Network Security

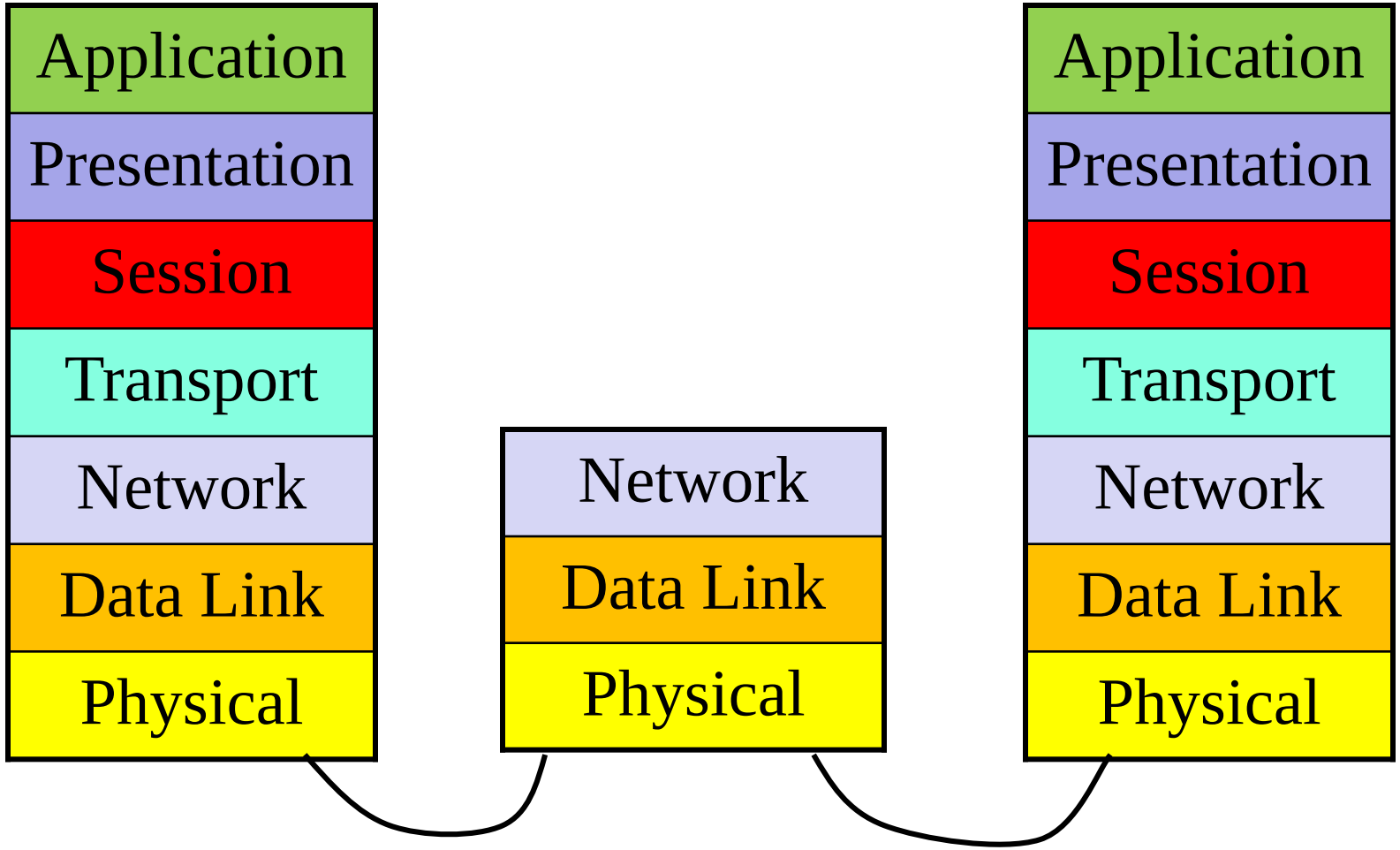
COMP620

“Cyber attacks rain down on us from many places. You have to make your systems secure and safe and teach your people cyber hygiene.”

