NETLAB+®
NETLAB Academy Edition®
NETLAB Professional Edition®
Installation Guide

Document Version: 2011-12-06

This guide covers features available in NETLAB+ version **2009.R5** and later.

1 Introduction 4
1.1 Planning 4
1.2 Interfaces 4
1.3 Outside IP Address 5
1.4 Inside IP Addresses 5
1.5 Network Address Translation 5
1.6 Ports and Firewall Requirements 6
1.7 Outbound HTTP and HTTP Proxy Servers 6
1.8 Power Requirements 7
2 Installing the NETLAB+ Server 8
2.1 Unpack the NETLAB+ Server 8
2.2 Hardware Appendices 8
2.3 Rack Mounting 9
2.4 Connect Server to Outside Network 9
2.5 Choose a Console Access Method 9
2.6 Connect Server to Power Source 10
2.7 Access the System Console 10
2.8 IP Configuration 12
2.9 Define Remote Access Ports 15
2.10 Outbound Firewall Test 17
2.11 Connect to the Web-based Interface 18
2.12 Troubleshooting: Accessing the Web-based Administrative Interface 19
2.13 Login to Administrator Account 21
2.14 Remote Access Test 22
2.15 Administrative Functions 24
2.16 Check for Software Updates 25
2.17 Configure Services 26
2.18 Maintenance Reminder 29
3 Installing The Control Plane 30
3.1 Install Control Switches 37
3.2 Install Access Server 41
3.3 Install Switched Outlet Device 48
3.4 Download System Images 53
3.5 Upload System Images to TFTP Directory 53
4 Add a Pod 55
4.1 Select Control Switch 57
4.2 Select Access Server(s) and Lines 58
4.3 Select Switched Outlet Devices 60
4.4 Select Device Types 61
4.5 Generic Console Devices 61
4.6 Select Software Images and Recovery Options 63
4.7 Select PC Options 65
4.8 VMware Settings 67

4.9 Select a Pod ID 68
4.10 Select a Pod Name 69
4.11 Verify Your Settings 69
4.12 Cable the Pod 71
4.13 Test the Pod 73
4.14 Bring the Pod(s) Back Online 75
5 Modifying Device Settings 76
5.1 Modifying Device Settings for Routers, Switches and Firewalls 78
5.2 Modifying Device Settings for Routers Using Pagent IOS 79
5.3 Modifying Device Settings for Cisco ASA Security Devices 80
5.4 Modifying Device Settings for Generic Console Devices 82
5.5 Modifying PC Settings 84
6 First Steps Using NETLAB+ 86
6.1 Add Communities 87
6.2 Add Accounts 89
6.3 Add Classes 91
6.4 Schedule a Lab Reservation 93
Appendix A Sun LX50 96
Appendix A.1 Rack Mounting 96
Appendix A.2 Console Connection 96
Appendix A.3 Hyper Terminal Settings 97
Appendix A.4 Labels 98
Appendix B IBM xSeries 305 99
Appendix B.1 Rack Mounting 99
Appendix B.2 Console Connection 99
Appendix B.3 Hyper Terminal Settings 99
Appendix B.4 Labels 100
Appendix C IBM xSeries 306 101
Appendix C.1 Rack Mounting 101
Appendix C.2 Console Connection 101
Appendix C.3 Hyper Terminal Settings 102
Appendix C.4 Labels 102

1 Introduction

NETLAB+ provides a safe “sandbox” for users to schedule, configure and interact with lab equipment. All lab equipment and supporting devices are located safely behind the NETLAB+ server and not directly exposed to outside or public networks. NETLAB+ is delivered as a network appliance and requires no knowledge of UNIX, web server software or other system administration.

This guide provides information on the installation of a NETLAB+ system. The NETLAB+ product line includes NETLAB Academy Edition® and NETLAB Professional Edition® server appliances. This install guide should be used to setup a NETLAB$_{AE}$ or NETLAB$_{PE}$ server.

1.1 Planning

Before setting up your NETLAB+ server, you should review the *NETLAB+ System Overview* documentation. The overview explains NETLAB+ basic concepts and how all of the components fit together.

NETLAB+ has some connectivity requirements that may influence the placement of the server on your network and the ports that are opened in your firewall. It may be necessary to work with your network administrators. To assist you in this task, we have prepared a white paper designed specifically for network and firewall administrators:

Detailed firewall connectivity requirements are explained in the CSS, Connectivity and Firewall Considerations white paper.

The NETLAB+ server can best be described as a *proxy server*. All connections to lab equipment are proxied through the NETLAB+. No connections are allowed unless the user is attending an active lab reservation. Because all connections are proxied (not routed), you only have to open one IP address and two TCP ports to provide access to NETLAB+ and the lab equipment behind it.

1.2 Interfaces

NETLAB+ has two Ethernet network interfaces.

- The *outside interface* (Ethernet 0) attaches to your network and faces your users.
- The *inside interface* (Ethernet 1) attaches to a NETLAB+ control switch and faces your lab equipment and various control devices.

1.3 Outside IP Address

You must allocate a static IP address for the outside interface. This address can be globally routable, or a private (RFC 1918) address. The server's default gateway will also be on the same network as the outside interface.

NETLAB+ does not support DHCP or BOOTP.

1.4 Inside IP Addresses

You do not allocate or configure IP addresses on the inside interface.

NETLAB+ automatically binds two IP addresses on the inside interface: 169.254.1.1/24 and 169.254.0.254/24. Other IP addresses used in the 169.254 range are predetermined and assigned to control devices and remote PCs. The network 169.254.0.0/16 is the IANA reserved block called LINKLOCAL. IP addresses in this range are not globally routable. This IP range has been chosen to avoid conflict with RFC1918 addresses that you may be using in your network

1.5 Network Address Translation

NETLAB+ supports static NAT. You can assign a fixed IP address for the NETLAB+ server on the outside of your firewall, then define a static translation to the IP address assigned to the NETLAB+ outside interface.

Port Address Translation (PAT) is not supported.

1.6 Ports and Firewall Requirements

NETLAB+ only requires one IP address and three inbound TCP ports for all inbound connections. NETLAB+ also initiates outbound traffic on ports that are normally open.

Inbound Port Requirements	
TCP 80	Provides HTTP access to the NETLAB+ web interface.
TCP 2201 (or selected alternate(s))	Factory default setting for the remote access port for proxied connections to lab equipment. Proxy servers are not supported – this port must be open, or a different remote access port number (or list of port numbers) must be selected. Please refer to section 2.9.
TCP 22	Provides SSH for NDG technical support only. In lieu of SSH, this function can also be performed over the TCP port(s) defined for remote access, by special arrangement.

Outbound Port Requirements	
TCP 80	Provides HTTP access to NETLAB+'s central support services (time, status, backup, software upgrades). See 1.7 for information about proxy servers.
UDP 53	Provides DNS lookups. You do not have to open UDP 53 in the firewall if you configure NETLAB+ to use a local DNS inside the firewall.
SMTP 25	Provides SMTP outbound mail. You do not have to open TCP 25 in the firewall if you configure NETLAB+ to use a local SMTP mail server inside the firewall.
PING	NETLAB+ uses ICMP echo for some diagnostic tests, although this is not critical to its operation.

1.7 Outbound HTTP and HTTP Proxy Servers

NETLAB+ makes outbound HTTP connections associated with support functions. These functions are essential to NETLAB+. It is highly recommended that you open TCP port 80 outbound for the NETLAB+ server. Some networks redirect outgoing HTTP requests to a proxy server. The proxy can be transparent or may require manual client configuration. A NETLAB+ configuration setting is provided for manual configuration of a HTTP proxy server. You only need to configure this if (1) you are using a proxy server, and (2) the proxy server is not transparent.

Although NETLAB+ provides an HTTP proxy server setting, it will only work with proxies that do not interfere with HTTP. NDG cannot provide support for problems caused by proxy servers.

1.8 Power Requirements

Determine your overall power requirement by adding up the power requirements for each device in your NETLAB+ installation. A dedicated circuit is recommended for your installation. Additional circuits may be required for very large NETLAB+ installations. Some of the lab devices in your installation will use switched outlets provided by your APC Switched Rack PDUs (or other supported models). The NETLAB+ server, standalone PCs, and control devices should connect to un-switched, surge protected outlets.

Do not connect the NETLAB+ server, control devices, or remote PCs to switched outlet devices (APCs). This may cause your system to become temporarily inoperable. Even though a switched outlet may be unassigned and turned on, these outlets may be turned off during certain events.

2 Installing the NETLAB+ Server

This section of the Installation Guide describes, step by step, how to install a NETLAB+ server.

2.1 Unpack the NETLAB+ Server

Carefully unpack your NETLAB+ server and save all boxes and packing materials. You should also review any safety notices and other reference material that has been packaged with your server.

2.2 Hardware Appendices

The appendices at the end of this document contain hardware-specific information. The appendix for your server will provide rack mounting information. It will also describe how to connect to the menu-driven console in order to perform IP configuration.

Refer the appendix section appropriate for your server:

- Sun LX 50 Server: See Appendix A.
- IBM xSeries 305 :See Appendix B.
- IBM xSeries 306: See Appendix C.

2.3 Rack Mounting

Your NETLAB+ server can be rack mounted. The appendix for your hardware will have specific instructions for rack mounting your server. You should mount your server in a rack in a way that will provide for maximum expansion of your installation.

2.4 Connect Server to Outside Network

Connect the NETLAB+ server outside interface to your network. Referring to the printed label on your server, make sure the cable is connected to Ethernet 0. Ethernet 1 will be connected later in the installation.

Ethernet 0 should connect to a functional 10/100 port on your LAN. When the server is on, the link lights should remain illuminated on both Ethernet 0 and your LAN switch port.

The IBM link lights do not come on unless the Ethernet network connection is 1 Gbps (see the appendix for server-specific information).

2.5 Choose a Console Access Method

To perform basic IP configuration, you will need to connect to the NETLAB+ console interface. There are two acceptable ways to do this:

1) Connect a VGA monitor and keyboard to the designated ports on your system. This method is preferred because you are able to observe the server when it is booting. Connect the monitor and keyboard before powering on the server.

2) Establish a serial port connection from another PC, laptop, or terminal using the server’s built-in serial port and communications software (such as Hyper Terminal). The serial port does not become active until the server has booted. The appendix specific to your server hardware contains the correct serial port settings.

2.6 Connect Server to Power Source

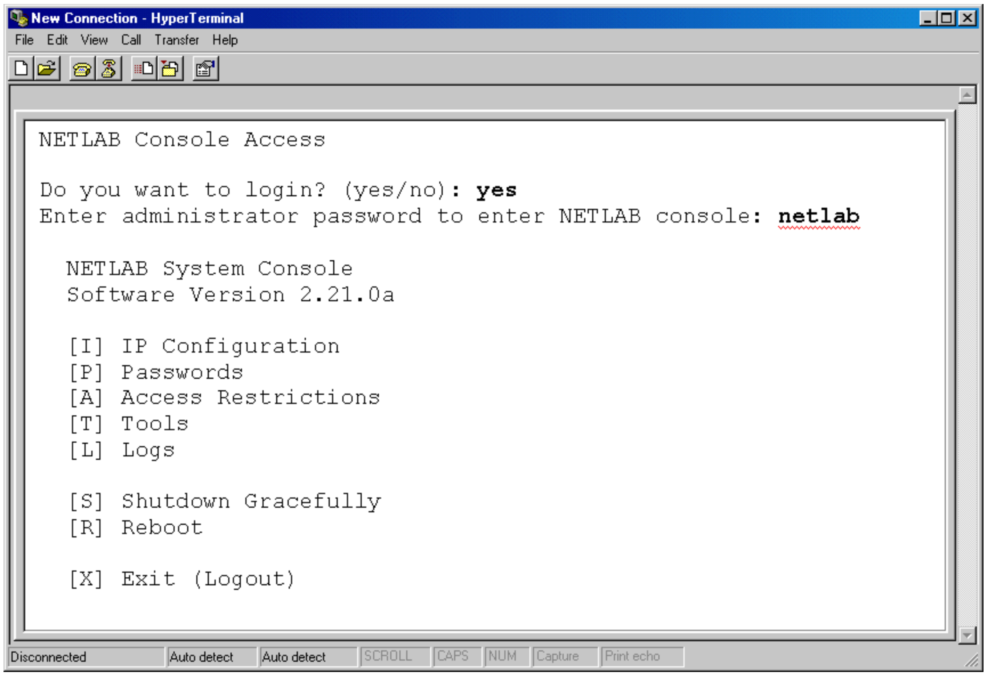
Connect the power cord of the NETLAB+ server to an un-switched, surge-protected outlet. Do not connect it to a switched outlet (APC device). A printed label has been placed on the top of the NETLAB+ server to help identify the power and reset buttons. You may need to remove the front cover to access these buttons. Remember to replace the front cover after the unit has been powered on. Find the power button or switch for your NETLAB+ server and power on the unit.

