Setting up a VPN using WIN2003 and XP; Linux and SmoothWall

Preparation

- A Linksys BEFW11S4 router
- Windows 2003 Advanced Server
- Windows XP professional (if possible, have one setup with out any service pack, another with SP2 installed for comparison purposes)
- WMARE Workstation software from http://www.vmware.com/products/ws they can provide an evaluation version that will last for 30 days, more than enough to finish the projects in this module.
- Download SmoothWall Express 2.0 from http://www.smoothwall.org/about/release/2.0.html , no need to burn the ISO image to a CD. The software is free.
- PC's with at least the following items: 256MB, PIV@1.8Ghz, 10 GB of free HDD space, the installed OS is of no concern, but it should run smoothly.
- The lab environment should have access to the Internet.
- Switches (2) are needed to create separate LAN segments or use VLAN's, so the students can demonstrate mastery of the subject.

Overview

This lab setup is conducive to individual learning because each student will be responsible for setting up a VPN server, the VPN client and develop the virtual network in just one PC. Allow and encourage the students to help each other, but ensure each one is doing their work. The network numbers here should be used once as part of the lesson, and then the student must come up with his own addressing scheme and repeat all the related steps, making sure each student has a unique addressing scheme using private IP numbers. This will get students thinking. Be ready, depending on your lab setup all of these virtual machines will be running on the same network segment. This will cause unpredictable results in the sense that one VPN might not connect no matter what is done, and the mistake will lie in something as simple as a wrong subnet mask. Be ready to spend plenty of time in troubleshooting. Showing how to troubleshoot is one of the goals, it will make students go beyond the usually perfectly controlled lab. Angry IP Scanner from http://www.angryziber.com/ipscan/ is a great tool, it gets a quick grasp of what IP addresses are already in use. It simply automates the process of pinging.

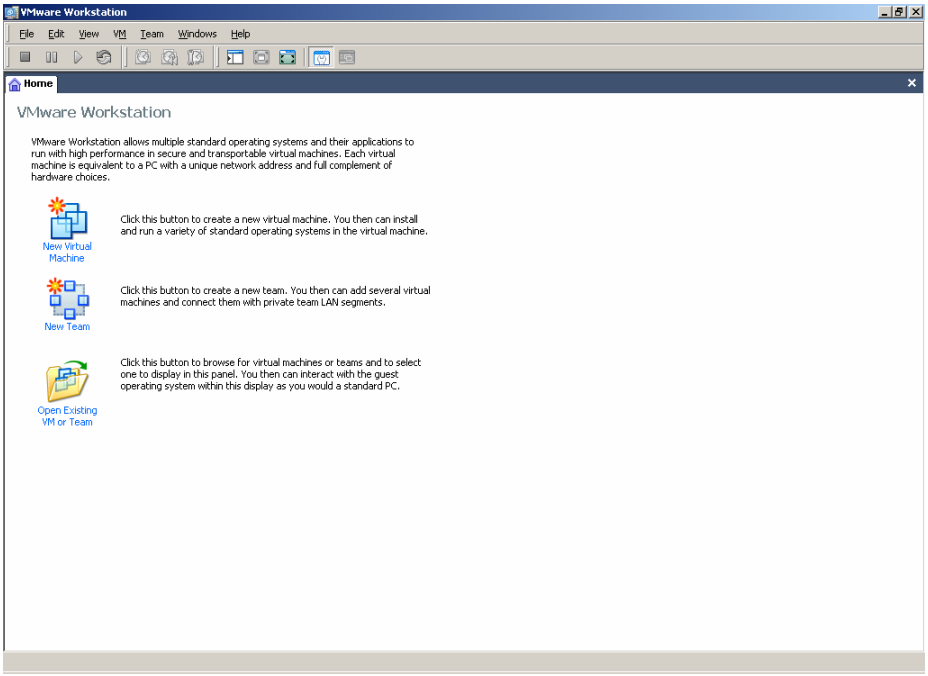
The VPN objective is to scramble (encrypt) the packet's contents as they travel over any kind of media. When using VPNs, the AP can be left completely open to everyone, and the security is established at the ends of the VPN tunnel. The client and servers are responsible for intrusion prevention. In reality, depending on your application, this layer of security could be enough. For the most part it is better to build a multilayered security system. Something that has not been mentioned so far: New malaware targets the endpoints, before the encryption is done by any security system. If any of the endpoints is compromised in any way, the network administrator has created a very secure venue for a virus to come in. Most firewalls/virus scanners can not inspect the traffic that travels inside the VPN: The malaware will not be detected.

A VPN is one type of security. It is pertinent to note that newer wireless AP can create a virtual LAN for each wireless client, and wireless clients can not see each other. Quoting from the router's manual:

> AP Isolation:
> Creates a separate virtual network for your wireless network. When this feature is enabled, each wireless client will be in its own virtual network and will not be able to communicate with each other. You may want to utilize this feature if you have many guests that frequent your wireless network.

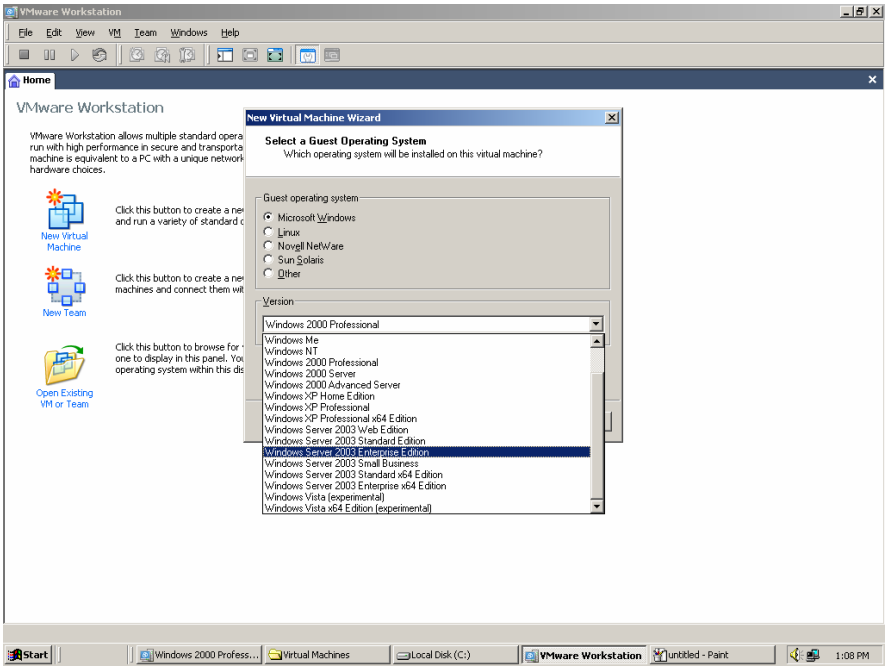
Part I: Setup a VPN using Windows Server 2003 Enterprise Edition and XP

1. Download and install VMWare
2. Once installed, click on the “New Virtual Machine” Icon.



Screenshot 1

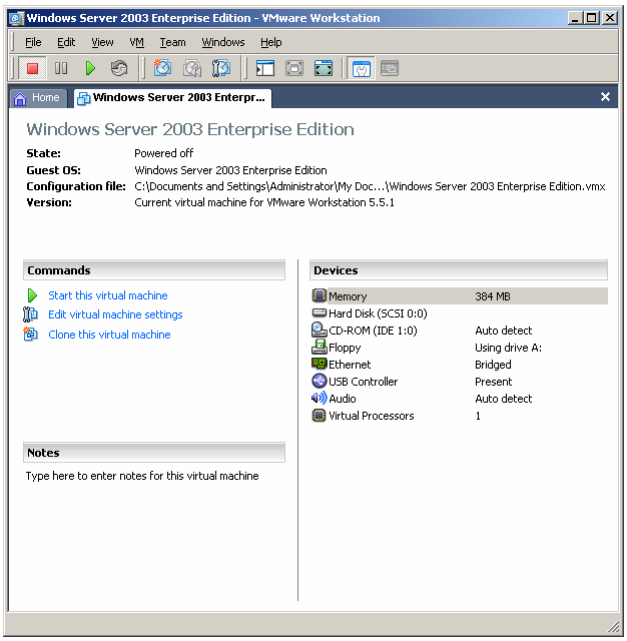
The New Virtual Machine Wizard displays



Screenshot2

3. Choose your operating system from the Version drop-down list.
   In our scenario, we are using Windows Server 2003 Enterprise Edition.

