Comp TIA A+ Core 1

▼ 24 / Feb / 2024

▼ Network Devices

- Different devices and components have different roles (Wireless router / switch / firewall) / SOHO routers

▼ Router

- Routes traffic between IP subnets (the router uses the IP address within the packets to determine to determine what the next hop might be, on its way to the final destination)
  - Because the routing takes place in the layer 3 of the OSI model we often refer to these as layer 3 devices
  - If we have a router that can be configured inside of a switch, u can refer to them as layer 3 switches
    - Makes forwarding decision based in IP address
- Routers can connect IP subnets that use the same topology
- Routers can also connect diffrent types of networks together
  - LAN, WAN, copper, fiber all on one single devices

▼ Switch

- Bridging done in hardware (Ex: Copper cable to plug in a swich)
  - Determines where traffic should be forwarded based on the destination MAC address (inside of the frame) / Forwards traffic based on data link address
  - Application-specific integrated circuit (ASIC) this allows for very fast throughput as all the decisions of traffic forwarding happens within the heart of the device
  - If you have a device that is in the core of a device, it can have either 10 or 100’s of interfaces on that switch in many switch cases they will also add additional power to the switch connection suing PoE (Power Over Ethernet)

- If the switch is able to turn on additional routing functionality , we refer to that as a multilayer switch

▼ Unmanaged switch

- Very few configuration options (Plug and Play)
- Fixed configuration (No VLANs) / all of the device will be on the same VLAN
- Very little integration with other devices and no other management protocol
- Has no SMMP capabilities, so although u can connect it to the network there could be no way to query the device or obtain performance information
- Low price point (simple is less expensive)

▼ Managed switch (office / larger organization)

Provides additional capabilities to someone who needs to confirm the device is working as expected

May allow u to configure differnt interfaces to be in completely different IP subnets, VLAN (different subnets)

Allows to prioritize traffic, (VOIP traffic can be set to a higher priority than FTP traffic)

Common for organisation to have multiple switches, to conect to their network one way which u could prevent loops between all of the switches is by enabling Spanning Tree Protocol (STP)

Port mirroring - where u can take traffic from one port in the switch, and copy the traffic to a different port on the switch, ideally to plug in a protocol analyzer to be able to view the packet traverse in the network . Used for troubleshooting an packet analysis

External management - Enable Simple network management protocol (another capability of a managed switch)

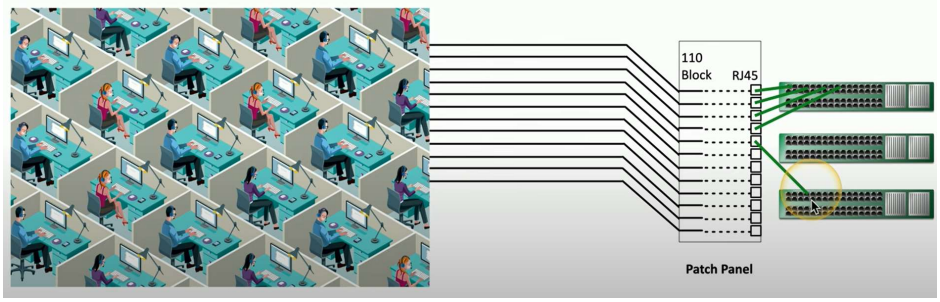
▼ Access Point (known as a bridge)

- Provides wireless connectivity for local networks (not a router). This only provides a link between the wireless and wired connection.

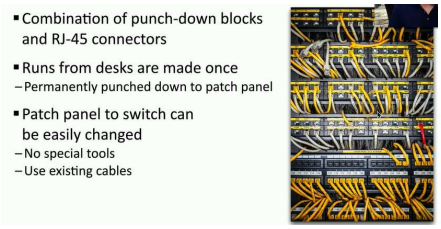
- An access point makes forwarding decision base don the destination MAC address (similar to switch) / Determines if the address is on the wireless network of it should be sent to the wired network.

▼ Cable infrastructure

1. All cables from the connections (every desk) go to a central wiring closet on that floor
2. In the wiring closet is a patch panel ← all the devices will be connected to the patch panel (this is a permanent run, as we dont tend to move that cable going forward)
3. RJ45 connectors (on the other sides) are extended to interfaces in switches in the other side of the wiring closet. This enables connections between desks nodes to the main infrastructure of a particular network.
4. If employee switch their desks, then u need to alter the connection between the switch and the RJ45 cable.



connection between a patch panel (top) and a switch



RJ45 side of a patch panel (inside of a wiring closet)

▼ 25 / Feb / 2024

▼ Network Devices

▼ Firewalls

(Allows and disables traffic flow from certain IP address and port numbers)

Filters traffic by the port number ← since the TCP and UDP ports operate at layer 4 of the OSI model, it is common to refer to firewalls as such as an OSI layer 4 device.

these days firewalls are able to understand application layer traffic, we call them a layer 7 device.

Some firewalls can also act as an endpoint for an encrypted tunnel. Which means that u can connect 2 sites together across a public network like the internet but all the traffic between the sites is encrypted.

Some firewalls can filter based on the application

Some firewalls can also act a proxy, so if someone is browsing a site on the internet the firewall will stop that communication, it will perform the browsing for the user, receive the response form that device over the internet, examine and make sure that nothing inside of that traffic maybe be dangerous or malicious and then send the results of that query back to the user,

And in many cases, probably like the SOHO type router used at home , this firewall can also cat as a router , this device is making forwarding decision based on the destination IP address therefore its acting as an OSI layer 3 device.

In many scenarios it is the firewall that is directly connected to the internet, so using that as a router allows for additionally functionality for forwarding traffic

▼ Power over Ethernet (PoE)

When using a laptop or desktop computer, we are accustomed to using a power source to power it up. There are some devices allow you to power that device using the ethernet cable that is already connecting to the device, we refer to this type of power as Power over Ethernet (PoE)

this allows you to run a single wire to the device that not only transfers data but also used as a power source for the device

- Power provided on an Ethernet cable
  - One wire for both network and electricity
  - Phones , cameras, wireless access points
  - Useful in difficult-to-power areas
- This type of power comes from the switch, we refer to these switches as Endspans (Built in power)
- If ur switch doesn't support PoE, it will require something in the middle in your connection that adds power to the ethernet cable , we refer to them as PoE injectors or Midspans

▼ PoE switch

Most switches will identify if they support PoE or not

▼ PoE, PoE+, PoE++

PoE

Original PoE specification → IEEE 802.3af-2003

This is now a part of the standard specification 802.3 ethernet standard

This provides 15.4 watts of DC power, 350 mA as max current

PoE+

specification → IEEE 802.3at-2009

This is also a part of the 802.3 standard

This provides 25.5 watts DC power, 600 mA max current

PoE++

specification → IEEE 802.3bt-2018

This provides (type 3) → 51 W, 600mA max current

(type 4) → 71.3 W, 960 mA max current

PoE with 10GBASE-T → This was a standard design to work with 10 Gigabit/s ethernet and provide power to those 10 Gig devices

▼ Hub

before switch we used Hubs to connect devices on the network

Known as a Multi-port repeater ← meaning that the hub is not an intelligent device, as the traffic going in one port is repeated to every other port

Half-duplex connection → Not efficient, as everything operates at half duplex

Becomes less efficient as a network traffic increases, since everything is being retransmitted to other ports

Outdated for modern devices as they are available in 10 megabit / 100 megabit speeds

▼ Cable modem

If your using the same cable for internet connection and cable television, u are using a cable modem.

Allows you to communicate in broadband communication as there are multiple frequencies of traffic beign used over a single wire. Hence we can connect phone lines , video signals, internet data

There is a standard for sending data on the cable network → DOCSIS (Data Over Cable Service Interface Specification)

Many cable modem can support up to speeds of 1Gigabit/s but what will be provided to you will be decided by your ISP.

Multiple services are available on these networks, hence we can connect to data / voice / video communication

▼ DSL modem

If your not using the cable company for your internet connection , you should be using the traditional telephone company to provide that connection , this is done through a DSL modem.

This is usually an → ADSL modem (Asymmetric Digital Subscriber Line) / uses the same telephone lines that we use for our analog telephone.

The reason we call asymmetric is cuz the speeds for downloading is much faster the speeds for uploading (52 Mbit/s downstream and 16Mbit/s upstream). There is also a distance limitation with DSL before the signal gets so weak that ur not able

to receive any data (This is usually 10,000 feet from the central office (CO)). Speeds are relative the distance which you are at from the CO, closer the faster

▼ ONT

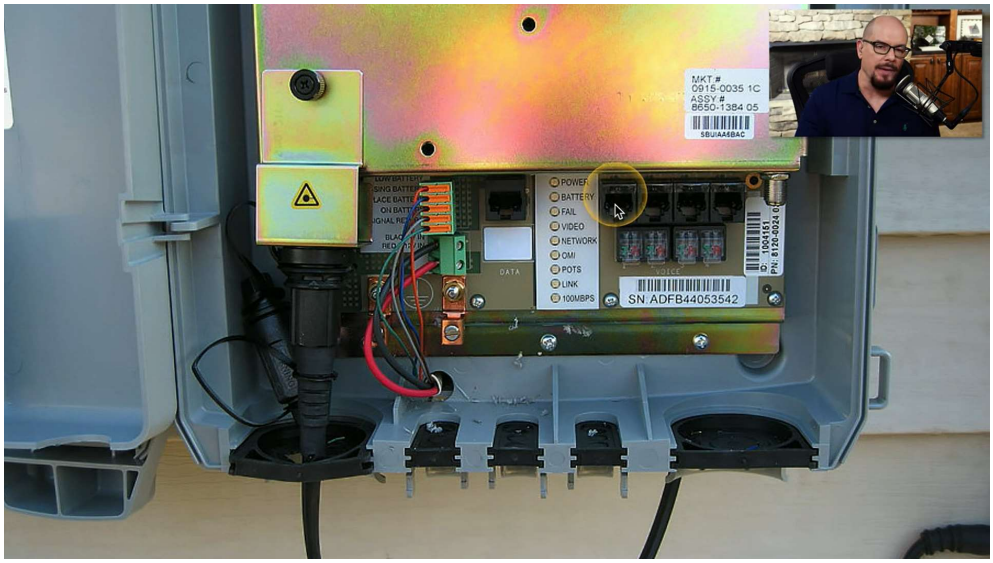
If you are not connected to the internet using copper or telephone lines, then you are using fiber.

To connect to the network you need an ONT (Optical Network Terminal) which is a device that is connected outside your home / premise

This connects an ISP fiber network and converting it to a copper ethernet signals that can be used inside your home

This ONT delineate the ISP's network from your own internal network. We describe this delineation as the Demarcation point (demarc) in the data center

Demarc is an important component as this specifies the responsibilities are for each party , you know that any of the wiring inside your house is your responsiblilty and anything outside is responsibility of the ISP



This is an ONT

▼ NIC (Network Interface Card)

If you are connecting to a copper-ethernet connection your using a NIC

Every computer on the wired ethernet connection have a NIC

Used in computers, servers, printers …

Specific to the network types of Ethernet, WAN, wireless

Often build into the motherboard or added as an expansion card

so whether u need copper connectivity or fiber connectivity (Single port, multi-port, copper, fiber) u always need a NIC.

▼ Software Defined Networking

▼ 26 / Feb / 2024

▼ SDN (Software Defined Networking)

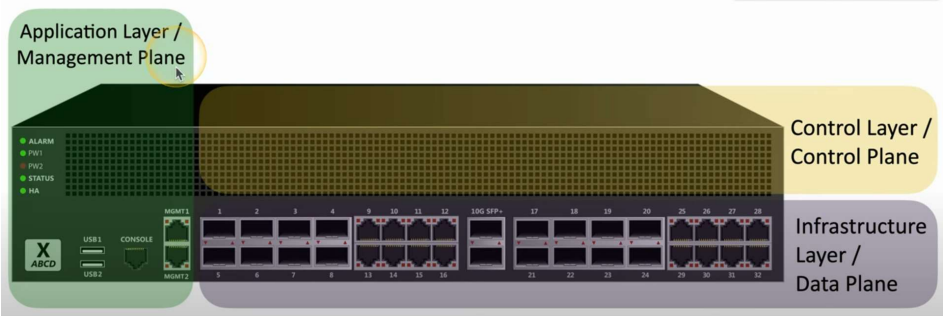
Since we dont have physical router in the cloud, instead we need to take these networking platforms we use in real world and move them into the virtualized cloud based environment, few ways to do this:

1. SDN ← Networking devices have different functional places of operation (Data, Control, Management planes). We take the devices routers, switches and firewalls and other networking devices and change them to be a software based platform which we can use in the cloud
    a. Ex: Dissecting each functionality of a switch into separate software that can be used to serve its functionality in the cloud
2. There are 3 layers to separate these devices so that we can create consistency between all of these networking components.
    a. Infrastructure layer / Data plane ← *Process the network frames and packets. Forwarding , trunking, encrypting, NAT*
    b. Control layer . Control plane ← When the routers and switches need to forward this traffic in the data plane, they need some type of reference to know where this traffic will be going. Most of these references will be in the control layer. Hence this *manages the actions of the data plane. Routing tables, session tables, NAT tables. Dynamic routing protocol updates.*
    c. Application layer / Management plane ← Another process has to be in place to manage that device we need to login or access the device via an API all of this

access is provided at the application layer. *Used to configure and manage the device.* SO when u SSH into a router u bring a graphical front end of a firewall you're managing that device from the management plane. *SSH, Browser, API*

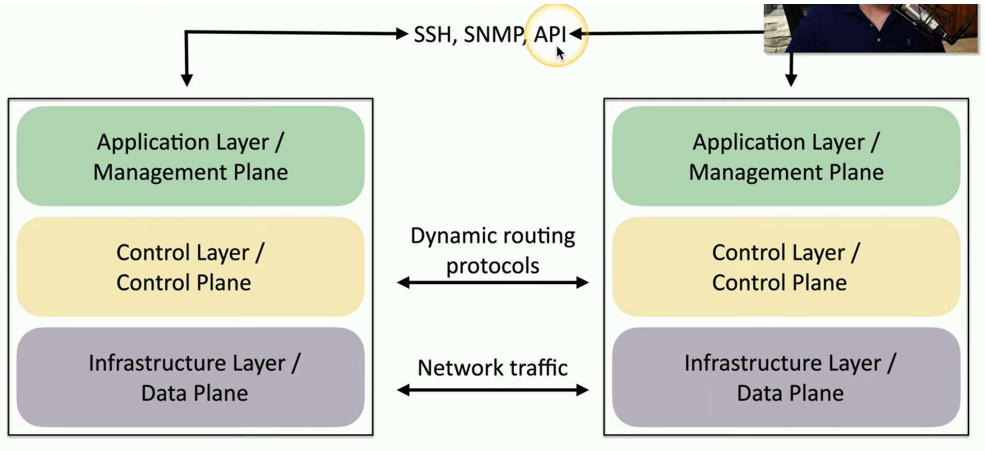
Example of Switch

1. Traffic forwarded between different interfaces on a switch all occurs in that data plane (a software version will be made on anything that will be used to forward traffic) → Infrastructure layer
2. Data income and forwarding structure and instructions of that data → Control layer
3. Management of device through a console port or management interface and that section of the device is the → Application layer



SDN data flows

- This creates modular layers that u can extend between devices, or create new devices all based on the SDN network
- Each layer can be managed by its respective protocols and traffic accordingly, this allows for communication to occur seamlessly between other device connected as well. Building blocks of a larger system capability



▼ Wireless standards

▼ Standards

Wireless networking (802.11) ← managed by IEEE LAN/MAN standards committee (IEEE 802)

Many updates have occurred, hence various versions. Wi-Fi Alliance body handles the interoperability testing, hence the Wi-Fi trademark is controlled by such.

