Name 1: _____ Group number: _____
Name 2: _____

COMPUTER NETWORKING
LAB EXERCISES (TP) 2
"IT DOESN'T WORK!"

September 14, 2009

Abstract

In computer networking it is quite common to encounter situations where something "doesn't work". You may have already experienced this when dealing with networking equipment at home. Suddenly, the email client that worked perfectly fine refuses to fetch new mail, the webpage that you accessed yesterday can no longer be displayed. These problems and situations are numerous. The goal of this TP is to learn how to deal with such problems. You will be put into situations where something doesn't work as expected. Your task will be to analyze what does not work, find out why it doesn't work and come up with a fix for the problem.

This lab heavily depends on the commands and techniques that you learned in TP1. In order to pass this lab successfully, make sure that you fully understood TP1.

1 ORGANIZATION OF THE TP

The setup for this TP is essentially the same as for TP1: A group of two students works on one work space. There are two computers per work space. The workspace number is written on stickers tagged to each computer. During one stage of the TP you will have to collaborate with a group from another work space. Before starting this part, you should choose the work space to collaborate with and synchronize the rest of the work with them (otherwise you might end up typing the same commands on two work spaces).

1.1 TP REPORT

The report is due on **October 22 at 12:15**. You can hand it in either during the lab session on October 15 or before the lecture on October 22 (in INM202 from 12:00 to 12:15).

During the TP, fill in your answers directly in the spaces provided in this document. That will be your TP report (one per group). Don't forget to write your names and group number on the first page of the report.

1.2 Main Principle of this Lab

Throughout this lab we will give you tasks to do, *e.g.,* send an email to some address. However, as the title of the TP already suggests, things will not always work out nicely. Before performing a task you will have to execute a script. This script will put your system into a problem situation where something doesn't work. You are then asked to find out what the problem is and to come up with a solution.

Each task is independent of the others. The scripts first reset the machine to a known correct state, and then create the problem. In particular, problems from earlier tasks do not still exist in later tasks.

1.3 How we grade your answers

For every task you have to tell us what the problem is, *i.e.,* why it does not work. Also tell us how you fixed it. But most importantly: Tell us exactly how you detected and located the problem. **The points you will get for your answer mostly depend on your explanations of how you located the problem!** You should use the scientific method when answering the questions. The methodology to follow is the following:

1. Pose a hypothesis
2. Run experiments to validate hypothesis
3. If validation is OK exit, else loop (go back to 1. by posing another hypothesis)

In your answer you should write all the steps. Especially, you should also write down hypotheses that later proved to be wrong. We would like to see the way you took to reach your final conclusion!

Example: Your task is to turn on the lights in a room. It doesn't work. If your answer is "The problem was the light bulb that was not working. I exchanged it and this fixed the problem." you will get 0 points. How could you know? Just by trial and error? Maybe the real reason was a short blackout and the electricity came back while you changed the light bulb. So you ended up throwing away a perfectly working light bulb without finding the problem at all. A correct answer that gives you all the points would be "I first suspected a blackout. So I checked the lights in the other rooms and they worked just fine. I concluded that a blackout seemed unlikely, my first hypothesis was thus wrong. I posed a second hypothesis: the problem could be the fuse of the room in question. I verified the fuse and found it intact. So I made a third hypothesis: the light bulb might not work. I checked the bulb and found its wire broken. From this I concluded that a broken bulb was the problem. I replaced it with a new one and the lights came back."

More specifically for this TP: What observations led you to the conclusion that exactly this thing didn't work? What were the commands you executed to get there? Up to which point did the system work as expected? What were the expected actions that never got executed? What was the packet that did not reach its destination? Where and why did it get dropped/lost/not sent?

2 Preparing your Workspace

The hardware in the IEW room is shown in the figure below. Each work space consists of one hub and two Linux PCs: one workstation PC and one router PC, each with two Ethernet cards. On the workstation PC, we will only be using one of the two cards, the one corresponding to the interface eth0.

