sales could think , I'm not getting a good enough signal in my office so let me just go buy a SOHO router and plug it in, no need to bother those IT guys. Thi but we have potentially given a hacker unsecured access to our wired network. Fuckin bob, always messing things up. When someone plugs it in accidentally it is called a Rogue Access Point , but when someone intentionally plugs one in and sets the SSID private , it is known as a Evil Twin.

802.11 jammer : An 801.11 jammer can knock evreyone off the network that they are on. The jammer sends a signal on a particular channel on a band , this can cause the devices to not be able to connect to that particular channel, which means they will try another channel which we might just happen to control. Which makes 802.11 jammers excellent tools for MITM (Man in the middle) attacks.

1.4. 802.15.1 : Bluetooth

1.5. Internet of Things (IOT)

1.5.1. ANT+

ANT / ANT+ : 2.4GHz , 30m , 20Kbps Heart rate monitors watches workout equipment

1.5.2. NFC

NFC : Close Range , 1.56MHz , 4cm , 424Kbps

1.5.3. Infrared

Infrared : Line of Sight , 1+m , 1Gbps

1.5.4. RFID

1.5.5. Z-Wave

Z-wave : 900Mhz , 30m , 9600bps

1.5.6. 802.15.4 : Zigbee

Zigbee : 2.4Ghz , 10m , 250Kbps

1.6. Modems

Modulation is on Layer 1. That is where bits are finally transformed into electrical signals, and that is what a modem is doing.

Modem : Modulator Demolulator. Transforms analog data to digital data. A modem recieves incoming traffic and sends it to a local device. If you only have only device on your local network then no more setup is needed. If you have multiple device (which almost everyone does) then the modem would pass this transformed internet traffic to your router. The router will then make the decision of which device on the LAN this internet traffic is actually destined for. Then if needed the router forwards the traffic to a WAP, or directly to the device using 802.xx wifi wirelessly or using ethernet since most routers come with an inbuilt switch. If not then the router would forward this traffic to a switch , which would then send the ethernet traffic to your computers and servers. There are different kinds of modems. The two most common types are cable and DSL modems. Cable modems use coaxial cables and are provided by cable television companies. DSL modems use phone lines and will use RJ-11 cables ? .

Dial up Modem : transforms data coming from telephone lines. Data coming from telephone lines is analog , which needs to changed to digital to be understood by the computer. Simply put it transforms analog data to digital data Max Speed : 56Kbps

1.6.1. 802.3b : Cable

Cable

Where FTTC is offered by providers with origins in the telephone network, a cable Internet connection is usually provided as part of a Cable Access TV (CATV) service. These networks are often described as Hybrid Fiber Coax (HFC) as they combine a fiber optic core network with coax links to customer premises equipment. Coax is another type of copper cable but manufactured in a different way to twisted pair.

The cable modem or modem/router is interfaced to the computer through an Ethernet adapter and to the cable network by a short segment of coax, terminated using an F-connector.

Cable based on the Data Over Cable Service Interface Specification (DOCSIS) version 3.0 supports downlink speeds of up to about 1.2 Gbps. Most service providers packages do not offer those kinds of speeds however, with about 100 Mbps being typical of a premium package at the time of writing.

Broadband is the most common form of internet access. The word "broadband" refers to wide-bandwidth data transmission, which is a fancy way of saying your internet is always connected and doesn't depend on a phone line connection.

There are four main types of broadband internet:

DSL Fiber-optic Cable Satellite

Broadband Internet service truly is the most used form of Internet access because of its high access speeds; it is offered in four different forms, DSL (or Digital Subscriber Line), also fiber-optic, cable, and satellite. The old dial-up connection is the only non-broadband internet service available, and even though it is cheaper,

most Internet users are moving towards the faster broadband Internet connection. DSL

The DSL (or Digital Subscriber Line) internet service makes its connection by utilizing unused telephone wires that cause no interruption to your telephone service. The speed you experience with a DSL connection varies with your distance from the switching station. Your speed will be slower the further away you are and faster the closer you are to the switching station and this may be a deciding factor when you attempt to select between a DSL line and a cable connection. Cable

The broadband cable connection is provided by the local cable TV provider. Here the cable Internet connection speed varies with the number of users on the service at a specific point in time. Given a specific geographical area, users of the broadband cable service share the connection bandwidth which slows the speed the more users are on the system. This will occur at the peak times for example late in the evenings after the work day is over when many people will be accessing the Internet. Somewhat misleadingly, often the cable company would estimate connection speeds that are based on the thinking that you are using the service. But that is clearly not the case.

Fiber-Optic

The newest broadband service is fiber-optic, which is the fastest Internet connection thus far. However, this type of Internet service is still in its infancy as its service areas are quite limited and because the laying down of the fiber-optic cable takes a while to complete. Wherever it is available, the cost not only competes with that of DSL and cable, but it provides a much faster connection than both of those services.

1.6.2. DSL

DSL Filter : Since regular telephones and your internet modem used to be on the same line , there used to be a lot of interference between the two. The DSL filter had one job , and that was to filter out the DSL noise so you could use your phone normally.

VDSL (Very high bit rate DSL)

1.6.3. Satellite

While a cabled Internet service will usually offer the best bandwidth, they are not always available. Wireless services can be used in areas where it is too difficult or expensive to lay cable. Microwave Satellite

Satellite systems provide far bigger areas of coverage than can be achieved using other technologies. The microwave dishes are aligned to orbital satellites that can either relay signals between sites directly or via another satellite. The widespread use of satellite television receivers allows for domestic Internet connectivity services over satellite connections. Satellite services for business are also expanding, especially in rural areas where DSL or cable services are less likely to be available.

Satellite connections experience severe latency problems as the signal has to travel thousands of miles more than terrestrial connections, introducing a delay of 4–5 times what might be expected over a land link.

To create a satellite Internet connection, the ISP installs a satellite dish (antenna) at the customer's premises and aligns it with the orbital satellite. The satellites all orbit the equator, so in the northern hemisphere the dish will be pointing south. The antenna is connected via coaxial cabling to a DVB-S (Digital Video Broadcast Satellite) modem. This can be installed in the PC as an expansion card or as an external box connected via a USB or Ethernet port.

commonly uses rg-6 type cables , and has their own modem that the isp will provide on installation.

Satellite internet

About 23,000 miles above your head right now, there' s a satellite floating around somewhere that can hook you up to the internet.

Unlike fiber or cable, with satellite internet, it doesn' t really matter where you live. So for those of you living in rural communities, satellite internet might be your best option.

You don' t have tons of options when it comes to satellite internet, but you can still get up to 100 Mbps of download speed (though it will likely end up being less than that).

Unlike most wireless technologies (Wi-Fi , Cellular , NFC) Sattelite communications use microwaves instead of radio waves to transmit data.

docsis: data on "cable" (tv) network is sent using the DOCSIS specification . It stands for Data over Cable Interface Specification. Important is to note that we can support voice , video and data in the same connection and therefore having multiple services. Speeds reach from 4 Mbps (bits) to 250 Mbps are common. Gigabit speeds also possible.

DSL / ADSL Modem : Digital subsriber line. It is sometimes also reffered to as ADSL or Asymmetric Digital Subscriber line. This uses telephone lines. It is called asymmetric because the download speeds are much faster then upload speeds. The problem with DSL connections is that there is a maximum distance limitation from the central telecom office to your home / office. The distance is roughly about 10,000 feet (3048m). Common speeds for DSL connections are 52 Mbps down and 16 Mbps upstream. If you get closer to the CO (central office) then faster speeds may be possible. DSL is not combatible with the boosting equipment that TV / Cable companies use , therefore max dist

Digital Subscriber Line (DSL)

Digital Subscriber Line (DSL) is one of the most popular SOHO Internet service types. DSL works over an ordinary telephone line, providing the line is of sufficient quality. The DSL modem/router is connected to the telephone line using a cable with RJ-11 connectors between the WAN port on the router and the telephone point. Data is transferred over the line using the high frequency ranges that voice calls don't need to use. The telephone point is fitted with a microfilter to prevent the data signals interfering with voice calls and vice versa.

Most residential DSL services are asymmetric (ADSL), meaning that the uplink (up to about 1.4 Mbps) is slower than the downlink (up to about 24 Mbps). The speeds achievable are heavily depending on the quality of the telephone wiring and the distance to the local telephone exchange. The maximum supported distance is about three miles.