- 802.11a
  - Original wireless standards (October 1999)
  - Operates in the 5GHx range ← or other frequencies with special listening
  - 54 Mbit/s
  - smaller range than 802.11b ← Higher frequency is absorbed by the objects this way
- 802.11b
  - Also an original 802.11 standard (October 1999) / this is not a update but a whole different system
  - Operates in the 2.4 GHz range
  - 11 Mbit/s
  - Better than 802.11a range (in contrast the signals bounce off rather than being absorbed, this improves range)
  - More frequency conflict ← baby monitors, cordless phones, microwave , Bluetooth
  - Not commonly seen today

- 802.11g
    - An upgrade to 802.11b (June 2003)
    - Operates in the 2.4 GHz range
    - 54 Mbit/s (similar to 802.11a)
    - Backwards compatible with 802.11b
    - Same 2.4GHx frequency conflict problems as 802.11b
- 802.11n (Wi-Fi 4)
    - The update to 802.11g, 802.11b, 802.11a (October 2009)
    - Operates at both 5GHz and 2.4GHz (40 MHz channel widths)
    - 600 Mbit/s ← 40 MHz mode and 4 antennas
    - 802.11m uses MIMO ← Multiple-input multiple-output
        - Multiple transmit and receive antennas. this means device can transfer much more information simultaneously between the end station and the access point
- 802.11ac (Wi-Fi 5)
    - Approved in January 2014
    - Significant improvement over 802.11n
    - Operates in the 5GHz band ← Less crowded, more frequencies (up to 160 MHz channel bandwidth)
    - Increased channel bonding ← larger bandwidth usage
        - Greater wireless spectrum up to 160MHz, this translates into more channels that can be used simultaneously and therefore more data that can be transferred over the wireless network simultaneously
    - This standard also changes how information is transferred over that wireless network we refer this as, Denser signaling modulation ← means faster data transfers at any time
    - Eight MU-MIMO downlink streams (Multiple Users can be communicating over MIMO)
        - Twice as many streams as 802.11n
        - Nearly 7 Gbit/s

    - If u find access points that operate at 802.11 ac at 5GHz and 2.4GHz in those cases the communication that occurs at 2.4GHz actually occurs at 802.11n standard and the 5GHz uses 802.11 ac standard
- 802.11ax (Wi-Fi 6)
    - Approved in February 2021 (The successor to 802.11ac / Wi-Fi 5)
    - Operates at 5 GHz or 2.4GHz (20,40,80 and 160 MHz channel widths)
    - 1,201 Mbit/s per channel
        - A relatively small increase in throughput
        - 8 bi-directional MU-MIMO streams
    - This standard was designed differently → Orthogonal frequency-division multiple access (OFDMA). Solves the problem of scrambling in wireless networks as a result of high density signals such as in sporting events or trade shows
        - Works similar to cellular communication
        - Improves high-density installations

	Frequencies	Maximum MIMO streams	Maximum theoretical throughput (per stream)	Maximum theoretical throughput (total)
802.11a	5 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	Not applicable	11 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11n	5 GHz / 2.4 GHz	4 x MIMO	150 Mbit/s	600 Mbit/s
802.11ac	5 GHz	8 x DL MU-MIMO	867 Mbit/s	6.9 Gbit/s
802.11ax	5 GHz / 2.4 GHz	8 x DL and UL MU-MIMO	1,201 Mbit/s	9.6 Gbit/s

Summary

▼ Wireless instruments

Long Range fixed wireless

Wireless access point in house with stock antennas (range of 40 50 meters)

Try connecting 2 buildings located miles from each other → Fixed directional antennas and increased signal strength

Outdoors → Minimal signal absorption or bounce

Directional antennas → Focused, point-to-point connection

wireless regulations are complex → refer to your country's regulatory agency

Frequency use

- Unlicensed 2.4GHz or 5GHz frequencies
- Additional frequencies may be available
- Additional licensing may be required

Signal strength (indoor and outdoor power is usually regulated)

Outdoor antenna installation is not trivial (Get an expert to do a safe job)

RFID (Radio Frequency Identification)

- Access badges
- Inventory / Assembly line tracking
- Pet / Animal identification
- Anything that need to be tracked

  Uses Radar technology

  - Radio energy transmitted to the tag
  - RF powers the tag, ID is transmitted back
  - Bidirectional communication
  - Some tag format can be active/powered

NFC (Near Field Communication)

Two-way wireless communication

- Builds on RFID, which is mostly one-way

Payment systems

- Major credit cards
- Online wallets

Bootstrap for other wireless

- NFC helps with Bluetooth pairing

Access token, identity "card"

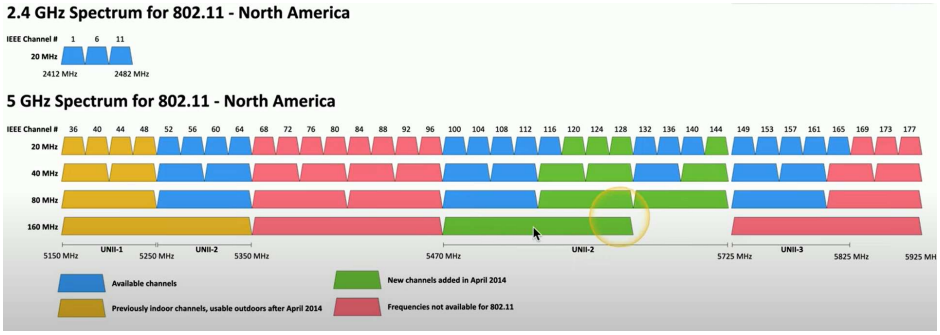
- Short range with encryption support

▼ 27 / Feb / 2024

▼ Wireless Network Technologies

▼ 802.11 Technologies

- Frequency → 2.4GHz or 5GHz (Sometime both)
- Channels are within these frequencies ranges.
  - These are groups of frequencies, numbered by the IEEE, so that we can easily refer to which channes we happen to be using.
  - This is we say when using multiple access point in an area we may want to make sure each of the access points are running on a different wireless channel
- Regulations. Depending on where you are situated
  - Most countries have regulations to manage frequency use.
  - Spectrum use, (max) power output, interference requirements



▼ Bluetooth

- Communicates using 2.4 GHz range
  - Bluetooth uses the unlicensed ISM part of the band (Industrial, Scientific and Medical). this is an area of the 2.4GHz band that require you to get any special licensing from the government as they are free to use by anyone.
  - Same as 802.11
- Short range
  - Most consumer devices operate to about 10 meters (PAN)
  - Industrial Bluetooth devices can communicate over 100 meters

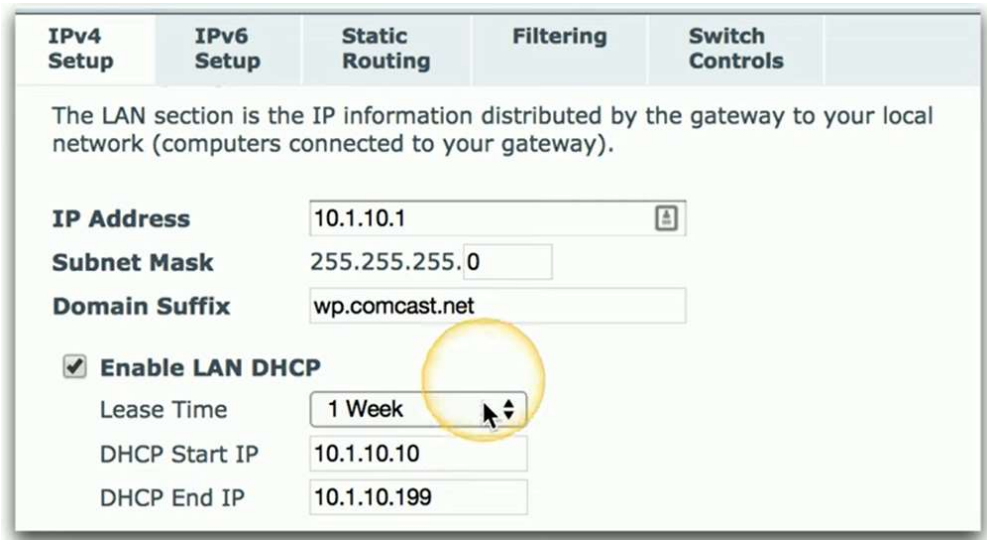
▼ Network Services

▼ DNS server (Domain Name System)

- Responsible for converting names to IP addresses and vice versa.
- DNS is a distributes naming system → meaning you will have many different DNS servers in your environment and outside your organization you may be communication with other DNS servers as well.
- this conversion process is usually managed by the ISP or enterprise IT department.

▼ DHCP server (Dynamic Host Configuration Protocol)

- Automatically assigns IP address configuration on you local device
- Very common services as we can automatically obtain IP address to communicate in that network.
  - If you have a modem wireless router , for internet connectivity then that is also running a DHCP server inside of it.
- Enterprise DHCP here you will find multiple DHCP servers, provide redundancy when one DHCP server becomes unavailable.



Home router configuration DHCP server / Lease time → after 1 week the IP will be renewed / IP range is provided

▼ File Server

- Centralized storage of documents, spreadsheets, videos, pictures, and any other files. (fileshare)

- Standard system of file management.
    - The OS has a common way of communicating with the file server.
    - Windows → SMB (Server Message Block)
    - Apple → Apple Filing Protocol (AFP)
- The front-end hides the protocol (Copy, rename, delete) → in the users perspective hey have no idea what protocols are use don’t the network, all they see is the file management front end.
-

▼ Print Server

- In an enterprise environment we connect printer to the network and put those printers in a centralized area close the other users.
- Connect a printer to the network by using a print server
    - This is a hardware or software that allows us to connect the printer to the network so everyone can access the centralized resource.
- This can be a software that’s running on a computer that has a printer connected to it. so everyone on the network will send their print jobs to this computer, which will be accessed by the print server and proceed with the print jobs
- This can be a hardware card. That allows the printer to be connected directly by an ethernet connection (some has wireless as well).
- Standard protocols that govern printing
    - SMB (Server Message Block)
    - IPP (Internet Printing Protocol)
    - LPD (Line Printer Daemon)

Hardware card, that connect via ethernet

▼ Mail Server

- Responsible for sending and receiving mail for your organization as well as storing
- Managed by the ISP or enterprise IT department → Complex set of requirements are in place
- Usually one of the most important services → there is 24 x 7 support

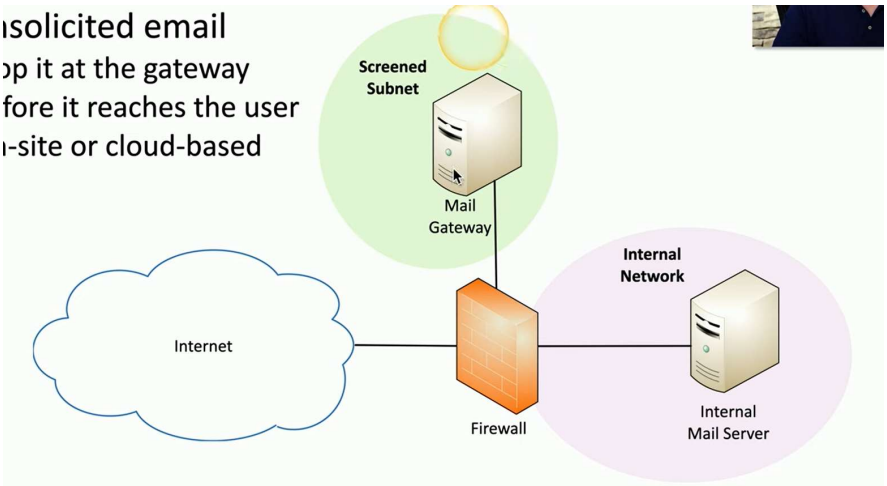
▼ Spam

- Takes any unsolicited messages
- Various content → Phishing attacks, Non-commercial proselytizing
- Significant Technology issue as identifying spam msgs will not be an easy task, after identification the space required (storage costs, resource utilization) all will be technology constraints

▼ Spam Gateways

Unsolicited emails are stopped at the gateway before it reaches the user. This could be on-site or cloud based.

Once the mail is scanned it will then be sent to the Internal network and stored on the local internal mail server, this gives the option to categorize mail as spam or reject its access to the mail server



▼ Syslog

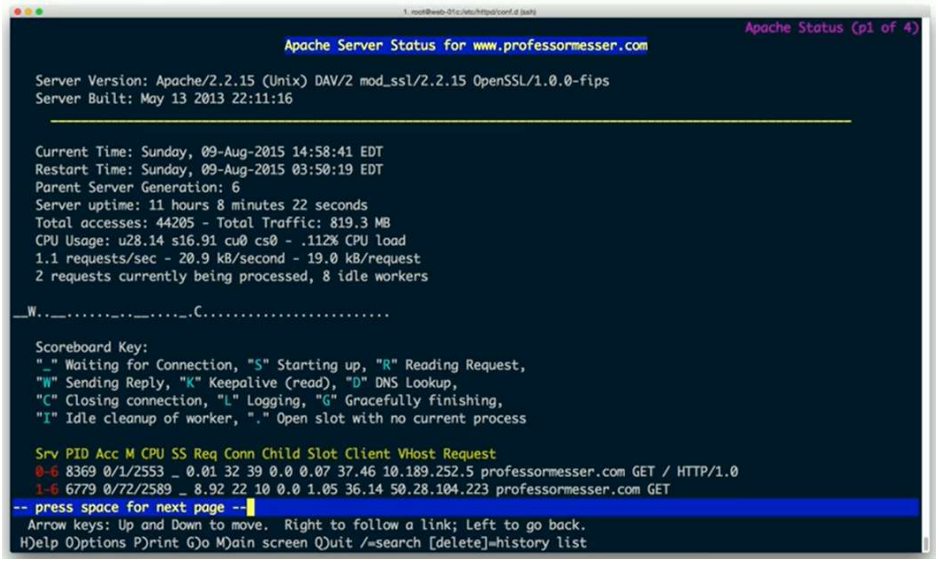
After the number of the servers we talked about previously, in each of these systems there are logs and messages that are important for administrators to have access to.

Syslog → A Protocol that enables logs and messages from various servers/ services to be sent into a central database, eliminating the hassle of individually accessing the logs.

