BI-SSB - Lab Manual 3
Install Cisco ACS in GNS3

1. Introduction

The Cisco ACS (Access Control Server) is a central point of management for managing switches, routers and other devices. It insures AAA services (Authentication, Authorisation and Accounting). In an enterprise network you need to define a lot of users for many administrators. For each user you need to define: username, password, certificate, privileges, rights, etc. If you have 1000 devices, to define them on each will be a pain. Thus you define them on the ACS and all the devices use RADIUS or TACACS+ protocols to complete the authentication.

Thus, instead of having authentication of administrators based on the local database of usernames and passwords (as we had it in the previous labs), we are going to use a preference list saying that we prefer to do the authentication based on the database stored on the ACS. When a user logs-in the router will send a request to the ACS to confirm if the credentials are OK and what rights are associated to the user.

There is however a best practice to define a simple local database containing a single username and password, with the highest privilege level (15) because in case the router cannot connect to the ACS, no administrator can log-in. By defining that local username, in case the connection to the ACS is lost, still the main admin can log-in and debug the problem.

2. Necessary Elements

For this lab you need the Windows XP virtual machine, VMWare Workstation (please download the trial version suited for your operating system), the ACS virtual machine (from your teacher) and the GNS3 lab (which you will build yourselves).

3. Installation

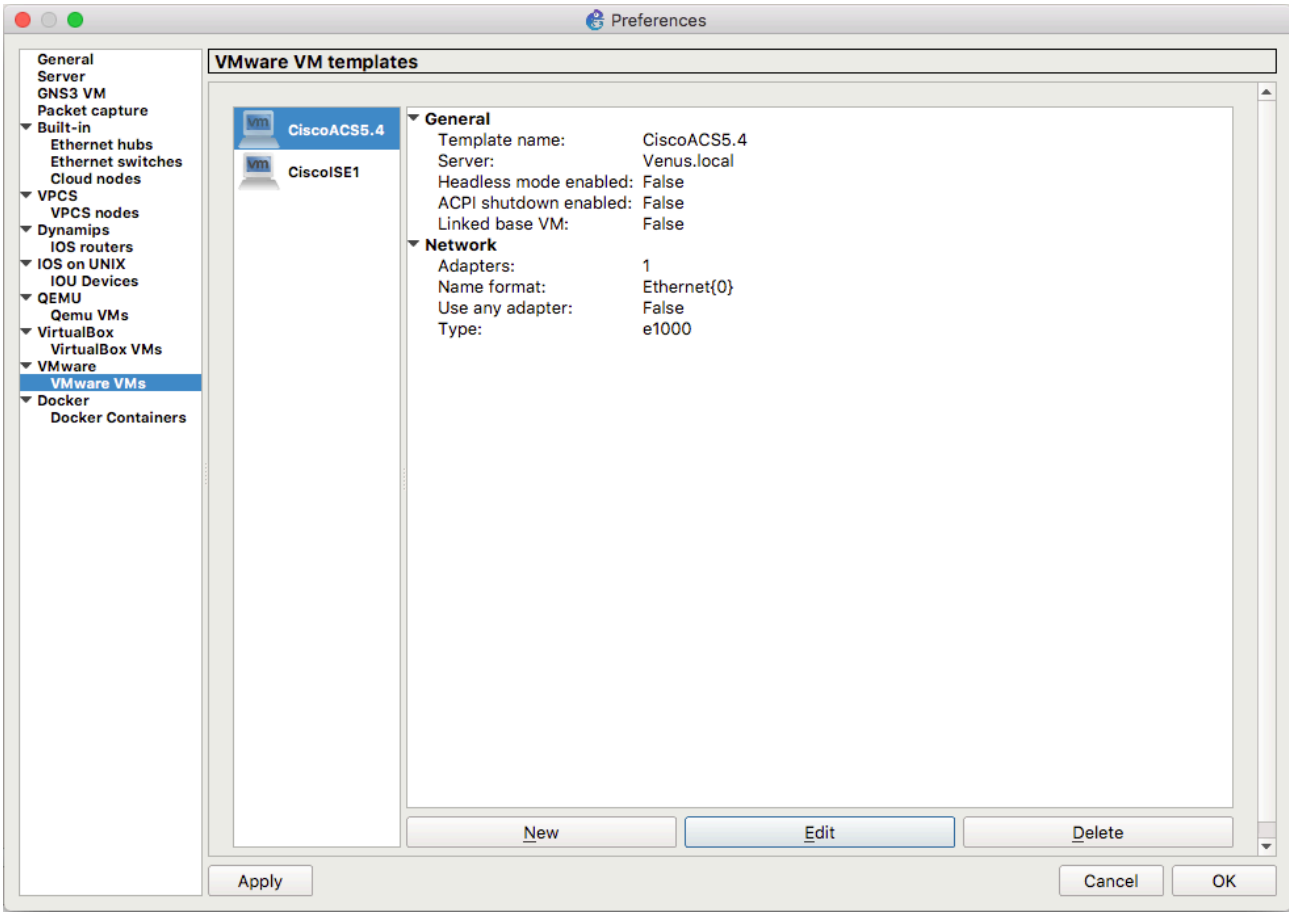
For this step we suppose you already have the GNS3, VMWare and Virtual Box installed. Also, we suppose that you have the router firmware 3725 in GNS3 and the Windows XP machine set up. The machine has the address 192.168.0.251/24.

