Virtual Computer Ports

Aylin DUBA, aylinduba@gmail.com

Abstract

Computer networks play a crucial role in today's businesses and homes. However, the complex nature of networks requires many different devices and services to communicate with each other. This communication is accomplished using many different physical ports. However, the number of these ports is limited and each device needs its own physical port. This is where virtual ports come into play.Virtual ports are virtual ports used to communicate between networks. These ports are used to provide data traffic between computers or between a computer and a device. Virtual ports are created via software and do not need physical ports. Virtual ports are commonly used in virtual environments, especially virtual networks. Virtual networks consist of a series of interconnected virtual machines or servers and are used to establish a secure connection between different devices. Virtual ports are used to route data traffic between these devices.

Content

1. Introduction to Port

Virtual points where network connections begin and stop are called ports. Ports are software-based and controlled by operating system. Each port is connected to a different procedure or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port number than webpages, for example , even though both reach a computer over the same Internet connection. Port number is a 16-bit logical address which is assigned to every application of your device and used to transmit data between computer network and application. [1]

Virtual ports are virtual ports used in computer networks instead of physical ports. Virtual ports are created through software and are an alternative way network administrators can use to enable different devices and services to communicate with each other. Virtual ports are often used in virtual environments such as virtual networks. Virtual networks consist of a series of interconnected virtual machines or servers and are used to establish a secure connection between different devices. Virtual ports are used to route data traffic between these devices.

Virtual ports have many advantages. First, virtual ports make it easy to move a device to different networks or between virtual machines. Because virtual ports are not physically connected to a particular network interface, it becomes easier to move virtual machines or servers. In addition, virtual ports reduce the number of physical devices, reducing costs and allowing network structures to become more flexible. Virtual ports can be used for different purposes. For example, a virtual port can be connected to a printer and print from another device. Another virtual port allows a server to connect to multiple networks virtually. Another use of virtual ports is network security. Virtual ports allow network administrators to monitor, limit or block the interactions of devices on the network. For example, a

network administrator can enable software on a computer to access only a certain virtual port, and access to other ports can be blocked.

The port, which exchanges data over numbers, is divided into values starting from 0 up to 65535 in order to perform many operations at the same time. In this context, the port is divided into two types, TCP and UDP.

2. Relationship of TCP/UDP Protocols to Ports

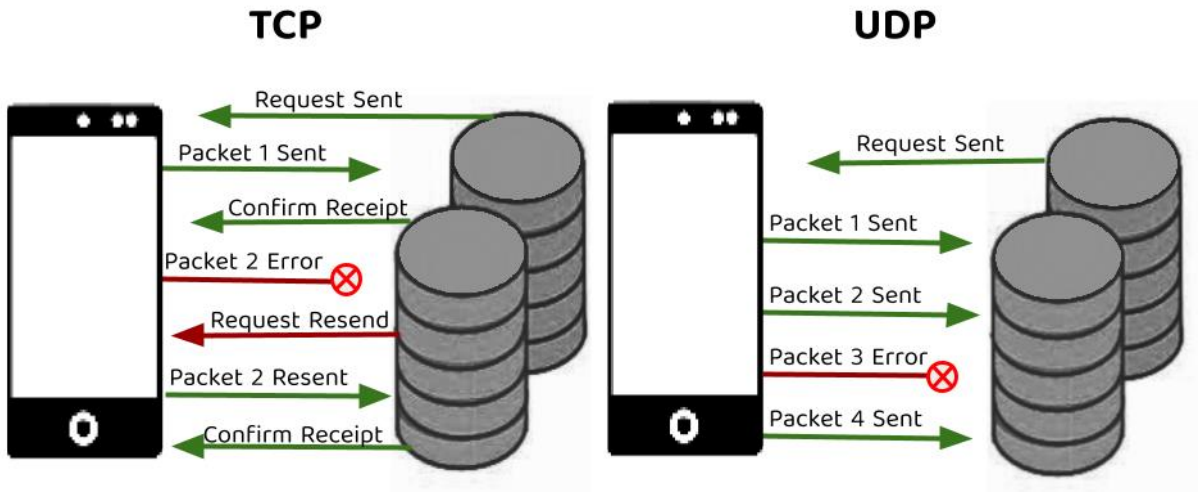

Figure 1: TCP/UDP Protocols [2]

TCP and UDP protocols are the two main protocols used for routing network traffic. These protocols are linked to virtual ports for proper routing of network data.

The TCP protocol provides reliable transfer of data packets. After the TCP connection is established, the data packets are enumerated and a successive series of numbered data packets is sent. Virtual ports assist in routing these enumerated data packets correctly. For example, a web server listens for web requests over TCP port 80.

The UDP protocol, on the other hand, provides fast transfer of data packets. UDP uses virtual ports to properly route data packets. However, the UDP protocol may experience problems such as lost or incorrect data packets. Therefore, the UDP protocol is used in situations where data packets need to

be transferred quickly, but its reliability is not the top priority. For example, a game server can listen for game requests over UDP port 27015.

Virtual ports also allow multiple protocols to correctly route data packets over the same network interface. This is common when multiple services are running on a single computer or server. For example, a web server can forward data packets of different protocols, such as HTTPS web traffic over TCP port 80 and TCP port 443, and DNS traffic over UDP port 53.

TCP and UDP protocols are linked to virtual ports for proper routing of network data. Virtual ports allow accurate routing of data packets of different protocols and make networking structures of network administrators more flexible.

2.1 Differences Between TCP and UDP

- TCP is slightly slower than UDP because it provides data integrity and authentication, but it comes before the UDP in terms of reliability,
- TCP is provided with this management flow system in UDP in packages and in order to send data during communication.
- TCP is preferred in holistic and lossless data streams, while UDP is preferred in sound and video communication.

	TCP	**UDP**
Reliability	High	Low
Speed	Low	High
Transmission Method Packages	Packages are sent in turn	Packages are sent in flow
Error Detection and Correction	Yes	No
Data Blockage	Yes	No
Received Approval	Yes	Only the sum of providing

3. Port Routing

Port routing, the direction of a communication protocol is a process to change the port number or to stop this communication protocol. Although the term referral is mentioned, it would be more accurate to say this processing port control. With a port orientation, the open ports of an IP address can be closed, closed ports can be opened, or open ports can be replaced by a different port number for cyber security reasons. [3]

- **Local Port Routing:** Local port orientation, which has the most common range of use, is the safest routing method for users. Local port orientation can also be defined as a safe tunnel. Users can use this tunnel to overcome firewalls that block some web pages.
- **Remote Port Routing:** This type of routing, which allows everyone to be connected to a single TCP protocol on a remote server, is the perfect for providing remote connection to a web server.
- **Dynamic Port Routing:** Contrary to the local routing method, dynamic port orientation, which is the least preferred type of routing, is another way to overcome the firewall obstacle. This orientation, which works with a tool label, is used to ensure the security of users on a public network.

4. Port Inquiry

The easiest way can be used to use port inquiry on the internet to make port inquiry on the Internet via IP address.

As a second method, you can also do the computer's command. For this you can follow the steps below:

1. Click the Start Menu and open the Command Prompt application by typing “Command Prompt” or “cmd” in the search section.

2. On the screen that opens, “telnet” command is in the form of space port number (Telnet 192.168.1.1 80) by typing a command.
3. With the netstat -an command, it is possible to see the ports where an IP address is open from the outside. With this command, you can see both the local code of the port and the outdoor code.

5. Cyber Security and Port Relationship

Virtual computer ports are ports specific to virtual machines created using virtualization technologies. These ports are used to communicate between virtual machines or between virtual machines and the physical network. In terms of cybersecurity, virtual computer ports can also pose a number of risks. Below are a few examples that will clarify the relationship between virtual computer ports and cybersecurity:

- **Vulnerabilities:** Vulnerabilities in virtual machine software could allow cyber attackers to access and attack the network through virtual computer ports.
- **Isolation:** Virtual computer ports must be configured correctly to achieve isolation, as they provide communication between different virtual machines. Misconfigured ports can expose one virtual machine to attacks that can harm others.
- **Data Integrity:** Data transported through virtual computer ports must be properly encrypted to maintain their integrity. Otherwise, an attacker could manipulate or steal the data.
- **Data Privacy:** Data transported through virtual computer ports must be properly encrypted to protect their privacy. Otherwise, an attacker could access the data and steal sensitive information.
- **Security Policies:** Virtual computer ports can be used to enforce network-specific security policies. However, if these policies are not configured

correctly, anyone with access to the network may be allowed to use the virtual computer ports.

In summary, virtual computer ports are used to communicate in virtualized environments. These ports can cause security vulnerabilities and data security issues. Virtual computer ports, when properly configured and protected, can improve network performance and enhance cybersecurity.

6. Top 100 Ports

Port Number	Service	Port Number	Service
20-21	FTP	989-990	FTP over SSL
22	SSH	**993**	IMAP over SSL
23	Telnet	**995**	POP over SSL
25	SMTP	**1194**	OpenVPN
43	WHOIS	**1337**	menandmice-dns
49	TACACS +	**1433-1434**	Microsoft SQL
53	DNS	**1521**	Oracle Listener
67-68	DHCP/BOOTP	**1701**	L2TP
69	TFTP	**1723**	PPTP
79	Finger	**1725**	MS PPTP
80	HTTP	**1741**	CiscoWorks 2000
82	Xfer	**1812-1813**	RADIUS
83	mit-ml-dev	**1985**	SAF
88	Kerberos	**2000**	Cisco SCCP
110	POP3	**2002**	Cisco ACS
111	RPC	**2049**	NFS
113	Ident	**2082-2083**	cPanel
115	SFTP	**2087**	eli
119	NNTP	**2100**	Oracle XDB
123	NTP	**2145**	GBM Pro
135	Microsoft RPC	**2222**	DirectAdmin
137-139	Microsoft NetBIOS	**3128**	HTTP Proxy
143	IMAP	**3260**	iSCSI
161-162	SNMP	**3306**	MySql
177	XDMCP	**3389**	RDP
179	BGP	**3478-3479**	STUN
194	IRC	**3689**	iTunes
201	AppleTalk	**4500**	NAT-T
389	LDAP	**4567**	Cisco TRAM
443	HTTPS	**5000**	UPnP
444	Microsoft SSP	**5001**	commplex-link
445	Microsoft DS	**5060**	SIP
464	Kerberos KDC	**5432**	PostgresSQL
465	SMTP Protocol over TLS/SSL	**5632**	PCAnywhere
497	Retrospect	**5800**	VNC over HTTP
500	ISAKMP	**5900**	VNC
512	exec	**5985**	WinRM
513	login	**6000-6001**	x11
514	syslog	**6379**	Redis
515	LPD	**6514**	Syslog using TLS
520	RIP	**6665-6669**	IRC
546-547	DHCPv6	**6881**	Bit Torrent
554	RTSP	**8000**	HTTP
587	SMTP	**8008**	HTTP Proxy
593	RPC over HTTPS	**8080- 8081**	HTTP
631	IPP	**8089**	Splunk
636	LDAP over SSL	**8443**	Mcafee
646	LDP	**9080**	IBM WebSphere Application Server
873	rsync	**10000**	BackupExec
902	Vmware	**11371**	OpenPGP

[4]

7. Missions of the Top 100 Ports

7.1 Ports 20 and 21: File Transfer Protocol (FTP)

FTP (File Transfer Protocol) runs on TCP/IP (Transmission Control Protocol/Internet Protocol) family protocols. TCP/IP is the basic set of protocols that allow computers on the internet to communicate with each other.

FTP establishes a connection using TCP (Transmission Control Protocol) protocol and transfers data over IP (Internet Protocol) protocol. TCP ensures data integrity and reliability and controls the process of receiving and delivering data packets. If it is IP, it makes sure that data packets are forwarded to the correct destination.

FTP typically uses TCP ports 20 and 21. Port 20 is used for FTP data connection, while Port 21 is used for FTP control connection. However, some FTP applications may also use different port numbers. For example, some FTP servers, when operating in passive FTP mode, transfer data using different port numbers. FTP (File Transfer Protocol), located on port 21, is a protocol used to transfer files. FTP is a standard for transferring files from one computer system to another computer system.

FTP establishes a connection between the server and the client and enables the transfer of files. The client connects to the server and performs file uploads or downloads. FTP also supports file management operations such as viewing the list of files on the server, changing the file name and size, deleting or creating files.

FTP is frequently used, especially for website administration. Website owners can upload and update their web pages and files to the server via FTP. There are alternative file transfer protocols available, especially since the use of FTP poses

a security risk. However, many businesses and websites still use FTP for file transfer.