- Standard for message logging
  - Diverse systems, consolidated log
- In many organizations we use a central logging receiver → this is integrated into the SIEM , to collect all the log files
- Since log files require a lot of space, SIEM takes a lot of disk space

▼ Web Server

- Respond to browser requests → Using standard web browsing protocols (HTTP / HTTPS)
  - Pages are built with HTML , HTML5
- Webpages are stored on the server
  - These could be static or built dynamically in real-time which is then sent to the browser



▼ Authentication Server

- An enterprise uses this server to streamline all the login authentication to resources to various servers using this one server → Centralized management
- Always used in an enterprise network
- Usually s set of redundant servers, since its always available and is an extremely important device

▼ All-in-one security appliance

- Next-generation Firewall, Unified Threat Management (UTM) / Web Security gateway
- Includes features such as:
  - URL filter / Content inspection facilities are available
  - Malware inspection, Spam filter
  - Other networking features → CSU / DSU
  - Often act as routers and switches
  - And built in firewalls
  - Can often act as IDS / IPS
  - Bandwidth shaper
  - VPN endpoint

▼ Load Balancer

- Enterprises are very sensitive to downtimes, if a server becomes unavailable it will cause the functionality of the user to be halted.
- To distribute the load you will need load balancers, this can be done by:
  - Multiple servers which will abstracted / Invisible to the end-user
- Large-scale implementations
  - Web server farms, database farms
- Fault tolerance
  - Server outages have no effect / Very fast convergence

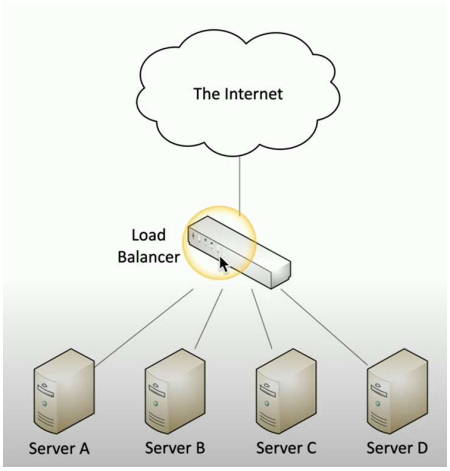
▼ Load balancer features

Installed with the primary function of distributing the load to multiple servers.

- Configure load → Manage across servers

Since this device is sitting centrally it is able to take action into the different ways how the protocols might work

- TCP offload → protocol overhead
- SSL offload → encryption / decryption (this will take place in the load balancer instead of the servers)
- Caching → fast response / so that the responses does not need to go down to the server as the reply may already be available in the load balancer
- Prioritization → We can perform advanced configuration of traffic so that certain websites are prioritized (QoS)
- Content switching → Application-centric balancing, this is where certain applications , websites are being handled by separate servers. This capability allows for optimized communication with the servers that can respond the best



▼ Proxy Servers (Extra layer of security)

An intermediate server

Users will make a request to the proxy server, the proxy then makes a request to the 3rd party service receives a response form the service, examines the response, to ensure nothing within the response is malicious, after scanning it is then sent to the end user.

- Client makes the request to the proxy
- The proxy performs the actual request
- The proxy provides results back to the client

Useful features

- Access control, caching
- URL filtering, content scanning

▼ SCADA / ICS (managing software for devices)

Supervisory Control and Data Acquisition System

Large-scale, multi-site Industrial Control Systems (ICS)

Responsible for control and management of these industrial machines (Ex: large companies with manufacturing equipment use SCADA to manage their devices)

PC manages equipment → Power generation, refining, manufacturing equipment, Facilities, industrial, energy, logistics

Distributes control systems → Real-time information, System control

Requires extensive segmentation (No access from outside)

▼ Legacy and Embedded systems

- Legacy systems (really old)
- They remain cuz once a service is installed it is very difficult to remove that service from the data center, we refer to these systems as legacy systems
  - However they can be really important
  - Since they are old it can be difficult to resolve a software or hardware issue
  - Learning old things can be just as important as learning new things
- Embedded systems
  - Purpose built device (alarm system door security, time card system)
  - Not usual to have direct access to the operating system, cuz the we are dependent on the manufacturer of the O.S. to give updates
  -

▼ IoT (Internet of Things) devices

- Appliances → Refrigerators
- Smart devices (smart speaker responding to voice commands)
- Air control (Thermostat, temp control)
- Access (Smart doorbells)
- May require a segmented network (Limit any security breaches)

▼ 28 / Feb / 2024

▼ IPv4 and IPv6

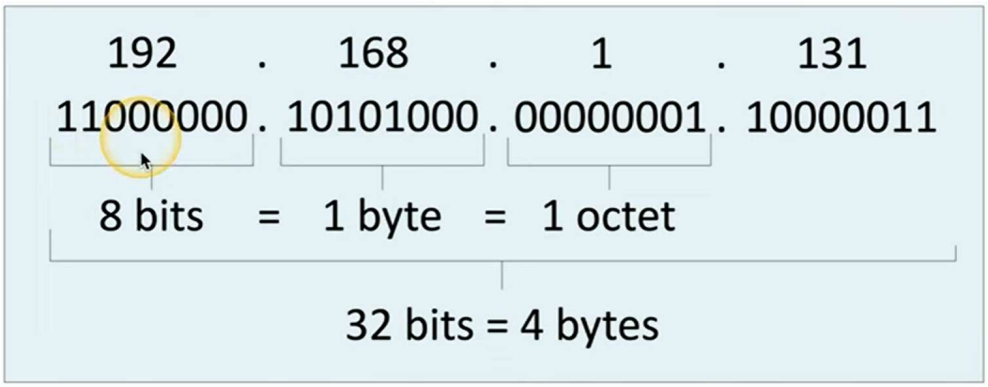
Compulsory for communicating over devices in a network

IPv4 is the primary protocol for everything we do in todays networks (Included in almost all configurations)

IPv6 is now part of all major operating systems (And the backbone of our internet infrastructure)

▼ IPv4 addresses (32 bits)

Internet Protocol version 4 (OSI Layer 3 address)



Since one byte is 8 bits the maximum decimal value for each byte is 255

▼ Networking with IPv4

IP address, eg:192.168.1.165

- Every device needs a unique IP address

Along with the IP address we need to assign the subnet mask, both of these are necessary to produce an IP

Subnet mask, eg:255.255.255.0

- Used by the local device to determine what subnet it's on
  - The subnet mask isn't (usually) transmitted across the network
  - You'll ask from the subnet mask all the time

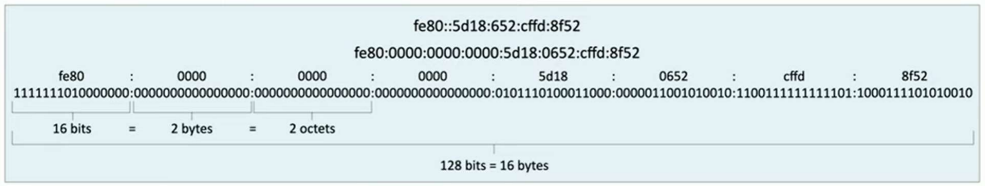
Default gateway, eg:192.168.1.1

- This enables router to communicate outside of your local subnet
- The default gateway must be an IP address on the local subnet

▼ IPv6 addresses (128 bits)

Internet Protocol v6 (128-bits addresses)

- 6.8 billion people could have 5 x 10^27 addresses each.

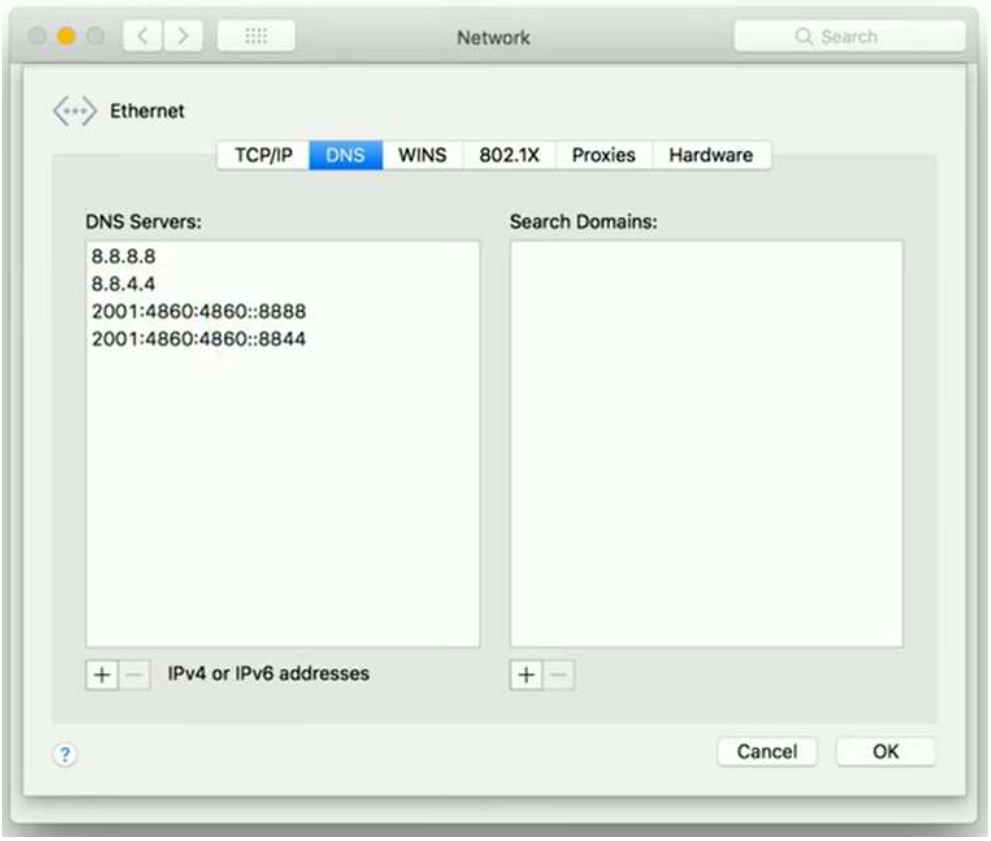


- since the address is difficult to remember the DNS is vital
- First 64 bits is generally the network prefix (/64)
- Last 64 bits is then the host network address

▼ DNS servers

- We remember names not remember the IP address, hence DNS abstracts this process
- Since internet router don’t know names, as Routers only know IP address
- Something has to translate between names and IP addresses (Domain Name Service)

You configure 2 DNS servers in your IP configuration. In case if one goes down, it is that important.



Both the servers are managed by google (8.8.#.#.)

▼ Assigning IP addresses

▼ DCHP

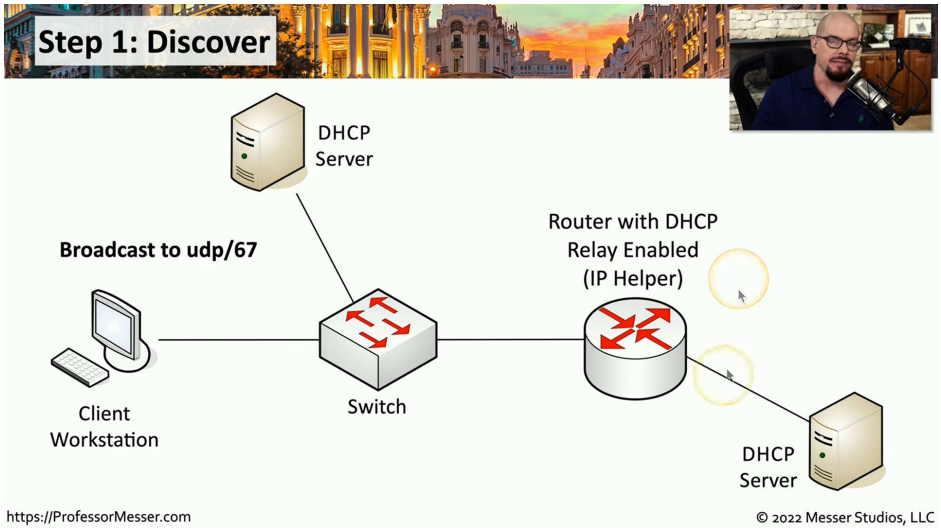
IPv4 Address configuration used to be manual

- IP address, subnet mask, gateway, DNS servers, NTP servers, plus more.
- October 1993 → The bootstrap protocol (BOOTP)
  - Built to automatically assign IP address, with the mishap of :
  1. BOOTP didn’t automatically define everything
  2. Some manual configuration were still required
  3. BOOTP also didn’t know when an IP address might be available again
- Dynamic Host Configuration Protocol (DHCP) / (Revision of BOOTP)
  - Initially release din 1997, updated through the years
  - Provides automatic address / IP configuration for almost all devices

▼ DHCP process

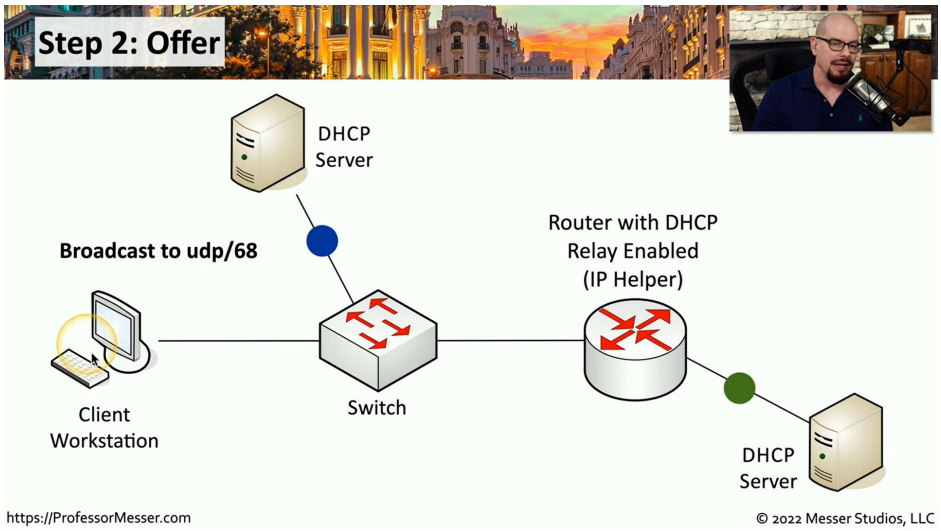
- DORA (4 step process)

1. Discover → Trying to locate a DHCP server on the local network



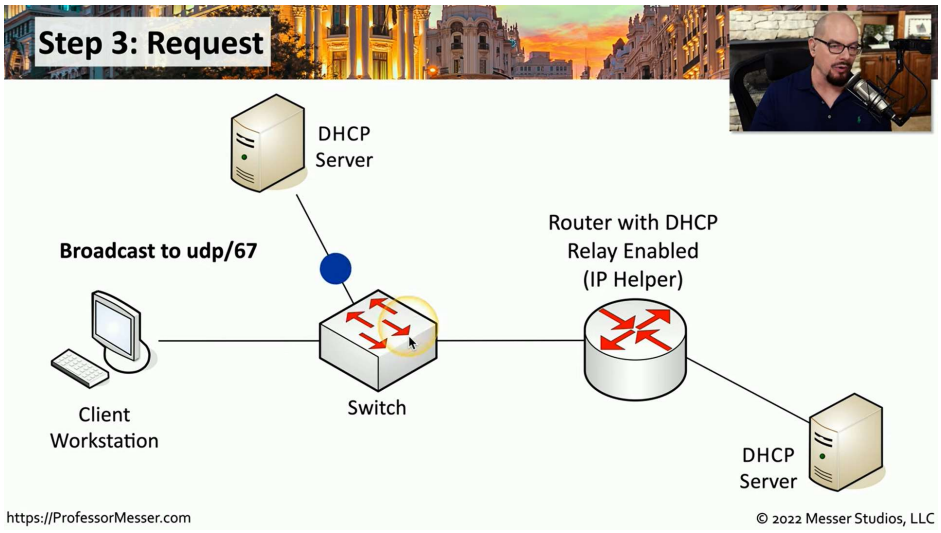
Client sends out Broadcast to UDP/67. Another thing to note is that routers dont send broadcast, but the one used here is configured as a DHCP proxy (DHCP Relay/IT helper) this is preconfigured before used so any broadcast received is forwarded to the DHCP server