2.1 Hardware Identification

For the first part of this session, we will not use the central hub located beneath the window. Instead, we will use the "EPFL"-hubs that are scattered on the shelves with the PCs. We will denote these hubs as epfl-hubs for the remainder of this TP. The epfl-hubs are connected to a gateway that gives you access to the Internet.

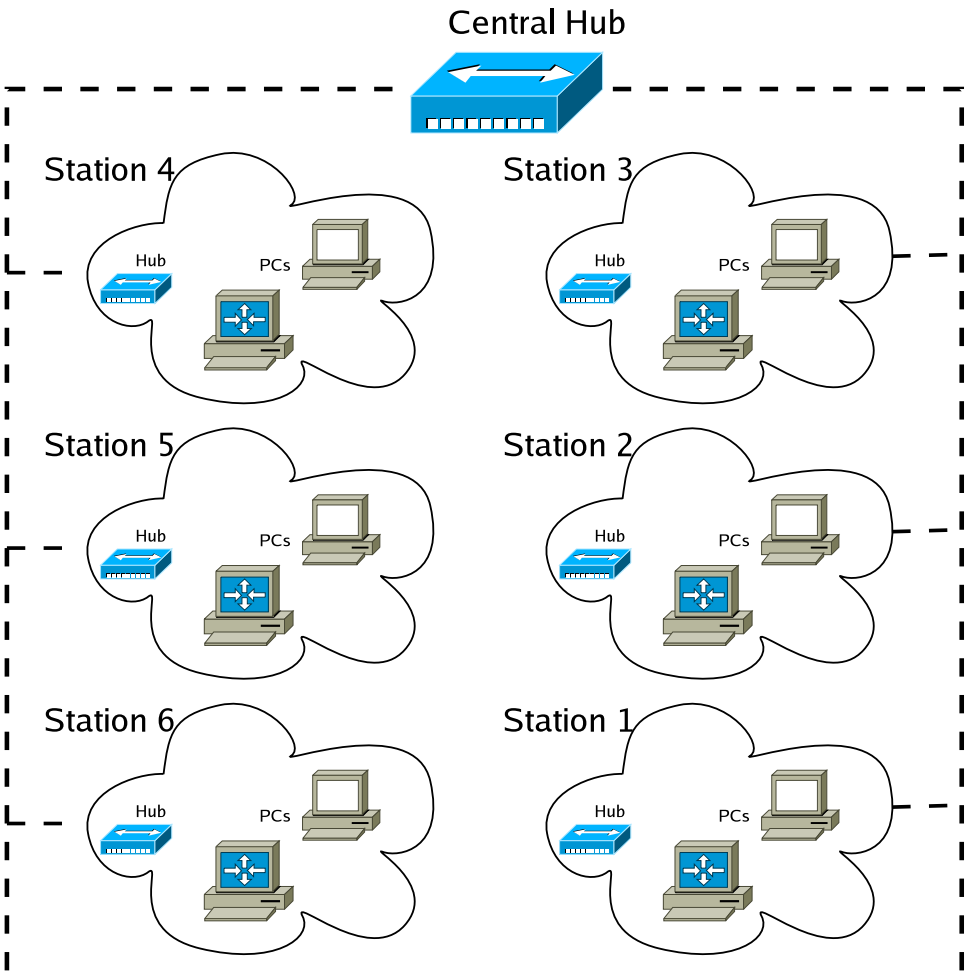


Figure 1: Existing networking hardware in the room.

For the second part of this session we change the configuration and use the central hub located beneath the window instead of the epfl-hub.

Identify the following components:

- 3 10BaseT cables (2 short, 1 long)
- 1 hub on your work space
- 1 epfl-hub somewhere near your PCs
- 1 central hub somewhere near the window
- 1 *Workstation PC*, with two Ethernet cards
- 1 *Router PC*, with two Ethernet cards

For now, make sure you disconnect the cable connecting your router PC to the central hub beneath the window (if any).