7.2 Port 22: Secure Shell Protocol (SSH)

Port 22 is a reserved port for SSH service. SSH is a network protocol used for secure remote access and file transfer. This protocol provides security features such as encryption of network connections and authentication methods. For this reason, SSH is often used on Linux and Unix-based systems.

A user can establish an SSH connection to a remote computer using an SSH client software. The SSH connection allows the user to securely access the remote server from the client software. Once the SSH connection is established, users can perform operations on the remote server or download and upload files from the remote server using a command prompt.

Port 22 may also be blocked by some network routers and firewalls. These blocks can be used to monitor or block inbound and outbound SSH traffic. Therefore, in case of problems during SSH connections, it is important to check if port 22 is open.

Port 22 is a TCP (Transmission Control Protocol) port reserved for the Secure Shell (SSH) protocol. TCP is a connection management protocol designed for reliable communication and is ideal for protocols that require security considerations such as SSH. TCP ensures that every packet arriving at the target device is verified and reconnects in case of interruptions in the connection. Because of these features, TCP is often the preferred protocol for reliable operation of protocols such as SSH.

7.3 Port 23: Telnet Protocol

Port 23 is a reserved port for the Telnet protocol. Telnet is a protocol used to provide remote access to a computer on a network. This protocol allows to connect to a remote computer and perform operations via command line interface.

The Telnet protocol uses a client-server model. Telnet client software allows a user to connect to a remote server, while Telnet server software is server-side software that allows remote access.

Telnet protocol runs on TCP (Transmission Control Protocol) and authentication information such as username and password is provided when opening the connection. Since Telnet provides access to the command line interface of a remote computer, it allows all operations that can be done on the server to be done remotely. However, the Telnet protocol is vulnerable because the authentication information is not encrypted.

The Telnet protocol performs a similar function to the SSH protocol. However, the SSH protocol provides more secure communication than the Telnet protocol and offers security features such as encryption and authentication. Therefore, SSH protocol is preferred over Telnet in modern networks.

7.4 Port 25: Simple Mail Transfer Protocol (SMTP)

Port 25 is a reserved port for Simple Mail Transfer Protocol (SMTP). SMTP is a standard network protocol used for sending electronic mail. Therefore, Port 25 is the access point of the servers used for sending e-mails.

Port 25 is typically used by SMTP servers provided by Internet service providers. These servers manage the incoming and outgoing e-mails of their customers' e-mail accounts. SMTP servers use other protocols such as POP3 or IMAP to receive and correctly deliver incoming email to customers' email accounts. It also uses the SMTP protocol to send customers' emails to different destinations.

Port 25 can also be used outside of the SMTP protocol. In some cases, port 25 can also be used to use a different protocol instead of a different SMTP server. However, usually port 25 is used as a reserved port for the SMTP protocol.

Port 25 is usually used over the TCP (Transmission Control Protocol) protocol. SMTP works over the TCP protocol and consists of many stages when establishing a connection. This data includes server authentication, using email sending, protecting email data, and terminating the connection after checking.

UDP (User Datagram Protocol) protocol provides fast and secure transport of data packets. However, the UDP structure does not provide any security in receiving data. Therefore, secure and critical services such as Port 25 are often run over the TCP protocol. The TCP structure encrypts secure and accurately delivers sockets, and performs a lot of error checking throughout the connection process. Therefore, TCP protocol is preferred for security and cages for secure and critical services such as SMTP.

7.5 Port 43: WHOIS Protocol

Port 43 is a reserved port for the WHOIS protocol. WHOIS is a protocol used to query the identity and ownership information of domain names registered on the Internet. Therefore, Port 43 is used for WHOIS queries.

Port 43 is typically used by WHOIS servers serving WHOIS data. These servers are operated by domain registrars or domain registrars. A WHOIS query displays information such as a domain owner's identity, contact information, registration date, last updated date, and the domain's status. This information helps to authenticate the domain name and identify authorized persons.

Port 43 can also be used outside of the WHOIS protocol. In some cases, port 43 can also be used to use a different protocol. However, usually port 43 is used as a reserved port for WHOIS queries.

Port 43 is usually used over the TCP (Transmission Control Protocol) protocol. The WHOIS protocol works over the TCP protocol and consists of many steps when establishing a connection. The WHOIS query establishes a TCP connection

to receive a response from the server. This connection remains open until it receives the server's response, and then terminates.

7.6 Port 49: TACACS+ Protocol

Port 49 is a reserved port for the TACACS+ protocol. TACACS+ (Terminal Access Controller Access Control System Plus) is a network security protocol that helps network administrators provide access and authentication control to devices on the network.

The TACACS+ protocol provides secure transfer of authentication information such as username and password to login to network devices. It also allows network administrators to control and manage access privileges to specific network devices.

Port 49 is used for the TACACS+ protocol to work. The TACACS+ server listens on port 49 and accepts incoming connection requests and authenticates via the TACACS+ protocol. Therefore, Port 49 is an important port that network administrators use to provide access and authentication control to network devices.

The TACACS+ protocol runs on TCP (Transmission Control Protocol). TCP is a protocol that provides secure and accurate data transmission. The TCP protocol is preferred because security and accuracy are important when transferring sensitive information such as the TACACS+ protocol, authentication information. The TCP protocol ensures the correct delivery of data packets and performs a lot of error checking during communication. Therefore, the TCP protocol is preferred for services that require security and accuracy, such as the TACACS+ protocol.

7.7 Port 53: Domain Name System (DNS)

Port 53 is usually reserved for the use of the DNS (Domain Name System) service. DNS resolves a computer name (hostname) or IP address on the internet,

so that the client is directed to the correct server for the service requested. DNS is critical to the operation of the internet and websites, email servers, application servers and many other internet services are made accessible to users through DNS. Other than that, there may be other services using port 53. However, port 53 is not recommended for services other than DNS service, because DNS service is a critical component for the correct functioning of the internet, and thus allocating port 53 to another service may threaten network security.

Port 53 handles both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols. However, usually DNS traffic is forwarded over the UDP protocol. UDP is a protocol that can carry small packets of data quickly and efficiently, and DNS typically works with short queries and replies, so it has the advantage that UDP is a faster and less resource consuming protocol. However, the TCP protocol can be used for some DNS operations, especially large queries or DNSSEC validation operations.

7.8 Port 67-68: Dynamic Host Configuration Protocol (DHCP) / Bootstrap Protocol (BOOTP)

Ports 67 and 68 are reserved for the DHCP (Dynamic Host Configuration Protocol) service. DHCP is a protocol that automatically assigns network configuration settings such as IP addresses, subnet masks, default gateways, DNS servers, and other network configuration information to devices (computers, phones, tablets, printers, etc.) on a network. DHCP simplifies network configuration for network administrators and prevents problems caused by misconfigured IP addresses or network settings.

DHCP consists of two main components: DHCP server and DHCP client. The DHCP server provides network configuration information, and DHCP clients communicate with the DHCP server to obtain this information. DHCP clients send a request to the DHCP server when they connect to the network, and the DHCP

server responds to the client with information it can use, such as its IP address, network configuration information, and lease duration.

DHCP is an enhanced version of BOOTP. DHCP is more flexible and scalable compared to BOOTP. BOOTP is designed to manage IP addresses of only a limited number of network devices. However, DHCP is designed to manage the IP addresses, network configuration information, and services of devices on larger networks. DHCP is based on the BOOTP protocol, and the DHCP server can also be understood by BOOTP clients. Although BOOTP does not have the features of DHCP, it is still used by some legacy systems.

DHCP (Dynamic Host Configuration Protocol) can use both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols. DHCP usually uses UDP on IPv4 networks. These messages are sent over UDP when the DHCP server responds to the DHCP client with network configuration information. These messages typically include the client's IP address, subnet mask, default gateway, and DNS server addresses. DHCPv6 (DHCP for IPv6) can use both UDP and TCP protocols when used on IPv6 networks. DHCPv6 messages are carried over UDP or TCP in the IPv6 protocol stack. DHCP uses TCP less frequently and is generally preferred, especially when a private connection is required between the DHCP server and its client. For example, TCP can be used when the DHCP server needs to use a remote resource such as a database or configuration file. However, for the core functions of DHCP, UDP is often the faster and more efficient option.

7.9 Port 69: Trivial File Transfer Protocol (TFTP)

Port 69 is used by the TFTP (Trivial File Transfer Protocol) protocol. TFTP is a protocol used to process files between devices on the network. TFTP has a simpler structure than the FTP (File Transfer Protocol) protocol and is specifically designed for fast handling of small files such as firmware or media files. TFTP runs over UDP and is faster than TCP but also less secure.

Port 69 is listened to by the TFTP server and used by TFTP receivers. TFTP guards can upload or download files by connecting to the TFTP server on the network. TFTP is mainly used hanging in embedded systems such as network devices (router, switch, access point, etc.). These devices often have very little memory and no disk cells, so it may not be possible to use larger protocols such as FTP or HTTP for uploading or downloading larger files. In this case, TFTP is an ideal solution for fast transfer of small files. Port 69 is used by the TFTP protocol and is used to transfer files between devices on the network. TFTP is especially used when transferring small files quickly, and images that cannot be used by larger protocols such as FTP are found especially in embedded systems.

TFTP (Trivial File Transfer Protocol) can use both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols, but works over UDP by default.

UDP is a more suitable choice for TFTP because TFTP file transfers can be handled by UDP, which is a unidirectional and lossless protocol. TFTP file transfers are performed in small packets and are provided by the TFTP protocol for data integrity. Therefore, there is no need to use a slower and more secure protocol such as TCP.

However, TCP can also be an option for TFTP if there are connection problems between the TFTP server and client or if large files need to be transferred. TFTP server can perform file transfer by establishing a connection with its client over TCP.

7.10 Port 79: Finger Protocol

Port 79 is used by the Finger protocol. Finger is a protocol that allows users on the network to exchange information. The Finger protocol is used to fetch information about the users they want to learn about, using the names or user IDs

of other users. This information usually includes personal information such as the user's name, phone number, e-mail address, last login date, role or title, if any.

Port 79 is listened by Finger server and used by Finger clients. Finger clients can get the information of the users they want to know about the users by connecting to the Finger server on the network.

Finger protocol is widely used especially for UNIX or Linux systems. Finger is supported by many systems, but nowadays it is disabled by default on many systems due to security vulnerabilities.

Finger protocol usually runs on TCP (Transmission Control Protocol). TCP provides reliable data transfer, so requests provided by Finger clients and responses by Finger servers are transmitted accurately and completely. However, in some cases, the Finger protocol can also work over UDP. In particular, UDP may be more appropriate when forwarding some queries that require fast responses. However, these situations are rare and TCP is generally preferred.

7.11 Port80: Hypertext Transfer Protocol (HTTP)

Port 80 is a port listened by web servers. Web servers are computers that host web pages on the internet and work to serve these pages to users. Web browsers are also programs that allow users to view web pages.

Web browsers send HTTP requests to web servers to get the web pages that the user requested. HTTP is a protocol that enables the transfer of web pages on the internet. HTTP requests are usually sent over TCP. TCP provides reliable data transfer and ensures that HTTP requests are transmitted accurately and completely.

Web servers send web pages to the web browser using the HTTP protocol in response to HTTP requests. These replies are also usually sent over TCP. Therefore, Port 80 usually runs over TCP.

In addition, Port 80 can also be used by the HTTPS protocol. HTTPS is a protocol that provides secure transfer of web pages. HTTPS provides data integrity and confidentiality by using SSL/TLS encryption protocols. When the HTTPS protocol runs on Port 80, it usually runs on TCP.

7.12 Port 82: Xfer

The term "Xfer" is short for "transfer" and means "transfer". "Port 82" is a port that is usually used for special purposes and is not used by a standard service.

In some cases, a particular application or service performs file transfer operations using Port 82. For example, some FTP (File Transfer Protocol) servers may use Port 82 as an alternative data connection port. In this case, the FTP server communicates between Port 21 (command port) and Port 82 (data port) for file transfer.

However, as there are no specific restrictions or guidelines on the use of Port 82, the term "Xfer" can also be used in other contexts. For example, the term "Xfer" may also be used when transferring files on a different port specified by a particular application or protocol.

Consequently, it is possible for Port 82 to be used as an alternative data connection port for file transfer operations, in which case the term "Xfer" may be used. However, the use of Port 82 is entirely dependent on a particular application or service and is often used for special purposes.

