Click to verify

Port number is a 16-bit numerical value that ranges from 0 to 65535. Well-known port (0-1023), registered port (1024-49151), and dynamic port is three types of port number space. (49152-65535). These ports can be opened and used by software applications and operating system services to send and receive data over networks (LAN or WAN) that employ certain protocols (eg TCP, UDP). For example, we use 80 for HTTP-web-based plain-text surfing and 443 for HTTPS-web-based encrypted websites in our daily work. To conclude, a port is a logical form to identify system activities or various network services used to create local or network-based communications. What are the functions of ports?When interacting over the Internet, TCP and UDP protocols make connections, recompile data packages after the transfer, and then deliver them to applications on the recipient's device. For this handover to work, the operating system must install and open the gateway for the transfer. Each door has a unique code number. After transmission, the receiving system uses the port number to determine where the data should be sent. The port numbers of the sender and receiver are always included in the data packet. Ports are assigned sequential numbers from 0 to 65535. Some of these codes are standardized, meaning they are assigned to certain uses. Since code numbers are universally recognized and permanently assigned, these standard ports are also known as well-known ports. Registered ports are those that organizations or software developers have registered for their applications. Registration is handled by the Internet Assigned Numbers Authority (IANA). A diverse selection of dynamically assigned port numbers is also available. For example, when viewing websites, browsers use these ports. After that, the port number is free again. Why is it important to know these ports?Any security researcher, bug bounty hunter, or anyone working with service configuration would benefit from this. Knowing how to do more thorough scans such as version detection or known vulnerabilities for ancient services that are still operating in the infrastructure, especially when using tools like Nmap, is handy when getting to know these protocols and services. The most 50 significant ports are listed here:The following are some of the most common service names, transport protocol names, and port numbers used to differentiate between specific services that employ TCP, UDP, DCCP, and SCTP. Port Number Service nameTransport protocolDescription7EchoTCP, UDPEcho service20FTP-dataTCP, SCTPFile Transfer Protocol data transfer21FTPTCP, UDP, SCTPFile Transfer Protocol (FTP) control connection22SSH-SCPTCP, UDP, SCTPSecure Shell, secure logins, file transfers (scp, sftp), and port forwarding23TelnetTCPTelnet protocolunencrypted text communications25SMTPTCPSimple Mail Transfer Protocol, used for email routing between mail servers53DNSTCP, UDPDomain Name System name resolver69TFTPUDPTrivial File Transfer Protocol80HTTPTCP, UDP, SCTPHypertext Transfer Protocol (HTTP) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP 88KerberosTCP, UDPNetwork authentication system102Iso-tsapTCPISO Transport Service Access Point (TSAP) Class 0 protocol110POP3TCPPost Office Protocol, version 3 (POP3)135Microsoft EPMAPTCP, UDPMicrosoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, used to remotely manage services including DHCP server, DNS server, and WINS. Also used by DCOM137NetBIOS-nsTCP, UDPNetBIOS Name Service, used for name registration and resolution139NetBIOS-ssnTCP, UDPNetBIOS Session Service143IMAP4TCP, UDPInternet Message Access Protocol (IMAP), management of electronic mail messages on a server381HP OpenviewTCP, UDPHP data alarm manager383HP OpenviewTCP, UDPHP performance data collector.443HTTP over SSLTCP, UDP, SCTPHypertext Transfer Protocol Secure (HTTPS) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP.464KerberosTCP, UDPKerberos Change/Set password465SMTP over TLS/SSL, SSMTCPAuthenticated SMTP over TLS/SSL (SMTPS), URL Rendezvous Directory for SSM (Cisco protocol)587SMTPTCPEmail message submission593Microsoft DCOMTCP, UDPHTTP RPC Ep Map, Remote procedure call over Hypertext Transfer Protocol, often used by Distributed Component Object Model services and Microsoft Exchange Server636LDAP over TLS/SSLTCP, UDPLightweight Directory Access Protocol over TLS/SSL691MS ExchangeTCPMS Exchange Routing902VMware ServerunofficialVMware ESXi989FTP over SSLTCP, UDPFTPS Protocol (data), FTP over TLS/SSL990FTP over SSLTCP, UDPFTPS Protocol (control), FTP over TLS/SSL993IMAP4 over SSLTCPInternet Message Access Protocol over TLS/SSL (IMAPS)995POP3 over SSLTCP, UDPPost Office Protocol 3 over TLS/SSL1025Microsoft RPCTCPMicrosoft operating systems tend to allocate one or more unsuspected, publicly exposed services (probably DCOM, but who knows) among the first handful of ports immediately above the end of the service port range (1024+).1194OpenVPNTCP, UDPOpenVPN1337WASTEunofficialWASTE Encrypted File Sharing Program1589Cisco VQPTCP, UDPCisco VLAN Query Protocol (VQP)1725SteamUDPValve Steam Client uses port 17252082cPanelunofficialcPanel default2083radsec, cPanelTCP, UDPSecure RADIUS Service (radsec), cPanel default SSL2483Oracle DBTCP, UDPOracle database listening for insecure client connections to the listener, replaces port 15212484Oracle DBTCP, UDPOracle database listening for SSL client connections to the listener2967Symantec AVTCP, UDPSymantec System Center agent (SSC-AGENT)3074XBOX LiveTCP, UDPXbox LIVE and Games for Windows Live3306MySQLTCPMySQL database system3724World of WarcraftTCP, UDPSome Blizzard games, Unofficial Club Penguin Disney online game for kids4664Google DesktopunofficialGoogle Desktop Search5432PostgreSQLTCPPostgreSQL database system5900RFB/VNC ServerTCP, UDPvirtual Network Computing (VNC) Remote Frame Buffer RFB protocol6665-6669IRCTCPInternet Relay Chat .6881BitTorrentunofficialBitTorrent is part of the full range of ports used most often6999BitTorrentunofficialBitTorrent is part of the full range of ports used most often6970QuicktimeunofficialQuickTime Streaming Server8086Kaspersky AVTCPKaspersky AV Control Center8087Kaspersky AVUDPKaspersky AV Control Center8222VMware ServerTCP, UDPVMware Server Management User Interface (insecure Web interface).9100PDLTCPPDL Data Stream, used for printing to certain network