Copy the ACS Virtual machine (from the teacher) on a known location on your computer.

Open VMware (Workstation or Fusion - depending if you are on a PC or a Mac, respectively). Click File -> Open and open the machine in VMWare. **DO NOT START IT FROM HERE!!!** Just open it.

Open GNS3. Under Preferences go to VMWare VMs and click New. From the list of VMWare virtual machines choose Cisco ACS5.4. Click Finish. The result is presented in Figure 1.

Figure 1 - The import of Cisco ACS VM into GNS3.



4. Goal

Goal: what we want if to use the ACS (Access Control Server) as a single point of AAA (authentication, authorisation and accounting). Before this lab, when we had to create a username, we created it on the router and then we specified the fact that we want to use the local database of defined usernames and passwords. For example, the Telnet configuration which we used looked like this:

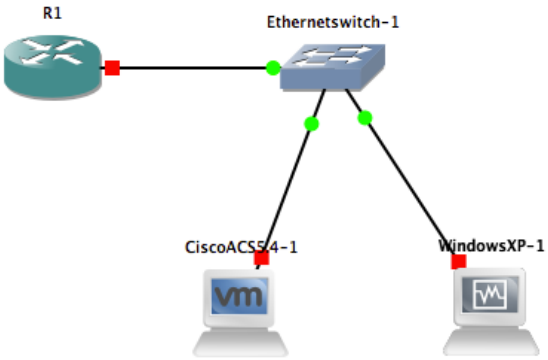
```
R-conf# username mama privilege 15 secret tata          //a locally defined username mama
R-conf# libe vty 0 15
R-conf-line# transport input telnet
R-conf-line# login local                                //telnet uses the local database
```

You realise that in a network of 1000 routers and switches we need to define all the credentials of all admins and users on each and every device. So we do it from a central location: the AAA server (ACS in this case). We have 2 protocols at choice: RADIUS (open source and more coarse) or TACACS+ (more granular but Cisco proprietary). We shall use Cisco TACACS+.

5. Building Your Topology

In GNS3 create a new project. Name it, for example BISSB-ACS. Add an ethernet switch and to it connect a 3725 router, the ACS VM and the Windows VM. Connect them with wires (as seen in Figure 2). This network will be 192.168.0.0/24 which represents your control plane network (the network on which you manage your devices). Of course, nothing prevents an ASA to be later added. ASA can make use of the ACS, too. Start the simulation. Be careful as it will eat your RAM alive.