7.13 Port 83: MIT-ML-Device (mit-ml-dev)

Port 83 is a port usually used for special purposes and is determined by a particular application or service. Mit-ml-dev, on the other hand, is a device or server used in the artificial intelligence laboratory of the Massachusetts Institute of Technology (MIT). This device or server may use Port 83 as an alternative HTTP (HyperText Transfer Protocol) port by a particular application or service.

However, given that this port is used by a specific application or service and is specific to a particular device or server, such as Mit-ml-dev, the connection between Port 83 and Mit-ml-dev may not be pinpointed. However, it is generally known that Port 83 is not widely used and is determined by a particular application or service.

7.14 Port 88: Kerberos Protocol

Port 88 is used by the network authentication protocol called Kerberos. Kerberos is used especially in large organizations to enable users and services to access the network securely.

Kerberos uses a three-component architecture to authenticate users: user, service, and trusted third party. The user provides a credential (username and password) and creates a request when they want to access the service. The service allows the user to access the resources they want, and the trusted third party manages the authentication and ensures that the users' credentials remain confidential during authentication processes.

Port 88 is used to forward Kerberos authentication traffics. Kerberos traffic can be sent over TCP or UDP. TCP is used for connections that require higher security, while UDP is preferred for connections that require lower latency.

Port 88 is used specifically by Microsoft's network authentication and management service called Active Directory. This service enables users to log on to Windows operating systems and allows them to access network resources. In addition, Kerberos can be used on other Linux and UNIX systems, and Port 88 is used on these systems.

7.15 Port 110: Post Offive Protocol version 3 (POP3)

Port 110 is used by an email protocol known as Post Office Protocol version 3 (POP3). This protocol allows a user to download their e-mail by accessing the e-mail server.

POP3 allows users to download their e-mail from the server and save it on their local computer. This allows the user to access their email at any time even without an internet connection. However, downloading emails from the server means backing up emails stored on the server to users' computers. Therefore, the POP3 protocol has become less popular like other email protocols (eg IMAP) that allow users to keep their emails on the server.

The POP3 protocol requires the user to connect to the email server via TCP. This connection starts with a login with authentication information such as the user's email address and password. Then the user can use different POP3 commands to list, download or delete the emails stored on the server. Popular email clients include Microsoft Outlook, Mozilla Thunderbird, and Apple Mail.

Port 110 carries POP3 traffic using the TCP protocol. However, modern email applications can encrypt traffic with SSL/TLS encryption using the POP3S (POP3 over SSL) protocol, which is a more secure version of POP3. POP3S communicates over TCP port 995.

7.16 Port 111: Remote Procedure Call (RPC)

Port 111 is a port used for the operation of protocols that provide access to remote servers on the network using the RPC (Remote Procedure Call) service. RPC is used as a protocol for the management and use of programs on a remote server on a computer network.

Port 111 is a port used especially in UNIX and Linux based systems. Programs running on this port include protocols such as Network File System (NFS), Network Information Service (NIS), and Remote Procedure Call (RPC). These protocols are used to provide data or services from servers to clients.

NFS is a protocol that provides remote access to files and folders on UNIX and Linux systems. This protocol is used to remotely access the disks of a

computer on a network. NIS is used to manage user accounts, passwords, and other network credentials on UNIX and Linux systems.

RPC, on the other hand, is used as a protocol for the management and use of programs on a remote server on a computer network. This protocol allows a program on one computer to call and use the functions of a program on another computer. RPC is mainly used for databases, e-mail, and other network services.

Port 111 can use both TCP and UDP protocols. However, some protocols such as NFS and NIS only use the UDP protocol, while other protocols can generally work with both TCP and UDP protocols. Therefore, the RPC protocol can be used over both TCP and UDP, depending on the specific type of network traffic the protocol will use.

7.17 Port 113: Identity Protocol (Ident)

Port 113 hosts a service also known as "authentication service", while the Ident protocol is a protocol used in authentication processes. The Ident protocol uses username and port information to authenticate a user.

The Ident protocol is used to authenticate a user when they connect to a server. Using port information, the Ident protocol can identify which user is connecting to which service. This information can be used by the server to perform authentication by sending it to an authentication server.

Since Port 113 is used for authentication processes, the Ident protocol also works over Port 113. Using Port 113, the Ident protocol connects to an authentication server and authenticates the user. Therefore, there is a tight coupling between Port 113 and the Ident protocol, and the Ident protocol is often associated with Port 113.

The identity protocol (Identifier Protocol) runs on TCP port 113.

7.18 Port 115: Simple File Transfer Protocol (SFTP)

Port 115 is a reserved port number for SFTP (Simple File Transfer Protocol). However, SFTP works using a different protocol, SSH (Secure Shell), and is forwarded to port 22, which is the port number that SSH uses.

SFTP is a network protocol used to transfer files. Although similar to FTP (File Transfer Protocol), SFTP is a completely different protocol and, unlike FTP, encrypts all data transfers. Therefore, SFTP is a more secure method of file transfer and is often used, especially when transferring files over the Internet.

SFTP runs on the SSH protocol and takes advantage of the authentication, encryption, and data integrity features that SSH provides. SFTP provides various commands to perform file management operations (upload, download, delete, rename, etc.). It also works with a limited user account on the server side, which makes SFTP more secure.

SFTP (Secure File Transfer Protocol) protocol uses TCP (Transmission Control Protocol). In order for SFTP to transfer files securely, the TCP protocol within the TCP/IP protocol family is used to ensure data integrity and security. TCP provides error correction and flow control to ensure data is transmitted correctly.

7.19 Port 119: Network News Transfer Protocol (NNTP)

Port 119 is the default port of Network News Transfer Protocol (NNTP). NNTP is a protocol for accessing and broadcasting Usenet newsgroups.

NNTP allows articles in newsgroups to be requested from servers and sent. By connecting to the server, the client can perform operations such as listing, reading and replying to articles in a particular newsgroup.

The NNTP protocol can set an expiration date to ensure regular deletion of messages posted in newsgroups. Thus, old messages can be deleted automatically and the newsgroup database can be cleaned.

Port 119 is used for NNTP's communication. NNTP works over TCP and port 119 is usually used. TCP is a communication protocol that provides error correction and flow control to ensure data integrity and security.

7.20 Port 123: Network Time Protocol (NTP)

Port 123 hosts a service called Network Time Protocol (NTP). NTP is a protocol used to synchronize accurate time over the internet. NTP servers take time information from their source and use it to provide accurate time to other devices on the network.

NTP is of great importance in time synchronization. For example, accurate timing is required in many areas such as banking systems, telecommunications infrastructure, aerospace systems, satellite systems, blogging and even scientific research. NTP ensures consistent time keeping between devices on the network, a critical requirement for many critical applications.

NTP usually uses the UDP protocol and runs on port 123 by default. NTP servers can be located locally on the network or on the internet. When using NTP for time synchronization, it is important to be careful with the NTP server selection for security reasons. An untrusted or unverified NTP server can prevent network devices and applications from getting the correct time and can even seriously affect system operation.

7.21 Port 135: Microsoft Remote Procedure Call (RPC)

Port 135 is a reserved port for the RPC (Remote Procedure Call) service used in Microsoft Windows operating system networks. RPC is a protocol used to communicate between different computers on a network. RPC allows many different services to communicate, especially those used on Windows operating system networks. Therefore, Port 135 is very important for communication between Windows operating systems.

RPC works using a client-server model. A client requests the server to perform a certain action by making an RPC call. The server receives the client's request and performs the requested action. The result is sent back from the server to the client. In this way, many different services can communicate with other computers using the RPC protocol.

RPC can use other ports besides Port 135. However, Port 135 is usually the first port used for RPC service. RPC also supports the DCOM (Distributed Component Object Model) protocol, and DCOM usually runs on Port 135.

Port 135 is usually used with the TCP protocol. However, in some cases, the UDP protocol can also be used. However, these situations are very rare and are usually seen in networks where RPC (Remote Procedure Call) traffic is heavily used.

7.22 Port 137-139: Microsoft NetBIOS

In the port range 137-139 there are some services used for Windows operating system network services called NetBIOS. These services are:

NetBIOS Name Service (NBNS) - Port 137 UDP: This service is used for NetBIOS name resolution. NetBIOS names are mapped to IP addresses and other computers on the network are accessed.

NetBIOS Session Service (NBSS) - Port 139 TCP: This service is used to perform NetBIOS operations. These processes include file and printer sharing, file transfer, and other network interactions.

NetBIOS Datagram Service - Port 138 UDP: This service performs data transmission over NetBIOS networks. This service provides a low-level data transmission service.

These services are used by the Windows operating system and are typically used for network sharing and file transfer. These services can use TCP and UDP

protocols. NBNS uses UDP port 137, NBSS uses TCP port 139, and NetBIOS Datagram Service uses UDP port 138.

7.23 Port 143: Internet Message Access Protocol (IMAP)

Port 143 is used for one of the e-mail protocols, IMAP (Internet Message Access Protocol). IMAP is a protocol where e-mail messages are stored on the server and client programs can access these messages over the network.

IMAP servers listen on Port 143 to give users access to their email accounts. Client programs can access e-mail messages by connecting to the IMAP server via this port. IMAP servers typically use SSL/TLS encryption to secure communications, in which case SSL/TLS encrypted IMAP connections over Port 993 are used.

IMAP provides many advantages to users due to the fact that e-mail messages are stored on the server. For example, e-mail messages can be accessed by more than one device or client program connecting to the IMAP server. In addition, email messages stored on the IMAP server can be downloaded to users' local computers, helping to save local storage space.

IMAP uses the TCP protocol. Therefore, TCP connections over Port 143 are accepted. IMAP servers typically use SSL/TLS encryption to secure communications, in which case SSL/TLS encrypted IMAP connections over Port 993 are used.

7.24 Port 161-162: Simple Network Management Protocol (SNMP)

Ports 161 and 162 are ports used for Simple Network Management Protocol (SNMP). SNMP is a protocol used for management and monitoring of network devices and servers. This protocol monitors the status of hardware, software, and network resources on network devices and provides reports to administrators.

SNMP administrators can access and manage network devices using the SNMP protocol.

Port 161 is used to carry request and response messages between the SNMP manager and the SNMP agent. Port 162 is used by the SNMP agent to send a trap message to the SNMP manager in case of a possible error.

The SNMP protocol is especially important for the management of large networks. Network administrators can monitor the status of network devices and servers using the SNMP protocol. In this way, they can detect problems that may occur in the network in advance and take measures to solve the problems. The SNMP protocol also supports management operations such as remotely accessing network devices, making configuration changes, and performing software updates.

The SNMP protocol uses the UDP (User Datagram Protocol) protocol over Port 161 and Port 162. SNMP request and response messages are transmitted as UDP packets between the SNMP manager and the SNMP agent. SNMP trap messages are also sent in UDP packets.

7.25 Port 177: X Display Manager Control Protocol (XDMCP)

Port 177 is used for X Display Manager Control Protocol (XDMCP). XDMCP allows one computer on the network to share another computer's screen and unlock passwords remotely. This protocol is used in the X Window System (a graphical user interface) and allows a computer to connect to a remote server computer.

Port 177 is used for XDMCP power-on operations and responses. XDMCP scope sends a request to the server that is requested to be retained, and if the server accepts the request, a login screen opens on its computer.

XDMCP uses TCP and UDP protocols. However, TCP is generally preferred because TCP provides a more reliable connection and better dealing with issues such as connection dropouts and packet loss.

7.26 Port 179: Border Gateway Protocol (BGP)

Port 179 is a port used for Border Gateway Protocol (BGP). BGP is a protocol used to manage IP routing between internet networks. BGP is used by internet service providers (ISPs) and allows different networks to communicate with each other.

Port 179 is used to carry control traffic for BGP. BGP carries a lot of information required for IP routing and shares information with other BGP hops over port 179.

BGP uses the TCP protocol. TCP provides reliable data transmission and is widely preferred for transmission of important network protocols such as BGP. TCP protocol provides precise sequencing, error checking, resending etc for BGP messages. performs transactions.

7.27 Port 194: Internet Relay Chat (IRC)

Port 194 is used for Internet Relay Chat (IRC). IRC is a protocol that allows users to instant messaging and chat over the internet. It was first developed in Finland in 1988 and is still used today. There are several different ports used by IRC servers and clients, but the most widely used is port 194.

On IRC, users can chat in channels or send private messages on different topics. It also has other features such as file sharing. IRC channels are often used to chat between people with similar interests. For example, channels such as #music to chat about a band and #gaming to chat about a video game.

One of the biggest advantages of IRC is that users can stay anonymous. Users can chat by choosing a nickname and do not have to give any information about

their real identity. However, IRC can also be a domain for spam, malware, and other security threats, so users need to be careful.