printers.10000BackupExecunofficialWebmin, Web-based Unix/Linux system administration tool (default port)12345NetBusunofficialNetBus remote administration tool (often Trojan horse).27374Sub7unofficialSub7 default31337Back OrificeunofficialBack Orifice 2000 remote administration tools As a server administrator, its essential to understand the functions of common services and their respective port numbers. Similar to how an IP address determines the computers identity, the network port is key in identifying the specific application or service operating on that computer. Without any doubt, Im sure youve heard the term port before, but what does it mean in the world of computers? In computer networking, a port is a virtual communication endpoint for exchanging data, which is pivotal in managing and directing internet traffic. In other words, you can imagine a network port as a virtual door on your computer. However, unlike a physical port (like a USB one, for example), a network port is a software-based identification number that helps computers differentiate between multiple types of network traffic. Typically, ports are identified by a specific network service assigned to them. Within an operating system, they serve as endpoints in the network communications process, primarily transferring data between a computer network and an application. Port ranges are a series of numbers assigned to various tasks and services in computer networking. These numbersrange from 0 to 65535and are divided into three different sub-ranges based on their use and the type of service they provide. Understanding these ranges is key to effectively managing network security, traffic, and services. RangePurposeWell-Known Ports0-1023Assigned to specific service by IANA (Internet Assigned Numbers Authority). These ports are reserved for common, widely-used services. For example, HTTP (web traffic) uses port 80, and HTTPS (secure web traffic) uses port 443.Registered Ports1024-49151Ports that an organization can register with IANA to be used for a particular service. Many software manufacturers use these ports for their applications.Dynamic or Private Ports49152-65535These are often used for client-side communication or temporary purposes. They are less regulated and more flexible in their usage. After discussing port rangers, lets now briefly examine another fundamental aspect of networking: transport protocols. Imagine the internet as a vast network of roads. Just like roads have traffic rules, the internet has transport protocols. These protocols are sets of instructions that manage how data packets move across the network. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the most common protocols. TCP is a is a connection-oriented protocol. For example, when you send an email or load a webpage, TCP ensures that all the data packets reach their destination correctly. If we were to make a comparison, we would say that TCP is like a reliable courier service. Lets say you send a fragile package with tracking and insurance. TCP notices and sends a replacement if a packet gets lost or damaged. This is why TCP is used for tasks where accuracy is crucial and is the most widely used networking protocol. On the other hand, UDP is a connectionless protocol. This is due to the lack of overhead associated with creating, maintaining, and terminating connections. So, its like a speedy messenger. UDP is used for tasks like live video streaming or online gaming, where receiving data quickly is more important than correctly receiving every packet. With UDP, theres no time spent checking if all packets have arrived or re-sending lost ones. Its all about speed, even if it means occasionally missing a piece of data. Now that we have introduced you to the fundamentals of a network port, its ranges, and the basic transport protocols, lets move on to the main topic exploring the most common network ports out there. As we delve into the specifics of each one, from well-known HTTP (port 80) and HTTPS (port 443) to others less familiar, we will uncover their roles in our daily digital interactions. Port 21 is commonly associated with FTP (File Transfer Protocol). FTP is for transferring files between a client and a server. Its usually regarded as a non-secure file transfer protocol. FTP sends data in clear text and provides an anonymous option that does not require a password. However, FTP is a trusted and widely used protocol for transferring files. SSH, or Secure Shell Protocol, is a network communication protocol used to perform operations on remote computers, but it may also beused for transferring data. A connection between the client and server is established whenever we run a command throughthe default SSH port number 22. SSH was developed as a safe substitute for the unencrypted Telnet protocol, and it utilizes cryptographic techniques to ensure that all communication to and from the remote server is encrypted. The telnet protocol typically uses port 23. Its often used for an administrative command-line interface in networking equipment such as routers and switches. However, because the protocol is unencrypted, its usually only used safely within a local area network, as the data is in cleartext. Port 25 is the original standard email SMTP (Simple Mail Transfer Protocol) port and the oldest since it first debuted in 1982. After four decades, SMTP on port 25 is the basic standard for sending email between mail servers via the internet. DNS (Domain Name System) turnsdomain names into IP addresses. As a result, thanks to DNS servers, people may type ordinary words into their browsers without remembering the IP address for each website. DNS has been designed to use UDP and TCP port 53, with UDP being the default, and falls back to using TCP when it cannot communicate on UDP. DHCP (Dynamic Host Configuration Protocol) provides network addresses to dynamically configured TCP/IP network hosts. It uses UDP ports 67 and 68. The server should use port 67, and the client should use port 68. Port 80 is the port number assigned to the commonly used internet communication protocol HTTP (Hypertext Transfer Protocol). The HTTP protocol defines the format for communication between internet browsers and websites. In other words, port 80 sends and receives web server requests. The web traffic that passes through the port remains in plain