Laboratory Assignment 2
Network Sniffing

April 21, 2008

1 Purpose

In this laboratory assignment,

- You will learn how to use network protocol analyzer to capture, interpret, and store network packets.
- You will get to know – what's on the network: an overview of some of the common protocols.
- You will use Wireshark (the latest version of ethereal), which are open sources and have equivalent linux and windows versions. If you work with workstation at room D512, you will have Wireshark already installed. If you work with your own laptop or PC, you are recommended to download and install Wireshark 1.0 at http://www.wireshark.org.
- You will be asked to build sample traces containing working examples of several different protocols and then discuss them in some detail.

2 Preparations

Recommended reading is specified as below.

1. The 7 layers of OSI
   (http://en.wikipedia.org/wiki/OSI_model)
2. Wireshark
   (http://www.wireshark.org, http://wiki.wireshark.org)
3. Ethereal
   (http://www.ethereal.com)
4. Packet Sniffing
   (http://www.sans.org/reading_room/whitepapers/networkdevs/244.php)

3 Reporting

To pass this assignment you have to send an email to your teacher at yan.wang@hh.se. The email should contain a report(1-3 pages) with at least the following items:

1. **Your names and IDs**.
2. **Introduction** giving an overview of the assignment and content of the report.
3. **Sample traces** providing traces which contain some important basic information of protocols and applications, and discuss them briefly by completing tasks listed in **Section Exercise**. The protocols include: ARP, TCP/IP, HTTP. The application maybe be more interesting: DNS and MSN messenger service.
4. **Conclusions** containing your reflections about the network sniffing problem and the assignment.

Out of the report — You have to answer the questions and do demonstrations to your teacher (*Please go to next Section for questions*) during the lab!

4 Questions

The following questions or demonstrations are supposed to be shown to your teacher during the lab.

1. Where is the packet list pane? Where is the packet details pane? Where is packet bytes pane?
2. Where can you find the highest-layer protocol that each packet contains?
3. Can you find the stack correlation from the packets panes?
4. Set a capture filter and a display filter which are semantically same but used during capture and after capture respectively. For example, ip.addr == 68.242.106.5.

5 Staring Wireshark

Start Wireshark from **All Progroms**. Launch the capture option screen (Capture – Options ... or Ctrl-K). This dialog allows you to select the network interface on which to listen, to specify capture filters, to enable name resolution (DNS).

You can find almost all the useful information about how to use Wireshark in Wireshark User's Guide (http://www.wireshark.org/docs/wsug_html_chunked/). You can go to **Chapter 4.3 Start Capturing**, **Chapter 4.8 Filtering while capturing**.

6 Exercise

We will not go into great detail about the design of each individual protocol; instead, you are welcome to learn by yourselves according to the associated RFC number for each. RFC is stand for ***R**equest **F**or **C**omments*, is the official document that defines the implementation standards for protocols in the TCP/IP stack. You can search for RFC documentation at the RFC Editor home page, http://www.rfc-editor.org.

The TCP/IP protocol suit is what we are going to look at. It is a stack of protocols for real use, consisting of several different protocols on both Layers 3 and 4 of the OSI model. These protocols include TCP, IP, ARP, DHCP, ICMP, and many others.

6.1 ARP

We start with one of the simpler protocols — Address Resolution Protocol (ARP), requiring only a few packets to complete its entire operation. ARP (RFC 826) is used to translate Layer 3 (IP) addresses into Layer 2 (MAC) addresses, thus allowing devices (such as switches and routers) to determine where other devices are located on each port.

When a computer wants to transmit data to another computer, it must first know where that computer is. This is done with the aid of the switch or router connecting the two computers and the ARP protocol. For example, if u want to locate a file on your remote disk H:, you have to know the the MAC address of the server. It is done by

1. The source computer(your computer) sends an ARP broadcast(**Packet 1**) as *who has 194.47.19.100?....*
2. The destination computers ARP response to the **Packet 1** by **Packet 2** as *194.47.19.100 is at 00:44:22:d3:10:a1.*

- **Your task 1**: List sample packets for **Packet 1** and **Packet 2** individually.
- **Your task 2**: What is the IP address and Ethernet address of your destination computer?

