Port numbers

Transport layer port numbers video

Web - 80

FTP - 21

Mail - 25

TCP and UDP port numbers

There are many services that we access through the internet in the course of a day.

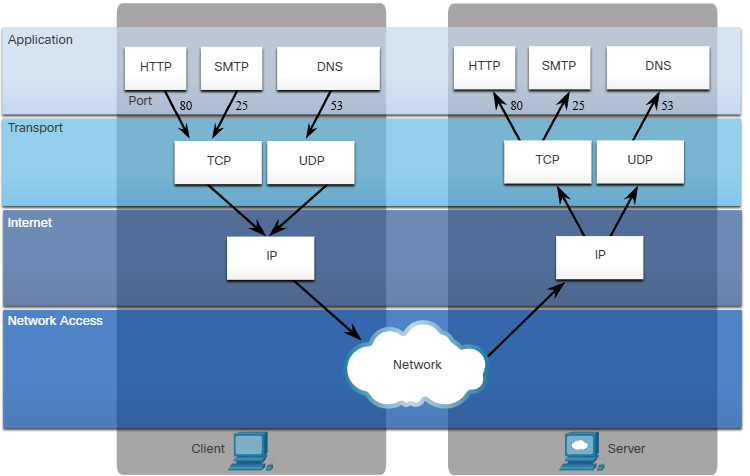
DNS, web, mail, FTP, IM and VoIP are just some of these services that are provided by client/server systems around the world.

These services may be provided by a single server or by several servers in large data center

**When a message is delivered using either TCP or UDP, the protocols and services requested are identified by a port number.**

**A port is a numeric identifier within each segment that is used to keep track of specific conversations between a client and server.**

**Every msg that a host sends contains both a source and destination port**



When a msg is received by a server, it is necessary for the server to be able to determine which service is being requested by the client.

Clients are preconfigured to use a destination port that is registered on the internet for each service.

An example of this is web browser clients which are preconfigured to send requests to web servers using port 80, the well-known port for HTTP web service

Ports are assigned and managed by an organization known as the internet corporation for assigned names and numbers (iCANN). ports are broken into three categories and range in number from 1 to 65 535:

Well-Known ports

- destination ports that are **associated with common network applications are identified as well-known ports**. These ports are in the range of **1 to 1023**

Registered ports

- ports **1024 to 49151** can be used as either source or destination ports.

These can be **used by organizations to register specific applications**

Private ports

- ports **49152 to 65535** are often used as source ports

These ports **can be used by any application**

Some of them are:

1. TCP file transfer protocol (FTP) - data
2. TCP FTP - control
3. TCP secure shell (SSH)
4. TCP telnet

25 TCP simple mail transfer protocol (SMTP)

53 UDP, TCP Domain name service (DNS)

67 UDP Dynamic host configuration protocol (DHCP) - server

68 UDP DHCP - client

69 UDP trivial file transfer protocol (TFTP)

80 TCP hypertext transfer protocol (HTTP)

1. TCP post office protocol version 3 (POP3)
2. TCP internet message access protocol (SNMP)
3. UDP simple network management protocol (SNMP)
4. 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

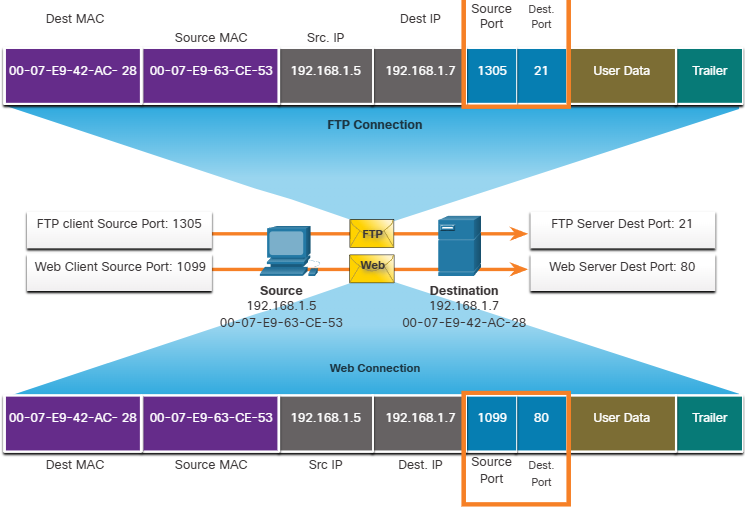
Socket pairs

- 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, 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 (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 later 2 and later 3 addresses.

However, it is using the source port number 1099 (-//-) 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.**

The netstat command

Unexplained TCP connections can pose a major security threat.

They can indicate that sometinh or smo 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.