Figure 2 - The topology

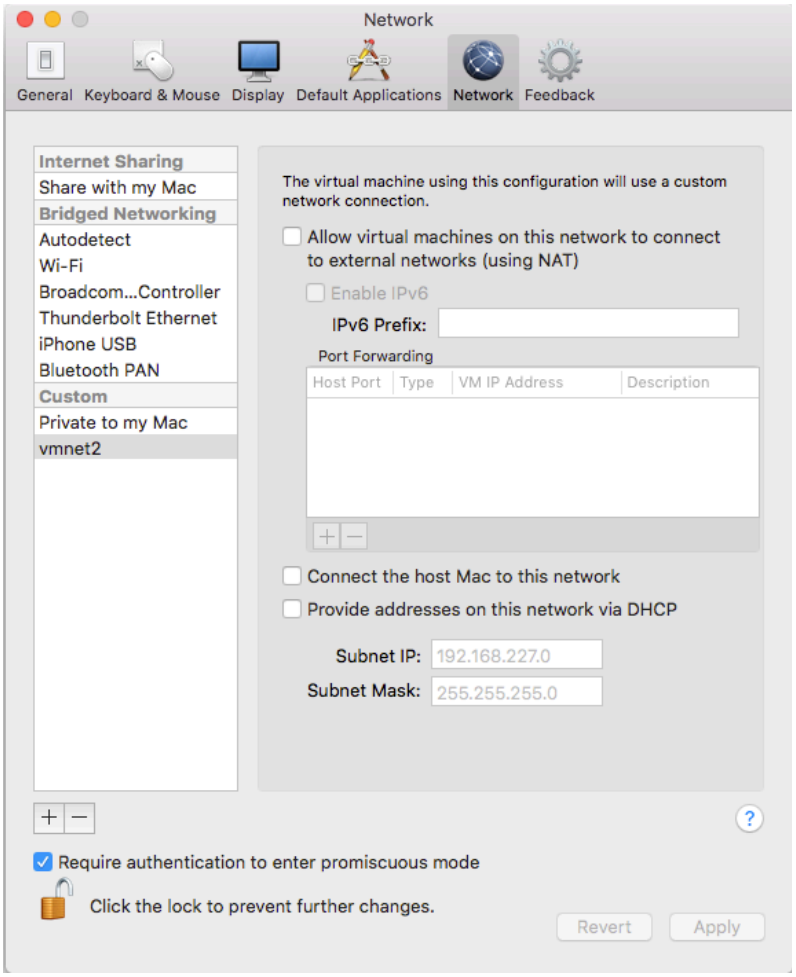


The router will be the supplicant (the one which has to authenticate the users), the ACS plays the role of the authentication server (AAA) and the Windows XP has the graphical interface to configure the ACS.

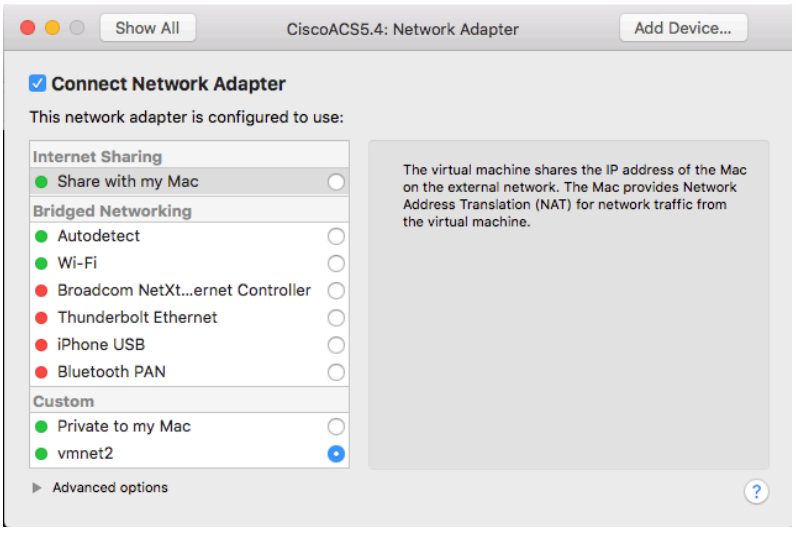
WARNING: It may happen that you are given by the GNS3 trying to start VMWare the following error: “No VMnet interface available between vmnet2 and vmnet100. Go to preferences VMware / Network / Configure to add more interfaces.” This is a network config mismatch between VMWare and GNS3.

Solution: Open VMware on your computer, go to the preferences of VMWare (Not those of the virtual machine). One tab will be Network. Add a private network; the name should be chosen by default as vmnet2 (by the system) - Figure 3. That is a virtual network bridge inside your computer. We do not need communication with the internet thus no NAT with any interface on the computer.

Figure 3 - The SVI (Switched Virtual Interface)

