Remote PC Guide for Standalone PC Implementation

Updated: 2007-01-22

The guide covers features available in NETLAB+ version 3.6.1 and later.

IMPORTANT

Standalone PC implementation is no longer recommended.

You are strongly encouraged to implement remote PCs using supported VMware Inc. server products. Standalone PC implementations should only be considered as a last resort, for the rare situations where VMware imposes technical limitations that can only be overcome using standalone PCs. Most of the newer NETLAB$_{AE}$ pods are designed for VMware implementations, and do not accommodate standalone PCs. For more information, please see the *NETLAB+ Remote PC Guide for VMware Implementation.*

1 Overview

This document explains how to setup a *Standalone Remote PC* – a remotely accessible PC or server lab resource for your NETLAB Academy Edition® or NETLAB Professional Edition™ system using a standalone machine.

Standalone PC implementation is no longer recommended. You are strongly encouraged to implement remote PCs using supported VMware Inc. server products. Standalone PC implementations should only be considered as a last resort, for the rare situations where VMware imposes technical limitations that can only be overcome using standalone PCs. Most of the newer NETLAB$_{AE}$ pods are designed for VMware implementations and do not accommodate standalone PCs. For more information, please see the *NETLAB+ Remote PC Guide for VMware Implementation.*

NETLAB+ supports three kinds of remote PCs, or the option not to implement a particular PC:

- **Direct/VMware**. The PC is implemented as a VMware virtual machine
  - Users can control the keyboard, video, and mouse.
  - Users can power on, shutdown, reboot, and revert to a clean state.
  - Users can have administrator rights.
  - Users can change interfaces and routing.
- **Direct/Standalone.** The PC is implemented on a standalone machine, or a virtual product emulating a standalone machine.
  - Users can control the keyboard, video, and mouse.
  - Users can revert to a clean state by rebooting.
  - Users have limited rights (administrative access not recommended).
  - Users cannot change interfaces and routing.
- **Indirect**. The PC is implemented, but not managed by NETLAB+.
  - Users may be able to interact with the PC, but cannot access the keyboard, video, or mouse through NETLAB+.
- **Absent**. The PC is not implemented.

1.1 Direct Access

A remote PC configured for *direct access* allows users to control the keyboard, video, and mouse using a Java based viewer. No special client software (other than Java) is required on the user's computer. NETLAB+ will download the viewer to the client whenever the user clicks on the PC shown in the lab topology.

Direct access is useful in scenarios that involve client related tasks, such as using a web browser, performing pings, generating traffic to test access control lists, experimenting with VPN client software, or any other applications that use a graphical user interface.

Several users can connect to and share the PC's graphical interface at the same time. This feature facilitates mentoring in instructor-led classroom lectures and teaming during student lab practice.

Direct access is based on Virtual Network Computing (VNC), a platform independent remote access protocol. VNC connections from the user's viewer are routed to the NETLAB+ server's *outside interface* on TCP port 23 (sharing the same port with Telnet). This means that you do not have to open any additional ports or IP addresses to support remote PCs. If the user has a valid lab reservation, NETLAB+ will open a second VNC connection from the NETLAB+ server to the desired remote PC. NETLAB+ then proxies all keyboard, video, and mouse events between the user's VNC connection and the remote PC's VNC connection, giving the appearance that there is a direct connection between the user and the PC. When the lab reservation is completed, all connections are terminated.

Compared to other PC access methods, the NETLAB+ approach offers several advantages:

- Access to the remote PC can be enforced by the scheduler.
- Remote PCs do not have to be connected to a routable network.
- One port is used for both router console access and PC access (TCP port 23).
- Only one IP address and port needs to be opened at the site firewall, regardless of the number of remote PCs and console-based devices (routers, switches, etc.).

1.2 Indirect Access

A remote PC that is configured for *indirect access* has a placeholder in NETLAB+, but does not provide remote access to the keyboard, video, or mouse. Indirect mode is often desirable for static resources that students or instructors do not actually configure. Examples of a static resource would include a Web server, FTP server, DNS/DHCP server, or TFTP server. Indirect access PCs and servers are not managed by NETLAB+. Therefore, there are no hardware or operating system restrictions, other than the specifications required by your curriculum (if any).

2 Standalone Machines and Virtualization Products

Direct access can be implemented on a *standalone* machine (Direct/Standalone), or a *virtual machine* (VM) environment (Direct/VMware) which integrates with the VMware API. This integration offers enhanced functionality and significant benefits.

You are strongly encouraged to implement direct access using VMware virtualization products rather than standalone machines. The advantages to this method vs. the use of standalone machines are described in the table below.

	Direct/Standalone	Direct/VMware
Hardware requirement	Requires one (1) low-end machine per remote PC.	Several remote PCs run virtually on a single high-end machine.
Direct access support (K/V/M)	On Windows XP, Windows 2000, and Windows Server 2003.	On any virtual machine, regardless of operating system.
Special software required on user PC	No, remote viewer is Java-based.	No, remote viewer is Java-based.
Special software required on remote PC	Yes, NETLAB+ Remote PC Software.	No, functionality is built into VMware.
Revert to clean state	Yes, requires third party software.	Yes, built into VMware.
Users can have administrator privileges	Not recommended.	Yes, no restrictions.
Backdoor network	Yes, remote PC requires a second network interface card.	No, all access to remote PC is proxied through the VMware host.
Users can change network interface configuration	No (not recommended)	Yes
VPN Client applications	No, interferes with routing	Yes
Users may power down machine	No	Yes
User may reboot without reverting to clean state	No	Yes

For a complete discussion of the benefits and information on the implementation of remote PCs using VMware, please refer to *the NETLAB+ Remote PC Guide for VMware Implementation:*

