# Port Numbers

14.4.1

## Multiple Separate Communications

As you have learned, there are some situations in which TCP is the right protocol for the job, and other situations in which UDP should be used. No matter what type of data is being transported, both TCP and UDP use port numbers.

The TCP and UDP transport layer protocols use port numbers to manage multiple, simultaneous conversations. As shown in the figure, the TCP and UDP header fields identify a source and destination application port number.


The source port number is associated with the originating application on the local host whereas the destination port number is associated with the destination application on the remote host.

For instance, assume a host is initiating a web page request from a web server. When the host initiates the web page request, the source port number is dynamically generated by the host to uniquely identify the conversation. Each request generated by a host will use a different dynamically created source port number. This process allows multiple conversations to occur simultaneously.

In the request, the destination port number is what identifies the type of service being requested of the destination web server.. For example, when a client specifies port 80 in the destination port, the server that receives the message knows that web services are being requested.

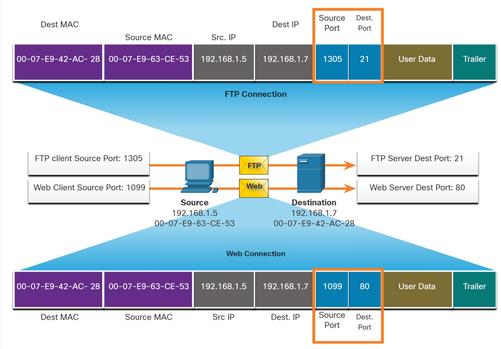
A server can offer more than one service simultaneously such as web services on port 80 while it offers File Transfer Protocol (FTP) connection establishment on port 21.

14.4.2

## Socket Pairs

The source and destination ports are placed within the segment. The segments are then encapsulated within an IP packet. The IP packet contains the IP address of the source and destination. The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a socket.

In the example in the figure, the PC is simultaneously requesting FTP and web services from the destination server.




In the example, the FTP request generated by the PC includes the Layer 2 MAC addresses and the Layer 3 IP addresses. The request also identifies the source port number 1305 (i.e., dynamically generated by the host) and destination port, identifying the FTP services on port 21. The host also has requested a web page from the server using the same Layer 2 and Layer 3 addresses. However, it is using the source port number 1099 (i.e., dynamically generated by the host) and destination port identifying the web service on port 80.

The socket is used to identify the server and service being requested by the client. A client socket might look like this, with 1099 representing the source port number: 192.168.1.5:1099

The socket on a web server might be 192.168.1.7:80

Together, these two sockets combine to form a *socket pair*: 192.168.1.5:1099, 192.168.1.7:80

Sockets enable multiple processes, running on a client, to distinguish themselves from each other, and multiple connections to a server process to be distinguished from each other.

The source port number acts as a return address for the requesting application. The transport layer keeps track of this port and the application that initiated the request so that when a response is returned, it can be forwarded to the correct application.

14.4.3

## Port Number Groups

The Internet Assigned Numbers Authority (IANA) is the standards organization responsible for assigning various addressing standards, including the 16-bit port numbers. The 16 bits used to identify the source and destination port numbers provides a range of ports from 0 through 65535.

The IANA has divided the range of numbers into the following three port groups.

| Port Group | Number Range | Description |
|---|---|---|
| **Well-known Ports** | **0 to 1,023** | • These port numbers are reserved for common or popular services and applications such as web browsers, email clients, and remote access clients.<br>• Defined well-known ports for common server applications enables clients to easily identify the associated service required. |
| **Registered Ports** | **1,024 to 49,151** | • These port numbers are assigned by IANA to a requesting entity to use with specific processes or applications.<br>• These processes are primarily individual applications that a user has chosen to install, rather than common applications that would receive a well-known port number.<br>• For example, Cisco has registered port 1812 for its RADIUS server authentication process. |
| **Private** and/or **Dynamic Ports** | **49,152 to 65,535** | • These ports are also known as *ephemeral ports*.<br>• The client's OS usually assign port numbers dynamically when a connection to a service is initiated.<br>• The dynamic port is then used to identify the client application during communication. |

**Note**: Some client operating systems may use registered port numbers instead of dynamic port numbers for assigning source ports.

The table displays some common well-known port numbers and their associated applications.

### Well-Known Port Numbers

| Port Number | Protocol | Application |
|---|---|---|
| **20** | TCP | File Transfer Protocol (FTP) - Data |
| **21** | TCP | File Transfer Protocol (FTP) - Control |
| **22** | TCP | Secure Shell (SSH) |
| **23** | TCP | Telnet |
| **25** | TCP | Simple Mail Transfer Protocol (SMTP) |
| **53** | UDP, TCP | Domain Name System (DNS) |
| **67** | UDP | Dynamic Host Configuration Protocol (DHCP) - Server |
| **68** | UDP | Dynamic Host Configuration Protocol - Client |
| **69** | UDP | Trivial File Transfer Protocol (TFTP) |
| **80** | TCP | Hypertext Transfer Protocol (HTTP) |
| **110** | TCP | Post Office Protocol version 3 (POP3) |
| **143** | TCP | Internet Message Access Protocol (IMAP) |
| **161** | UDP | Simple Network Management Protocol (SNMP) |
| **443** | TCP | Hypertext Transfer Protocol Secure (HTTPS) |

Some applications may use both TCP and UDP. For example, DNS uses UDP when clients send requests to a DNS server. However, communication between two DNS servers always uses TCP.

Search the IANA website for port registry to view the full list of port numbers and associated applications.

14.4.4

## The netstat Command

Unexplained TCP connections can pose a major security threat. They can indicate that something or someone is connected to the local host. Sometimes it is necessary to know which active TCP connections are open and running on a networked host. Netstat is an important network utility that can be used to verify those connections. As shown below, enter the command **netstat** to list the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state.

```
C:\> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.124:3126     192.168.0.2:netbios-ssn  ESTABLISHED
  TCP    192.168.1.124:3158     207.138.126.152:http     ESTABLISHED
  TCP    192.168.1.124:3159     207.138.126.169:http     ESTABLISHED
  TCP    192.168.1.124:3160     207.138.126.169:http     ESTABLISHED
  TCP    192.168.1.124:3161     sc.msn.com:http          ESTABLISHED
  TCP    192.168.1.124:3166     www.cisco.com:http       ESTABLISHED
 (output omitted)
C:\>
```

By default, the **netstat** command will attempt to resolve IP addresses to domain names and port numbers to well-known applications. The **-n** option can be used to display IP addresses and port numbers in their numerical form.

14.4.5

## Check Your Understanding - Port Numbers

Check your understanding of port numbers by choosing the correct answer to the following questions.

1. Assume a host with IP address 10.1.1.10 wants to request web services from a server at 10.1.1.254. Which of the following would display the correct socket pair?

- 1099:10.1.1.10, 80:10.1.1.254
- 10.1.1.10:80, 10.1.1.254:1099
- **10.1.1.10:1099, 10.1.1.254:80**
- 80:10.1.1.10, 1099:10.1.1.254

2. Which port group includes port numbers for FTP, HTTP, and TFTP applications?

- dynamic ports
- private ports
- registered ports
- **well-known ports**

3. Which Windows command would display the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state?

- ipconfig /all
- ping
- **netstat**
- traceroute

Check | Show Me | Reset