# Rigged and Wired

Everything is Connected. Connection is Power.

## CS3210 - Computer Networks Lab

Instructor: Krishna M. Sivalingam
*Spring 2015, Indian Institute of Technology Madras*

## Introduction

In this assignment, the goal is to understand and setup network configurations for a system of computers and also to observe, analyze and deduce important information from network traffic. In the process, you will be learning several command line utilities that help configure networking functionalities in your system. In addition, you will be capturing and analyzing network traffic using wireshark, a powerful networking tool. Firstly, here are some ground rules:

- You will be working in teams of TWO in this session.
- You will use your LAN cables **only** to connect your own laptops to each other. You will not connect them to the Systems Lab LAN ports.
- You are allowed to google all you want for the session. The objective is to solve the given problems in the timespan of the lab. Avoid inter-group communication.
- You will try your best to minimize the Internet load in the DCF (Avoid network-heavy applications like Gmail, Facebook, Youtube etc.). Keep in mind that there are at least 70 people that will simultaneously be using the Internet in the lab.
- You will document what you did in this lab in a single document file per group. Include the relevant screenshots if necessary in the document. Upload this file in pdf format on moodle by 11.55pm. The file name must be of the format. Roll1_Roll2_Lab2.pdf).

There are two parts to this session.

## 1 Networking, Network-king or Not-working?

In this section, you will be using command line utilities to configure systems on a small network. Assume that A and B are the two laptop computers that your group has.

### 1.1 Initiation

1. Enable Networking on both computers. Disable Wi-Fi on B. Enable Wi-Fi on A. Disconnect both A and B from all other wired connections.
2. Connect A to the nearest Wi-Fi hotspot and ensure that Internet is active and working on it.
3. Now, connect both A and B using the LAN cable.

### 1.2 The Task

Your task is to now connect B to the Internet *through* A by configuring A and B suitably on the command line. Here are some hints to get you going.

- Manually configure the IP addresses of A and B's ethernet interfaces to belong to a subnet of your choice - For example 192.168.123.*
- Set A as the default gateway node in B's routing table.
- Configure NAT on A to forward packets from the ethernet interface to the wireless interface and back. You can follow the tutorial here to set up the NAT.
- Set the DNS server in B to the department DNS server - `10.6.0.11`. (Modify `/etc/resolv.conf`)

The following utilities will be useful: `ifconfig, ip addr, route, route add, /sbin/iptables, etc.` Look up their man pages or google them to find out more. Also, to enable ip forwarding in linux, use the following command

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

### 1.3 Take Home Task (Ungraded)

**Alias IP Addresses** : IP Aliasing is the concept of associating multiple IP addresses with the same physical interface. For example, the `eth0` interface can have both IP addresses `192.168.1.3` and `192.172.54.4`.

To add an Alias IP address `192.172.54.4` with a subnet mask of `255.255.255.0` to an interface with an already existing IP address, just execute:

```
sudo ifconfig eth0:0 192.172.54.4/24
```

You can learn more about Alias IP addresses here.

### 1.4 Documenting

1. Once you get the system working correctly, show it to your TA.
2. Document all the commands you used, why you used them and also the meaning of each of the arguments/parameters used in each command. What will happen if ip forwarding is not enabled?

## 2 Network Forensics & Sleuthing

In this part, you will be using wireshark to capture and analyze packets on the network. You will use it to deduce important information about the network.

## 2.1 Warming Up

- Setup wireshark on your computer and begin capturing packets on the wireless interface that is connected to the Internet.
- Open up a terminal and ping `www.cse.iitm.ac.in`
- In wireshark, observe the following. Use the filters `dns, arp, icmp, http` for the first four.:
  1. *DNS Request and reply packets for* `www.cse.iitm.ac.in`: What transport layer protocol does the DNS request use?
  2. *ARP Request and response*: What is the destination MAC address for ARP requests?
  3. *ICMP Echo and Reply packets*: What is the value present in the `type` field of the ICMP header in those packets? What is the size in bytes of the ICMP data field? What is the data being sent?
  4. Open up your browser and visit `http://www.google.com/loon/`. Find the corresponding HTTP GET requests for images in the webpage in wireshark. What all information does the user-agent field in the HTTP header contain?
  5. Experiment with filters: Filters are extremely powerful and can simplify analysis if used intelligently; Here is an example:

     ```
     tcp && not ssh && (ip.src == 10.6.16.244 || ip.dst == 74.123.4.23)
     ```

     List any two filters your tried along with snapshots of the output.

## 2.2 The Treasure Hunt

You are given a pcap file (packet capture file) which was captured by wireshark on a certain computer in IIT Madras (Download the file from Moodle). Among other things, the pcap file contains the trace of a conversation between two people X and Y. Mr. A.G, the master of information extraction, was spying on this conversation to extract as much information as he can. He has discovered the following information so far:

- The chat conversation happened over a UDP connection.
- A file was transferred between the two parties over an un-encrypted FTP (similar to the protocol implemented in the first assignment)
- The first 4 bytes of the file transferred are `FF D8 FF E0` and the last 4 bytes are `FF D9 40 24`.

Mr. A.G is busy with TA work and hence needs your help to analyze the trace and to answer the following questions.

1. What are the IP addresses and names of X and Y? What is the first and last message of the chat conversation?
2. How many packets was the file that was transferred split into? Use the packet trace to reconstruct the entire file. What is the type of the file?
3. What is the game that Bob was talking about?

## 2.3 Documenting

Document the answers to the above questions along with the methods (including filters, other software etc.) you used and/or tried to get to the answer.