Your modem serves as a bridge between your local network and the Internet. Historically, the term "modem" is shorthand for modulator-demodulator. Modems were used to modulate the signals on telephone lines so that digital information could be encoded and transmitted over them and then demodulated—and decoded—on the other end. Though more modern broadband connections—like cable and satellite—don't really work the same way, we kept using the term "modem" because it's a device people were already familiar with and associated with connecting to the Internet.

How a modem attaches to your network depends on the type of connection you have. The modem plugs into whatever type of infrastructure you have—cable, telephone, satellite, or fiber—and gives you a standard Ethernet cable output that you can plug into any router (or a single computer) and get an Internet connection.

Since the modem communicates with your Internet service provider, you'll need the correct type of modem that will work with your ISP's infrastructure.

Some ISPs offer a modem and router in a single device. That device has the electronics and software in it to provide both functions, acting as a modem that communicates with your ISP and functioning as a router to create a home network. Some ISPs also bundle a phone interface into the same box so you can use their VOIP offerings.

While a combined unit has its attractions—just having one device cluttering up your office being one—there are also disadvantages. Using separate devices offers more flexibility in what you can do with your network and lets you make sure you're using the best quality devices you can. And using your own devices instead of the ones your ISP provides can save you some money.

dsl connection frequencies

Dry loop connection

SDSL

DOSIS

1.7. Cellular Network

Cellular Radio

Cellular data connections use radio transmissions but at greater range than Wi-Fi. Cellular data is more closely associated with Internet access for cell phones and smartphones than with computers.

That said, a cell phone can share its Internet connection with a computer (tethering), if the computer has no other means of Internet access.

A cellular phone makes a connection using the nearest available transmitter (cell or base station). Each base station has an effective range of up to five miles (eight km). The transmitter connects the phone to the mobile and PSTN networks. Cellular radio works in the 850 and 1900 MHz frequency bands (mostly in the Americas) and the 900 and 1800 MHz bands (rest of the world).

Cellular digital communications standards developed in two competing formats, established in different markets:

- GSM (Global System for Mobile Communication)-based phones. GSM allows subscribers to use a SIM (Subscriber Identity Module) card to use an unlocked handset with their chosen network provider. GSM is adopted internationally and by AT&T and T-Mobile in the US.

- TIA/EIA IS-95 (cdmaOne)-based handsets. With CDMA, the handset is managed by the provider not the SIM. CDMA adoption is largely restricted to the telecom providers Sprint and Verizon.

There are many different cellular Internet service types, marketed in terms of "generations" (3G, 4G, and 5G). Support for a particular type is dependent on the local cell tower. Some of the technologies used include:

- GPRS/EDGE (General Packet Radio Services/Enhanced Data Rates for GSM Evolution) is a precursor to 3G (2.5G) with GPRS offering up to about 48 Kbps and EDGE about 3–4 times that.

- Evolved High Speed Packet Access (HSPA+) is a 3G standard developed via several iterations from the Universal Mobile Telecommunications System (UMTS) used on GSM networks. HSPA+ nominally supports download speeds up to 168 Mbps and upload speeds up to 34 Mbps. HSPA+-based services are often marketed as 4G if the nominal data rate is better than about 20 Mbps.

- CDMA2000/Evolution Data Optimized (EV-DO) are the main 3G standards deployed by CDMA network providers. EV-DO can support a 3.1 Mbps downlink and 1.8 Mbps uplink.

- Long Term Evolution (LTE) is a converged 4G standard supported by both the GSM and CDMA network

providers. LTE has a maximum downlink of 150 Mbps in theory, but no provider networks can deliver that sort of speed at the time of writing, with around 20 Mbps far more typical of the speed that might actually be obtained.

- LTE Advanced (LTE-A) is intended to provide a 300 Mbps downlink, but again this aspiration is not matched by real world performance. Current typical performance for LTE-A is around 40 Mbps.

HSPA HSPA+ LTE Tethering

Mobile Access Control - On Boarding - - Captive portals - Geofencing - MAC Filtering

1.7.1. Generations

rough timeline :

1940 : 0G 1980 : 1G 1990 : 2G 2003 : 3G 2009 : 4G 2020 : 5G

0G

The system was actyally called the 'mobile radio telephone'. That's why this system is reffered to in retroactive terms such as 'zero generation' or 'precellular'.

Pioneers of 0G include motorola and bell systems.

Phones could be mobile, but they were specially mounted inside breifcases or were mounted inside vehicles.

1G

This was the first generation in cellular mobile phones. They used analog radio signals and remained the standard until 2G. The first automated cellular netowrk for commercial use was launches by NTT (Nippon Telegraph and Telephone) in 1979. In 1979 Nordic Mobile Company (NMT) introduced international roaming in a cellular network. In the USA it was introduced by Motorola DynaTec.

2G

Was the first to use digital data in phone conversations. This improved quality dramatically over analog data.

Was the first generations to offer short messaging service (SMS) text messaging.

2.5G

Introduced GPRS

offered network speeds that ranged from 56 to 114 Kbps.

Also started support of services such as MMS , SMS-based mobile games and WAP

2.75G

marked evolution of GPRS to EDGE network , which improved data transmission rates.

Even though EDGE came about in 2.75G the international telecommunicatios union (ITU) officially defined it as a 3G technology.

3G

First mobile broadband capable wireless network.

Data transmission rates of about 200 Kbps ,

Allowed web applications , such as browsing , email , voice and video calls , online games , teleconfrencing etc ...

3.5G

3.5G is interchangeable with 'High Speed Packet Access' (HSPA) - which is a combination of two protocols the high speed downlink packet access (HSDPA) and the high speed uplink packet access (HSUPA). Touted to be almost 5x faster than 3G.

3.5G uses WCDMA which is Wideband Code Division Multiple Access protocol

3.75G

Provided Evolved High Speed Packet Access or HSPA+

Uses MIMO (Multiple input Multiple Output) , i.e. mutiple antennas are used at both the transciever and the reciever.

4G

provided first true braodband data transmission rates.

First commercially deployed in norway and sweden.

Promises rates 10x the speeds of 3G

4G LTE

Long term evolution , which is a mobile communications standard for high-speed wireless internet connection for mobile devices and data terminals.

Long Term Evolution (LTE) is a converged 4G standard supported by both the GSM and CDMA network providers. In theory, LTE has a maximum downlink of 150 Mbps.

EDGE (Enhanced Data Rates for GSM Evolution) is a precursor to 3G (2.5G) with GPRS offering speeds up to 144–192 Kbps.

Evolved High Speed Packet Access (HSPA) is a 3G standard developed from GSM networks. HSPA+ nominally supports download speeds up to 168 Mbps and upload speeds up to 34 Mbps.

Evolution Data Optimized (EV-DO) is the main 3G standard deployed by CDMA network providers. EV-DO can support a 3.1 Mbps downlink and 1.8 Mbps uplink.

1.7.2. 802.16 : WiMAX

Commonly referred to as WiMAX or less commonly as WirelessMAN or the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

1.8. Protocols

Bluetooth DSL MAC Ethernet Physical Layer Including 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties Wi-Fi (802.11) DSL ISDN FDDI SMB SONET/SDH USB

-§-

2. Layer 2 : Data Link

Layer 2, the Data Link Layer

This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The principal purpose of this layer is to detect transfer errors by adding headers to data packets.

The protocols are used by the Data Link Layer include: ARP, CSLIP, HDLC, IEEE.802.3, PPP, X-25, SLIP, ATM, SDLS and PLIP.

2.1. Switches

repeater : gets a signal , regenerates it and sends it on. Used to extend range of networks , since cables and topologies have maximum lengths they can reach. Originally known as a digital regenerator since it only works for digital signals. the analog equivalent is called a analog amplifier. Reapeaters have an advantage over amplifiers since the digital signal is regenerated back to original quality and all noise is removed from the signal. Whereas amplifiers would only boost whatever analog signal they recieve which includes the noise.

multi-port repeater : this is also known as a hub

bridge : filter by mac between hubs by using MAC table

multilayer switches layer 3 switch content switch

frame switching

no loops

spanning tree protocols

flooding for unknown MACS

Switches can be connected to each other over any port using a crossover cable. Switches can also have an uplink port , which means that this particular port can be configured (by pressing a button) to either be a pre crosslink port or a normal port. As a crosslink port the switch would treat the plugged in cable as a cross link which means that we would use a straight through cable because the switch is doing the crossover for us. If we use the uplink port on the normal setting then that means we should be using a crossover cable to connect our other switch. Nowwdays most switches have Auto sensing ports , which will self configure to the type of cable attached so we dont really have to worry about all of this straight through and crossover business. What this also means is that everyone basically just uses straight through TIA 568A standard cables.