   The Windows Server 2003 Enterprise Edition – VMWare Workstation window displays

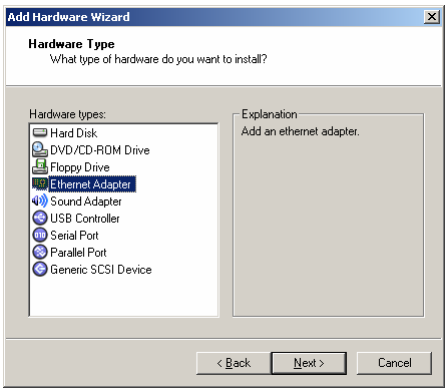


Screenshot3

The virtual machine needs 2 NIC cards

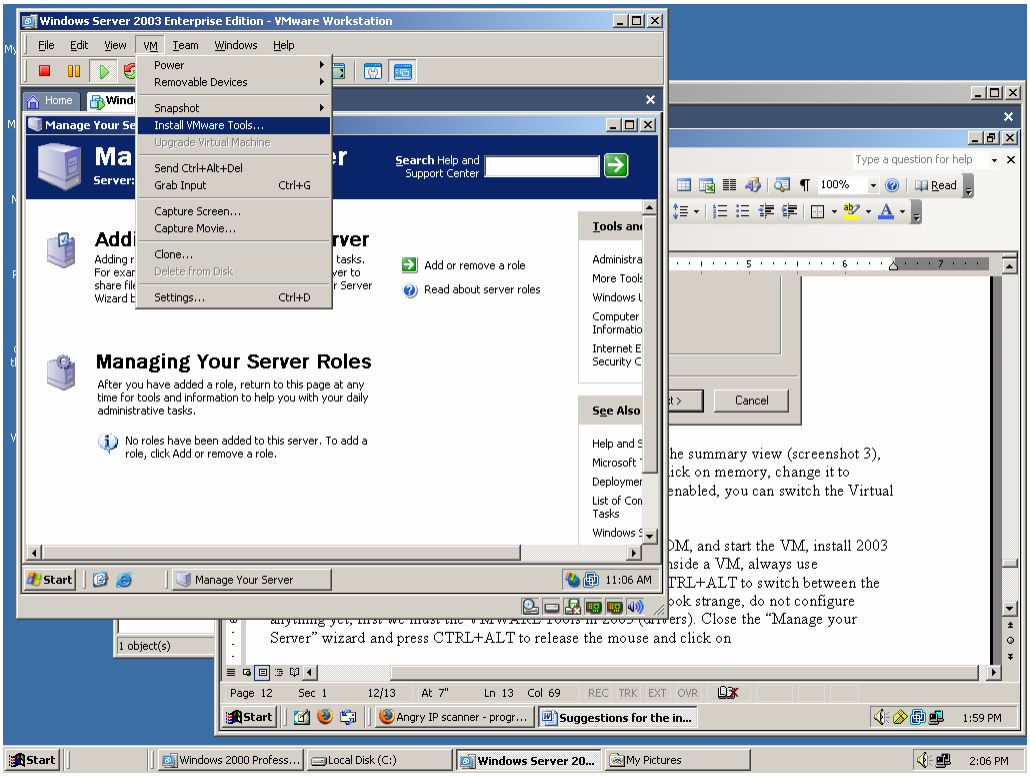
- One will simulate the intranet
- The second one will simulate the Internet.
- The amount of RAM should be decreased.
  The intent is to run several virtual machines at the same time in the same PC, so RAM will be scarce if you only have 256MB of physical RAM.

4. Under the Commands group in the left pane click “Edit Virtual Machine Settings”;
5. Click Add…
   The Add Hardware Wizard displays



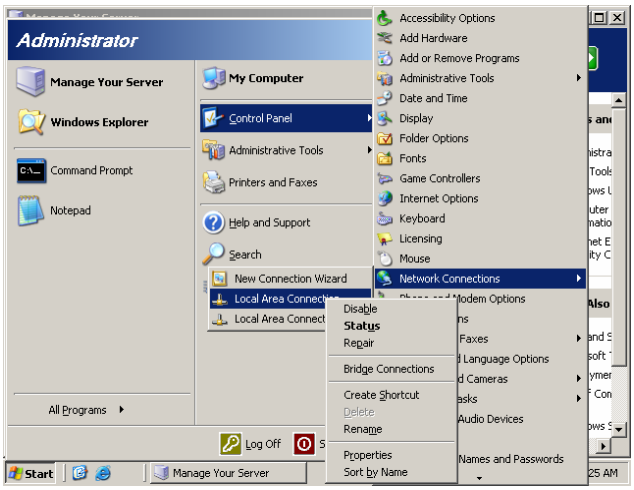
Screenshot 4

6. Click Ethernet Adapter
7. Accept the default values on the rest of the screens until you are returned to summary view (screenshot 3), you must now see listed 2 Ethernet adaptors. Under Devices click on memory, change it to 128MB. If you have the hyper-threading option available and enabled, you can switch the Virtual Processors option to two.
8. Insert the Windows Server 2003 Enterprise Edition CD in the PC’s CD-ROM, and start the VM.
9. Install 2003 with the default options.
   - When we are dealing with anything inside a VM, always use CTRL+ALT+INS instead of CTRL+ALT+DEL as needed, or CTRL+ALT to switch between the VM window and the actual OS.
10. Once done, the screen might look strange, do not configure anything yet, first we must the VMWare Tools (drivers) in 2003.
11. Close the “Manage your Server” wizard and press CTRL+ALT to release the mouse and click on the VM menu, followed by install VMWare tools (See screenshot 5 on the next page).
12. Accept the default settings on all of the following screens (do not cancel).
    - You might get a note regarding setting hardware acceleration, it is important to proceed accordingly. Hardware acceleration can be set either before restarting or afterwards.



Screenshot 5

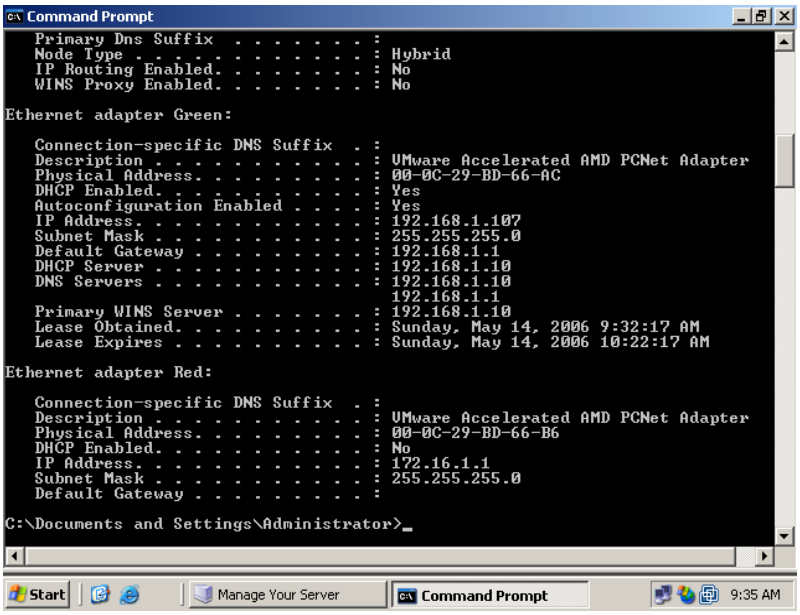
13. Time to start the VPN setup process: There are different procedures; we will follow one that uses the wizards provided in 2003.
14. As always, before anything is done, it is best to setup the network topology.
    - Just as a comment, the host name for the server is 2003ONVMWare.
    - By now we have a server with 2 NIC's, one is going to be the outside interface or RED interface, the other one is going to be the GREEN interface or the internal interface.
    - It does not matter which one is which, because VMWare has virtualized them and these NIC are now connected to the same network segment.



Screenshot 6

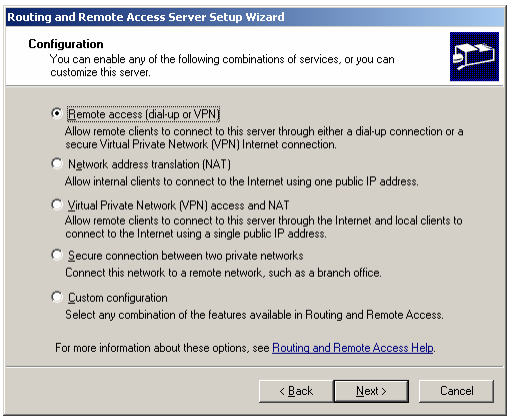
15. Look at screenshot 6, notice the two installed NICs.
16. Rename one NIC to RED, the other to GREEN, it will simplify the visualization process of the network topology, and these names will be used from now on when we refer to them.
17. Change the IP address on the RED interface to 172.16.1.1/24
    - The info related to gateway and DNS can be left blank.

18. Once done, the information for the RED interface has to follow the information in the following screen shot (the ipconfig /all command provided the info)
    - The GREEN interface should have the needed information to allow the server to connect to the Internet, and it will vary:



Screenshot 7

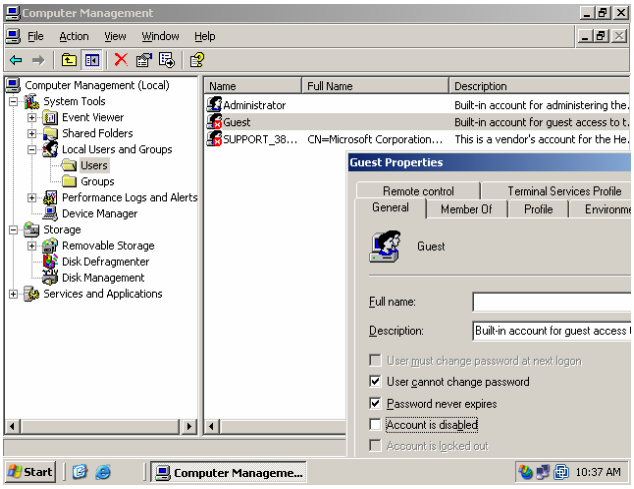
19. Now, time to setup the VPN and other related services.
20. If needed open the “Manage My Server” window
21. Click on “add or remove a role”
22. Choose “Custom configuration” on the next screen
23. Choose Remote access/VPN server
24. You will click Next two times
    - Windows Server 2003 Enterprise Edition CD might be needed.
25. Choose the option “Remote access [dial-up or VPN] listed below (Screenshot 8):



Screenshot 8

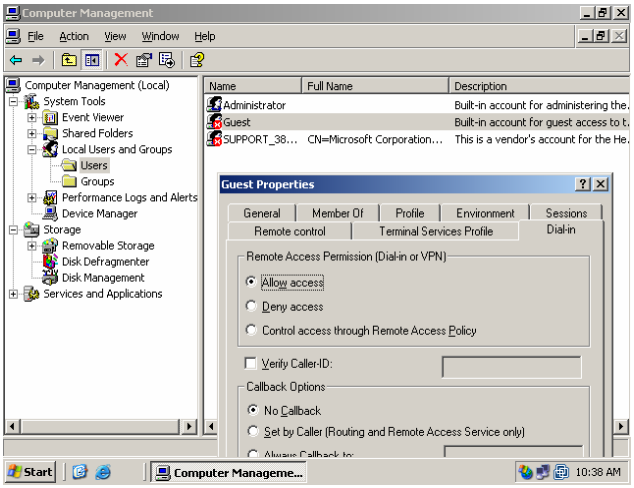
26. Click Next
27. . On the next screen select the VPN option and click Next.
28. Choose the Red interface, and click Next.
29. Choose “Routing and Remote Access to authenticate requests”.
    - The Radius option will be use later on in a different lab.
30. Notice the messages:
31. Click Finish and wait 4 hours/
32. Right-click My Computer and select Manage

The Computer Management window displays



Screenshot 9

33. For simplicity sake (this is not a good policy in a production environment),
    - The Guest account has to be enabled, and
    - The Dial In Tab has to have “Allow Access” enabled.