text. POP3 (Post Office Protocol version 3) is a mail protocol to retrieve mail from a remote server to a local email client.Its a relatively simple mail protocol, making it less prone to errors and more straightforward implementation. The default POP3 port is 110. Portmapper service is required to run NFS both on the client and the server side. It runs on port 111 for both TCP and UDP protocols. Portmap makes the dynamic binding of remote programs possible. Port 137 is utilized by NetBIOS (Network Basic Input/Output System) Name service. NetBIOSs primary purpose is to allow applications on different computers to communicate and establish sessions to access shared resources like files and printers and locate each other via a local area network (LAN). IMAP (Internet Message Access Protocol) is a mail protocol to access email on a local clients remote web server. The IMAP protocol works on port 143, the default IMAP non-encrypted port. The SNMP (Simple Network Administration Protocol) protocol suite collects network management and monitoring protocols. Its often used to monitor firewalls, routers, switches, servers, printers, bridges, NAS disks, UPS, and other network devices. SNMP ports are utilized via UDP on port 161 for SNMP Managers communicating with SNMP Agents and via UDP on port 162 when agents send unsolicited SNMP traps to the SNMP Manager. HTTPS stands for HyperText Transfer Protocol Secure. Port 443, a web browsing port, is primarily used for HTTPS services. Its a port that billions of people across the globe use every single day. Over95%of secured websites use HTTPS via port 443 for secure data transfer. Port 587 is the standard secure SMTP (Simple Mail Transfer Protocol) port. Its the default mail submission port. This is the one that will provide the best results when users submit an email to be routed via a proper mail server. The use of port 587 in conjunction with TLS encryption ensures that email is sent securely and following the IETFs requirements. IMAPS (IMAP over SSL)means IMAP traffic travels over a secure socket to a secure port. When using an encrypted IMAP connection, the default port is993. It helps ensure your safety and privacy on the internet. In this article, we have journeyed through the most commonly used network ports, uncovering their pivotal roles in our everyday internet activities. Understanding these is not just for IT professionals its valuable knowledge for anyone who uses the internet, offering insights into how our online interactions are facilitated and secured. See RFC 1700 or IANA for a complete list of network port numbers for more information. The keyword here is socket. A socket is one endpoint of a two-way communication link between two programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to. On most operating systems, SOCKETS are identified by a number, similar to a file descriptor, that index a single entry into a table containing information about a connection. This information is usually in the following format: SOURCEIP:SOURCEPORT DESTINATIONIP:DESTINATIONPORT PROTOCOL STATE This table can be accessed, generally, via the NETSTAT command (or its equivalent) on most operating systems. In no event you can have two entries on such table with equal values (in other words: two entries with the exact same sourceip, sourceport, destinationip, destinationport and protocol at the same time). You can have two entries with same destination ports, source ports etc, any value, but never exact same values on two or more entries. And each entry is indexed (identified) by a single socket number. (There are exceptions to this rule) This socket number is returned when you issue a SOCKET() function call. (on linux/freebsd/windows). Later, your program will decide what to do with the socket requested from the operating system. It can issue a CONNECT() call and connect this socket into a remote machine or a BIND() and LISTEN() calls to use it to wait for inbound connections. This means that two processes CAN share a port, if they happen to share the SOCKET associated to the port. This is even a common way to do network programming. You can fork or spawn another process when your listening socket receives a connection request and you call ACCEPT() to accept it. ACCEPT() will return a socket number that will identify a new SOCKET created for that incomming connection, you will then pass the socketnum to the spawned/forked process. For example on Windows: The WSADuplicateSocket function is introduced to enable socket sharing across processes. A source process calls WSADuplicateSocket to obtain a special WSAPROTOCOL_INFO structure for a target process identifier. It uses some interprocess communications (IPC) mechanism to pass the contents of this structure to a target process. The target process then uses the WSAPROTOCOL_INFO structure in a call to WSPSocket. The socket descriptor returned by this function will be an additional socket descriptor to an underlying socket which thus becomes shared. Sockets can be shared among threads in a given process without using the WSADuplicateSocket function because a socket descriptor is valid in all threads of a process. In other words, ports are used to help identify SOCKETS on a computer, which are single connections between TWO hosts on the network. This is true for both TCP and UDP protocols. They do not, usually, identify processes and most operating systems wont bother if two processes act on the same port. The keyword here is SOCKET, not process. Sockets are the things that must be unique, because they identify a unique connection between two hosts. So, answering your question. Why are ports needed ? Because if there were no ports, the table i refered to in the start of the text would be limited to: SOURCEIP DESTINATIONIP PROTOCOL STATE In other words, you could have only a single SOCKET for each host accessible to your computer, wich is not very usefull at all. Sources:What Is a Socket?Sockets TutorialShared Sockets This article provides an overview of network port numbers and their importance in computer networking. It explains what port numbers are and how they work, as well as the different types of port numbers and their uses. The article also covers the most commonly used port numbers and why they are important, as well as some frequently asked questions about port numbers. By reading this