Switching / Bridging Loops : These occur when we have a loop between network switches. If this is allowed to exist without fixing it then the data will continue to loop around inside the network causing lots and lots of

collisons. There was a protocoll developed exclusively to avoid this kind of shit. It was called the spanning tree protcol (STP). STP is built into the switches. What happends when switches are first connected to each other is that one of them automatically becomes the 'root switch'. This root switch will watch any of the data that goes through , and upon detection of a bridge loop , it will disconnect one of its ports that is connected to any one of the switches. This means that the loop is broken , but all the switches will keep functioning and will remain connected to each other.

Flood Protection : Works similar to the STP , where when a computer or network device is flooding the network with traffic (usually because they are trying a layer 2 DDoS attack) , then the port connected to that machine will get turned off by that switch.

console Port : Console ports allow you to go in and manage the switches. These require rollover (a.k.a Yost cable). THe better idea is that to just use SSH to this instead of physically connecting.

switch port vs ports : Switch Ports do not use IP adresses or work with Layer 3

root guard :

BPDU Guard : A Cisco method allowing only non-switch devices to connect to the switch. If there is another switch that is plugged into a port that is marked with BPDU guard , then the port automatically turns itself off , and can only be turned back on by an administrator logging in and reenabling it.

DHCP Snooping : Similar to BPDU guard , we can specify certain ports in the swith as ports that are communicating with a DHCP server. This means that any other port on the switch that is not the certified DHCP port , will be automatically shut down if it senses a DHCP server plugged into it. This prevents things like rouge DHCP servers.

Autosensing in the switch will cause the switch port to re-wire into s crossover configuration. Straight-through cables can connect switches together. Switch ports work in full-duplex mode when connected together with either straight-through or crossover cables. A switch cannot rewire the terminating connector on a cable, only the internals of the port.

2.2. MAC / EUI Addresses

media access control

EUI-48 is the link-layer address of ethernet devices (used almost nowhere else) EUI-64 is the link-layer address used pretty much everywhere else.

Historically, both EUI-48 and MAC-48 were concatenations of a 24-bit OUI (Organizationally Unique Identifier) assigned by the IEEE and a 24-bit extension identifier assigned by the organization with that OUI assignment (NIC). The subtle difference between EUI-48 and MAC-48 was not well understood; as a result, the term MAC-48 is now obsolete and the term EUI-48 is used for both (but the terms "MAC" and "MAC address" are still used).

In other words, EUI-48 and the MAC number of a device represent the same thing! Usually it is represented in 12 hex (e.g. 0023.a34e.abc9), equivalent to 48 bits or 6 bytes.

2.3. Protocols

ICMP : works on layer 2 (internet) of TCP/IP and layer 3 (network) on the OSI

ARP : If two systems are to communicate using IP, the host sending the packet must map the IP address of the destination host to the hardware address of the destination host. The Address Resolution Protocol (ARP) is the protocol that enables this process of local address discovery to take place. Hosts broadcast ARP messages onto the local network to find out which host MAC address "owns" a particular IP address. If the destination host responds, the frame can be delivered. Hosts also cache IP:MAC address mappings for several minutes to reduce the number of ARP messages that have to be sent.

RARP

2.4. VLANs

VLAN : A VLAN (Virtual Local Area Network) splits one broadcast domain into two or more smaller broadcast domains. In a VLAN , the computers , servers ,a dn other network devices are logically connected regardless of their physical location. These are super upseful when you dont want traffic from devices that are physically on the same network to intermingle (e.g. accounting shouldnt be able to connect to shipping computers etc ...). To do this we basically break up the physical network into smaller distinct virtual networks. You can designate VLANs on a switch by specifiying ports or ranges of ports. Vlans can also help with traffic management because of the smaller broadcast domain , we can alleviate the broadcast traffic on the network.

Inter VLAN Routing : If we set up a VLAN we have multiple broadcast domains. This means that we want the traffic between these domains to remain segregated. We want this on the switch side , as well as the router side. So one solution is that we can just plug in one port from each VLAN into the router to create indipendent default gateways. The problem with this approach is that you are going to have to keep adding more router cause they usually dont ship with a whole bunch of ports (usually only 2). So the solution is something called inter VLAN routing. This is a virtualization of the functions of the router. So we are basically creating new virtual routers to interact with these virtual LANS.

Trunk Ports : A trunk port is assigned to carry traffic from all the VLANs connected to a specific network switch.

802.1q adds a tag to the ethernet frame header , labeling it as belonging to a certian VLAN.

Trunk Line

Port Bonding / NIC Teaming / Link Aggregation / Channel Bonding / Port Trunking / NIC Trunking : It is the process of taking two ports and bonding them together such that they act as on higher speed port. In cisco switches at least , the way we do this is by creating groups and assigning each individual port we want bonded onto that group. Use LACP for the trunking protocol and make sure at least one of the ports is set as active. If both ports are set as passive it wont work.

LACP

Port Mirroring : Port Mirroring enables the traffic flowing through one port to be monitored on another port. This feature enables administrators to remotely insepect traffic from a suspicious machine. It is configured on a switch by providing a source port and a destination port.

2.5. PPP

2.5.1. AAA

ACL : Access Control List

MAC : Mandatory Access Control : uses specific labels to restrict access to individual files DAC : Discretionary Access Control : gives / restricts acess to users RBAC : Role Based Access Control : uses groups that are then assigned to users to grant permissions

AAA : Authentication , Authorization , Accounting

2.5.2. RADIUS

2.5.3. TACACS+

2.6. Kerberos

Single Sign On Kerberos : Handles authentication and authorization for wired networks. It relies heavily on timestamps KDC (Key Distribution Center) AS (Authentication Service) TGS (Ticket Granting Service) TGT (Ticket Granting Ticket / Token)

2.7. Layer 2 VPNs

When it comes to the Data Link Layer VPNs, there are two private networks which are linked or connected on to the Layer 2 of the OSI model while utilizing a suitable protocol like Frame Relay or ATM.

However, these two procedures simultaneously give off a quite suitable way towards the development of VPNs. These layers are often found to be expensive as they require dedicated Layer 2 pathways for its creation and functioning.

Frame Relay and ATM protocols, both of these protocols usually don' t provide encrypting mechanisms. Instead, these two mechanisms are only responsible for allowing the network traffic for the segregation based on how Layer 2 is connected and how it relates to it.

To wrap it up, we could say that for an extra layer of security and protection you would need to develop some encrypting mechanism in its place.

-§-

3. Layer 3 : Network

Layer 3, the Network Layer

This is the most important layer of the OSI model, which performs real time processing and transfers data from nodes to nodes. Routers and switches are the devices used for this layer that connects the notes in the network to transmit and control data flow.

The network layer assists the following protocols: Internet Protocol (IPv4), Internet Protocol (IPv6), IPX, AppleTalk, ICMP, IPSec and IGMP.

3.1. Routers

router : sends data by observing ip information , also forwards

A router connects multiple networks and routes network traffic between them. It' s really that simple. In the case of your home network, your router has one connection to the Internet and one connection to your private local network. In addition, most routers also contain built-in switches that let you connect multiple wired devices. Many also contain wireless radios that let you connect Wi-Fi devices.

The simple way to think about routers—especially on your home network—is like this. The router sits in between your Internet connection and your local network. It lets you connect multiple devices to the Internet through one physical Internet connection and also lets those devices communicate with one another over the local network. In addition, the router offers some protection to your devices over being exposed directly to the Internet. To the Internet, all the traffic coming from your house looks like it' s coming from a single device. The router keeps track of what traffic goes to which actual device on your network.

But you can' t connect directly to the Internet with just a router. Instead, your router must be plugged into a device that can transmit your digital traffic over whatever type of Internet connection you have. And that device is a modem.

It is worth mentioning that the "Internet" is basically just a huge network of these routers talking to each other.

The IP address of the router itself is also commonly reffere to as the default gateway. Typing this IP address into your browser will allow you to visit the configuration page for the router.

Enterprise Network Routers

While the switches and access points can provide thousands of ports and network connections, it is inefficient to have that many connections to the same "logical" network. The ports are divided into groups using a technology called Virtual LAN (VLAN) and each VLAN is associated with a different subnet. Communications between different VLANs have to go through a router.

Do different bands on the router get different public IP adresses

single band router

dual band router

tri band router

mesh wifi

wifi extender vs repeater vs WAP

router interface

loopback interface

upstream router address

gateway routers

router remote access

3.1.1. NAT

3.1.2. PAT

Port forwarding allows for unsolicited network traffic to come from the outside internet into our local networks. This allows us to run servers and other similar devices that act like web servers , because these have no idea when someone is going to access them , and who is going to be asking for the information.