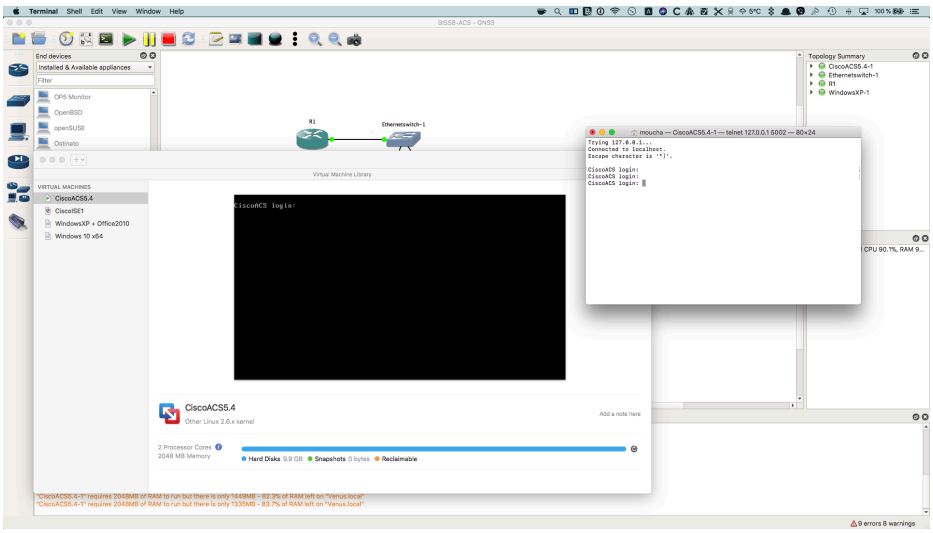


Go now on the preferences for the ACS in VMWare software and go under Network Adapter Settings. Make the network adapter of the ACS connect to the vmnet2, as in Figure 4.



Start again the machine from GNS3. It will prompt you to upgrade it. D**O NOT UPGRADE IT** and click NOT TO SHOW THE MESSAGE AGAIN. It will also prompt you with a modification notice. **Choose: “I copied it”.**

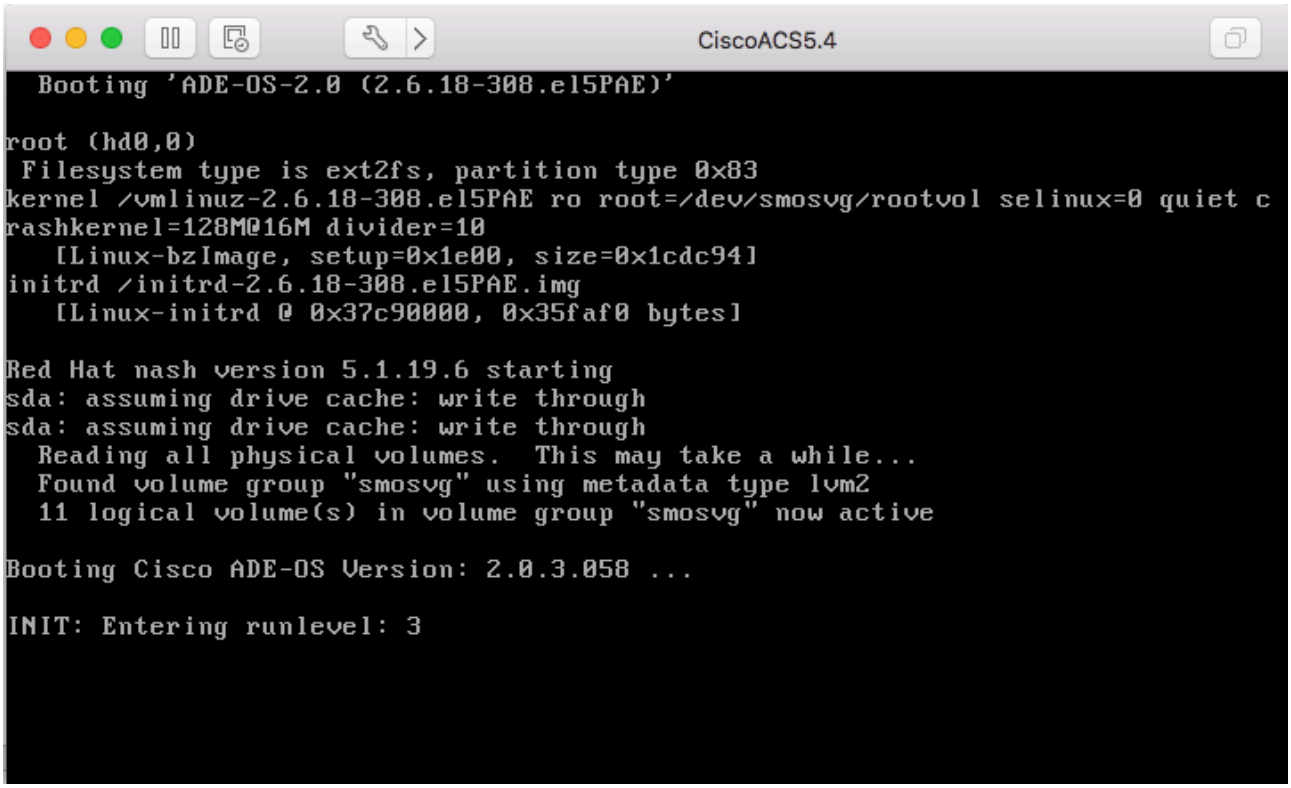
The ACS will boot up and prompt you with the login screen - Figure 5:



The login screen may be accessed from a new window of VMWare or the GNS3. I recommend you to use the window generated by GNS3 as it is native to your operating system. If you click on the VMWare window, your mouse will be stuck there and you need the escape sequence CTRL+ALT+ESC to get it out.