2.2 Download the Scripts

2.2.1 Identify Workspace Number and Login

Identify your workspace number (the workspace number is written on blue stickers tagged to the computers). You will need it later to know which IP addresses to use while configuring the computers.

What is your workspace number?

2.2.2 Put your Computers into a Clean State

You need to reset the network configuration to a clean state to make sure you don't get troubles with configurations left behind from another group. Load the lab1 default configuration from the IEW software on your desktop.

2.2.3 Unpack the Scripts

On both the router and the workstation PC there should be a file called `lab2-scripts.tar.gz` in the `/root/lab2` directory. Unzip it and extract the files:

```
# cd /root/lab2
# tar -xzvf lab2-scripts.tar.gz
```

This will create a directory `lab2-scripts/` containing the scripts used in this TP.

Check that on the router PC and the workstation PC you have a `lab2-scripts/` directory with the following content

```
# ls lab2-scripts
header.sh lab2-pb1.sh.x lab2-pb2.sh.x lab2-pb3.sh.x lab2-pb4.sh.x
default_script.sh.x
```

If all the files are there, you are now ready to start the lab.

3 Part 1: Your first day at IEW

Today is your first day at your new company IEW (Internet Enterprises Worldwide). Unfortunately, your new employer had to cut down the costs in its IT department during a recent restructuring. As a result, every new employee has to setup his workstation all by himself, making sure he is connected to the company's LAN and to the global Internet. The only support given by the IT department is through a webpage on IEW's intranet that can be found under `http://www.iew.epfl.ch`. Further, they also provide you with a figure of their network topology (see Figure 2).

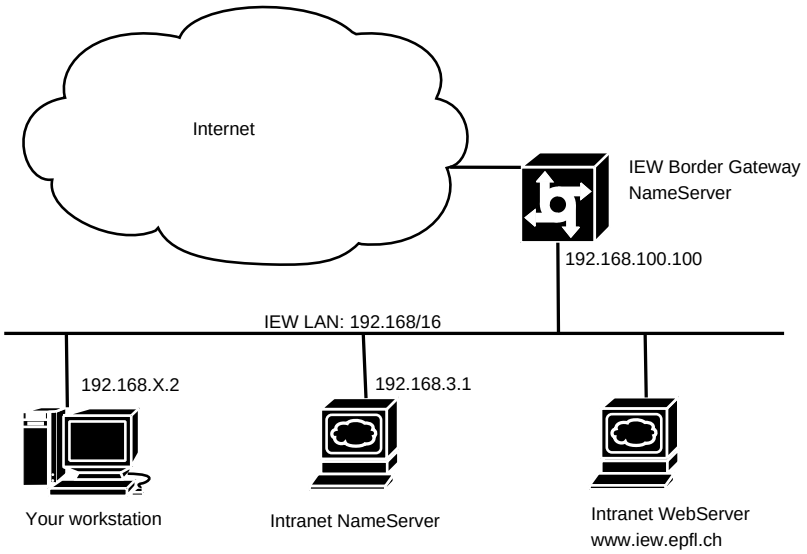


Figure 2: Network topology for the first part of the lab.

3.1 Wiring and Addressing Scheme

The topology of the network for this part of the lab is shown on Figure 2. For this part we do not need the router PC, but we will only work with the workstation PC. Further, you do not have to change the wiring, you can leave the workstation PC connected to the epfl-hub. Through the epfl-hubs you connect directly to the IEW LAN. The addressing scheme is the following: the interconnecting network (IEW LAN) has address range `192.168/16`; your station has the IP address `192.168.X.2`, where X is your workplace number.