article, readers can gain a better understanding of how port numbers are used in networking, and how they can be used to improve network security and efficiency. Ports and protocols are essential elements of network communication. Lets take a closer look at what they are and how they work. In computer networking, a port is a logical address that identifies a specific process or service running on a computer. Ports are numbered between 0 and 65535, with some numbers reserved for specific protocols or services. For example, port 80 is commonly used for HTTP traffic, while port 443 is used for HTTPS traffic. Ports allow computers to establish connections with other devices, exchange data, and communicate with specific services or applications. For example, when you open a web browser and navigate to a website, your computer uses port 80 (or 443 for HTTPS) to connect to the web server hosting the site. A protocol is a set of rules and standards that govern how data is transmitted between devices on a network. Protocols define the format and structure of messages, how data is encoded and decoded, and how errors and other issues are handled. There are many different protocols used in computer networking, each designed for a specific purpose or application. Some common protocols include HTTP (HyperText Transfer Protocol) for web traffic, SMTP (Simple Mail Transfer Protocol) for email, and FTP (File Transfer Protocol) for file transfers. Protocols ensure that data is transmitted correctly and reliably, and help to ensure that devices from different manufacturers and vendors can communicate with each other. Without protocols, it would be difficult to establish and maintain connections between devices on a network. These are reserved ports in the range of 1 to 1,023 and have been registered with IANA for a specific service. This range is also registered with IANA but is not as commonly used. IANA reserves this port range for dynamic use for proprietary services or private use. Port NumberProtocolDescription20TCPFTP Data Transfer21TCPFTP Control22TCPSSH (Secure Shell)23TCPTelnet25TCPSMTP (Simple Mail Transfer Protocol)53TCP/UDPDNS (Domain Name System)67UDPDHCP (Dynamic Host Configuration Protocol)68UDPDHCP (Dynamic Host Configuration Protocol)80TCPHTTP (Hypertext Transfer Protocol)88TCP/UDPKerberos Authentication System110TCPPOP3 (Post Office Protocol v3)119TCPNNTP (Network News Transfer Protocol)123UDPNTP (Network Time Protocol)135TCPMicrosoft RPC (Remote Procedure Call)137UDPNetBIOS Name Service138UDPNetBIOS Datagram Service139TCPNetBIOS Session Service143TCPIMAP (Internet Message Access Protocol)161UDPSNMP (Simple Network Management Protocol)389TCP/UDPLDAP (Lightweight Directory Access Protocol)443TCPHTTPS (HTTP Secure)445TCPMicrosoft SMB (Server Message Block) over TCP/IP514UDPSyslog636TCPLDAPS (LDAP Secure)993TCPIMAPS (IMAP Secure)995TCPPOP3S (POP3 Secure)1433TCPMicrosoft SQL Server1521TCPOracle SQL3306TCPMySQL3389TCPMicrosoft Remote Desktop Protocol (RDP)5432TCPPostgreSQL Note that this list is not exhaustive and there may be other ports in use in different contexts. Also, some protocols may use multiple ports depending on the configuration. The most commonly used ports depend on the context of use. Here are some of the most commonly used ports in various applications and protocols: Port 80: HTTP (Hypertext Transfer Protocol) web traffic Port 443: HTTPS (HTTP Secure) web traffic Port 53: DNS (Domain Name System) traffic Port 25: SMTP (Simple Mail Transfer Protocol) email traffic Port 110: POP3 (Post Office Protocol v3) email traffic Port 143: IMAP (Internet Message Access Protocol) email traffic Port 3389: RDP (Remote Desktop Protocol) traffic Port 22: SSH (Secure Shell) traffic Port 21: FTP (File Transfer Protocol) traffic Port 23: Telnet traffic Port 1194: OpenVPN traffic Port 1723: PPTP (Point-to-Point Tunneling Protocol) traffic Port 3306: MySQL database traffic Port 5432: PostgreSQL database traffic These are just a few examples of commonly used ports. The use of specific ports can vary depending on the application or protocol being used, and different organizations may use different ports for the same applications or protocols. Web traffic is one of the most common types of network traffic, and there are several ports and protocols that are commonly used to transmit web data. Lets take a closer look at some of these: HTTP is the primary protocol used for transferring data between web servers and clients. It is used to request and transmit HTML pages, images, videos, and other web content. HTTP operates over port 80 by default, but can also operate over other ports such as 8080 or 8000. HTTPS is a secure version of HTTP that uses SSL/TLS encryption to protect data transmitted between web servers and clients. It operates over port 443 by default, but can also use other ports such as 8443. FTP is a protocol used for transferring files between computers over a network. It operates over port 21 by default, but can also use other ports such as 2121. FTPS is a secure version of FTP that uses SSL/TLS encryption to protect data transmitted between computers. It operates over port 990 by default. SMTP is a protocol used for sending email messages between computers. It operates over port 25 by default, but can also use other ports such as 587. POP3 is a protocol used for retrieving email messages from a mail server. It operates over port 110 by default. IMAP is a protocol used for retrieving and managing email messages on a mail server. It operates over port 143 by default. A port number is a 16-bit unsigned integer that identifies a specific process or service running on a computer in a network. It is used to help route network traffic to the correct application or service. How many port numbers are there? There are 65,536 possible port numbers, ranging from 0 to 65,535. What are well-known ports? Well-known ports are port numbers in the range of 0 to 1023 that are assigned to specific services or applications by the Internet Assigned Numbers Authority (IANA). These ports are reserved for standard services, such as HTTP, FTP, and SMTP. What are registered ports? Registered ports are port numbers in the range of 1024 to 49,151 that are assigned to applications or services by the IANA. These ports can be used by applications that are not considered standard, but still need a reserved