http://www.netdevgroup.com/ae/documentation.htm

2.1 Direct / Standalone

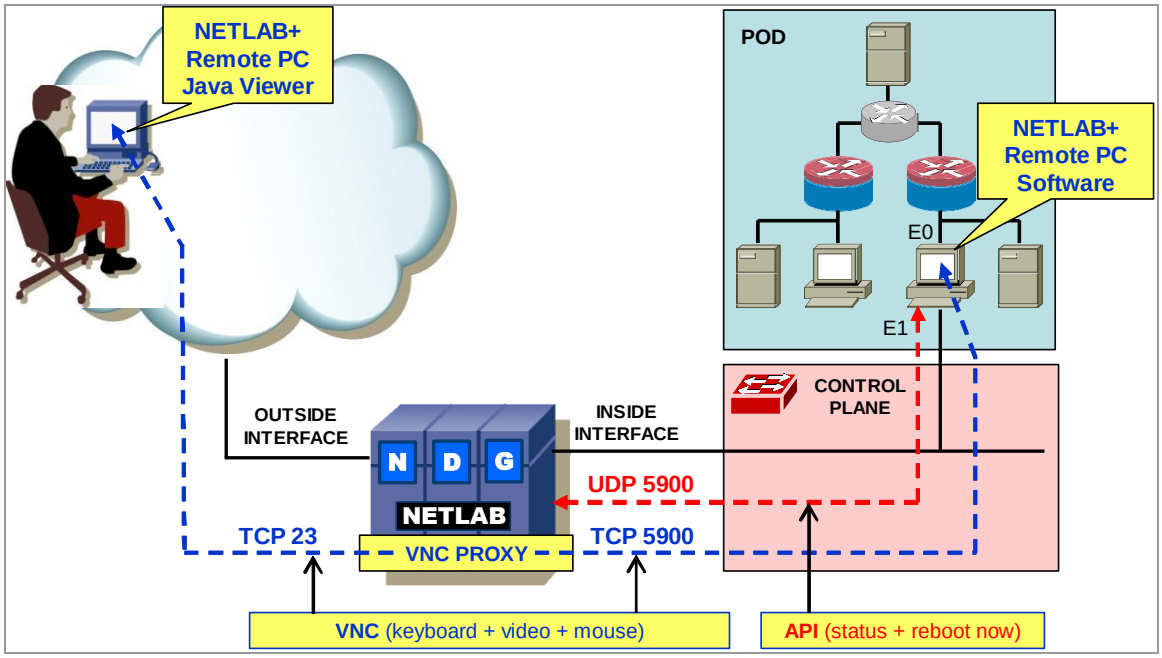
A Direct/Standalone remote PC typically uses real hardware and runs a single operating system. There are no special CPU requirements, and you can use older "surplus" machines with slower processors.

Direct/Standalone is suitable for labs that:

- Do not require administrative access.
- Use DHCP or a consistent IP addressing from lab to lab.
- Do not utilize user-configurable VPN client software, or other applications that can potentially isolate the PC from NETLAB+ as the result of a user action.

Direct/Standalone is currently supported on PCs or servers running Windows XP, Windows 2000, or Windows Server 2003. NETLAB+ provides a software package that is loaded on the remote PC. This software provides both *VNC* and *API* functions on the remote PC side. The API component is an application interface that allows NETLAB+ to check the status of the PC and to request a reboot at the end of a reservation or when requested by the NETLAB+ user.

The NETLAB+ software also provides the ability to reboot the remote PC at the end of a lab reservation. This feature, used in conjunction with third party software, can restore the PC to a "clean state".



The diagram above illustrates Direct/Standalone remote PCs. Please be aware of several considerations:

- The remote PC requires a "backdoor network" (depicted as the E1 interface). This usually implies that a second network interface must be installed. The backdoor network is only used to communicate between the remote PC and the NETLAB+ server's inside interface on an internal LAN segment. This means that (1) you can still have a default gateway on the E0 interface, pointing towards the lab, and (2) the remote PC does not need to be on an externally routable network. Since NETLAB+ proxies the VNC connection, the remote PC does not need any external routes in its route table.

- Users with administrative rights on the remote PC can modify interface settings and can potentially isolate it by changing the E1 interface settings. Therefore, it is advisable to create a limited user account for lab users and use the policy editor to prevent changes to the E1 interface. Currently, Windows does not allow different policies for different interfaces. By locking down E1, you must also lock down E0. This effectively means that you cannot use the standalone PC solution for labs that require changes to interface settings (unless you provide the student with administrative access and accept the associated risks). Note: A future version of NETLAB+ is planned that will allow users to change E0 through the NETLAB+ web interface.

- Users could also isolate the remote PC by shutting it down. Using the policy editor, you can prevent this action.

- VPN clients and other applications that manipulate routing tables can isolate the PC and prevent it from being remotely accessed. While a VPN connection exists, the routing table of the workstation is modified, restricting non-VPN enabled access to the PC. *Split tunneling* can be used to prevent this isolation by allowing continuous VNC access over the second network interface. However, the user must be restricted from changing the split tunnel configuration to prevent isolation.

The limitations listed above are not unique to NETLAB+. Without NETLAB+ serving as a proxy, an externally routable backdoor network would be required. This would restrict the network addresses that could be used on the lab side (E0) and create difficult routing scenarios.

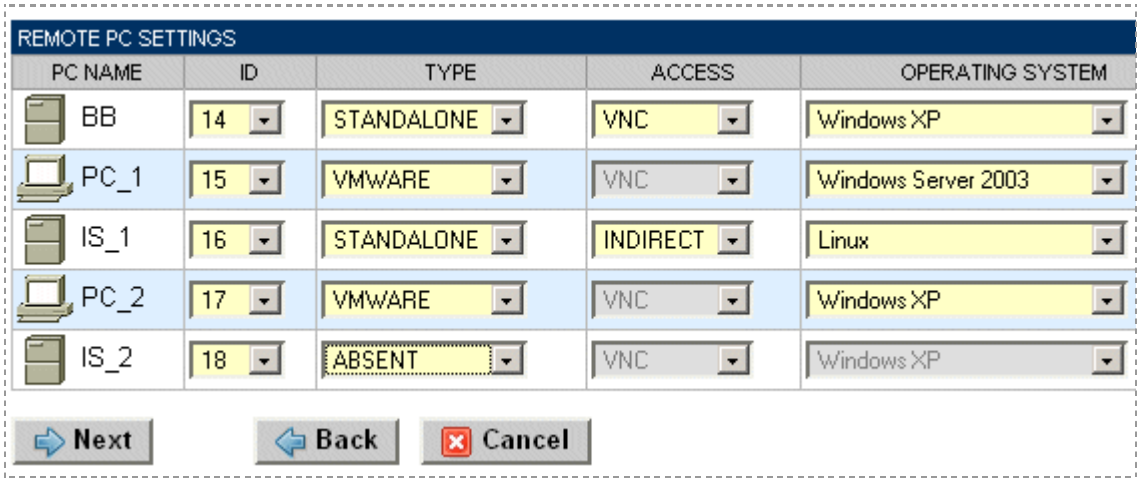
You can effectively use the Direct/Standalone method if your labs do not require administrative tasks on the PC, use consistent addressing (DHCP or a single static IP address) from lab to lab, and do not utilize software that can alter the PC routing table.

If your labs require administrative tasks on the remote PC or changes to network interfaces, you should consider VMware virtualization. This solution is roughly equivalent to KVM-over-IP and is not subject to backdoor network and routing issues.

3 Adding Remote PCs

Remote PCs are part of a lab topology, so they are configured in NETLAB+ when a new equipment pod is added. All settings (except ID) can be modified later. Remote PCs are only available in pods where the network topology indicates the existence of lab PCs.

Remote PC settings will appear in the New Pod Wizard when you add an equipment pod that supports remote PCs. Each PC has an ID, type, access method, and operating system setting.



The **PC ID** setting provides a unique identifier for each PC. If the PC is configured for direct access and is running the NETLAB+ Remote PC Software package, the ID you choose is also used for the last octet (X) in the address 169.254.0.X. This address is bound to the control network interface (see section 4.1 below). You should accept the default ID unless you want to influence the last octet of the IP address (i.e., you already setup the PC and assigned an address).