Kersti Kaljulaid

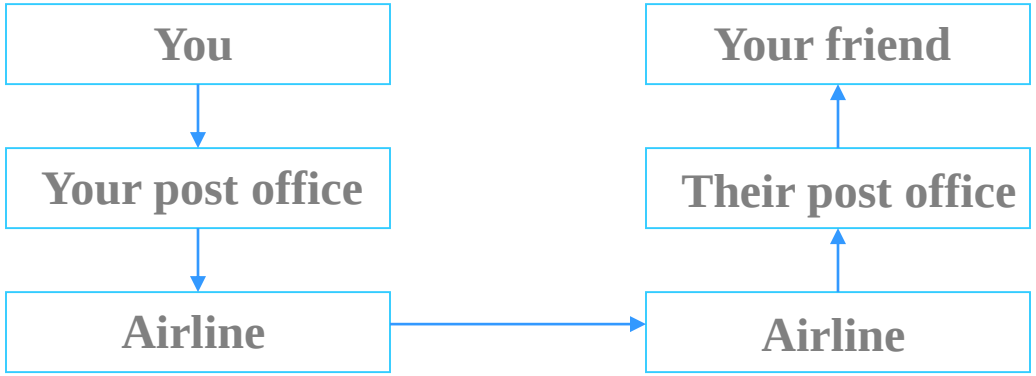
president of Estonia

Network Layers



OSI Analogy

Ex: U.S. Mail



- You do not have to worry about how to find your friends house in the distant city
- The post office does not need to know how to fly the airplane
- Each layer assumes that the layer below it will provide certain functions
- Each layer provides additional functionality

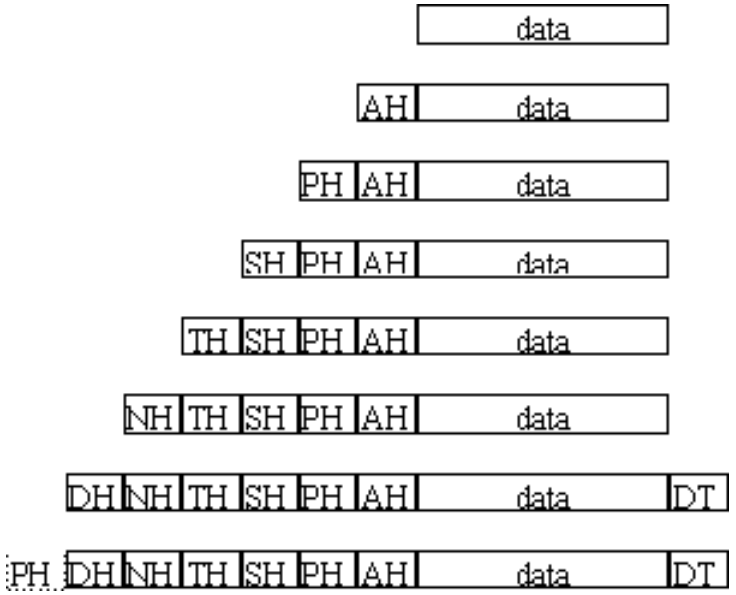
layer	purpose	example
Application	Provides network services.	X.400 email, HTTP, FTP
Presentation	Converts the data to the representation used by the local computer.	
Session	Establishes sessions.	
Transport	Directs packets to the correct user on a computer. This is the first end-to-end layer. May also provide error correction.	TCP UDP
Network	Finds a route for packets to take through the network.	Internet Protocol (IP)
Data link - logical data link	Detects and corrects any errors on the link. Provides flow control.	
- media access control	Determines which node may transmit.	Ethernet, Token Ring
Physical	Defines the characteristics of the physical connections. This is the only layer that actually sends bits to another computer.	SONET, RS-232C

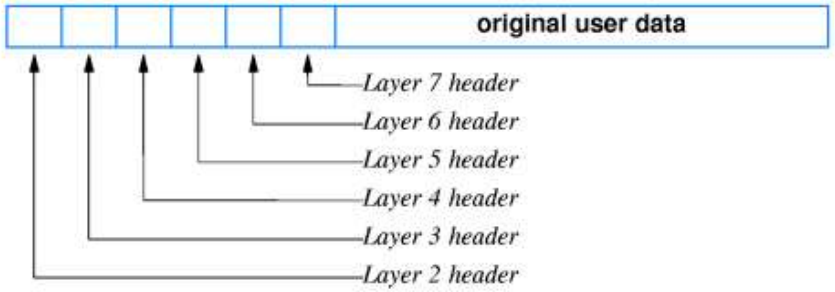
Internet Protocol Stack

- The Internet Protocol uses a similar, but slightly different model than OSI.
- The Internet Protocol does not define the lower levels.

