Experiment 2:

Lower Layers Protocols / Broadcast Protocols

References

- Andrew S. Tanenbaum: Computer Networks
- RFC0768: UDP - User Datagram Protocol
- RFC0783 / RFC1350: TFTP - Trivial File Transfer Protocol
- RFC0791: IP - Internet Protocol
- RFC0951: BOOTP - Bootstrap Protocol
- RFC1034 / RFC1035: DNS - Domain Name System
- RFC2131: DHCP - Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- Preboot Execution Environment (PXE) Specification, Version 2.1
ftp://download.intel.com/labs/manage/wfm/download/pxespec.pdf
http://www.pix.net/software/pxeboot/archive/pxespec.pdf)

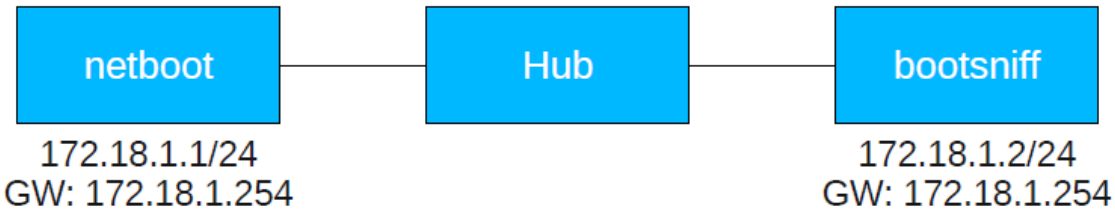
Preparatory Questions

1. What is the hierarchy of DNS?
2. Are the IP addresses distributed in a hierarchical way?
3. What are the most important DNS record types?
4. What does authoritative and non-authoritative reply mean?
5. What does `Leasing' mean?
6. How does BOOTP function?
7. What problem did the original BOOTP version have?
8. Explain the meaning of the following packets:
   DHCP-DISCOVER, DHCP-OFFER, DHCP-REQUEST, DHCP-ACK, DHCP-NACK, DHCP-DECLINE and DHCP-RELEASE
9. What is the purpose of DHCP relay agent?
10. What is TFTP and how does it function?
11. What is PXE (Preboot Execution Environment)?
12. How does the process of boot run when using PXE ?

Experiment Setup

This experiment consists of two computers connected on a hub, so that each of them can sniff the traffic of the other computer. These two computers are:

- bootsniff
- netboot



To start the experiment: open a terminal and type: "./run_exp2.sh"

Experiment Procedure

Part 1: Domain Name Service (DNS)

1. Start wireshark on 'bootsniff'
   - The command for starting wireshark is '*sudo wireshark &*'

2. Ping met.guc.edu.eg. Record the network traffic and describe the process of name resolving.

3. Answer the following questions:
   - What type of record is requested?
   - What information is sent back by the DNS server/s?

4. Now we will take a look on the hierarchical structure of DNS. With the tool dig you can query any DNS server.
   - Login in to the remote shell '*ssh gucstud@sdf.lonestar.org*' and enter the password: HelloGUC
   - To use dig type dig <queried domain>
   - Query the root name server about the next hierarchical stage(for Egypt's domains its "eg")
   - Now query for the domain "edu.eg"
   - Finally query for the domain "guc.edu.eg"

5. Answer the following questions:
   - What was the reply in each query? Attach snapshots with your answers
   - Are they all the same?

6. Dig any domain for their mail servers e.g. yahoo.com or google.com
   - check the manual of dig for that by typing man dig

7. Get the authoritative servers of any domain and try to make a query from the server itself.
   - Again open the manual for that purpose.

8. Answer the following questions:
   - Which of all the previous queries were authoritative replies and which were not?
   - What was the statement used to query an authoritative server for its domain?

9. Now you are going to make a reverse query i.e. typing an IP and get its domain name.
   - Find the domain of the IP address 196.204.161.5

10. Answer the following questions and attach a snapshot
    - What was the parameter given to dig to make the reverse query?
    - What was the type of DNS record queried?
    - What was the domain of the IP?

Part 2: PC (Diskless Client) boot via DHCP/TFTP

In this part, the PC netboot will boot from the network. Bootsniff will act as a DHCP server a TFTP server for the boot process.

1. Stop the capture process in wireshark and restart the process

2. Set the packets filter to 'bootp or tftp'

3. We have to make sure that the DHCP and TFTP services are running successfully on 'bootsniff'
    a. *sudo service isc-dhcp-server restart*
    b. *sudo service tftpd-hpa restart*

4. Boot netboot from the network by restarting it and pressing F12

5. When the Splash screen appears, press 'L' for LAN

6. Answer the following questions:
    - What transport layer protocol is used under TFTP? What problem may arise because of this? How is this problem solved?
    - Which files are transmitted via TFTP? What are these files required for?
    - What is the role of the detected protocols in the network booting process?