Modern snoop lab
lite version

Laboration in data communication
OpenIPLab
Department of Information Technology, Uppsala University

Overview

This is a lab constructed as part of the OpenIPLab project.

Administration

Student

Name: 
Email: 
Personal number: 

Student

Name: 
Email: 
Personal number: 

Agreement

We have independently worked on the following assignment solution.

Sign: 
Sign: 
Sign: 
General

Course instance (e.g. Datakom DV1): ____________________________

Date: ____________________________

Note to the lab assistant

_________________________________________________________________

_________________________________________________________________

_________________________________________________________________

_________________________________________________________________

_________________________________________________________________

Comments from the lab assistant

_________________________________________________________________

_________________________________________________________________

_________________________________________________________________

_________________________________________________________________

_________________________________________________________________

Grade: ____________________________

Sign: ____________________________
1 About the lab

This is a mandatory lab in the Datakom courses (1TT821,1IT070) during fall 2004. You will only get access to the lab machines during your booked session, so make sure you get all data you need to answer the questions. You can only perform this lab on the lab machines.

Objectives

- Understanding of network layers (e.g. TCP, IP, MAC)
- Understanding the role of services offered by each layer
- Gain deeper insight into web transactions using HTTP, and the resulting network traffic
- Practicing network tools and command usage

Reading instructions

Computer Networking - a top-down approach featuring the Internet (3d edition) Kurose, Ross

- 2.2.1-2.2.3 (HTTP)
- 2.5.0-2.5.1 (DNS)
- 4.1-4.2.0 (routing)
- 4.4 (IPv4), especially 4.4.1 (packet format)
- 5.1 (MAC layer)
- 5.4 (ARP)

Theoretical and practical questions

There are a number of questions marked with a star (*) which do not require you to use your computer. I.e., these questions can be done after the lab. Please save the theoretical questions until the end of the lab in order to get all the data you need to finish the lab.

2 Lab description

General

In this lab you will use a network monitoring program ("sniffer") to listen to all packets that are sent on the wire that your machine’s network card is connected to.
It can be seen as a wire tapper, which all packet go through. Due to the network setup (switched network) you will only see packets to and from your computer + broadcast packets. That is, you can’t easily eavesdrop your neighbours traffic in this kind of network by sniffing from your computer’s network card.

The sniffer program, Ethereal, contains a graphical interface which allows the user to see the captured packets in a systematic and structured way. The packets are seen in the order they were captured, and the program automatically parses and presents them in a tree-view based of the headers in the packet. This makes it easier for the user to quickly get an overview of the packets that are captured.

However, it is important to realize that the packets that are captured are really just a chunk of bytes (as presented in the bottom window), and that Ethereal is just a tool for presenting the data.
Startup

- Login to the machine using the graphical login program. Enter the username lab and the password lab.

- Start a web browser, such as Mozilla (available in the toolbar as a big red star icon).

- Switch to a different virtual desktop by clicking on the upper toolbar, which contains four (grey) desktops.

- Press the Ethereal icon (the red apple) (or `sudo ethereal` in a terminal window) to start the network monitoring program.

- Notice your IP address for the tap3XX interface using the `ifconfig` command in a terminal window (the icon with a screen and a footprint). You will get an IP address of the format 10.x.1.1 where x is your team number. You will need this team number in the lab.

Your team number:
Stage 1 - Packet examination

Introduction

- In Ethereal: use Menu bar Capture, select interface tap3XX, select Start and press the OK button. Now the program will listen to all packets that are sent to/from your computer. **Make sure you select the correct interface!**

- Go back to the web browser and go to http://www"your teamnumber".openiplab.net/ (e.g. http://www2.openiplab.net). You will see a new page appear in your web browser.

- **Wait approximately 20 seconds** to capture all packets, before performing next step.

- Switch back to Ethereal, and press the Stop button, to stop collecting data. Now the upper table is filled with data. Each row of the table corresponds to a packet. To see more detailed information about each packet, mark the row and look at the middle window. You can press the rows with a plus (+) sign to expand a category, to see more detailed information. When marking a row in the middle window, you will see the corresponding HEX dump in the bottom window.

Assignment

Visit the web page at http://www"your teamnumber".openiplab.net/lab1/ (e.g. http://www2.openiplab.net/lab1/). You will see a page with two links. Now start ethereal. Capture data for the first page with Ethereal. You should use the data from Ethereal to answer these questions:

1. (a) Which transport protocol is used for web traffic?

   ___________________________________________________________

   (b) In which field of the IP header do you see it?

   ___________________________________________________________

   (c) Which value (number) identifies this transport protocol?

   ___________________________________________________________
2. (a) Which application protocol is used for web traffic?

(b) Your computer receives an TCP/IP packet. How does it decide which application should handle the packet? E.g. to choose whether your web server or mail server should handle the packet?