layer	purpose	OSI equivalent	example
Application	Provides network services.	Application, Session and Presentation	HTTP, FTP, Telnet
Transport	Multiplexes data streams from different applications. May also provide error correction.	Transport	TCP, UDP
Internet	Routing.	Network	IP
Network Interface	Provides access to the Data Link The IP stack does not define the lower levels.	Data Link	Ethernet

Nested Protocol Headers





- The data link layer often adds a trailer to the packet that contains a cyclic redundancy check (CRC) to detect errors.
- It is the bottom frame, with all of the headers, that is actually sent across the network

Standard Packet

- Header contains destination address, maybe source address and other parameters.
- Data bytes are sent without start, stop or parity bits. Only the data is sent.
- Trailer contains error checking values.

Ethernet frame format

Preamble	Destination	Source	type	data	CRC
8	6	6	2	46 - 1500	4

Media

- Fiber optic cables
- Wires
- Infrared
- Radio
- Satellite

sorted by security

Network Identifiers

Computers on the Internet are referred to as hosts. Each host as at least three identifiers:

- **Internet name** for humans to use
  (e.g. williams.comp.ncat.edu)
- **Internet address**, a 32 bit binary number written in decimal as four bytes (e.g.152.8.110.47)
- **hardware address**, such as an Ethernet address
  (e.g. 00-e0-63-03-76-c0)

Internet Names

- Hierarchical starting from the right

  `host.subnet.organization.type`

- Rightmost identifies the type or organization or country
  - edu, com, mil, org, net
  - us, ca, de, uk
  - .top, .loan, .xyz, .club, .online, .vip, .site, .ltd, .win, .work

Internet Addresses

- Internet Names map to Internet Addresses
- An Internet Address is composed of two parts, a netid and a hostid
- The hostid identifies the particular host on a network
- The netid identifies the network where the host is connected
- A computer physically connected to two networks needs two Internet addresses

Internet Address Classes

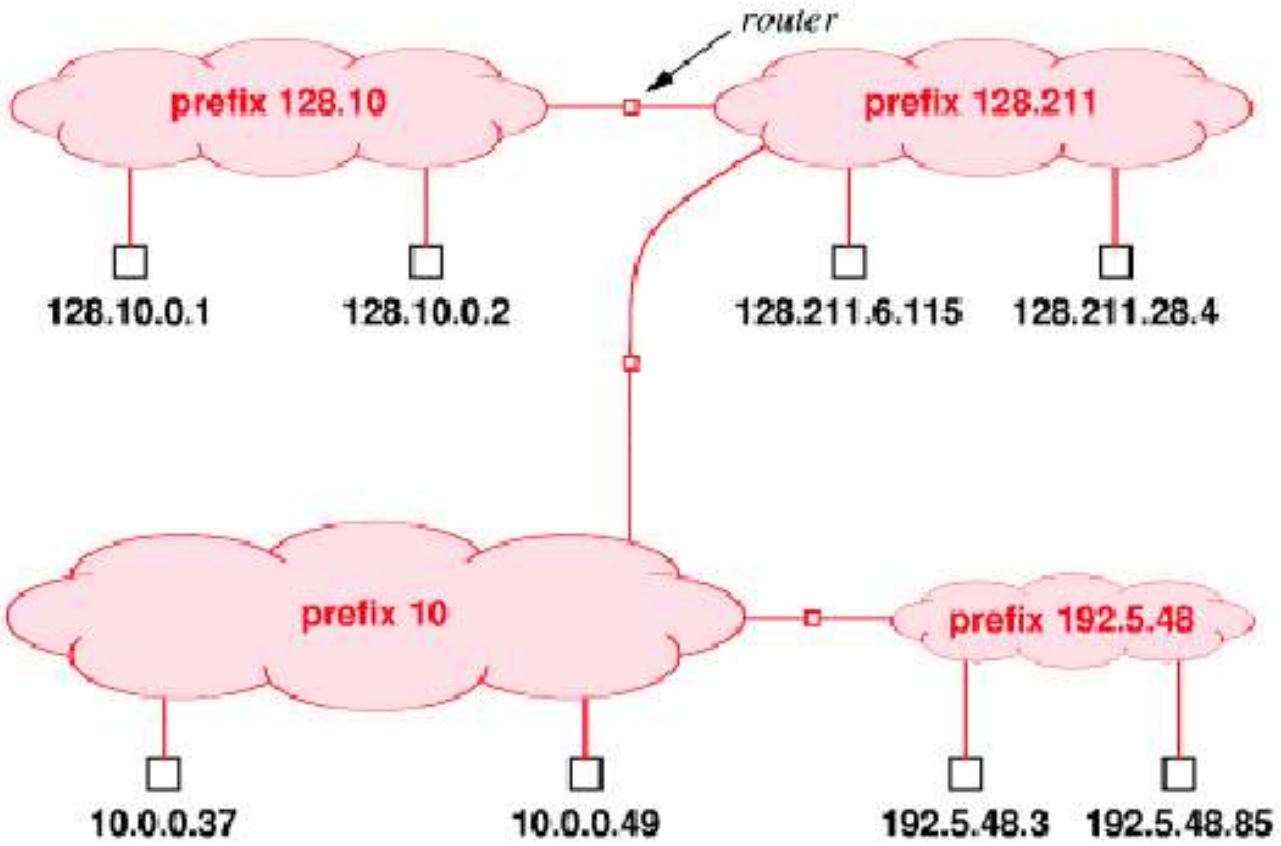
class				
A	NetID	hostID	hostID	hostID
B	NetID	NetID	hostID	hostID
C	NetID	NetID	NetID	hostID