3.2 Your First Task: Connect your Workstation to the Internet

The first task of every new employee at IEW is to make sure his computer is connected to the Internet and that he is able to browse the world wide web (exclusively for work purposes of course, even though IEW has quite a relaxed policy and so far no cases are known where someone was fired because of excessive web surfing). IT believes that this is quite a simple task. Therefore, don't expect to find anything on this topic on their support website (and thus do not waste time looking for it).

3.2.1 Execute Script

You will now have to execute a script on your workstation in order to put it into the state required for this task.

Close all applications except the terminal. Load the lab1 default configuration from the IEW software on your desktop. Then navigate to the `/lab2-scripts` folder and execute script `lab2-pb1.sh.x` as shown in the following code snippet. Instead of X you have to type in your workspace number:

```
# cd /root/lab2/lab2-scripts
# ./lab2-pb1.sh.x -u X -m 2
```

3.2.2 Try to Connect to the Internet

You are now ready to start a web browser and try to connect to the Internet.

```
# firefox &
```

Try to display the page of `http://www.google.com`.

What is the error message?

3.2.3 Fix the problem

It is now your task to find what the problem is and to fix it. Please make sure to stick to the guidelines given in Section 1.3 when answering the questions.

What was the problem?

How did you find the problem? How did you conclude this was the problem?

How did you fix it?

3.3 Your Second Task: Make your Workspace Fully Operational

Now that you are able to surf the web, you are almost ready for the real work. However, at IEW most of the communication inside the company relies on email. So you definitely need to configure your email client to be fully operational.

3.3.1 Execute Script

You will now have to execute a script on your workstation in order to put it into the state required for this task.

Close all applications except the terminal. Load the lab1 default configuration from the IEW software on your desktop. Then navigate to the `/lab2-scripts` folder and execute script `lab2-pb2.sh.x` giving it a parameter X corresponding to your workspace:

```
# cd /root/lab2/lab2-scripts
# ./lab2-pb2.sh.x -u X -m 2
```

3.3.2 Configure the Email Client

The preferred email client at IEW is Evolution. Open it by typing:

```
# evolution &
```

You will now have to configure the client. In your welcome package from the IT department you find the following instructions:

- **server type:** IMAP

- **incoming mailserver:** mail.iew.epfl.ch
- **outgoing (SMTP) server:** postman.iew.epfl.ch
- **username:** stationX (where X has to be replaced by the number of your workspace)
- **password:** stationXp (where X has to be replaced by the number of your workspace)
- **your email address:** stationX@iew.epfl.ch (where X has to be replaced by the number of your workspace)

Once configured, you will have to send an email to your boss (`boss@iew.epfl.ch`), so that he knows that you are ready to work. He will then reply with the instructions for your further work at IEW.

Send an email to `boss@iew.epfl.ch`. Does it work? Do you get a reply from your boss?

If your answers to above questions are "No", you will have to make it work ASAP, otherwise your boss (who is well-known to sometimes be in a very bad temper) might get really upset.

Once you fixed the problem, please make sure that you really got a reply to the message YOU sent to your boss. There could be some messages left in your inbox from an earlier group, so don't mistakenly take one of these for the reply to your message!

3.3.3 FIX THE PROBLEM

It is now your task to find what the problem is and to fix it. Please make sure to stick to the guidelines given in Section 1.3 when answering the questions.

What was the problem?

How did you find the problem? How did you conclude this was the problem?

How did you fix it?

4 PART 2: YOUR FIRST PROMOTION

As its name already suggests, IEW is a worldwide operating company. They thus have quite a big number of branch offices that are scattered all over the world. For the correct functioning of the company, the computer networks of all these branch offices have to be interconnected. However, it turns out that this interconnection doesn't work well. Every day there are complaints of employees that are not able to work due to network failures. This is causing a lot of headaches to the managers of IEW (which is of course partly their own fault as a lot of their networking specialists had to leave the company when they decided to cut down costs in IT. The rumor goes that some of the let down engineers even introduced errors on purpose to cause damage to the company...). In short, the managers are very desperate and need a quick solution. They are also very impressed by the networking skills you have shown when solving all the problems encountered during your first day at work. So at your second day at work you already get a promotion: over night you were made manager of one of IEW's uncountable branch offices and thus responsible for the seamless interconnection of your branch to the rest of the company.