To reduce the risk of accidental data loss, follow the warnings on the printed label. Always perform a graceful shutdown from the system console or administrator web interface before powering down the server. Similarly, these interfaces should be used to perform a reboot. Pressing the reset button on the front panel will NOT perform a graceful reboot and should be avoided.

2.7 Access the System Console

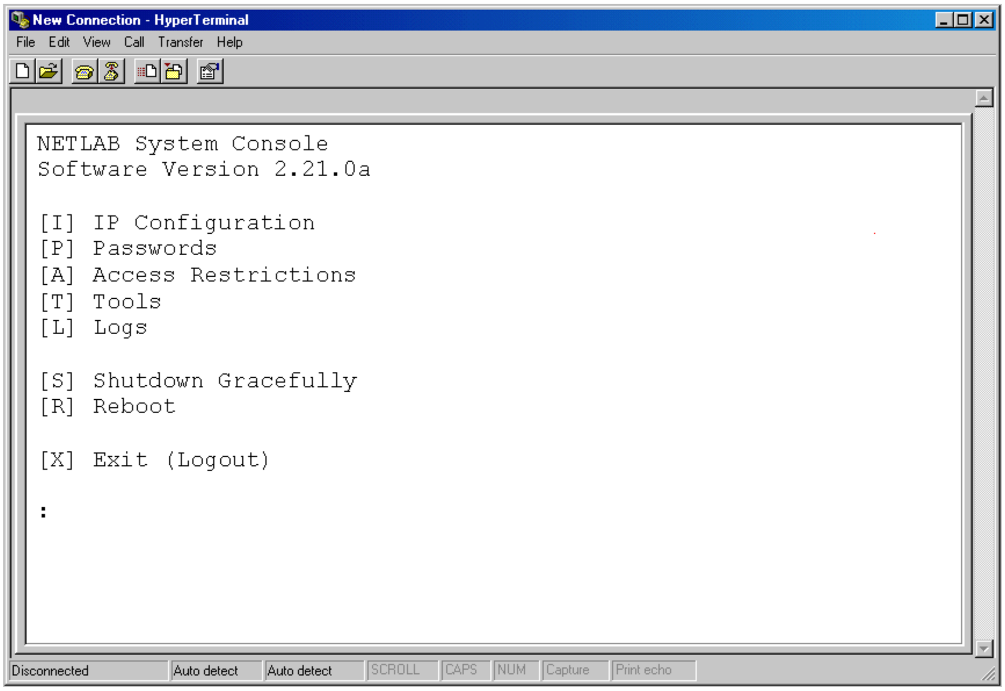
Initial server configuration tasks are performed using a menu-driven console interface. These tasks establish necessary IP connectivity prior to using the web-based administrator interface.

Connect to the console using either method described in section 2.5. If you are using a serial connection, the console will not respond until the server has booted. Press the ENTER key. When asked if you want to login, respond **Yes**. You will be prompted to enter the administrator’s password. The system default administrator password is **netlab**.



```
NETLAB Console Access

Do you want to login? (yes/no): yes
Enter administrator password to enter NETLAB console: netlab

  NETLAB System Console
  Software Version 2.21.0a

  [I] IP Configuration
  [P] Passwords
  [A] Access Restrictions
  [T] Tools
  [L] Logs

  [S] Shutdown Gracefully
  [R] Reboot

  [X] Exit (Logout)
```

Each menu item has a hot-key identified by brackets.



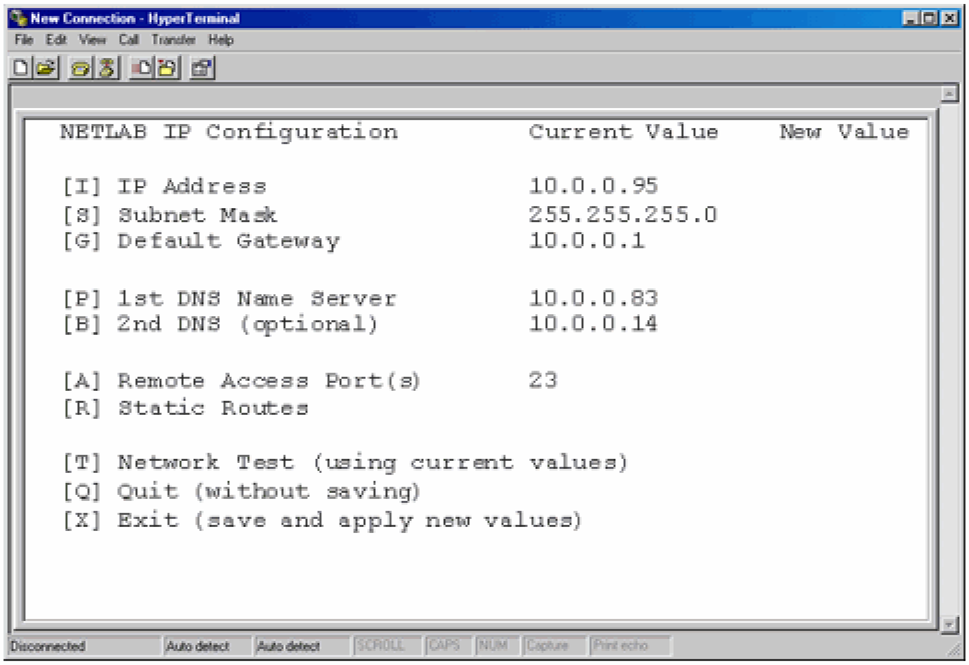
```
NETLAB System Console
Software Version 2.21.0a

[I] IP Configuration
[P] Passwords
[A] Access Restrictions
[T] Tools
[L] Logs

[S] Shutdown Gracefully
[R] Reboot

[X] Exit (Logout)

:
```

2.8 IP Configuration

As discussed previously in the previous section, the NETLAB+ server will require a static IP address. If you are using Network Address Translation (NAT) at your site, you will need to allocate a unique external IP address to NETLAB+ and open a static mapping between the external and internal NETLAB+ IP addresses.

You must assign a unique static IP address.

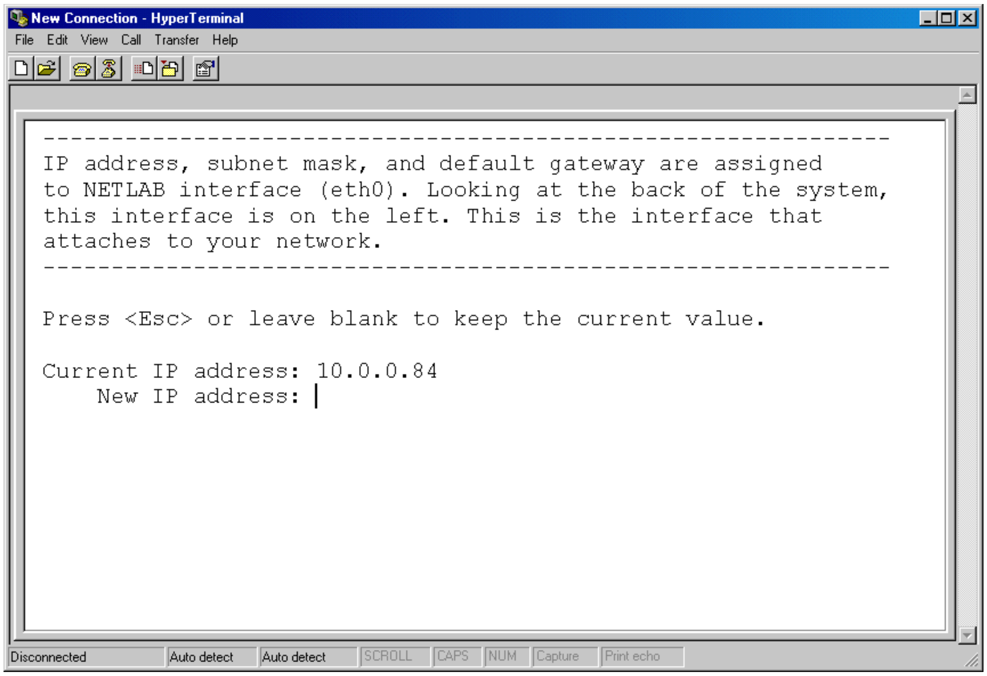
Enter “I” to access the NETLAB+ IP Configuration menu and begin IP Configuration of the server.



```
NETLAB IP Configuration          Current Value      New Value

[I] IP Address                   10.0.0.95
[S] Subnet Mask                  255.255.255.0
[G] Default Gateway              10.0.0.1

[P] 1st DNS Name Server          10.0.0.83
[B] 2nd DNS (optional)           10.0.0.14

[A] Remote Access Port(s)        23
[R] Static Routes

[T] Network Test (using current values)
[Q] Quit (without saving)
[X] Exit (save and apply new values)
```

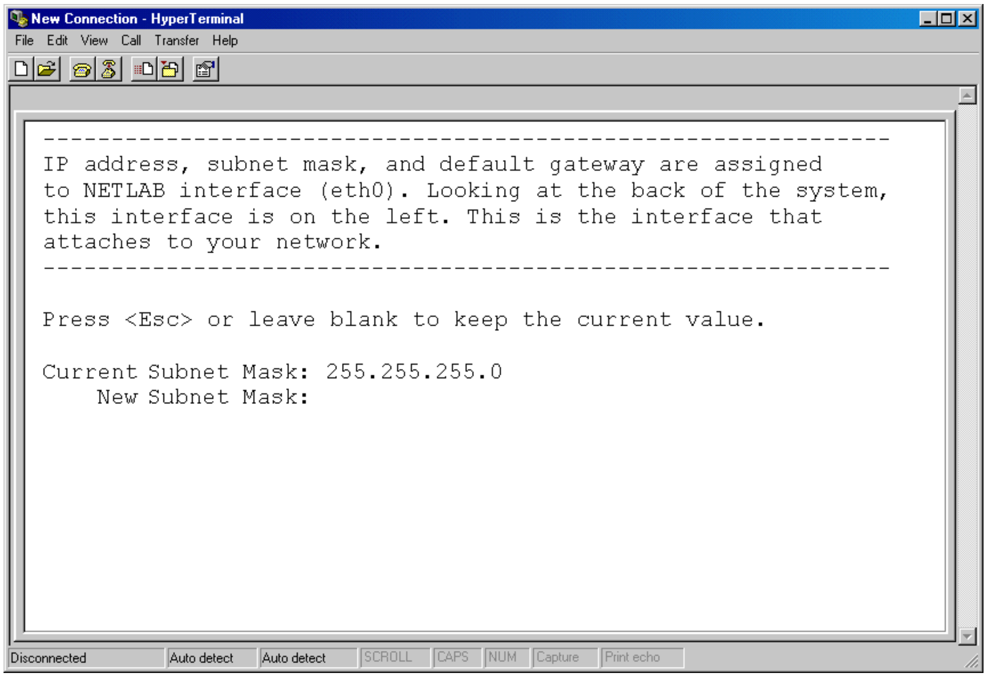
Any Current Values will be displayed. Any new values configured during your session will be displayed in the New Value column. The values will be applied once you choose [X] Exit to save and apply the new values.

Choose [I] to configure the IP address you will use at your site. This IP address must be compatible with your LAN network address space. At the prompt, enter the IP address in dotted decimal format.