CIDR addresses

- The division between NetID and HostID can be expressed explicitly using the Classless Inter-Domain Routing (CIDR) notation.
- IP addresses can be written in the usual dotted notation followed by a slash and the number of bits to be used for the NetID.

152.8.108.138/22

IP Assignment Address Example



All hosts connected to a network have the same Internet address prefix.

Mapping Between Addresses

- Humans use Internet Names. The hardware uses the MAC addresses
- Internet Names are converted to Internet Addresses by a Domain Name Server (DNS)
- Internet Addresses are converted to MAC addresses by using the Address Resolution Protocol (ARP)

Domain Name Servers

- Domain Name Servers (DNS) map Internet Names to Internet Addresses
- A DNS maintains a distributed database of names and addresses
- Computers can send a request to a DNS to get the IP address of a computer
- Hosts and DNS cache addresses they have found

DNS Vulnerabilities

- The original Domain Name System did not specify any security
- It was possible to send fraudulent information to the DNS
- Clients requesting the IP address of www.acme.com might be given the address of badguys.com
- A DNS server can be overwhelmed by a DOS attack

Domain Name System Security Extensions

- DNSSEC was first deployed at the root level in July 2010
- It had to be backward compatible so a world of users would continue to run
- Information one DNS sends to another is digitally signed
- Google Public DNS is a freely provided, public DNS service, fully supporting DNSSEC

Address Resolution Protocol (ARP)

- Used by a computer to find the MAC or physical address of another computer on the **same** network
- To find a MAC address, ARP broadcasts a request containing the desired IP address to all computers on its local network
- All computers receive the ARP request and compare the requested address to theirs
- Only if the address matches, does the computer send a response back to the source

IP Routing

- If a host has the IP name of the destination but does not know the IP address, it must send a request to the DNS
- If a host does not know the MAC address of a destination computer on it’s local network, it must use ARP to find the address

Local Routing Decision

- When sending an IP datagram, the source computer must decide if it can send the packet directly to the destination on the local network or if it must send the packet to a router or gateway.
- Each host must be aware of the address of its local DNS and default gateway.

Local Destinations

- If the NetID of the destination's IP address is the same as the NetID of the source's IP address, then the destination is in the same Internet domain
- The frame can be sent directly to the destination
- ARP may be needed to find the destination's MAC address

Global Destinations

- If the NetID of the destination's IP address is different from the NetID of the source's IP address, then the destination is in another Internet domain
- The frame must be sent to a gateway
- ARP may be needed to find the gateway's MAC address
- The IP destination address will be the IP address of the final destination

Routing Security

- If the DNS *(or a DNS look alike)* returns a false IP address for a name, the computer will route packets to the false destination
- ARP broadcasts packets to all local computers. A malicious system could respond with false data.