port. What are dynamic or private ports? Dynamic or private ports are port numbers in the range of 49,152 to 65,535 that are used by client applications to initiate a connection with a server. These ports are assigned by the operating system on the client side and are not reserved. Why are port numbers important? Port numbers are important because they help identify the specific application or service that network traffic is intended for. This allows network traffic to be correctly routed to the appropriate destination, ensuring that applications and services can communicate effectively over a network. Can port numbers be changed? Port numbers can be changed by configuring the application or service that is using the port. However, it is important to ensure that the new port number is not already in use by another application or service to avoid conflicts. In conclusion, port numbers are an important aspect of computer networking as they help identify the specific application or service that network traffic is intended for. Understanding port numbers can help troubleshoot network issues, configure firewalls and routers, and secure networks by ensuring that traffic is routed to the appropriate destination. By knowing which port numbers are commonly used for specific applications and protocols, network administrators can better manage their network and ensure efficient and secure communication. If youre a student studying networking or a budding IT courteous,, understanding common ports is essential. Ports serve as data gateways for data to enter and exit a computer, and understanding which services and applications use which ports is critical for network troubleshooting and security. Well provide you a complete list of the most often used ports and their associated services in this common ports cheat sheet, making it easier for you to traverse the world of networking. What Are Ports in Networking and Types What Are Ports? Before we go into the list of common ports, lets define ports and why theyre important in the networking world. A port number is a 16-bit number with a 0 to 65535 decimal value range. There are three various types of port number spaces: well-known ports (01023), registered ports (102449151), and dynamic ports (49152-65535). Well-known or Reserved Ports: 01023Registered Ports: 102449,591Dynamic Ports: 49,59265,535 These ports can be opened and utilised by operating system services and software programmes to send and receive data via LAN or WAN networks using certain protocols (such TCP, UDP, etc.). For example, when you visit a website as a web blogger, your computer normally connects to the typical web on port 80 (HTTP) or a secure, virtual web connection to the web server on the port 443 (HTTPS). Goes for it. With whom he communicates. Identifying which port belongs to which service facilitates firewall conversion to network diversion, but results in insufficient defence against the problem. What are well-known ports Well-known ports have port numbers ranging from 0 to 1023. The Internet Corporation for Assigned Names and Numbers (ICANN) assigned these port numbers. These ports, often known as privileged ports, are reserved for common TCP/IP applications. Each port has been given a specific application. Unencrypted online browsing is done via the Hypertext Transfer Protocol (HTTP) on port 80. POP3 (Post Office Protocol version 3) over port 110 is used to receive emails through a server. What are registered ports Registered ports have port numbers ranging from 1024 to 49,591. Although these port numbers are neither assigned or managed, they can be registered to minimise repetition. The Internet Assigned Numbers Authority (IANA) is the institution that can issue these ports; before, they were assigned by ICANN. What are dynamic ports Dynamic ports, also known as ephemeral ports, are ports that are only active for a short amount of time. They are temporary because they are opened and closed as a user is using an application. Assume I wish to connect to the internet. The first step is, of course, opening a web browser. When you start a web browser and connect to the internet, you will be connected to port 80 (HTTP) or port 443 (HTTPS), depending on the encryption of that web page. It will select a random open port, such as 49,695, to send that web page to you. When you finish looking at the web page and exit the browser youre using, the port 49,695 on your end will be closed. Common Ports Cheat Sheet Now, lets explore the most common ports with which you should acquaint yourself. Well categorize them for easier reference. Well-Known Ports (0-1023) These ports commonly associate with widely-used services and applications. Firstly, Port 21 FTP (File Transfer Protocol) is used for transferring files over a network.Secondly, Port 22 SSH (Secure Shell) provides secure remote access to systems and secure file transfers.Next, Port 23 Telnet is a less secure remote access protocol used for managing network devices.Moving on, Port 25 SMTP (Simple Mail Transfer Protocol) handles outgoing email communication.Additionally, Port 53 DNS (Domain Name System) resolves domain names to IP addresses.Subsequently, Port 80 HTTP (Hypertext Transfer Protocol) is used for unencrypted web traffic.Moreover, Port 443 HTTPS (Hypertext Transfer Protocol Secure) provides secure, encrypted web communication.Furthermore, Port 110 POP3 (Post Office Protocol version 3) retrieves email from a mail server.Similarly, Port 143 IMAP (Internet Message Access Protocol) allows access to email on a remote mail server.Lastly, Port 3389 RDP (Remote Desktop Protocol) enables remote desktop connections. Registered Ports (1024-49151) These ports are frequently linked with applications and services that are less well-known than those in the well-known range but are nevertheless required for certain purposes. Port 3306 MySQL Serves as a popular database management system.Port 5432 PostgreSQL Represents another widely-used open-source database management system.Port 8080 HTTP Alternate (HTTP Proxy) Frequently used as a secondary HTTP port.Port 27017 MongoDB Addresses high-volume data storage needs through a NoSQL database.Port 5060 SIP (Session Initiation Protocol) Facilitates voice and video calls across IP networks.Port 6660-6669 Internet Relay Chat (IRC) Enables real-time text communication.To begin with, Port 