IRC usually works over TCP (Transmission Control Protocol). TCP is used to provide a reliable flow of data and is required in IRC to prevent messages from being lost.

7.28 Port 201:AppleTalk Routing Maintenance

Port 201 is used for AppleTalk Routing Maintenance. AppleTalk is a network protocol developed by the Apple company and was previously used for file sharing, printer sharing, and other network services between Apple products.

AppleTalk Routing Maintenance is used to update routing information, create routing tables, and make routing decisions over the AppleTalk protocol. These functions are important to enable communication between computers on the network.

However, the AppleTalk protocol was officially abandoned in 2011 and is no longer supported by Apple. Therefore, Port 201 is not generally used and is rarely seen nowadays.

7.29 Port 389: Lightweight Directory Access Protocol (LDAP)

LDAP is a protocol typically used for managing large organizations' access to network resources. These resources can include user accounts, passwords, groups, email addresses, address books, devices, and other data. This data is stored in a hierarchical structure called an LDAP directory.

The LDAP protocol is based on the client-server model, and an LDAP client can connect to an LDAP server to read, write, update and delete data. LDAP runs over TCP and uses port 389 by default. However, secure LDAP (LDAPS) port 636 can also be used for SSL/TLS encryption.

The LDAP protocol uses a simple, query-based language and provides clients with a set of standard commands to interact with resources on the LDAP server. These commands can include user authentication, changing passwords, querying the address book, and searching for an e-mail address.

LDAP is especially frequently used by large organizations as it helps organizations manage their network resources from a central location. In addition, the LDAP protocol is supported by a number of popular directory service providers such as Active Directory.

7.30 Port 443: Hypertext Transfer Protocol Secure (HTTPS)

Port 443 is reserved for HTTPS (Hypertext Transfer Protocol Secure), a communication protocol used on the internet. HTTPS provides secure encryption of data transfer between websites. There are various services to provide secure communication using port 443.

1. **HTTPS (HTTP Secure):** It is the secure version of the HTTP protocol. It allows Internet users to securely connect to websites. HTTPS provides encryption of all data between the website and the user using TLS/SSL protocols.
2. **SMTPS (Simple Mail Transfer Protocol Secure):** SMTPS is a protocol used for e-mail communication. SMTPS provides secure sending of emails using TLS/SSL protocols. This prevents emails from being read or modified by third parties.
3. **FTPS (File Transfer Protocol Secure):** FTPS is a protocol used for file transfer. FTPS provides secure transfer of files using TLS/SSL protocols. This prevents files from being intercepted or modified by third parties.
4. **VPN (Virtual Private Network):** VPN is a technology that securely encrypts communication between devices in a network. Using VPN, internet traffic is encrypted and users' data cannot be intercepted by third parties.

5. **RDP (Remote Desktop Protocol):** RDP is a protocol used to provide remote access to a computer. RDP allows users to remotely connect to their computers and keep working. This protocol uses TLS/SSL protocols to secure remote access operations.
6. **IMAP (Internet Message Access Protocol) SSL:** IMAP is a protocol used for email clients to communicate with email servers. IMAP SSL provides secure transfer of emails using the IMAP protocol. This protocol prevents emails from being intercepted or modified by third parties.

These services are designed to keep internet users' data safe. Thanks to these protocols, users can securely transfer their sensitive data on the internet.

HTTPS (Hypertext Transfer Protocol Secure) is a secure protocol used for data transfer over the internet. HTTPS is the secure version of the HTTP protocol and uses Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols to encrypt data. These protocols ensure that data is transmitted securely.

HTTPS is especially preferred for transferring sensitive data such as financial transactions. HTTPS prevents data from being intercepted or modified by third parties. This protocol takes various measures to ensure the security of users' data.

Primarily, HTTPS uses TLS or SSL protocols for data encryption. These protocols use symmetric key cryptography or public key cryptography, which is used to encrypt data. The data is encrypted during the communication between the website server and the user's browser, thus preventing it from being intercepted or modified by third parties.

Second, HTTPS provides the authentication process between the website server and the user's browser. Using SSL/TLS certificates, the website server is authenticated and the user's browser makes sure that it is communicating with the correct server.

HTTPS uses TCP. HTTPS is the secure version of the HTTP protocol and uses TLS/SSL protocols for data encryption. These protocols run on TCP and ensure that data is transmitted correctly.

7.31 Port 444: Microsoft Security Socket Proxy Protocol

The Microsoft Secure Socket Proxy (SSP) protocol is a protocol used by Windows operating systems and is designed for authentication and secure communication. SSP is mainly used in Active Directory Domain Services (AD DS) environments and provides secure authentication between computers.

SSP works at the operating system level and uses SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols to establish a secure connection. SSP is part of the Windows Authentication Architecture and uses the Active Directory database to authenticate the user's credentials. In this way, users can securely authenticate and perform transactions in accordance with their authority.

Port 444 is a port number recommended by the SSP protocol. SSP communicates over this port, thus providing a secure connection. However, the SSP may also use a different port number other than port 444. Since the SSP protocol is a protocol used primarily in Windows operating system and Active Directory environments, it is not usually used by a specific application or service.

SSP protokolü, TCP (Transmission Control Protocol) tabanlı bir protokoldür ve güvenli bir bağlantı sağlamak için TCP üzerinden çalışır. TCP, bağlantı tabanlı bir protokol olduğu için, SSP'nin güvenli bir şekilde veri transferi yapabilmesi için önce bir bağlantı kurması gerekir. SSP, bu bağlantıyı kurduktan sonra, verileri güvenli bir şekilde iletebilmek için SSL ve TLS protokollerini kullanır.

7.32 Port 445: Microsoft Domain Controller (DC)

Microsoft DC (Domain Controller) resides within a database-based authentication and management system called Microsoft Active Directory (AD). Active Directory is a database used to manage user accounts, computer accounts,

printers, and other network resources in a network environment. Active Directory provides management of all resources in the network through DCs.

DC is a central authentication mechanism that enables users to authenticate in the Active Directory environment. DCs host and allow or deny use of user accounts, computer accounts, and other network resources. Users' access permissions to network resources are managed by the DC and access permissions to these resources are assigned to users.

DC is also a server role used to manage all the resources available in the Active Directory environment. DCs are servers that host the Active Directory database and they run a Windows service called Active Directory Domain Services (AD DS). This service handles the management and authentication of resources in the Active Directory environment.

DC is used to manage user accounts, computer accounts, printers, and other network resources in large-scale network environments. Because DCs provide centralized management of resources in the network, they are used by network administrators and help the network run efficiently. Port 445 can use TCP and UDP protocols. However, TCP is generally preferred.

7.33 Port 464: Kerberos Key Distribution Center (KDC)

The Kerberos Key Distribution Center (KDC) is one of the central components of the Kerberos protocol. The KDC manages users' credentials and entitlements in Kerberos-based authentication.

KDC includes two main components: Authentication Server (AS) and Ticket Granting Server (TGS). The authentication server is used to authenticate users, and the ticket issuer server issues tickets to users to access services.

When the user wants to access a service, he makes a request to the KDC. The KDC authenticates the user and approves the user's ticket request. The KDC signs the user's ticket request and encrypts it using the password of the ticketing

server. The user receives the encrypted ticket request and sends it to the ticket issuing server. The ticket issuing server validates the user's ticket request and issues the user a ticket to access the service.

Kerberos KDC is used on many networks and is also available on Windows Active Directory, UNIX, and Linux systems. KDC provides secure authentication processes and is an important component for network security.

Port 464 is important for network security and in systems where this port is open, necessary precautions must be taken to ensure that user authentication processes are performed correctly.

Kerberos KDC (Key Distribution Center) can use both TCP and UDP. Depending on the client query protocol, it can be sent over TCP or UDP protocol. However, usually requests to the KDC are sent over UDP and TCP is used for larger packets.

7.34 Port 465: SMTP Protocol over TLS/SSL

Port 465 is reserved for an SMTPS (SMTP over SSL) service used over the TCP protocol. This port is used for SMTP traffic protected by SSL/TLS security. SMTP (Simple Mail Transfer Protocol) is a protocol for sending and receiving e-mail. SMTPS works similarly to the regular SMTP protocol, but data is moved securely using SSL/TLS encryption. Port 465 is a port used especially in corporate e-mail systems.

7.35 Port 497: Retrospect

Port 497 is often used by backup software called "Retrospect". Retrospect is backup software available for various operating systems such as Windows, Mac, and Linux. Port 497 is used to communicate with the server-side software of the Retrospect software.

Retrospect software is a tool for backing up, restoring and managing data. This software offers many backup options, for example full, differential and

incremental backup options. Retrospect also provides a scheduler for scheduling backup operations and provides a management interface to facilitate the management of backup operations.

Port 497 is used by Retrospect software only and not by other software. However, some malware tries to detect vulnerable devices by scanning open ports, and this way they can identify systems where Retrospect software is used. Therefore, it is recommended to close unused and unnecessary open ports for security purposes.

Retrospect software uses Port 497 using the TCP protocol. The TCP protocol is used to provide a secure connection for a secure and stable data transfer. Retrospect software transfers data over TCP protocol for safe backup operations.

7.36 Port 500: Internet Security Association and Key Management Protocol

Port 500 is used by the IKE (Internet Key Exchange) protocol, also known as ISAKMP (Internet Security Association and Key Management Protocol).

IKE is a protocol used for key exchange for IPsec (Internet Protocol Security) implementation. IPsec is a protocol for the security of data on the network and is used to ensure the confidentiality, integrity and authentication of data.

The IKE protocol is a key exchange protocol for securing data transmitted using IPsec. The IKE protocol is used to establish a security relationship between two devices that trust each other. During this relationship, authentication is done between devices and keys used for a secure connection are generated.

Port 500 is used for key exchange operations over the IKE protocol. This port is often used in networks that use IPsec, such as virtual private networks (VPN). VPNs are a network used to securely transmit data over the internet, and IPsec is a protocol for securing that data.

The IKE protocol uses UDP by default, but IPsec VPN applications can use TCP.

7.37 Port 512: exec

Port 512 is a port number used natively in Windows operating systems. This port is used by the "exec" service, which is usually used with the "who" command.

The "Exec" service is used to send commands to a remote system. The "who" command lists who is logged into a remote system. This service is widely used, especially on older Unix systems. However, nowadays, different methods and port numbers are preferred for these functions.

Port 512 is generally not secure and should not be accessible over the internet. Leaving this port open could allow an attacker to gain unauthorized access to the system. Therefore, port 512 and other potential vulnerabilities should be regularly scanned and protected by system administrators.

7.38 Port 513: login

There is a service called "login" on port 513. This service is used to access a system existing in a network with user credentials.

The "login" service is usually used to access from one Unix/Linux system to another and authenticates the user's name and password. The service allows the user to interact with the shell or another program when the login process is complete.

However, this service is not widely used anymore because it can be potentially dangerous due to security vulnerabilities. Modern systems use SSH (Secure Shell) or other more secure remote access protocols instead.

7.39 Port 514: syslog

Port 514 is a port that network devices, servers, and other systems use to receive and process syslog messages. Syslog is a protocol that allows the

collection, storage and analysis of log records produced by network devices, servers and other systems in a central location. These logs are important for monitoring a system's performance, security, and other operational characteristics.

The service on port 514 receives syslog messages and saves them to a specific file or other storage device. This service can also be used to process, analyze and report messages.

Since syslog is a protocol supported by many different systems, the service on port 514 can use a variety of different applications and tools to receive and process syslog messages. These may include open source and commercial solutions such as rsyslog, syslog-ng, Splunk, and Graylog. Port 514 is usually used over the UDP protocol. However, in some cases, the TCP protocol can also be used. TCP 514 can be used especially for applications that require TCP connection such as syslog.

7.40 Port 515: Line Printer Daemon (LPD)

Port 515 is a reserved port number for the Line Printer Daemon (LPD) protocol. LPD is a protocol for sharing print jobs between printers on a network. This port number allows one computer to offer printer services to other computers.

Although LPD started to be used in UNIX-based systems, it is used in many different platforms today. The working principle of this protocol is based on the printers connected to the LPD sequentially performing the print operations collected in a queue.

The LPD protocol manages the print queue by queuing jobs sent to the print server and informs clients about the status of print jobs. A client sends a print task to the LPD server, which is collected in a queue. The LPD server processes the print tasks sequentially, sending the results back to the clients.

Port 515 is mostly used over the TCP protocol. However, some LPD implementations may also use the UDP protocol.

7.41 Port 520: Routing Information Protocol (RIP)

Port 520 is used for network management protocols. These protocols include Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).

