**IP Addresses**

* Public IP addresses are provided by Internet Service Providers (ISPs) for a monthly fee
* IPv4 uses a 32-bit numbering system, allowing for 2^32 (approx. 4.29 billion) IP addresses
* IPv6 uses a 128-bit numbering system, supporting up to 2^128 (approx. 340 trillion) IP addresses, resolving the limitations of IPv4

**Windows Firewall Defender**

* This is a Host firewall (a host firewall is a program that ships as part of your system or is installed)

**MAC Address**

* MAC stands for Media Access Control
* A MAC address is a 12-character hexadecimal number split into two's and separated by colons (e.g., a4:c3:f0:85:ac:2d)
* The first 6 characters represent the manufacturer, and the last 6 are a unique identifier

**Ping and ICMP**

* Ping uses ICMP (Internet Control Message Protocol) packets to test the performance and reliability of a connection between devices
* Ping measures the time taken for ICMP echo packets to travel between devices and receive a reply
* Ping can be performed against devices on a network or websites using the command ping <IP address or URL>

**LAN Topologies**

* Star Topology: Devices are individually connected to a central networking device (switch or hub)
* Bus Topology: Devices are connected to a single backbone cable, which can cause bottlenecks and difficulty in troubleshooting
* Ring Topology: Devices are connected directly to each other in a loop, requiring less cabling and dedicated hardware

**Network Devices**

* Switch: Used to centrally connect multiple devices on a local network and transmit data to the correct location
* Router: Connects networks and passes data between them using routing

**Subnetting**

* Subnetting divides a network into smaller pieces
* There are 32 bits in a subnet mask, and each octet can range from 0-255

**Network Addressing**

* Network Address: Identifies the start of a network
* Host Address: Identifies devices within a network
* Default Gateway: The device responsible for sending data to another network

**Address Resolution Protocol (ARP)**

* ARP allows devices to identify themselves on a network by associating their MAC address with an IP address
* Devices keep a log of MAC addresses associated with other devices
* When a device wants to communicate with another, it sends a broadcast to the entire network searching for the specific device's MAC address
* If a device has the requested IP address, it sends an ARP reply with its MAC address
* The initial device stores this MAC address and IP address mapping in its ARP cache

**IP addresses can be assigned in two ways:**

1. **Manual Assignment**
   * IP addresses are physically entered into a device**.**
2. **Automatic Assignment (Most Common)**
   * A **DHCP (Dynamic Host Configuration Protocol)** server is used.
   * When a device connects to a network and does not have a manually assigned IP address, it follows these steps:
     + The device sends a **DHCP Discover** request to check for DHCP servers on the network.
     + The DHCP server responds with a **DHCP Offer,** suggesting an IP address for the device to use.
     + The device sends a **DHCP Request,** confirming its acceptance of the offered IP address.
     + The DHCP server sends a **DHCP ACK (Acknowledgment)**, allowing the device to start using the assigned IP address.

**OSI (Open Systems Interconnection) Model**

* Fundamental, critical model in networking
* Provides framework for how networked devices send, receive, interpret data
* Benefit: Allows devices with different functions/designs to communicate on a network
* Data sent follows OSI model uniformity, understandable by other devices

**7 Layers of OSI Model (Layer 7 to Layer 1):**

**Key Points:**

* Each layer has different responsibilities
* As data travels through layers, specific processes occur
* Information is added to data (encapsulation process)

**Layer 7: Application Layer**

* Most familiar layer to users
* Provides protocols and rules for user interaction with data (send/receive)
* Examples:
  + Email clients
  + Web browsers
  + File transfer software (e.g., FileZilla)
  + Provide Graphical User Interface (GUI) for user interaction
* Other protocols:
  + DNS (Domain Name System)
    - Translates website addresses to IP addresses

**Layer 6: Presentation Layer**

* Standardization of data begins
* Acts as a translator for data to/from Application Layer (Layer 7)
* Allows different software/formats to communicate
  + Example: Different email clients can display email content consistently
* Handles data encryption and security features
  + HTTPS (secure website) encryption occurs at this layer

