Network Review

Goal

- Understand the basics of how the Internet works
- Be mindful of the security threats

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

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

### Internet Protocol Stack

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

<table>
<thead>
<tr>
<th>Layer</th>
<th>Purpose</th>
<th>OSI Equivalent</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Provides network services.</td>
<td>Application, Session and Presentation</td>
<td>HTTP, FTP, Telnet</td>
</tr>
<tr>
<td>Transport</td>
<td>Multiplexes data streams from different applications. May also provide error correction.</td>
<td>Transport TCP, UDP</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td>Routing.</td>
<td>Network IP</td>
<td>IP</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Provides access to the Data Link</td>
<td>Data Link Ethernet</td>
<td></td>
</tr>
</tbody>
</table>

### Nested Protocol Headers

- The data link layer often adds a trailer to the packet that contains a cyclic redundancy check (CRC) to detect errors.
- The physical layer might, or might not, append a header or trailer to the packet.
- It is the bottom frame, with all of the headers, that is actually sent across the network. When it is received at the other end, the headers are stripped off as the packet is passed up the stack to the user application.

### 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

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination</th>
<th>Source</th>
<th>type</th>
<th>data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>46-1901</td>
<td>4</td>
</tr>
</tbody>
</table>

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
  (i.e. williams.comp.ncat.edu)
- **Internet address**, a 32 bit binary number written in decimal as four bytes
  (i.e. 152.8.110.47)
- **hardware address**, such as an Ethernet address
  (i.e. 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
Internet Addresses

- Internet Addresses map to Internet Names.
- 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

<table>
<thead>
<tr>
<th>class</th>
<th>NetID</th>
<th>hostID</th>
<th>hostID</th>
<th>hostID</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>NetID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>NetID</td>
<td>NetID</td>
<td>NetID</td>
<td>hostID</td>
</tr>
</tbody>
</table>

IP Addressing Classes

- The five classes of IP addresses in the classful scheme. The address assigned to a host is either class A, B, or C; the prefix identifies a network, and the suffix is unique to a host on that network.

<table>
<thead>
<tr>
<th>class</th>
<th>prefix</th>
<th>suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>1[0]</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>1[1][0]</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>1[1][1]</td>
<td>multicast address</td>
</tr>
<tr>
<td>E</td>
<td>1[1][1]</td>
<td>reserved for future use</td>
</tr>
</tbody>
</table>

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.

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 its 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.

DHCP

- The Dynamic Host Configuration Protocol 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.

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.
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

<table>
<thead>
<tr>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Oriented</td>
<td>Connectionless</td>
</tr>
<tr>
<td>Complete reliability</td>
<td>best effort delivery</td>
</tr>
<tr>
<td>corrects lost, corrupted</td>
<td></td>
</tr>
<tr>
<td>and out-of-order packets</td>
<td></td>
</tr>
<tr>
<td>Full Duplex communication</td>
<td>Full Duplex communication</td>
</tr>
<tr>
<td>Point to Point communication</td>
<td>Point to Point, 1 to many, many to 1, many to many</td>
</tr>
<tr>
<td>Stream Interface</td>
<td>Message Oriented</td>
</tr>
<tr>
<td>Reliable connection startup</td>
<td>no connection</td>
</tr>
</tbody>
</table>

Creating a Connection

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

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 CRLFCRLF
```

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 (\r\n).

HTTP Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>Get a file from the server.</td>
</tr>
<tr>
<td>HEAD</td>
<td>Get information about a file from the server.</td>
</tr>
<tr>
<td>POST</td>
<td>Send information to the server.</td>
</tr>
<tr>
<td>PUT</td>
<td>Send a file to be stored on the server.</td>
</tr>
<tr>
<td>DELETE</td>
<td>Delete a file on the server.</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Request the available server options.</td>
</tr>
<tr>
<td>TRACE</td>
<td>Invoke a loop-back of the request message</td>
</tr>
</tbody>
</table>
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.