Port range forwarding : Instead of specifying the specific port that can be accessed on an internal machine from an external network we can specify an entire range of ports.

Port forwarding is a setting that, when enabled, forwards a network port from one network node to another.

Port triggering is a setting that automates port forwarding by specifying triggering ports to which inbound traffic is automatically forwarded.

3.1.3. Routing Tables

routing tables : routing tables contain address information for destination , subnet mask , gateway and NIC.

router metric : when a router has two different ways to get to a particular place , the metric value allows it to pick which one of these ways it would rather use. Earlier routing metrics used to use something called the hop count , and just pick the lower count value to set as the metric.

Nowdays routers use all kinds of things to arrive at the final metric of a particular route. Some of these things are :

- Hop count : this is the number of routers it takes to

get to a particular network ID. - MTU : The maximum transmission unit. This basically tells us the maximum amount of data we can haul in a frame. E.g ethernet has a MTU of 1500 bytes

- Bandwidth - Cost - Latency : How long does it take this particular route to react to what I want to get done.

3.1.4. Routing Protocols

static route : A static route is a fixed route that is manually configured and is persistent. We are essentially entering the all the routing table information ourselves for any computers that we might want to connect to. this also means that if we want to connect to another computer on another LAN , we have our router manually configured to send information to the router of that particular LAN , but if the connection breaks then there is no other way to talk to that particular network. The only way to get that particular connection up and running again would be for us to rewrite the routing tables. This is why outisde of personal inbuliding LANs static routing is very uncommon.

Dynamic routing : Dynamic routing is basically builds some smarts inside routers ,so that they are able to rewrite their own routing tables and keep everything that is supposed to be accesible in a network , accessible on the network. This is opposed to static routing where we would be rebuilding our routing tables ourselves , and not just us , everyone who wants to get in touch with a particluar router which has lost one of its routes. When all the routers reconfigure themselves automatically to reflect a new route it is called convergence. There are essentially two sets of dynamic routing protocols :

- Distance Vector : this is the old granddaddy of dynamic routing protocols. When some router is using distance vector , they will be sending their entire routing tables to its neighbors. These neighbors will then look at the routing tables , compare it to their own and then determine which is the best route that they can use. Distance vectors lean heavily on the idea of hop count as a metric.

- Link State : Link state regularly makes a hi / how you doin call to the connected routers. Just to make sure these routers are actually there , and if there are any changes (somebody doesnt say hi back , or some other dude says hi instead of the guy we called), Then the guy who initiated the interaction would update its routing table , and send a message to the other connected routers being like hey , I updated my routing table , are you guys interested in updating your contacts info too ? And over time the entire network gets resolved. This is known as advertising and results in much faster convergence than distance vector dynamic routing protocol.

Dynamic routing protocols can also be broken up into the following categories :

- EGP (Exterior Gateway Protocol) : When a dynamic routing protocol wants to talk to something that is outside the sphere of influence of one route controller (e.g. an ISP like comcast) they will use the EGP protocol. This being said , there is only one EGP in the entire world and this is the BGP or the border gateway protocol. The ISPs will use the BSP to communicate with each other using autonomous system numbers that are assigned to them.

- BGP : It is a hybrid protcol that contains aspects of link state and dynamic vector. BGP breaks the entire internet into roughly 20,000 autonomous systems. The entire job of the BGP is to route data between different autonomous systems. This means one peice of data that has a AS number destination from one AS to another only needs to go to a router that lives on the 'edge' of an AS zone instead of always bouncing around slowly making its way to the border of the current AS network. This router on the edge only needs to know where to forward into one router on the next AS zone and all of this is done using the AS numbers.

Autonomous Systems (AS) : An AS is a group of one or more router networks that are under the control of a single entity (ISP , university , goverment system etc...) An AS has direct or indirect control of all of the routers , all the networks , all the subnets etc.. within their own AS. This allows ASs to route within their own "internal network" howver they want. When these AS systems want to talk to each other though they have to use BGP. Each AS has its own autonomous system number (ASN).

- IGP (Interior Gateway Protocol) : When you want to talk to someone who is within the same routing sphere of influence as you (e.g. you and your actual physical apartment neigbor both use comcast) then you will use IGP. There are a couple of kinds of IGPs :

- - RIP : Rip is a distance vector protocol and an interior gateway protocol (IGP) that uses hop count to deterimine routes. If a route is found with a shorter hop count to the same destination, the routers with a choice to the said path will simply delete the longer path from the routing table. There are versions of RIP. RIP1 is only used in classful networks (e.g Class A , B etc...). Rips maximum hop count is 15. Since we are using distance vector , the routers will only talk to each other every so often , therefore it can take a longer time to convergence as opposed to other link state based IGP protocols.

- - EIGRP : Another example of a distance vector routing protocol.

- - OSPF : Open shortest path first. Most popular dynamic routing IGP. Uses Link state protocol. As soon as OSPF routers are connected together they start sending link state advertisments and calculating their links. These links are based mainly on bandwidth. They will automatically elect one out of all of the routers connected (on this particualar AreaID) as the

designated leader router, and another as the backup leader. The link state advertisments will communicate information about who the individual routers are connected to , this is in opposition to sending out entire routing tables as is done in dynamic vector. Since we are only sending small quick connection information , the routers can quickly update thier own tables and know which path leads them where. This leads to faster convergence. OSPF also works with CIDR (classes subnets) and also works with BGP.

3.2. IPv4

An IP address encodes two pieces of information:

- The network number (network ID)—this number is common to all hosts on the same IP network.

- The host number (host ID)—this unique number identifies a host on a particular network or logical subnetwork.

In order to distinguish the network ID and host ID portions within an address, each host must also be configured with a network prefix length or subnet mask. This is combined with the IP address to determine the identity of the network to which the host belongs.

There are some IP adresses that are special.

Private ip address : there are three different types of adresses that you can only access on a private network. You cant go through the internet or google to these addresses. These are used on internal networks for systems that do not do any sharing outside of the network. These are :

- 10.x.x.x : Any IP starting with a 10 is a private IP address. - 172.16.x.x - 172.31.x.x : - 192.168.x.x :

Loopback Addresses : This is an address that you get only when you try to ping yourself using a loopback adaptor (a RJ plug looped in on itself). This used to be a good way to test the working of your network cards. Nowdays loopbacks are not that useful. The actual address for IPV4 is 127.0.0.1 , and for IPV6 is ::1: .

Public ip address :

The first octet of a Class A address goes from 1 to 126. The first octet of a Class B address goes from 128 to 191. The first octet of a Class C address goes from 192 to 223.

examples :

B : 130.222.255.170 C : 216.53.12.11 C : 223.255.6.88

gateway vs interface

ip broadcast vs mac broadcast

ARP : Address Resolution Protocol.

CIDR : Classless Inter-Domain Routing

unicast :

Multicast : a multicast allows a computer to have multiple different IP addresses assigned to it. One will be your normal regular IP adress and the second one will be a multicast address. This adress is then used in conjucntion with IGMP protocol to be able to send the same stream of traffic from a server (like a video) to multiple different devices , while only having opened one IP connection. Namely the multicast connection with the multicast IP.There are a special batch of IP adresess reserved for this type of thing. All IP adresses starting with 224.x.x.x are multicast adrresses.

broadcast :

3.3. IPv6

IPv6 is 128 bits compared to 32 bit Ipv4 Address. This gives IPv6 2^{128} addresses , as opposed to the 2^{32} that IPv4 has. IPv6 uses 8 segments that are traditionally seperated by 7 colons, and look something like :

00 00:00 00:00 00:00 00:00 00:00 00:00 00:00 00

IPv6 addresses all have /64 subnet masks with no exceptions. This means that there is no more classfull or classless subnetting.

Ipv6 allows data to move much faster through the internet.

Another thing about Ipv6 is that we no longer need private IP adresses. This is because IPv4 private adresses mainly came about cause we were running out of adresses to use, so we decided to recycle as many as we could using clever tricks.

Now that we have plenty of addresses to hand out we dont need your little trickses. The problem however is that since IPv6 addresses are all public and unique there is a certain degree of traceability to your system anytime you are communicating on the internet. People could trace your traffic down to your individual unique NIC MAC address , so there is a loss of privacy. To advoid this instead of using EUI-64 , we just use a randomizer to generate the last half of the link-local address. A system admin could however force the machines on the LAN to use EUI-64 if he wants to for some reason.