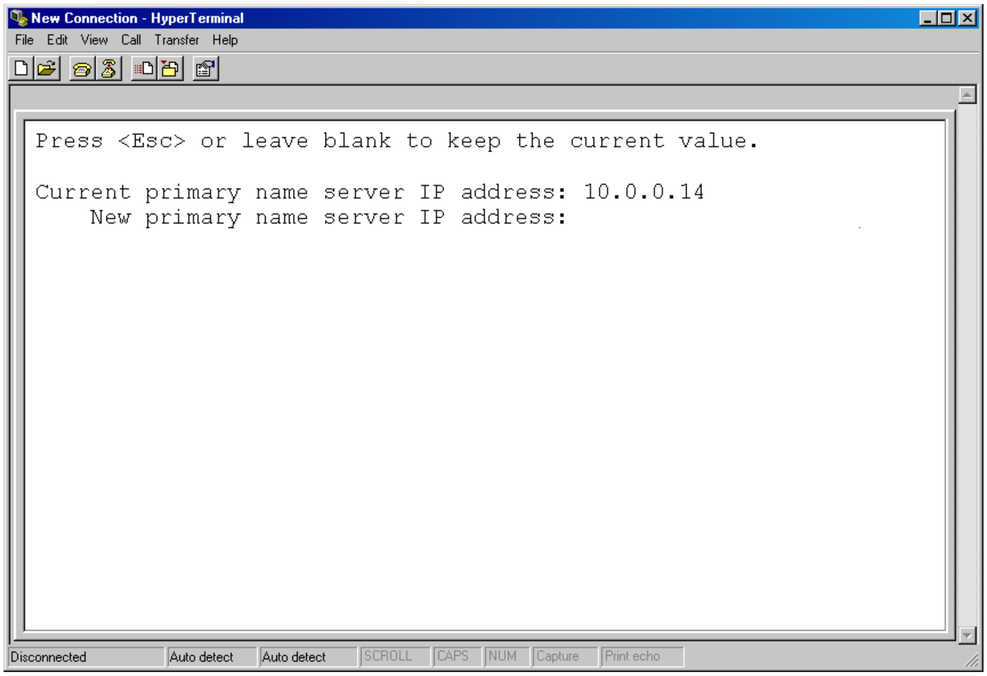
```
--------------------------------------------------------------
IP address, subnet mask, and default gateway are assigned
to NETLAB interface (eth0). Looking at the back of the system,
this interface is on the left. This is the interface that
attaches to your network.
--------------------------------------------------------------

Press <Esc> or leave blank to keep the current value.

Current IP address: 10.0.0.84
    New IP address: |
```

Next, enter values for the subnet mask and default gateway. The default gateway address must be on the same network as the IP address and subnet mask you assign.



```
--------------------------------------------------------------
IP address, subnet mask, and default gateway are assigned
to NETLAB interface (eth0). Looking at the back of the system,
this interface is on the left. This is the interface that
attaches to your network.
--------------------------------------------------------------

Press <Esc> or leave blank to keep the current value.

Current Subnet Mask: 255.255.255.0
    New Subnet Mask:
```

A Domain Name Server (DNS) provides host name to IP address resolution. Enter the IP address of the primary and backup DNS servers. You are required to enter a primary DNS. The backup, or secondary DNS, is optional but highly recommended.



```
Press <Esc> or leave blank to keep the current value.

Current primary name server IP address: 10.0.0.14
    New primary name server IP address:
```

Proceed to the next section if you would like to define remote access ports to use in place of the default remote access port selection, port 2201.

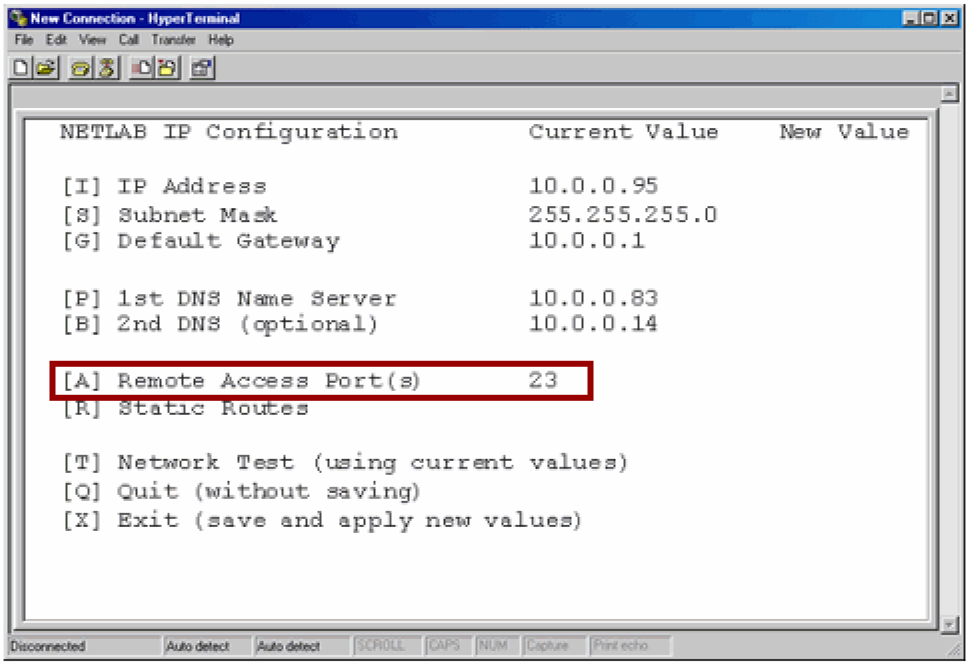
The default remote access port is 2201; this is a change from previous NETLAB+ software versions. Existing systems with software prior to 2009.R1.beta.2 will continue to have the former default setting of 23. The remote access port selection may be changed, as described in section 2.9.

Otherwise, in order to complete the configuration process you must select [X] Exit to save the newly configured values for your server. Once the new values have been saved, you should run a [T] Network Test. Details of the Outbound Firewall Test are discussed in the section 2.10.

2.9 Define Remote Access Ports

The factory default port used by NETLAB+ for remote device access, remote PC access and chat functions is TCP port 2201 (existing systems with software prior to 2009.R1.beta.2 will have the former default setting of 23). Chat functions will be available in a future software release). At some organizations, it may be desirable to select a different port, in order to remain compliant with your organization's security policies. You may select one or more port numbers to be used in place of the factory default.

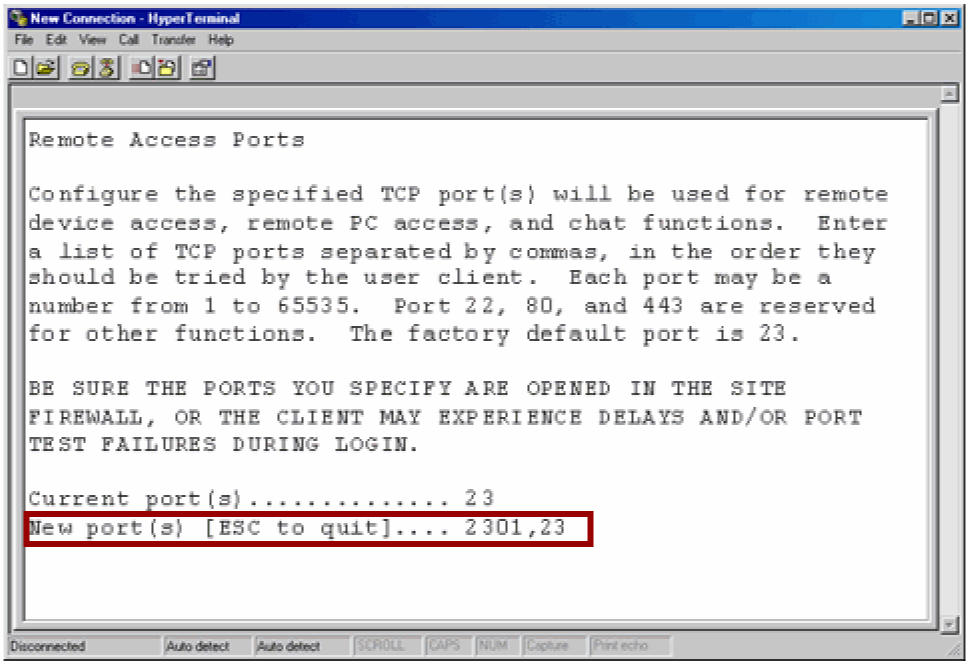
A Remote Access Test is performed during each user login. This test will fail if a connection using the TCP port(s) cannot be established. If you define more than one port for use as the outbound TCP connection, the test will attempt to establish a connection using each port number, in the order they are listed, until the Remote Access Test detects a successful connection. The system will keep track of which port results in successful access and will use that port first for the user's next login.



```
NETLAB IP Configuration               Current Value    New Value

[I] IP Address                        10.0.0.95
[S] Subnet Mask                       255.255.255.0
[G] Default Gateway                   10.0.0.1

[P] 1st DNS Name Server               10.0.0.83
[B] 2nd DNS (optional)                10.0.0.14

[A] Remote Access Port(s)             23
[R] Static Routes

[T] Network Test (using current values)
[Q] Quit (without saving)
[X] Exit (save and apply new values)
```

Select [A] and enter a list of TCP ports separated by commas, in the order they should be tried by the user client. Each port may be a number from 1 to 65535.

Port 22, 80, and 443 are reserved for other functions and cannot be used as Remote Access ports.



```
Remote Access Ports

Configure the specified TCP port(s) will be used for remote
device access, remote PC access, and chat functions.  Enter
a list of TCP ports separated by commas, in the order they
should be tried by the user client.  Each port may be a
number from 1 to 65535.  Port 22, 80, and 443 are reserved
for other functions.  The factory default port is 23.

BE SURE THE PORTS YOU SPECIFY ARE OPENED IN THE SITE
FIREWALL, OR THE CLIENT MAY EXPERIENCE DELAYS AND/OR PORT
TEST FAILURES DURING LOGIN.

Current port(s).............. 23
New port(s) [ESC to quit].... 2301,23
```

Here, ports 2301 and 23 have been entered as Remote Access Ports.

It is critical that the ports you specify are opened in the site firewall, or the client may experience delays and/or port test failures during user login.

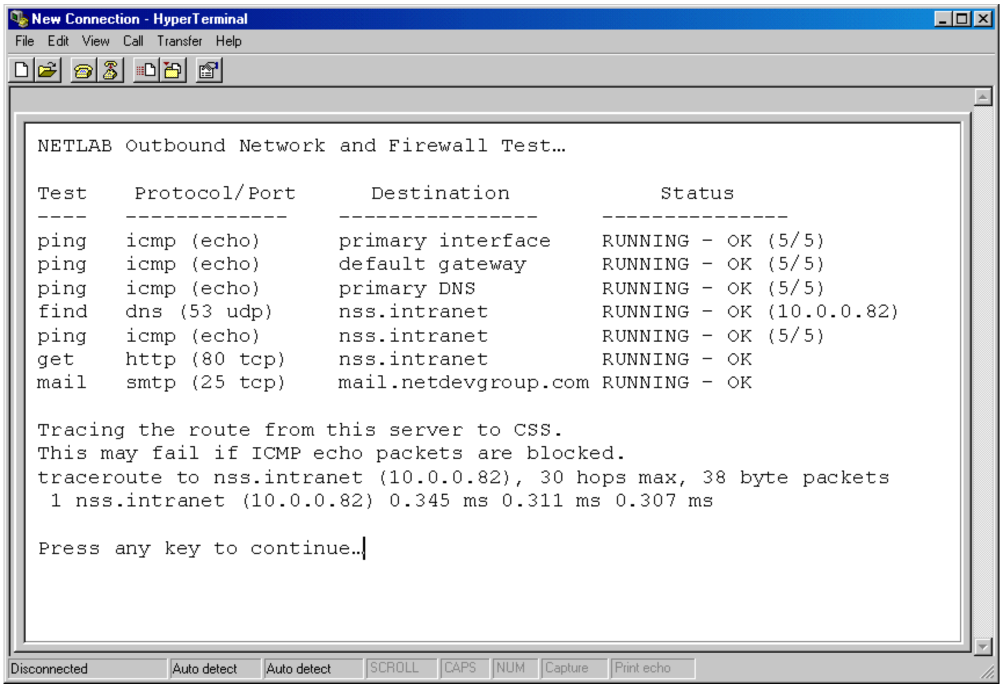
2.10 Outbound Firewall Test

NETLAB+ must be able to send certain types of data through the network in order to function properly. This outbound traffic includes DNS lookups, outbound mail, and HTTP to NETLAB+ Central Services.

The Outbound Firewall Test will determine if the interface, gateway and DNS are reachable. It will also test the server's ability to communicate with NETLAB+ Central Support. Failure of any of these tests will indicate a network problem and should be corrected for proper functionality of NETLAB+. A successful test will indicate **OK** for all test types.