2. Offer → where a DHCP will offer an IP address to our device.



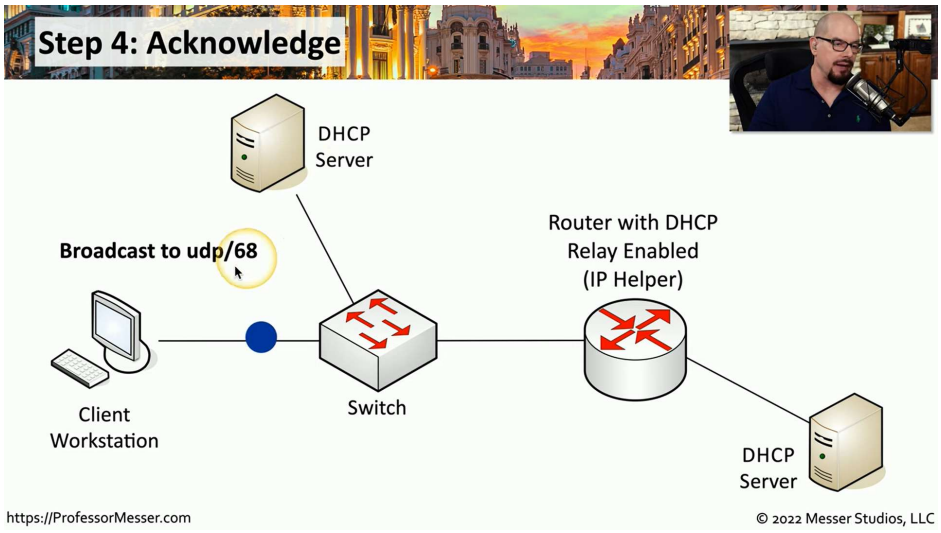
Offers are sent back to the user in Broadcast to UDP/68, reason of using broadcast is that the client still doesn't have an IP address. It can then examine the offer its going to take

3. Request → Our device will then look at one from the many offers we receive and pick one of the offers and request that IP address from the offering DHCP servers



Another broadcast request is sent, which contains a formal request, to take the offer that was originally sent. Although one signal is shown, this broadcast signals travels throughout the subnet

4. Acknowledge → DHCP confirmation, and provide your device with all the IP configuration settings it needs



Server sends a message back to the client on Broadcast UDP/68, confirming the request from the previous phase has been acknowledged and the device can now assign itself with the configuration settings included in the offer

The 4 step DORA process occurs every time a device connects to the network

▼ Turning Dynamic into Static

DHCP assigns an IP address form the first available from a large pool of addresses (Your IP address will occasionally change)

You may not want your IP address to change, such when some devices will want the same IP address every time it connects to a network (Such as server, printer, personal preference)

- One way to counter this is to disable DHCP on the device.
  - Configure the IP address information manually
  - Requires additional administrational authorization
  - In large environments this won't be practical
  - Instead of manually configuring an IP, we can configure a reservation on the DHCP server this means we will configure a specific MAC address of a printer , server and tell the DHCP server that every time it sees this MAC address to give the same IP address

▼ Avoid Manual Configurations

Because there will be no DHCP reservations, as you can configure the IP address manually.

Difficult to change later, you must visit the device again. When u need to make changes to the IP addresses you will have to do it one by one.

As a result using a DHCP reservation is preferable as you can change the IP address rom the DHCP server.

▼ APIPA → Automatic Private IP Addressing

There will be times when your device is configured to obtain a DHCP address, but on your local network, there is no longer a DHCP server. In that situation your device will be assigned an APIPA address.

Also known as a link-local address (No forwarding by routers)

- Because any device that is configured with an APIPA address range can only communicate to other devices on the local network.
- Hence an device with an APIPA address cannot communicate outside the network

There is a standard for APIPA the entire range is reserved from IETF 169.254.0.0 through 169.254.255.255

- First and last 256 addresses are reserved
- Functional block of 169.254.1.0 through 169.254.254.255

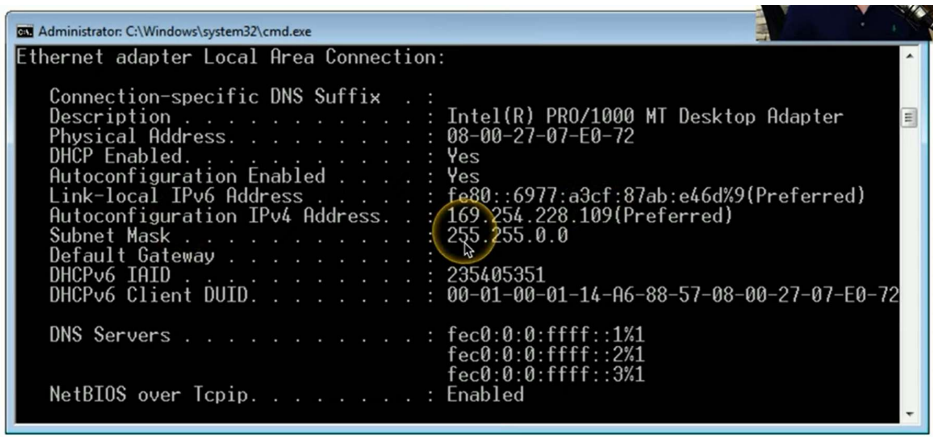
- If u see this IP addresses we can assume that a DHCP server was not available

Like DHCP APIPA addresses are also assigned automatically, hence only our local device will determine what IP address it will receive

How does it work:

1. Your device will automatically pick a random address between the range
2. Perform ARP (Address Resolution Protocol) to ensure anyone else on the local network is using this IP address, if no response is received it assigns as the address

   From this picture we can identify the following:



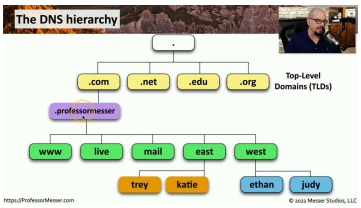
1. Mentions “Autoconfiguration” enabled / 2. Default subnet mask is provided of APIPA 3.Default gateway option has been left blank.

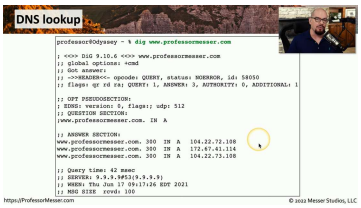
▼ 29 / Feb / 2024

▼ DNS Configuration

▼ Domain Name System

- Translates human-readable names into computer readable IP addresses. This is not a stand-alone server that provides this resource, as there are multiple servers across the world that provide these translations and they work on a hierarchy basis on all of the FQDN’s
- Distributes database because there are many different DNS servers
  - 13 root server clusters (Over 1,000 actual servers)
  - Hundreds of generic top-level domains (gTLDs) → .com .org .net, etc.
  - Over 275 country code top-level domains (ccTLDs) → .us .ca .uk, etc



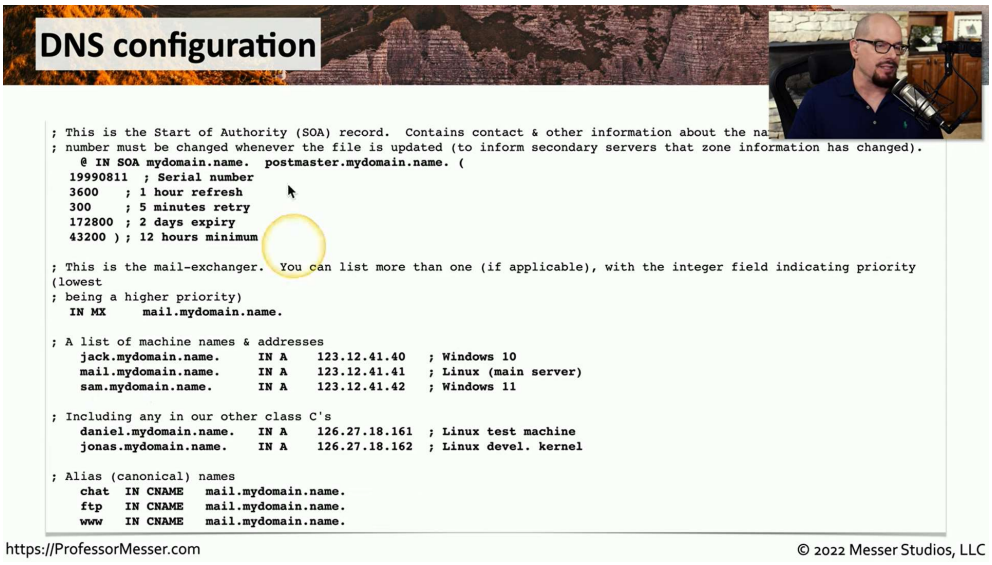


-

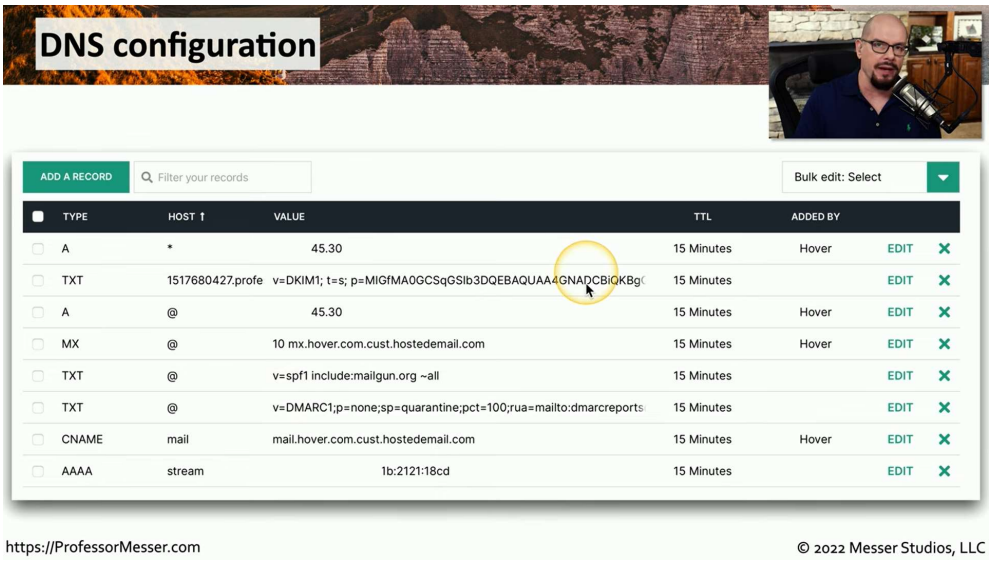
▼ DNS records

Resource Records (RR) → The database records of domain name services, FQDN’s

- Over 30 record types are available → IP addresses, certificates, host alias names, etc
- These are important and critical configurations → Make sure to check your settings, backup, and test. This is why it is important to have backup of the previous configurations so that in case of modification or change you can always ensure and check what u have changed.



Configuration file written in text (Useful in modifications)



Web-based front-end of DNS configuration (Much more easier to understand)

▼ Address Records (A) / (AAAA)

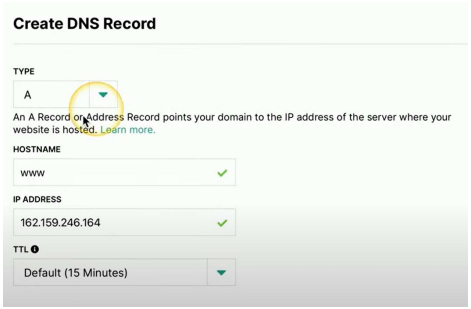
Defines the IP address of a host (This is the most popular query)

The A records are for IPv4 addresses (Modify the A record to change the host name to IP address resolution)

AAAA records are for IPv6 addresses (The same DNS server, different records)

```
www.professormesser.com.    IN A    162.159.246.164  ; Professor Messer
```

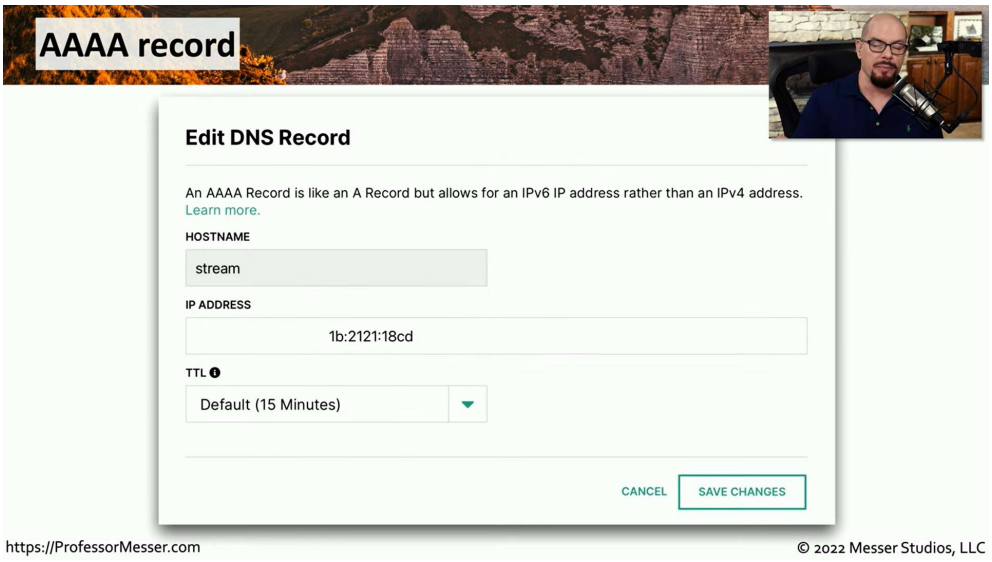
TTL (Time To Live) → How long an end station will remember this match between fully qualified domain name and IP address.



Web-based

This 15 minute TTL specifies that:

1. The device will make a request to the DNS server, and store or cache that information for 15 minutes.
2. After 15 minutes that info, is removed from the cache, and if this device needs to communicate back the www.server.
3. It will need to request again, the IP address for that particular record.