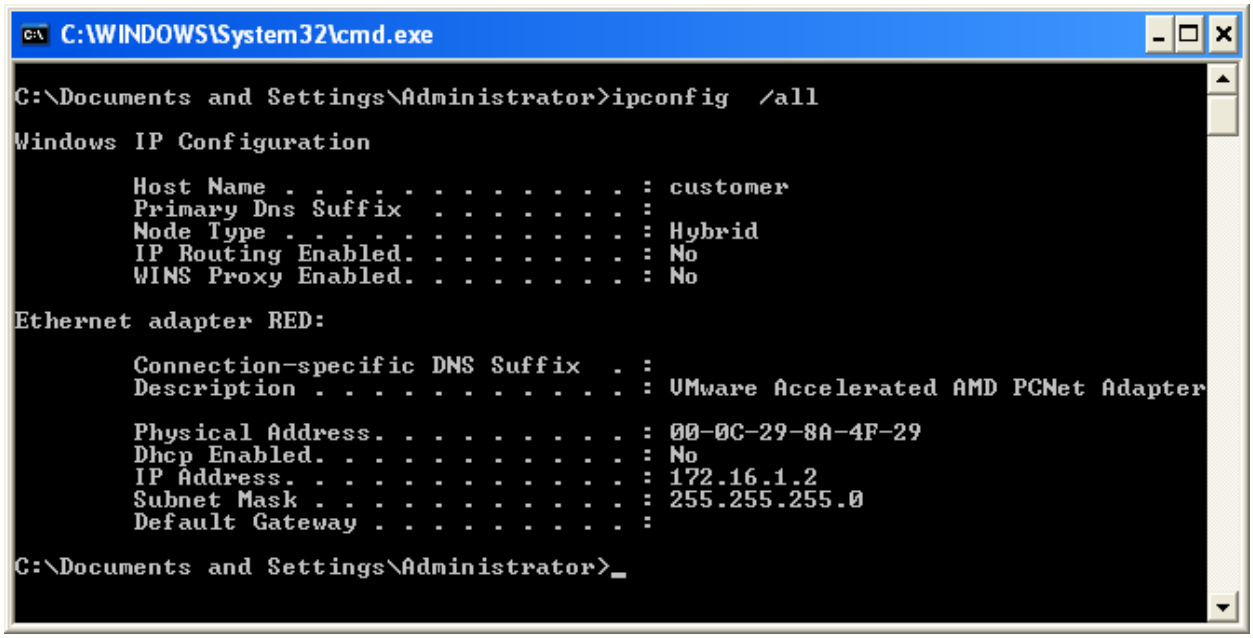
Screenshot 10

34. Once those two options for the Guest user have been set, click on Apply/OK.
35. Just in case, go ahead and reboot the server so all the changes are accounted.

Part II: Setup Windows XP

By now the student should be able to setup on his own Windows XP VM by extrapolating the information given in the above section.

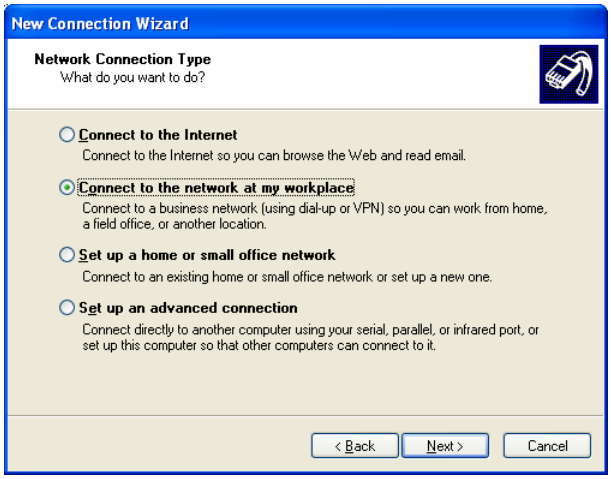
1. It is suggested to allocate 64MB of RAM and use only one NIC card for this virtual machine.
2. Rename the NIC to RED, and after setting up, it should look similar to the following screenshot.



Screenshot 11

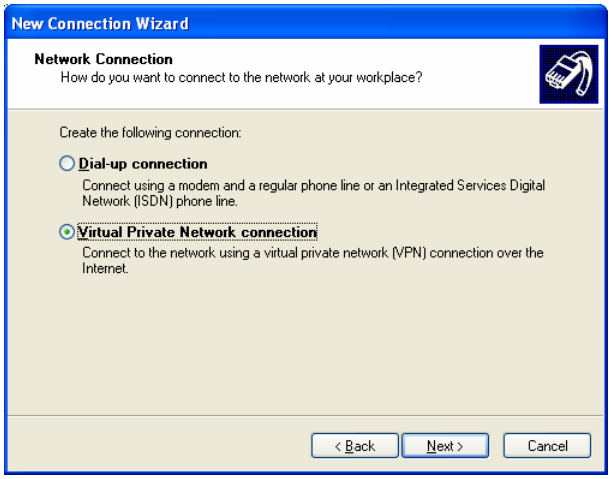
Notice: No gateways and DNS numbers are configured.

3. Setup a new connection in XP.
   - As you through the Wizard, look for the screen below, and choose the second option.



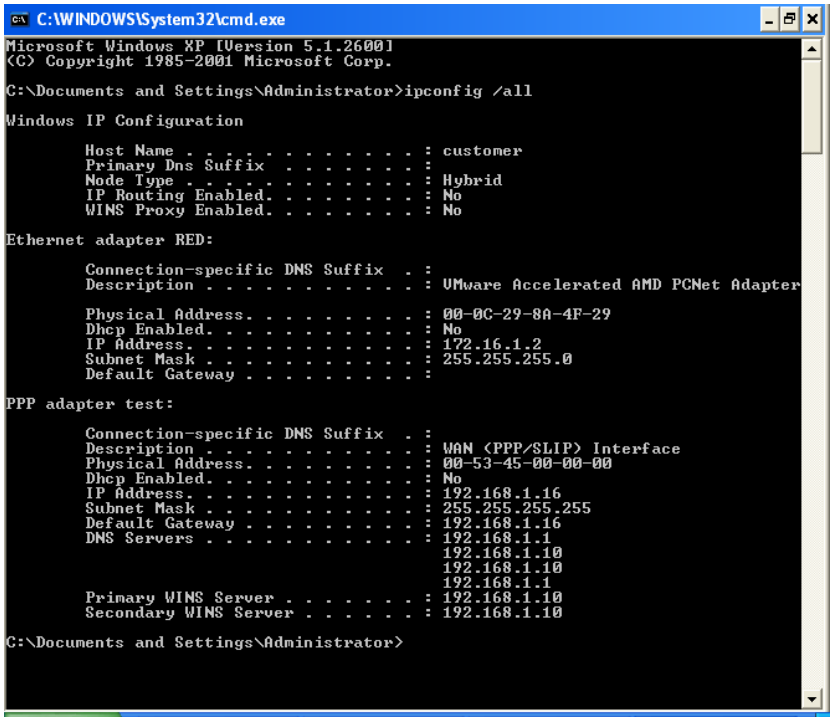
Screenshot 12

4. On the following screen choose:



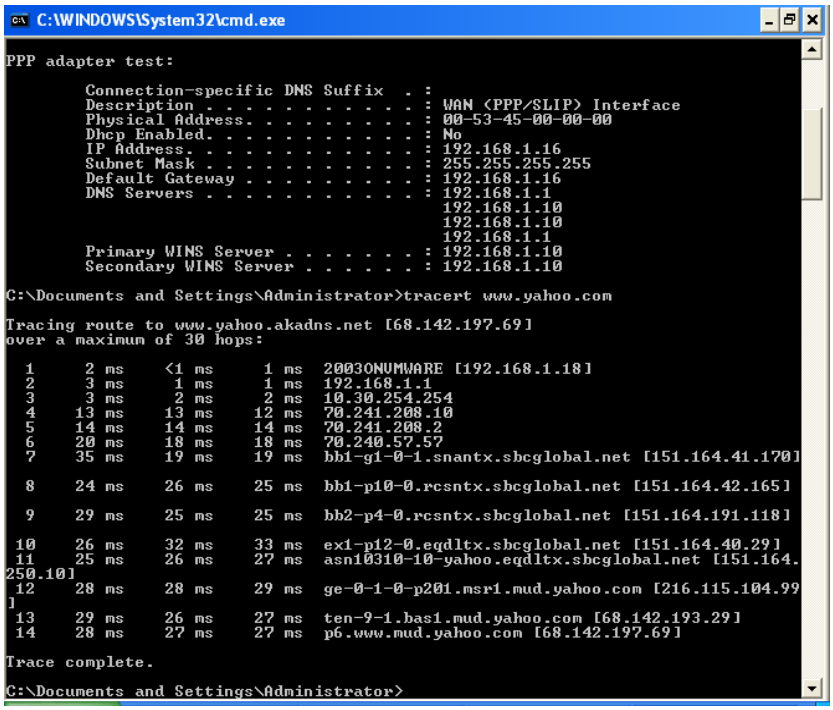
Screenshot 13

5. In the screen regarding the connection name, enter “test”.
6. For the screen regarding hostname or IP address enter 172.16.1.1
7. Select the option of adding a shortcut on your desktop
8. Click Finish
9. Double click on the Desktop icon.
10. In the connect test window
    a. Enter Guest for the username
    b. Leave the password blank.
11. Enter `ipconfig /all` in the CMD prompt.
    - The results should look similar to screenshot 14, found on the next page