ARP Poisoning

- All computers keep a cache of the MAC addresses they have received via ARP
- The cache is updated when new ARP packets are received
- An attacker can send fraudulent ARP messages to a victim
- A victim might send a packet to the wrong MAC address

Possible Assignment

- Write four questions that are suitable for the next COMP620 exam
  - Not too hard, not too easy
  - Does not require you to memorize trivial information
- Should be an easy way to get more points
- Should be an easy way for the instructor to write the exam
- Exam 3 is on Monday, November 19, before Thanksgiving

DHCP

- The **D**ynamic **H**ost **C**onfiguration **P**rotocol provides IP configuration information for computers when they are booted.
- When DHCP is used, you do not have to configure the IP address and other information when you install TCP/IP on a computer.

Source of Information

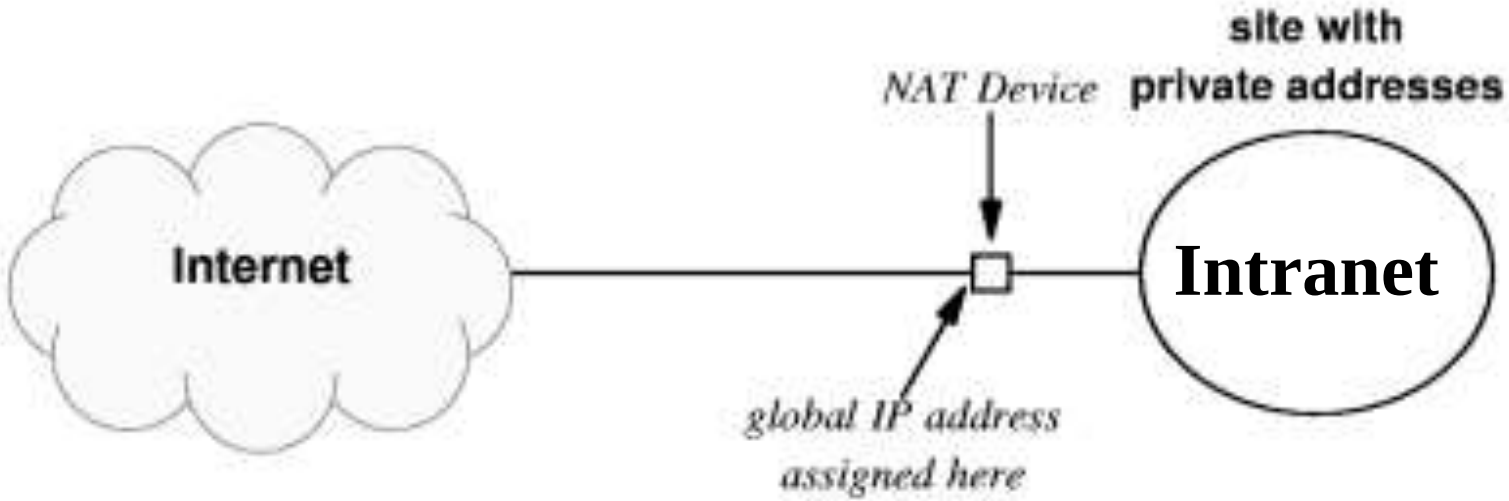
A computer learns

- Its own address from DHCP
- Its local gateway from DHCP or router
- The address of remote systems from DNS
- The hardware address of local systems from ARP

- Each of these can be an attack opportunity

Network Address Translation (NAT)

- A NAT router sits between the Internet and a private network.



Changing Addresses

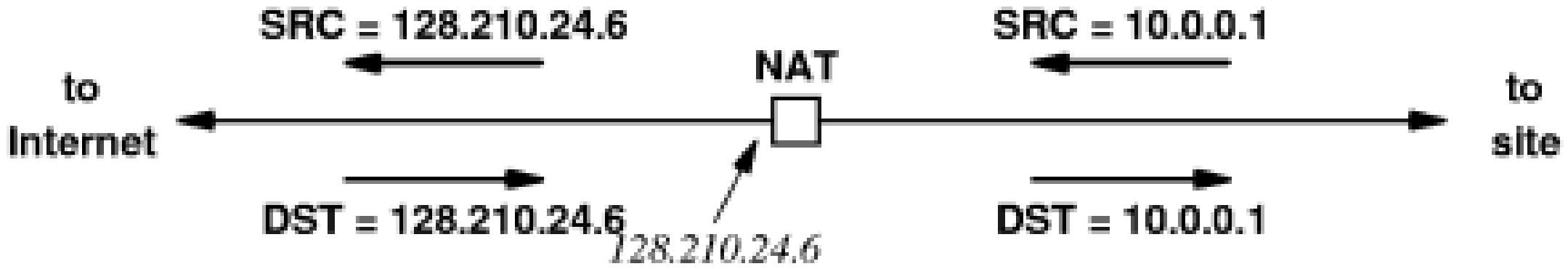
- The NAT router has a single internet address. This is the address that the rest of the world sees.
- Computers within the private intranet have addresses that are never used outside of the private intranet