When we use IPv6 then we always have at least two addresses :

- Link Local Address (IPv6) : The link local address is automatically generated by any IPv6 capable host as soon as the device starts up. The link-local address always starts with -

fe80:0000:0000:0000

The second part of the link-local address comes from the MAC address. The conversion from MAC to IPv6 happens using EUI-64.

- Internet Address (IPv6) : The internet address is given to you at least in part by your gateway router.

Link local adresses cannot connect to the internet.

NDP : Neighbor Discovery Protocol

Neighbor Solicitation Messages are sent out right after the computers boot up and have generated their Link-Local Address. This is sent to the switch using ICMPv6 which is a multicast version of ICMP.

Neighbor Advertisment

Router Solicitation

Router Advertisment

Stateless auto Configuration

3.4. Firewalls

Types of Firewall

On a TCP/IP network, each host is identified by an IP address, while each application protocol (HTTP, FTP, SMTP, and so on) is identified by a port number. Packet filters on a firewall can be applied to IP addresses and port numbers.

A more advanced firewall (stateful inspection) can analyze the contents of network data packets, so long as they are not encrypted, and block them if any suspicious signatures are detected and identify suspicious patterns of activity.

A hardware firewall is a dedicated appliance with the firewall installed as firmware. A software firewall is installed as an application on a workstation or server. Most Internet routers also feature a built-in firewall, configured via the web management interface.

A simple host firewall (or personal firewall) may be installed on a client PC to protect it. Windows features such a firewall. There are also numerous thirdparty host firewalls.

On an enterprise network, a network firewall is likely to be deployed to monitor and control all traffic passing between the local network and the Internet. On networks like this, clients might not be allowed to connect to the Internet directly but forced to use a proxy server instead. The proxy server can be configured as a firewall and apply other types of content filtering rules.

Some proxy servers work transparently so that clients use them without any extra configuration of the client application. Other proxies require that client software, such as the browser, be configured with the IP address and port of the proxy server. This information would be provided by the network administrator.

A firewall exists between the internal network and the external public internet.

A firewall basically blocks unwanted traffic from entering the network , and allows wanted traffic.

The word firewall comes from the actual physical firewalls that exist inside buildings. In case of fire such walls exists to contain fires within specific zones to prevent them from spreading and burning your whole house down.

A firewall becomes more and more essential , the larger your internal network gets. It sits on the router and prevents any traffic from accessing devices on your internal network that people on the outside have no business acessing anyway.

The rules according to which the firewall will allow or block traffic are defined inside a file called the access control list. Firewall rules can be based upon :

- IP addresses - Domain names - Protocols - Progams - Ports - Key words

Host Based Firewall A host based firewall is installed as a peice of software on a computer instead of a router. This means that only that specific computer is protected instead of the whole internal network. An example of this is the Microsoft Windows firewall that runs locally on your computer.

Network based Firewall A network based firewall is a combination of a hardware and software based firewall. This firewall is so named because it operates at layer 3 or rather the network layer. It is placed between the private network and the public internet. These can be built into a router , or in case of larger organizations they can also be a stand alone device that can be purchased, or they can also be part of a service providers cloud infrastructure.

Stateless firewalls examing packets / ports etc ... independently based on different variables. As long as a specific incoming or outgoing packet meets the predefined requirements from the ACL (Access Control List) then they will be indiviually allowed through , with no reference to any preceding packets that may have passed the firewall before.

The following functions fall under simple static stateless filtering :

- Port Filtering : Allow or deny certain port communications. Closing Port 80 will deny all web page traffic. While allowing port 25 will allow sending emails.

MAC Filtering : Allow or deny commnication in or out of a device based upon the MAC number of the NIC (Network Interface Card)

IP Filtering : This is also known as packet filtering and will block packets in layer 3. This can allow blocking of incoming or outgoing traffic by a specific IP address or range of IP addresses.

Content Filtering : this is also known as information filtering. This blocks traffic by matching strings of characters. Common examples might be ‘Hate’ ‘Violence’ and ‘Pornography’.

Dynamic or statefull filtering is a more comprehensive inspection of all the incoming data packets. Statefull or dynamic filtering goes all the way from layer 2 to layer 7. It will not only inspect the source and destination IPs / MACs included in the packet / frame , it will also go so far as the application layer and will inspect

the content inside the payload.

A thing to keep in mind though is that dynamic / stateful inspection is not a simple sum of all of the stateless inspection models.

The most important feature of dynamic firewalls is tha packets are exmined as steams , and the decision on whether to pass a packet depends onwhat packets have already been though the firewall.

- Edge Firewall - Interior Firewall

3.5. IDS

Intrusion detection systems detect and report possible attacks to the administrators.

3.6. IPS

An intrusion prevention system is an evolution of IDS. It was originally known as active IDS.

Intrusion Prevention systems run in-line with networks and act to stop detected attacks.

The difference is that a firewall filters malicious traffic , the IDS notifies on detection on malicious traffic , the IPS acts to stop malicious traffic.

- inline IPS

3.7. Layer 3 VPNs

The purpose of the Network Layer VPNs has deviated towards the Layer 3 tunnelling as well as the adoption of encryption mechanisms and techniques that were lacking in Layer 2.

For example, we are using the IPsec tunnelling and encrypting protocol for the development of VPNs, although some of the other technical examples are GRE and L2TP protocols.

It would be quite interesting if we notice that however L2TP tunnels Layer 2 traffic, along with that, it uses Layer 3 which is the IP layer, to help perform this mechanism. Due to such functioning, we call it a network layer VPN.

This pretty much sums up the working of network Layer VPNs. Network Layers are responsible for providing an extremely accurate and suitable site to do encryptions.

The network layer is quite low as compared to the stack for providing a robust and seamless network and internet connectivity to all applicants running freely on the top of the Network Layer. The functioning of Network Layers is steady enough to let the suitable granularity arose for the traffic regarding being the part of the VPN based on its IP address architecture.

3.8. Protocols

IGMP : works on layer 2 (internet) of TCP/IP and layer 3 (network) on the OSI

Network Address translation (NAT) : Converts IP addresses between internal networks and 'the internet'. This is also known as Port address translation (PAT). You can think about this as translating an 'IP address' to an 'internet address'. NAT works at layer 3 because it is modifying the IP header. If you use PAT you could argue that it is working at layer 4 as well because it MIGHT change the source port of the packet in case it is not unique.

Several internal addresses can be NATed to only one or a few external addresses by using a feature called Port Address Translation (PAT) which is also referred to as "overload", a subset of NAT functionality.

PAT uses unique source port numbers on the Inside Global IP address to distinguish between translations. Because the port number is encoded in 16 bits, the total number could theoretically be as high as 65,536 per IP address.

PAT will attempt to preserve the original source port, if this source port is already allocated PAT will attempt to find the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023 or 1024-65535.

If there is still no port available from the appropriate group and more than one IP address is configured, PAT will move to the next IP address and try to allocate the original source port again. This continues until it runs out of available ports and IP addresses.

Static NAT (SNAT) : The router will assign one IP address to one machine on the internal network so that any incoming traffic will always be sent to that machine.

Dynamic / Pooled NAT (DNAT) : Assigns IP address to a machine only when it is tryign to communicate with something over the internet. The problem is that routers only have a finite amount of IPs to give out and if we need more machines on the internal network , and are using DNAT , we are shit outta luck.

LAN Address vs WAN address

-§-

4. Layer 4 : Transport

Layer 4, the Transport Layer

The transport layer works on two determined communication modes: Connection oriented and connectionless. This layer transmits data from source to destination node.

It uses the most important protocols of OSI protocol family, which are: Transmission Control Protocol (TCP), UDP, SPX, DCCP and SCTP.

4.1. Proxy Servers

A proxy server, also known as a "proxy" or "application-level gateway", is a computer that acts as a gateway between a local network (for example, all the computers at one company or in one building) and a larger-scale network such as the internet. Proxy servers provide increased performance and security. In some cases, they monitor employees' use of outside resources.

A proxy server works by intercepting connections between sender and receiver. All incoming data enters through one port and is forwarded to the rest of the network via another port. By blocking direct access between two networks, proxy servers make it much more difficult for hackers to get internal addresses and details of a private network.

Some proxy servers are a group of applications or servers that block common internet services. For example, an HTTP proxy intercepts web access, and an SMTP proxy intercepts email. A proxy server uses a network addressing scheme to present one organization-wide IP address to the internet. The server funnels all user requests to the internet and returns responses to the appropriate users. In addition to restricting access from outside, this mechanism can prevent inside users from reaching specific internet resources (for example, certain websites). A proxy server can also be one of the components of a firewall.