RIP (Routing Information Protocol) is network routing protocol and it helps all routers in a given network to connect with each other. This way all routers can get information about the network and choose the best route. Port 520 is used for RIP messages.

OSPF (Open Shortest Path First) is another network routing protocol and is used in place of RIP in larger and complex networks. OSPF calculates the topology of the network and broadcasts this information to all routers for faster and more efficient routing. Port 520 is used for OSPF messages.

BGP (Border Gateway Protocol) is a routing protocol for wide area networks and is used for routing internet traffic. It is used by Internet service providers and large organizations. Port 520 is used for BGP messages.

Port 520 is usually used using UDP.

7.42 Port 546-547: Dynamic Host Configuration Protocol version 6 (DHCPv6)

Ports 546 and 547 are generally used for the DHCPv6 (Dynamic Host Configuration Protocol version 6) protocol.

DHCPv6 is a protocol used to automatically provide IP addresses, DNS server addresses, gateways, and other network configuration information to devices on IPv6 networks. DHCPv6 is used to distribute IPv6 addresses assigned

to IPv6 address pools and other information needed to automate IPv6 network configuration.

Port 546 is used by DHCPv6 clients, while port 547 is used by DHCPv6 servers. DHCPv6 servers respond to clients' DHCPv6 requests and provide network configuration information. DHCPv6 clients send requests to DHCPv6 servers and receive IP addresses and other network configuration information.

DHCPv6 usually runs over the UDP protocol. Port 546 is used for messages that DHCPv6 clients send to DHCPv6 servers, while port 547 is used for messages that DHCPv6 servers send to DHCPv6 clients. Therefore, both ports use the UDP protocol.

7.43 Port 554: Real Time Streaming Protocol (RTSP)

Port 554 uses a network protocol called RTSP (Real Time Streaming Protocol), which is used for real-time communication. This protocol is used by a client program to access real-time media resources such as video or audio on a server.

RTSP establishes a communication channel between a media server and one or more clients and manages the streaming of media content. Therefore, many programs or services that stream video or audio provide this functionality using the RTSP protocol.

For example, an IP camera can stream video recording through an RTSP server. Then an RTSP client can access this resource and watch the video stream. Similarly, an audio streaming service can stream music using the RTSP protocol, and customers can access this stream using an RTSP client.

Port 554 usually runs over TCP. However, some applications may also use UDP to distribute RTSP media streams.

7.44 Port 587: Simple Mail Transfer Protocol (SMTP)

Port 587 is used as an alternate port for SMTP (Simple Mail Transfer Protocol). This port is usually used for sending e-mail.

SMTP is a protocol used to send email. Traditionally, TCP port 25 is used for sending email. However, some Internet providers or networks may block port 25. Therefore, port 587 is used as an alternate port for sending e-mail.

Port 587 can also be used to send encrypted email over SMTP. In this case, communication is encrypted and secured using a secure protocol such as TLS (Transport Layer Security) or SSL (Secure Sockets Layer). This way, the connection used to send emails is more secure and prevents emails from being intercepted or read by third parties.

7.45 Port 593: Remote Procedure Call (RPC) over HTTPS Protocol

Port 593 is used for the Remote Procedure Call (RPC) over HTTPS protocol developed by Microsoft. This protocol enables RPC traffic to be forwarded over HTTPS (HTTP Secure).

RPC is a protocol for remotely calling a process on one server from a program on another server. RPC over HTTPS provides a more secure solution by providing secure and encrypted transmission of RPC traffic.

Port 593 uses the TCP protocol used to forward RPC over HTTPS traffic.

7.46 Port 631: Internet Printing Protocol (IPP)

Port 631 is used for Internet Printing Protocol (IPP). This protocol is used to connect to network printers and other printing devices.

IPP is a standard for managing network printing operations. Printers using IPP allow users to print directly to the printer over the network. This allows you

to print from any computer where the printer is connected to the network, rather than connecting the printer directly to a computer.

Port 631 can also be used to access web interfaces used for managing printers. These web interfaces allow users to check printer status, manage print queues, configure settings, and perform other printer management tasks.

7.47 Port 636: LDAP over SSL

Port 636 is an HTTPS (HTTP over SSL) port used using TCP (Transmission Control Protocol) and is used for relaying LDAP (Lightweight Directory Access Protocol) traffic under SSL/TLS security. Services running on this port are usually LDAP servers and are used by domain controllers using Active Directory Domain Services (AD DS).

Active Directory Domain Services (AD DS) is a directory service for storing and managing objects in the domain, such as user accounts, computer accounts, and other resources. This service is available on all computers and servers of the domain.

Port 636 provides a secure connection by encrypting LDAP traffic. This is important for the security of authentication and authorization information. Specifically, this port is used for the LDAPs (LDAP over SSL) protocol used in Active Directory environments.

7.48 Port 646: Label Distribution Protocol (LDP)

LDP (Label Distribution Protocol) is a routing protocol generally used for MPLS (Multiprotocol Label Switching) networks. LDP is used to route data packets over the network via MPLS tags.

LDP is a protocol used to distribute tag information among devices running on MPLS networks. These tags are read and directed by the devices on the path used while the packets reach the destination. LDP distributes tag information

among all devices in MPLS networks and provides information on how to use tags.

LDP provides automatic tag generation and routing between devices running on MPLS networks. Thus, data routing can be done quickly and effectively in MPLS networks using LDP. In addition, other protocols used with LDP provide the traffic management and error management functions required for MPLS networks.

7.49 Port 873: rsync

Port 873 is a network port used in the TCP/IP protocol and is used by a file synchronization protocol called rsync. Rsync is a tool for quickly syncing large files. This allows files to be synchronized and updated between two different computers.

Rsync transfers only the parts that change when syncing files, so it reduces network traffic and allows it to be synced quickly. Therefore, it is often used to copy large data files to remote servers or other computers.

There is no information about whether there are other services running on port 873. However, port scanning tools can be used to determine which service is using a particular port on a network.

Rsync usually works over TCP (Transmission Control Protocol). TCP provides reliable data transfer and prevents data loss with error correction and retry features. For this reason, protocols used for file synchronization such as rsync generally prefer TCP.

7.50 Port 902: Vmware

Port 902 is a port used by virtualization products such as VMware ESXi and VMware Workstation. This port is used for management and communication traffic to virtual machine operating systems.

VMware ESXi is a hypervisor software that allows running multiple virtual machines on a physical server. ESXi provides tools used to manage and create virtual machines. Port 902 is used by ESXi servers and provides communication between virtual machines and ESXi server.

VMware Workstation is a desktop virtualization software and is used to run multiple operating systems on a computer. This software uses port 902 for management and communication of virtual machines.

Port 902 runs on TCP protocol and can be protected by SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption method.

7.51 Port 989-990: FTPS (FTP over SSL/TLS)

Ports 989 and 990 are ports used for FTPS (FTP over SSL/TLS).

FTP (File Transfer Protocol) is a protocol used for file transfer over the internet. FTPS, on the other hand, is a secure version of the FTP protocol and provides encryption of data using SSL/TLS.

Port 989 is usually used for FTPS control traffic, while port 990 is used for data traffic. These ports are usually listened by the FTPS server and used by the FTPS client.

FTPS is preferred to FTP, especially when transferring sensitive data (for example, financial data or health information). Encrypting data using SSL/TLS prevents third parties from accessing the data and maintains data integrity.

7.52 Port 993: IMAP over SSL

Port 993 is a port used in the TCP/IP protocol and is usually used for the IMAP-SSL protocol. IMAP is known as the Internet Message Access Protocol and is a protocol that allows e-mail to be received and managed from the server. IMAP opens a connection to the mail server, allowing the user to download and edit their email from the server.

When port 993 is used for the IMAP-SSL protocol, the connection is encrypted via the SSL (Secure Sockets Layer) protocol. This allows users to download and manage their email securely from the server.

Other services available on port 993 may be:

1. **Secure IMAP:** Provides encrypted IMAP connections using SSL protocol. This allows users to download and manage their email securely from the server.
2. **IMAPS:** Provides encrypted connections for the IMAP protocol. This allows users to download and manage their email securely from the server.
3. **Encrypted Email Services:** Many email services allow users to secure their email by encrypting it. These services usually encrypt emails using SSL or TLS protocols and allow messages to be received and managed securely from the server.

7.53 Port 995:POP over SSL

Port 995 is reserved for POP3 (Post Office Protocol Version 3) protocol encrypted with Secure Sockets Layer (SSL) or Transport Layer Security (TLS) over TCP. POP3 is an internet protocol used to receive emails. Port 995 is a standard port number used by POP3 clients and provides security during communication.

The POP3 protocol establishes a connection between the email server and the client and is used to download emails. When the client connects to the server, it downloads the emails provided by the server and stores it on a local computer. POP3 allows users to manage their mailboxes and is used to download messages stored on the email server.

Port 995 can also be used for other services that require a secure connection. For example, some VPN (Virtual Private Network) protocols, FTPS (FTP

Secure), and SMTP (Simple Mail Transfer Protocol) protocols can also work on port 995.

Port 995 usually uses TCP (Transmission Control Protocol). TCP is a protocol used for applications that require a secure connection and strives to ensure data integrity, accuracy and reliability. The POP3 protocol is also a TCP-based protocol.

7.54 Port 1194: Open VPN

Port 1194 is reserved for OpenVPN (Virtual Private Network) over UDP. OpenVPN is an open source virtual private network software used to securely create private network connections over the internet.

OpenVPN is a protocol used to establish a secure connection between two points. This connection allows an organization's employees or remote users to access the office network. OpenVPN uses SSL/TLS protocols to provide a secure connection and works over port 1194.

It can run on OpenVPN, TCP and UDP protocols. However, the UDP protocol is the recommended protocol for OpenVPN as it provides a fast and less latency connection. Therefore, port 1194 is usually used over the UDP protocol for OpenVPN.

Port 1194 can also be used by other applications. For example, some games or other applications can also run on port 1194. However, the protocol and purpose used in this case may differ from OpenVPN.

7.55 Port 1337: menandmice-dns

Menandmice DNS is a DNS (Domain Name System) management software developed by Men&Mice. This software is used to facilitate the management of DNS records in large-scale networks.

Menandmice DNS provides a set of tools and features for DNS management. These tools include editing, monitoring, checking, backing up, restoring and reporting DNS records. In addition, Menandmice DNS can also be used to monitor and analyze the performance of DNS servers.

Menandmice DNS is especially useful for companies, institutions and service providers who have to manage DNS in large-scale networks. This software is designed to automate the DNS management process, make operations faster and more efficient, and reduce errors.

Menandmice DNS can use both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols. DNS servers usually respond to DNS queries using the UDP protocol. However, in networks with large DNS record databases, the TCP protocol can also be used. Because Menandmice DNS supports both TCP and UDP protocols, it can switch between these two protocols for DNS management operations.

7.56 Port 1433-1434: Microsoft SQL

Port 1433-1434 are the ports used for Microsoft SQL Server. These ports are used to access SQL Server database systems.

Port 1433 is used to establish a TCP/IP connection to the SQL Server database. Port 1434 is used by a SQL Server Browser service that assists in browsing and naming SQL Server.

SQL Server is widely used as a database management system that can be used for many different purposes. It is especially used in large-scale corporate databases, financial systems, web applications and various similar application areas.

To access SQL Server, a connection can be made using a SQL client by specifying the IP address or name and port number of the SQL Server. These links are supported by many different programming languages and frameworks.

As a result, ports 1433 and 1434 are ports used for Microsoft SQL Server and are used to access SQL Server database systems. These ports are important for the correct operation of SQL Server, which is a widely used database management system in various application areas.

Microsoft SQL Server uses TCP (Transmission Control Protocol) port 1433 by default. However, dynamically assigned TCP ports can also be used for named instances. SQL Server can also manage its connections using UDP (User Datagram Protocol), but this is rarely used. Generally, SQL Server performs data transfer and connection management using TCP.

7.57 Port 1521: Oracle Listener

Port 1521 is a port used by the Oracle database management system. This port is used to listen and forward connection requests to the Oracle database server.

Oracle database is a database management system used to manage business critical data. Port 1521 is the default listening port of Oracle database server and users can connect to Oracle database server through this port.

Oracle Net Listener running on port 1521 listens for connection requests to Oracle database services and directs these requests. In this way, users can access the Oracle database and perform database management and query operations. Also port 1521 is a TCP port used by Oracle database services.

7.58 Port 1701: Layer 2 Tunneling Protocol (L2TP)

L2TP (Layer 2 Tunneling Protocol) is a protocol used to securely transmit data over virtual private networks (VPNs). L2TP, used in conjunction with the IPsec (Internet Protocol Security) protocol, provides a secure connection on the internet by encrypting and protecting VPN traffic.