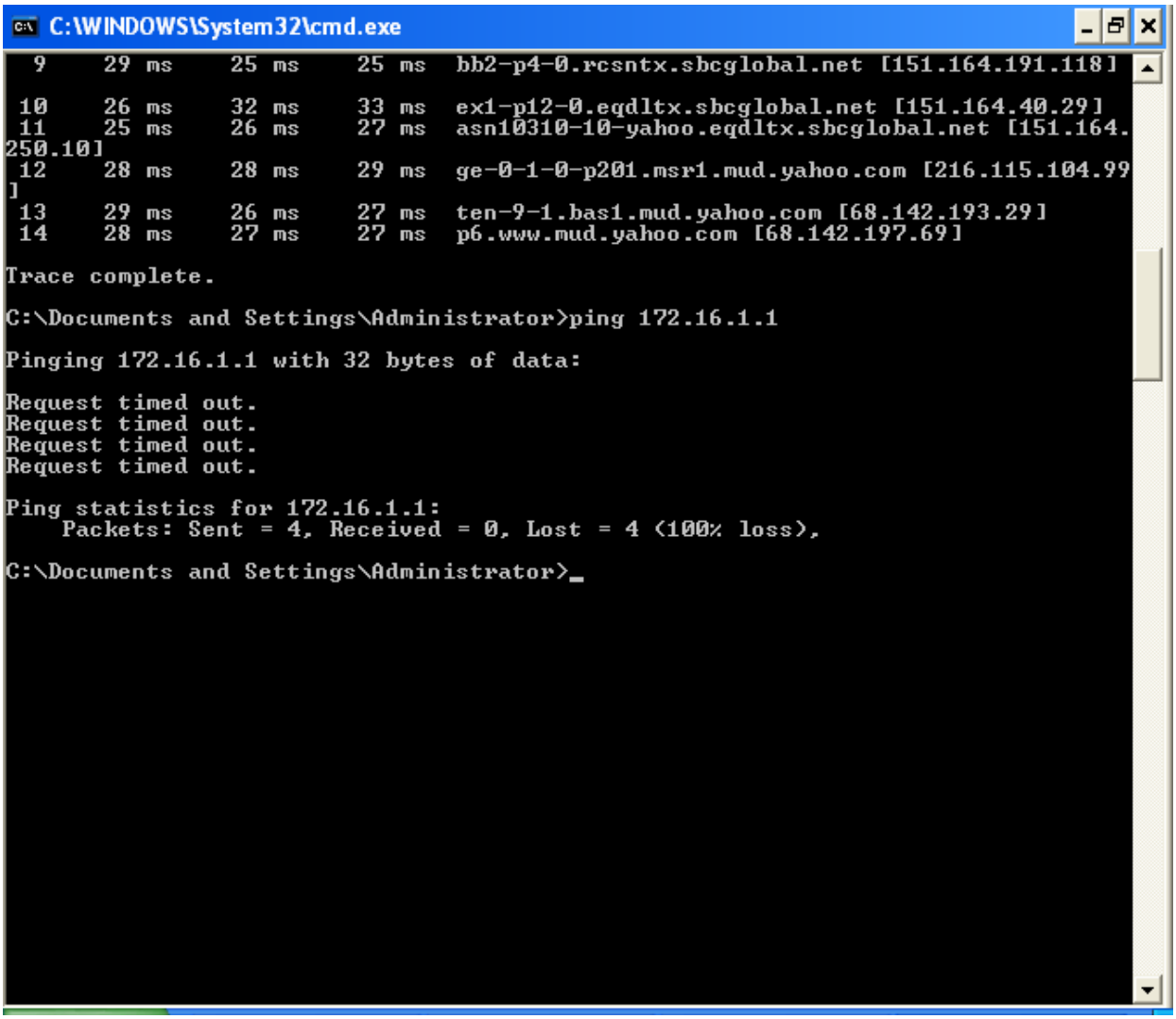
Screenshot 14

12. Enter the command `tracert www.yahoo.com`.
13. Compare the results with Screenshot 15.
    - Notice the route of IP addresses (or hops) the packets are traveling through to reach the server hosting www.yahoo.com.



Screenshot 15

14. Look at the following screenshot:



Screenshot 16

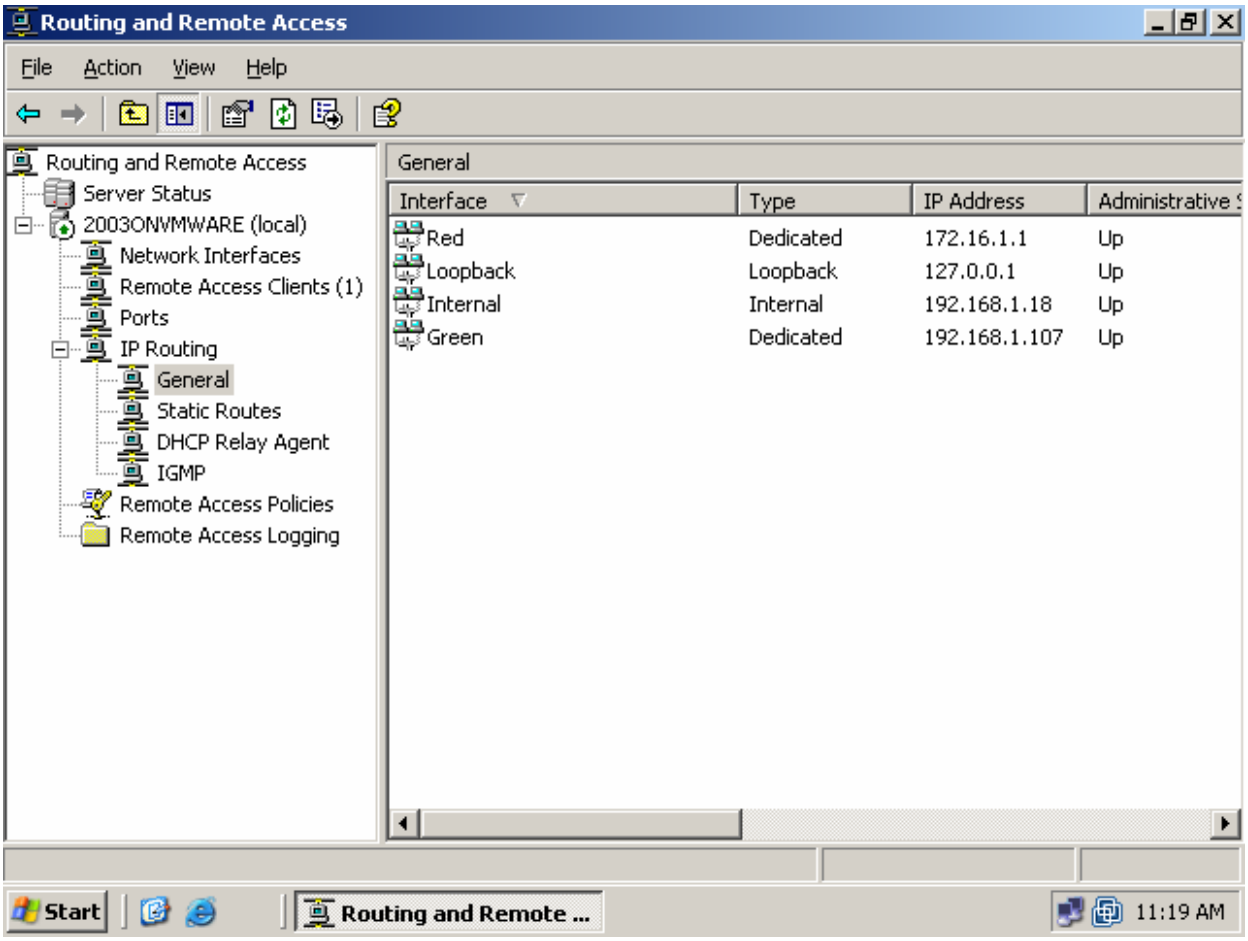
15. Can you explain why? Are you getting the same results?

16. Look at the IP addresses assignment provided by the local DHCP server running on the 192.168.1.X network segment.

```
Client IP Address  Name          Lease Expiration      Type   Unique ID Description
192.168.1.1        bad_address   5/19/2006 1:34:39 PM  DHCP   0101a8c0  This address is already in
use
192.168.1.2        01e306.       5/19/2006 2:34:53 PM  DHCP   000c298ed6f1
192.168.1.3        onvmware.     5/19/2006 2:45:46 PM  DHCP   000c29213e16
192.168.1.5        01e306.       5/19/2006 1:50:31 PM  DHCP   000c29087c72
192.168.1.6        2003onvmware  5/19/2006 2:30:06 PM  DHCP   RAS
192.168.1.7        2003onvmware  5/19/2006 2:30:12 PM  DHCP   RAS
192.168.1.8        01e306.       5/19/2006 2:27:34 PM  DHCP   000c296df01a
192.168.1.9        2003onvmware  5/19/2006 2:30:17 PM  DHCP   RAS
192.168.1.10       bad_address   5/19/2006 2:14:42 PM  DHCP   0a01a8c0  This address is already in
use
192.168.1.11       2003onvmware  5/19/2006 2:30:23 PM  DHCP   RAS
192.168.1.12       2003onvmware  5/19/2006 2:30:28 PM  DHCP   RAS
192.168.1.13       2003onvmware  5/19/2006 2:30:34 PM  DHCP   RAS
192.168.1.14       e30603.       5/19/2006 2:23:03 PM  DHCP   001111655801
192.168.1.15       2003onvmware  5/19/2006 2:30:39 PM  DHCP   RAS
192.168.1.16       2003onvmware  5/19/2006 2:30:45 PM  DHCP   RAS
192.168.1.17       2003onvmware  5/19/2006 2:30:50 PM  DHCP   RAS
192.168.1.18       2003onvmware  5/19/2006 2:30:56 PM  DHCP   RAS
192.168.1.19                     5/19/2006 2:29:42 PM  DHCP   00b0d0d08002
192.168.1.107      2003onvmware. 5/19/2006 2:29:38 PM  DHCP   000c29bd66ac
192.168.1.155      customer.     5/19/2006 2:14:45 PM  DHCP   000c298a4f29
```

a. What is the IP address assigned to the XP machine?
b. Under what host name is it registered?
c. How many IP’s is the server using?
d. We never installed a DHCP server, how is the XP machine getting its IP?

17. This screenshot comes from the Windows Server 2003 Enterprise Edition, as we look at the IP Routing section:



Screenshot 17

a. To which network does the Windows XP machine belong?
b. Recall that the RED interface is the one connected to the Internet, and we did not configure a gateway, nor a DNS. Yet both Windows XP and the server have access to the Internet, why?

18. Draw a map showing the network numbers and logical connections between these machines.
19. Do the same and make a map showing the actual topology.
20. All the NIC's are on the same network segment, this is never a good production policy. Why?
21. The student should now setup Windows Server 2003 Server and XP machine, and repeat these steps using their own network numbers.
    - As a suggestion, the students could use 172.16.XX.Y, where the XX represent the last two digits of their ID number as the network number used for the RED NIC cards.