Proxies may also cache web pages. Each time an internal user requests a URL from outside, a temporary copy is stored locally. The next time an internal user requests the same URL, the proxy can serve the local copy instead of retrieving the original across the network, improving performance.

Do not confuse a proxy server with a NAT (Network Address Translation) device. A proxy server connects to, responds to, and receives traffic from the internet, acting on behalf of the client computer, while a NAT device transparently changes the origination address of traffic coming through it before passing it to the internet.

For those who understand the OSI (Open System Interconnection) model of networking, the technical difference between a proxy and a NAT is that the proxy server works on the transport layer (layer 4) or higher of the OSI model, whereas a NAT works on the network layer (layer 3).

A proxy is any device that acts like an intermedieary between two different devices tha are in a session. This means that a proxy will sit between a client and a server when they are talking.

Proxies are all going to be application specific. As an example if we want to channel HTTP traffic through the proxy then we would have a web proxy. Other types of proxies , all application specific are :

- Web Proxy - FTP Proxy - VoIP Proxy

Transparent Proxy

A forward proxy sits behind the network firewall and in front of the client. In this case the client would be aware of the existence of this proxy. The client would speak to the proxy and then the proxy after doing whatever it is doing would forward the clients request to whichever server that the client wanted to talk to.

Forward Proxies can be a dedicated box , or a peice of software that is running on any computer somewhere.

Most forward proxy servers would act like firewalls , by providing content filtering , ad blocking and stuff.

This is a complete reverse of a forward server. In this case the proxy will represent the actual server that we are communicating with. This means that the client will send a request , the proxy server will intercept the request , and send that request to the actual server on behalf of the client , the server responds not to the client , but to the request of the proxy server. The proxy then returns whatever information was requested to the original client.

The main functions of reverse proxy servers is to protect the server instead of the client. Therefore they have features such as :

high security - handle DoS attacks - load balancing - caching - encryption acceleration

4.2. TCP

NCP : Network Control protocol , precursor to tcp

TCP Acceleration : TCP acceleration is the name of a series of techniques for achieving better throughput on a network connection than standard TCP achieves, without modifying the end applications. It is an alternative or a supplement to TCP tuning.

4.3. UDP

4.4. Ports / Port Numbers

Yes, its the 4th layer (transport) of the 7 layers for the OSI model.

Reading your last post/question, if you're also asking about the TCP/IP model, it's the 3rd layer (transport) of the 4 layers for that model.

Port numbers, in IP, are used by both TCP and UDP. Port numbers all quick "sorting" of received packets to processes that want them. Some applications have been "assigned" specific port numbers. For example, HTTP has assigned to it port 80. So, when a client wants to contact a HTTP server, its uses destination port of 80 and a source port unique to the process making the request. This allows the receiving host to send any received packets with a destination of port 80 to the processes "listening" for those packets, which if there is one, would normally be a HTTP server process.

When the HTTP server responds, it uses the client's source port as the reply's destination port and it might use port 80 for the reply packet's source port. This allows the original client to forward the port quickly to the process that made the request.

Although many applications have "assigned" ports, applications might use other port numbers. I.e. the port number doesn't control an application, it's just a convenience. For example, you could configure a HTTP server to "listen" on port 8080. Now, either the client needs to know that too, or it would need to send its HTTP request to all possible 65K port numbers.

DCCP SCTP RSVP

-§-

5. Layer 5 : Session

Layer 5, the Session Layer

The session layer creates a session between the source and the destination nodes and terminates sessions on completion of the communication process.

The protocols used are: PPTP, SAP, L2TP and NetBIOS.

5.1. Protocols

-§-

6. Layer 6 : Presentation

Layer 6, the Presentation Layer

The functions of encryption and decryption are defined on this layer. It ensures that data is transferred in standardized formats by converting data formats into a format readable by the application layer.

The following are the presentation layer protocols: XDR, TLS, SSL and MIME.

6.1. DHCP

DHCP : gives a computer a dynamic ip , subnet mask and gateway from its scope

DHCP Reservation : asks for specific mac to be given specific IP everytime from DHCP server , usually given to network printers and servers , that need to maintain a constant IP

DHCP Lease : amount of time an IP is assigned to a computer

DHCP Relay :

BootP

DHCP Client

DHCP servers can be included within the routers you buy , or they can be special software that is sitting on your system. Most commonly however a DHCP server is an actual computer server sitting out there on the network , whose only job it is to be a computer running the DHCP software.

DHCP Discover DHCP Offer DHCP Request DHCP Acknowledge

You want to make sure that each broadcast domain only has one DHCP server running, because otherwise if you send out a broadcast you can get back conflicting information from two different DHCP servers that are operating on the same network. This is one of those so called "bad things". This also means that the DHCP Server has to be within the broadcast domain , i.e. within your LAN. It cannot be outside the network.

DHCP Relay DHCP Server Scope : When you are creating your own DHCP server , one of the first things you are going to want to do is set the scope. Which means you are going to set the starting IP address , and an end IP address. As an example ,

Start IP address : 192.168.15.100 End IP address : 192.168.15.105

passes out a total of 6 IP Adresses In addtion you will also decide which subnet to pass out , as well as exclusions. This basically means that if there are any special IP adresses within the scope that you specified earlier , you can specify them and the server will not hand them out when some device is making a DHCP request. Another thing you will specify is the lease duration. Basically how long will the host that got a specific IP address be along to keep it for. On most Windows DHCP servers , the default is something like 8 days. But if you are in something like a coffe shop or some other public facing network , you might want to reduce this setting down to just a couple of hours.

Rogue DHCP Server : If you have a DHCP server running on the local network and you are not getting an APIPA , and you have an IP address which is different than what you know yours to actually be , then that means that you have a rogue DHCP server. Rogue DHCP servers can assign incompatible IP addresses to hosts on a network making them unable to communicate with other hosts or the Internet. Rogue DHCP servers cause IP address incompatibilities or worse - they do not increase network performance by either increasing DHCP assignment speeds or the size of IP address pools. The existence of a DHCP server, rogue or approved, ensures that hosts will not generate APIPA addresses.

WAN DHCP

APIPA : automatic private IP address assignment , if DHCP cannot be reached then all computers post Windows 98 will assign an IP to themselves which looks like 169.254.0.0. We can still use the APIPA address to communicate on the internal network. We cannot however use it to connect to a machine over the internet.

Dynamic IP addressing : gets IP from DHCP (dynamic host configuration protocol) , the dhcp has a pool of IPs that it can lease to a particular device for certain periods of time ,

6.2. DNS Server

6.2.1. DNS Hierarchy

Host File : Before DNS Servers existed , computers used to use something called a host file to resolve domain names to ip addresses. This was basically a text file containing a list of domains and ips. Even though DNS Servers can do everything a host file was supposed to do, the hosts files still exist on every computer that uses TCP/IP. What is even more interesting is that the records in the host file take precedence over any DNS server that you might be using. The one job that Domain Name System Servers (DNS Servers) have is to resolve resource names to IP addresses. In the DNS, the clients are called resolvers because the are requesting a resolution of domain name to an IP-Address and the servers are called name servers.

DNS databases are distributed because no one DNS server holds all possible DNS records. This would be far too much information for a single server to store. Instead if the particular record that the client is asking for does not exist in this particular DNS servers table

, then it will just ask some other DNS server for the information. The way they figure out which one of the numerous DNS servers to ask for this information is by looking at the requested domain name. Then they use a tree structure where just below the root are a set of Top Level Domains (TLD) that define broad classes of entities (.com , .gov , . . .) or national authorities (.uk , .ca . . .). Within these top level domains, companies, universities, non-profits, governments, or even just one guy can all register individual domains.

6.2.2. Lookup Zones

Lookup Zone : When we create our own DNS server for a LAN , we need to input the domain to ip mappings in a table that will allow the server to resolve requests. These records in the table are called lookup zones.

There are two different types of zones (or requests) that you can make to your local Authoritative DNS server :

- Forward Lookup Zone : This basically resolves the domain name to an ip address. The server will query its table for some string "name" and then return the address in the corresponding "data" column in the table.

- Reverse Lookup : The other type of request we can make from a DNS server is to ask for domain names , based on provided IP addresses. Unfortunately, it is a limitation by design that DNS server cannot just lookup at the value on "Data" column to find the associated "Name" value. To fix this we store the ip addresses as regular "names" in the table and the corresponding "data" column would then contain the domain name. So a lookup for a domain based on provided ip address is called a reverse lookup. Reverse Lookup zones are useful for mail servers.