L2TP carries VPN traffic using layer 2 (datalink layer) network protocols and combined with PPP (Point-to-Point Protocol) provides a secure connection. PPP is combined with the L2TP protocol to create a secure tunnel that L2TP will use.

L2TP can also be used to securely transfer data between two different points on a network. For example, it can be used to establish connections between branches of a company or to provide remote access.

L2TP is a protocol that provides a high level of security and maintains privacy when transmitting data over the internet, especially when combined with IPsec.

L2TP can be used over both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). However, UDP is generally preferred because it is a faster protocol and does less data validation, resulting in less latency. Also, the use of UDP does not adversely affect the performance of L2TP, as the security layer of L2TP is usually provided by IPsec. However, TCP may be more appropriate in some situations, especially when the network is experiencing high packet loss or L2TP traffic is experiencing a high traffic level on the network.

7.59 Port 1723: Point-to-Point Tunneling Protocol (PPTP)

Port 1723 is used by the PPTP (Point-to-Point Tunneling Protocol) protocol. PPTP is a protocol used to create virtual private networks (VPNs). PPTP is widely used in situations where remote users need to connect to the network, especially remote access connections.

Port 1723 is used to transmit surveillance traffic for PPTP connections. This control traffic provides functions such as initiating, validating and terminating the PPTP connection.

PPTP connections allow the user to connect to the network remotely, allowing the user to access network resources and access computers within the network. This is especially useful for corporate networks because employees can

do their work from home or even while traveling, with remote access to resources within the company.

However, the PPTP protocol is no longer recommended due to security vulnerabilities and has been replaced by more secure protocols. Therefore, if PPTP service is used on Port 1723, it is recommended to replace this service with a more secure protocol.

PPTP (Point-to-Point Tunneling Protocol) protocol can work over both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). However, it usually works over TCP.

PPTP connections can run on both TCP and UDP, but data traffic (PPP frames) is usually carried over the TCP connection, while PPTP control traffic (TCP connection) runs over Port 1723. Therefore, PPTP connections usually work over TCP.

7.60 Port 1725: Microsoft Point-to-Point Tunneling Protocol (PPTP)

Port 1725 is reserved for Microsoft Point-to-Point Tunneling Protocol (PPTP). PPTP is a protocol used to create a virtual private network (VPN) connection. PPTP allows users to securely access the corporate network or the internet using a remote access server and a VPN client. Therefore, port 1725 is used to forward PPTP VPN traffic.

PPTP is used to create a private encrypted tunnel between two computers with an internet connection. This tunnel provides secure encryption of data sent over the internet. PPTP uses Microsoft CHAP (Challenge Handshake Authentication Protocol) or EAP (Extensible Authentication Protocol) for encryption.

Port 1725 is typically used for a PPTP VPN connection, but may be used by a different application in some cases. However, these cases are quite rare and

are often confused with port 1723, which is used for PPTP VPN traffic forwarding.

Port 1725 is used over TCP (Transmission Control Protocol). This port, reserved for Microsoft Point-to-Point Tunneling Protocol (PPTP), is typically used for a PPTP VPN (Virtual Private Network) connection and TCP is the protocol of choice for this connection to ensure reliable data transfer.

7.61 Port 1741: CiscoWorks 2000

Port 1741 is reserved for CiscoWorks 2000. CiscoWorks 2000 is a network management solution that allows network administrators to manage Cisco network devices. Port 1741 is reserved for the CiscoWorks 2000 SunNet Manager Daemon (snmpdm) service, used by CiscoWorks 2000.

SNMP (Simple Network Management Protocol) is a protocol that enables management operations on network devices. CiscoWorks 2000 can monitor, configure, and manage network devices using the SNMP protocol. SNMPDM (SNMP Daemon) is a backend service used to perform these functions. SNMPDM accesses and manages network devices using the SNMP protocol.

Port 1741 is used to communicate with the SNMPDM service used to perform these operations. However, port 1741 can sometimes be used by a different application. Therefore, to give precise information about the use of port 1741, other components in the network used must also be considered.

The term "cisco-net-mgmt" is used to refer to a management model used for Cisco network devices. This model resides on the SNMP protocol used for the management of Cisco network devices and is used by tools such as CiscoWorks 2000 in the management of network devices.

Therefore, the relationship between port 1741 and Cisco-net-mgmt takes place in the communication of CiscoWorks 2000's SunNet Manager Daemon (SNMPDM) service on the SNMP protocol used for management of network

devices. SNMPDM accesses network devices over the SNMP protocol and performs device management. These operations enable network administrators to configure, manage, and monitor Cisco network devices.

Port 1741 can be used over UDP (User Datagram Protocol) or TCP (Transmission Control Protocol). However, it is often used over TCP. The TCP protocol is preferred because CiscoWorks 2000 requires reliable data transfer for network management operations.

7.62 Port 1812-1813: Remote Authentication Dial-In User Service (RADIUS)

Ports 1812 and 1813 are the ports used by the RADIUS (Remote Authentication Dial-In User Service) protocol.

RADIUS is a protocol used to authenticate users trying to access a network. The RADIUS server processes requests from devices trying to access the network to authenticate the user's credentials. These requests are usually sent over PPP (Point-to-Point Protocol).

Port 1812 is the port to which RADIUS authentication requests are sent. The RADIUS server listens on this port and processes incoming authentication requests.

If port 1813 is the port to which RADIUS account transactions are sent. The RADIUS server listens on this port and processes incoming account transaction requests. Account operations are used to monitor and record the user's activities on the network. For example, information such as what time the user connects to the network and how much data he transfers are recorded through account transactions.

The RADIUS protocol can work on both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), but UDP is generally preferred.

7.63 Port 1985: Service Advertisement Framework (SAF) Protocol

Port 1985 contains services used by the Service Advertisement Framework (SAF) protocol developed and managed by Cisco Systems.

SAF is a protocol used to advertise services on the network. This protocol is used to automatically discover the services and resources of devices on the network. The SAF protocol is designed to facilitate the discovery of distributed applications, services, and resources in IP-based networks.

Port 1985 is used by the SAF protocol and is listened by software modules called SAF Agent. SAF Agent is used to advertise and discover devices and services on the network. In addition, the SAF Agent also performs tasks such as processing communication messages, communicating with other SAF Agents using the SAF protocol, and promoting discovered services to other devices.

Therefore, port 1985 is the communication channel required for the SAF protocol to work. This port must remain open to enable services discovered and advertised using the SAF protocol.

The SAF protocol runs on UDP (User Datagram Protocol) and port 1985 is the UDP port number used by this protocol.

7.64 Port 2000: Cisco Skinny Client Control Protocol (SCCP)

Port 2000 can be used by a variety of different services. Therefore, depending on which services are used, the tasks of port 2000 may vary. However, some commonly used services are:

1. **Cisco SCCP (Skinny Client Control Protocol):** It is a protocol used in IP phone systems. This protocol is used to manage IP phones and perform call control.

2. **Cisco VTS (Virtual Tape Server):** This is a service used in backup servers. This service provides access to virtual tape devices to perform backup operations.
3. **IBM Tivoli Storage Manager:** This is a port used by the backup and restore software. IBM Tivoli Storage Manager is used to manage data backup, archive and restore operations.
4. **EyeTV:** This is television software for the Macintosh operating system. This software is used to record and play television broadcasts and manage other media files.
5. **CiscoWorks Common Services:** This is a component of CiscoWorks software and is used to perform network management operations. This service is used for management and monitoring of network devices.

Each of these services uses port 2000 for different purposes, and their duties may differ depending on which service is using this port.

Cisco Skinny Client Control Protocol (SCCP) is a protocol used to communicate between Cisco IP phones and other telephony devices. This protocol is used to control, manage and perform functions of IP phones.

SCCP is primarily used among Cisco IP phones and is not supported by other manufacturers. This protocol uses less bandwidth when communicating between IP phones and other devices compared to the standard SIP (Session Initiation Protocol) protocol. SCCP can communicate directly between IP phones or be routed through a Cisco CallManager server.

SCCP is used to perform the following functions:

1. **Call control:** SCCP is used to make, answer calls, forward calls, and perform other calling functions.

2. **Volume control:** SCCP is used to adjust audio properties, adjust volume, and manage sound from speakers, headphones, or other devices.
3. **Phone settings:** SCCP is used to manage phone settings. These settings include display settings, key layouts, timers, and other phone features.
4. **Security:** SCCP is used to provide security measures when communicating between IP phones and other devices. This protocol supports authentication, encryption, and other security features.

SCCP is often used with Cisco IP phone systems and other Cisco network devices. Cisco IP phones can communicate with other phones using the SCCP protocol and can also connect to other Cisco devices. SCCP is designed to provide secure and effective communication between IP phones and other devices.

7.65 Port 2002: Cisco Secure Access Control Server (ACS)

Port 2002 is used by Cisco Secure Access Control Server (ACS), a server routing protocol that runs on Secure Sockets Layer (SSL). ACS is a network security management system used to control and manage access to devices in a network.

Port 2002 is used to communicate with ACS' RSA (Rivest-Shamir-Adleman) Authentication Manager. RSA Authentication Manager works as an authentication management system and supports various authentication methods used by ACS.

Port 2002 handles communication between ACS and RSA Authentication Manager via SSL protocol, including encryption functionality. ACS acts as an AAA (authentication, authorization, and accounting) server providing access control to network resources and port 2002 is a port used for authentication functions of ACS.

Port 2002 is used by Cisco Secure Access Control Server (ACS), a protocol that runs on Secure Sockets Layer (SSL). The SSL protocol runs over TCP.

7.66 Port 2049: Network File System (NFS)

Port 2049 is used by the Network File System (NFS) protocol. NFS is a network file system used to share files between different computers.

NFS allows a remote computer's file system to be used like a local computer. This makes it possible for computers on a network to share files and navigate each other's file systems. Port 2049 is used by the server side of NFS and provides the communication required for file sharing.

Port 2049 is used by the Network File System (NFS) protocol. NFS is a network file system for file sharing and can run over TCP or UDP. However, by default NFS uses the UDP protocol. However, NFSv4 can use TCP or there are NFSv3 implementations that support TCP. So the protocol that NFS will use depends on the NFS version and configuration.

7.67 Port 2082-2083: cPanel

Ports 2082 and 2083 are the ports used by the cPanel web hosting control panel. These ports provide HTTP and HTTPS access to cPanel, an interface used to manage websites and servers.

Port 2082 is used for HTTP access of cPanel. Through this port, users can access cPanel from their web browser and manage a number of features such as websites, databases, email accounts and other server settings.

Port 2083 is used for HTTPS access of cPanel. This port makes access to cPanel more secure because HTTPS establishes an encrypted connection and protects the confidentiality of the information in the communication.

Ports 2082 and 2083 are the ports used by the cPanel web hosting control panel and these ports use the HTTP and HTTPS protocols. HTTP and HTTPS protocols run on the TCP protocol. So ports 2082 and 2083 use the TCP protocol.

7.68 Port 2087: EasyApache (eli)

Port 2087 is a port used by the cPanel web hosting control panel and generally allows users to securely connect to their servers.

This port is used for secure shell (SSH) access of cPanel. SSH is a network protocol used to securely access servers. In this way, users can connect to their servers via command line and perform management operations.

The application referred to as "eli" is the module of cPanel named "EasyApache" and is used for configuring and managing the Apache web server on the server. Port 2087 is a port used for secure shell (SSH) access of cPanel, and through this port, users can securely connect to their servers and perform management operations.

Since EasyApache is used to configure and manage the Apache web server, it is essential for the administration of websites on cPanel servers. The use of port 2087 allows cPanel administrators to securely connect to their servers and use critical tools such as EasyApache.

7.69 Port 2100: Oracle XML DB HTTP (Oracle XDB)

Port 2100 is a port typically used by Oracle database software such as Oracle iSQLPlus or Oracle XML DB HTTP Server.

Oracle iSQLPlus is a component of the Oracle database management system and offers a web-based SQL query interface. Through this interface, users can connect to the Oracle database server via a web browser and create SQL queries. Port 2100 is used to transmit HTTP traffic of iSQLPlus.

Oracle XML DB HTTP Server is another component of the Oracle database and handles storing, managing and querying XML data. This server can process and manage XML data over HTTP protocol. Port 2100 is used to transmit HTTP traffic of Oracle XML DB HTTP Server.

Port 2100 usually uses TCP (Transmission Control Protocol). Since both Oracle iSQLPlus and Oracle XML DB HTTP Server work over the HTTP protocol, it should be noted that this protocol is also TCP-based.

