RECAP/

TCP and UDP

UDP

- delivery system that does not require acknowledgment of receipt

- is preferable with applications such as streaming audio and VoIP

- some packets may be lost but it is usually not noticeable

TCP

- each packet has a sequence number

- TCP kkeeps track of the number of sengments that have been sent to a specific host from a specific application

- if the sender does not receive an acknowledgment within a certain period of time, it assumes that the segments were lost and retransmits them. Only the portion of the msg that is lost is resent.

Port numbers

When a msg is deliver using 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 detrmine 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.

Ports are assigned and managed by an organization known as the iCANN. Ports are broken into 3 categories in numbers from 1 to 65535

Well-known ports

1 to 1023

Registered ports

1024 to 49151

Used as either sourve or destination ports

Used by organizations to register specific applications such as IM apps

Private ports

49152 to 65535

Can be used by any application

The source port number is dynamically generated by the sending device to identify a conversation between 2 devices. This process allows multiple conversations to occur simultaneously. It is common for a device to send multiple HTTP service requests to a web server at the same time. Each separate HTTP conversation is tracked based on the source ports

The client places a destination port number in the segment to tell the destination server what sevice is being requested. A server can offer more than one sevice simultaneously, such as web services on port 80 at the same time that it offers FTP connection establishment on port 21

Unexplained TCP connections can pose a major security threat. They can indicate that smt or smo is connected to the local host. Sometimes it is necessart 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. The command netstat is used to list the protocols in use, local address and port number, the foreign address and port numbers, and the connection state.