3306 MySQL is a popular database management system.Next up, Port 5432 PostgreSQL is another widely-used open-source database management system.If you need an alternate HTTP port, Port 8080 HTTP Alternate (HTTP Proxy) is often used as a secondary HTTP port.For NoSQL database enthusiasts, Port 27017 MongoDB is a go-to choice for high-volume data storage.In the realm of communication, Port 5060 SIP (Session Initiation Protocol) facilitates voice and video calls over IP networks.If youre a fan of real-time text communication, Port 6660-6669 Internet Relay Chat (IRC) is the way to go.And for secure web communication through an alternate port, dont forget Port 8443 HTTPS Alternate (HTTPS Alt). Dynamic and Private Ports (49152-65535) These ports are often used for dynamic, private, or temporary purposes. They are not assigned to specific services but are available for use as needed. Additionally, Port 49152-65535 Ephemeral Ports (also known as dynamic ports) are used by client applications for temporary purposes, such as establishing connections. Additional Ports to Know While the above ports cover the most common ones, its worth mentioning a few more ports that may be important in specific contexts. Port 161/162 SNMP (Simple Network Management Protocol) is used in network management to manage and monitor network devices.For simpler file transfers, Port 69 TFTP (Trivial File Transfer Protocol) is a viable option. Conclusion Understanding common ports and their associated services is vital for anyone involved in networking or IT systems. This cheat sheet is a helpful resource for navigating the world of networking. Remember that, while these are the most frequent ports, there are many more, and new ones may emerge as technology improves. Maintain your interest and keep learning in order to keep your networking knowledge up to date. Whether youre a student or an IT professional, this information will help you master the complexities of networking. Here are some of the most often-encountered network ports and their associated services. The physical ports on your computer allow communicate with peripheral devices such as your keyboard and mouse and to connect with internet devices via Ethernet cables. Witin computer networking,ports serve a similar purpose. When a computer system seeks to connect to another computer, the port serves as a communication endpoint. It is also possible for different services running on the same computerto expose various ports and communicate with one another using these ports. In simple terms, if a software application or service needs to communicate with others, it will expose a port. Ports are identified with positive 16-bit unsigned integers, ranging from 0 to 65535. Other services use this port number to communicate with the service or app. Port numbers are divided into three ranges: well-known ports, registered ports, and dynamic or private ports.Well-known ports (also known as system ports) are numbered from 0 through 1023. For example, to connect to the host example.com via SSH, I would use this command:ssh username@example.com -vIn this example, -v stands for verbose, andyou should see output similar to this:debug1: Connecting to example.com [] port 22As shown, SSH is trying to connect to example.com using port number 22. You may use the -p option to specify another port number; otherwise, SSH will defaultto 22.The Internet Assigned Numbers Authority (IANA) has assigned port numbers to commonly used services like SSH, FTP, HTTP, HTTPS, and others. Here are some of the most common ones:Port NumberUsage20File Transfer Protocol (FTP) Data Transfer21File Transfer Protocol (FTP) Command Control22Secure Shell (SSH)23Telnet - Remote login service, unencrypted text messages25Simple Mail Transfer Protocol (SMTP) E-mail Routing53Domain Name System (DNS) service80Hypertext Transfer Protocol (HTTP) used in World Wide Web110Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server119Network News Transfer Protocol (NNTP)123Network Time Protocol (NTP)143Internet Message Access Protocol (IMAP) Management of Digital Mail161Simple Network Management Protocol (SNMP)194Internet Relay Chat (IRC)443HTTP Secure (HTTPS) HTTP over TLS/SSL In my work, I most commonly come across ports 80, 443, 20, 21, 22, 23, 25, and 53. Knowing these portscan help you work more efficiently.What ports do you use the most, and why?Learn more about Linux networking Port numbers are an essential aspect of computer networking that facilitate the communication between devices over TCP/IP networks. They are numerical identifiers that are used by protocols to distinguish different services or applications running on the same device. This article provides an in-depth exploration of port numbers, covering their classification, common protocols associated with them, their purpose in networking, and best practices. What are Port Numbers?A port number is a 16-bit numeric value that ranges from 0 to 65535. These numbers are crucial for establishing network connections and ensuring that data is transmitted accurately between devices. Each service or application listening on a device is assigned a specific port number, making it possible for a single IP address to handle multiple connections simultaneously.When a device sends or receives data via the Internet, it does so using a combination of an IP address and port number, often represented as IP:Port. For instance, in a web server scenario, a typical address might be 192.168.1.1:80, where 80 is the port number associated with HTTP service.Classification of Port NumbersPort numbers are categorized into three ranges: Well-Known Ports (0-1023): These ports are reserved for specific services and protocols. They are recognized universally and are associated with standard network communication protocols. For instance, port 80 is used for HTTP, and port 443 is utilized for HTTPS.Registered Ports (1024-49151): These ports are not reserved but can be registered with the Internet Assigned Numbers Authority (IANA) for use by specific applications. Developers use these ports to avoid conflicts and ensure that their applications can communicate without interference from other services.Dynamic or Private Ports (49152-65535): Also known as ephemeral ports, these are used for temporary communication and are often assigned dynamically by the operating system as