Port (computer networking)

In computer networking, a **port** is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service. A port is identified for each transport protocol and address combination by a 16-bit unsigned number, known as the **port number**. The most common transport protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

A port number is always associated with an IP address of a host and the type of transport protocol used for communication. It completes the destination or origination network address of a message. Specific port numbers are reserved to identify specific services so that an arriving packet can be easily forwarded to a running application. For this purpose, port numbers lower than 1024 identify the historically most commonly used services and are called the well-known port numbers. Higher-numbered ports are available for general use by applications and are known as ephemeral ports.

Ports provide a multiplexing service for multiple services or multiple communication sessions at one network address. In the client–server model of application architecture, multiple simultaneous communication sessions may be initiated for the same service.

Contents

Port number

A port number is a 16-bit unsigned integer, thus ranging from 0 to 65535. For TCP, port number 0 is reserved and cannot be used, while for UDP, the source port is optional and a value of zero means no port. A process associates its input or output channels via an internet socket, which is a type of file descriptor, associated with a transport protocol, an IP address, and a port number. This is known as *binding*. A socket is used by a process to send and receive data via the network. The operating system's networking software has the task of transmitting outgoing data from all application ports onto the network, and forwarding arriving network packets to processes by matching the packet's IP address and port number to a socket. For TCP, only one process may bind to a specific IP address and port combination. Common application failures, sometimes called *port conflicts*, occur when multiple programs attempt to use the same port number on the same IP address with the same protocol.

Applications implementing common services often use specifically reserved well-known port numbers for receiving service requests from clients. This process is known as *listening*, and involves the receipt of a request on the well-known port potentially establishing a one-to-one server-client dialog, using this listening port. Other clients may simultaneously connect to the same listening port; this works because a TCP connection is identified by a tuple consisting of the local address, the local port, the remote address, and the remote port.[1] The well-known ports are defined by convention overseen by the Internet Assigned Numbers Authority (IANA). In many operating systems special privileges are required for applications to bind to these ports because these are often deemed critical to the operation of IP networks. Conversely, the client end of a connection typically uses a high port number allocated for short term use, therefore called an ephemeral port.

Common port numbers

IANA is responsible for the global coordination of the DNS root, IP addressing, and other protocol resources. This includes the registration of commonly used port numbers for well-known internet services.

The port numbers are divided into three ranges: the *well-known ports*, the *registered ports*, and the *dynamic* or *private ports*.

The well-known ports (also known as *system ports*) are those numbered from 0 through 1023. The requirements for new assignments in this range are stricter than for other registrations.[2]

Notable well-known port numbers

Number	Assignment
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) email delivery
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP3)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL
546, 547	DHCPv6 IPv6 version of DHCP

The registered ports are those from 1024 through 49151. IANA maintains the official list of well-known and registered ranges.[3]

The dynamic or private ports are those from 49152 through 65535. One common use for this range is for ephemeral ports.

Network behavior

Transport-layer protocols, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), transfer data using protocol data units (PDUs). For TCP, the PDU is a segment, and for UDP it is a datagram. Both protocols use a header field for indicating the source and destination port numbers. The port numbers are encoded in the transport protocol packet header, and they can be readily interpreted not only by the sending and receiving hosts but also by other components of the networking infrastructure. In particular, firewalls are commonly configured to differentiate between packets based on their source or destination port numbers. Port forwarding is an example application of this.

Port scanning

The practice of attempting to connect to a range of ports in sequence on a single host is commonly known as port scanning. This is usually associated either with malicious cracking attempts or with network administrators looking for possible vulnerabilities to help prevent such attacks. Port connection attempts are frequently monitored and logged by hosts. The technique of port knocking uses a series of port connections (knocks) from a client computer to enable a server connection.

Examples

An example of the use of ports is the delivery of email. A server used for sending and receiving email generally needs two services. The first service is used to transport email to and from other servers. This is accomplished with the Simple Mail Transfer Protocol (SMTP). A standard SMTP service application listens on TCP port 25 for incoming requests. The second service is usually either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP) which is used by email client applications on users' personal computers to fetch email messages from the server. The POP service listens on TCP port number 110. Both services may be running on the same host computer, in which case the port number distinguishes the service that was requested by a remote computer, be it a user's computer or another mail server.