22. From this point on and until the remainder of this lab, an AP is considered a to be a device that has a router/gateway, a wireless AP plus a small Ethernet switch connecting 4 LAN; and all this is bundled in the same box. What follows next is to use the AP in conjunction with all these setups. An open AP is the default setting for most of them. To understand the different interactions that could happen between an AP and this network, ask the students to now connect the AP to the network segment. Quick points to consider as the students setup these items:
    - The WAN interface will be setup as part of the RED network. The WAN interface is the usual label given to the interface that gets connected to the ADSL/Cable modem.
    - On this setup, on the LAN side, should the DHCP server be left on?
    - Setup a laptop or a PC wireless connection to link to the AP first, and then setup the VPN.
    - What would happen if the WAN port (or side of the AP) has the same network number as the LAN side of it? For example: The IP for the WAN port is 192.168.1.1 and the IP of the LAN interface is 192.168.1.254.
    - Real life scenario:
      The cable modem dynamically supplied this information to the WAN port of the AP:
      IP: 10.27.40.55/24
      Gateway: 10.0.0.254/24
      DNS: 192.168.1.1/24

      The LAN side had this information:
      LAN IP Int. 192.168.1.1/24

      The computer connected to the LAN side (used 1 of the 4 ports available) got this information from the AP
      IP: 192.168.1.100/24
      Gateway: 192.168.1.1/24
      DNS: 192.168.1.1/24
      DHCP server: 192.168.1.1/24

      The PC directly connected to the modem worked OK, but if the router was placed in the middle, it failed. Why? This problem was corrected by changing one network number (it automatically changes when the IP is changed), which one should be changed?

    - We have mentioned that a typical wireless router is actually 3 devices bundled together: An AP, a router, and a switch. How are these connected? Draw a topological map of these connections.

http://www.naphill.org/points/scrolls/scroll04.asp

Part III: Setup a VPN using Linux

SmoothWall is distributed as an ISO image (see http://en.wikipedia.org/wiki/ISO_image for more info on ISO images), and VMWare has a nice feature regarding ISO images. We will use this it later.

The "Smoothies" are designed to run on old Pentium I machines, and they can do very good job in sharing your dial up connection. In case of emergency, you can keep mail going with a Smoothie and a Dial Up connection. With the build in transparent WWW caching feature, it can make that dial-up connection seem "surprisingly fast". Do not be misguided; any Pentium I machine has more computing power than your regular cable/DSL router, with far more RAM resources. Smoothies can move network information quite fast. If later on somebody is interested in physically building one, use NIC's from either 3COM's 3c90X series or Intel Pro 10/100 series to get the best results.

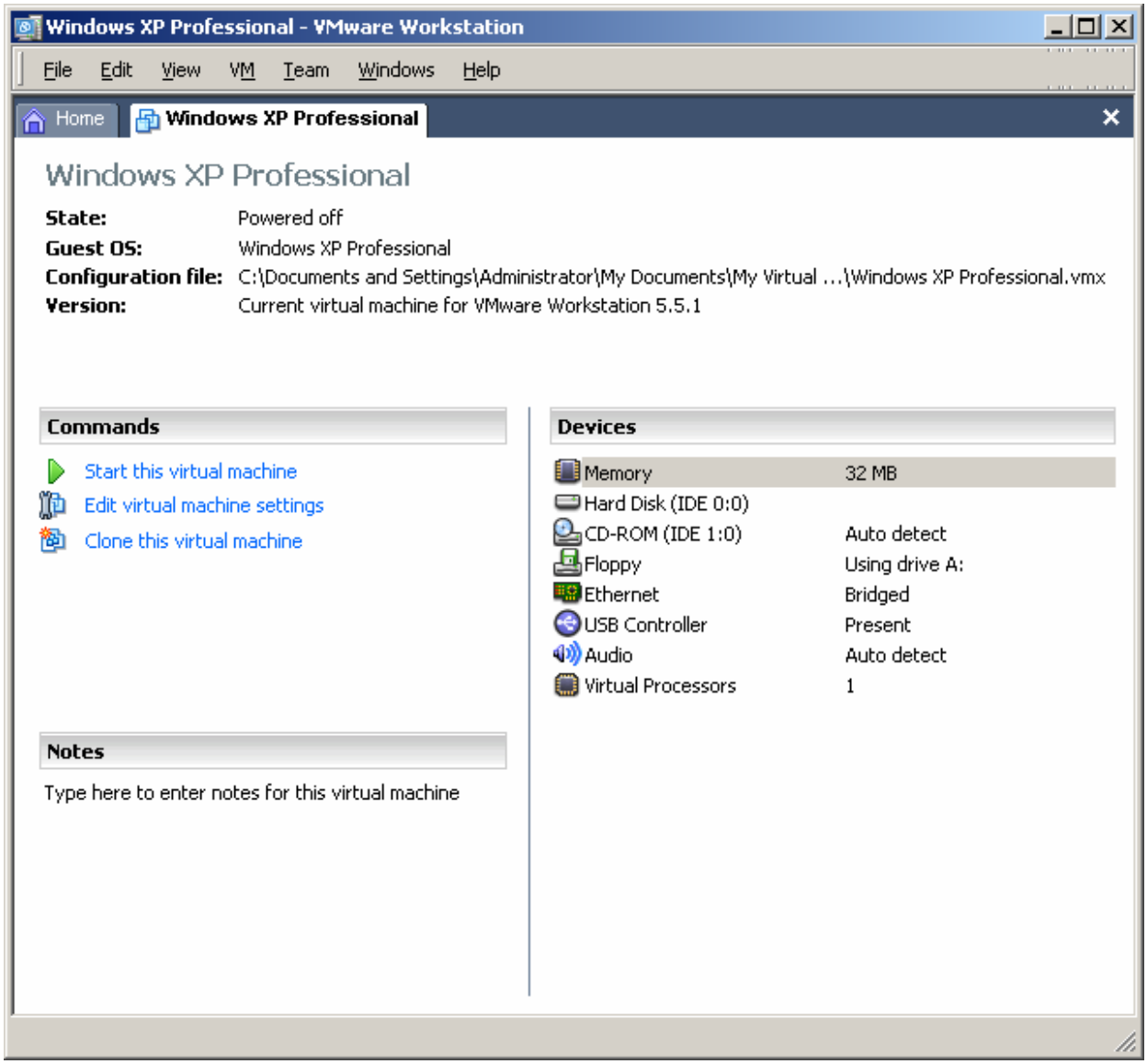
We need two virtual machines with the SmoothWall software, but we will set it up only once. Later on we will simply copy the finished virtual machine and have two up and running. Each Smoothie (SmoothWall) will be in charge of one end of the VPN

To setup the Virtual machine that will contain the Smoothie software we must have the following characteristics:

- 2 NIC's
- 32 MB of RAM (we can go as low as 8MB, but let's be generous)
- The virtual HDD must be the IDE type.

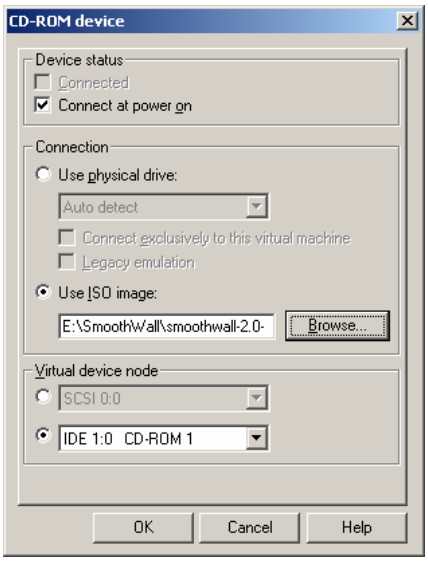
Installing the Smoothie in the virtual machine.

1. Start by creating a virtual machine based on Windows XP Home edition.
   - The reason behind this is that XP does not recognize the SCSI hardware that VMWare provides for better performance. VMWare is aware of this, so the hardware provided in the VM for XP has an IDE controller; just what the Smoothie uses saving us one extra step.
2. Add 2 NIC cards; again one of them will be RED, the other GREEN in the future.
3. Your screen should look similar to the Screenshot 18 shown on the next page.



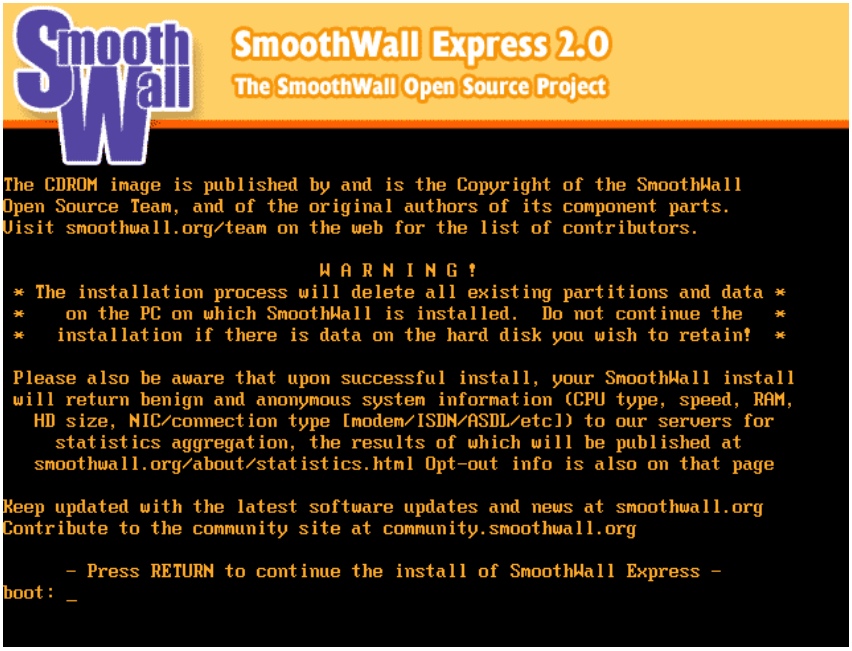
Screenshot 18

4. Under the Devices group in the right pane,
   - Double click on CD-ROM
   - Choose ISO Image
   - Browse and open the ISO image downloaded from the SmoothWall website.
   - Before you click OK, your screen should look similar to Screenshot 19, shown on the next page.



