Global Information Assurance Certification Paper

An Explanation of Ports

Arthur Hunt

February 3, 2001

Introduction

Being new to this field, I was somewhat confused by the term "ports". I was vaguely aware that they had something to do with program use. Taking my "Security Essentials" course at GIAC was a bit of a problem with this limited knowledge. Discussions turned to blocking of this or that port, and to look to see if a certain port was open to detect a security compromise. The night after the first class, I bought and read books, surfed the net, and tried to get up to speed on what ports were, how they were used, and which ones were used for what purpose. I felt as though I was the only one attending this class without this knowledge. However, just in case I wasn't, I decided to write this paper.

General Port Information

All upper layer applications that use TCP or UDP have a port number. Port numbers are 16-bit numbers that range from 0 to 65535. They are used to determine which service is being called upon. Theoretically, port numbers could be assigned to a particular service however an operating system chooses. However, certain conventions have been adopted to allow for better communication. The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of ports, and does so in its Request For Comments (RFC) 1700. These commonly accepted port assignments allows the port number to identify the type of service that one TCP or UDP system is requesting from another. For example, TCP port 23 is used for the service named Telnet, and UDP port 69 is used for the service named Trivial File Transfer Protocol (TFTP).

A partial /etc/services file from an HP-UX is shown below. You can see the port numbers are paired with transport protocol names because different protocols may use the same port number.

```
/  $cat /etc/services
# @(#)services $Revision: 1.30.212.3 $ $Date: 96/04/05 11:18:17 $
#
# This file associates official service names and aliases with
# the port number and protocol the services use.
#
# The form for each entry is:
# <official service name>  <port number/protocol name>  <aliases>
#
tcpmux          1/tcp                   # TCP port multiplexer (RFC 1078)
echo            7/tcp                   # Echo
echo            7/udp                   #
discard         9/tcp  sink null        # Discard
discard         9/udp  sink null        #
systat          11/tcp  users           # Active Users
```

```
daytime     13/tcp                  # Daytime
daytime     13/udp                  #
qotd        17/tcp  quote           # Quote of the Day
chargen     19/tcp  ttytst source   # Character Generator
chargen     19/udp  ttytst source   #
ftp-data    20/tcp                  # File Transfer Protocol (Data)
ftp         21/tcp                  # File Transfer Protocol (Control)
telnet      23/tcp                  # Virtual Terminal Protocol
smtp        25/tcp                  # Simple Mail Transfer Protocol
time        37/tcp  timeserver      # Time
time        37/udp  timeserver      #
rlp         39/udp  resource        # Resource Location Protocol
whois       43/tcp  nickname        # Who Is
domain      53/tcp  nameserver      # Domain Name Service
domain      53/udp  nameserver      #
```

Port numbers are divided into two types as defined in RFC 1700 located at ftp://ftp.isi.edu/in-notes/rfc1700.txt, dated October 1994: Well Known Ports and Registered Ports.

Until 1992, the Well Known Ports were between 0 and 255. The IANA now manages ports between 0 and 1023 as Well Known Ports. As defined in RFC 1700:

> The Well Known Ports are controlled and assigned by the IANA and on most systems can only be used by system (or root) processes or by programs executed by privileged users.
>
> Ports are used in the TCP [RFC793] to name the ends of logical connections which carry long term conversations. For the purpose of providing services to unknown callers, a service contact port is defined. This list specifies the port used by the server process as its contact port. The contact port is sometimes called the "well-known port".
>
> To the extent possible, these same port assignments are used with the UDP [RFC768].
>
> The assigned ports use a small portion of the possible port numbers.

Registered Ports range from number 1024 to 65535. The IANA does not register these ports, it only lists them as a convenience.

Examples of Port Use

Each transport layer segment has a field that contains a destination port number. The destination host uses this port number to deliver the segment's data to the correct application process. This task of delivering the segment's data to the correct application process is called demultiplexing. In the source host, the task of gathering the data from an application process and adding the data

to the header information to create a segment is call multiplexing. To give a non-computer related example, in a household one person will pick up all the mail from the mailbox. That person then gives the mail to the correct individual by matching the name on the envelop to the person in the household. This is demultiplexing. The reverse is one person collecting all the mail from members of the household and placing the mail in the mailbox to be delivered. That is multiplexing. Demultiplexing is illustrated in Figure 1.

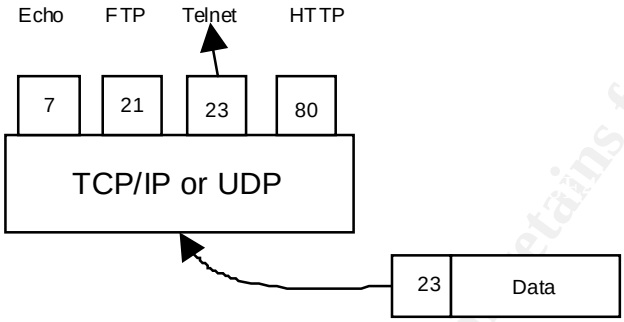
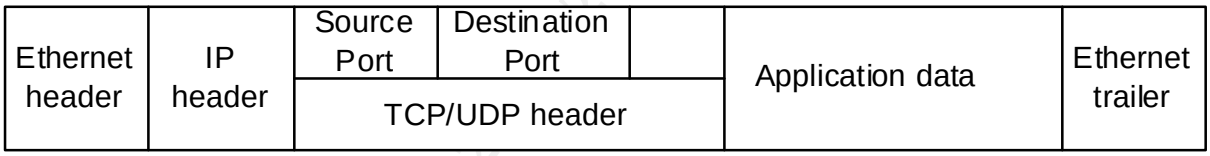


Figure 1

Port information is contained in the first 32 bits of the TCP or UDP header. The first 16 bits are the port number of the source computer, while the second 16 bits, the port of the destination computer. This is illustrated in Figure 2.