Configuring an IPv6 record

▼ Mail Exchange record (MX)

Another important record in the DNS is where all your emails should be delivered. This is as the name suggest, is a mail exchange record. To make this work:

- You will need 2 separate records inside your DNS:
  - The first would be the MX record → You could see the mail exchange record in this server points to mail.mydomain.name
  - To be able to obtain the IP address for mail.mydomain.name, we need to look at A record

Determines the host name for the mail server (This isn't an IP address, it's a name)

```
; This is the mail-exchanger.  You can list more than one (if applicable),
; with the integer field indicating priority (lowest
; being a higher priority)
  IN MX   mail.mydomain.name.

; A list of machine names & addresses
    jack.mydomain.name.     IN A    123.12.41.40   ; Windows 10
    mail.mydomain.name.     IN A    123.12.41.41   ; Linux (main server)
    sam.mydomain.name.      IN A    123.12.41.42   ; Windows 11
```

▼ Text Records (TXT)

DNS servers have many different function one of which is to save txt info. TXT record

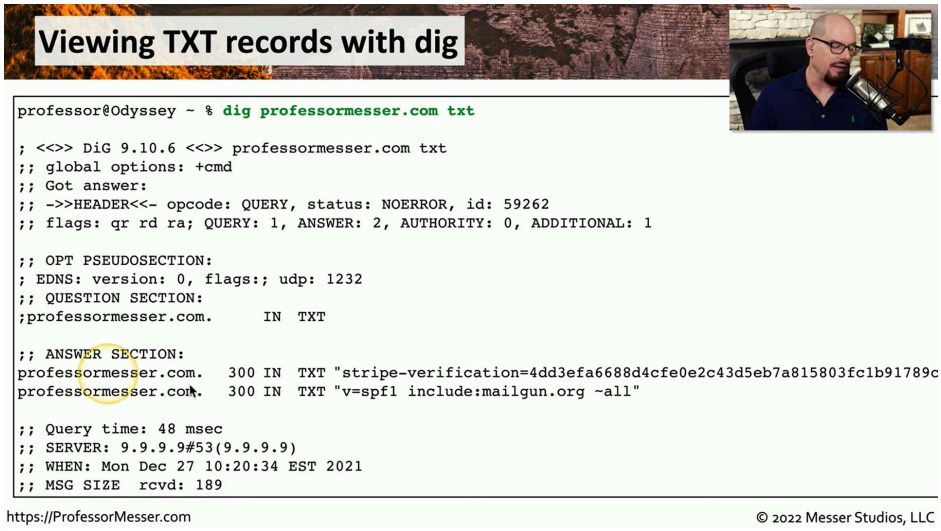
Human-readable text information (Useful public information, Was originally designed for informal information)

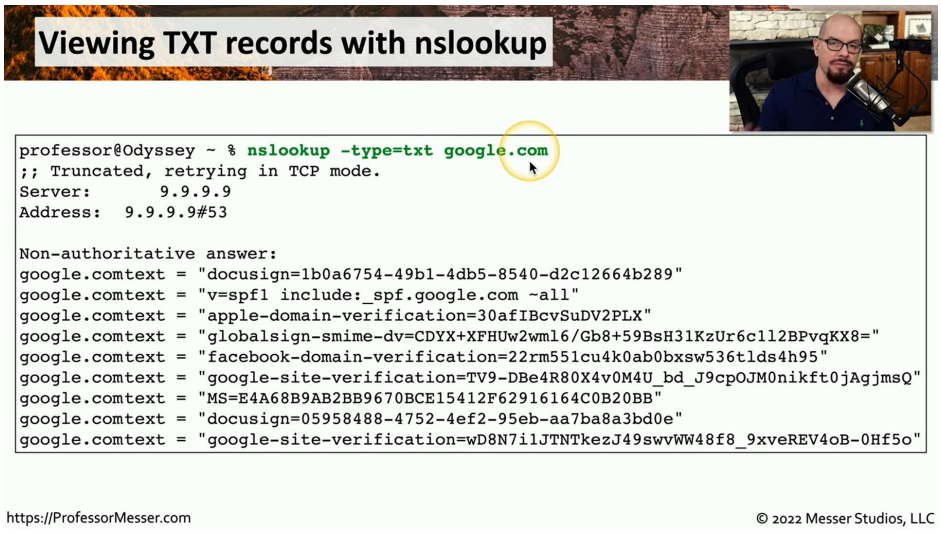
Can be used for verification purposes.

- If you have access of the DNS, then you be the administrator of the domain name
- When making a config change to our domain, and that domain change requires that u add something very specific to a text record in your DNS server.

Commonly used for email security.

- External email servers validate information form your DNS





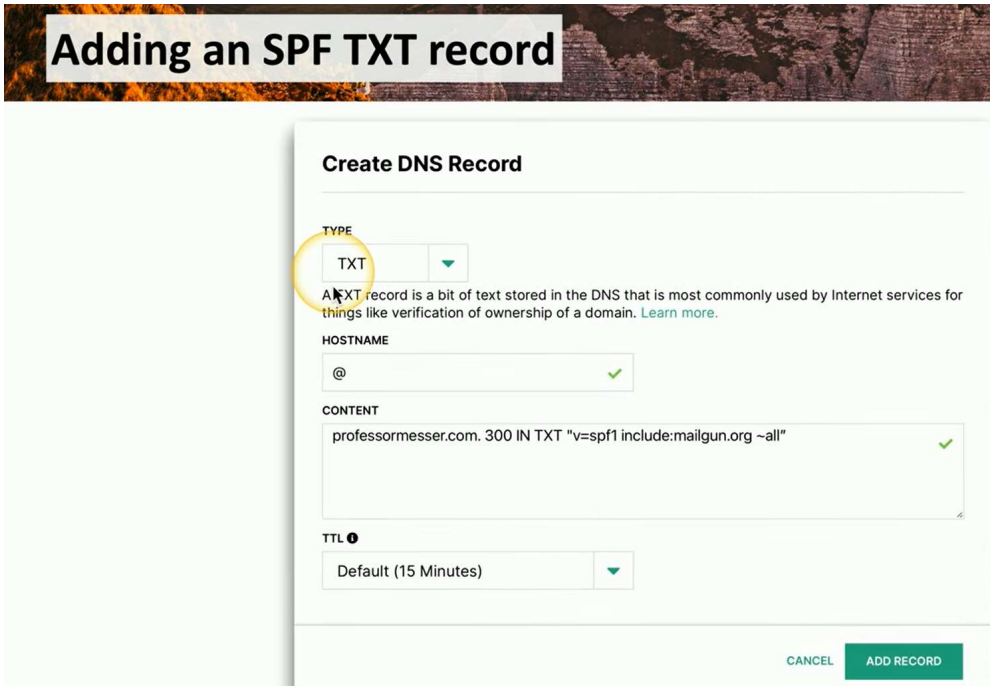
2 different way to inspect TXT records

▼ Sender Policy Framework (SPF)

A common TXT record you will find is a SPF record

SPF protocol

- A list of all email servers authorized that are authorized to send messages using your FQDN
- Was built to prevent mail spoofing your FQDN and send email as if you would send it to yourself
- A mail server receiving an email says it was from professormesser.com will query the professormesser.com DNS server retrieve the SPF record in the DNS server, and be able to determine is this something that really came from an authorized host ?



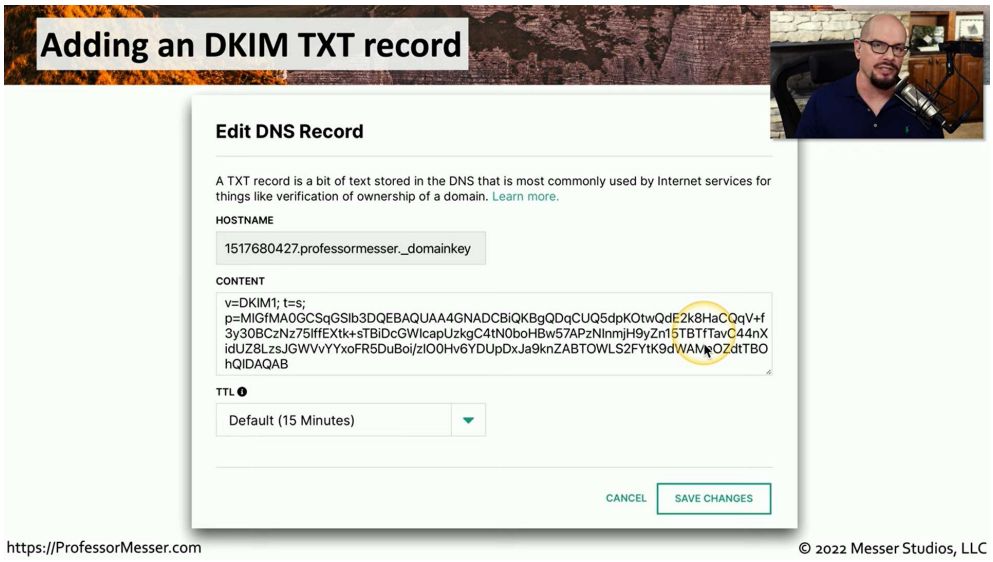
Creating a text based DNS record

- Mail servers perform a check to see if incoming mail really did come from an authorized host

▼ Domain Keys Identified Mail (DKIM)

When we take this email security one step further, and provide a digital signature that we can, associate with outgoing mail.

We do this through the use of DKIM text record. This is going to be validated by the mail servers as that message is traversing the network, and the public key associated with this digital signature, is added to a text record in your DNS server

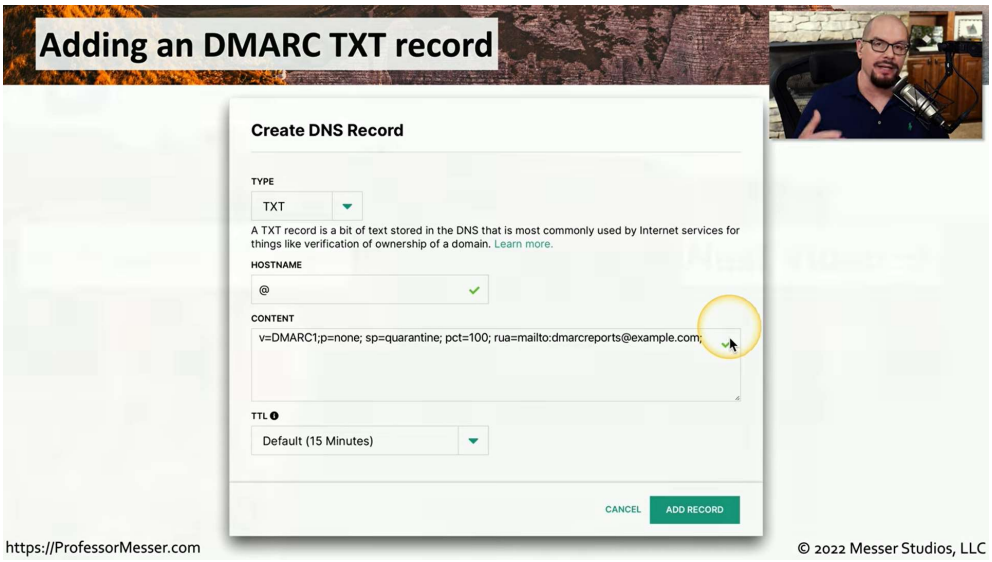


These are the public keys for all digital signatures that have been sent from my domain

▼ DMARC (Domain Based Message Authentication, Reporting, and Conformance)

Now that we have a way to verify messages that have been sent, and to digitally sign messages that have been sent, we need some way to determine what we do with those messages, if the verification fails. This is when we will use DMARC

- Prevent unauthorized email use (spoofing) . An extension of SPF and DKIM process we saw before except that DMARC takes the extra step to determine the deposition that should be used when someone receives a message that can’t be validated
- You decide what external email servers should do with email that don’t validate through SPF or DKIM
    - That policy is written into a DMARC TXT record
    - Accept all, send to span, or reject the email
    - Compliance reports can be sent to the email administrator
- Mail servers keep a track of validated and rejected mails, which could be helpful in producing you a report . This will show how many were able to get through based on the DKIM or SPF configuration
-



Content shows what to do with your email messages and where to send the report so that u can examine how your mail is distributes

▼ 01 / Mar / 2024

▼ DHCP Configuration

▼ DHCP Configuration

We saw the DHCP process as seen from teh workstation. But what configurations do we need to configure in teh DHCP iteslef.

1. IP address range (And excluded addresses)
2. Subnet mask
3. Lease durations
4. Other scope options → **DNS server** settings (so that your end stations can be configured with an appropriate DNS server IP address a **default gateway, VOIP servers**)

▼ DHCP pools

Grouping of IP addresses → A DHCP chooses an available address from a pool of previously configured IP addresses for a device.

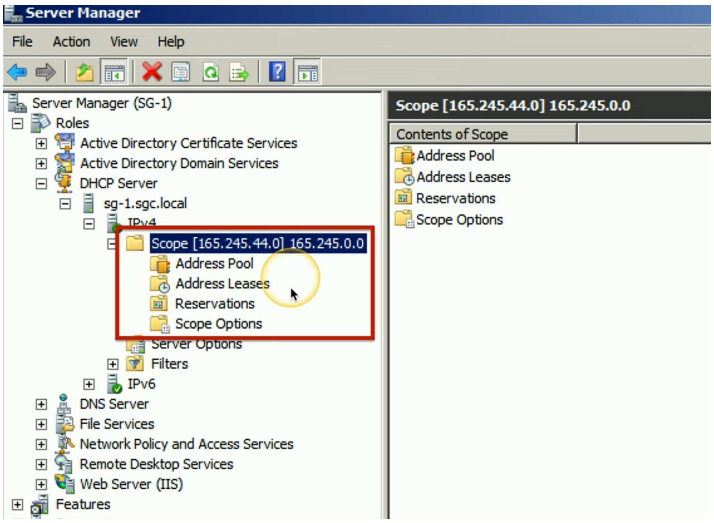
Subnet pools:

- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

So anything inside the subnets can be assigned as an IP address from the DHCP server

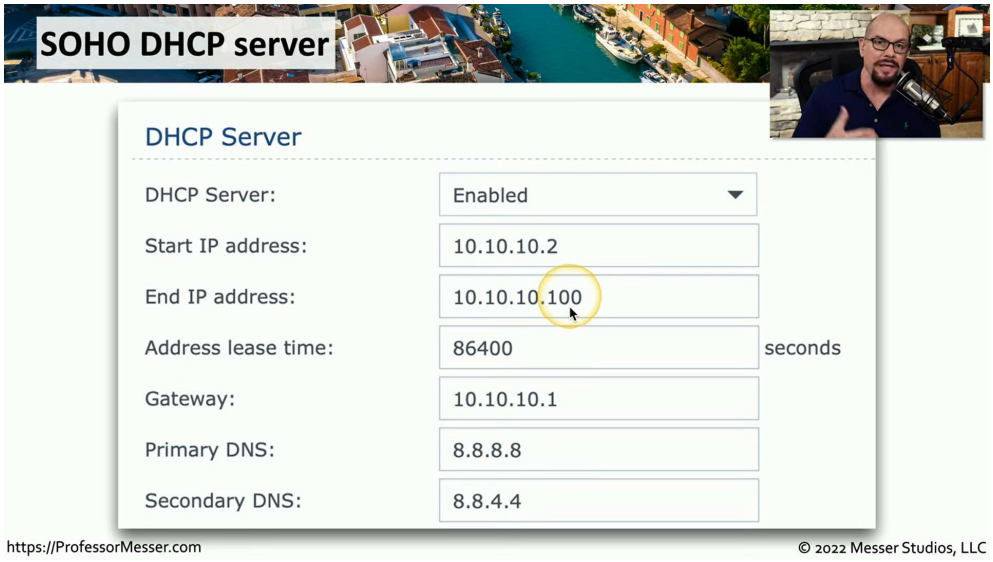
A scope is generally a single contiguous pool of IP addresses (DHCP exceptions can be made inside of the scope/ and any exception inside this range can also be specified)

In corporate use:



Address Pool → We know what IP addresses will be assigned. Address Leases → To see what IP addresses have been assigned Reservations → When certain device should always recieve the same IP. Scope Options → additional parameters (Ex: adding an IP address of a VoIP gateway, so that all devices will know which IP address to contact, in a network)

In home use:



Embedded router showing that DHCP is enabled

▼ DHCP address assignment

How devices receive IP addresses

1. Dynamic assignment

- DHCP server has a big pool of addresses to give out.
- Addresses are reclaimed after a lease period

2. Automatic assignment

- Similar to dynamic allocation
- DHCP server keeps a list of past assignments, so if u disconnect and connect again you will receive the same IP if it hasn't been taken.
- You will always get the same IP address

▼ DHCP address reservation

This is configured administratively, where IP addresses will be reserved for that device and that device alone, based on the MAC address

- Table of MAC addresses → Each MAC address has a matching IP address
- Also goes by : Static DHCP Assignment, Static reservation

▼ DHCP Leases

Leasing your address

- Its only temporary
- But it can be set to permenanta

Allocation

- assigned a lease time by the DHCP server
- Administratively configured

Reallocation (Renewing your IP address after reboot)