Note, that the scenario described here just serves as an illustration: In reality one would not try to achieve worldwide interconnection with the methods you learned in TP1 (i.e., static routing). One would rather rely on routing protocols such as BGP, which you will discover later on in this course.

4.1 WIRING SCHEME

The wiring scheme for this part of the TP is shown in Figure 3.

Make sure that you disconnected your router from the epfl-hub. Eth1 of the router should now be connected to one of the central hubs close to the windows.

Site X thus represents the branch office you are responsible of. Site Y is another branch office. Each branch office owns one router which allows interconnection to the other branch offices via the interconnection network (WAN).

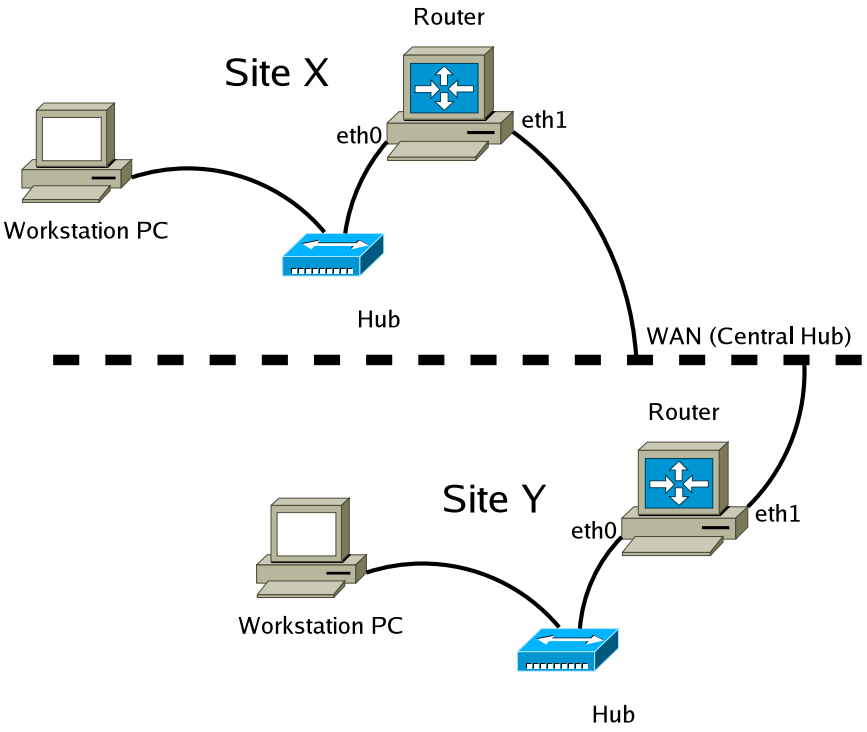


Figure 3: Network topology for the second part of the lab.

4.2 Addressing Scheme

The following address scheme is imposed to you by the central IEW IT department (as you noticed they are not of much help in general, but they are still very good at issuing rules...):

- for the local network at your branch office you will use addresses from the space 192.168.X/24 where X is your workspace number. The host part of the workstation PC's IP address is 2, the host part of the router's internal IP address is 1.
- IEW's company network uses addresses from the space 192.168.100/24. The host part of your router's external IP address must correspond to your workspace number X.

4.3 Cooperating with Another Group

Luckily you are not the only manager of a branch office with networking troubles. There are other freshly promoted managers at other branches that are in the same situation you are. For the following tasks you need to find one of them that is connected to the same central hub and synchronize your groups from here on.

What is the number (Y) of the workspace you cooperate with?