This is an outbound test only.

Since this is only an outbound test, it will not determine if inbound clients can access the NETLAB+ server. Inbound access problems must be addressed on a client-by-client basis, since this will involve the client's ability to reach the NETLAB+ server via HTTP and remote access ports. Any errors reported during the test should be evaluated and corrected. Most errors are caused by firewall configuration issues.

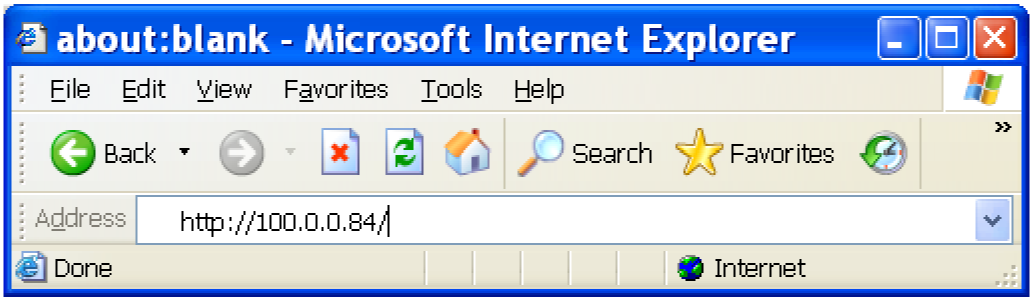


```
NETLAB Outbound Network and Firewall Test…

Test   Protocol/Port     Destination          Status
----  -------------    ----------------     ---------------
ping  icmp (echo)      primary interface    RUNNING - OK (5/5)
ping  icmp (echo)      default gateway      RUNNING - OK (5/5)
ping  icmp (echo)      primary DNS          RUNNING - OK (5/5)
find  dns (53 udp)     nss.intranet         RUNNING - OK (10.0.0.82)
ping  icmp (echo)      nss.intranet         RUNNING - OK (5/5)
get   http (80 tcp)    nss.intranet         RUNNING - OK
mail  smtp (25 tcp)    mail.netdevgroup.com RUNNING - OK

Tracing the route from this server to CSS.
This may fail if ICMP echo packets are blocked.
traceroute to nss.intranet (10.0.0.82), 30 hops max, 38 byte packets
 1 nss.intranet (10.0.0.82) 0.345 ms 0.311 ms 0.307 ms

Press any key to continue…
```

When your test runs correctly, you can exit the NETLAB+ System Console interface and continue with your NETLAB+ installation tasks. You can choose to logout from your main menu. Do not shut down or power off the server at this time. The Outbound Firewall Test may also be accessed from the web interface, see the Test Outbound Access section of the *NETLAB+ Administrator Guide* .

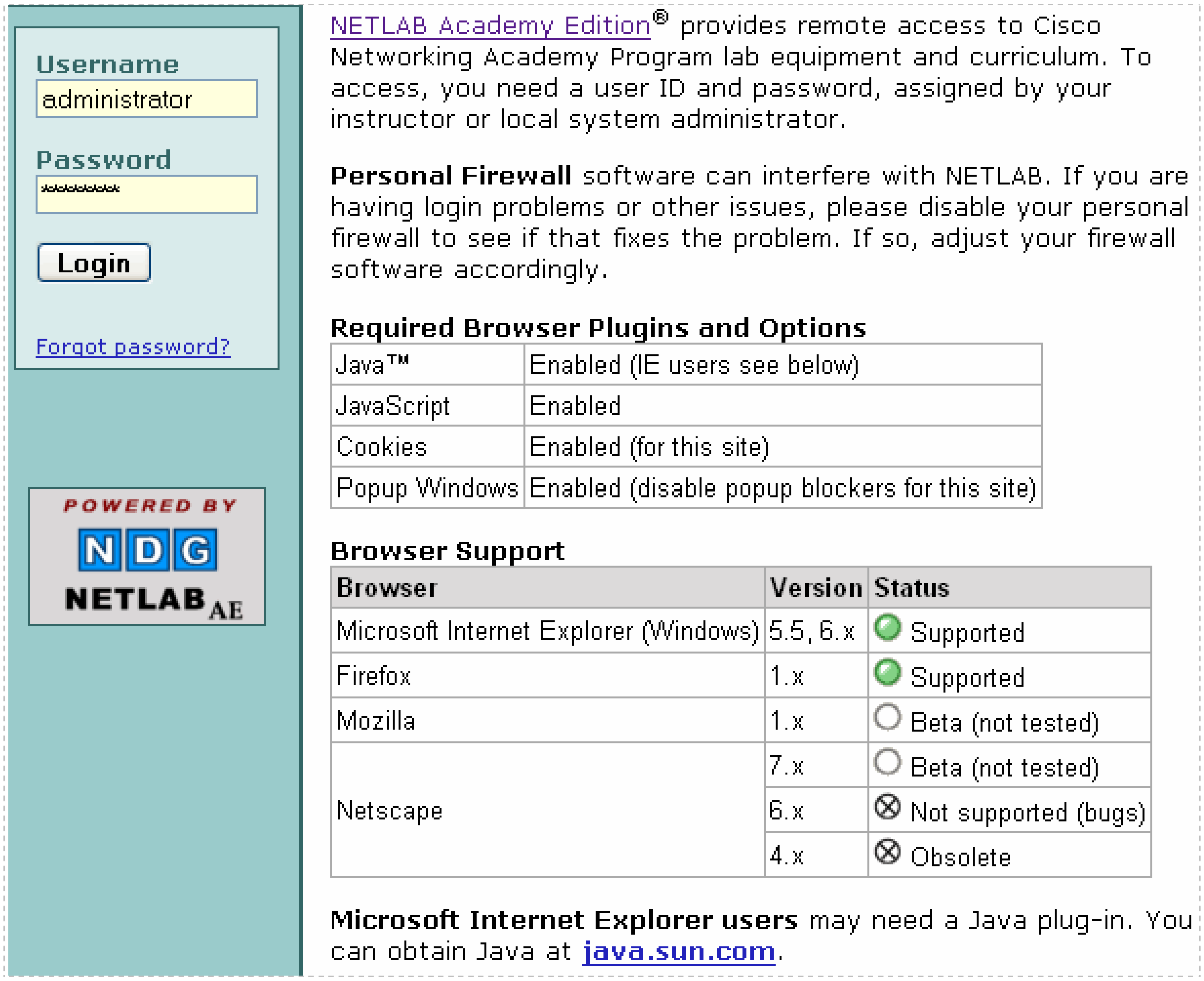
2.11 Connect to the Web-based Interface

After the IP configuration of the NETLAB+ server is complete, you will be able to access the web-based interface to perform the remainder of your configuration tasks. Using a PC connected to the LAN, open a web browser and connect to the web-based administrator interface of the NETLAB+ server by entering the IP address you assigned to the NETLAB+ server in the IP configuration step.


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Done
Internet

http://100.0.0.84/

The web browser should open the NETLAB+ login page allowing you to login using the administrator account.



Username
administrator

Password
****

NETLAB Academy Edition® provides remote access to Cisco Networking Academy Program lab equipment and curriculum. To access, you need a user ID and password, assigned by your instructor or local system administrator.

Personal Firewall software can interfere with NETLAB. If you are having login problems or other issues, please disable your personal firewall to see if that fixes the problem. If so, adjust your firewall software accordingly.

Required Browser Plugins and Options

Java™	Enabled (IE users see below)
JavaScript	Enabled
Cookies	Enabled (for this site)
Popup Windows	Enabled (disable popup blockers for this site)

Browser Support

Browser	Version	Status
Microsoft Internet Explorer (Windows)	5.5, 6.x	● Supported
Firefox	1.x	● Supported
Mozilla	1.x	○ Beta (not tested)
Netscape	7.x	○ Beta (not tested)
	6.x	⊗ Not supported (bugs)
	4.x	⊗ Obsolete

Microsoft Internet Explorer users may need a Java plug-in. You can obtain Java at java.sun.com.

2.12 Troubleshooting: Accessing the Web-based Administrative Interface

If the server is not accessible from the web browser of your PC, installation cannot continue. In order to continue installation, you must troubleshoot your connectivity problem now. Here are some things to try:

- The most common connectivity issue is incorrect cabling. Recheck the printed label on top of your NETLAB+ server to ensure that your server is connected to your LAN via Ethernet 0.

- To avoid routing issues, it is recommended that your PC and the NETLAB+ server be connected to the same LAN during the installation process. In this case, both your PC and the NETLAB+ server should have IP addresses within the same network range.

- Confirm that all configured IP parameters are correct and that this is the IP address you entered in your web browser's address bar.

- Test the LAN port used to connect the NETLAB+ server to your LAN to ensure that it is operational. This port should not be in a segregated VLAN that is inaccessible to other network ports.

- Test the Ethernet cable used to connect the NETLAB+ server to your LAN. This cable should operate at 100 Mbps. A manufactured cable should be used when available.

2.13 Login to Administrator Account

When prompted for the username and password, login as **administrator** using the default password **netlab**. Remember that NETLAB+ usernames and passwords are case sensitive.

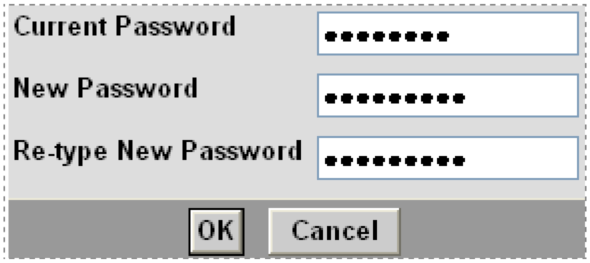
A password change is required during the initial login to the administrator account. You will be prompted to change the Administrator's password after you successfully login with the default password. This step is mandatory; choosing **Cancel** will log you out of the server, and require you to log in again.

To change the administrator password, enter the current password, and the new password. The new password must then be retyped. Select **OK** to change the password.

Passwords must meet the following requirements:

- Not found in the dictionary and not too simple
- Between 7 and 16 characters
- Contain both numbers and letters

An error message will be displayed if the new password does not meet these requirements.



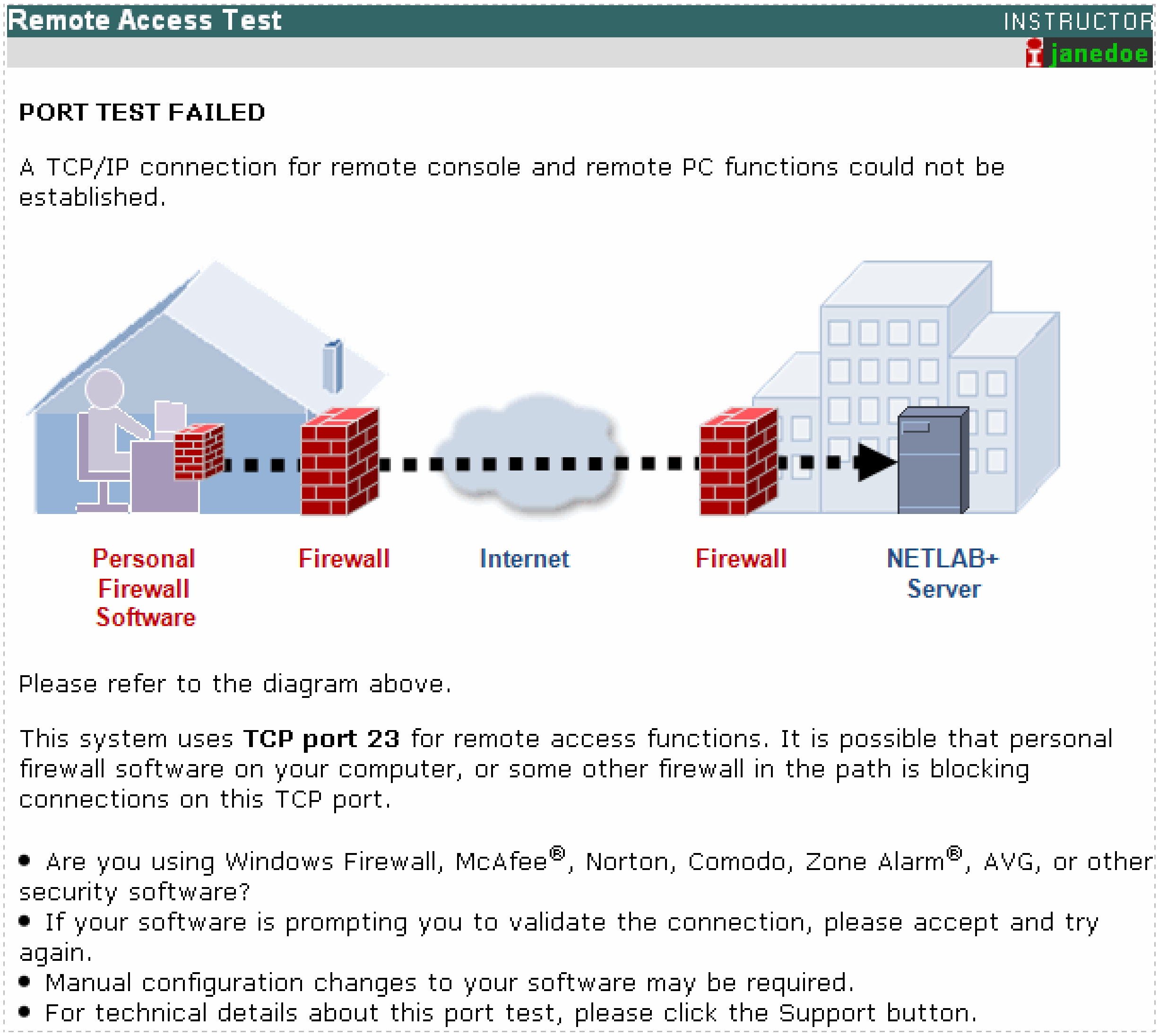
Current Password ●●●●●●●●
New Password ●●●●●●●●●
Re-type New Password ●●●●●●●●●

For additional information on the administrator account, see the Administrator Account section of the *NETLAB+ Administrator Guide*.