Ethernet Frame

Figure 2

The TCP or UDP protocol looks at the port information contained in the header to determine which application in the next layer will receive the data. The source and destination ports are both required in order for the destination host to have the ability to run more than one process of a certain type at the same time.

As previously stated, Well Known Ports are standardized port numbers that enable remote computers to know which port to connect to for a particular network service. However, another type of port is a Dynamically Allocated Port. Dynamically Allocated Ports are not preassigned, but are assigned to processes when they are needed. This dynamic allocation of port numbers provides the flexibility to support multiple users. The system ensures that it does not assign the same dynamically allocated port number to two processes.

For example, suppose a user wished to connect to a telnet session with a computer. The source would dynamically assign a port number as the source port (say, 3044) and 23 as a destination port. It assigns 23 as the destination port because it is the Well Known Port for Telnet services.

The destination host receives the segment, and responds back using 23 as its source port and 3044 as its destination port.

The combination of a port number with an IP address is called a socket. A socket uniquely identifies a single network process within the entire Internet. A pair of sockets, one for the source and one for the destination host define a connection for connection-oriented protocols like TCP.

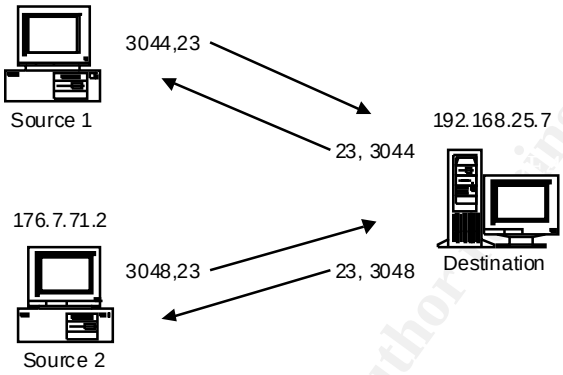


Figure 3

If a second user also requests Telnet services from the same destination host, the second user is given a different random source port number and the same destination port (See Figure 3). It is the pair of port numbers, source and destination, that uniquely identifies the application process within the destination host. The pair of sockets uniquely identifies the Internet connection between each source and destination host.

Active and Passive Ports

One more final distinction needs to be made about different types of ports. This is the difference between active and passive ports.

Using TCP, there are two methods to establish a connection: active and passive. A passive connection is one in which an application process instructs TCP to wait for the arrival of a connection request from a source host. When TCP receives the request, it assigns a port number. An active connection is one in which the TCP actually issues a request for an instruction from an application process that provides the port number. Most TCP connections are established by an active request to a passive port. However, it should be noted that TCP could be configured to allow a request for a connection that includes both a local socket and the remote socket number.

References

Enders, Matthias and Hayes, Steve. "2.10 Ports and Sockets." "TCP/IP Tutorial and Technical Overview." 5th Edition. June 1995. http://www4.ulpgc.es/tutoriales/tcpip/pru/3376c210.htm#sokapi. 29 January 2001.

Hunt, Craig. "2.7 Protocols, Ports, and Sockets." "TCP/IP Network Administration." 2nd Edition. December 1997. http://www.dimas.burnet.ru/oreilly/cdrom/tcpip/ch02_07.htm. 29 January 2001.

Kurose, James F. and Ross, Keith W. " 3.2 Multiplexing and Demultiplexing Applications." "Computer Networking: A Top-Down Approach Featuring the Internet." http://www-net.cs.umass.edu/kurose/transport/fund.html, 1 February 2001.

Pavincich, Marco. "TCP/IP In More Detail." 04 July 1997. http://home.mira.net/~marcop/tcpip_detail.htm, 1 February 2001.

Postel, J. and Reynolds, J. "RFC1700 Assigned numbers." October 1994. ftp://ftp.isi.edu/in-notes/rfc1700.txt. 25 January 2001.

Other Suggested Reading

Raz, Uri. "Uri's TCP/IP Resources List: TCP/IP Resources List: FAQs, tutorials, guides, web pages & sites, and books about TCP/IP." http://www.ce.unipr.it/~mczane/tcip_rl.html. 2 February 2001 – This page is a wealth of resources about anything at all to do with TCP/IP. It starts off will a list of published books and on-line descriptions of them then on to on-line books and magazines. If you want to know anything about TCP/IP, this should be a stop.

Simovits Consulting, "Ports Used by Trojans." 25 September 2000. http://www.simovits.com/nyheter9902.html. 28 January 2001. – Just what it says, a listing of many Trojans and which port they utilize. You can sort by name or port or any number of different ways.