4.4 Your Third Task: Access Webpage of Other Branch Offices

For all subsequent problems, the task will be the same. Each branch office is running a webserver. Your goal is to access the webpage of the cooperating group from your workstation PC. Don't worry, webserver setup and configuration is one of the few services which are provided by IEW's IT department. You do not have to do it yourself and could in principle assume that they work properly (still you should not trust IT blindly, it is always a good idea to test anyway). The webservers are running on the workstation PCs, *not* on the router PCs.

4.4.1 Execute Scripts

You will now have to execute a script on every machine in order to put them into the state required for this task.

Both groups should execute the following on their workstation PCs: Close all applications except the terminal. Load the lab1 default configuration from the IEW software on your desktop. Then navigate to the `/lab2-scripts` folder and execute script `lab2-pb3.sh.x` giving it the following parameters (X corresponds to your group number, Y to the group you cooperate with and 2 corresponds to the workstation):

```
# cd /root/lab2/lab2-scripts
# ./lab2-pb3.sh.x -u X -g Y -m 2
```

Example: Groups 21 and 23 cooperate. Group 21 thus executes

```
# ./lab2-pb3.sh.x -u 21 -g 23 -m 2
```

Group 23 executes

```
# ./lab2-pb3.sh.x -u 23 -g 21 -m 2
```

Both groups should execute the following on their router PCs: Close all applications except the terminal. Load the lab1 default configuration from the IEW software on your desktop. Then navigate to the `/lab2-scripts` folder and execute script `lab2-pb3.sh.x` giving it the following parameters (X corresponds to your group number, Y to the group you cooperate with and 1 corresponds to the router):

```
# cd /root/lab2/lab2-scripts
# ./lab2-pb3.sh.x -u X -g Y -m 1
```

4.4.2 Connect to the Other Group's Webserver

Start the web browser on your workstation.

```
# firefox &
```

How would you check whether your web server on your workstation PC is running correctly? Check it just to be sure. What is the result?

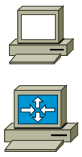
Try to reach the website of the other group by pointing your browser to `http://192.168.Y.2`.

If it doesn't work (actually, if you did all the above steps correctly it should not work ;-)), you unfortunately have to fix it.

4.4.3 Fix the problem

It is now your task to find what the problem is and to fix it. Please make sure to stick to the guidelines given in Section 1.3 when answering the questions.

What was the problem? Why did it not work?



How did you find the problem? How did you conclude this was the problem? Always point out what you did on the router (and on which one, yours X or the one of the other group Y?) and what you did on the workstation (and on which one, yours X or the one of the other group Y?).

How did you fix the problem? Always point out what you did on the router (and on which one, yours X or the one of the other group Y?) and what you did on the workstation (and on which one, yours X or the one of the other group Y?).

4.5 YOUR FOURTH TASK: ACCESS WEBPAGE OF OTHER BRANCH OFFICES AGAIN

This time you will have to access the webserver of the group with the bigger workplace number from the workstation PC of the group with the smaller workplace number.

Example: Groups 21 and 23 cooperate. The task is thus to access the webpage of group 23 from the workstation PC of group 21.

4.5.1 EXECUTE SCRIPTS

Execute a script on every machine in order to put it into the state required for this task.

Both groups should execute the following on their workstation PCs: Close all applications except the terminal. Load the lab1 default configuration from the IEW software on your desktop. Then navigate to the `/lab2-scripts` folder and execute script `lab2-pb4.sh.x` giving it the following parameters:

```
# cd /root/lab2/lab2-scripts
# ./lab2-pb4.sh.x -u X -g Y -m 2
```

Example: Groups 21 and 23 cooperate. Group 21 thus executes

```
# ./lab2-pb4.sh.x -u 21 -g 23 -m 2
```

Group 23 executes

```
# ./lab2-pb4.sh.x -u 23 -g 21 -m 2
```

Both groups should execute the following on their router PCs: Close all applications except the terminal. Load the lab1 default configuration from the IEW software on your desktop. Then navigate to the `/lab2-scripts` folder and execute script `lab2-pb4.sh.x` giving it the following parameters (X corresponds to your group number, Y to the group you cooperate with and 1 corresponds to the router):

```
# cd /root/lab2/lab2-scripts
# ./lab2-pb4.sh.x -u X -g Y -m 1
```

4.5.2 Connect to the Other Group's Webserver

Start the web browser on your workstation.

```
# firefox &
```

Check locally whether your webserver on your workstation PC is running correctly (it should run if you executed all of the above scripts correctly).

