Homework 1 (April 10, 2013)

Jason Dreisbach

1. Read Chapter 1

Okie Dokie

2. OSI Network Model

The 7 Layer Model

1. Physical

The physical layer provides the actual transmission of data to the wire. It handles reading and writing data to the wire on the bit level.

2. Data Link

The data link layer provides the physical addressing of devices on the network. This is often associated with the hardware MAC address.

3. Network

The network layer provides the routing information for packet forwarding through multiple routers. It is the logical address of the device with respect to the network.

4. Transport

The transport layer provides the protocol for which the bits will be transmitted to the intended target machines. For example, TCP and UDP are transport protocols that designate different behavior when transmitting the application data.

5. Session

The session layer handles connection management. It will automatically try to provide live connections when the an application needs them.

6. Presentation

The presentation layer dictates how application data is serialized to be sent across the network. For example, protocol buffers are a possible presentation layer.

7. Application

The application layer is responsible for deserializing and displaying the information to the user in an acceptable format.

3. RFC's

a. What is an RFC?

A request for comment (RFC) is a document published to describe methods, behavior, or research.

b. Who can write an RFC?

Anyone can submit an independent internet draft of an RFC for review by a RFC editor. Once it is reviewed and approved it may be published.

c. RFC 1541

- **Purpose:** The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network
- **Date:** October 1993
- **Author:** R. Droms

d. RFC 2104

- **Purpose:** HMAC: Keyed-Hashing for Message Authentication
- **Date:** February 1997
- **Author:** H. Krawczyk, M. Bellare, R. Canetti

e. RFC 5246

- **Purpose:** The Transport Layer Security (TLS) Protocol
- **Date:** August 2008
- **Author:** T. Dierks, E. Rescorla

4. IETF

a. What is IETF?

The Internet Engineering Task Force (IETF) develops and promotes internet standards.

b. How do you become a member?

There is no membership. It is an open group. You must only participate.

c. The 6man IETF group

5. IANA

a. What's IANA stand for?

Internet Assigned Numbers Authority

b. What does it do?

IANA manages the IP addresses and domain names in the DNS root zone.

c. What are these ports?

- **22:** SSH
- **23:** Telnet
- **53:** UDP
- **80:** HTTP

d. What are these protocol numbers?

A protocol number defines the communication standard that the transmission is using. So it is possible to use a nonstandard port for communication. *

4: IPv4 * **6:** TCP * **17:** UDP

6. DHCP

a. What does DHCP stand for?

Dynamic Host Configuration Protocol

b. DHCP does what?

DHCP does the initial configuration of a host to allow for proper IP communications to occur over a LAN.

c. Process

- **Discovery:** The discover packet is sent out by a machine to discover the DHCP servers on the LAN
- **Offer:** The DHCP responds with an available IP for the machine to take.
- **Request:** The machine accepts the address from the server.
- **Acknowledgment:** The server then acknowledges that the machine has secured the address.

7. ARP

a. What does it stand for?

Address Resolution Protocol

b. What's its purpose?

ARP facilitates translating between network layer and link layer addresses.

c. How does it work?

The ARP protocol creates a table that maps the hardware address of a machine it its network address. It then is used to translate the values in the table when queried by the machine.

e. ARPing on subnet or off, what's the difference?

When the other device is off the LAN ARP does not cache the actual hardware address of the other device. Instead it caches the hardware address of the first intermediate device it reaches on the path to the intended target device.

d. Security Issues

ARP is susceptible to cache poisoning attacks which can lead to a man in the middle attack.

8. P2P vs Client Server

a. Read 2.1.1 and 2.6

b. What's the difference?

A P2P network may make equal transactions between the two peers where the client and server model requires all of the transactions to be initiated by the client.