While the listening port number of a server is well defined (IANA calls these the well-known ports), the client's port number is often chosen from the dynamic port range (see below). In some applications, the clients and the server each use specific port numbers assigned by the IANA. A good example of this is DHCP in which the client always uses UDP port 68 and the server always uses UDP port 67.

Use in URLs

Port numbers are sometimes seen in web or other uniform resource locators (URLs). By default, HTTP uses port 80 and HTTPS uses port 443, but a URL like `http://www.example.com:8080/path/` specifies that the web browser connects instead to port 8080 of the HTTP server.

History

The concept of port numbers was established by the early developers of the ARPANET in informal cooperation of software authors and system administrators. The term *port number* was not yet in use. It was preceded by the use of the term *socket number* in the early development stages of the network. A socket

number for a remote host was a 40-bit quantity.[4] The first 32 bits were similar to today's IPv4 address, but at the time the most-significant 8 bits were the host number. The least-significant portion of the socket number (bits 33 through 40) was an entity called *Another Eightbit Number*, abbreviated AEN.[5] Today, *network socket* refers to a related but distinct concept, namely the internal address of an endpoint used only within the node.

On March 26, 1972, Vint Cerf and Jon Postel called for documenting the then-current usages and establishing a socket number catalog in RFC 322. Network administrators were asked to submit a note or place a phone call, "*describing the function and socket numbers of network service programs at each HOST*".[6] This catalog was subsequently published as RFC 433 in December 1972 and included a list of hosts and their port numbers and the corresponding function used at each host in the network. This first registry function served primarily as documentation of usage and indicated that port number usage was conflicting between some hosts for "*useful public services*".[5] The document promised a resolution of the conflicts based on a standard that Postel had published in May 1972 in RFC 349, in which he first proposed official assignments of port numbers to network services and suggested a dedicated administrative function, which he called a *czar*, to maintain a registry.[7] The 256 values of the AEN were divided into the following ranges:

AEN ranges

Port number range	Assignment
0 through 63	Network-wide standard functions
64 through 127	Host-specific functions
128 through 239	Reserved for future use
240 through 255	Any experimental function

The Telnet service received the first official assignment of the value 1. In detail, the first set of assignments was:[7]

Port assignments in RFC 349 (https://datatracker.ietf.org/doc/html/rfc349)

Port number	Assignment
1	Telnet
3	File transfer
5	Remote job entry
7	Echo
9	Discard

In the early ARPANET, the AEN was also called a *socket name*,[8] and was used with the Initial Connection Protocol (ICP), a component of the Network Control Protocol (NCP).[9][10] NCP was the forerunner of the modern Internet protocols. Today the terminology *service name* is still closely connected with port numbers, the former being text strings used in some network functions to represent a numerical port number.

References

1. Postel, John. "RFC 793" (http://www.ietf.org/rfc/rfc793.txt). Retrieved 29 June 2012.

2. Michelle Cotton; Lars Eggert; et al. (August 2011). *Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry* (https://datatracker.ietf.org/doc/html/rfc6335). IETF. doi:10.17487/RFC6335 (https://doi.org/10.17487%2FRFC6335). BCP 165. RFC 6335 (https://datatracker.ietf.org/doc/html/rfc6335).
3. "Port Numbers" (https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml). Internet Assigned Numbers Authority (IANA).
4. RFC 36, *Protocol Notes*, S. Crocker (16 March 1970)
5. RFC 433, *Socket number list*, J. Postel, N. Neigus (22 December 1972)
6. RFC 322, *Well Known Socket Numbers*, V. Cerf, J. Postel (26 March 1972)
7. RFC 349, *Proposed Standard Socket Numbers* J. Postel (30 May 1972)
8. RFC 197, *Initial Connection Protocol--Reviewed*, A. Shoshani, E. Harslem (14 July 1971)
9. NIC 7104, *ARPANET Protocol Handbook*
10. Postel, Jon; Feinler, E. (1978). *ARPANET Protocol Handbook*. Menlo Park, CA: Network Information Center.