- Reboot your computer
- Confirms the lease

Workstation can also manually release the IP address

- Moving to another subnet

▼ DHCP renewal

Theres a time that start ones an IP address is allocated. there are timers that begin: Length of the lease time that’s configured to that server

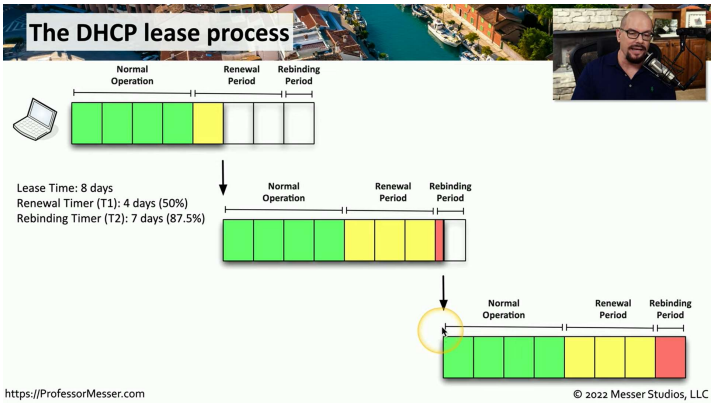
T1 Timer (**Renewal** Timer)

- Check in with the lending DHCP server to renew the IP address, halfway (50%) through the lease time (by default)

T2 Times (Gives a chance to device to maintain IP by **rebinding** other redundant DHCP servers)

- If the original DHCP server is down (unavailable) and that your not able to check in with T1 timer, if that server never returns to the network the least time begin to count down. Once you get to 87.5% of the lease time (7/8ths) it will try rebinding with any other DHCP server in the network so that it can retain that IP address

▼ DHCP lease process

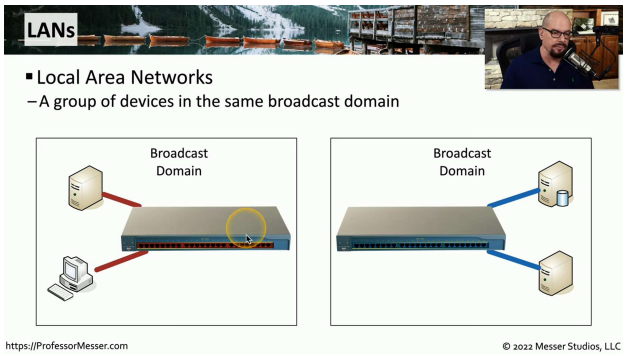


1. After 50% the lease restarts (Yellow bars)
2. If the original server is not available the rebinding process starts and moves onto another server and initiates connection, and if required start the lease again with that server

▼ VLAN’s and VPN’s

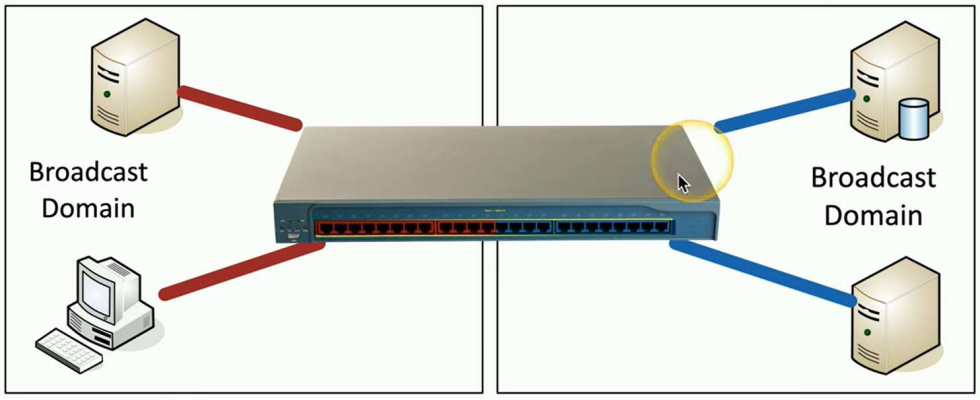
▼ LAN

Local area Network (Group of devices in the same broadcast domain)



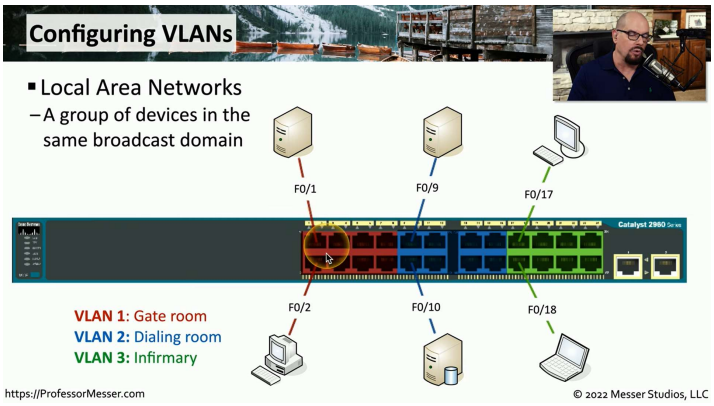
▼ Virtual LAN’s

A group of devices in the same broadcast domain. Separated logically instead of physically into. the 2 domains cannot talk to each other as they are divided.



▼ Configuring VLAN’s

Grouping devices in the same broadcast domain



▼ VPN’s

Virtual Private Network → Encrypted(private) data traversing a public network

Concentrator → Encryption / Decryption access device. Often integrated into a firewall. *In some devices* when accessed from a PC this is connected to a VPN hardware in some place this is known as a Concentrator (This could be a standalone device or integrated into a firewall)

Many deployment options:

- Specialized cryptographic **hardware**
- **Software-**based options available

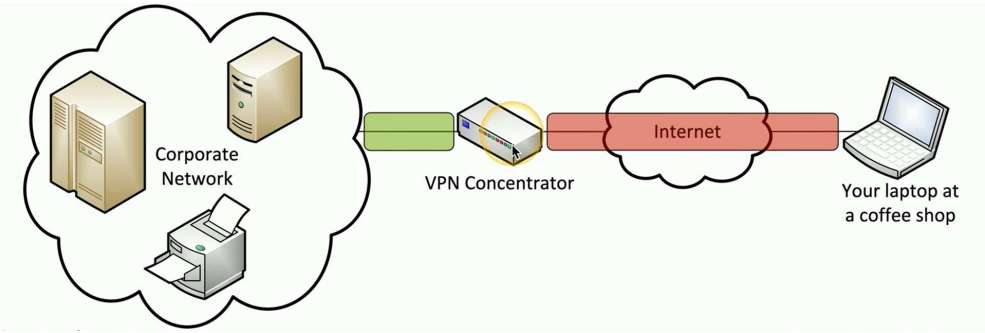
Usually Used with client software (Sometimes built into the O.S.) / **Software**

▼ Client-to-site VPN

This means you can be protected from a vulnerable public Wi-Fi that is not encrypted

On demand access from a remote device (Software connects to a VPN concentrator)

Some software can be configured as always-on



Green shows decryption / encryption

▼ Internet Connection Types

▼ Satellite Networking

Using a satellite dish to communicate with a satellite that is in the lower earth orbit

Communication to a satellite → Not terrestrial communication

High cost relative to terrestrial networking (Complicated)

- 50 Mbit/s down, 3 Mbit/s up are common
- Remote sites, difficult-to-network sites

High latency

- 250ms up, 250ms down
- Starlink advertises 40ms and is working on 20ms

High frequencies - 2 GHz

- Line of sight, rain fade → When rain occurs between you and the satellite there will be loss of connection

▼ Fiber

Higher speed data communication

- Frequencies of light, large data capacities over a short period.

- Higher installation cost than copper
  - Equipment is more costly
  - More difficult to repair
  - Communicate over long distances
- Large installation in the WAN core
  - Supports very high data rates
  - SONET, wavelength division multiplexing
- Fiber is slowly approaching the premises → for business and home use

▼ Cable Broadband

If your home or business is serviced by a cable company,(this is known as cable broadband) this is will bring u internet from the same cable you will use for cable television, broadband describes a method of communication where u can send multiple streams of data across a single wire, by communicating across multiple frequencies on that wire.

This means in a single wire we can transmit video, voice and data, by using different frequencies on that same medium

Data on the “cable” network

- DOCSIS (Data Over Cable Service Interface Specification)
- High-Speed networking
  - 50 Mbit/s through 1,000+ Mbit/s are common

▼ DSL

Making use of the copper we have in our home

In most cases this is ADSL (Asymmetric Digital Subscriber Line)

- Making use of telephone lines
- This is usually an → ADSL modem (Asymmetric Digital Subscriber Line) / uses the same telephone lines that we use for our analog telephone.

The reason we call asymmetric is cuz the speeds for downloading is much faster the speeds for uploading (downstream speeds of about 200 Mbit/s and 20 Mbit/s of upstream) . There is also a distance limitation with DSL before the signal gets so weak that ur not able to receive any data (This is usually 10,000 feet from the central office (CO)). Speeds are relative the distance which you are at from the CO, closer the faster

▼ Cellular Networks

Mobile devices → “Cell” phones (Separated land into “cells” as antennas cover a cell with certain frequencies)

Instead of sending voice over the network we are communicating by sending data (for internet connectivity)/ one way to provide this connection is through tethering. Where we would physically connect our phone via USB or Bluetooth and use our phone as an internet connection.

Many Phones also support hotspot so they would enable 802.11 capability and anything in range would be able to access the network through your phone, hence accessing the internet

Tethering → Turning your phone into a wireless router

▼ WISP (Wireless Internet Service Provider)

Some ISP’s send data over a wireless network to your home

- Terrestrial internet access using wireless

Usually found in rural or remote locations → Internet access for everyone

Many different deployment technologies

- Meshed 802.11
- 5G home internet
- Proprietary wireless

You will need an outdoor antenna to send and receive info from the WISP → Speeds can range from ~10 to 1,000 Mbit/s

WISP

▼ Network Types

▼ LAN

Building or group of buildings (High speed connectivity)

Ethernet and 802.11 wireless (Any slower and it isn’t local)

▼ WAN

Spanning around the globe

Generally connects LANs across the distance (And generally much slower than the LAN)

Many different WAN technologies

- Point-to-Point serial, MPLS
- Terrestrial(fiber) and non-terrestrial

▼ PAN

Your own private network (Bluetooth, IR , NFC)

Automobile (Audio output, integrate with phone)

mobile phone (wireless headset)

Health (Workout telemetry, daily reports)

▼ MAN

Metropolitan Area Network

A network in your city (Larger than a LAN, often smaller than a WAN)

Historically MAN-specific topologies were available in numerous names (Today we commonly see Metro Ethernet → where your given an ethernet connection on both sides and the service provider provides the link between the locations)

Common to see government ownership (As they own the right of way), tend to have a fiber connection

▼ SAN

Storage Area Network → Centralized form of storage network. This allows us to communicate to a centralized storage facility with huge data capacity

- Looks and feels like a local storage device
- Block-level access is provided (this is similar to what we have in the storage devices)
- Very efficient reading and writing

Requires a lot of bandwidth

- May use an isolated network and high-speed network technologies

▼ WLAN

Wireless LAN → 802.11 technology

Mobility , within a building , in a limited geographical area

Expand coverage with additional access points

Used in Downtown area , Large campus, etc.

▼ 02 / Mar / 2024

▼ Network Tools

▼ Cable crimpers

Pinch the connector onto the wire → Supports for coaxial, twisted pair, fiber

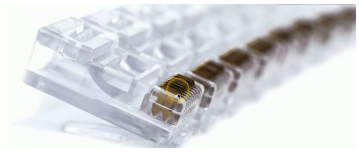
This is used to add the connectors at the end of the cable

Connects the modular connector to the ethernet cable (The final step of the process)

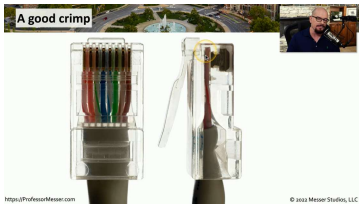
for twisted pair cables these Metal prongs are pushed through the insulation (The plug is also permanently pressed onto the cable sheath)

▼ Modular connectors

All the copper connections will be pushed down into the wire when a crimper is used



Before usage in a crimper



The sharp edges are pushed against each of the cables, the connections are made

▼ Crimping best-practices

Good crimpers include a pair of electricians scissors / cable snips and a good wire stripper

Make sure you use the correct modular connectors (Difference between wire types)

▼ Wi-Fi analyzer

When working with wireless networks it is incredibly easy to monitor (Everyone hears everything)

However you need to have sound knowledge of different frequencies over the wireless network

Purpose-built hardware or mobile application (software)add-on (specializes in 802.11 analysis

Very useful in areas with lot of Wi-Fi access points and allows you to identify errors and where interferences are occurring (Validate antenna location and installation), also helps in future modifications as everything being graphically represented streamlines the process of changing something and the result it generates

▼ Tone Generator

A.K.A. Toner Probes are used to identify one cable out of a bunch of a hundred, this is done by exerting an analog sound on the copper wire which can later be tracked down

Inductive probe this doesn’t need to touch the copper that’s inside the wire, u just need to get close to the cable so that u can hear the tone through a small speaker from the device

Left Tone Generator | Right Inductive Probe

This enables you to easily trace the wire (Even in complex environments)

1. Connect the tone generator to one end of the wire (This could be a modular jack, coax, Punch own connectors, alligator clips)
2. Then go to the other end of where the cable is, using the inductive probe from cable to cable to identify which cable contains that tone.

▼ Punch down tool

In some environments your not connecting RJ45 connectors instead your connecting to punch down blocks. For this you require a specific tool to connect to cables to the punch down block permanantly

Can be tedious (As every wire must be individually punched), when working with a lot of cables, cuz ur using pulling out individual wires, then putting each of the wires into a slot in the punch down block and using the punch down tool to individually fasten the wires to the punch down block

Using this tool not only pushes it down into the “” but also removes any excess making a neat connection.

▼ Punch down best practices

Since a lot of cables are in play it is necessary to organize the wires (Cable management through numbers)

Maintain your twists (Your category 6A cables) all the way into the punch down block

Document everything (Written, Tags, Graffiti)

▼ Cable testers

Another tool that comes in handy.

Relatively simple (Continuity test, a simple wire map)

These will connect either ends of the connectors to 2 devices that ensure correct pins are connected and that they work , attaining the ability to identify missing pins or crossed wires or wires that haven’t been punched down properly

Not usually used for frequency testing (crosstalk values , or the signal loss for those you require a TDR → Time Domain Reflectometer)

▼ Loopback plugs

When troubleshooting it is important to know whether the issue is related to the cable or the interface in the device

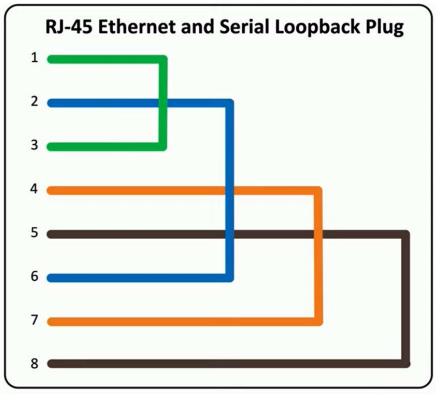
This can be done using a loopback plug.

This allows you to send info out using serial ports and receive that info immediately back in that serial port (Serial / RS-232 (9 pin or 25 pin)) and be able to compare the 2 values to see whether they match. If they dont match it is positive that there is an issue related to the interface.