Try to reach the website of the group with the bigger number from the workstation PC of the group with the smaller number (it should not work. So you unfortunately have to find the problem and fix it).

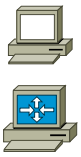
4.5.3 Fix the problem

In a first phase of locating the problem, assume you only have access to the workstation and router of the group with the smaller workplace number (Group 21 in the above example).

What are all possible conclusions you can get from this phase?

Please make sure to stick to the guidelines given in Section 1.3 when answering the questions.

From what you can conclude at the moment: what is the problem, why does it not work?



Which experiments did you make? How did you make your conclusions? Always point out what you did on the router (of the group with the smaller number) and what you did on the workstation (of the group with the smaller number).

Now, in the second phase you are allowed to access all the machines of both groups. Verify whether the conclusions you drew in the first phase hold, track down the problem completely and fix it.

Which additional experiments did you perform and what are your conclusions now? Always point out what you did on the router (and on which one, yours X or the one of the other group Y?) and what you did on the workstation (and on which one, yours X or the one of the other group Y?).

How did you fix the problem? Always point out what you did on the router (and on which one, yours X or the one of the other group Y?) and what you did on the workstation (and on which one, yours X or the one of the other group Y?).

4.6 YOUR FIFTH TASK: UNDER ATTACK

For this task, you will use three more tools: *nmap* and *hping* (at the workstation), and *iptables* (at the router). Make sure that they are installed, e.g., for *hping*:

```
# which hping
```

If it is installed, the above command should return the path to the executable, otherwise it returns nothing. In the latter case, contact the TAs.

Make sure the webserver at your workstation is still running, and that you can access the webserver at the workstation of group Y. If one is not running, start it as follows:

```
# /etc/init.d/apache2 start
```

4.6.1 THE ART OF ATTACK

You will attack the webserver of group Y from your workstation PC, and group Y will defend. Then, you will switch roles: they will attack and you will defend. Synchronize with group Y about who will attack first, and who will attack next. The workplace number of the attacking group will be denoted A and of the defending D. Read the viewpoints (see below) of both attackers and defenders before you continue.

The defenders should start wireshark on the three interfaces that they control, and the attackers on the workstation PC interface.

Synchronization Point 1: Make sure the other group has reached this point before continuing further.

4.6.2 THE ATTACKERS' VIEWPOINT

The first step in an attack against a network is to identify the active hosts in that network. Group A, therefore, should identify the active hosts (machines that exist) in the network 192.168.D.0/24.

How do you propose to identify these hosts?

nmap is a tool that automates many network exploration (nmap = Network MAPper) functions. Execute the command

```
# nmap -vv -sP 192.168.D.0/24
```

(-vv means very verbose)

What do you conclude from the output of nmap? What do you see at wireshark that nmap did?

Synchronization Point 2: Make sure the other group has reached this point before continuing further.

The second step in an attack is to identify the services (open ports) that are running on the active hosts. Assuming that only TCP ports are open, how can you identify these open ports? Recall the RFC-prescribed responses of open and closed TCP ports.

Execute the command

```
# nmap -vv 192.168.D.activehost
```

for all the activehosts that you found previously.

What do you conclude from the output of nmap? What do you see at wireshark that nmap did?

Synchronization Point 3: Make sure the other group has reached this point before continuing further.