Do not close the VMWare windows as this will suspend the machine. Just leave them in the background or minimised. If you get stuck, just stop and start again the ACS from GNS3. Be careful that the ACS may spend a long time in this screen - Figure 6. Grab a coffee and wait.

Figure 6 - Patience is the virtue of the virtual network administrator.



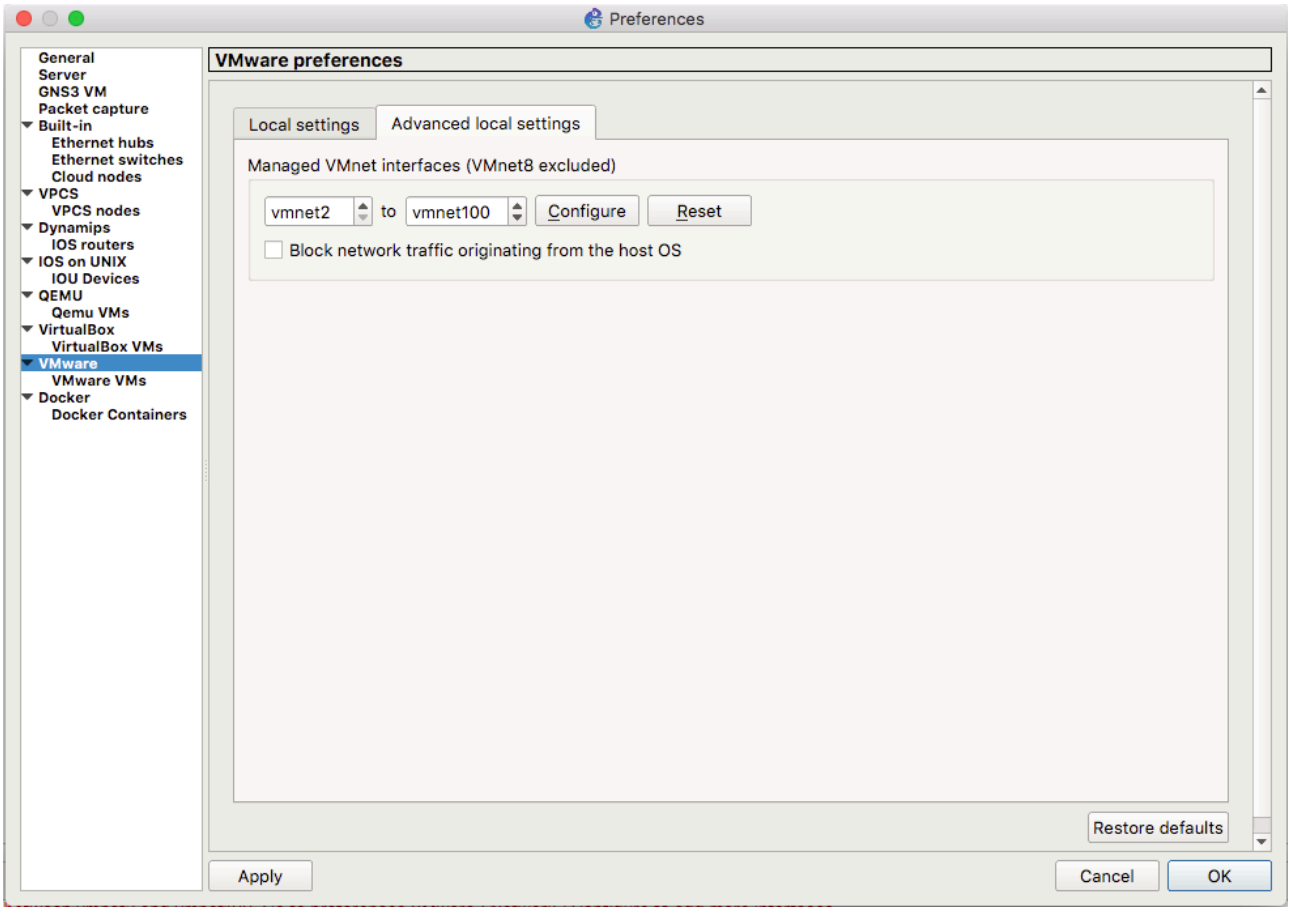
The CLI credentials are: username: admin ; password: student.