Screenshot 19

5. Start the virtual machine
   - The following screen should come up after a while:

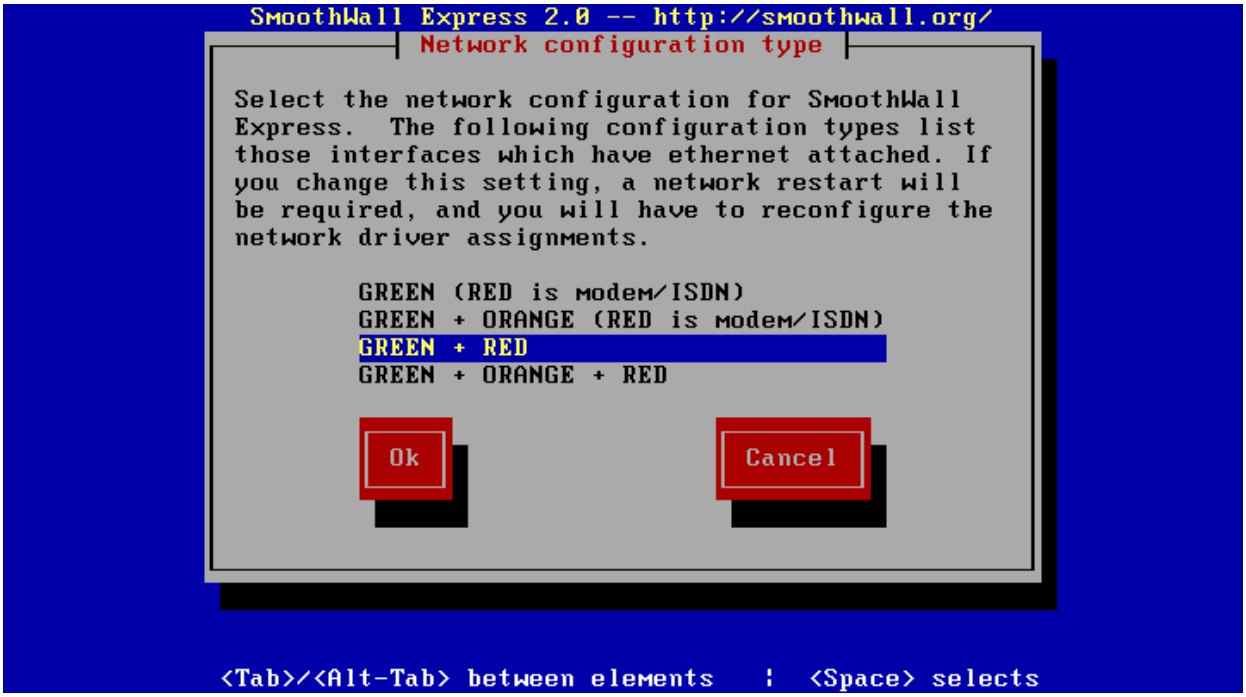


Screenshot 20

6. Follow the instructions on the screen.
   Keep in mind that all entry will be done by the keyboard, the mouse will not work. To release control of the current VMachine, press [CTRL]+[ALT], to go back into the VMachine, just click anywhere inside of its screen. Since this setup is text based, the [TAB] key will let you move from one field to another. Pressing [Enter] will accept the on-screen values.
   - The setup will be performed for the virtual CD-ROM, press [Enter] as needed

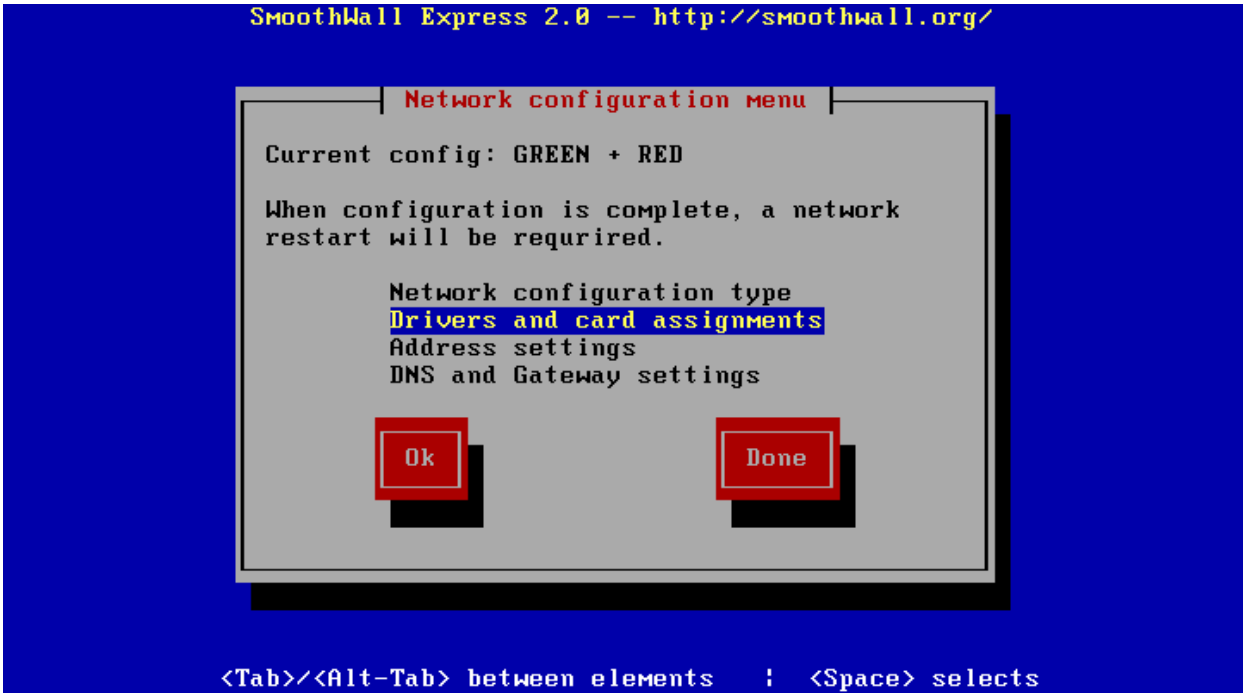
- Partitioning is needed press [Enter] as needed
- In the Configuring network section, choose [Probe], the system will find a NIC made by AMD, confirm and continue.
- We are still working on the GREEN card, change that IP to 172.16.1.5/24 and confirm.
- It will begin to install needed packages, later on confirm the reboot screen
- We do not want to restore from a previous backup,[No] is already highlighted, press [Enter]
- The keyboard is us, and the hostname can be anything, use the lastname for example.
- If you have a web proxy, configure the information on that screen.
- Disable ISDN
- Disable ADSL (yes, the Smoothie can be your DSL router if needed)

Make sure the network configuration looks like this:



Screenshot 21

7. As of now, the RED interface is not yet configured, after confirming the screen above, you will be moved to the next screen (Screenshot 22 shown on the next page).

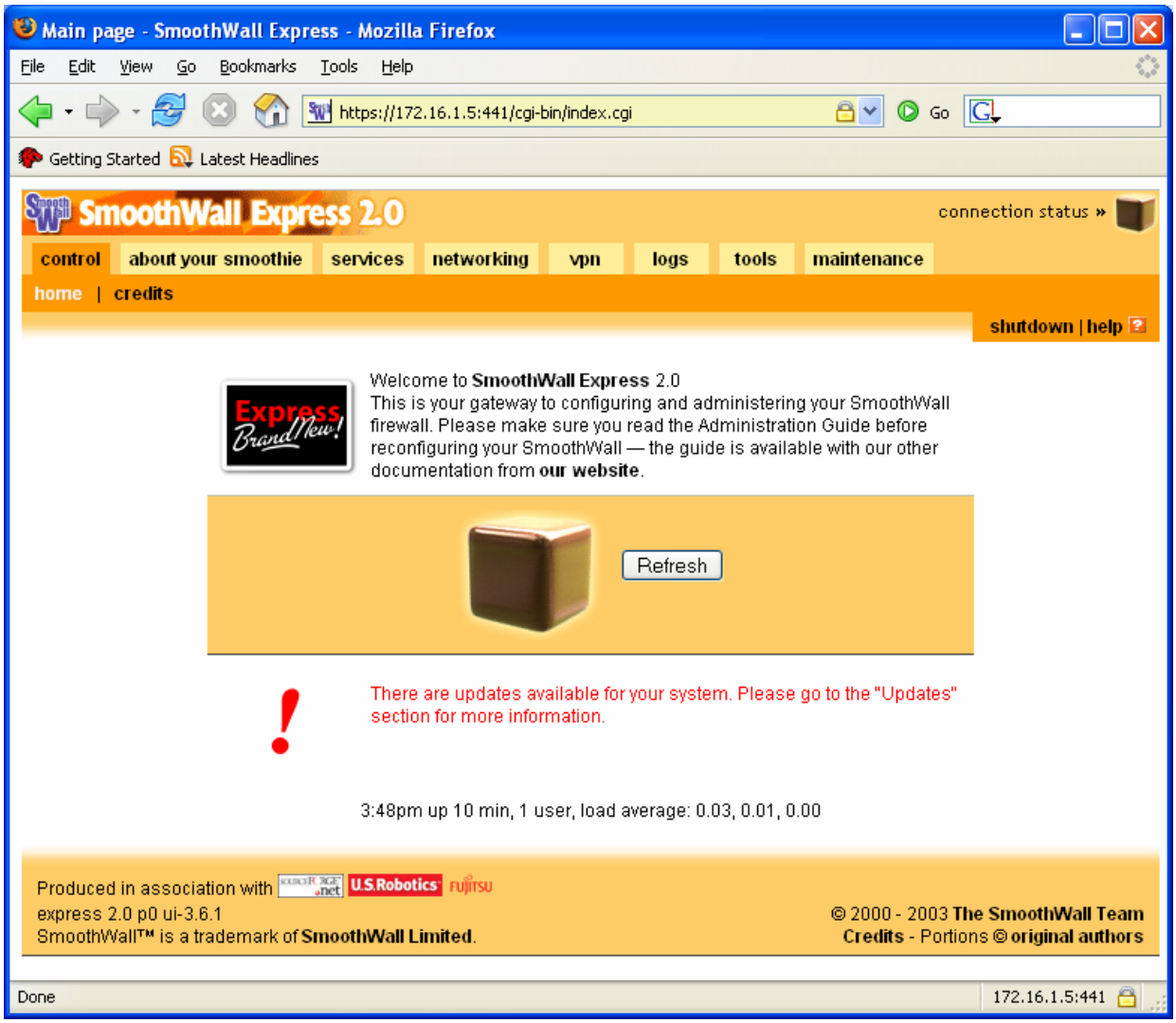


Screenshot 22

8. Highlight “Drivers and card assignments”
9. Keep pressing [Enter] until you are taken back to screen displayed in Screenshot 22.
10. From there choose “Address settings”
11. Choose the RED interface
12. Choose DHCP by using the space bar, and confirm that screen f your network provides the DCHP service.
    - Otherwise, type in the needed info so it can connect to the Internet.
13. Highlight the [Done] button and press [Enter] several times until you reach the screen regarding DHCP server info.
    - We will not activate the DHCP server. Notice that the DHCP server is ready to work with the GREEN network number and the Smoothie itself is the DNS server.
14. Skip right down to OK and press [Enter].
15. Now, do not forget the password you will be typing at each screen.
    - As a suggestion, use toor as the password for all the screens that follow.
16. If all is fine, the last screen will ask you to reboot, press [Enter] to confirm.