needed. When an application wants to initiate a connection, it can use any available dynamic port.Importance of Port Numbers in NetworkingPort numbers play a vital role in enabling communication between devices on a network. Their importance can be highlighted in several key areas:Multi-Service Support: Multiple applications can run on a single server without interference. Since each application listens to a unique port number, data can be routed correctly based on the destination port.Protocol Differentiation: Different protocols utilize different port numbers to differentiate between service types. For example, a web server uses port 80 for HTTP and port 443 for HTTPS, ensuring that browsers know which protocol to use.Firewall and Security Configurations: Network security devices can filter traffic based on port numbers. By restricting access to certain ports, organizations can protect their network from unauthorized access.Load Balancing: Port numbers enable load balancing across multiple servers by directing traffic based on specific service ports, ensuring efficient use of resources.Troubleshooting and Network Management: Knowledge of port numbers fosters effective network troubleshooting. Administrators can diagnose issues related to specific services and determine whether they are operational.Commonly Used Port Numbers and Their AssociationsThe following is a list of common port numbers along with their associated protocols and services:Port 20: FTP (File Transfer Protocol, data transfer)Port 21: FTP (control/protocol)Port 22: SSH (Secure Shell)Port 23: TelnetPort 25: SMTP (Simple Mail Transfer Protocol)Port 53: DNS (Domain Name System, name resolution)Port 67: DHCP (Dynamic Host Configuration Protocol, server)Port 68: DHCP (client)Port 80: HTTP (HyperText Transfer Protocol)Port 110: POP3 (Post Office Protocol version 3)Port 143: IMAP (Internet Message Access Protocol)Port 443: HTTPS (HTTP Secure)Port 3306: MySQL DatabasePort 3389: RDP (Remote Desktop Protocol)The Role of Transport Protocols: TCP and UDPThe two primary transport layer protocols that utilize port numbers are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Each plays a distinct role in how data is transmitted over a network. Transmission Control Protocol (TCP):Connection-Oriented: TCP establishes a connection before data is sent, ensuring reliability and order.Error Checking: TCP implements mechanisms to check for errors and retransmit lost packets, making it ideal for applications where accuracy is critical, such as web browsing and file transfers.Flow Control: TCP manages data transmission rates to prevent overwhelming the receiver.User Datagram Protocol (UDP):Connectionless: UDP sends data without establishing a connection, making it quicker but less reliable.Low Overhead: Because UDP lacks error-checking and flow control, it is more efficient for applications that require speed over reliability, such as video streaming or online gaming.Port Scanning and its ImplicationsPort scanning is a technique used to identify open ports on a networked device. Security professionals and malicious actors alike utilize port scanning to discover vulnerabilities in a system. Types of Port Scans:TCP Connect Scan: Attempts to complete a full TCP handshake to identify open ports.SYN Scan: Sends SYN packets to discover listening ports without establishing a full connection (stealthier than a TCP Connect Scan).UDP Scan: Sends UDP packets to detect open UDP ports.Implications: Port scanning can expose services that should not be accessible over the internet. For instance, a port scanner might identify a vulnerable version of an FTP server that could be exploited. Therefore, organizations should regularly monitor their networks for unauthorized scanning and employ firewalls to restrict access to unnecessary ports.Securing Port NumbersSecurity best practices for managing port numbers are essential in protecting networked assets. Here are some recommended strategies:Minimize Open Ports: Keep only essential services running and restrict access to the necessary ports. Close any unused ports to reduce risk.Use Firewalls: Utilize hardware and software firewalls to filter incoming and outgoing traffic based on port numbers. This can help prevent unauthorized access and attacks.Regular Network Audits: Conduct periodic audits to identify open ports and running services. This practice helps ensure that security policies are consistently adhered to.Change Default Ports: For services like SSH, changing the default port (22) to a non-standard port can provide additional obscurity against automated attacks.Implement Intrusion Detection Systems (IDS): Use IDS to monitor network traffic for suspicious activity, including unexpected port scans and access attempts.Educate Employees: Phishing attacks and social engineering techniques can lead to security breaches. Training staff on the importance of network security will bolster overall protection.ConclusionUnderstanding port numbers is fundamental for anyone involved in computer networking, whether for everyday users, system administrators, or cybersecurity experts. This numerical system not only enables multiple applications to coexist on a single machine but also plays a pivotal role in communication protocols and network security. By recognizing the significance of well-known, registered, and dynamic ports, along with the services they represent, one can appreciate the structured environment in which modern networks operate. Additionally, securing these ports contributes to a holistic approach to network management, significantly reducing vulnerabilities that could be exploited by malicious actors.As technology continues to evolve, the importance of port numbers within computer networks will remain a critical aspect of networking environments. By understanding and implementing best practices regarding port management and security, organizations can safeguard their networks against an increasingly complex landscape of security threats. Port number is a 16-bit numerical value that ranges from 0 to 65535. Well-known port (0-1023), registered port (1024-49151), and dynamic port is three types of port number space. (49152-65535). These ports can be opened and used by software applications and operating system services to send and receive data over networks (LAN or WAN) that employ certain