The **PC Type** setting can be set to STANDALONE, VMWARE or ABSENT.

- STANDALONE provides direct or indirect access to a regular PC or a virtual machine product emulating a regular PC.
- VMWARE provides direct access to a VMware virtual machine and enables automation through the VMware API.
- ABSENT indicates that you are not implementing the PC in this pod. Users will get a friendly popup message if they try to connect to it, informing them that the PC is not implemented.

The **Access** setting specifies a direct access protocol, or indirect access.

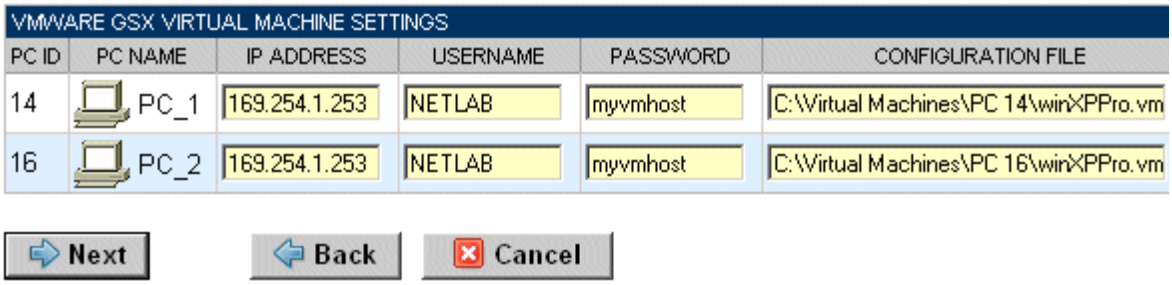
- VNC allows direct access to the PC's keyboard, video and mouse using the VNC protocol. You must load the NETLAB+ Remote PC software on PCs whose PC type setting is set to STANDALONE.
- INDIRECT specifies a static PC resource as described in section 1.2. Users will not have access to the keyboard, video, or mouse.

The **Operating System** setting specifies an OS for this PC. The availability of a selection does not guarantee compatibility with all labs.

The following table depicts the type and access settings for the categories described in section 1:

To implement…	Set TYPE to…	Set ACCESS to…
Direct/VMware	VMWARE	VNC
Direct/Standalone	STANDALONE	VNC
Indirect	STANDALONE	INDIRECT
Absent (no PC)	ABSENT	(not applicable)

If you select VMWARE for any of the PC's, NETLAB+ will prompt for additional settings on the next page.



Each virtual machine requires four VMware-specific settings.

The **IP Address** setting is used to connect to the VMware server. This IP address should belong to an interface on the VMware host operating system that is accessible by the NETLAB+ external or internal network interface. NETLAB+ uses this address to connect to the VMware API. It is also be used for VNC (keyboard / video / mouse) access to virtual machines. Different TCP port numbers will be used to distinguish VNC connections among different virtual machines.

Username specifies an operating system account on the VMware host. NETLAB+ will use this account to login to the VMware host and control virtual machines through the VMware API.

Password specifies the password associated with the host account.

Configuration File specifies the full pathname of the virtual machine's configuration file, typically in the form of C:\Virtual Machines\<pc name>\<operating system>.vmx.

4 Configuring Direct / Standalone Remote PCs

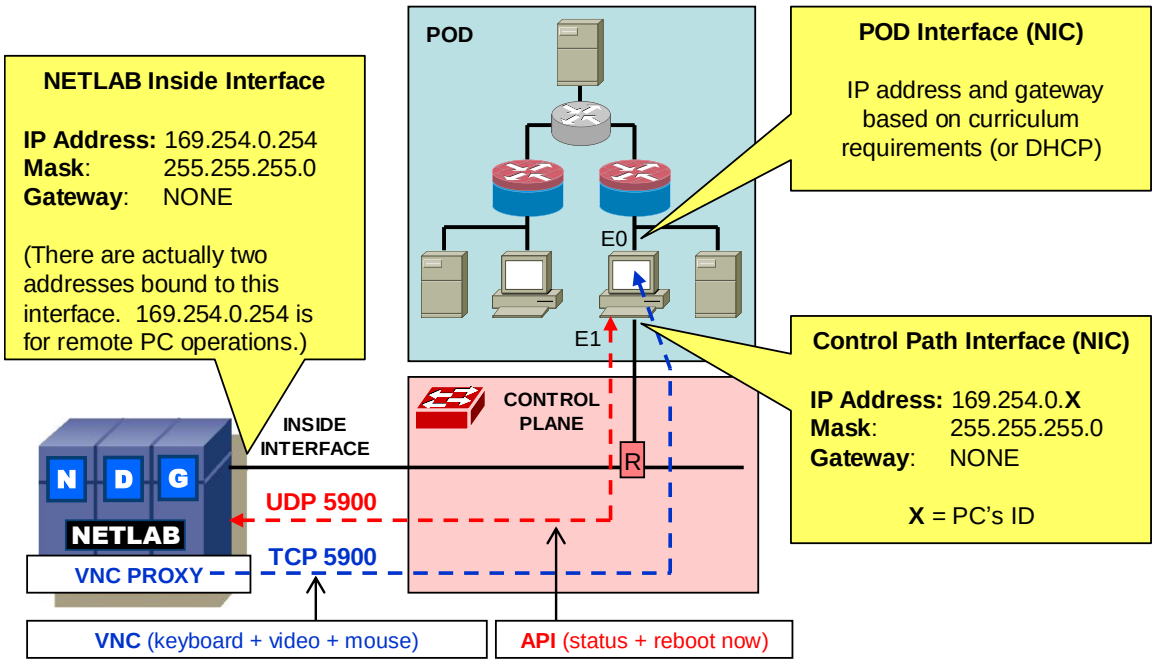
This section discusses configuration tasks for Direct/Standalone PCs.

This section is applicable if the PC's Type setting is set to STANDALONE and the Access setting is set to VNC.

4.1 Network Interfaces

Normally, a PC has a network interface (NIC) that connects to the lab equipment pod. This NIC is assigned an IP address and default gateway that is applicable to the lab environment. DHCP is also an available configuration option.

In addition, you must configure a 2nd NIC that provides a control path for the NETLAB+ VNC and API functions. If your PC only has one built in NIC, you should install a second NIC. This NIC is assigned the address 169.254.0.X, where X is the PC ID setting. You can view the specific IP addresses for each PC on the Pod Management page. There is no default gateway assigned to this interface. The control path NIC is connected to any *reserved port* on your control switch. Recall from the Administrator Guide that a reserved port is not assigned to any particular pod and is normally bound to VLAN 1. Therefore, it shares a common VLAN with the inside interface of your NETLAB+ server. This provides a network path for remote control and viewing.