3. Why are there so many packets (other than those that contains HTTP data) sent to/from your computer when clicking on a link? Identify the other packets. Why is it important to wait 20 seconds before ending the capture, as you did and recently carefully read in the introduction?

4. (*) Draw a picture of a complete HTTP packet (including all headers, like the IP header, etc.) and mark where the different headers and the data are located. Do not draw individual fields in the headers. Draw the packet as a rectangular box.
5. Restart the capturing then visit a page with pictures, more specifically, http://www"your
teamnumber".openiplab.net/lab1/volvo.html. Could you tell if it is a persis-
tent or non-persistent HTTP session? (See page 91 in textbook.) Do you see
any contradictory facts or something that seems unnecessary? Discuss this
with your teaching assistant if you don’t discover this by yourself. Give an
exhaustive motivation and what the contradiction may be. Motivate why it
is like this. What are the pros and cons of such an approach?

Note: To answer this question you must study the packets in great detail.

6. How much overhead do the packets have for the page /lab1/overhead.html.
   Calculate all packets’s size (all packets that you captured), from Ethernet
   frame to data. The total packet size can be found in in the middle window
   of Ethereal, by expanding the Frame x (where x is a number). The payload
   is considered to be the HTML code that is sent to the client. Present your
calculations and give an answer in percentage (%).
Stage 2 - Address resolution at different layers

You will be visiting the link http://www"your teamnumber".openiplab.net/search which is a minimalistic google site (http://www.google.com/). Search for pages with cars using the search word "cars". You will get a hit list of three entries. Pick the one you like most and click on it. The URL will be shown in the field at top of the web browser.

Assignment

1. Where is the page located? Answer with the host name (Fully Qualified Domain Name). (Hint: use information from the URL)

2. Use DNS (Domain Name System) to resolve the IP address of the host. Try the host command in a terminal window. What is the IP address?

3. (a) Which transport protocol is used for DNS?

(b) Which protocol number has this transport protocol?

(c) (*) Why do you think this protocol has been chosen?

4. Capture the packets while retrieving the web page of your choice (inside the openiplab.net domain). Look at the "Destination Address" field in the Ethernet frame of a packet sent from your machine. Try the arp -n command in a terminal window, to see the ARP (Address Resolution Protocol) cache. (HWaddress == MAC address)
(a) Which IP address does the MAC address resolve to? (Ignore the 192.168.0.x addresses.)

(b) Look at the IP header of the packet, especially the field destination. Why do the destination address in the Ethernet II frame (which you resolved to an IP address in (a)) and the IP header differ?

5. From question 4 you will see that the packet is not sent directly to the destination. You can confirm this by running `traceroute www"your teamnumber".openiplab.net`, which prints the route to the host.

(a) How does the sender decide whether to send a packet directly or not? (Hint: `route` command)

(b) (*) Why is routing/IP forwarding an important concept? Explain and give an example where routing/IP forwarding is necessary.
Stage 3 - The big picture

In this step you will capture packets at the server. The server is located on 192.168.0.140.

Login to 192.168.0.140 with SSH with `ssh -l teamXX 192.168.0.140` in a terminal window, using the username teamXX and the password teamXX. (Replace XX with your teamnumber!) Answer yes to the question SSH prompts you with. Start Ethereal with `sudo ethereal` and capture data here using interface tap2XX.

*Important!* Before accessing a web page, delete the ARP entry (if any) on your client machine for your default gateway (10.your teamnumber.1.30), e.g. `sudo arp -d 10.your teamnumber.1.30`.

Assignment

1. Capture data at both 192.168.0.140 and your client, while accessing a web page. Compare the data from both computers. For simplicity, choose one packet (e.g. the first HTTP packet) and compare the same packet on both computers. How do they differ?

2. Compare the packets that are captured now with the packets you captured (and analyzed in stage 1, question 3). Are there any new kinds of packets appearing? What are their purposes?
If not, read the introduction in stage 3 and conduct those steps again, before trying to repeat the capture.

3 The report

You should answer all of the questions above. Also make sure that you covered all subquestions.

You may write in English or in Swedish.

Hand in this printed out lab with your answers filled (in a legible style) to the lab assistant’s pigeonhole. This should be done before the date announced at the lab page for your course instance.

4 Marking guidelines

Laboratory results are allocated according to the one of the following grades.

<table>
<thead>
<tr>
<th>Grade</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Godkänd</td>
<td>G</td>
<td>You have answered all the related questions in a satisfactory manner.</td>
</tr>
<tr>
<td>Komplettering</td>
<td>K</td>
<td>The questions need further work in order to address shortcomings. The lab assistant will contact you with information how this is done. The code or questions need further work in order to address shortcomings or implementation bugs revealed during the tests associated with marking.</td>
</tr>
<tr>
<td>Underkänd</td>
<td>U</td>
<td>Failed. Questions have not been answered to the satisfaction of the marker, and the time limit (generally one year from the date when the work was due) for handing in material has expired.</td>
</tr>
</tbody>
</table>