There are also loopback cables that you can get for ethernet, T1 wide area network, Fiber connections

These are not cross over cables

Cross over cables → Connect 2 devices directly to each other. Loopback → Connect a device to itself



Useful for testing physical ports (Or fooling your application)

▼ Taps and Port mirrors

When troubleshooting a network it is sometimes useful to the data that goes over the wire itself.

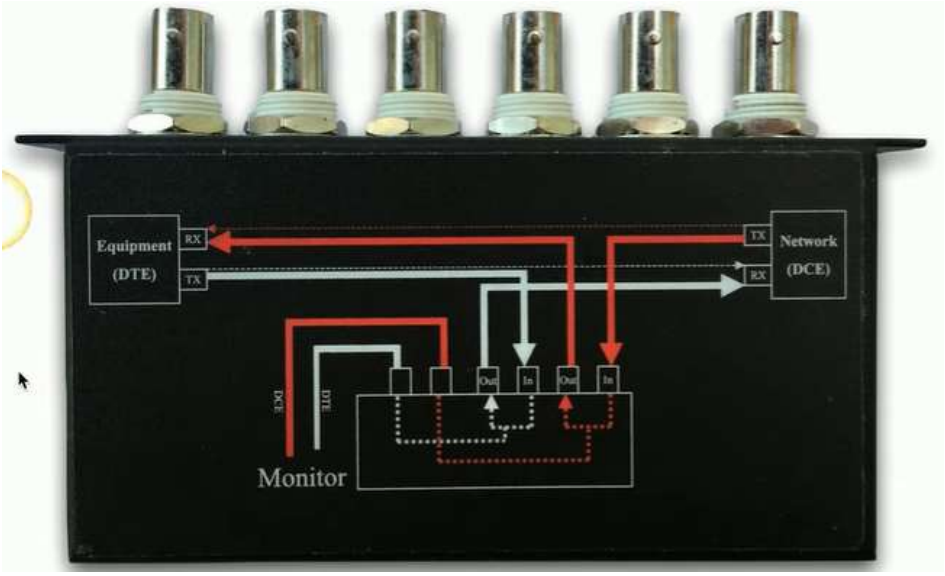
Pysical taps

- One way you could see the data in that connection is with a Physical Network Tap → This allows you to disconnect a link put our physical tap in the middle, and take a copy of all that data and send it to an analyzer
- This is passive tap that doesn't require fiber, we commonly see that with fiber taps or it might with an active tap that can tap copper connection but requires power to be able to do that.

Port Mirror (Software based taps)

- Instead of a physical tap you can use a tapping function that is built into your switch this is called a port mirror or a SPAN, port redirection
- SPAN → Switched Port ANalyzer , this function takes data into the switch , that is able to take data that's going between different interfaces on the switch and send a copy of that data to a third interface, which you can then connect to an analyzer
- (However there are resource limitations on the switch and bandwidth limitations on the interface themselves, hence if u need a simple temporary fix u can use a port analyzer or a port mirror

Intercept network traffic → Send a copy to a packet capture device



a copy of the captured data is sent to a monitor/analyzer

▼ Network Cables

Fundamental connection to the internet occurs through network cables. Nevertheless wireless communication is available it is these cables that provide Wi—Fi and bulk of our communication takes place.

▼ Twisted Pair copper cabling

Balanced pair operation

- Two wires with equal and opposite signals
- Transmit+, Transmit- / Receive+, Receive- (opposite signals)

Difference in cable + Twist in the cable is necessary for communication to occur

Keeps a single wire constantly moving away from the interference

The opposite signals are compared on the other end

This twisting helps to move away from the interference

Interference that may have occurred through the wire can be identified cuz we now have 2 different signals to compare

Another factor is that pairs in the same cable have different twist rates, this produces different signals on the other end

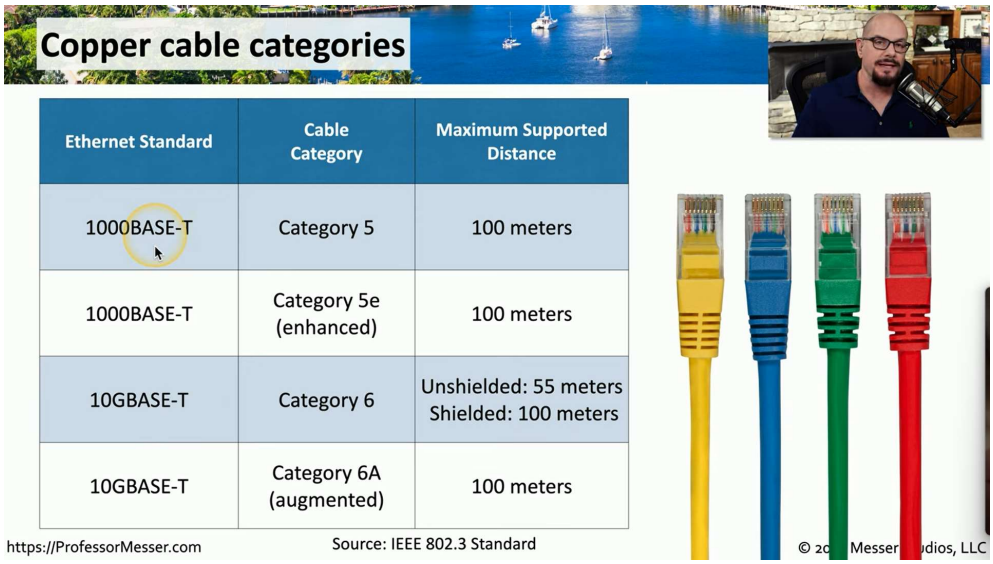
▼ Copper Cable categories

1000BASE-T → 1GB/s ethernet standard that operates on twisted pair copper cabling

Support category 5 cables and 100 meters

- → enhanced (additional validations are made on this revision)

10GBASE-T → 10GB/s ethernet that also runs on twisted pair copper cabling

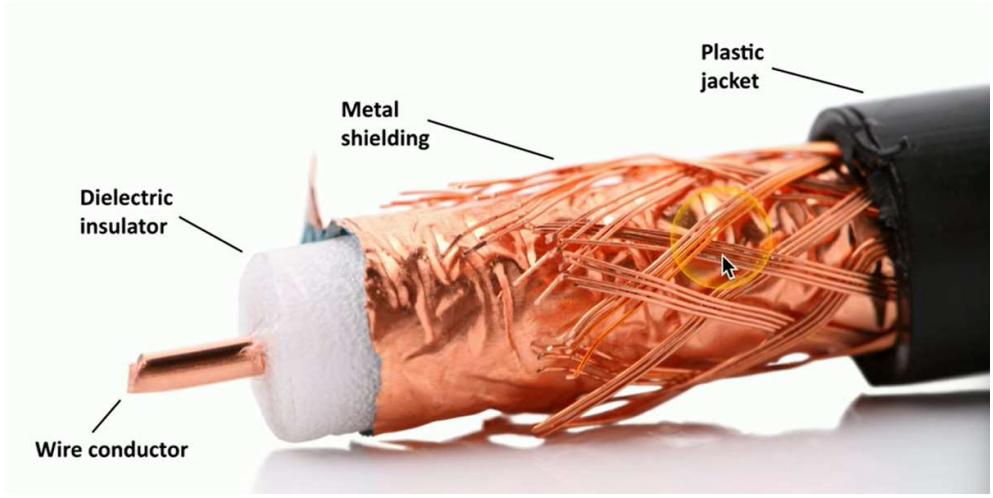


2 different standards are shown here (1000 BASET & 10G BASET)

▼ Coaxial Cables

2 or more forms share a common axis, used on cable modem networks. there are 2 or more forms that share a common axis.

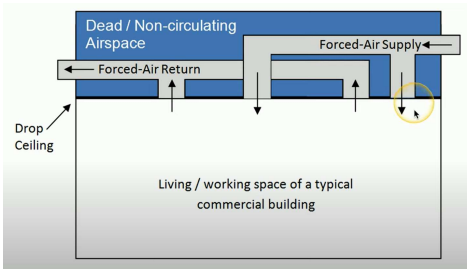
Commonly used in RG-6 (televisions/digital cable) / and high speed internet over cable

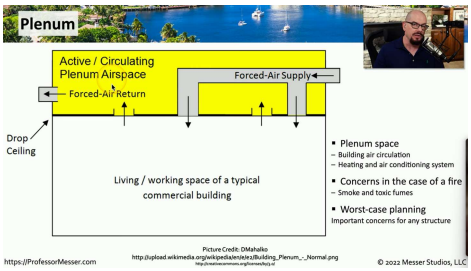


▼ No plenum

Air goes to a shared air space known as a plenum.

We wouldn’t want the network cables to create smoke or poisonous gas which will be returned back to the same room through the forced air supply





To prevent this issue there are different types of cable available:

▼ Plenum-rated cable

Traditional cable jacket → Polyvinyl chloride (PVC)

If ur putting this cable i a plenum then you will need a

- Fire-rated cable jacket
  - Fluorinated ethylene polymer (FEP) or low-smoke polyvinyl chloride (PVC)
- Plenum-rated cable may no be as flexible, and have the same bend radius

Worst-case planning (important concerns for any structure)

▼ Unshielded and shielded cable

In most cable runs we use UTP

- No additional shielding
- The most common twisted pair cabeling

STP i used to provide more additional details to the cable in a environment where theres much more interference

- Additional shielding protects against interference
- Shield each pair and or the overall cable
- Requires the able to be grounded (for additional protection)

Types of cable

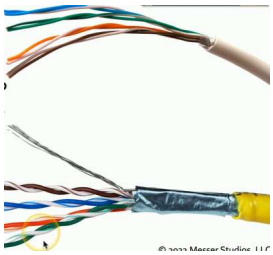
U → Unshielded

D → Braided shielding

F → Foil shielding

Overall cable / individual pair (TP)

- Braided shielding around the entire cable and foil around the pairs is S/FTP
- Foil around the cable and no shielding around the pairs is F/UTP



▼ Direct burial STP (Shielded Twister Pair)

Overheads cable isn’t always a good option (put the cable on the ground)

Direct burial STP (for shielded twisted pair)

These cables are designed to be outside hence the link the finished with jelly that helps keep away from the bloc k.

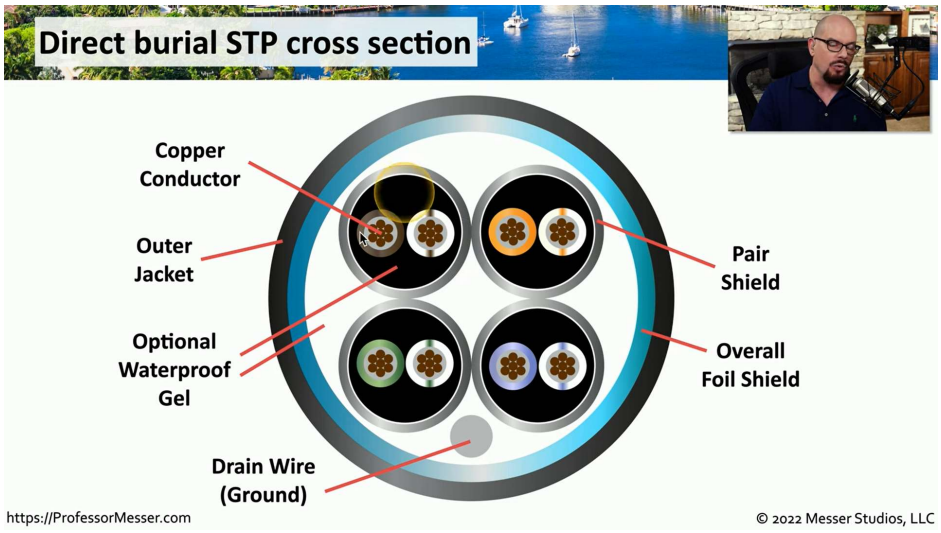
Provides protection from elements

- Designed to be water Froom
- Often filled with gel to repel water
- Conduct may not be needed

This means u can have it directly on the ground, and easily accessible later, instead of a conduit

Shielded twisted pair

- Provides grounding
- Adds strength
- Protects against signal interference (adds rigidity % strength to the cable)



4 pairs of the ethernet cables. Waterproof gel/ Drain wire is used to drain away any additional voltages are absorbed through a ground wire that extends the length of the cable

▼ 03 / Mar / 2024

▼ Optical Fiber

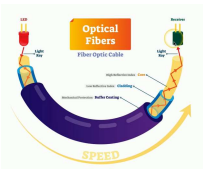
Transmission by light in the visible spectrum

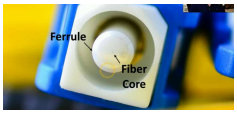
No RF signals

- Since no radio frequency (as connection over radio frequency can be intercepted) is emitted it is very difficult to monitor or tap the connection.

Signal slow to degrade → Transmission over long distances is possible much more than copper

Immune to radio interference as there is no RF, signals of light make up the network





There are 2 categories of Fiber optic cables

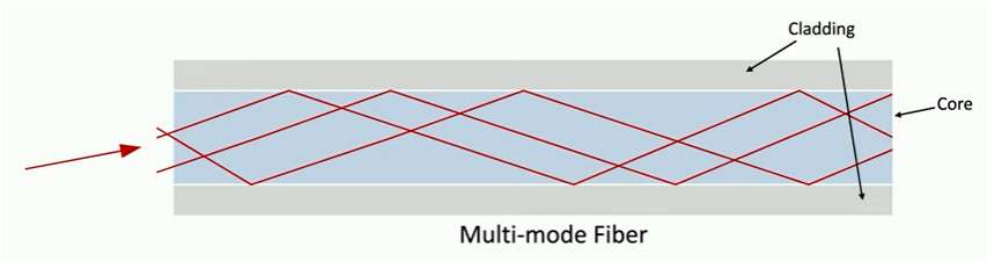
▼ Multimode fiber

Short range communication

- Up to 2 Kms

Relatively inexpensive light source → LED

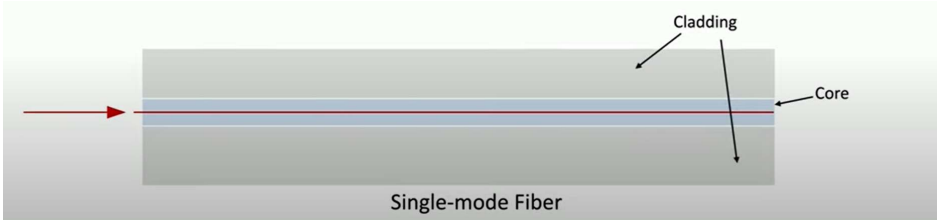
It is called multimode because more than one signal(mode) can be sent within the tube, which are collected at the opposite end/



▼ Single-mode fiber

Long-range communication

- Up to 100 Km without needing to regenerate that signal
- Expensive light source→ hence they commonly use lasers



▼ 568A & 568B Colors

▼ Structured Cabling Standard

There are international standards on how cabling is set up in commercial workspaces

One of these standards is the International ISO/IEC 11801 cabling standards

- Defines classes of networking standards

Telecommunications Industry Association (TIA) → (U.S. north)

- Standards, market analysis, trade shows, government affairs, etc.
- ANSI/TIA-568: Commercial Building Telecommunication Cabling Standard (http://www.tiaonline.org)

Under TIA-568 standard we re going to talk about one specific standard that delas with what colors are used in specific pins in an ethernet connection.

Commonly references for pin and pair assignments of eight-conductor 100-ohm balanced twisted pair cabling (-T568A and T568B)

▼ TS68A & T568B termination

This standard gives u 2 option when punching down or applying different colored wires to your ethernet connection

If u look at a ethernet RJ45 connector or a punch down block used for ethernet you will notice that there are 2 different standards that are addresses.