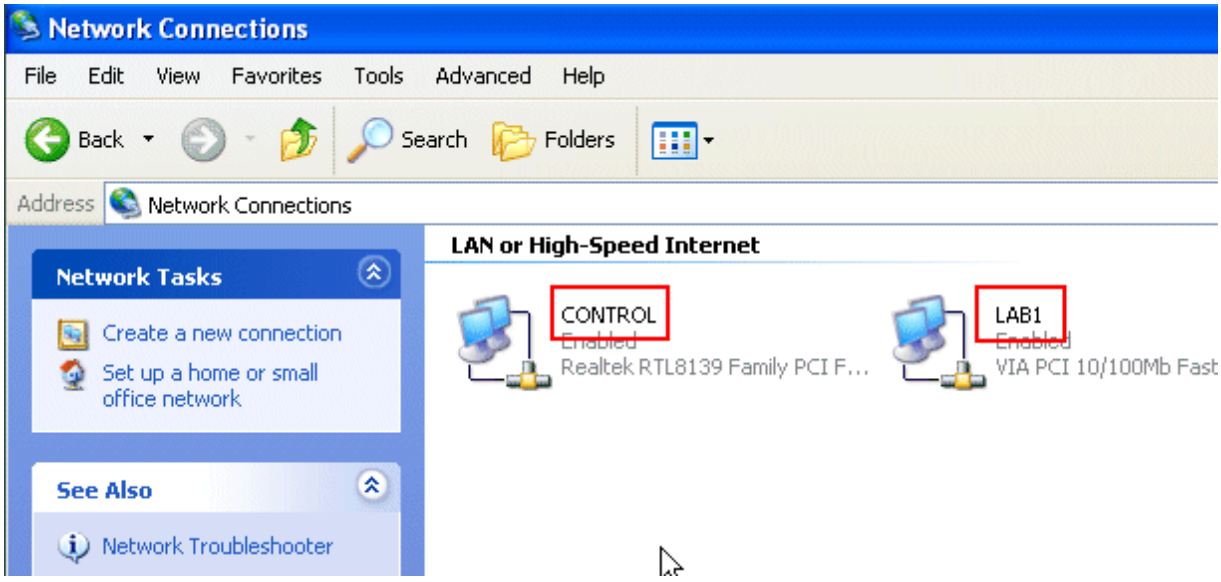


CAUTION: Do not set a default gateway on the control path interface.

4.2 Rename Interfaces

Using the control panel, rename the lab-facing (pod) interface to **LAB1**. In a future version of NETLAB+, users will be able to change the IP parameters of the **LAB1** interface using the NETLAB+ web interface. This feature will require the interface to be named **LAB1**.

To distinguish the two interfaces, you should also rename the control path interface to **CONTROL**.



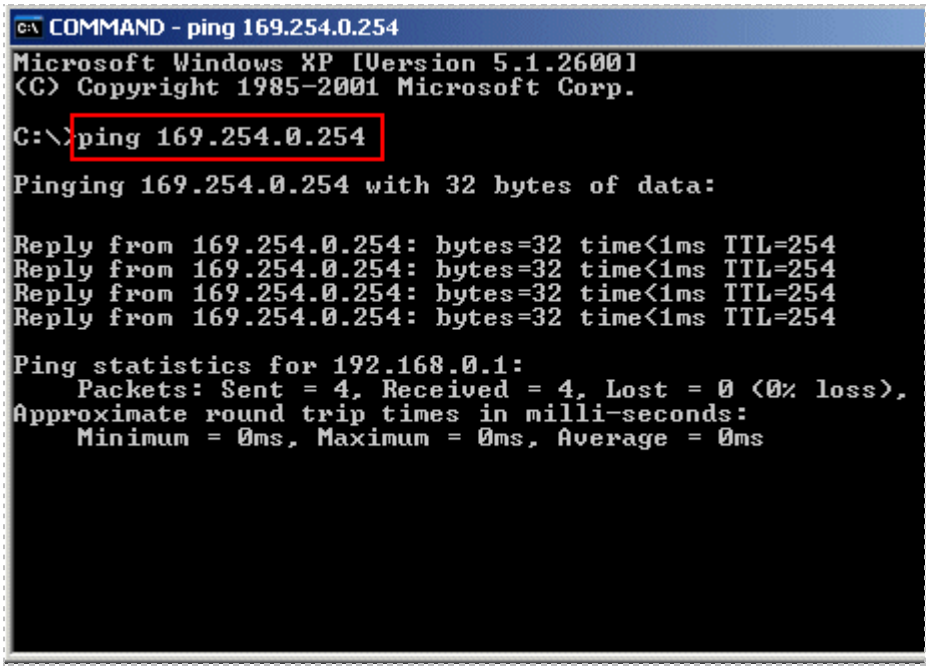
4.3 Test the Control Path

Once you have connected the PC as shown, test connectivity from the remote PC to the inside interface of the NETLAB+ server at address 169.254.0.254 (this is one of two addresses bound to the NETLAB+ server inside interface).

All interfaces and switch ports in the control path should be administratively enabled and should have a green link light.

In order to test connectivity, open a command window on the remote PC and ping the NETLAB+ server inside address **169.254.0.254**.

NETLAB+ also binds 169.254.1.1 on its inside interface, but you will not be able to ping this address from a properly configured remote PC.

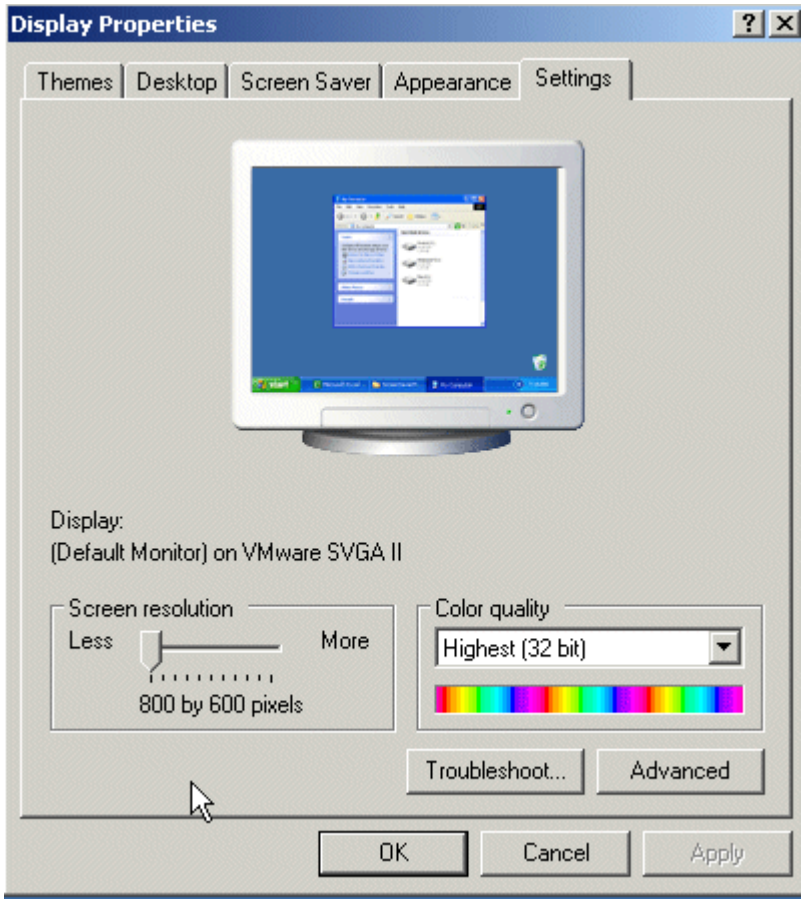


4.4 Change Screen Resolution

Change the remote PC screen resolution to 800 x 600.