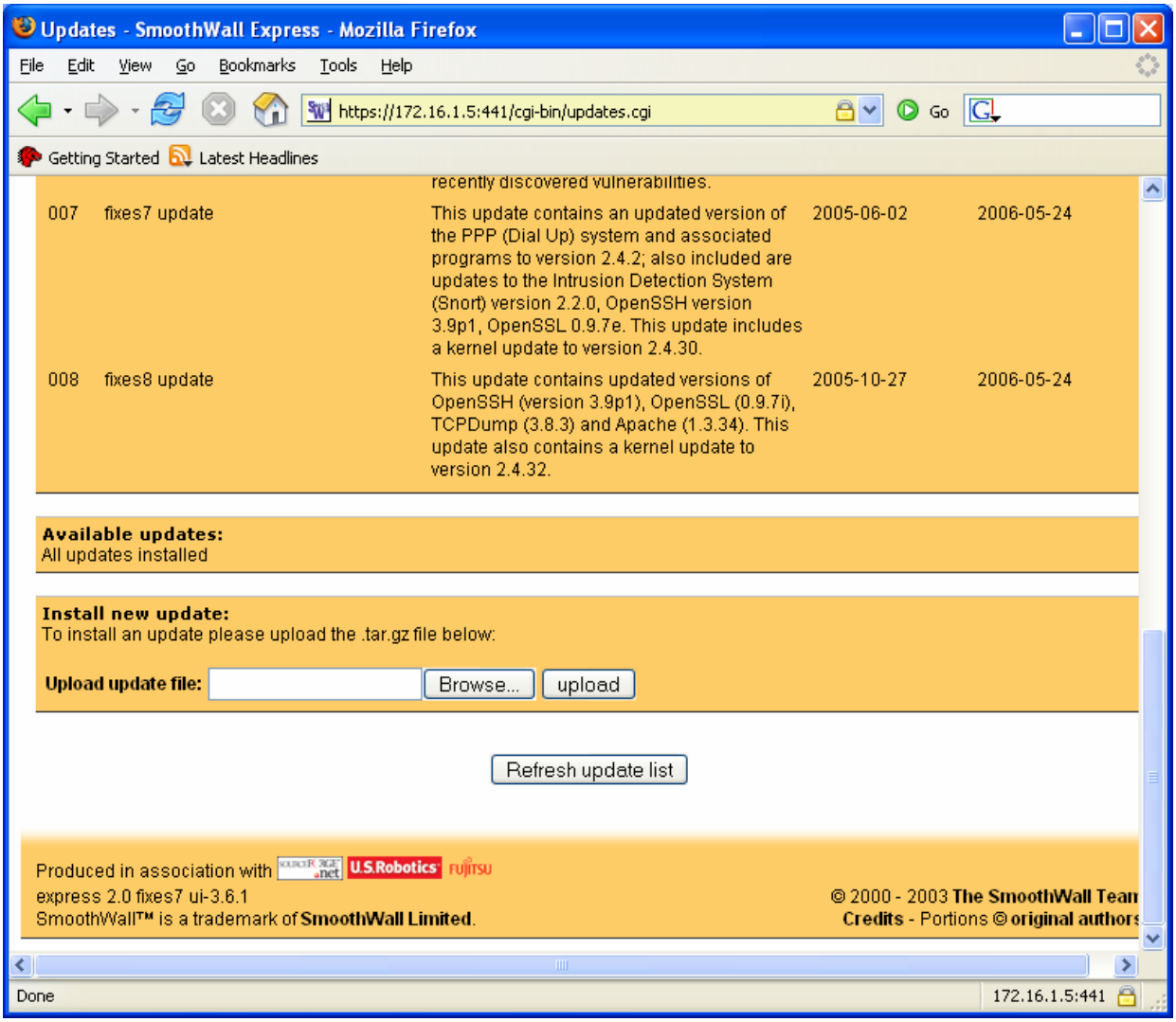
Theoretically we no longer need to anything at the Smoothie if you paid attention as the information scrolled. At some point the IP address assigned to the RED interface via DHCP is shown, in my case it was 192.168.1.2. If it was missed, login as root, password toor, and then type `ifconfig` [Enter]. To see a particular interface just add eth0 or eth1 after the command (i.e. `ifconfig eth0` or `ifconfig eth1`.

17. Start up our XP virtual machine
    - make sure it has an IP address that belongs to the network 172.16.1.X
18. In XP, open the web browser and connect to the website https://172.16.1.5:441.
19. Allow and/or accept the certificates
20. Afterwards you should see the following screenshot:



Screenshot 22

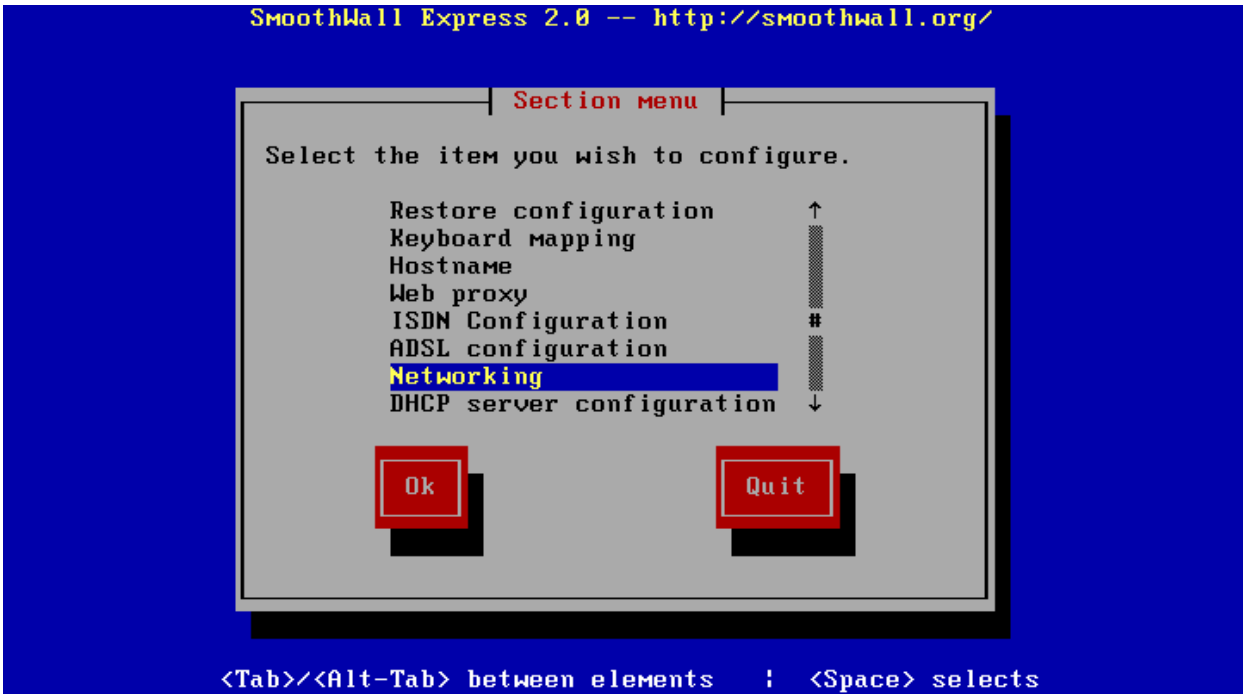
21. Notice the message in red color: “There are updates available……”.
    - The students will carry out the process of finding and applying the needed updates.



Screenshot 23

22. As a tip, it is recommended that after each patch, to reboot. There are two options:
    - Click on shutdown (shown in the screenshot above), then click on the reboot button or
    - simply login to the VM running the Smoothie and then type reboot at the command prompt.
    - Once done with all the updates, the maintenance tab should indicate “All updates installed”.
23. Now, we are ready to duplicate our virtual machine, and setup the two endpoints for the VPN.
    - In Screenshot 22, to the right, there is an option for shutting down.
    - Click it, then press the button shutdown.
24. If the default settings regarding the VM files placement were used, then the VM files are located under My Documents\My Virtual machines.

25. In the “My Virtual Machines folder” there is a folder with a name that begins with “Windows XP…….”
    - Right-click it
    - Choose copy from the context menu,
    - Right click anywhere in the white area below it and choose paste.
    - It will copy the folder, and add before the original name the words “Copy of…”.
    - Now we have two virtual machines.
26. We are almost done setting up the VPN. The VPN done in 2003 and the one being configured by using the SW have the characteristic of a pre-shared key.
    - The 2003 can place the client directly into the network.
    - The Smoothie in the other hand requires that both ends of the network have different network numbers.
27. Setup the copy of the Smoothie to the network number of 10.0.0.X/24.
28. From VMWare open the VM in the folder that contains the copy
    - It might ask about an ID number, choose create.
29. Login with the username setup password toor