**Layer 5: Session Layer**

* Establishes connection (session) between computers for data transfer
* Session remains active while connection is live

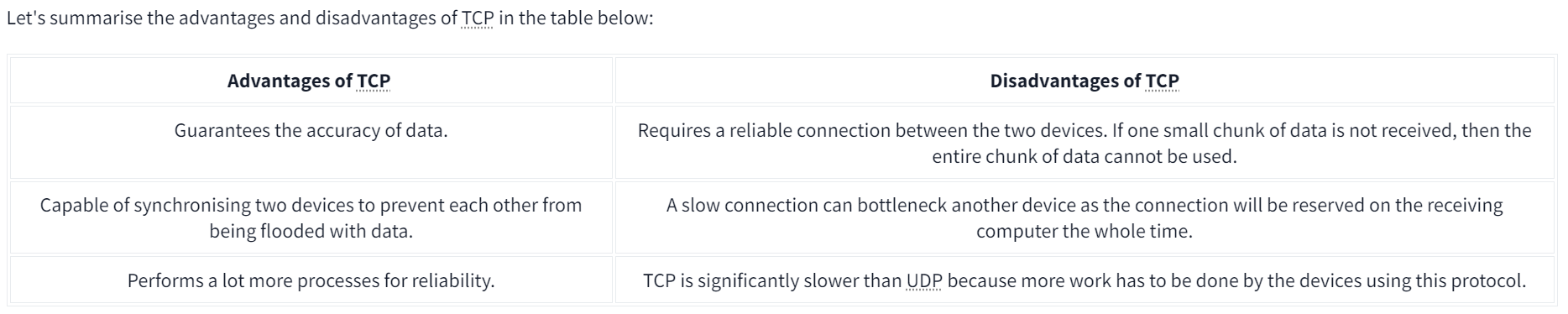
Responsibilities:

* Synchronizes computers to ensure readiness before data exchange
* Divides data into smaller chunks (packets) for transfer
  + Beneficial for recovering from connection loss (only resend remaining chunks)
* Sessions are unique - data cannot travel across different sessions

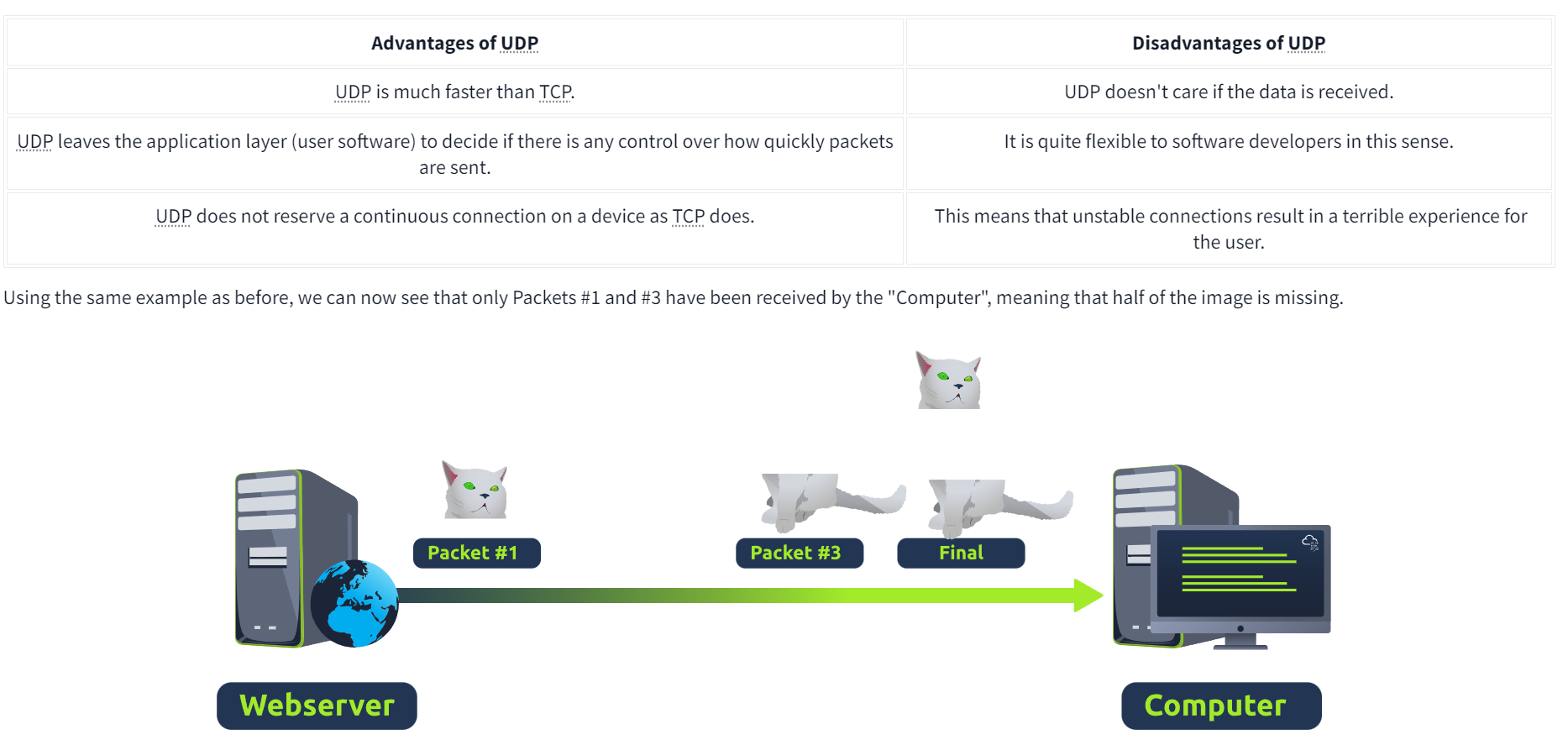
Key Points:

* Manages sessions between computers
* Prepares data for transfer by dividing into packets
* Improves reliability by allowing partial retransmission if needed

**Layer 4: Transport Layer**

* Vital for transmitting data across a network
* Uses one of two protocols based on specific factors:
  1. TCP (Transmission Control Protocol)
     + Designed for reliability and guarantee
     + Establishes constant connection between devices for data transfer
     + Incorporates error checking
       - Ensures data chunks from Session Layer are received and reassembled in order
     + Used for services that require accuracy and completeness
       - File sharing, web browsing, email, etc.

In the diagram below, we can see how a picture of a cat is broken down into small pieces of data (known as packets) from the "webserver", where the "computer" re-constructs the picture of the cat into the correct order.

* 1. UDP (User Datagram Protocol)
     + Less advanced than TCP
     + No error checking or reliability features
     + Data is sent without synchronization or guarantee of delivery
     + Useful for small data transfers and situations where some data loss is acceptable
* Device discovery protocols like ARP, DHCP
* Video streaming (some pixelation is okay)

**Layer 3: Network Layer**

* Where routing and reassembly of data chunks (packets) occur
* Routing determines optimal path for packet delivery

Routing Factors:

* Shortest path (fewest devices to cross)
* Most reliable path (least packet loss)
* Fastest physical connection (fiber > copper)

Routing Protocols:

* OSPF (Open Shortest Path First)
* RIP (Routing Information Protocol)
* Determine optimal routes based on factors above

IP Addressing:

* Operates using IP addresses (e.g. 192.168.1.100)
* Devices like routers capable of IP routing = Layer 3 devices

Key Points:

* Handles routing and reassembly of packets
* Routing protocols find optimal delivery paths
* Uses IP addressing for packet delivery
* Layer 3 devices (routers) operate at this layer

**Layer 2: Data Link Layer**

* Focuses on physical addressing for data transmission
* Receives packets from Network Layer (with IP address)
* Adds physical MAC (Media Access Control) address of receiving endpoint

MAC Addressing:

* Network Interface Card (NIC) has unique MAC address
* MAC addresses set by manufacturer and burned into NIC
* Cannot be changed (but can be spoofed)
* Physical MAC address used to identify where to send data

Responsibilities:

* Present data in suitable format for transmission
* Package data into frames for sending over physical layer