16-bit color quality will provide faster screen updates with less color depth. 32-bit color provides more color depth with slower screen updates (on a slow network connection).

Improved compatibility has been noted using 32-bit mode, and is therefore the recommended option.



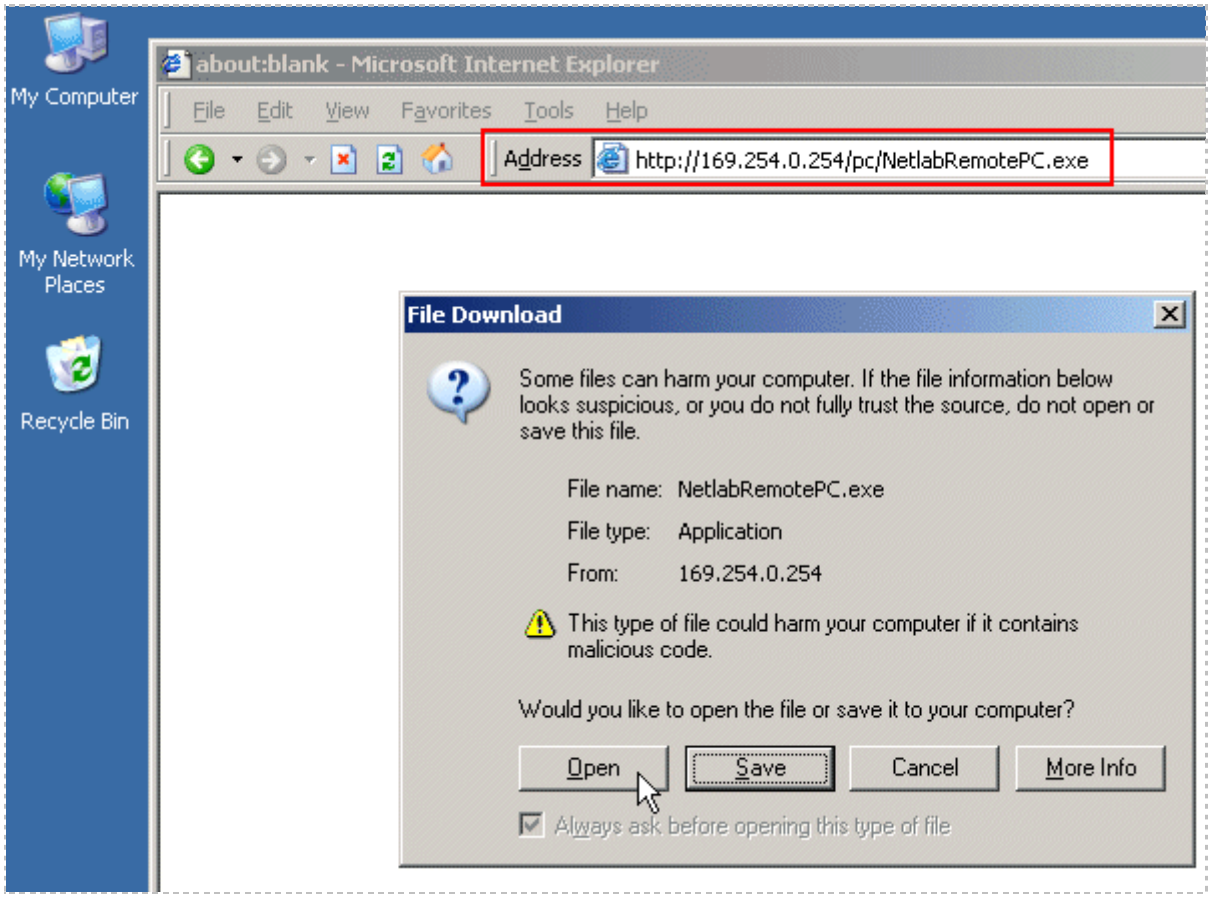
4.5 Load Remote PC Software Package

The NETLAB+ Remote PC software package provides VNC and API functions. It is currently supported on Windows XP, Windows 2000, and Windows 2003 Server.

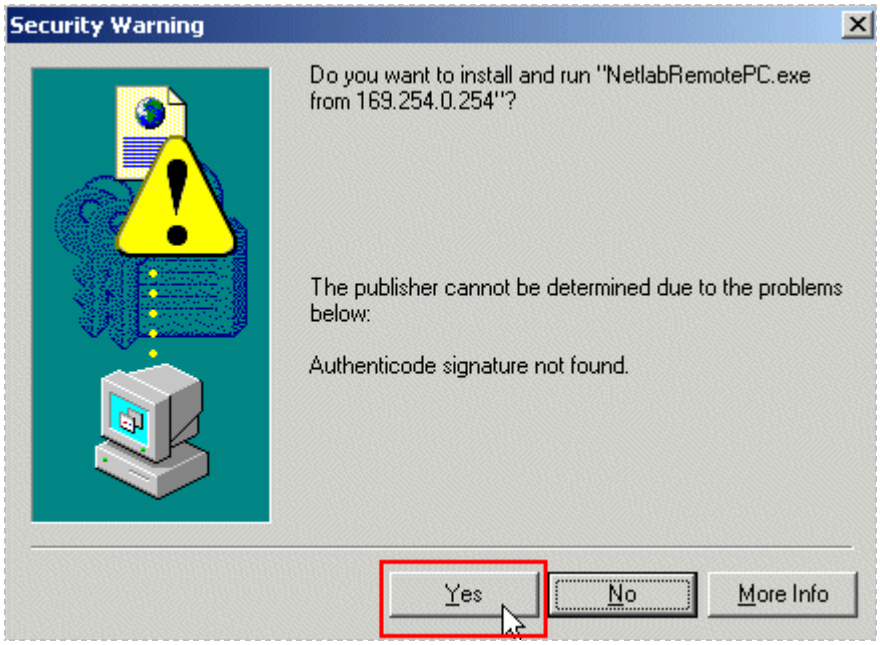
The installation package is stored on the NETLAB+ server and is downloaded using a web browser on the PC.

You must install this software on Direct/Standalone PCs. It should not be installed on Direct/VMware, Indirect remote PCs, or end-users PCs.