2.14 Remote Access Test

A Remote Access Test is performed during each user login. The purpose of the test is to attempt to establish an outbound TCP connection. This connection is necessary for remote device access, and remote PC access and access to chat functions (chat functions will be available in a future software release).

This test will fail if a connection using the TCP port(s) defined by the NETLAB+ administrator cannot be established. The procedure for defining ports for remote access is described in section 2.9.



PORT TEST FAILED

A TCP/IP connection for remote console and remote PC functions could not be established.

Please refer to the diagram above.

This system uses **TCP port 23** for remote access functions. It is possible that personal firewall software on your computer, or some other firewall in the path is blocking connections on this TCP port.

- Are you using Windows Firewall, McAfee®, Norton, Comodo, Zone Alarm®, AVG, or other security software?
- If your software is prompting you to validate the connection, please accept and try again.
- Manual configuration changes to your software may be required.
- For technical details about this port test, please click the Support button.

In this example, the Remote Access Test failed when instructor “janedoe” logged in.

NETLAB+ now allows the administrator to define the Remote Access Port (or list of ports) that may be used in place of the factory default, port 23.

It is critical that the ports specified are opened in the site firewall, or the client may experience delays and/or port test failures during user login.

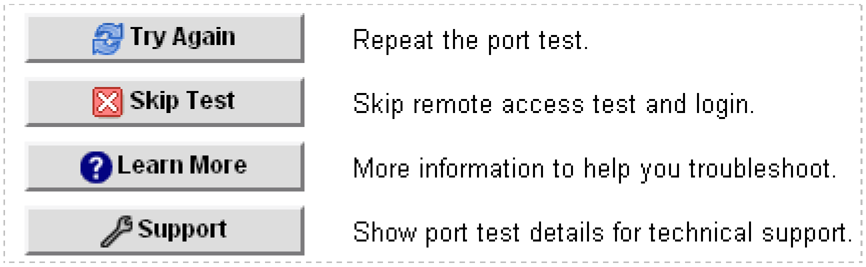
Please see section 2.9 for details on defining remote access ports.

There are several reasons why the Remote Access Test may fail:

1) Personal Firewall settings on your computer: The personal firewall software on your computer may be set by default to prohibit the port connection. This issue is routinely resolved by selecting to allow the connection when prompted by a pop-up window from your personal firewall software.

2) Security policy at your current location: It is possible that local security policy does not allow outbound access using the port(s) chosen by the NETLAB+ administrator. This is the most likely diagnosis if you are able to successfully access the system from another location.

3) Ports have not been opened in the site firewall: As part of the installation process, you must be certain to open the ports in the site firewall that have been designated available for outbound client connections. This is only likely to be the problem if all users are unable to establish a connection.

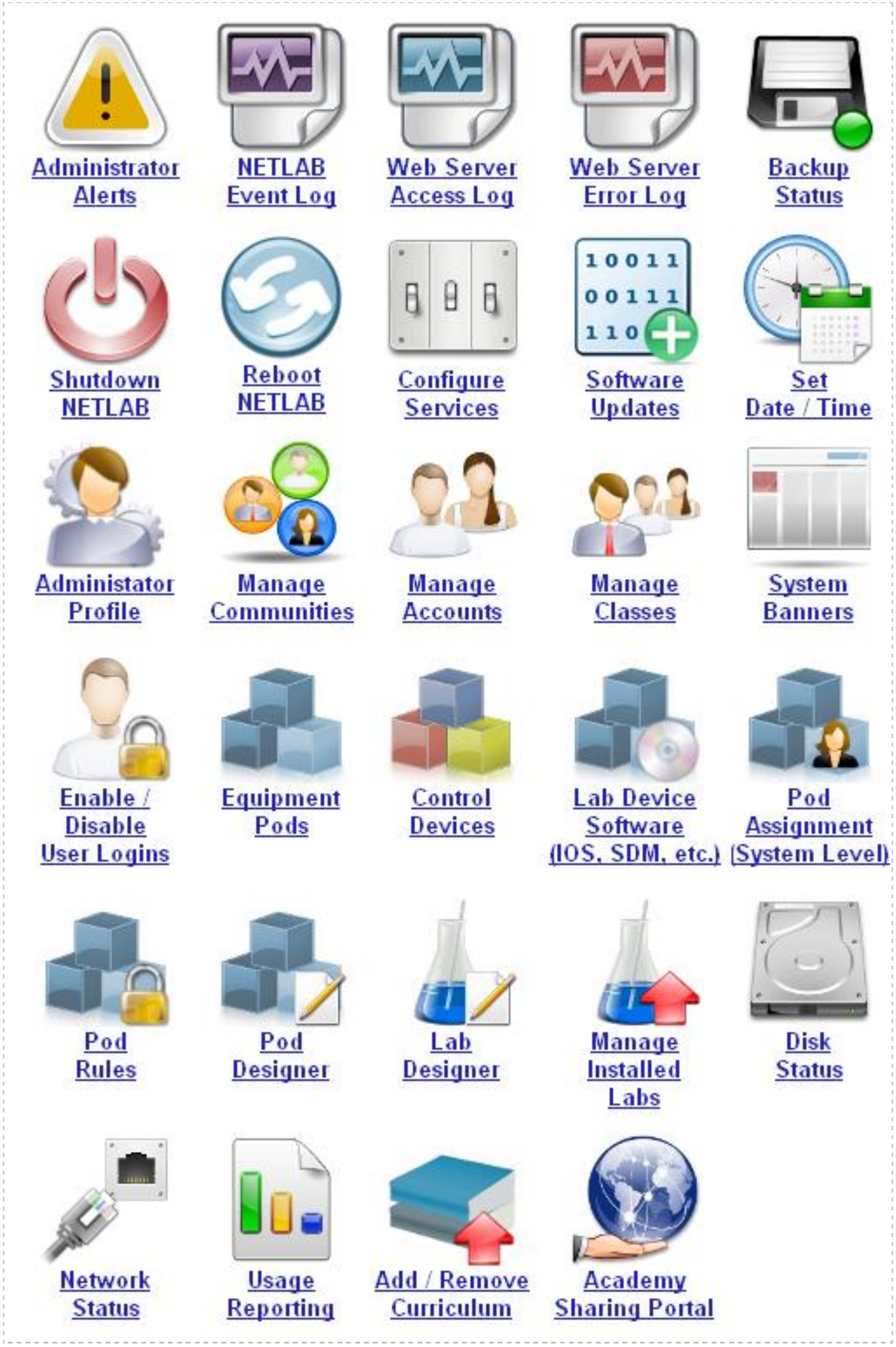


Try Again	Repeat the port test.
Skip Test	Skip remote access test and login.
Learn More	More information to help you troubleshoot.
Support	Show port test details for technical support.

Use the **"Try Again"** option if you wish to repeat the test after adjusting your personal firewall settings. You may select **"Skip Test"** if you prefer to proceed to your MyNETLAB page without resolving the issue at this time. You will not have remote device access, remote PC access or chat functions (chat functions will be available in a future software release).

2.15 Administrative Functions

After successful login, the Administration page will be displayed. Tasks may be selected by clicking on the icon or the function name.

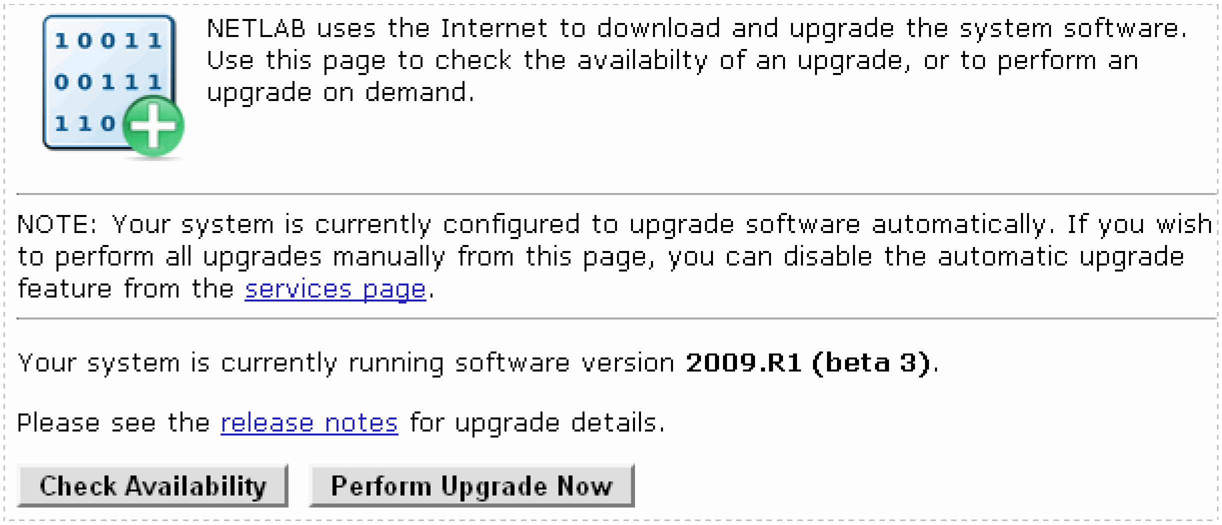


2.16 Check for Software Updates

It is recommended at this time to check for software updates. Your NETLAB+ server was shipped with the latest available software version installed. However, the possibility exists that a new software update may have become available while the server was enroute to your site. Checking to see if an update is available will allow you receive the updated version immediately.

Select Software Updates from the Administrator functions displayed. Select the **Check Availability** option. The NETLAB+ system will query the Central Support System to see if an updated version exists and display an informational message indicating whether an update is available. If an updated version is available, select **Perform Upgrade Now** to perform the software update.

It is recommended that the Software Update Service remain in its default configuration setting, which will allow the NETLAB+ system to receive software updates automatically. NETLAB+ will periodically check the Central Support site. If a software upgrade is available, it will be downloaded and installed when the lab is not in use.


NETLAB uses the Internet to download and upgrade the system software. Use this page to check the availabilty of an upgrade, or to perform an upgrade on demand.

NOTE: Your system is currently configured to upgrade software automatically. If you wish to perform all upgrades manually from this page, you can disable the automatic upgrade feature from the services page.

Your system is currently running software version **2009.R1 (beta 3)**.