Mapping Addresses and Ports

- When a computer within the private intranet creates a connection to an Internet site, the NAT router changes the address and port
- The packet on the Internet has the NAT routers IP address as the source
- The NAT keeps a table mapping the Internet addresses and ports to private address and ports

Translation

- The only address seen on the Internet is the NAT router's IP address. Remote systems do not know this is a translated address



Multiple Computer Mapping

- What happens if two computer on the private intranet want to connect to the same Internet host?
- The NAT router will change the port numbers that appear on the Internet
- The NAT mapping tables include the port number and the remote Internet address

Mapping Example

- Imagine two computer, 10.0.0.1 and 10.0.0.2 use port 30000 to connect to the same web server at 128.10.19.20

NAT mapping table

Direction	Fields	Old Value	New Value
out	IP SRC:TCP SRC	10.0.0.1:30000	128.10.19.20:40001
out	IP SRC:TCP SRC	10.0.0.2:30000	128.10.19.20:40002
in	IP DEST:TCP DEST	128.10.19.20:40001	10.0.0.1:30000
in	IP DEST:TCP DEST	128.10.19.20:40002	10.0.0.2:30000

Home Products Available

TCP/IP

- TCP operates on top of the Internet Protocol, a connectionless, unreliable network.
- TCP provides a connection oriented transport that corrects lost packets, corrupted packets, out-of-order packets and delayed packets.
- IP gets packets to the correct computer. TCP gets packets to the correct application

TCP and UDP

TCP	UDP
Connection Oriented	Connectionless
Complete reliability corrects lost, corrupted and out-of-order packets	best effort delivery
Full Duplex communication	Full Duplex communication
Point to Point communication	Point to Point, 1 to many, many to 1, many to many
Stream Interface	Message Oriented
Reliable connection startup	no connection

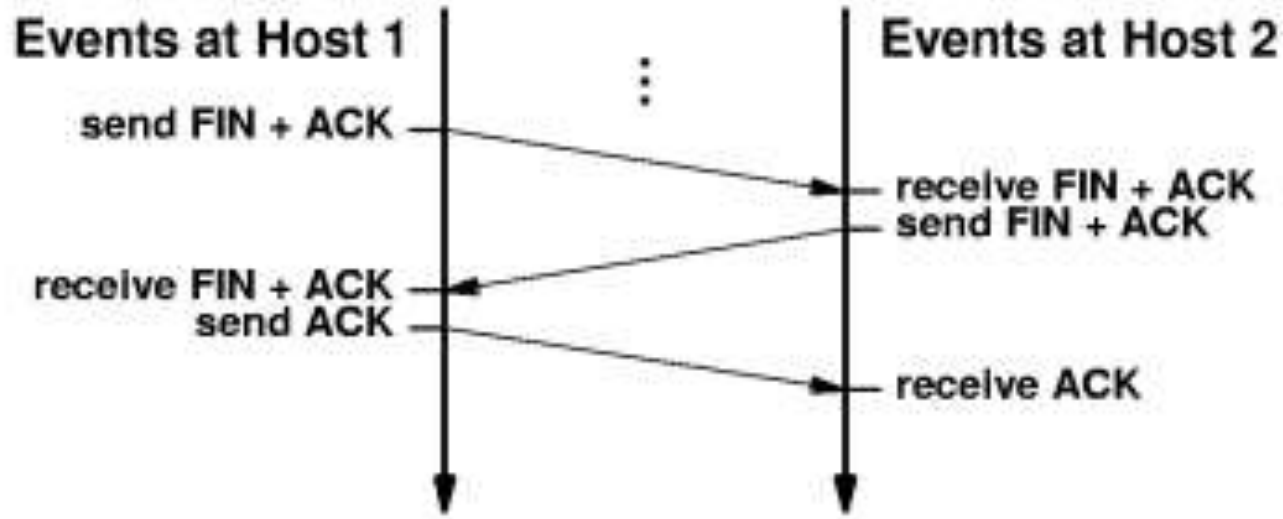
Popular TCP Applications

- HTTP - web protocol
- telnet - terminal protocol
- ftp - file transfer protocol
- any program that has lengthy transfers that require reliability.

