Port 22 – ssh

Port 80 – http

Port 443 – https

Port 5000 (arbitrary) – web server (api)

Port 80 is a well-known port number used in computer networking to facilitate communication between devices over the Internet using the Transmission Control Protocol (TCP). In the context of the Internet Protocol Suite, port numbers act as endpoints for network services and applications.

Specifically, port 80 is commonly associated with the Hypertext Transfer Protocol (HTTP), which is the primary protocol used for transmitting web pages and other web-related content across the Internet. When you enter a website address in your web browser, such as "http://www.example.com," the browser initiates a request to the web server hosting that website. This request is sent over port 80 by default, allowing the server to receive and respond with the requested web page.

In simple terms, port 80 serves as the default channel for web traffic. It is used by web servers to listen for incoming requests and send responses back to the client devices, enabling the retrieval and display of web content.

It's worth noting that port 80 is not limited to HTTP traffic. Other protocols, such as Hypertext Transfer Protocol Secure (HTTPS) and some application-specific protocols, can also utilize port 80. However, HTTPS typically operates on port 443 to ensure secure encrypted communication.

In summary, port 80 is a standard port number reserved for HTTP traffic, enabling the exchange of web content between clients (e.g., web browsers) and servers (e.g., web hosting providers).

Port 5000 is an arbitrary port number that can be used for various purposes. Unlike well-known port numbers (0-1023) that are assigned to specific services by the Internet Assigned Numbers Authority (IANA), port numbers above 1023 are generally considered unassigned and available for general use.

In the context of computer networking, port 5000 might be used by applications or services that require a specific port for communication. It is often selected by developers or system administrators for running web servers, APIs, or other networked applications.

For example, many developers choose port 5000 as the default port for running Flask applications, which is a popular Python web framework. When a Flask application is launched locally, it typically listens on port 5000 by default, allowing clients to access the application through that port. However, it's important to note that the choice of port number is not exclusive to Flask or any specific technology. Port 5000 can be used by various applications based on the preferences of the developers or system administrators.

In summary, port 5000 is an arbitrary port number that can be used for running networked applications or services. While it does not have any specific assignment or standard protocol associated with it, it is often chosen by developers for hosting web servers or APIs.

Port 22 is a well-known port number used for Secure Shell (SSH) protocol communication. SSH is a network protocol that provides a secure, encrypted method for remotely accessing and managing devices over an unsecured network, such as the internet.

Port 22 is specifically designated for SSH traffic, allowing secure communication between a client and a server. When a client wants to establish an SSH connection to a remote server, it initiates the connection on port 22. The SSH server listens for incoming connections on this port, and upon successful authentication, allows the client to securely log in and interact with the server.

SSH is widely used for various purposes, including remote administration of servers, secure file transfers, and tunneling encrypted connections. It offers strong encryption and authentication mechanisms, making it a popular choice for secure remote access to networked devices.

While port 22 is the default port for SSH, it is worth mentioning that some organizations or system administrators may choose to use a different port for SSH to enhance security. This practice, often referred to as "changing the SSH port," aims to make it harder for potential attackers to discover and target SSH services.

In summary, port 22 is the default port number assigned to SSH protocol communication. It enables secure remote access and management of devices over an unsecured network by establishing encrypted connections between clients and servers.

Port 443 is a well-known port number used for secure web communication. It is primarily associated with the Hypertext Transfer Protocol Secure (HTTPS), which is the secure version of HTTP used for transmitting web pages and other web-related content over the Internet.

HTTPS ensures that data exchanged between a client (such as a web browser) and a server (hosting a website) is encrypted and secure. When a client requests an HTTPS connection to a website, it initiates the connection on port 443. The server hosting the website listens for incoming HTTPS connections on this port, allowing the client to establish a secure, encrypted channel.

Port 443 is widely used for secure online transactions, secure logins, and any other web-based activity that requires data confidentiality and integrity. It is commonly utilized by e-commerce websites, online banking platforms, social media platforms, and other applications where secure communication is crucial.

HTTPS employs Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL), to establish an encrypted connection. TLS/SSL protocols provide encryption, authentication, and data integrity, ensuring that data transmitted between the client and server remains confidential and tamper-proof.

It is important to note that while port 443 is the default port for HTTPS, it can also be used for other secure protocols or applications. For example, some VPN (Virtual Private Network) services use port 443 to bypass network restrictions or firewall blocks that may be in place for other ports.

In summary, port 443 is the default port number assigned to secure web communication using HTTPS. It facilitates encrypted and secure data transmission between clients and servers, ensuring privacy and data integrity for web-based activities.