Key Points:

* Handles physical addressing using MAC addresses
* Obtains IP addresses from Network Layer and adds MAC addresses
* Prepares data for transmission over the Physical Layer

**Layer 1** Physical- For example ethernet cables

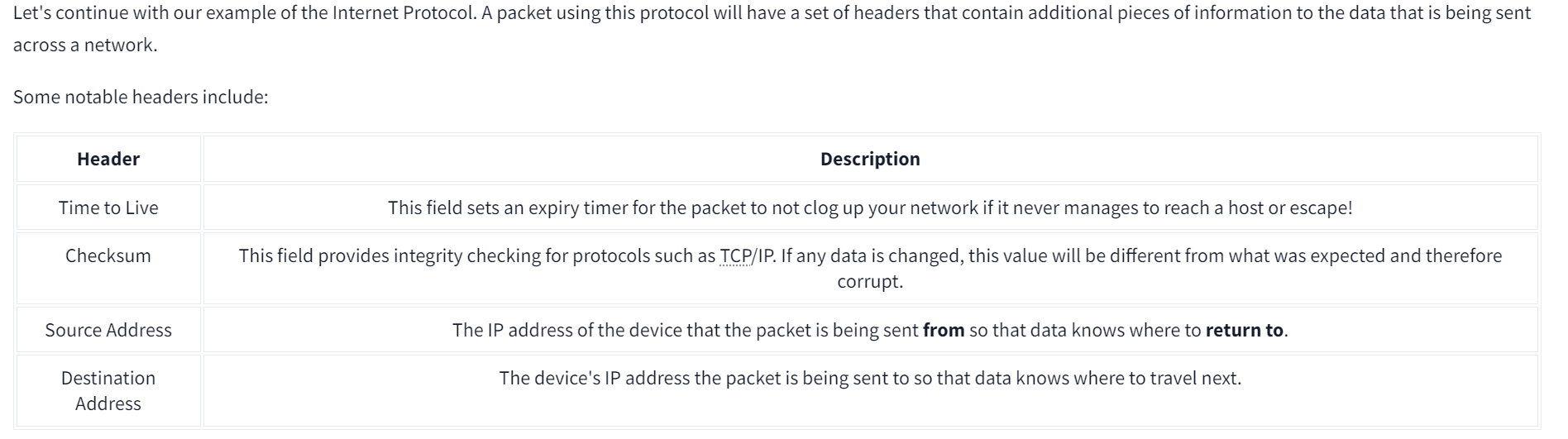
**Packets and Frames**

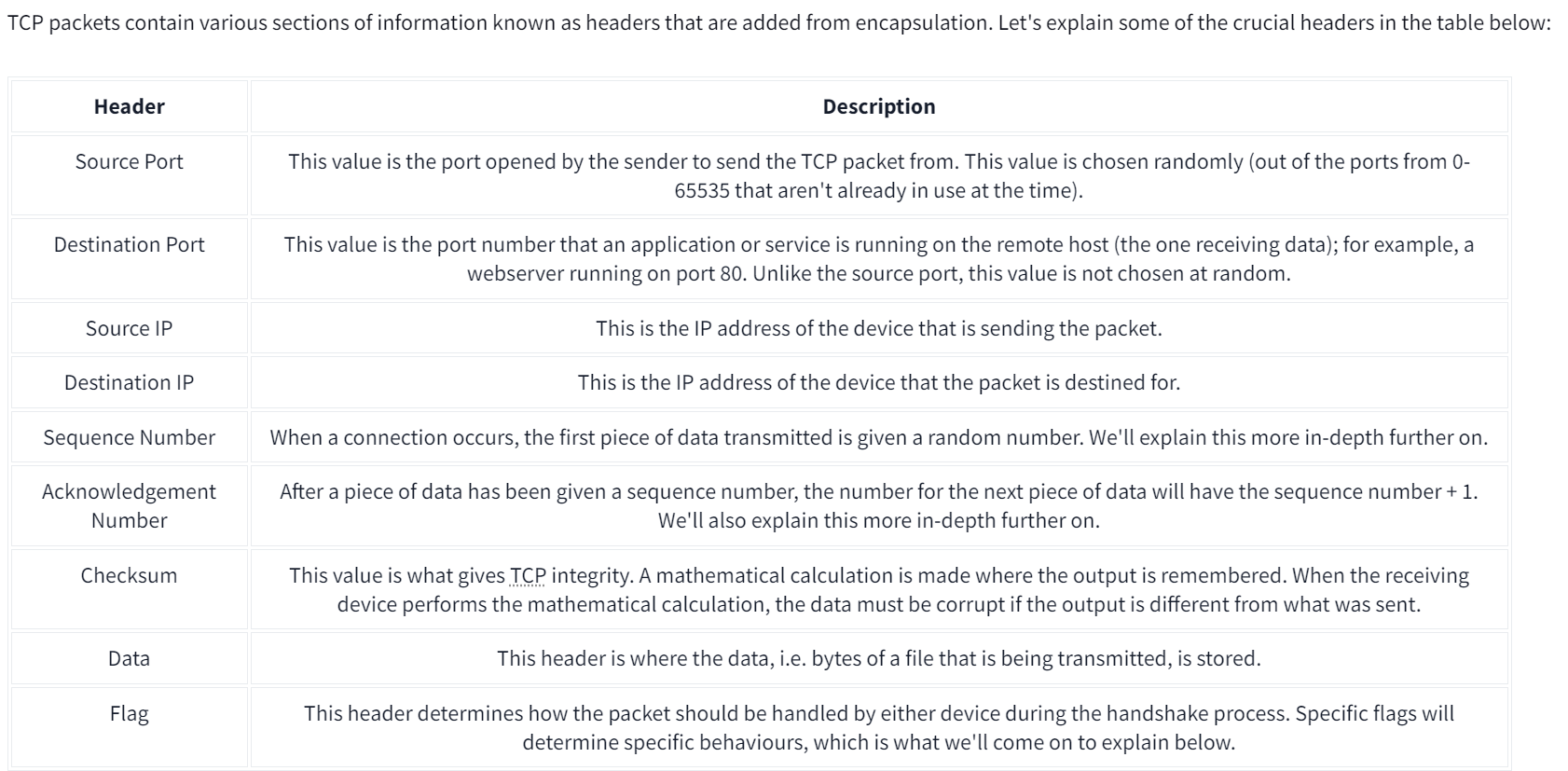
* Small pieces of data that form a larger message/information

**Encapsulation**

* Process discussed in OSI model
* Packet: Contains IP addresses
* Frame: Data inside packet after encapsulating info stripped away

**Advantages of Packets**

* Efficient communication across networked devices
* Less chance of bottlenecking than sending large messages at once
* Example: Loading website image - sent in small pieces, reconstructed on computer



**Ports**

* Essential for data exchange
* Analogy: Ships docking at compatible ports in a harbor
* Ports enforce compatibility rules for devices communicating