Popular UDP Applications

- DNS requests
- WINS requests
- Streaming Audio
- Any application that needs to send a short amount of data that can be resent if necessary *(idempotent or at-least-once).*
- Time critical applications

Creating a Connection *(or not)*



- It takes three messages to create a connection.
- A well known Denial of Service attack starts many connection requests without completing them

Distributed Denial of Service

- A computer can send a request to a server with an incorrect source address
- If computer A sends a request to computer B with a fraudulent source of computer C, B will respond to C
- If computer A broadcasts a request to all computer on the network with a source address of C, they will all respond to C
- An attacker can easily make many computers send lots of data to a victim

Amplification

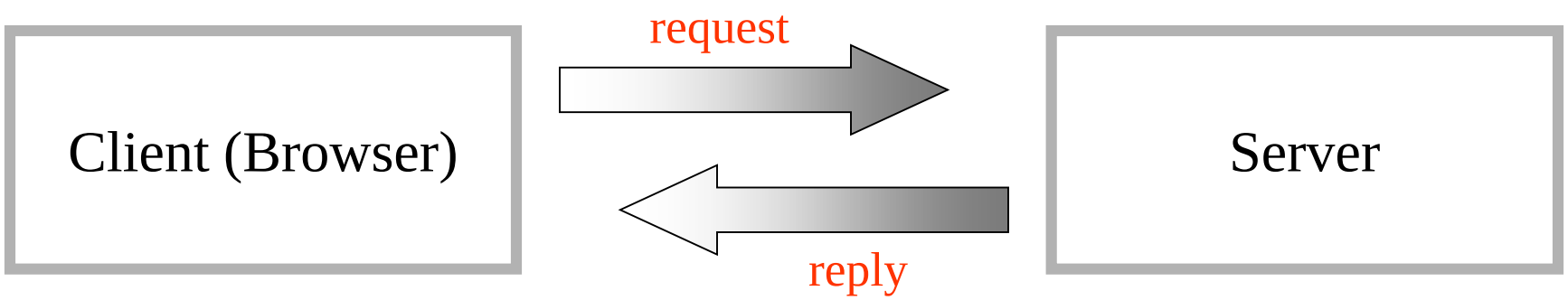
- Amplification attacks are used to magnify the bandwidth that is sent to a victim
- Some services send a response that is much larger than the request
- A large collection of compromised computers can reflect their attacks through servers that will amplify the attack

Hyper-Text Transfer Protocol

- Hyper-Text Transfer Protocol is the main request-response (client-server) protocol used to transfer web documents.
- HTTP is an application layer protocol using TCP.
- Other high level protocols for the Web include FTP and Telnet.

Web Document Transfer & HTTP

- When a browser interacts with a Web server, the two programs follow the Hyper-Text Transfer Protocol.
- HTTP allows a browser to request a specific item, which the server then returns.



HTTP Request Format

The protocol sends requests and responses in ASCII characters that can easily be read. The request is always terminated by a blank line. The format of the request sent by a client browser (such as Mozilla or Internet Explorer) to a web server is:

***Method filename* HTTP/1.1**

options *CRLF CRLF*

Example HTML **GET**

```
GET /mypage.html HTTP/1.1↵
HOST: williams.comp.ncat.edu↵↵
```

- This example requests the server to send the web page, mypage.html, to the client's browser. The browser has indicated that it is using version 1.1 of the protocol. Note that the request is terminated by two end of line characters(↵↵).

HTTP Methods

GET	Get a file from the server.
HEAD	Get information about a file from the server.
POST	Send information to the server.
PUT	Send a file to be stored on the server.
DELETE	Delete a file on the server.
OPTIONS	Request the available server options.
TRACE	Invoke a loop-back of the request message

Server Response

- The server responds with a status line, including the message's protocol version and a success or error code and possibly message content.

```
HTTP/1.1 statuscode reason↵
response options↵↵

 file contents
```

Response Example

```
HTTP/1.1 200 OK
Date: Sun, 26 Nov 2000 23:48:00 GMT
Server: Apache/1.3.6 (Win32)
Last-Modified: 17 Nov 2000 12:51:44
Content-Length: 4683
Connection: close
Content-Type: text/html
<html>
<head> etc.
```