

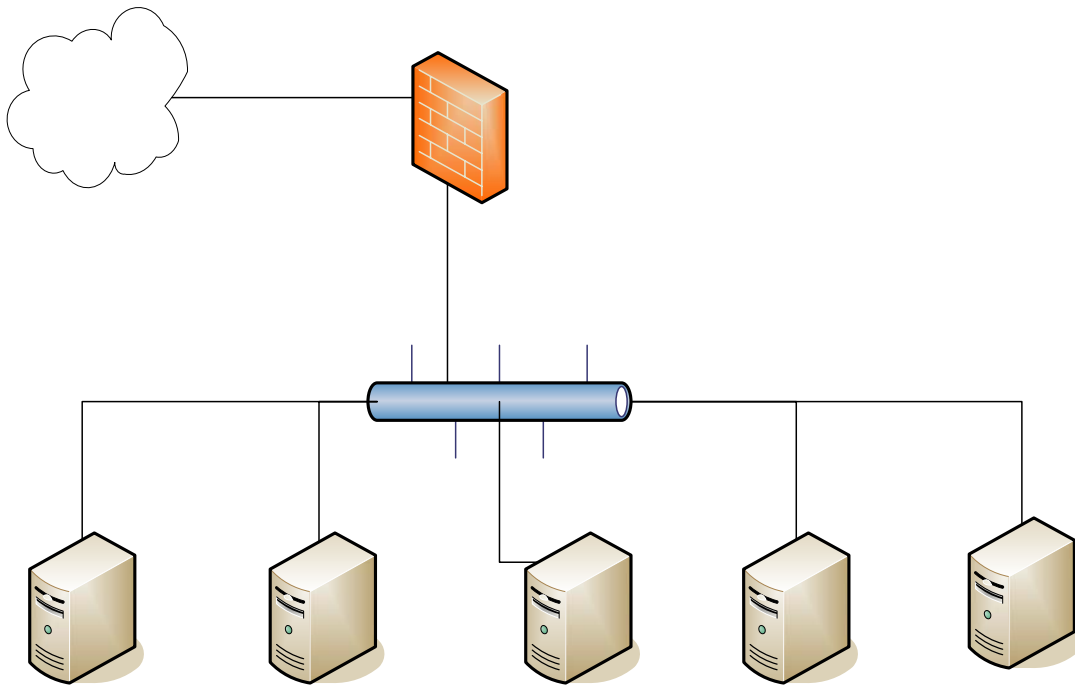
# Overview of Cyber Security Laboratory

cs498sh  
Spring 2006

The laboratory for the Cyber Security course is in 0222 Siebel Center. This room is shared with several other classes. The machines associated with the security class are on the right hand wall as you enter the room.

## Initial machine configuration

The diagram below shows the initial logical configuration of the machines.



The first portion of the course will concentrate on the 5 older Dell systems, sclass1 through sclass5. All machines have Fedora Core 4 installed. Sclass1 through 4 also dual boot to Windows XP. You must press space during the boot process to get the boot loader menu to select windows.

The machines use DHCP to retrieve their IP addresses and DNS information from FW 1, a PIX firewall. The firewall enables connections initiated from the lab to the outside world, but no connections initiated from the outside world in. The connections between

the machines, the firewall, and the outside world are made through two VLAN's implemented on the 24 port switch.

**Note:** The firewall is not configured to allow ping replies to return. Therefore, you cannot use ping to test for connectivity to the outside world. Instead try accessing a web page through a browser or wget, or try to access a machine using ssh/putty.

## **Users on Windows**

On the windows installations, 6 non-standard users are defined and two non-standard groups.

Alice and Bob are non-privileged users. They are members of the engineering group. Alice is also a member of the finance group.

Carol and Dave are also non-privileged users. They are members of the finance group.

Ellen and Gus are privileged users. They are members of the Administrators group.

In general the passwords for the users are <user name>-test. For example Alice's password is alice-test.

The Administrator password is class-test.

## **Users on Linux**

On linux, a similar set of users are defined with the same passwords. Instead of an Administrator user, we have a root user. The root password is class-test.

The users are assigned to similar groups: eng, finance, and sysadm.

## **Determining Addresses on Windows**

If you bring up a command window (i.e. run the "cmd" command), you can invoke "ipconfig" which will show the IP address currently assigned to your machine's interface. "ipconfig /renew" will try the dhcp request again. "ipconfig /all" will show additional address details like DNS addresses.

## **Determining Addresses on Linux**

From a terminal window, you can use the "ifconfig" command to see all the addresses associated with the interfaces. This is in the /sbin directory (in case it is not on your path). You can call "ifdown eth0" and "ifup eth0" to retrigger the DHCP request. Or you can call "dhclient" to restart the address negotiation.

**Note:** last year, we had some network connectivity problems particularly with sclass2. Please let me know if you see similar problems this year. I have an extra network card in reserve, but I have not yet seen the problem this year.

## **Windows Installed Software**

Visual studio 6.0 is installed to provide a C++ development environment. Putty, thunderbird, and firefox are also installed.

## **Linux Installed Software**

Eclipse, gcc, gdb, vi, and emacs are installed for program development. Standard network client applications are installed like firefox and ssh. Many server and network programs are also installed.