1. Open a web browser on the remote PC.
2. Enter the case-sensitive URL exactly as shown:
   `http://169.254.0.254/pc/NetlabRemotePC.exe`
3. Click Open to install the package.



4. Answer **Yes** at the Security Warning.



5. Agree to the license.
6. Read the README file.

5 Securing a Direct/Standalone Remote PC

A Direct/Standalone PC should be secured so that it remains usable from one reservation to the next. This section provides tips for Direct/Standalone PCs, where users will have login privileges and remote access to the PC's keyboard, video, and mouse.

Indirect PCs should also be configured using standard security practices typical of servers. It is assumed that you will not be providing login access to indirect PCs, so we do not provide detailed guidance in this document.

NETLAB+ does not prescribe any specific security policies for your PCs. However, you should implement a policy appropriate for your user community. For Direct/Standalone machines, we recommend that you:

1. Setup a limited account for casual user access (see section 5.1). A user logged in with a limited account generally cannot install software or hardware, but can access programs that have already been installed on the computer. A limited user cannot change the limited account type.

2. You should only allow very trusted users access to the administrator account (or equivalent) if you allow this at all.

3. $NETLAB_{AE}$ users should consult Appendix A of the pod specific guides to obtain information on labs that may require admin privileges. Most labs do not require access to the PC with an administrator level account.

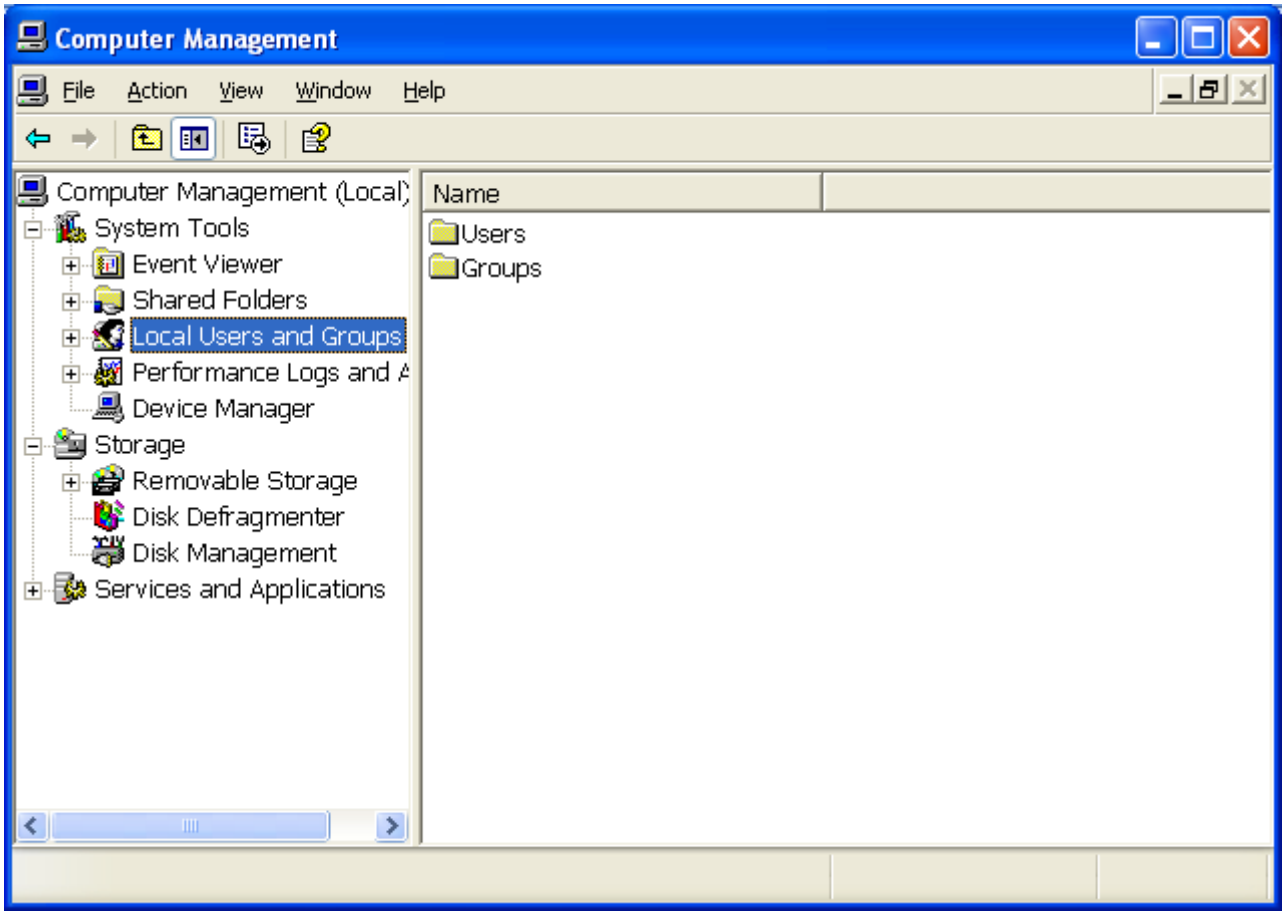
4. Use the Group Policy Editor to remove the Shutdown option from the limited user account. If a user shuts down a PC, that PC is unusable until someone physically powers it on (see section 5.2).