6.2.3. DNS Records

Any computer holding records for a part of the namespace is said to be a name server. Name servers that contain the requested resource records for a particular namespace are said to be authoritative. If they are not authoritative for a namespace, they will have pointers to other name servers which might be authoritative.

Resolvers are software programs running on client computers. For example, name resolution is a critical part of web browsing, so web browser software will implement a resolver. Authoritative (Local) DNS Servers : One of the few reasons to deal with implmenting or at least spinning up your own DNS server is to allow computers on the local network to talk to each other. Usually by convention the domains that are supposed to be used on LANs are marked .local as opposed to .com / .edu / .org or something like that. The name server (local DNS server) that resolves local domain names is called an Authoritative DNS Server. If we have multiple DNS servers on a LAN , then one of them is designated the primary one we should attempt to use. This sever is called the Start of Authority. The rest of the local DNS servers will all just be called Name servers. It can in addition resolve your nomal website domains like google.com by sending an upstream request from other internet DNS servers. To be able to resolve these domain names into ip addresses , we need a table that holds these records. These records are called lookup zones. If not then we can just statically enter the domains and the ips. If we are using IPv4 records that is called a "A" record , and if we are using IPv6 then it is reffered to as a "AAAA" record. We can also have CNAME (Canonical Names) and are used as aliases for the host names. MX Record SRV Record (Service Location) :

TXT Records DKMI SPF

6.2.4. DDNS

Dynamic DNS : We can either manually go into the DNS servers we have created and enter the records into our table , or we can get this information dynamically. If we are using DHCP to get our IP addresses , then the DNS server would need to be configured to get the table records from the DHCP server. This is called DDNS or dynamic DNS.

Enables you to use a DHCP-assigned IP address for connection.

6.3. Protocols

-§-

7. Layer 7 : Application

Layer 7, the Application Layer

This layer works at the user end to interact with user applications. QoS (quality of service), file transfer and email are the major popular services of the application layer.

This layer uses following protocols: HTTP, SMTP, DHCP, FTP, Telnet, SNMP and SMPP.

Cookies

A cookie is a plain text file created by a website when you visit it. The purpose of cookies is to store session information so that the website can be personalized for you. For example, cookies may record information you type into forms, preferences you choose for the way the site works, and so on. They may also be used to display targeted advertising to you or collect information (metadata) about the browser you are using, your IP address, the links you click, how often you visit a site, and so on. An IP address can often be tied quite closely to a geographic location.

This sort of information is referred to as Personally Identifiable Information (PII). Anyone able to collect this information might be able to track the sites you visit and work out where you live. You can configure browser settings to try to limit the way sites can gather PII from your browser.

There are two classes of cookies:

- First-party cookies—set by the domain you visit. For example, if you browse comptia.org and the server creates a cookie owned by comptia.org then this is a first-party cookie.

- Third-party cookies—set by another domain. For example, if you browse comptia.org and a widget on the site tries to create a cookie for adtrack.com, this is a third-party cookie.

Cookies cannot spread malware, but if your computer is infected with a virus or a Trojan, it may be able to steal the information contained within cookies.

Spyware and adware may make use of cookies to track what sites you visit and display targeted adverts.

7.1. Protocols

7.2. Domain Names / Host Names

Host / Node : a host is a network end point. Some say that a computer 'hosts' or 'serves' the clients that use an application. This is the orgin of the terms host and server. A host is not neccessarilly a single computer. It is possible for a single computer to use multiple IP addresses, especially when it is providing multiple services such as an e-mail server and a web server at the same time. One IP address will be used to identify the e-mail server software, the other IP address will identify the web server software but both server applications are running at the same time on the same computer. The IP addresses allow each to be accessed individually.

Hostname : A hostname is just the name given to an IP host. A hostname can be configured as any string with up to 256 alphanumeric characters (plus the hyphen), though most hostnames are much shorter. The hostname can be combined with information about the domain in which the host is located to produce a Fully Qualified Domain Name (FQDN). For example, if www is a host name, then the FQDN of the host www within the comptia.org domain is www.comptia.org.

A hostname is a label assigned to a device (a host) on a network. It distinguishes one device from another on a specific network or over the internet. The hostname for a computer on a home network may be something like new laptop, Guest-Desktop, or FamilyPC.

Hostnames are also used by DNS servers so you can access a website by a common, easy-to-remember name. This way, you don't have to remember a string of numbers (an IP address) to open a website.

Each of the following is an example of a Fully Qualified Domain Name with its hostname written off to the side:

www.google.com: www images.google.com: images products.office.com: products www.microsoft.com: www

The hostname (like products) is the text that precedes the domain name (for example, office), which is the text that comes before the top-level domain (.com).

A fully qualified domain name (FQDN) contains both a host name and a domain name. For a landing page, the fully qualified domain name usually represents the full URL or a major portion of the top-level address.

In looking at a fully qualified domain name, the host name typically comes before the domain name. The host name represents the network or system used to deliver a user to a certain address or location. The domain name represents the site or project that the user is accessing.

One example is the use of various networks to access educational websites. Typically, the domain name will consist of the identifier for a specific school' s web domain, along with the top-level .edu suffix. For example, the domain name for America University would be americauniversity.edu. The host name would consist of either "www" where the global internet is the host, or some proprietary network name that represents the host – for example, if the school uses a custom internal network called "myAUnet" then "myAUnet" would be the host name.

URL : Uniform Resource Locators . When a web

browser is used to request a record from a web server, the request must have some means of specifying the location of the web server and the resource on the web server that the client wants to retrieve. This information is provided as a Uniform Resource Locator (URL). The URL (or web address) contains the information necessary to identify and (in most cases) access an item.

Protocol : https://

hostname : www.

domain name : comptia

top level comain : .com

filepath : /home/index.html

A URL consists of the following parts:

1. Protocol—this describes the access method or service type being used. URLs can be used for protocols other than HTTP/HTTPS. The protocol is followed by the characters ://

2. Host location—this could be an IP address, but as IP addresses are very hard for people to remember, it is usually represented by a Fully Qualified Domain Name (FQDN). DNS allows the web browser to locate the IP address of a web server based on its FQDN.

3. File path—specifies the directory and file name location of the resource, if required. Each directory is delimited by a forward slash. The file path may or may not be case-sensitive, depending on how the server is configured. If no file path is used, the server will return the default (home) page for the website.

7.3. Layer 7 VPNs

Application layer VPNs have especially been designed with specified specific applications, unlike the other two categories.

Some justifying examples of Application Layer VPNs include the VPNs such as SSL-based VPNs. SSL based VPNs provide encryption between the Web browsing and webs serving while running the SSL.

A second suitable example for application layer VPNs is functioning of SSH, which is pushed as an encrypting mechanism dedicated to the secure login sessions to access various network devices. SSH tends to encrypt, thus by encrypting it can create suitable VPNs for different other similar functioning application layer protocols, for example, FTP and HTTP.

However, one persistent drawback that has been seen continuously while running Application Layer VPNs is its non-seamless functioning.

The users of this VPN are asked to enable the end devices for the creation of a better VPN designated to each application.

Just as more services for corresponding applications are being added, it is inevitable to create the development for them separately as well.

This functioning feature of Application Layer VPNs differs from the Network Layer and Link Layer VPNs. Those two VPNs are responsible for providing seamless VPN connectivity for all the setup applications.

-§-

8. Security

something you know : password , pin , captcha , security questions something you have something about you somewhere you are something you do : typing speed

federated trust system

8.1. Symmetric Encryption

RC4 AES

Symmetric Encryption uses one key for both encryption and decryption.

Super basically symmetric encryption will change some plaintext into cyphertext using a key and an algorithm.

8.2. Asymmetric Encryption

8.2.1. hashing

MD5 SHA1

hashes confirm data integrity , they are not forms of encryption.

Hash values are always fixed in size.

8.2.2. Digital Signatures

Asymmetric Encryption uses two keys. One key only encrypts and the other key only decrypts. The key that encrypts is also called the public key. The key that decrypts is called the private key.

Now that we have two keys , we can share one of them with others. The one we share is the public encryption key. The guy who has this key can then send over his own public key. This process is known as a key exchange.

Public keys aernt really protected all that much , since the only thing you can do with it is encrypt data. The only person who can actually decrypt the data is the guy who has the exact corresponding private decryption key to that public encryption key.

