

## Practice #0: Procedure for Remote Access to the Networks Lab (Lab B6)

All rights reserved © 2013-2022 by José María Foces Morán and José María Foces Vivancos

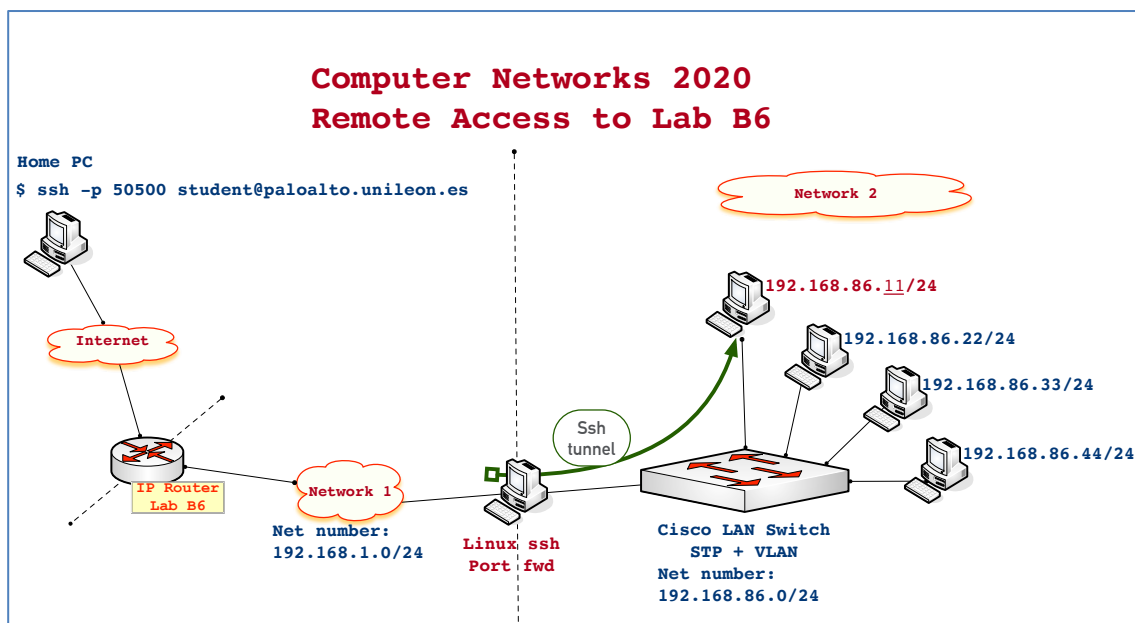


Figure 1. Abstract Lab B6 network diagram

Check the remote access to Lab B6 network from your Linux host at your home by following this outline:

1. Compose the following command in a terminal window in your Linux -note, you will have to replace student0 by your real login name at host paloalto.unileon.es at port 50500. In practice 1 you can find additional examples about the use of the ssh and scp utilities (<http://paloalto.unileon.es/cn/labs/CN-Lab1-2019.pdf> ). In the outline below, assume the shell prompt in your Linux host is:

```
[my pc] $
```

Replace <your-login-name> with the login name that you should have received via e-mail from [jmfocm@unileon.es](mailto:jmfocm@unileon.es) and press return:

```
[my pc] $ ssh -p 50500 <your-login-name>@paloalto.unileon.es
```

Students who use Windows and who haven't their Linux ready yet, can download the Putty secure terminal emulator, in which case they will enter the host paloalto.unileon.es and port number 50500 in the initial Putty dialog Window.

2. If this is the first time that you connect with paloalto.unileon.es at port 50500, the system will send you its digital fingerprint which you'll have to accept if the fingerprint that you received is equal to the one right below (In red):

```
The authenticity of host 'paloalto.unileon.es (paloalto.unileon.es)' can't be established.  
ECDSA key fingerprint is SHA256:qm7zH7xmmjsAjvpOwpbGYi6t9KrpBewG21svavP7h4.  
Are you sure you want to continue connecting (yes/no)?
```

3. When prompted to do so, type your password. Now, you can type several simple commands to acquaint yourselves with the Linux system in this host. Observe the results are what you expect:

```
[paloalto] $ id  
[paloalto] $ whoami  
[paloalto] $ who  
[paloalto] $ pwd  
[paloalto] $ date  
[paloalto] $ ifconfig  
[paloalto] $ uname -a
```

4. Break your connection by composing the combination ctrl-D or by typing the exit command:

```
[paloalto] $ exit
```

5. Net<sub>2</sub> is not connected to Internet except via the ssh tunnel, consequently, you will not be able to download files from any host within it, however, you can ***upload files to*** your account in host paloalto.unileon.es. Fortunately, the ssh tunnel allows ssh virtual terminal connections *and* also scp remote copying of files -both, ssh and scp use the same application protocol, ssh. Let's create a new file and upload it to your account in paloalto.unileon.es:

```
[my pc] $ echo "My valuable new file!!!" > myfile  
[my pc] $ ls myfile  
myfile  
  
[my pc] $ scp -P 50500 myfile student0@paloalto.unileon.es:copyofmyfile
```

6. Type your student0 password when prompted to do so.

Now, let's check that the file was successfully uploaded. We'll connect again with host paloalto.unileon.es at port 50500:

```
[paloalto] $ ssh -p 50500 student0@paloalto.unileon.es
```

7. When prompted, type your password, observe the prompt from the remote host and check the file was successfully uploaded:

```
[paloalto] $ ls  
copyofmyfile
```

8. Let's check the file contents:

```
[paloalto] $ cat copyofmyfile  
My valuable new file!!!
```

9. Close your session:

```
[paloalto] $ exit
```

So far, we have checked the remote access to host paloalto.unileon.es at port 50500 by using ssh and scp commands.