7.70 Port 2145: Genie Backup Manager Pro (GBM Pro)

Port 2145 is generally used by Genie Backup Manager Pro (GBM Pro) software. GBM Pro is a backup management software and this port is a communication channel that GBM Pro Agent can use to perform backup operations.

GBM Pro Agent is software that runs on client machines and connects to Genie Backup Manager Pro server to perform backup operations. This connection is made over port 2145. GBM Pro server scans, compresses and backs up files and folders on client machine during backup operations. After the backup process is complete, it saves the backup files to the server.

Port 2145 is a TCP (Transmission Control Protocol) port that Genie Backup Manager Pro Agent uses to connect to the GBM Pro server. TCP is a suitable choice for this type of backup because it is a reliable and connection-oriented protocol.

7.71 Port 2222: DirectAdmin

DirectAdmin is a web hosting control panel and allows customers to manage their websites and servers. DirectAdmin is an interface for managing web servers and users have access to all the tools they will need to manage their websites.

DirectAdmin provides access to the administration panel using port 2222 by default. This port is used to log into the DirectAdmin control panel. They are logged in using a combination of DirectAdmin, username and password, and then customers can access an interface that allows them to manage the website, email accounts, databases, file management and other functions.

DirectAdmin, like other web hosting control panels, is designed to facilitate the management of a server's web services. Port 2222 is used to access the DirectAdmin control panel and is therefore not used by other non-DirectAdmin related services.

7.72 Port 3128: HTTP Proxy

Port 3128 is a port number used by proxy servers. This port is used to forward HTTP and HTTPS traffic. Proxy servers are used to manage users' access to the internet, and during this process they monitor and route inbound and outbound traffic.

Port 3128 is used by many popular proxy server software, for example Squid, Polipo, Varnish and others. These softwares are used to manage network traffic and help users to control their access to the internet. Proxy servers are used to provide security, speed and access control in accessing the internet. In addition, proxy servers can also help users access websites that are blocked or restricted.

Port 3128 is typically used to forward HTTP and HTTPS traffic and runs over the TCP protocol. Proxy servers may also use different port numbers to route network traffic, but 3128 is often the preferred port number. Also port 3128 works over TCP protocol.

7.73 Port 3260: Internet Small Computer System Interface (iSCSI)

Port 3260 is reserved for the iSCSI (Internet Small Computer System Interface) protocol. This port allows SCSI devices (disk drives, tape drives, CD/DVD drives, etc.) to communicate over the IP network.

The iSCSI protocol carries SCSI commands over the TCP/IP network and is used to access remote storage areas. In this way, a computer connecting to iSCSI devices can pretend to be connected to a remote storage unit virtually.

Port 3260 is used to enable communication between iSCSI servers and iSCSI clients. iSCSI is a storage management solution typically used in large enterprises and data centers. Also it works on port 3260 TCP protocol.

7.74 Port 3306: MySQL

Port 3306 is a TCP port used by MySQL database management systems. This port is used to connect to the MySQL server and is used by many tools used for database management.

MySQL is widely used as an open source database management system and is used for data storage in many web applications. Having port 3306 open enables access to the MySQL server and therefore the security of this port is important.

Port 3306 is also used by many programming languages and frameworks that require a direct connection to MySQL server, for example PHP, Python, Ruby on Rails etc. These languages connect to the MySQL database server and exchange data over this protocol, mostly using the MySQL protocol to connect to the MySQL server.

7.75 Port 3389: Microsoft Remote Desktop Protocol (RDP)

Port 3389 is a reserved TCP port for Microsoft Remote Desktop Protocol (RDP). RDP is a protocol used to make a remote desktop connection and is supported by the Windows operating system.

The RDP protocol allows a user to remotely access a computer. This allows a computer to be connected to and processed from another location without physical access to it. This feature is especially useful when working remotely or providing support.

Since port 3389 is used for RDP connections, if one computer allows this port, it is possible for another computer to connect via the RDP protocol and make a remote desktop connection. Port 3389 uses the TCP protocol.

7.76 Port 3478-3479: Simple Traversal of UDP through NATs (STUN)

Port 3478-3479 is reserved for the Simple Traversal of UDP through NATs (STUN) protocol.

STUN is a protocol that helps devices behind network address translation (NAT) determine their true IP addresses and network ports. STUN servers can assign network ports to devices behind NAT and thus learn the real IP addresses of the devices. This is important for communicating based on real IP addresses and is especially used in VoIP and video conferencing applications.

STUN usually runs on the UDP protocol, but the TCP protocol is also supported. Port 3478 is generally used for the STUN protocol, while port 3479 is a less commonly used alternative.

Ports 3478 and 3479 support the STUN and TURN (Traversal Using Relays around NAT) protocols used in some online communication tools such as Microsoft Teams and Skype. STUN is used to solve IP address and port number

translation problems created by NAT (Network Address Translation) devices that may be found in online communication applications, while TURN enables direct connections that are not possible using NAT. Therefore, online communication tools such as *Microsoft Teams and Skype* use the STUN and TURN protocols to work on these ports, bypassing the problems caused by NAT and providing better connection quality.

7.77 Port 3689: iTunes

Port 3689 is a port used by the iTunes service. iTunes is a media player and library program developed by Apple. This port allows the iTunes library to be shared and accessed on the network.

This port is often used to stream media between Apple products. For example, a user can stream music or videos to an Apple TV or other devices using the iTunes app on iPhone or iPad. Also, sharing the iTunes library allows another computer or device on the same network to access the iTunes library.

Port 3689 is a TCP port and allows users to share iTunes libraries with other devices and use features such as iTunes Radio. However, care must be taken as this port can allow malicious people to attack your computer when left open.

7.78 Port 4500: NAT-Traversal (NAT-T)

Port 4500 is a UDP port used by the NAT-Traversal (NAT-T) protocol. NAT-T is designed to allow IPsec VPN traffic to be traversed by NAT devices. IPsec VPN traffic is usually sent using IP protocol numbers 50 and 51. However, NAT devices cannot handle these protocols correctly because their IP addresses and port numbers cannot be changed.

To solve this problem, the NAT-T protocol carries IPsec VPN traffic over UDP. NAT devices can handle UDP traffic correctly because UDP traffic works using varying IP addresses and port numbers. Because NAT-T carries IPsec VPN traffic over UDP, it can pass VPN traffic over NAT devices.

NAT-T protocol can be used in IKEv1 and IKEv2 protocols. IKE (Internet Key Exchange) is a protocol used to establish IPsec VPN connections. IKEv2 is an enhanced version of IKEv1 and comes with NAT-T support. IKEv2 can pass IPsec VPN traffic using NAT-T and communicate over NAT devices using port 4500.

Therefore, port 4500 and NAT-T protocol allow IPsec VPN traffic to pass through NAT devices and be handled correctly.

7.79 Port 4567: Cisco Transparent Remote Access Method (TRAM)

The term "TRAM" stands for "Transparent Remote Access Method" and is a feature available on Cisco devices.

Cisco TRAM provides a security feature for devices that require remote access. This feature does not require a device to be directly connected to the internet and provides a secure tunnel for remote access to devices. This tunnel allows the device to communicate with other devices within the local network, while at the same time providing access to the device by remote users connecting to the internet.

TRAM runs on TCP port 4567 as standard. Therefore, port 4567 is a port used by Cisco TRAM. When using TRAM to access Cisco devices, users first establish a VPN connection and then a secure tunnel is created between the devices. This secure tunnel allows users to access devices securely and encrypted.

7.80 Port 5000: Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is a protocol designed to facilitate communication between devices on a home network. This protocol is used as a component of TCP/IP-based home networking protocols specified by the Internet Engineering Task Force (IETF).

UPnP provides many different features to make it easier for network devices to communicate with each other. For example, UPnP devices can automatically detect each other on the network and thus communicate directly with each other. Also, UPnP devices can query each other's features and thus learn the functions of other devices and become compatible with each other.

The UPnP protocol can be used for many different device categories. For example, UPnP can be used for devices such as smart televisions, digital media players, printers, home automation devices, security cameras, and network storage devices.

The UPnP protocol is extremely useful as it makes it easy for home network devices to communicate with each other and share data on the network. However, the UPnP protocol also has some security risks. Therefore, it is important to take appropriate measures to ensure the security of UPnP devices.

7.81 Port 5001: Commplex-link

Commplex-link is a proxy server used to access a specific IP address or URL. Port 5001 is a network port that Commplex-link uses by default.

Commplex-link receives incoming requests and forwards them to the destination IP address. This routing is done according to the previously configured Commplex-link settings. These settings include which IP addresses can be accessed, which ports can be used, what protocols can be used, etc. takes place.

Port 5001 is Commplex-link's default port used for HTTPS connections. Since this port is a port specifically used for secure connections, this port is usually used when forwarding HTTPS traffic over the Commplex-link. However, Commplex-link may also use different ports depending on the configuration settings.

In summary, Commplex-link is a proxy server for accessing a specific IP address and by default it uses port 5001 for HTTPS connections.

7.82 Port 5060: Session Initiation Protocol (SIP)

Port 5060 is a network port used between IP-based phone systems and is used for Session Initiation Protocol (SIP) traffic. SIP is a protocol for the management of voice and video traffic over an IP network and is used for services such as internet-based phone calls.

Services running on port 5060 are usually SIP servers. These servers are used to manage voice or video traffic between IP phones, web-based phones or other SIP compatible devices.

SIP servers are also central components of VoIP (Voice over Internet Protocol) telephone systems. SIP traffic is routed through the SIP server, which handles inbound and outbound call traffic. SIP server, for example call forwarding, call recording, voicemail etc. It can provide many different features such as.

Port 5060 is also used by IP telephone exchanges, PBX (Private Branch Exchange) systems, and IP telephony devices configured for SIP-based communication systems.

In summary, Port 5060 is a network port used for SIP traffic and is used by many different SIP compatible devices such as SIP servers, IP telephone exchanges and IP telephony devices.

7.83 Port 5432: PostgresSQL

Port 5432 is a network port used by the PostgresSQL database management system. This port is usually the default port of PostgreSQL servers.

PostgreSQL is an open source relational database management system (RDBMS) and is mainly used for large-scale, complex database applications. PostgreSQL also provides advanced features and works in compliance with SQL standards.

The services running on port 5432 are usually PostgreSQL database servers. These servers serve client applications to perform database operations. The PostgreSQL server provides access to the database and performs database operations when connected by client applications.

PostgreSQL offers a number of features to ensure high performance, data integrity and security. These features include ACID-compliant transactions, parallel querying, JSON data type support, advanced indexing, and database security.

Port 5432 can use both TCP and UDP protocols. However, usually the PostgreSQL database management system communicates over the TCP protocol.

7.84 Port 5632: PCAnywhere

Port 5632 is a network port used by the PCAnywhere application. PCAnywhere is a remote access software developed by Symantec Corporation and is used to provide remote access to computers.

Services running on port 5632 are usually PCAnywhere servers. PCAnywhere servers accept remote access requests and allow client applications to establish connections. PCAnywhere servers can provide full access to connected computers and support file transfer, printer sharing, session recording, desktop sharing, and other remote access functions.

PCAnywhere is widely used by businesses and individual users and is particularly useful for remote work and support operations. However, PCAnywhere has been criticized by some security experts for having vulnerabilities and users should be careful. PCAnywhere usually transmits data using the TCP protocol.

7.85 Port 5800: Virtual Network Computing (VNC) over HTTP

Services running on port 5800 are usually VNC servers. VNC servers accept remote access requests and allow client applications to establish connections. In this way, users can remotely view and control a computer's screen.

VNC is software that can run on many different platforms and therefore can be used to provide remote access between different operating systems. VNC is often used by computer administrators or technical support teams. However, it can also be used by individual users.

VNC servers running on port 5800 connect via HTTP by default. Therefore, in some cases, port 5900 can be used instead of port 5800. Also, some VNC servers may provide additional features such as encryption and authentication for security purposes.

7.86 Port 5900: Virtual Network Computing (VNC)

Port 5900 is the default port of the Virtual Network Computing (VNC) application. VNC is a remote desktop software that provides access from a computer to a remote computer. Via this port, VNC servers accept connections and allow client applications to establish connections.

VNC servers are used to remotely control a computer's screen. In this way, users can view the screen of a computer and control that computer remotely. VNC can be used to provide remote access between different operating systems. For example, it can be used to access a Mac computer or Linux server from a Windows computer.

VNC servers accept connections over the VNC protocol by default. However, some VNC servers may also provide additional features such as encryption and authentication for security purposes.

