COSCS340 Software Engineering
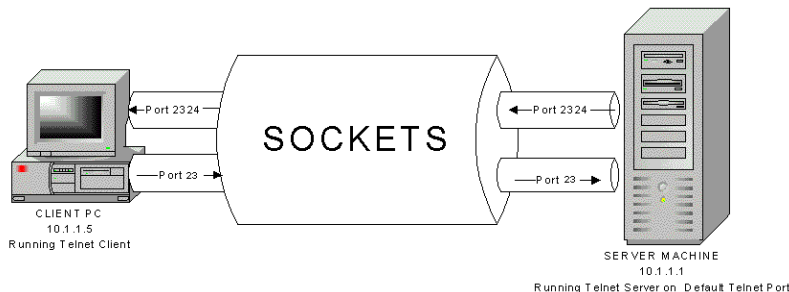
Audris Mockus\ University of Tennessee\
audris@utk.edu

TCP- the Transmission Control Protocol.

- ▸ TCP is a fundamental building block of the Internet.
- ▸ Built on top of IP, it is the transport mechanism for many application-level Internet protocols such as FTP, Telnet, HTTP, SMTP, POP, IMAP, and SSH.
- ▸ A TCP connection is a virtual, full-duplex circuit between two communicating parties, acting like a two-way pipe. Either side may write any number of bytes at any time to the pipe.

Sockets and Ports

- When a program establishes a TCP connection to a service, it needs two pieces of information: the IP address and port (service).

- The combination of an IP address and a port number (and protocol) is called a socket.

CLIENT PC
10.1.1.5
Running Telnet Client

Port 2324

SOCKETS

Port 23

Port 2324

Port 23

SERVER MACHINE
10.1.1.1
Running Telnet Server on Default Telnet Port

"Listening"

- In order for a connection attempt to a socket to succeed, something must be "listening" on that socket.
- If you've ever attempted a TCP connection and received the response "connection refused," it means that the remote machine is up and running, but nothing is listening on the target socket.

Standard Ports

- How does a client program know the target port number of a listening server?
  - Internet Assigned Numbers Authority or IANA,
  - See /etc/services
  - SSH uses port 22, and IMAP uses port 143.
  - Port numbers allow multiple services at the same IP address.

  - Once established, a TCP connection is completely determined by the combination of its source and target sockets. Therefore, multiple TCP clients may connect to the same target socket.

Firewalls

- ▸ You need a firewall, so that your computer (network) is not visible

on the Internet to the bad guys. These are bad guys who find computer ports and access your computer through one of them.
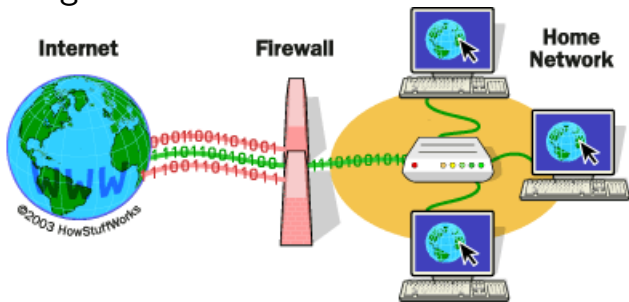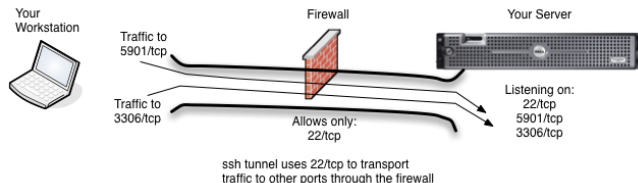
Firewalls can differentiate

- E.g., da1, da2, da3, da0 are behind firewall
  - different ports are open depending if you are
    - on one of da servers
    - in eecs domain
    - on UTK's nnetwork
    - off campus network
- most of the ports (if you are off campus) except for 90XX you use.

Tunnels

- Tunnel allows to by pass the firewall

Your Workstation — Firewall — Your Server

Traffic to 5901/tcp

Traffic to 3306/tcp

Allows only: 22/tcp

Listening on:
22/tcp
5901/tcp
3306/tcp

ssh tunnel uses 22/tcp to transport
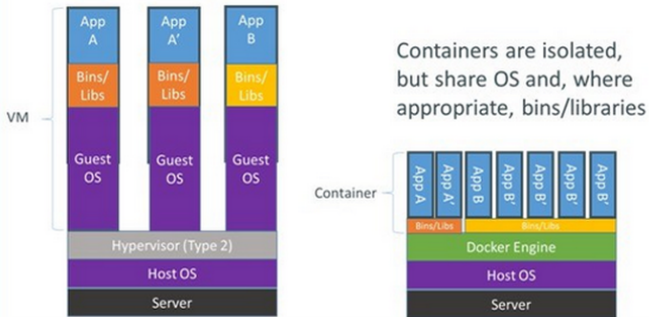traffic to other ports through the firewall

- Also, if we can only contact remote hosts on certain ports, the solution would be to contact remote hosts via allowed port and piggyback the connection on already established link.

- -L LocalPort:RemoteHost:RemotePort

Docker
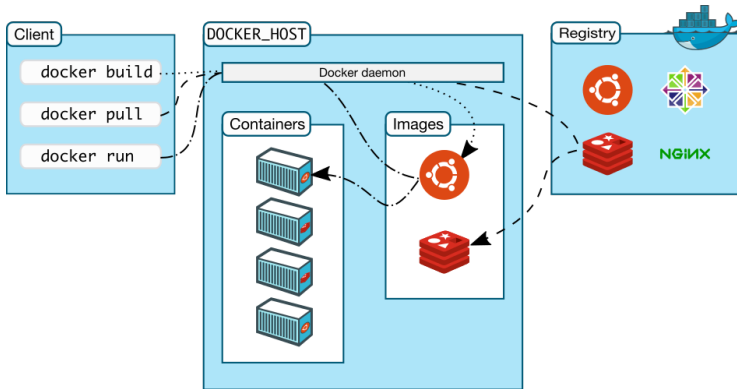
Docker containers

Docker images

- Each image consists of a series of layers. Docker makes use of union file systems to combine these layers into a single image. Union file systems allow files and directories of separate file systems, known as branches, to be transparently overlaid, forming a single coherent file system.