After doing the reconnaissance, you must have found the webserver at the workstation. It's time to start the real attack. One of the most popular attacks against servers (not just web servers) is the Denial of Service (DoS) attack. You will not actually crash the webserver of the defenders, but they will certainly feel something...

Execute the command

```
# hping2 IPaddressOfWebServer -p 80 -c 5 -S
```

where `IPaddressOfWebServer` is the IP address of the webserver you discovered.

What do you see at wireshark that hping2 did?

Check the man page for hping2 (man hping2) and see what the options -c, -i, and -a do. Can you design a DoS attack based on the previous hping2 command and what you saw in the man page for -c and -i? Explain why it would be effective. (Hint: check also what the option -S does, and try to imagine what the webserver will feel like)

Synchronization Point 4: Make sure the other group has reached this point before continuing further.

Execute the command

```
# hping2 IPaddressOfWebServer -p 80 -c 1000 -i u1 -S -a 192.168.211.200
```

Observe the output, and wireshark. Do you think the attack was successful? Are your packets reaching the webserver? Do you expect to see any responses to the packets that you are sending? Write what you can say by observing only your own wireshark, and then consult with the defenders, too.

Synchronization Point 5: Make sure the other group has reached this point before continuing further.

Execute, exactly as before, the command

```
# hping2 IPaddressOfWebServer -p 80 -c 1000 -i u1 -S -a 192.168.211.200
```

Observe the output, and wireshark. Do you think the attack was successful? Are your packets reaching the webserver? Write what you can say by observing only your own wireshark, and then consult with the defenders, too.

Synchronization Point 6: Make sure the other group has reached this point before continuing further.

Execute the command (note the difference at the last IP address)

```
# hping2 IPaddressOfWebServer -p 80 -c 1000 -i u1 -S -a 192.168.211.201
```

Observe the output, and wireshark. Do you think the attack was successful? Are your packets reaching the webserver? Write what you can say by observing only your own wireshark, and then consult with the defenders, too.

Now it is your turn to be the defenders!

4.6.3 THE DEFENDERS' VIEWPOINT

Wait a little until the attackers start attacking, and then observe wireshark.

What do you see at wireshark? What is happening in your network? (Hint: The wireshark display filter (ip.dst==Find what IP address to put here)&&(icmp.type==0)&&(icmp.code==0) may be useful)

Synchronization Point 2: Make sure the other group has reached this point before continuing further.

What do you see at wireshark? What is happening in your network? (Hint: The wireshark display filter

(ip.dst==Find what IP address to put here)&&(tcp.flags.syn==1)&&(tcp.flags.ack==1) may be useful)

Synchronization Point 3: Make sure the other group has reached this point before continuing further.

What do you see at wireshark? What is happening in your network? Are you suspecting anyone as attacker?

At the workstation execute the command

```
# netstat -n --inet
```

This shows you the open TCP and UDP ports in the normal state of your network.

Synchronization Point 4: Make sure the other group has reached this point before continuing further.

Execute the command `netstat -n --inet` a few more times a few seconds from each other (the command `watch` might be useful). Do you notice anything? What do you see at wireshark? What is happening

in your network?

Are you ready to do something about this attacker?

If yes, execute the following command at the router

```
# iptables -A FORWARD -s IPaddressOfAttacker -j DROP
```

This command instructs the kernel to drop all the packets coming from the IP `IPaddressOfAttacker` that ask to be forwarded to another host.

Wait until `netstat -n --inet` shows normal output again.

Synchronization Point 5: Make sure the other group has reached this point before continuing further.

Observe wireshark and guess what is happening.

Synchronization Point 6: Make sure the other group has reached this point before continuing further.

Observe wireshark and guess what is happening.

You are now done. Remember to tear down the packet filter you set up before.

At the router, execute the command

```
# iptables -D FORWARD -s IPaddressOfAttacker -j DROP
```

(exactly as before, only with -D instead of -A).

Now it is your turn to be the attackers!