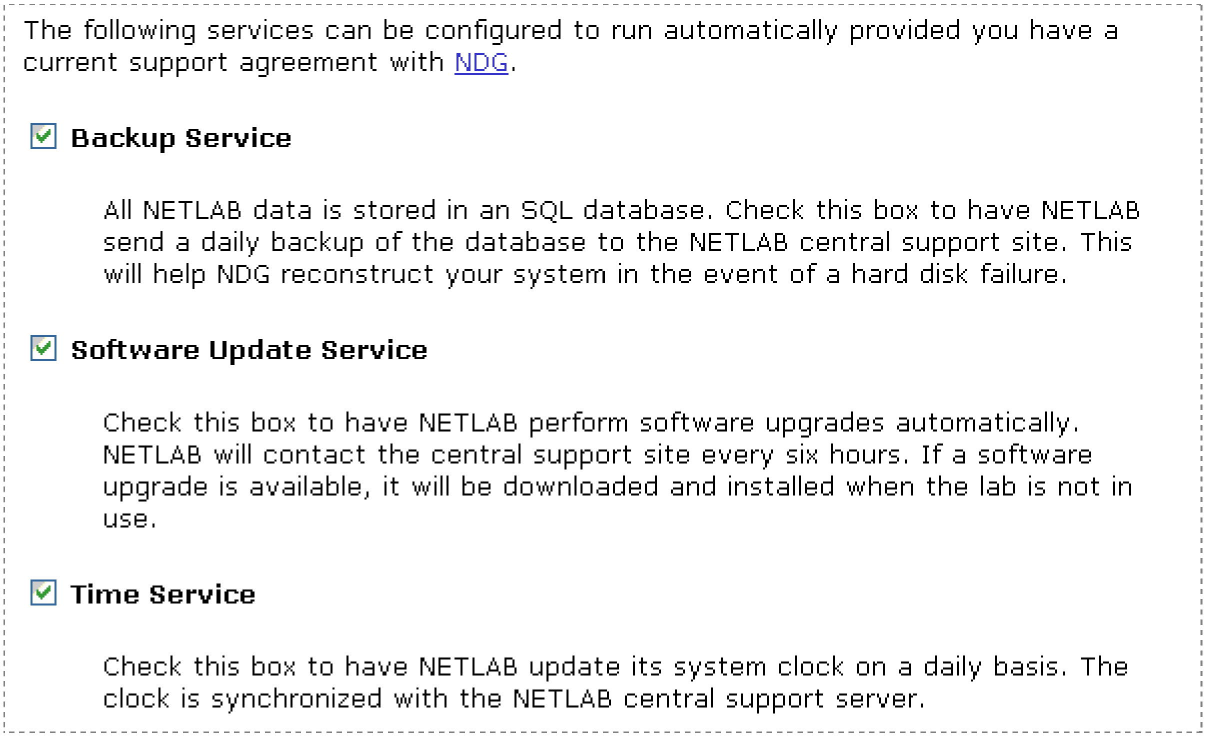
Please see the release notes for upgrade details.

For more information on the Software Update Service, please see the Software Updates section of the *NETLAB+ Administrator Guide*.

2.17 Configure Services

Next, select the Configure Services from the Administrator page. The first section of the page lists several services configured to run automatically. These services are available to all NETLAB+ systems with a current support agreement with the Network Development Group, Incorporated. If Backup Service, Software Update Service, and Time Service are enabled, your NETLAB+ database will be automatically backed up, software upgrades will be installed, and the system clock will be updated daily. These services are enabled by default. You must select **Update Settings** at the bottom of the page to save any changes made to these settings.

It is strongly recommended that these services remain enabled.



The following services can be configured to run automatically provided you have a current support agreement with NDG.

☑ **Backup Service**

All NETLAB data is stored in an SQL database. Check this box to have NETLAB send a daily backup of the database to the NETLAB central support site. This will help NDG reconstruct your system in the event of a hard disk failure.

☑ **Software Update Service**

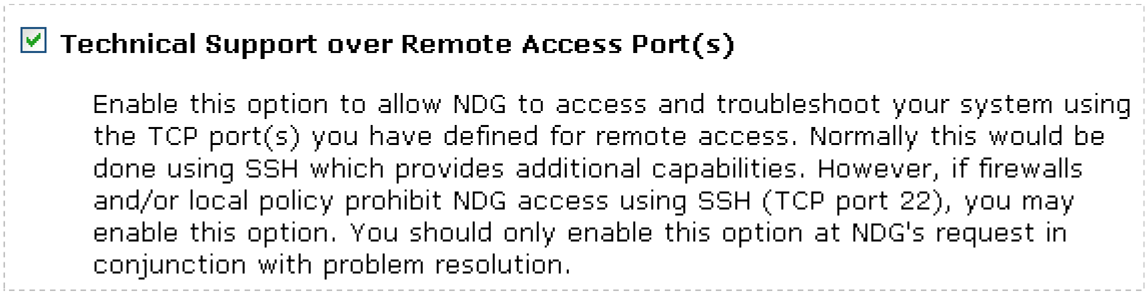
Check this box to have NETLAB perform software upgrades automatically. NETLAB will contact the central support site every six hours. If a software upgrade is available, it will be downloaded and installed when the lab is not in use.

☑ **Time Service**

Check this box to have NETLAB update its system clock on a daily basis. The clock is synchronized with the NETLAB central support server.

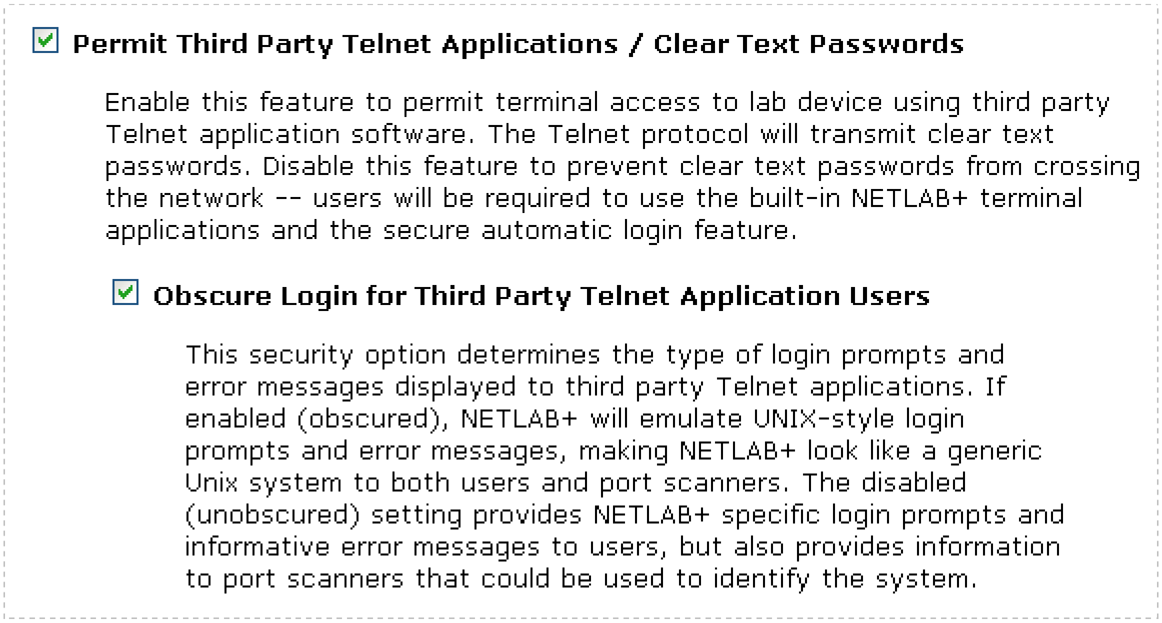
The Technical Support Over Remote Access Ports Service is used for troubleshooting only, and should only be enabled at the suggestion of the product vendor.

.



☑ **Technical Support over Remote Access Port(s)**

Enable this option to allow NDG to access and troubleshoot your system using the TCP port(s) you have defined for remote access. Normally this would be done using SSH which provides additional capabilities. However, if firewalls and/or local policy prohibit NDG access using SSH (TCP port 22), you may enable this option. You should only enable this option at NDG's request in conjunction with problem resolution.



☑ **Permit Third Party Telnet Applications / Clear Text Passwords**

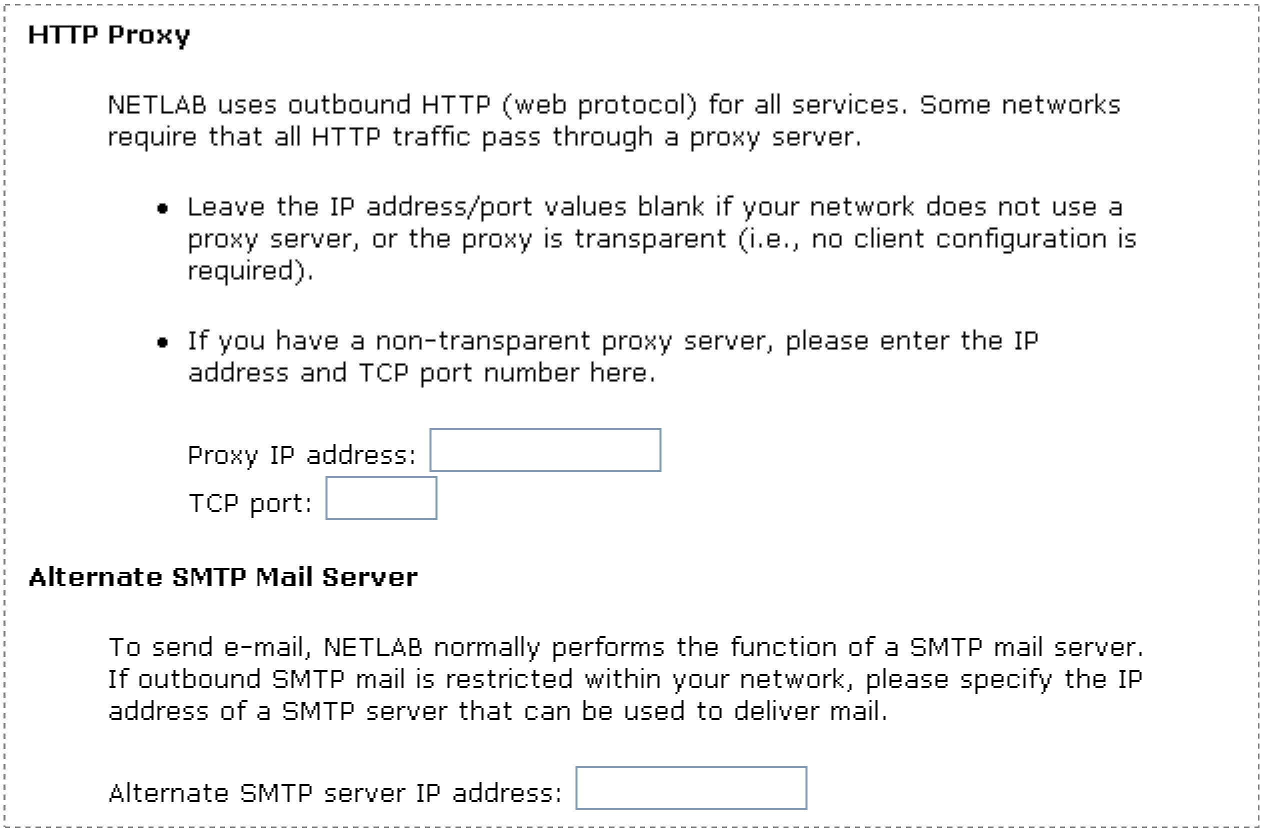
Enable this feature to permit terminal access to lab device using third party Telnet application software. The Telnet protocol will transmit clear text passwords. Disable this feature to prevent clear text passwords from crossing the network -- users will be required to use the built-in NETLAB+ terminal applications and the secure automatic login feature.

☑ **Obscure Login for Third Party Telnet Application Users**

This security option determines the type of login prompts and error messages displayed to third party Telnet applications. If enabled (obscured), NETLAB+ will emulate UNIX-style login prompts and error messages, making NETLAB+ look like a generic Unix system to both users and port scanners. The disabled (unobscured) setting provides NETLAB+ specific login prompts and informative error messages to users, but also provides information to port scanners that could be used to identify the system.

If your site has a non-transparent proxy server, you must enter the IP address and TCP port number in the indicated fields on this page. These values are only required for proxy servers that are non-transparent. If the proxy server at your site does not require manual client configuration, the fields should be left blank. If changes are made to the proxy server settings, click the **Update Settings** button to apply the new values.

Although NETLAB+ provides an HTTP proxy server setting, it will only work with proxies that do not interfere with HTTP. NDG cannot provide support for problems caused by proxy servers.