Play a little bit in the CLI. Try *show version*. Try "*?*" To see some commands. What do you see? A Cisco language on top of a Linux core. Yep: ACS runs Linus. As did ASA. This is also true on the real devices. So look: a Cisco IOS runs on top of Linux which runs on top of GNS3 which runs on top of your OS. Triple virtualisation.

The command *show ip interface brief*, etc are no longer available as this is not a router. Do a *show interface* and see that the IP address is 192.168.0.250.

Try the connectivity with Windows: ping ip 192.168.0.251.

If you have problems pinging, go to GNS3 Preferences -> VMWare -> Advanced local settings and reset the managed VMWare interfaces and unblock traffic originating from the host OS, as in Figure 7.



```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

CiscoACS login: admin
Password:
Last login: Sat Nov 25 15:58:57 on ttyS0
Copyright(c) 2012 Cisco Systems, Inc. All rights Reserved

CiscoACS/admin# ping ip 192.168.0.251
PING 192.168.0.251 (192.168.0.251) 56(84) bytes of data.
64 bytes from 192.168.0.251: icmp_seq=1 ttl=128 time=12.8 ms
64 bytes from 192.168.0.251: icmp_seq=2 ttl=128 time=1.37 ms
64 bytes from 192.168.0.251: icmp_seq=3 ttl=128 time=0.908 ms
64 bytes from 192.168.0.251: icmp_seq=4 ttl=128 time=0.728 ms

--- 192.168.0.251 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3275ms
rtt min/avg/max/mdev = 0.728/3.973/12.883/5.149 ms

CiscoACS/admin#
```

6. Configuring the Topology for AAA

On the XP machine open Firefox. Go to URL: https://192.168.0.250/acsadmin

The GUI credential is user: acsadmin with pass: student.

6.1. On the router we need to:

1. Configure the ip address. Put it: 192.168.0.1 /24.

R1-conf-if# ip address 192.168.0.1 255.255.255.0

And no shutdown.

2. Create a local username credentials. In case the contact between the router and the ACS is lost and you have no backup username list, you are now locked outside the router

R1-conf# username backup privilege 15 secret backpass

3. Activate the new authentication model (using external authentication server):

R1-conf# aaa new-model

4. Modify the preference login list (called default) to use the AAA server first and then local database of users.

R1-conf# aaa authentication login default group tacacs+ local
R1-conf# aaa authentication enable default group tacacs+ enable
R1-conf# aaa authorization exec default group tacacs+ local

5. Define a TACACS+ server:

R1(config)#tacacs-server host 192.168.0.250

5. Set a TACACS+ shared password (let us set it as “tacpass”):

R1-conf# tacacs-server key tacpass

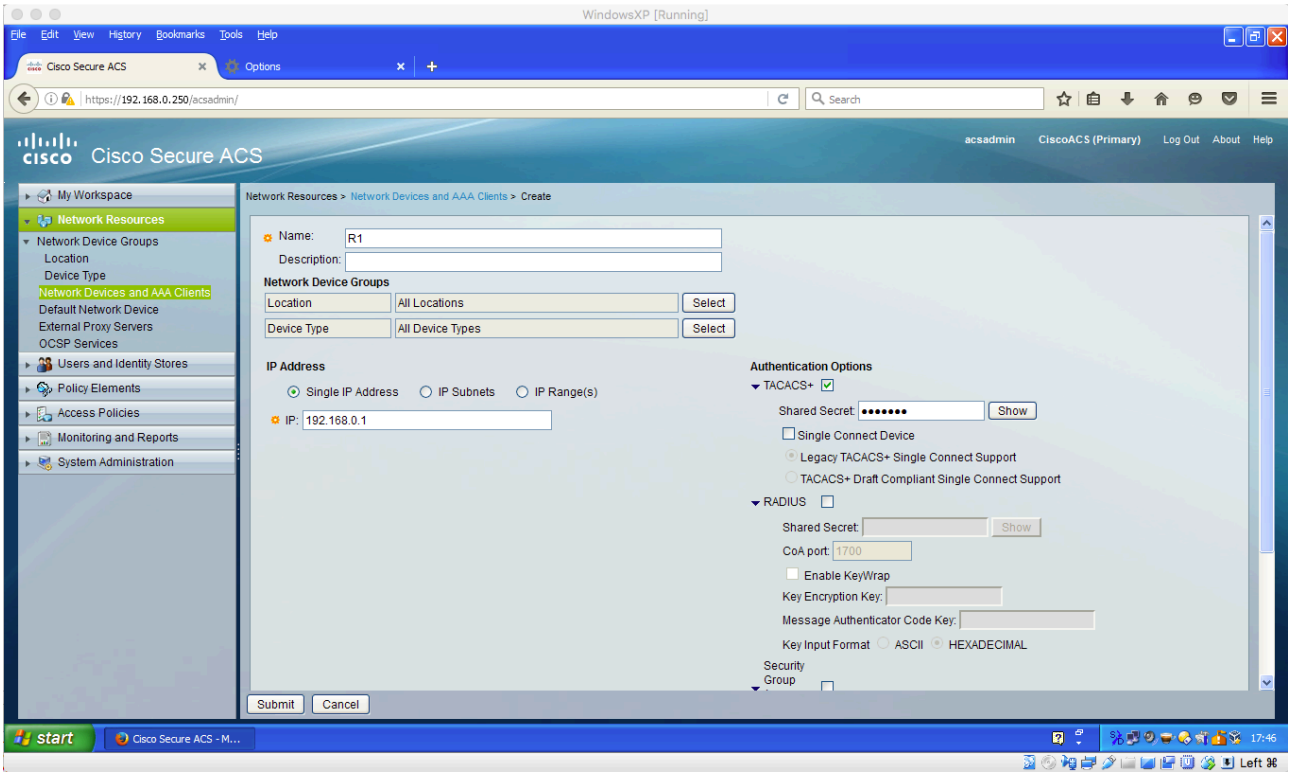
Do not forget to save the configuration: *R1# write memory*