Screenshot 24

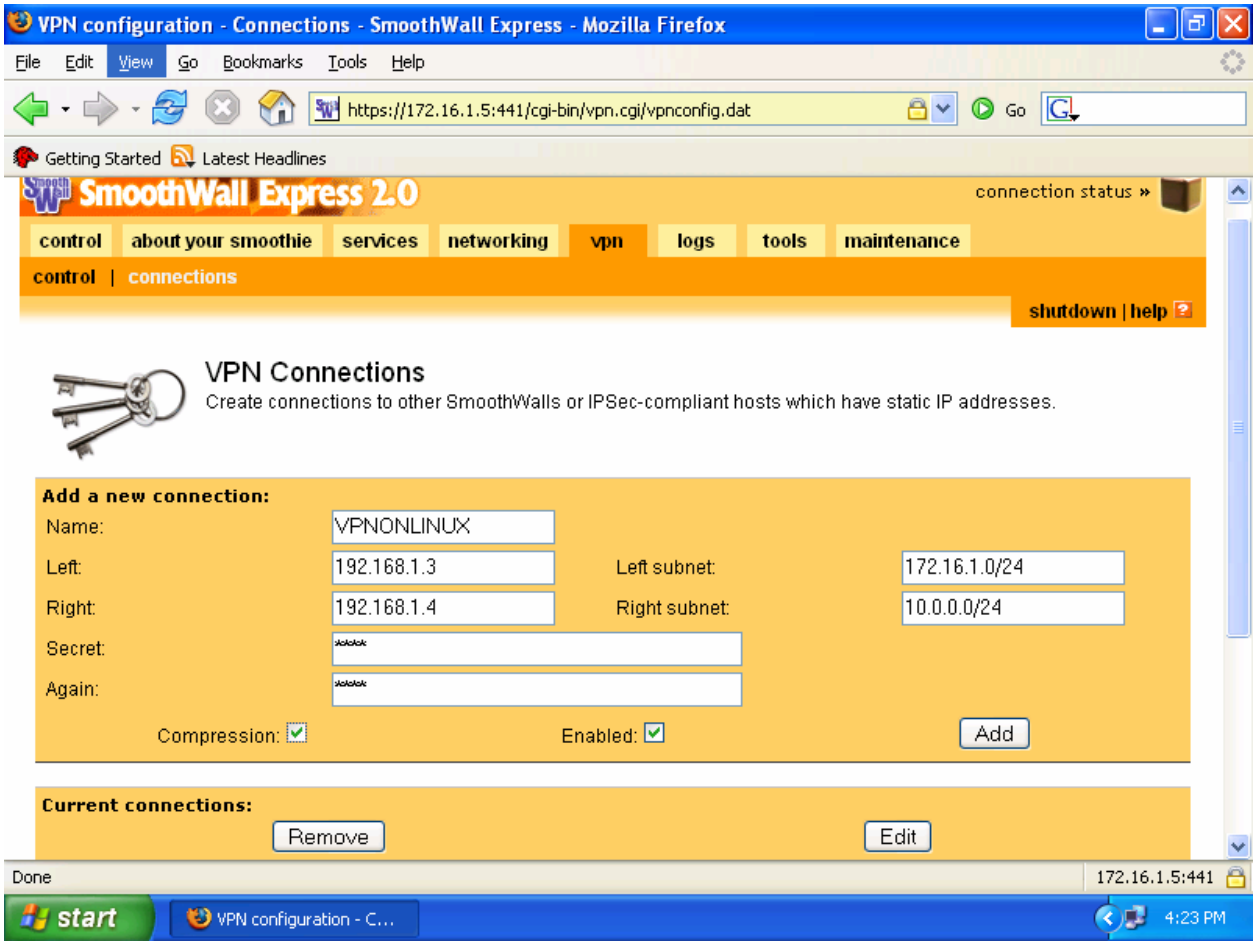
30. You will see the screen pictured above
    - Choose “Networking” and press [Enter]
    - Go to “Addressing” and press [Enter].
    - Choose the GREEN Interface, and change the 172.16.1.5/24 IP to 10.0.0.1/24.

31. Select the “Done” button as needed then “Quit”. After this step, you should see the login screen.
32. Determine the IP address of the copy on the RED interface.
    - Since both Smoothies have the default settings, the IP address they have on the RED interface will not allow connections. We need to have a browser connection to each of them (start the other one now) by using the IP addresses on the GREEN interface. The virtual XP machine is connected to the first one, the virtual machine server is not being used for anything, and you can use it. Set 2003 to work on the 10.0.0.X/24 network and connect to the Smoothie.

In my case this is the information for both smothies:

	IP RED	IP GREEN
SW 1	192.168.1.3/24	172.16.1.5/24
SW 2	192.168.1.4/24	10.0.0.1/24

33. Let us connect to SW 1 (The first one we created) and open the VPN tab
    - Login as admin, password toor
    - Choose “connections”. The information will be filled as shown below:



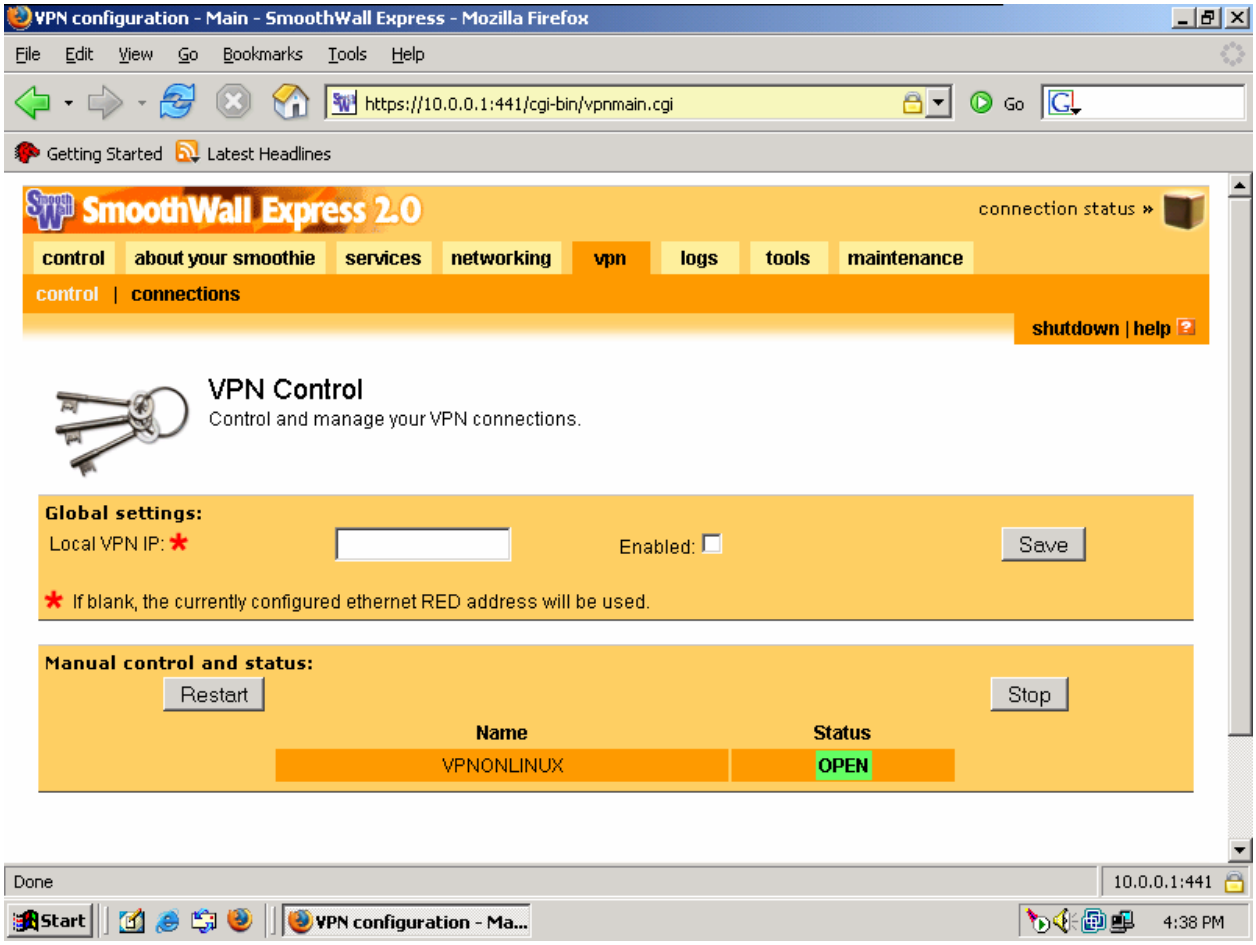
Screenshot 24

34. The secret (password) can be anything, as long as it matches.
    a. The Compression: check box can be left blank
    b. Enabled: must be checked
    c. Click the Add button.

35. One Smoothie is now configured, we can either manually type in the same information in the other one or we can export it. We will export it.
    a. Scroll down and you will see the Export Button.
    b. Before clicking on it, check the "Mark" box now available for the recently configured VPN.
    c. Save the vpnconfig.dat file on the XP desktop.
    d. Minimize your browser; you will see the vpnconfig.dat file on the desktop.
        - VMWare allows moving files between the desktop of the virtual machine to the desktop of the "real machine".
    e. Drag that file from the VM desktop to the desktop of the real machine.
    f. Drag the file into the desktop of 2003 server.

36. Connect to the Smoothie, using https://10.0.0.1:441,
    a. Login as admin, password toor.
    b. Click on VPN, connections, choose "Browse"
        a. The button is almost at the bottom of the page, on the right side.
    c. Find the vpnconfig.dat file on the desktop (the .dat extension will be hidden), select it and choose open.
    d. Click on "Import".

The VPN Control window displays



Screenshot 25

37. What follows will be done in both Smoothies:
    a. To the left of connections, there is a link for control.
    b. Choose it then press the “Restart” Button.
    c. The Status must change to OPEN on the last Smoothie where these steps are performed.

Part IV: Lab research for the student:

This is a challenging assignment.

In the VPN setup using XP and 2003, the Internet service is more or less provided through 2003, and the client gets the services from the 2003 network, including the Internet. How the configuration of both Smoothies needs to be changed so:

b. SW 1 is connected to the Internet via the GREEN interface.
c. SW 1 & 2 are linked together via the RED interface, both RED interfaces are on their own network number
d. A machine placed in the same network number as the GREEN interface of SW 2 connects to the Internet through SW 2, passing by SW 1.

1. How can the Smoothie be used to secure a wireless connection?
   a. Before answering this question, always envision where and how the packet will travel and how it can be compromised. Setup a wireless connection that is secured by using the SmoothWall software. Keep in mind that the SmoothWall is design to connect to another SmoothWall.

Questions for the student:

1. What is the protocol that it is being used to secure the connection between 2003 and XP in the VPN?
2. What is the protocol that it is being used to secure the connection between the two Smoothies VPN?
3. Which approach is more secure? Having the client inside the network once the VPN is established or having the client in a different network?

So far we have worked at setting up a VPN to secure the “inside” of the packets as they travel on any media, what follows will secure the surrounding of the packets as it travels over a wireless connection.