Keep in mind though that both the public encryption key and the private decryption key are basically just strings of binary. There is no rule built into the key itself saying that you can only decrypt with this key. The simple faact is that the algorithmn generated two keys (binary strings) and we happen to be using one of those strings arbitrarily as a public encryption key and another one as a private decryption key.

There are two problems that arise here :

1. How do you know that the domain claiming to send the public key is the real domain you wished to get the public key for ?

2. How do we verify that the the person who sent the information is actually the owner of the public key that was sent ?

To solve this problem we use a digital signature.

8.2.3. Certificates

Digital Certificates and Anti-phishing

When a web browser communicates with a secure (HTTPS) server, it accepts the server's digital certificate to use its public key to encrypt communications. Because of the special way that the keys are linked, the public key cannot be used to decrypt the message once encrypted. Only the linked private key can be used to do that. The private key must be kept secret. This is referred to as asymmetric encryption.

Having a certificate is not in itself any proof of identity. The browser and server rely upon a third-party —the Certificate Authority (CA)—to vouch for the server's identity. This framework is called Public Key Infrastructure (PKI).

A browser is pre-installed with a number of root certificates that are automatically trusted. These represent the commercial CAs that grant certificates to most of the companies that do business on the web.

Digital Signature : When we are trying to have secure communications and verify the integrity of the files sent as well as the identity of the sender (because the sender could be some evil dude) , we use encryption and hashing together. A digital signature basically serves to verify the owner / sender of the private key as well as the information being sent.

what I as a sender do is the following :

1. Participate in public key exchange 2. Encrypt the entire information being sent (e.g. webpage) using a private key 3. Hash the entire encrypted page 4. Send the hashed encrypted page to the guy who has my public key and requested the info 5. Dude will unencrypt the page using the public key

This is called a digital signature

Digital Certificate : A digital certificate is a collection of a public key , a digital signature of the sending party (i.e. the guy who owns this particular public key) to verify that the public / private key belongs to the sender , as well as a third party signature that verifies that the sender actually is who he says he is.

Unsigned Certificate :

Self Signed Certificate : A self-signed certificate can throw a 443 error, as the certificate has not been issued by a certifcate authority.

Any expired certificate can be viewed , then fiexed by getting a new certificate from the issuer or accepting the certificate in its current state.

Web of Trust :

PKI (Public Key Infrastructure) :

Certificate Authorities (CA) :

CRL

OCSP :

8.3. Wireless Security

There are types of malware :

- Viruses and Worms - Tojan Horse - Adware - Spyware - Randomware / Crypto-Malware - Logic Bomb - Rootkit and Backdoors

RAT (Remote Access Trojan) Polymorphic Malware Keyloggers Armored Viruses

Distributed Denial of Service

A Denial of Service Attack Basically Prevents other from accessing a system.

A Distrubuted Denial of Service does the same thing as a DoS attack except this time using a bunch of different computers.

There are three types od DoS (Denial of Service) :

- Volume Attack : Flood the server with ping , or udp etc ...so that the server is not able to handle the amount of network traffic and goes down. - Protocol Attack - Application Attack

Slow Loris Attack Smurf Attack

BotNet

-§-

ipconfig /all ipconfig /release ipconfig /renew ipconfig /displaydns ipconfig /flushdns

nslookup

arp -a netstat

route print route print is the exact same as : netstat -r

tracert www.google.com pathping www.google.com

ftp ftp open ¡ServerName¿

net view net user net use net share ¡filename¿=¡filepath¿ net share ¡foldername¿=¡folderpath¿

show current computer name nbtstat -n

show remote cache table nbtstat -c

dig ifconfig arp -a traceroute tcpdump

QOS (Quality of Service) : QOS Controls help better manage available bandwidth. One type of quality of service control is traffic shaping.

Quality of Service is the feature that allows you to prioritize certain types of network traffic over other types of lesser importance.

Traffic Shaping : We can set the different priorities (based on application / MAC etc ...) of the network traffic that is coming through to always make maximum use of our bandwidth. Simple QoS on SOHO routers allows priority setting for different protocols.

The various VPN Tunneling Protocols are :

- PPTP : Point to Point Tunneling Protocol - - Encapsulation : Encapsulates PPP frames in IP datagrams - - Encryption : PPP frame is encrypted with Microsoft Point to Point Encryption (MPPE) - - TCP Port 1723 - - GRE (Protocol 47) - - Older and does not provide data integrity (proof that the data was not modified in transit) , or data origin authentication (proof that the data was sent by the authorized user) - - Support was dropped with some newer operating systems.

- L2TP : Layer 2 Tunneling Protocol - - Encapsulation : 2 Layers - PPP frame is wrapped in IP datagram then wrapped with IPsec Encapsulating Security Protocol (ESP) - - Encryption : IPsec encryption algorithm - - UDP Port 500 and 4500 - - ESP (Protocol 50) - - Will support most older clients and can use certificates or preshared key for IPsec. - - Support for 3DES and AES encryption algorithms - - Considered secure when using AES and not a pre-shared key - - Some difficulty when NAT is involved

- IKEv2 : Internet key exchange version 2 - - Encapsulation : Uses IPsec and the Encapsulating Security Protcol (ESP) - - Encryption : IPsec encryption algorithm - - UDP Port 500 and 4500 - - ESP (Protocol 50) - - Mainly supported by newer clients - - Some difficulty when NAT is involved - - Suppoorts VPN RE-connect , MOBIKE

- SSTP : Secure Socket Tunneling Protocol - - Encap-

sulation : Encapsulates PPP frames in IP datagrams over port 443. - - Encryption : Encryption with the SSL channel of the HTTPS protocol. - - TCP Port 443 - - Pretty much always works becuase it only uses port 443. - - Support is limited with operating systems other thant windows because it's a Microsoft owned protocol.

- OpenVPN : This is an open source technology that uses the OpenSSL library and the TLS protocols. It can be similar to SSTP in that it can be configures to use port 443. It needs a 3rd party VPN client. Should use with perfect forward secrecy (PFS) .

PAP CHAP MS-CHAP

IP Tunneling

PPTP (Point to Point Tunneling Protocol)

VPN : A VPN creates a secure tunnel so that a remote machine or network can be part of a local network.

L2TP/IPSec (Layer 2 Tunneling Protocol)

SSTP (Secure Socket Tunneling Protocol)

VPN Concentrator : This is a dedicated box that acts as an endpoint for the entire network.

client-to-site VPN : A client-to-site VPN connects a remote computer to a local network.

site-to-site VPN : A site-to-site VPN connects distant networks into a single network.

Introduced by CITRIX

TightVNC : Port 5900

Remote Desktop Server : RDP : Port 3389

Storage Area Network (SAN) : A SAN is a high speed network that stores and provides access to large amounts of data. This is basically a dedicated networok (or subnet) that is use donly for data storage. This is in opposition to a NAS (Network attached storage) device since a NAS would live on the same network but comes with the disadvantage of a single point of failure. As an example if the power supply to the NAS fails , then all the computers on that network cannot use it. A SAN contains mutiple disk arrays , its own siwtches and servers. Since there are multiple disks arrays that share the data this makes the SAN a lot more fault tolerant than a NAS. When a server accesses a drive on the SAN it is accessed as a local drive , as opposed to a network drive as we would see in NAS. SANs are also very scalable since we can just add more disks and disk arrays. Another adavantage is that SANs are not affected by the actual network traffic , so there is no danger of not being able to access files becuase the network is clogged up. All this being said SANs cost a lot of money so they are only used by huge companies.

A dmz allows unsoliticied internet traffic from outside the local network to enter inside. The difference between this and port forwarding is that the DMZ will send all traffic that tries to get in to one specified machine. Port forwarding however works on pre specified ports or port ranges that can span multiple machines. You are basically placing this machine outside of military procetion zone of your router.

This is super scary cause all bad evil internet traffic can get in and wreck you. So do not do this on SOHO routers.

DMZs are used to protect public-facingservers by creating an isolated area for those devices.

Two firewalls are used in a DMZ : one allowing unsolicited traffic to the public service , and the second maintaining isolation of the private network.

Load Balancing : This is basically the act of being able to handle the amount of traffic that is being requested from them. The easiest way to do this is to just plug in more servers , all of which are serving the exact same content as the original. But now we need to spread the traffic out amongst all of these so as not to cause one to overload. This can be done in a variety of ways such as :

- DNS Load balancing : This can be done using DNS servers. We can send the information to the servers using a round robin scheduling algorithmn. If the servers are in different physical locations though (like different continents) then we want to use the server that would be physically the closest one.

- Server Side Load balancing :

9. References