6.2 TCP/IP

Transmission Control Protocol (TCP, RFC 793) is a Layer 4 protocol that is commonly used because it provides an efficient method of transparent, reliable, and bi-directional communication between devices. Bi-directional communication means that data can be transmitted and received simultaneously from a single host. Internet Protocol (IP, RFC 791) is the Layer 3 protocol that provides the addressing system that allows communication on a network. IP is a connectionless protocol, which means that it requires the functionality of

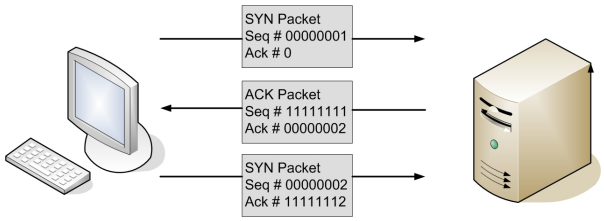

Figure 1: The Steps Handshake

TCP bundled with it to ensure the reliability of transmitted data. For exaple, the traffic in the capture file would begin with the establishment of a TCP/IP session, followed by the request and transmission of HTTP data and the termination of the session. Stepping through this simple communication between client and server is going to help us in understanding how TCP and IP work. It takes a three-step process to establish a connection between two computers in TCP, which is called *TCP handshake*.

1. **SYN** First of all, the client sends a SYN packet to the server(**Packet 1**). The SYN packet carries with it a 32-bit sequence number, located in the header of a TCP packet.

2. **SYN/ACK** And then, the server the responses, once it receives the initial SYN packet from the client. It reads the packets sequence number and uses that number in the packet it returns. The response packet is called a SYN/ACK packet(**Packet 2**).

3. **Final ACK** Finally, the client sends an ACK packet(**Packet 3**) to the server. This packet tells the server that the client received its SYN/ACK packet. As with step two of the process, the sequence number is incremented by one and sent as an acknowledgment number to the server.

- **Your task**: capture and list sample packets of **Packets 1 to 3** for the TCP handshake.

Once this last ACK packet is received, communication session is established and communication can begin.

6.3 HTTP

Hypertext Transfer Protocol (HTTP, RFC 2616) is the server/clientbased protocol used to request and transmission of the web page. Every time you check information by using windows internet explorer, foxnet, etc, you are transferring data via TCP/IP using HTTP.

To get a web page from web server,

1. First, the client(your computer) send a HTTP packet(**Packet 1**) to the server(it would be any web server, such as www.google.se) to ask transmitting a web page. The packet invokes a **GET** command, which means the request method is **GET**

2. The server lets the client know the request was valid by sending an HTTP OK message(**Packet 2**) before transmitting the data. After that, the data transmitting can be started.

When there is no more data to be sent over an established connection, the connection can be terminated using FIN and ACK packets. If your are intereted in it, you are welcome to capture the packets.

- **Your task 1**: List sample packets of **Packets 1** and **Packet 2**.
- **Your task 2**: Point out the host address and **Get** command in the **Packet 1**.
- **Your task 3**: Point out the **Ok** message in the **Packet 2**.

6.4 DNS

The Domain Name System (DNS, RFC 1034) translates one form of address into anotherspecifically. In more detail, it translates DNS addresses, such as www.google.com, into their corresponding IP addresses, xxx.xxx.xx.xxx.

DNS gets the job done in most cases using only two packets. For exampke, if you want to know *what is the IP address of www.hh.se?*, you should

1. Firstly, send a request packet(**Packet 1**) to your networks local DNS server that asks(for example, www.google.com).

2. Secondly, (**Packet 2**) is responsed from that DNS server, saying that www.hh.se resides on a server with an IP address of XX.XX.XX.XXX.

- **Your task 1**: List sample packets of **Packets 1** and **Packet 2**.
- **Your task 2**: What is the IP address of www.hh.se?

6.5 MSN messenger service

There are several popular instant messaging applications, msn, yahoo message, etc. Image that you are the boss in a company, and you suspect an employee giving away financial information over messager software. What can you do? Yes, catch him (or her)! Here well focus specifically on traffic from the MSN Messenger Service (MSNMS).

- **Your task 1**: List some sample MSNMS packets.
- **Your task 2**: Can you recognize the email address of the guy you are talking with by MSNMS packets? If u can, what is it?

- **Your task 3**: Can you recognize the content of sending and recieving messages by MSNMS packets? If u can, what are they? (By simply right-clicking one of the MSG pakcets, and selecting **Follow TCP stream**.)

References