VNC clients can view and control a computer's screen. VNC clients can connect to multiple VNC servers and thus control many computers remotely.

VNC can be used in many different applications and scenarios. For example, an IT administrator might use VNC to fix a problem on a remote computer. Also, a home user can use it to control a computer in a different room.

7.87 Port 5985: Windows Remote Management (WinRM)

Port 5985 is the default port of the Windows Remote Management (WinRM) service. WinRM is a protocol for remote administration of a computer. Through this port, WinRM service servers can communicate with WinRM clients.

The WinRM service is a component of Microsoft's Windows operating system. The WinRM service is designed for system administrators who want to access and manage remotely. The WinRM service is used to facilitate the management of many computers, especially in large companies.

WinRM clients are used for remote administration of a computer. In this way, a system administrator can remotely administer a computer, start and stop a service, or fix a problem.

WinRM runs on Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) APIs, which is an open web service protocol. In this way, it can be used with different programming languages.

WinRM can be used in many different scenarios. For example, a system administrator might use WinRM to fix a problem on a server. Also, an application developer can remotely manage a Windows server using WinRM APIs.

7.88 Port 6000-6001: X11

Port 6000-6001 is used for network-based graphical interface applications running on the X11 protocol.

The X11 protocol is a protocol for accessing a computer from a remote server using a graphical desktop environment. This protocol is an ideal method for sharing a computer's desktop and using it for remote access.

Port 6000 is the default port of the X11 server and is used by X11 applications. Port 6001 is used for communication between X11 servers.

The X11 protocol provides many applications for remote access and managing computers using a graphical desktop environment. For example, a system administrator can use the X11 protocol to access and administer a remote server. In addition, a user can also use the X11 protocol to access a remote computer from home or outside the office.

Port 6000-6001 is typically used on Unix or Linux based operating systems. These operating systems provide access to the X11 protocol and network-based graphical interface applications.

7.89 Port 6379: Redis

Port 6379 is used for an open source, in-memory data storage system called Redis. Redis is a key-value data store and is used by many applications due to its fast performance and flexibility.

Redis is a memory-based data store used for high performance data storage. Redis supports many different data structures, for example, key-value, lists, aggregations, queues, and more. These data structures allow easy creation of complex data models on Redis.

Port 6379 is used to access the Redis server. Redis is capable of serving multiple clients simultaneously, so an application can connect to the Redis server via port 6379 to store, search and query data.

The use of Redis is common in web applications, data analytics systems, games, and more. For example, a web application can store user session

information on Redis and then provide quick and easy access to this information. Also, Redis can be used in data analytics systems, for example, in an advertising data platform, Redis can provide rapid search and query of advertising data.

7.90 Port 6514: Syslog using TLS

Port 6514 is used by software called syslog-ng. Syslog-ng is a syslog management tool that provides functions for collecting, managing, and processing network and syslogs. Port 6514 is used for SSL/TLS connections to the syslog-ng server.

Syslog-ng moves the logs of servers and network devices to a central location and makes these logs more useful. Syslog-ng provides data collection, data routing and storage capabilities from multiple sources. It also offers advanced tools for editing, filtering and analyzing logs.

Port 6514 ensures safe operation of the syslog-ng server. SSL/TLS connections ensure data is encrypted and transported securely. This is important in cases where sensitive data is sent to the syslog-ng server.

Syslog-ng is a tool frequently used by network administrators and system administrators. Syslog-ng can be used in many areas such as network security, debugging, performance monitoring, alert management, and regulatory compliance.

7.91 Port 6665-6669: Internet Relay Chat (IRC)

There are usually IRC (Internet Relay Chat) services in the port 6665-6669 range. IRC is a protocol that allows multiple users to chat in real time. These services allow users to chat with each other, share files and play games.

There may also be malware used by some hackers in this port range. These software can hijack computers and use the user's personal information or computer resources for malicious purposes.

Therefore, open ports, such as port 6665-6669, are generally considered to be risky from a security point of view. To protect users' security, it is recommended to regularly check these ports and other open ports and close any unnecessary ones. It is also important to use firewall and antivirus software.

IRC services usually run over TCP (Transmission Control Protocol). TCP is a reliable and flow-controlled protocol and is therefore the protocol of choice for IRC connections. TCP ensures that data is delivered correctly and errors are corrected, so it is a viable option for IRC connections.

7.92 Port 6881: BitTorrent

Port 6881 is a port used by the BitTorrent protocol. BitTorrent is a P2P (peer-to-peer) file sharing protocol that allows large files to be shared quickly and efficiently.

This port is used by one BitTorrent client and is used to download and share file fragments from another BitTorrent client. Clients download parts of a shared file from other users and then share the downloaded parts to other users, allowing the file to be distributed more quickly.

Port 6881 is a default port used by BitTorrent clients but can be changed in client settings. Also, BitTorrent clients can often share files using multiple ports.

This port can be used for legal and illegal purposes due to file sharing. The BitTorrent protocol can be used for the distribution of legally shared files, as well as for the distribution of copyright infringing materials. Therefore, it is important to comply with the law when sharing files with the BitTorrent protocol.

7.93 Port 8000: HTTP

Port 8000 is a port used by various web applications. This port is usually used to run an HTTP (Hypertext Transfer Protocol) server. HTTP is a standard protocol used for displaying web pages.

Port 8000 is mainly used for development and testing purposes. During the development of web applications, they are often tested on a local server. This test server can handle various HTTP requests and allows developers to test and debug their applications.

Port 8000 is also widely used in the use of some web-based tools. For example, it is a default port used by Docker Compose. Docker Compose is a tool for coordinating multiple Docker containers.

However, since port 8000 is a port that many different applications can use, other services other than the web application can also use this port. Therefore, the nature and security of the service using port 8000 may vary depending on how the port is used.

7.94 Port 8008: HTTP Proxy

Port 8008 is a port typically used by HTTP proxy servers. HTTP proxy servers are proxy servers used to provide access to web pages.

HTTP proxy servers can be used to manage, filter and monitor network traffic. For example, a corporate network can use an HTTP proxy server to prevent users from accessing websites that do not comply with company policies.

Port 8008 is used by some web browsers, especially Google Chrome. Google Chrome calls this port "Alternate HTTP Port" and can be used in place of normal HTTP requests. For example, some applications use this alternate port to connect to an HTTP server.

Also, some other applications may use port 8008. For example, Amazon Echo can use this port for voice interactions with Alexa.

However, port 8008 should not be used directly for an HTTP server unless an HTTP proxy server is used. Because this port is only used by certain applications, its use may pose different security risks.

7.95 Port 8080-8081: HTTP

Port 8080 and 8081 are a common range of ports used by web applications. These ports are used to run the HTTP (Hypertext Transfer Protocol) server.

HTTP is a standard protocol used for displaying web pages. A web server receives HTTP requests from the user's browser and returns the corresponding web page.

Ports 8080 and 8081 are mainly used for development and testing purposes. During the development of web applications, they are often tested on a local server. This test server can handle various HTTP requests and allows developers to test and debug their applications.

Ports 8080 and 8081 are also commonly used in the use of some web-based tools. For example, many process management tools like Jenkins use these ports by default.

However, since ports 8080 and 8081 are ports that many different applications can use, other services other than the web application can also use these ports. Therefore, the nature and security of the service using ports 8080 and 8081 may vary depending on how the ports are used.

7.96 Port 8089: Splunk

Splunk is software for analyzing and viewing large-scale data. Splunk collects and analyzes data from log files, objects, application servers, databases, and other data sources.

Splunk can monitor data in real time and perform filtering, querying, graphing, reporting and visualization on the data. In this way, system administrators, security analysts and other data analysts can identify problems faster and produce solutions by making large data sets more understandable.

Splunk provides a web interface for viewing and managing analysis data, using port 8089 by default. Splunk provides many features such as creating custom dashboards and reporting, data discovery, real-time alerts, data management and usage, application monitoring and management.

Splunk also provides preconfigured applications used in many industries. For example, there are preconfigured applications used in areas such as network security, business intelligence, application performance monitoring, marketing analytics, systems administration, and cloud management.

Splunk is not an open source product and uses a paid licensing model. However, Splunk offers a free version on a small scale and trial versions are also available.

7.97 Port 8443: McAfee ePolicy Orchestrator (ePO)

The McAfee ePolicy Orchestrator (ePO) management console typically uses port 8443 for HTTPS traffic. ePO serves as a central management console for managing, auditing, and reporting McAfee products.

McAfee ePO provides secure connection of clients and McAfee agents (McAfee Agent) connecting to the management console interface using the HTTPS (Secure HTTP) protocol. Therefore, a port 8443 is generally preferred as a secure HTTP port that ePO should use.

7.98 Port 9080: IBM WebSphere Application Server

Port 9080 is an HTTP/HTTPS port commonly used on various application servers such as IBM WebSphere Application Server. The services running on this port are usually those provided by the application servers themselves.

For example, IBM WebSphere Application Server can be used as an application server for running Java EE applications. In this case, port 9080 is used as the HTTP or HTTPS port served by the WebSphere Application Server. This port is intended for applications to be used by browsers and other clients.

Other services offered by WebSphere Application Server on port 9080 may include the application server's management console and other management tools. These tools can be used for administration and configuration of the application server.

As another example, an open source application server such as Apache Tomcat can also use port 9080. Tomcat is an application server for running Java EE applications. Port 9080 can be used by Tomcat as an HTTP or HTTPS port and is intended for applications to be accessed by browsers and other clients.

In summary, port 9080 is an HTTP/HTTPS port used by application servers and is typically used for running and managing Java EE applications.

7.99 Port 10000: Backup Exec Remote Agent (BackupExec)

Port 10000 is a port number that can be used for many different services. Here are some possible services and their functions:

1. **Webmin:** Webmin is a web-based interface used to manage many functions on a Unix or Linux system. Port 10000 is used to access the Webmin interface.
2. **Backup Exec Remote Agent:** Backup Exec is backup software developed by Veritas Technologies. Backup Exec Remote Agent is used to perform backup operations of a server. Port 10000 is used to access the management console of the Backup Exec Remote Agent.
3. **Network Data Management Protocol (NDMP):** NDMP is a protocol for network-based backup and recovery. Port 10000 is used for NDMP connections.
4. **Snet-Sensor-Mgmt:** Snort Intrusion Detection System is a network security tool. Snet-Sensor-Mgmt is an interface for managing Snort sensors. Port 10000 is used to access the Snet-Sensor-Mgmt interface.

5. **SOPHOS:** SOPHOS is an antivirus software. Port 10000 is used to access the SOPHOS Management Console interface.
6. **VNC Remote Console:** Virtual Network Computing (VNC) is a protocol used for remote desktop connection. Port 10000 is used to access the VNC Remote Console.

Apart from the above services, port 10000 can be used by other software and services. Therefore, in order to determine what access to port 10000 is used for, it is important to understand which service is using that port number.

Backup Exec Remote Agent is software developed by Symantec Corporation and is part of Symantec Backup Exec backup software. Backup Exec Remote Agent is used to back up servers and client machines.

Backup Exec Remote Agent is a tool used to retrieve data from server or client machines during the backup process. This software works with the backup server to back up files, databases, application data and system settings on server or client machines.

Backup Exec Remote Agent is software that runs on server or client machines and communicates with the backup server. In this way, it is ensured that files, databases and other data on server or client machines are stored on the backup server.

Backup Exec Remote Agent helps to perform backup operations faster and more efficiently. It also enables data recovery on server or client machines in case of data loss.

7.100 Port 11371: OpenPGP (Pretty Good Privacy)

Port 11371 is used for the OpenPGP (Pretty Good Privacy) key server protocol. This protocol is used to communicate with a networked key server where users can store and find their keys.

OpenPGP is the foundation of many cryptographic applications and is used for privacy, authentication and data integrity. For example, it can be used for e-mail encryption, digital signature, file encryption, and network traffic encryption.

Port 11371 is a communication port used to facilitate key sharing and key queries between key servers. By connecting to one keyserver, this port can search and download keys from other keyservers. In this way, a user can discover other users' keys and securely send messages to other users or encrypt their files.

[5]

References

[1] «scaler,» Available: https://www.scaler.com/topics/computer-network/what-is-port/.

[2] «privateinternetaccess,» Available: https://www.privateinternetaccess.com/blog/tcp-vs-udp-understanding-the-difference/.

[3] «berqnet,» Available: https://berqnet.com/blog/port.

[4] «networkverge,» Available: https://networkverge.com/common-ports/.

[5] «geeksforgeeks,» Available: https://www.geeksforgeeks.org/50-common-ports-you-should-know/.