HTTP Proxy

NETLAB uses outbound HTTP (web protocol) for all services. Some networks require that all HTTP traffic pass through a proxy server.

- Leave the IP address/port values blank if your network does not use a proxy server, or the proxy is transparent (i.e., no client configuration is required).
- If you have a non-transparent proxy server, please enter the IP address and TCP port number here.

Proxy IP address:

TCP port:

Alternate SMTP Mail Server

To send e-mail, NETLAB normally performs the function of a SMTP mail server. If outbound SMTP mail is restricted within your network, please specify the IP address of a SMTP server that can be used to deliver mail.

Alternate SMTP server IP address:

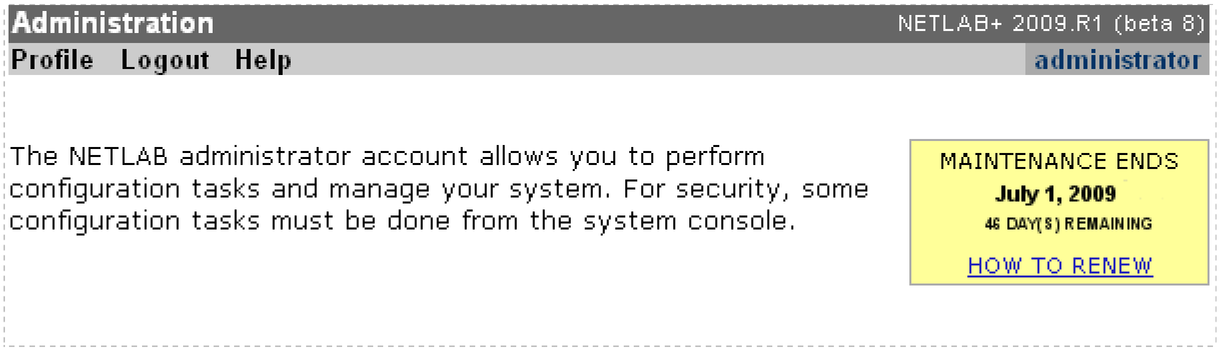
NETLAB+ performs SMTP services to deliver email as part of the configurable services offered to administrators and instructors. If email delivery is restricted within your network to a specific SMTP server, you can configure NETLAB+ to use the SMTP server at your site to deliver email. This configuration is not tested for all SMTP servers or configurations. Some mail servers may not deliver email generated from NETLAB+ due to restrictions based on email headers.

If you enter an Alternate SMTP Mail Server IP address, click the **Update Settings** button.

2.18 Maintenance Reminder

For your convenience, your NETLAB+ system displays the status of your system maintenance agreement. The maintenance fee covers the cost of technical support and software updates.

The last day of your current maintenance agreement is displayed in the upper right-hand corner main page when logged in to the administrator account. This notice will be displayed in green until 60 days before the maintenance end date. The status message will then change from green to yellow. You can review your renewal options by selecting the **Please Renew** link.



The NETLAB administrator account allows you to perform configuration tasks and manage your system. For security, some configuration tasks must be done from the system console.

MAINTENANCE ENDS
July 1, 2009
46 DAY(S) REMAINING
HOW TO RENEW

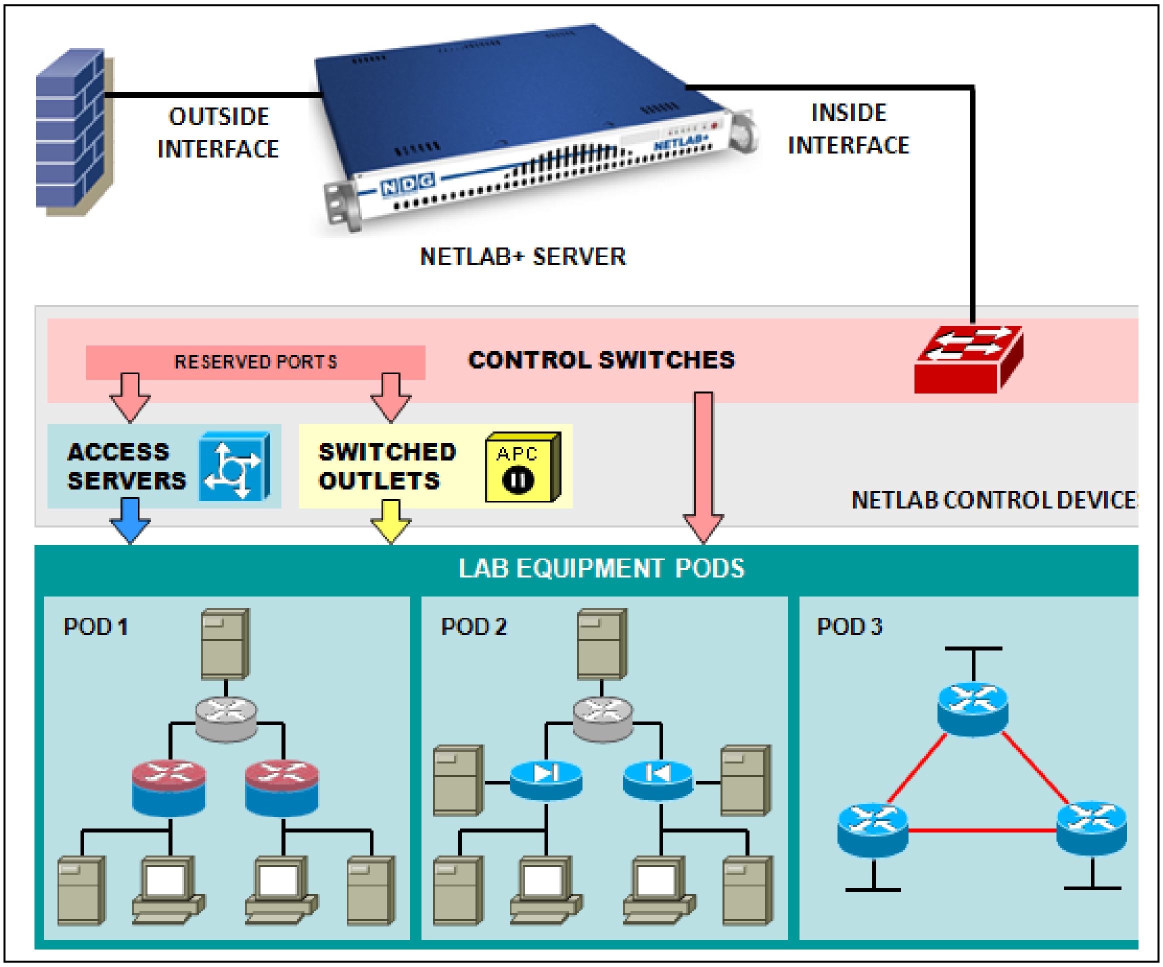
If your maintenance agreement is not renewed by the maintenance end date, the notification message color will change from yellow to red. You are strongly encouraged to make immediate arrangements to continue maintenance to avoid any disruption of services.

You may find it helpful to enable the display of the maintenance reminder to instructors who use the system on a regular basis. This is recommended particularly if you do not log into the administrator account frequently. Please refer to the *NETLAB+ Administrator Guide* for more information.

3 Installing The Control Plane

The NETLAB+ *control plane* forms the foundation needed to interconnect various components of the NETLAB+ system. The control plane consists of devices that are required in order for NETLAB+ to function, but are not accessible to students and instructors.

Control devices may be control switches, access servers, or switched outlet devices.



Control switches provide internal connectivity between NETLAB+, access servers, remote PCs, and switched outlet devices. The control switch also provides a network path for NETLAB+ to download IOS images to Cisco lab devices in the event flash has been erased (or the correct image is not installed).

Access servers provide console connections to lab routers, lab switches, and lab firewall devices so that users can access these devices from NETLAB+.

Switched outlets provide managed electrical power, allowing NETLAB+ and users to turn lab equipment on and off.

Careful planning is necessary in order to make efficient use of your equipment. Port requirements vary depending on the type and number of pods you will be installing in NETLAB+.

The port requirements for control devices of each pod type are listed in the table below. Each pod type requires control switch ports, access server lines, and switched outlets.

Port Requirements Reference Table				
Pod Types	**Control Switch**		**Access Server Lines**	**Switched Outlets**
	Pod Ports	**Reserved Ports**		
Basic Router Pod V1	3	0	3	3
Basic Router Pod V2 (PCs)	6	1	3	3
Cuatro Router Pod	8	1	4	4
Basic Switch Pod V1	3	0	3	3
Basic Switch Pod V2 (PCs)	4	1	3	3
Cuatro Switch Pod	4	1	4	4
Advanced Router Pod	3	0	3	3
Advanced Switch Pod	8	0	8	8
Network Security Pod 2.0	11	1	2	2
Security Router Pod (FNSR)	10	3	2	2
Security PIX Pod (FNSP)	14	3	2	2
CCNA 2.1 Pod	6	0	6	6
Custom Pods	As needed based on your unique requirements			

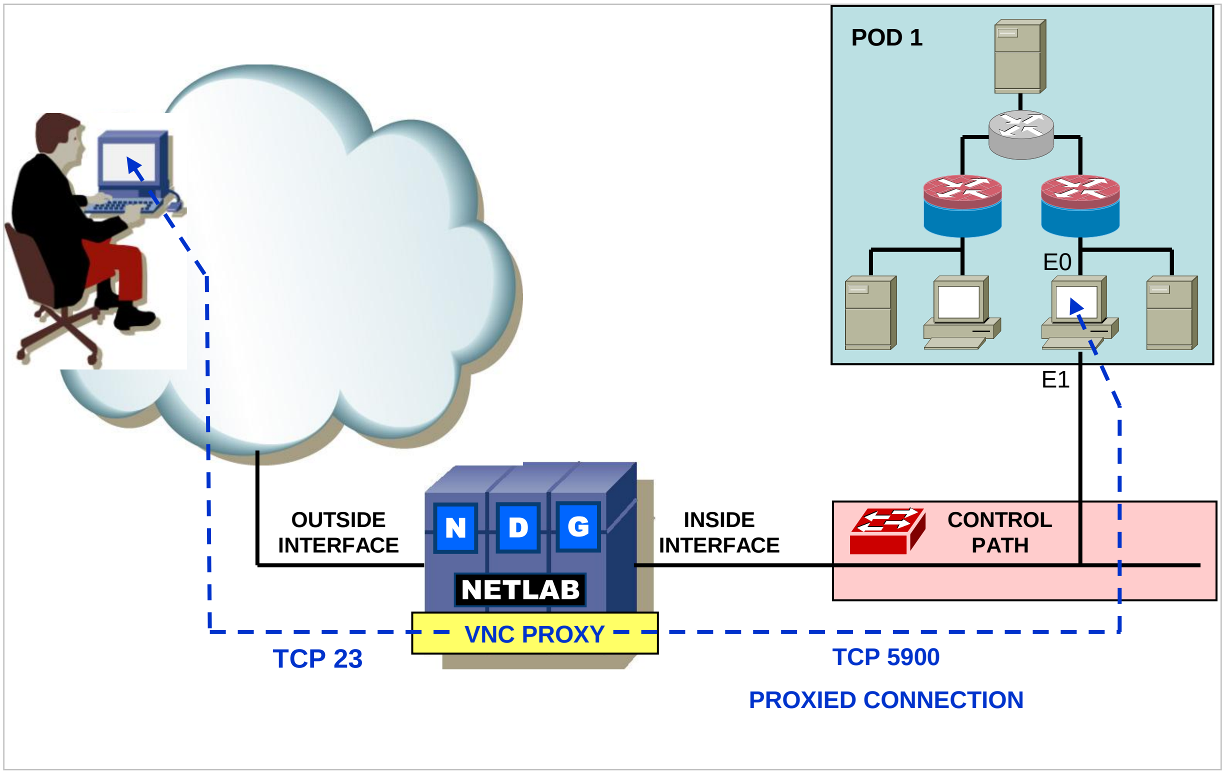
Control switch ports are broken down into *pod ports* and *reserved ports*.

Pod ports connect lab equipment to NETLAB+. During normal operation, pod ports are automatically placed in unique or common VLANs to simulate one or more Ethernet segments required by the topology of the pod. In the event that NETLAB+ must download an IOS image to a lab device, NETLAB+ will temporarily place the device in

VLAN 1 so that it can access the NETLAB+ TFTP server. Pod ports must be consecutive and reside on the same switch. A single control switch can have pod ports for several pods, as long as all pod ports are consecutive on the switch.