6.2. On the ACS, using the GUI from the XP we need to:

1. Login to the Cisco ACS GUI: https://192.168.0.250/acsadmin

2. In the GUI, under Network Resources -> Network Devices and AAA Clients:

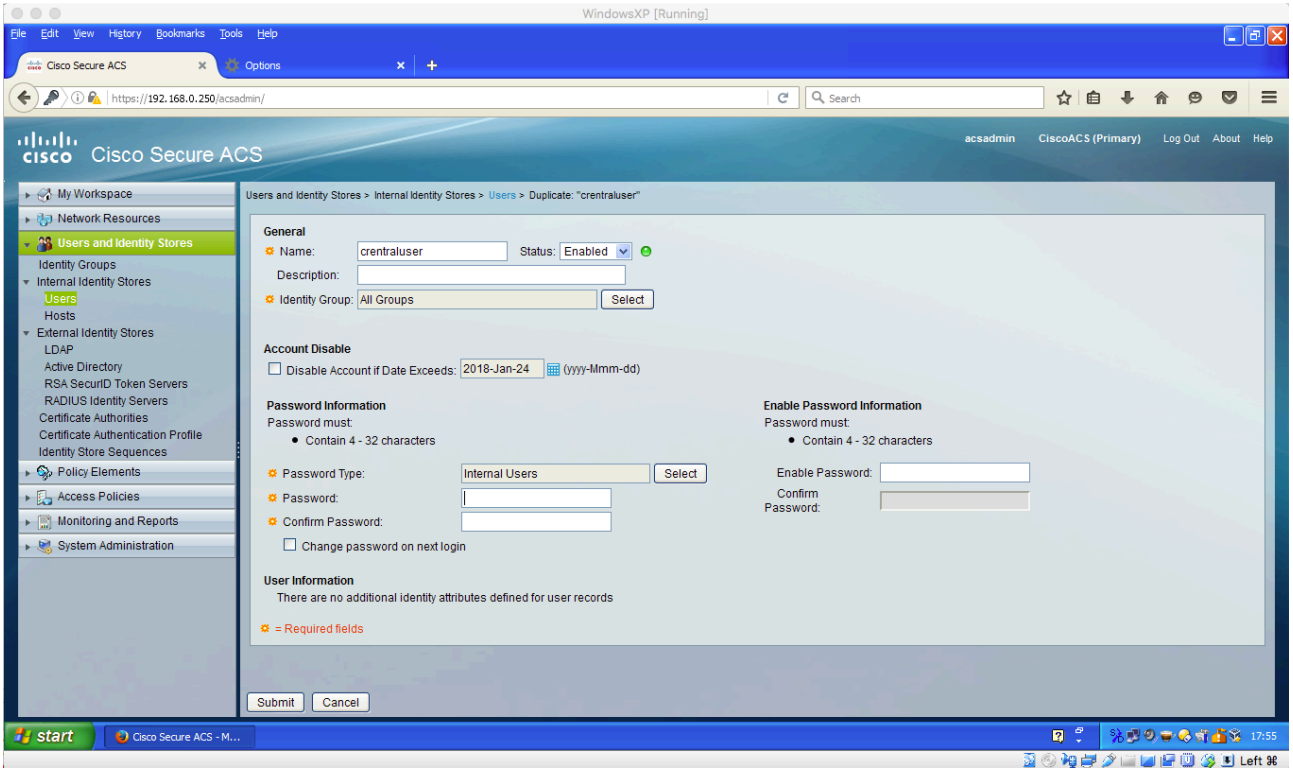
Create a device called R1, with the IP address 192.168.0.1, tacacs+ checked, tacacs+ password tacpass, as in Figure 8:



3. We define a username “centraluser” with password “centralpass” and enable password “enapass”:

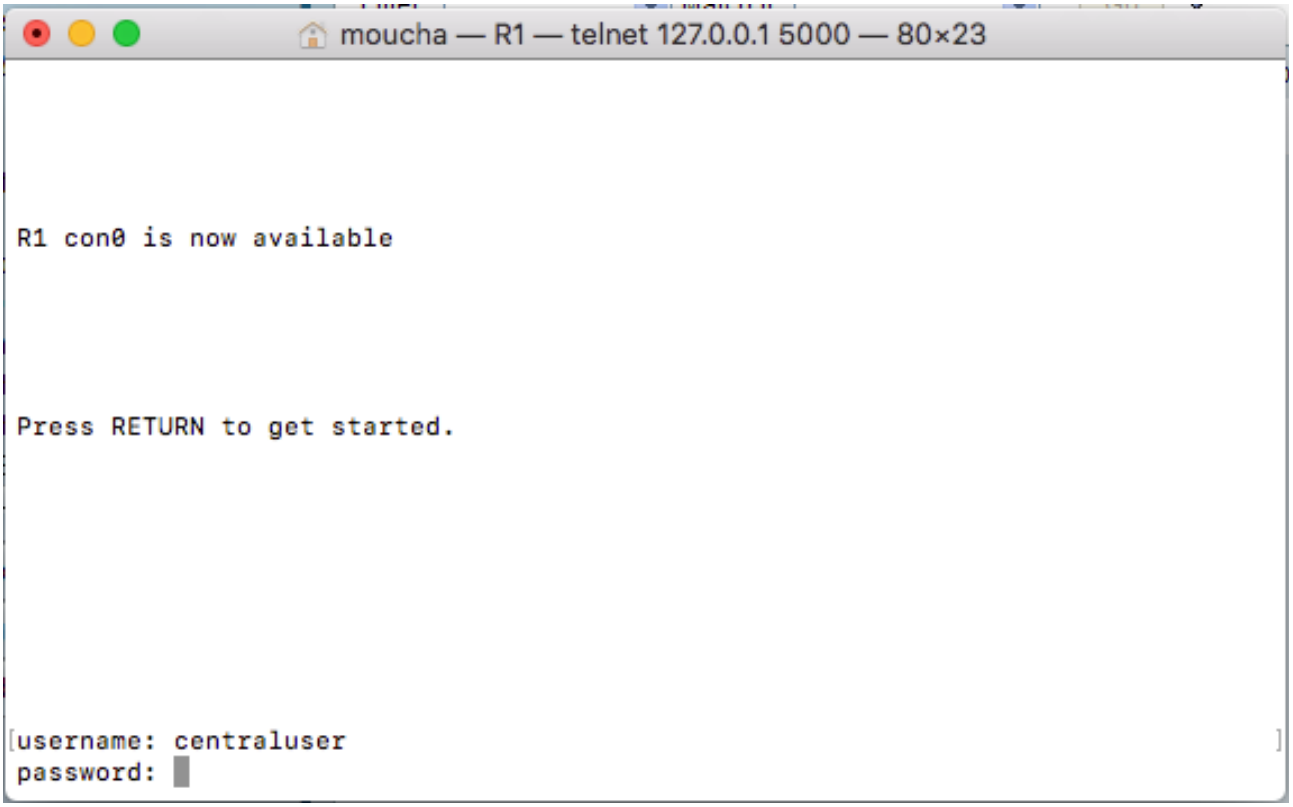
In GUI, under Users and Identity Stores -> Internal Identity Stores -> Users

Figure 9:



6.3. Testing

On the router exit all and try to login (Figure 11):



One more thing: delete the cable between the router and the switch. Try to login again.

You can create another user and click “change password at next login”. See what happens when you log in.

You can also add more routers, create a router group, define users for that group.

You may also try to allow centralised login users for TELNET or SSH by creating login preference lists on lines not on the login… The sky is the limit.

You now have an AAA lab ready. Do not forget that ACS is Cisco IOS like, thus to save the configuration you need to issue at the CLI ACS# *write memory*