Most Common TCP Ports

TCP/IP (Transmission Control Protocol/Internet Protocol), the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

UDP(User Datagram Protocol) a connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network.

In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are preassigned to them by the IANA, and these are known as well-known ports (specified in RFC 1700). IANA Internet Assigned Numbers Authority, an organisation working under the auspices of the Internet Architecture Board (IAB) that is responsible for assigning new Internet-wide IP addresses Port numbers range from 0 to 65536, but only ports numbers 0 to 1024 are reserved for privileged services and designated as well-known ports. This list of well-known port numbers specifies the port used by the server process as its contact port.

Port Number Description

1 TCP Port Service Multiplexer (TCPMUX)

5 Remote Job Entry (RJE)

7 ECHO

18 Message Send Protocol (MSP)

20 FTP Data. File Transfer Protocol is a protocol used on the Internet for sending files.

21 FTP -- Control

22 SSH Remote Login Protocol. Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.

When using ssh's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.

SSH is available for Windows, Unix, Macintosh, and OS/2, and it also works with RSA authentication.

23 Telnet. A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

25 Simple Mail Transfer Protocol (SMTP). Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

29 MSG ICP

37 Time

42 Host Name Server (Nameserv)

43 WhoIs

49 Login Host Protocol (Login)

53 Domain Name System (DNS). Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

69 Trivial File Transfer Protocol (TFTP). Trivial File Transfer Protocol, a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP)and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

70 Gopher Services . A system that pre-dates the World Wide Web for organising and displaying files on Internet servers. A Gopher server presents its contents as a hierarchically structured list of files. With the ascendance of the Web, many gopher databases were converted to Web sites which can be more easily accessed via Web search engines.

Gopher was developed at the University of Minnesota and named after the school's mascot. Two systems, Veronica and Jughead, let you search global indices of resources stored in Gopher systems.

79 Finger. A UNIX program that takes an e-mail address as input and returns information about the user who owns that e-mail address. On some systems, finger only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course, the user must first enter this information into the system. Many e-mail programs now have a finger utility built into them.

80 HTTP. Short for HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

103 X.400 Standard. An ISO and ITU standard for addressing and transporting e-mail messages. It conforms to layer 7 of the OSI model and supports several types of transport mechanisms, including Ethernet, X.25, TCP/IP, and dial-up lines.

108 SNA Gateway Access Server.

109 POP2

110 POP3

115 Simple File Transfer Protocol (SFTP)

118 SQL Services

119 Newsgroup (NNTP)

137 NetBIOS Name Service. Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities.

139 NetBIOS Datagram Service

143 Interim Mail Access Protocol (IMAP)

150 NetBIOS Session Service

156 SQL Server

161 SNMP

179 Border Gateway Protocol (BGP) Border Gateway Protocol, an exterior gateway routing protocol that enables groups of routers (called autonomous systems) to share routing information so that efficient, loop-free routes can be established. BGP is commonly used within and between Internet Service Providers (ISPs). The protocol is defined in RFC 1771.

190 Gateway Access Control Protocol (GACP)

194 Internet Relay Chat (IRC)

197 Directory Location Service (DLS)

389 Lightweight Directory Access Protocol (LDAP)

396 Novell Netware over IP

443 HTTPS

444 Simple Network Paging Protocol (SNPP)

445 Microsoft-DS

458 Apple QuickTime

546 DHCP Client Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

DHCP client support is built into Windows 95 and NT workstation. NT 4 server includes both client and server support.

547 DHCP Server

563 SNEWS

9 MSN

1080 Socks

Source: http://www.go4expert.com/articles/common-tcp-ports-t498/