5. Install and activate image restoration software such as *Horizon DataSys Drive Vaccine* (see section 5.3).

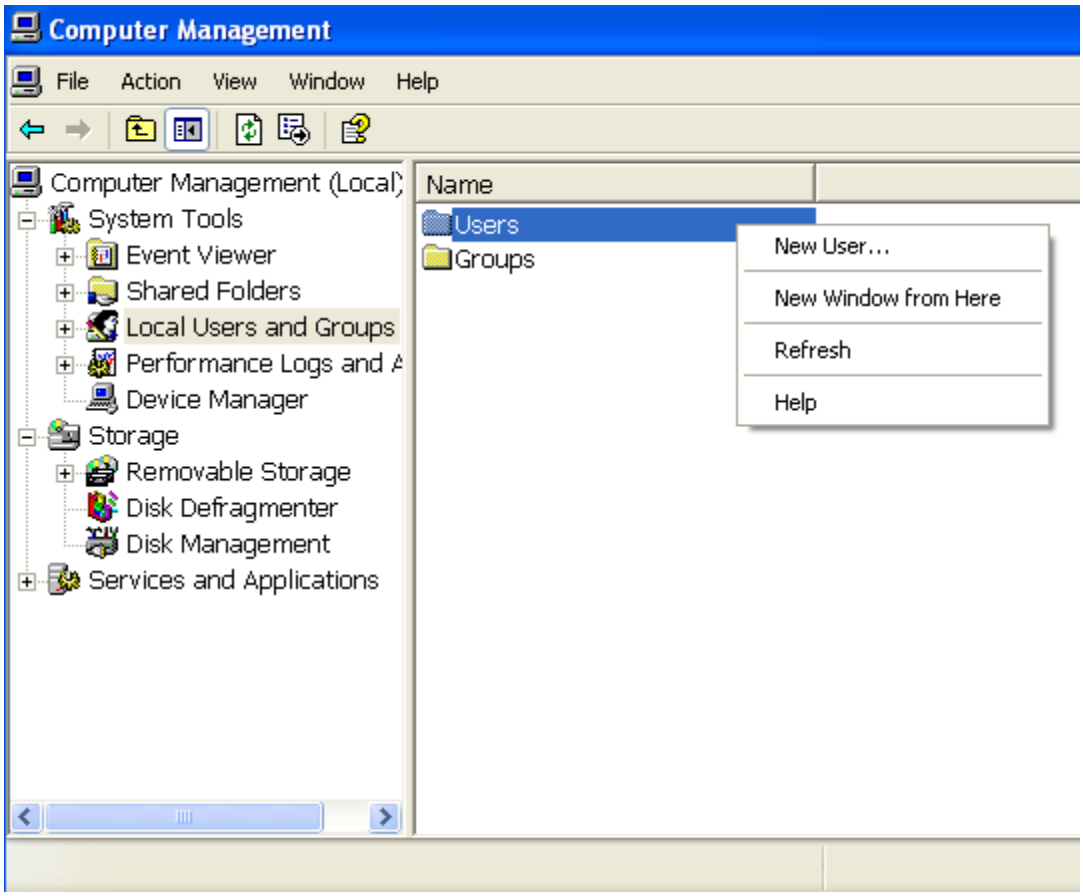
5.1 Create User Account

The following example shows how to create a new user account.

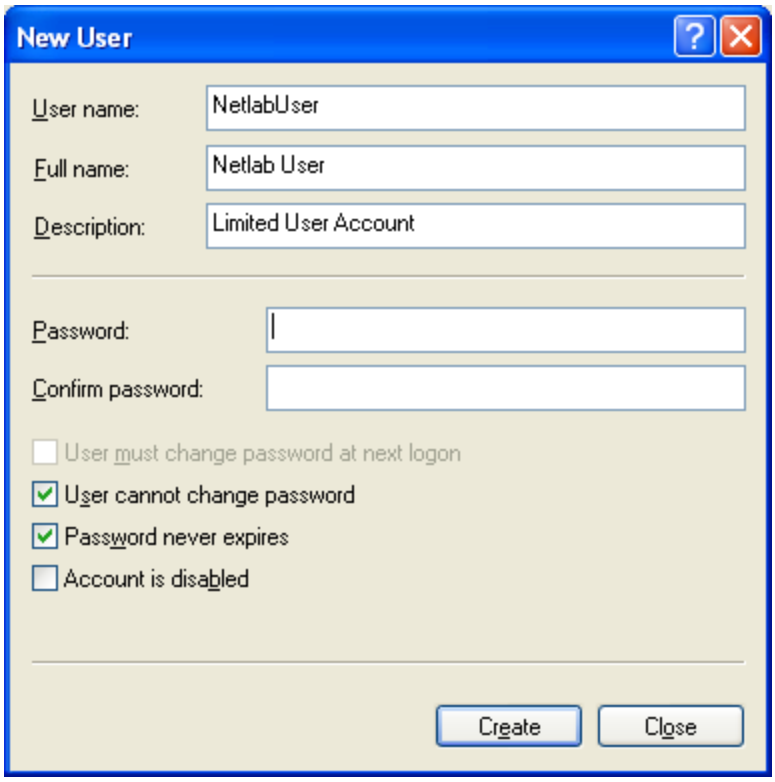
Right click on ‘My Computer’
From the drop down list of options, select ‘Manage’



Select Local Users and Groups.
Next, right click on the users folder in the right hand pane.
Select ‘New User’.



Complete the new user account information insuring to uncheck ‘user must change password at next logon’ After doing so, check the ‘user cannot change password’ and the ‘password never expires’ boxes.



5.2 Remove Shutdown

If a Direct/Standalone PC is shut down by a remote user, it will remain shut down until someone physically powers it back on, making it unavailable to subsequent users. In order to restrict users from being able to shutdown the remote PC during lab reservations, it is possible to disable the shutdown option using the Windows group policy editor.

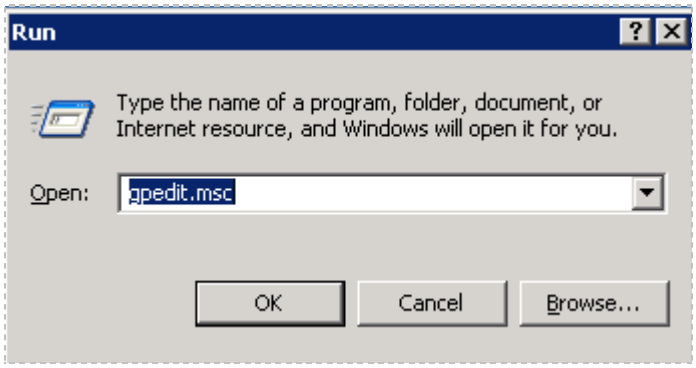
It is also necessary to disable the option allowing the system to shutdown without having to log on. Otherwise, users would still have access to shutdown the PC from the Log On welcome screen.

The following example shows how to remove the shutdown option in Windows XP Professional. The process is similar in Windows 2000 and Windows 2003.

Policy Editor is included with Windows XP Professional. It is not included with XP Home Edition.

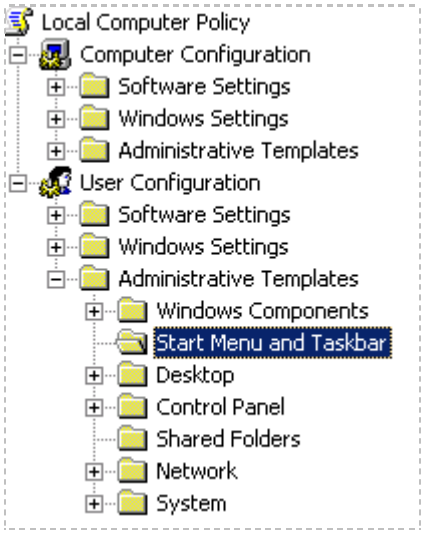
Then, do the following:

Start
Run
Enter **gpedit.msc**



Navigate to:

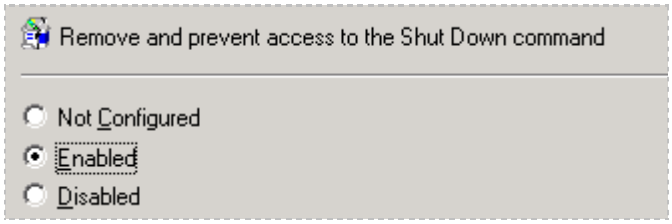
Local Computer Policy>User Configuration>Administrative Templates>
Start Menu & Taskbar



Select in the right hand plane:

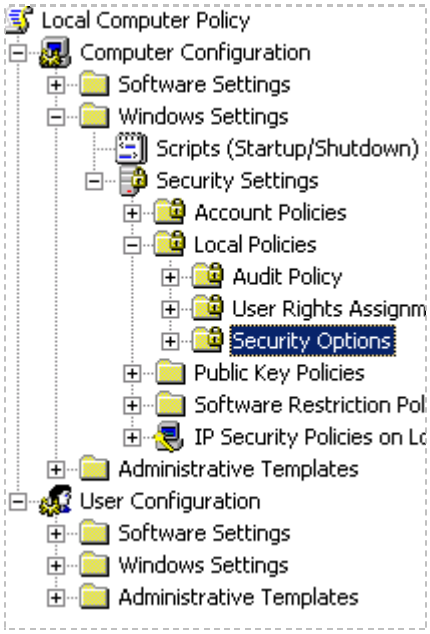
Remove and prevent access to the Shut Down Command

Double-click and select **Enabled**



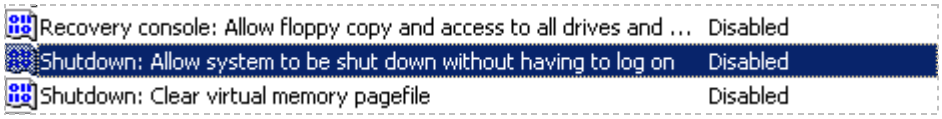
Next, Navigate to:

Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>Security Options

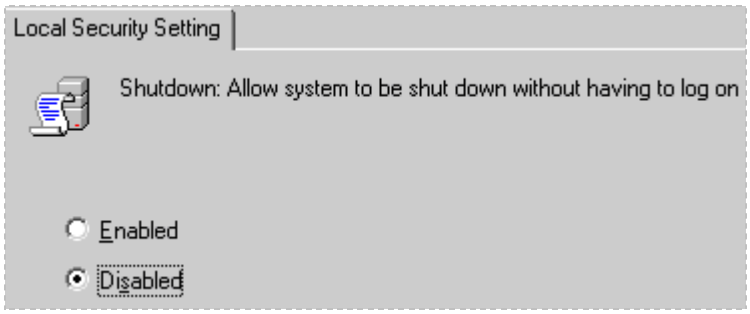


Select in the right hand plane:

Shutdown: Allow system to be shut down without having to log on.



Double-click and select **Disabled**.

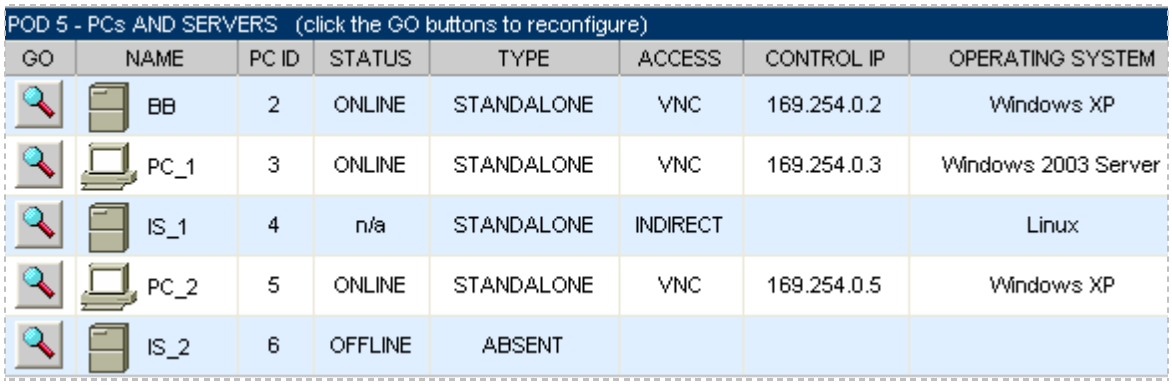


Exit the group policy editor.

5.3 Snapshots and Rollback

It is highly recommended that *Horizon DataSys Drive Vaccine*, or other third party desktop protection is also loaded onto Direct/Standalone remote PCs. This image restoration software will take a "snapshot" of the PC and create a rollback file at the sector level. The PC will rollback to its original state when the PC is rebooted.

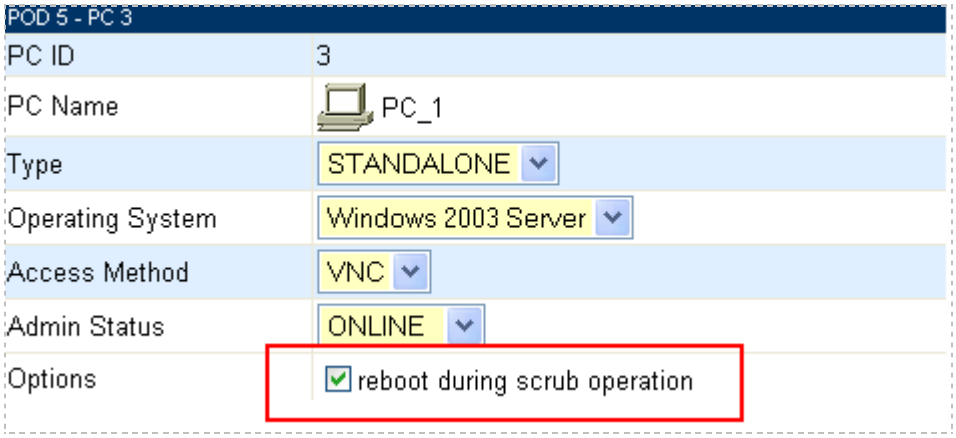
The NETLAB+ Remote PC software package provides a signaling mechanism (API) that allows NETLAB+ to reboot the PC between lab reservations. This feature is automatically enabled for Direct/Standalone PCs. You can disable this feature from the Pod Management Interface as follows:



POD 5 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
	BB	2	ONLINE	STANDALONE	VNC	169.254.0.2	Windows XP
	PC_1	3	ONLINE	STANDALONE	VNC	169.254.0.3	Windows 2003 Server
	IS_1	4	n/a	STANDALONE	INDIRECT		Linux
	PC_2	5	ONLINE	STANDALONE	VNC	169.254.0.5	Windows XP
	IS_2	6	OFFLINE	ABSENT			

 Select a PC, to display the PC configuration page.



POD 5 - PC 3

PC ID	3
PC Name	PC_1
Type	STANDALONE
Operating System	Windows 2003 Server
Access Method	VNC
Admin Status	ONLINE
Options	reboot during scrub operation

Uncheck the "reboot during scrub operation" to disable the rollback feature.

5.4 Offline Feature

Direct access PCs are ONLINE by default. If you are experiencing problems with a particular direct access PC, or for any other reason do not wish to have the PC in use, you may change the PC status to OFFLINE. This will allow the remaining equipment in your lab topology to be online and available for use. This feature is also available from the PC configuration page.