1. 568A
2. 568B

These 2 standards provide us with the colors that we'll use for our 8P8C connectors these are 8 position 8 conductor connecters.

Most often the 568A coloring scheme is associated with horizonal cabling

and most organizational the connection for end users are using the 568B color standard

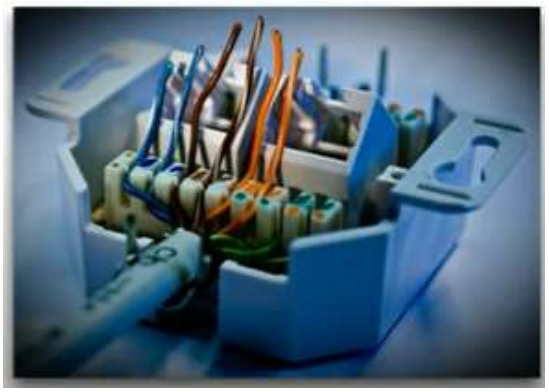
Ultimately it doesn't matter what is use das both of these exactly same having the same functionality therefore one isn't better or worser than the other.

Gigabit Ethernet cross over cable is clearly not a 568A color scheme on one side of the cable and a 568B color scheme on the other side of the cable

As 568A and 568B is not associated with ethernet crossover cables but only specify the colors

Pin assignment from T568-B standard

- Eight conductor 100-ohm balanced twisted-pair cabling



T%^*A and T568B are different pin assignments for 8P8C connectors

- Assigns the T56A pin-out to horizontal cabling

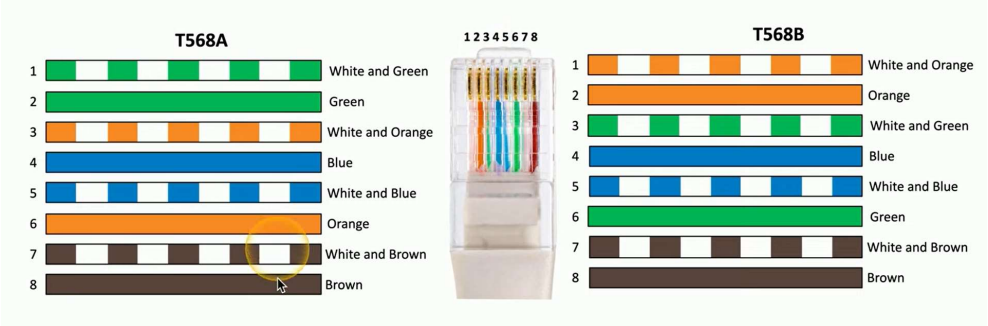
Main organizations traditionally use 568B

- difficult to change in mid-stream

You cant terminate one side of the cable with 568A and the other with 568B

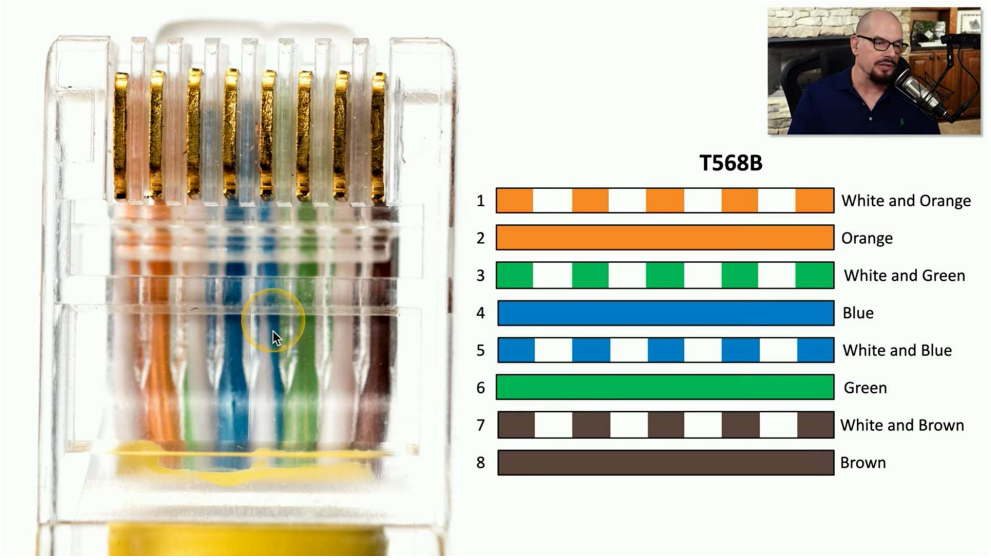
- This has never been the definition of a gigabit ethernet crossover cable

▼ 568A and 568B Termination

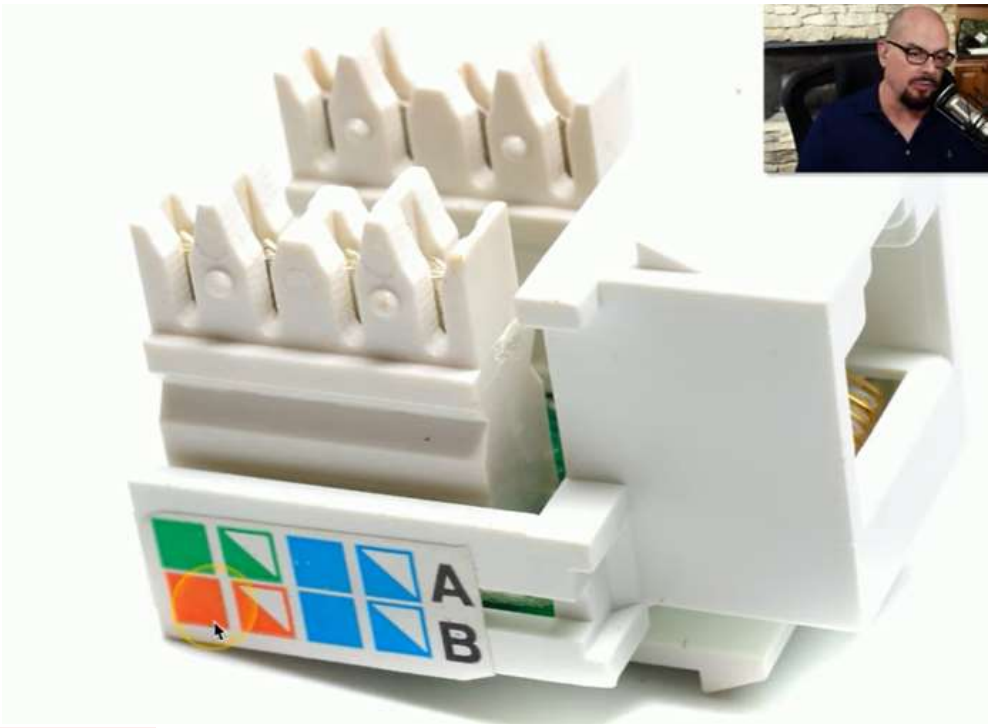


8 different wires are available in ethernet RJ45 / If T568A is used in wiring then the left hand side should be used (vice versa)

as u can see there is a slight difference



Punch down blocks / 568A (A at top B at bottom)



▼ 04 / Mar / 2024

▼ Peripheral Cables

▼ USB (Universal Serial Bus)

Simplify connections → Used in printer, storage devices, keyboards, mouse

USB 1.1 (Provided in 2 speeds)

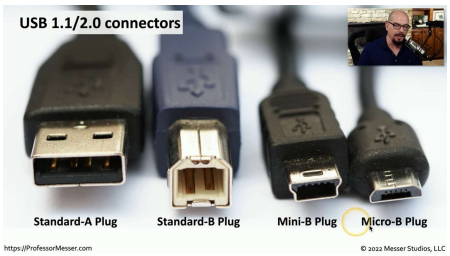
- Low speed → 1.5 Mb/s , 3 meters
- Full speed → 12 Mb/s , 5 meters

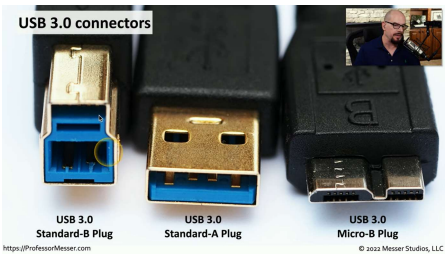
USB 2.0

- 480 Mg/s , 5 meters

USB 3.0

- Known as Superspeed
- 5 Gb/s , ~3 meters
    - Standard does not specify a cable length





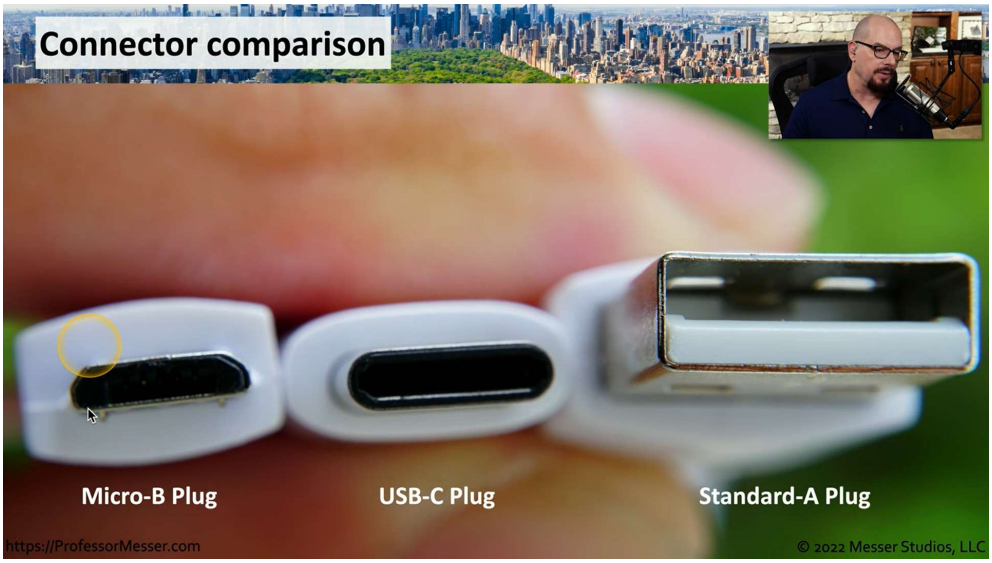
▼ USB-C

USB has a lot of different connectors → and they have changed over time

Can be annoying to connect USB-A → 3rd times the charm (either orientation works)

USB-C replaces all of these → One connector to rule them all

USB-C describes the physical connector → It doesn't describe the signal . Different types of signals can be sent not only related to data but video as well.



▼ USB versions and naming

Theres a lot to keep track of (The names keep changing)

The standard doesn't change (Just the names)

USB 3.0 Name	Marketing Name	Maximum Speed
3.0	SuperSpeed	5 Gbit/sec

▼ USB 3.1

Released in July 2013 (Doubles the throughput over USB 3.0)

(Name change 3.0 → 3.1 Gen 1)

USB 3.0 is USB 3.1 Gen 1 (Old)

- SuperSpeed USB
- 5 Gbit/s

USB 3.1 is USB 3.1 Gen2 (New)

- SuperSpeed +
- Twice the rate of USB 3.0/ USB 3.1 Gen 1

USB 3.1 Name	USB 3.0 Name	Marketing Name	Maximum Speed
USB 3.1 Gen 1	3.0	SuperSpeed	5 Gbit/sec
USB 3.1 Gen 2		SuperSpeed+	10 Gbit/sec

▼ USB 3.2

Released in September 2017

Bandwidth can double with the USB-C cables

Uses an extra “lane” of communication associated with the lip-flop wires in USB-C

USB 3.0 → 3.1 Gen 1 → USB 3.2 Gen 1

- Superspeed USB 5 Gbps (single lane)

USB 3.1 → 3.1 Gen 2 → USB Gen 2

- SuperSpeed USB 10 Gbps (single lane)

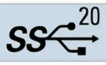
USB 3.2 Gen 1 x 2

- 10 Gbps using two “Gen 1” lanes

USB 3.2 Gen 2 x 2

- SuperSpeed USB 20 Gbps using two “Gen 2” lanes

“When a new standard is released the old standards get renamed”

USB 3.2 Name	USB 3.1 Name	USB 3.0 Name	Marketing Name	Maximum Speed	Logo
USB 3.2 Gen 1	USB 3.1 Gen 1	3.0	SuperSpeed USB 5Gbps	5 Gbit/sec	
USB 3.2 Gen 2	USB 3.1 Gen 2		SuperSpeed USB 10Gbps	10 Gbit/sec	
USB 3.2 Gen 1x2				10 Gbit/sec	
USB 3.2 Gen 2x2			SuperSpeed USB 20Gbps	20 Gbit/sec	

▼ Thunderbolt

High-speed serial connector

- Data and power on the same cable
- Based on Mini DisplayPort (MDP) standard

Thunderbolt v1

- 2 channels
- 10 Gbit/s per channel x 2
- 20 Gbit/s total throughput
- Mini DisplayPort connector

Thunderbolt v2

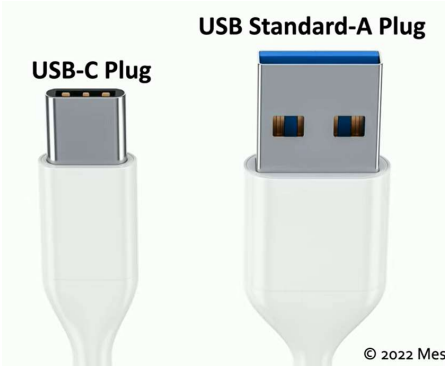
- 20Gbit/s aggregated channels (2 channels in 1)
- Mini DisplayPort connector

Thunderbolt v3

- 40 Gbit/s aggregated throughput
- USB-C connector

Maximum 3 meters if copper is used

- Maximum of 60 meters of (optical=fiber) is used
- Daisy-chain up to 6 devices (single thunderbolt interface in the back of your computer , but u can have 6 devices that uses thunderbolt, hence u can extend that one cable to 6 different devices)



▼ Serial Console Cables

Before USB we were using 9 pin and 25 pin serial connections to connect peripherals

D-subminiature or D-sub

- The letter refers to the connector size

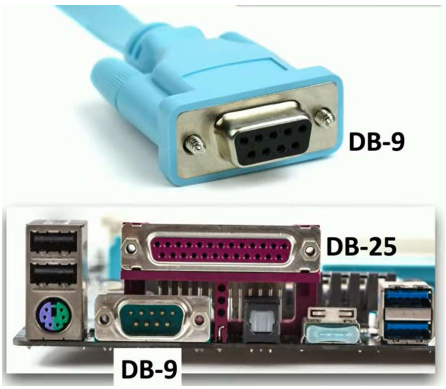
Commonly used for RS-232

- Recommended Standard 232
- An industry standard since 1969

Serial communication standard that has been around for a long time hence it is common to find in modern connections, in serial consoles that might be in a

peripheral device, used to plug in a switch, firewall, router and configure that device from the command line

- Built for modern communication
- Used for modems, printer, mice, networking



▼ 06 / Mar / 2024

▼ Video Cables

▼ VGA (Video Graphics Array)

- DB-15 connector → More accurately called DE-15
- Blue color → this color is associated by the PC system guide standards. This is a standard that supports video displays but has no way to integrate video connections.
- Video only no audio signals
- Analog signal
  - No digital
  - Since analog as the signal / cable is extended by 5-10 meters the image degrades

15 pin connector