protocols (eg TCP, UDP). For example, we use 80 for HTTP-web-based plain-text surfing and 443 for HTTPS-web-based encrypted websites in our daily work. To conclude, a port is a logical form to identify system activities or various network services used to create local or network-based communications. What are the functions of ports?When interacting over the Internet, TCP and UDP protocols make connections, recompile data packages after the transfer, and then deliver them to applications on the recipient's device. For this handover to work, the operating system must install and open the gateway for the transfer. Each door has a unique code number. After transmission, the receiving system uses the port number to determine where the data should be sent. The port numbers of the sender and receiver are always included in the data packet. Ports are assigned sequential numbers from 0 to 65535. Some of these codes are standardized, meaning they are assigned to certain uses. Since code numbers are universally recognized and permanently assigned, these standard ports are also known as well-known ports. Registered ports are those that organizations or software developers have registered for their applications. Registration is handled by the Internet Assigned Numbers Authority (IANA). A diverse selection of dynamically assigned port numbers is also available. For example, when viewing websites, browsers use these ports. After that, the port number is free again. Why is it important to know these ports?Any security researcher, bug bounty hunter, or anyone working with service configuration would benefit from this. Knowing how to do more thorough scans such as version detection or known vulnerabilities for ancient services that are still operating in the infrastructure, especially when using tools like Nmap, is handy when getting to know these protocols and services. The most 50 significant ports are listed here:The following are some of the most common service names, transport protocol names, and port numbers used to differentiate between specific services that employ TCP, UDP, DCCP, and SCTP. Port Number Service nameTransport protocolDescription7EchoTCP, UDPEcho service20FTP-dataTCP, SCTPFile Transfer Protocol data transfer21FTPTCP, UDP, SCTPFile Transfer Protocol (FTP) control connection22SSH-SCPTCP, UDP, SCTPSecure Shell, secure logins, file transfers (scp, sftp), and port forwarding23TelnetTCPTelnet protocolunencrypted text communications25SMTPTCPSimple Mail Transfer Protocol, used for email routing between mail servers53DNSTCP, UDPDomain Name System name resolver69TFTPUDPTrivial File Transfer Protocol80HTTPTCP, UDP, SCTPHypertext Transfer Protocol (HTTP) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP 88KerberosTCP, UDPNetwork authentication system102Iso-tsapTCPISO Transport Service Access Point (TSAP) Class 0 protocol110POP3TCPPost Office Protocol, version 3 (POP3)135Microsoft EPMAPTCP, UDPMicrosoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, used to remotely manage services including DHCP server, DNS server, and WINS. Also used by DCOM137NetBIOS-nsTCP, UDPNetBIOS Name Service, used for name registration and resolution139NetBIOS-ssnTCP, UDPNetBIOS Session Service143IMAP4TCP, UDPInternet Message Access Protocol (IMAP), management of electronic mail messages on a server381HP OpenviewTCP, UDPHP data alarm manager383HP OpenviewTCP, UDPHP performance data collector.443HTTP over SSLTCP, UDP, SCTPHypertext Transfer Protocol Secure (HTTPS) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP.464KerberosTCP, UDPKerberos Change/Set password465SMTP over TLS/SSL, SSMTCPAuthenticated SMTP over TLS/SSL (SMTPS), URL Rendezvous Directory for SSM (Cisco protocol)587SMTPTCPEmail message submission593Microsoft DCOMTCP, UDPHTTP RPC Ep Map, Remote procedure call over Hypertext Transfer Protocol, often used by Distributed Component Object Model services and Microsoft Exchange Server636LDAP over TLS/SSLTCP, UDPLightweight Directory Access Protocol over TLS/SSL691MS ExchangeTCPMS Exchange Routing902VMware ServerunofficialVMware ESXi989FTP over SSLTCP, UDPFTPS Protocol (data), FTP over TLS/SSL990FTP over SSLTCP, UDPFTPS Protocol (control), FTP over TLS/SSL993IMAP4 over SSLTCPInternet Message Access Protocol over TLS/SSL (IMAPS)995POP3 over SSLTCP, UDPPost Office Protocol 3 over TLS/SSL1025Microsoft RPCTCPMicrosoft operating systems tend to allocate one or more unsuspected, publicly exposed services (probably DCOM, but who knows) among the first handful of ports immediately above the end of the service port range (1024+).1194OpenVPNTCP, UDPOpenVPN1337WASTEunofficialWASTE Encrypted File Sharing Program1589Cisco VQPTCP, UDPCisco VLAN Query Protocol (VQP)1725SteamUDPValve Steam Client uses port 17252082cPanelunofficialcPanel default2083radsec, cPanelTCP, UDPSecure RADIUS Service (radsec), cPanel default SSL2483Oracle DBTCP, UDPOracle database listening for insecure client connections to the listener, replaces port 15212484Oracle DBTCP, UDPOracle database listening for SSL client connections to the listener2967Symantec AVTCP, UDPSymantec System Center agent (SSC-AGENT)3074XBOX LiveTCP, UDPXbox LIVE and Games for Windows Live3306MySQLTCPMySQL database system3724World of WarcraftTCP, UDPSome Blizzard games, Unofficial Club Penguin Disney online game for kids4664Google DesktopunofficialGoogle Desktop Search5432PostgreSQLTCPPostgreSQL database system5900RFB/VNC ServerTCP, UDPvirtual Network Computing (VNC) Remote Frame Buffer RFB protocol6665-6669IRCTCPInternet Relay Chat .6881BitTorrentunofficialBitTorrent is part of the full range of ports used most often6999BitTorrentunofficialBitTorrent is part of the full range of ports used most often6970QuicktimeunofficialQuickTime Streaming Server8086Kaspersky AVTCPKaspersky AV Control Center8087Kaspersky AVUDPKaspersky AV Control Center8222VMware ServerTCP, UDPVMware Server Management User Interface (insecure Web interface).9100PDLTCPPDL Data Stream, used for printing to certain network printers.10000BackupExecunofficialWebmin, Web-based Unix/Linux system administration tool (default port)12345NetBusunofficialNetBus remote administration tool (often Trojan horse).27374Sub7unofficialSub7 default31337Back OrificeunofficialBack Orifice 2000 remote administration tools

Port over number. Why do we use port numbers. Why use port number. Why use different ports.