**Port Numbers**

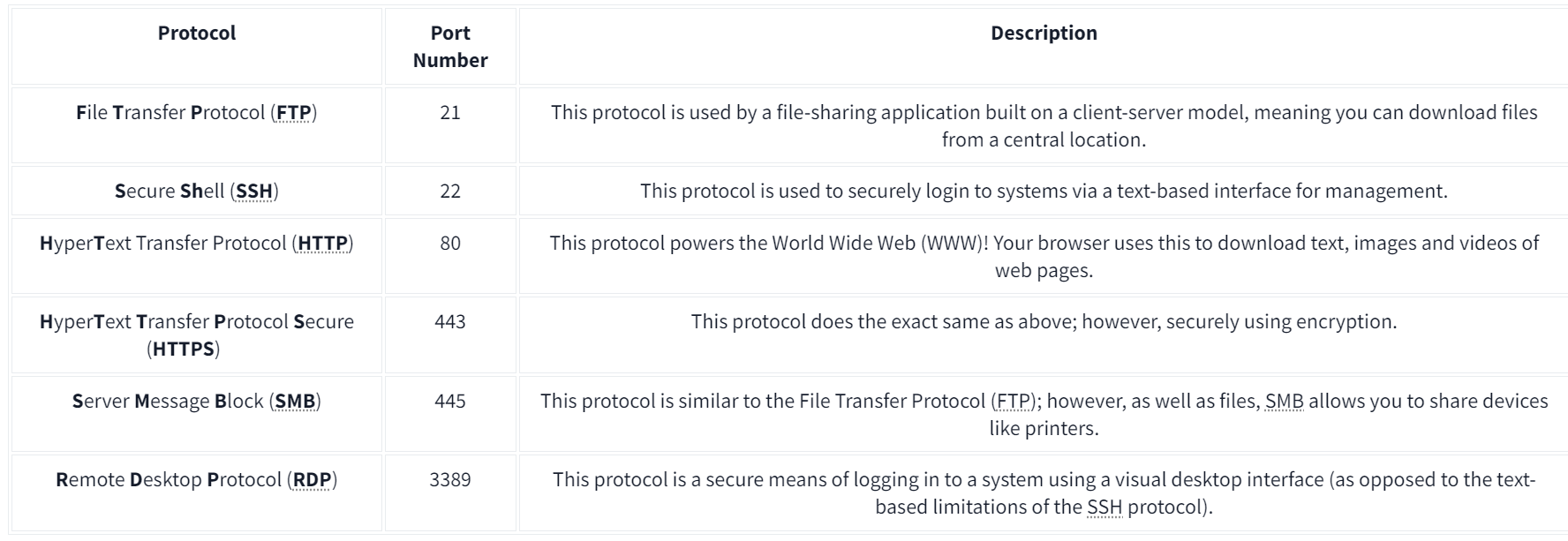
* Numerical values between 0 and 65535
* Risk of losing track of applications using each port

**Standard Port Assignment**

* Associate applications/software with standard port numbers
* Example: Web browsers use port 80
* Allows different software to interpret data consistently

**Common Ports**

* Ports between 0 and 1024 are common ports
* Standard rules assigned for common protocols/applications

