# Network Devices

**Hub** – Device used broadcast messages sent by other devices connected to its ports. The hub does not care who the recipient is it simply sends the message to all connected parties. No network address are used by the Hub.

**Bridge** – this is used to segment networks into smaller sections. Unlike hubs a calculated decision is made on where or if the data will be forwarded. Normally they have only two ports.

**Switch** – this is similar to a Hub and Bridge compiled into one. Task are performed in a smarter and more configurable manner using devices address for the. The switch learns device Mac addresses and therefore is more efficient and Bandwidth conscious. Data is only received by the device it was sent to.

**Router** – this is the doorway out of the network. This is the device that forwards data from one network to the other. It uses both Mac Address and IP address.

A close up of text on a white background

Description automatically generated

# Network Commands

**PING** – this is used to identify if a device with a specified IP address is connected to the network and to verify that the host machine can communicate with other devices on the network.

**TARCERT** – this command is used to determine the route that a request takes to reach its destination. This is helpful in a situation where data is sent but not received or data takes longer expected to reach its destination.

**ROUTE PRINT** – this displays the routing table used by the device in question. A Routing table is a list of intermediate devices that the host device uses to forward data packets: each computer has a routing table that it uses to determine the route through which it will send data.

**NETSTAT-R** – this displays information on active connections on a device and protocol statistics. This can be used to show active connections to the device in question and can help in a situation where you need to identify any unwanted TCP/IP connection to your device or it can be used to identify the connections being used by a specific process running on the device.

**Network Tim Protocol (NTP)** – these commands are used to configure and get information about the time and time synchronization status of the device. This can be used to synchronize the time on a server when troubleshooting issues that can come from updates not being installed on a machine because of incorrect time on the device.

# IP Address

The difference between IPv4 and IPv6 are:

* IPv4 uses a 32-bit number addressing scheme when identifying devices while IPv6 uses a 128-bit number scheme. Because of this IPv6 can provide more unique address.
* Ipv4 is written in dotted decimal Notation (192.168.100.1) while IPv6 uses Hexadecimal Notation (3FFE:F03D:AB00:2109:3254:4328:ABCD).
* IPv6 has a les complex heard which means it is optimized for faster transfers. As a replacement for IPv4, IPv6 aims to tackle the issue of not having enough unique address for the growing number of devices connected to the internet.

A **subnet** is a smaller network derived from the segmentation of a larger network: large networks are subdivided into smaller ones. They are used to help minimize traffic on a large network by creating smaller interconnected networks.

**NAT (Network Address Translation)** is a router feature that converts one set of IP address to another set of IP addresses. This is used to give computers on a private network the ability to communicate to computers through the internet with out needing a public IP address. The internal IP address of the device is translated into the public IP address of the network that device is on and then sent into the internet.

**Routes**

**Static** IP routes are manually set on the device and have a benefit of being faster and less complex because they are not automatically derived. It carries low overheads and requires no additional resources for route storing. **Dynamic** routes are automatically set by complexed algorithms that would require more resources to produces the routes. Dynamic routes are more secure but less fault tolerant because if one node along the route fails then the route is no longer good and will prevent data from being transported. Dynamic routs are less secure because they need to send broadcast which, by nature, can be intercepted and the are fault resistant because a failure along the established route will result in the route being removed and an alternate one added.

# Network Protocols

UDP – User Datagram Protocol. This is the protocol is also known as a connection less protocol. This is because the protocol is not concerned with establishing the connection between two peers. It is primarily focused on just sending the data. UDP is used when speed and efficiency is more critical that data integrity. UDP is used in situations like online games, VoIP and DNS.

TCP – Transmission Control Protocol. TCP is known as a connection-oriented protocol. Its focus is primarily on establishing a reliable connection that guaranties the delivery of the data being sent. This makes it slower and less efficient than UDP but it ensures that the data reaches the destination in the order that it was sent. Email and websites are two types of applications that use TCP. TCP is more reliable than UDP and as a result is much slower.

# Network Tools

**Wireshark** is a tool used to examine, in detail, all the traffic that is going through a devices network interface card. Wireshark captures the data on a packet level and reveals the internals of each packet. This is used when trouble shooting transmission problems on networks or some developers use it to analyze packet movement when developing solutions that use the OSI stack.

**Nmap** (Network Mapper) – This tool is used to scan other network devices to identify any running services. Nmap send packets to the host and analyzes the response. Based on the response it can be determined if the host has any running services, Operating system type, open ports and type. Auditing the security of a device is one use of this tool.

**Putty** is a terminal emulation software that uses remote connection protocols to establish secure connections to remote computers and provide the user with access to the terminal of that remote computer. It can be used to remotely control another computer or to remotely configure network devices like firewalls and switches.

For network monitoring, **SolarWinds** is a tool used to gather information and report on the status of network devices. Administrators used this get consistent updates on health/status of devices on their network and also to get an inventory of network devices.

**Metasploit** is a group of tools and utilities put together to provide a framework for finding and taking advantage of vulnerabilities found on devices and in software. Penetration testers use it to infiltrate systems to highlight weaknesses and identify threats to the system.