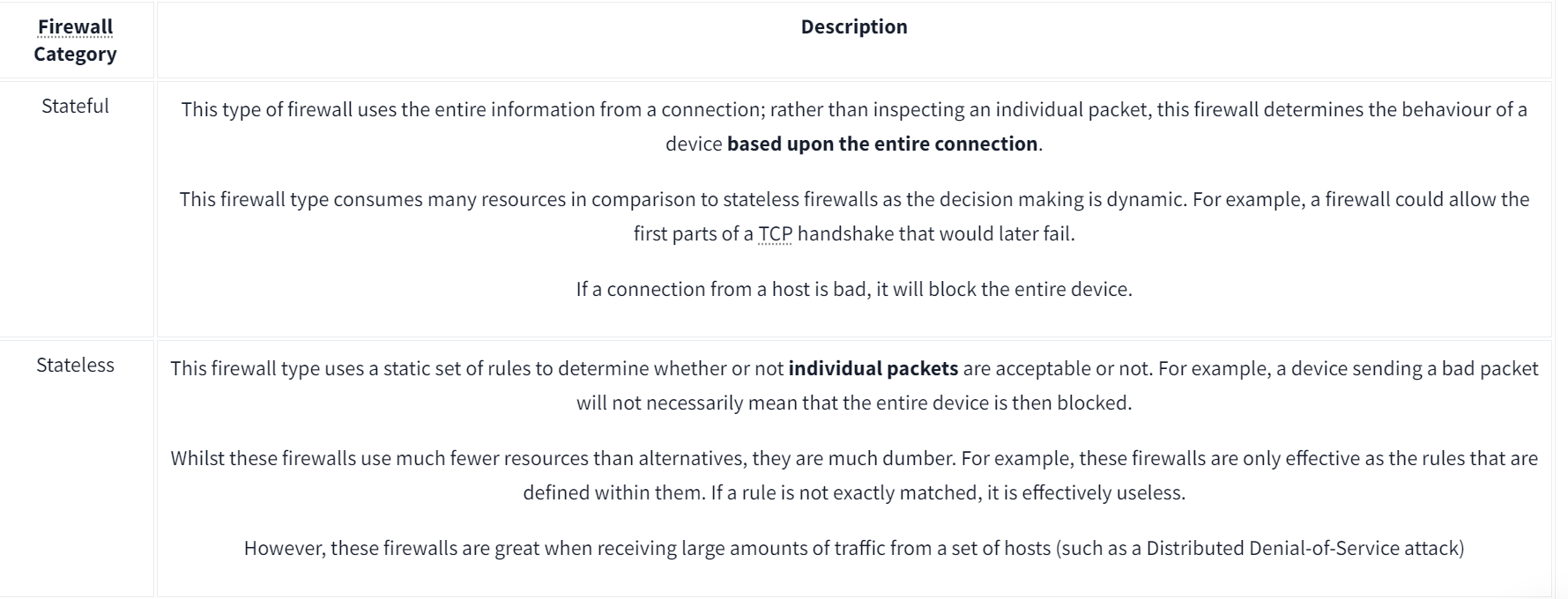


**To connect to a port such as 1234 using the IP address 8.8.8.8 you use this command:**

**nc 8.8.8.8 1234**

**Firewalls:**

Operate at layers 3 and 4. A stateful firewall inspects the entire connection while the stateless firewall inspects the individual packets.



# **VPN Basics**

## **What is a VPN?**

* A **V**irtual **P**rivate **N**etwork (VPN) is a technology that allows devices on separate networks to communicate securely by creating a dedicated path (tunnel) between them over the internet.
* Devices connected within this tunnel form their own private network.

## **Benefits of a VPN**

1. **Allows connecting networks in different locations**
   * Useful for businesses with multiple offices to access resources like servers/infrastructure remotely.
2. **Offers privacy**
   * Uses encryption to protect data, making it only understandable between the source and destination devices.
   * Protects traffic on public WiFi networks where no encryption is provided.
3. **Offers anonymity**
   * Used by journalists and activists to safely report in countries with controlled freedom of speech.
   * Hides traffic from ISPs and intermediaries, but anonymity level depends on VPN logging practices.
4. **Secure access to TryHackMe vulnerable machines**
   * Allows secure interaction with machines without making them directly accessible on the internet.
   * Prevents ISPs from thinking you're attacking machines on the internet.
   * Provides security to TryHackMe by not exposing vulnerable machines directly.

## **VPN Technologies**

1. **PPP (Point-to-Point Protocol)**
   * Used by PPTP for authentication and data encryption.
   * Uses private keys and public certificates for connection.
   * Non-routable (can't leave a network by itself).
2. **PPTP (Point-to-Point Tunneling Protocol)**
   * Allows PPP data to travel and leave a network.
   * Easy to set up and supported by most devices.
   * Weakly encrypted compared to alternatives.
3. **IPSec (Internet Protocol Security)**
   * Encrypts data using the existing Internet Protocol (IP) framework.
   * Difficult to set up but offers strong encryption if successful.
   * Supported on many devices.

# **What is a Router?**

* Job: Connect networks and pass data between them
* Uses routing process to create paths for data to travel across networks
* Operates at Layer 3 (Network Layer) of OSI model
* Interactive interface for configuration (port forwarding, firewalling, etc.)
* Dedicated devices, different from switches
* Routing protocols decide optimal path based on factors like shortest path, reliability, medium speed

# **What is a Switch?**

* Dedicated networking device for connecting multiple devices
* Operates at Layer 2 (Data Link Layer) or Layer 3 (Network Layer) of OSI model

## **Layer 2 Switches**

* Forward frames using MAC addresses
* Solely responsible for sending frames to correct devices

## **Layer 3 Switches**

* More sophisticated than Layer 2
* Can perform some router responsibilities
* Forward frames to devices (like Layer 2)
* Route packets to other devices using IP protocol

# **VLANs (Virtual Local Area Networks)**

* Technology to virtually split devices within a network
* Provides network separation and security
* Devices can share Internet connection but are treated separately
* Rules determine how specific devices communicate with each other
* Example: Sales and Accounting departments can access Internet but not communicate with each other