The *reserved ports* on a control switch provide the framework to interconnect NETLAB+ and control devices. Reserved ports always operate in VLAN 1 and provide a common network for NETLAB+ to communicate with control devices. A reserved port is never allocated to equipment pods, thus the name “reserved”.

Reserved ports are also used by standalone remote PCs in conjunction with Virtual Network Computing (VNC). VNC provides a method to remotely access the keyboard, video, and mouse. A remote PC that offers VNC typically has two network interfaces. One interface connects to the lab topology; the other connects to a reserved port on a control switch. The VNC connection traverses the control plane and is proxied back to a Java-based VNC client window on the user’s workstation.



Pods that do not have remote PCs do not require reserved ports.

Reserved ports operate in VLAN 1, so there are no consecutive port requirements. However, it is desirable to connect NETLAB+, access servers, switched outlet devices, and all other control switches to Control Switch 1, in a hub and spoke fashion. You should avoid cascading control switches.

You can change the number of reserved ports on each switch as required. The most efficient scheme is to allocate from the highest port and work towards the lowest. For pod ports, you work from lowest to highest.

The next table illustrates an example of the control port requirements for a NETLAB$_{AE}$ system, based on the selection of pods for the site. In this example, two Basic Router Pods, a Basic Switch Pod, a Security Router Pod and a Security PIX Pod will be installed in NETLAB+. The values for port requirements are taken from the Port Requirements Reference table for each pod type.

Port Requirements Example

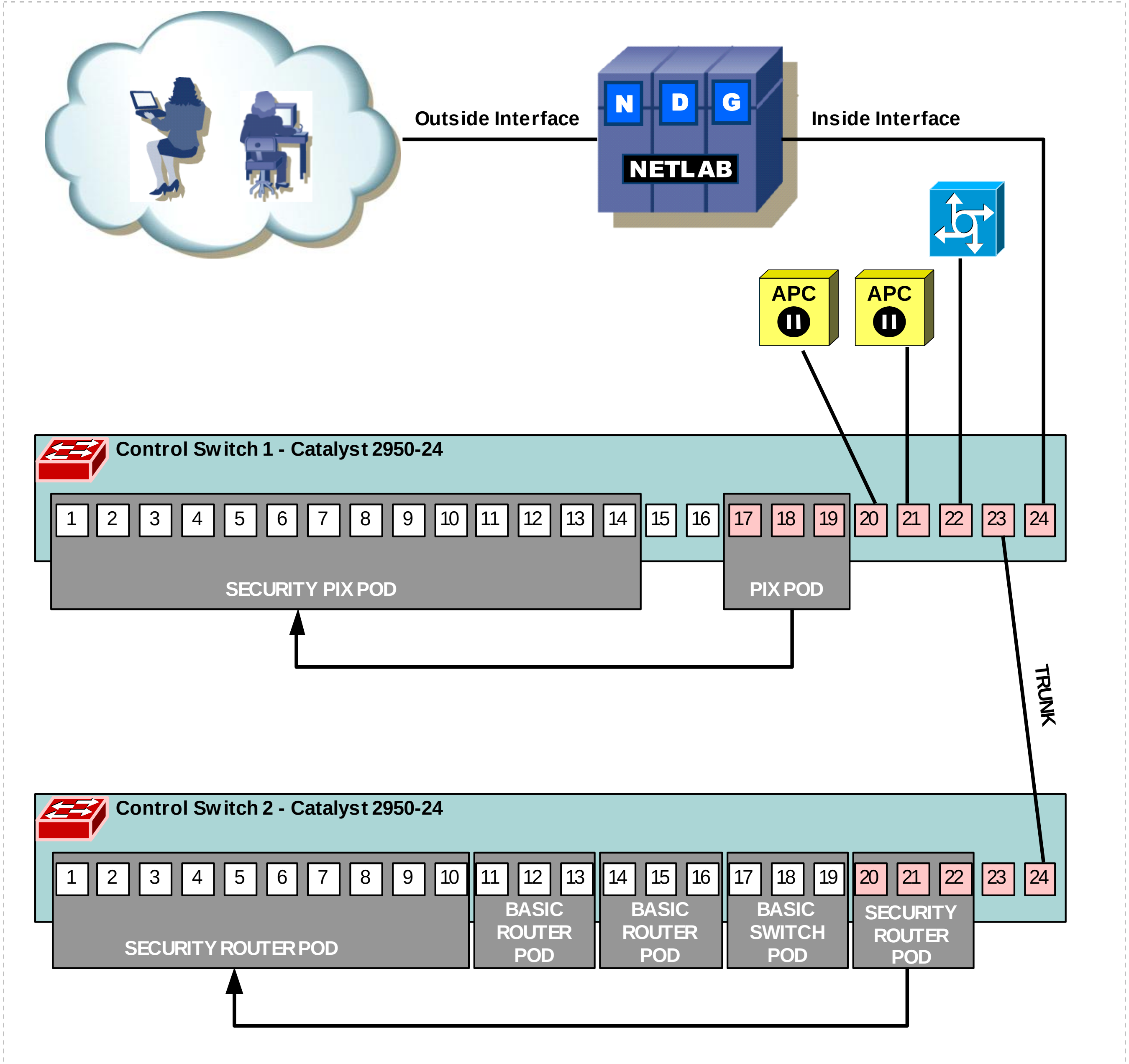
POD	Type	Control Switch		Access Server Lines	Switched Outlets
		Pod Ports (consecutive)	Reserved Ports		
1	Basic Router Pod V1	3	0	3	3
2	Basic Router Pod V1	3	0	3	3
3	Basic Switch Pod V1	3	0	3	3
4	Security Router Pod	10	3	2	2
5	Security PIX Pod	14	3	2	2
	Total	**33**	**6**	**13**	**13**

The total number of access server lines and switched outlet ports can be simply added up. We will use a 16-port Cisco 2511-RJ to provide the 13 necessary access server lines. We will use two 8-port APC 7900 Switched Rack PDUs to provide the 13 switched outlet devices.

Less straightforward is the total number of control switches needed. Since the pod ports for each pod must be consecutive and on the same switch, you will need to fit everything into place carefully. Also, it will be necessary to use ports on the control switches to connect to the NETLAB+ server, trunk switches together and to connect each access server and switched outlet device. First, let’s compute the minimum number of control switch ports we need.

Control Switch Port Requirements Example	
	Control Switch Ports
Pod Ports (from above)	33
Reserved Ports (from above)	6
NETLAB+ server inside port	1
Access Servers	1
Switched Outlet Devices	2
Trunks to other control switches	2 (estimated)
Total	**45**

We have now calculated that we need at least 45 control switch ports. This might fit on two 24-port Cisco 2950 switches. However, the consecutive requirement for pod ports might make this difficult. By careful arrangement of the pods and reserved ports, we can indeed fit this on two 24-port control switches:



The red-shaded ports are reserved ports. Normally NETLAB+ reserves port 17 to 24 on a 24 port control switch. On control switch 1, this range worked out fine. On control switch 2, we changed the reserved range to 20-24 in order to free up pod ports 17-19 for the Basic Switch Pod.

Use the table below to calculate the port slot requirements for your installation. First, write down the pod type for each pod that you plan to install. Then, just as in the example above, enter in the values for each pod from the Port Requirements Reference Table.

Pod	Type	Control Switch		Access Server Lines	Switched Outlets
		Pod Ports	Reserved Ports		
1					
2					
3					
4					
5					
6					
7					
8					
9					
	Total				

Continue the process calculating the additional control switches needed for your NETLAB+.

Control Switch Port Requirements	
	Control Switch Ports
Pod Ports (from above)	
Reserved Ports (from above)	
NETLAB+ server inside port	1
Access Servers	
Switched Outlet Devices	
Trunks to other control switches	
Total	

3.1 Install Control Switches

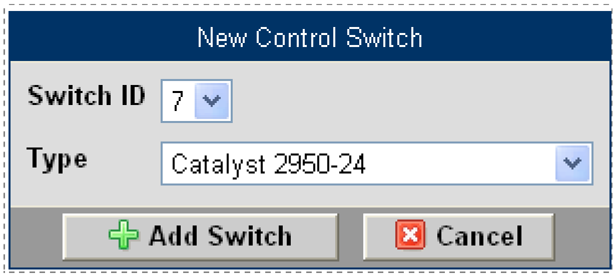
Log into NETLAB+ using the **administrator** account (see 2.13) and select the **Control Devices** function.

Select **Control Switches** from the Manage Control Devices page. Depending on your specific pod topology and hardware, you may need to configure one or more control switches for the pod.

If this is not the first control switch to be installed on the system, the existing control switches will be displayed.

Select the option to **Add a control switch**, from the Configure Control Switches screen. The Add Control Switch Screen will be displayed.

Select a switch ID and switch type, then click **Add Switch**. Based on your selections, you will be able to view and set other parameters for the switch on the next screen.

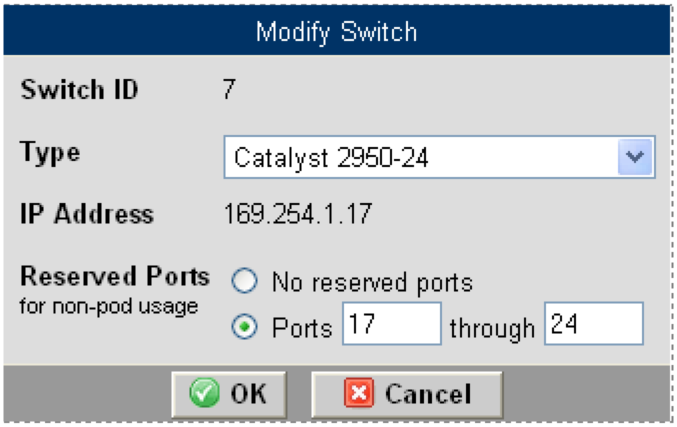

New Control Switch

Switch ID: 7

Type: Catalyst 2950-24

Edit the information for this control switch as needed, and then click **OK**. Some of the values cannot be changed. Normally NETLAB+ reserves port 17 to 24 on a 24 port control switch. To meet your specific port requirements, (see section 3) you may change the range of reserved ports being used on the switch.

After editing the information as needed, select **OK**. The Control Switch Management screen will be displayed.



Modify Switch

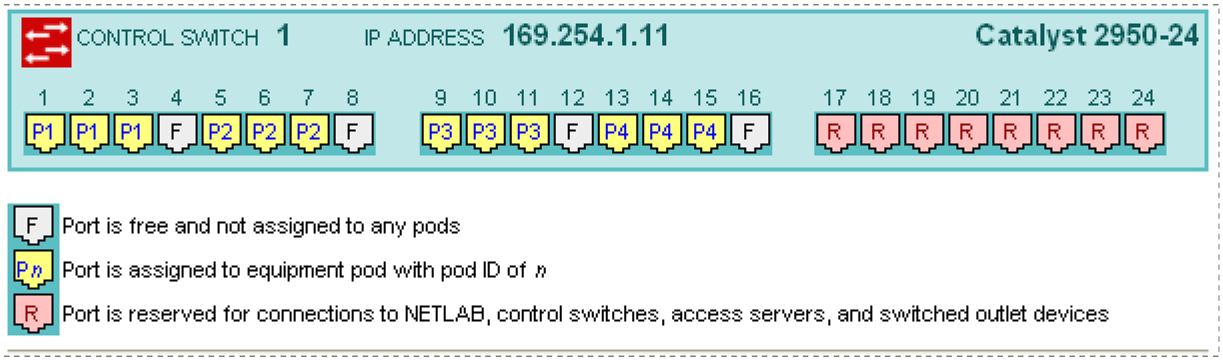
Switch ID 7

Type Catalyst 2950-24

IP Address 169.254.1.17

Reserved Ports for non-pod usage
○ No reserved ports
● Ports 17 through 24

The Control Switch Management screen displays a diagram showing the port assignments for the selected switch.



CONTROL SWITCH 1 IP ADDRESS 169.254.1.11 Catalyst 2950-24

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
P1	P1	P1	F	P2	P2	P2	F	P3	P3	P3	F	P4	P4	P4	F	R	R	R	R	R	R	R	R

F Port is free and not assigned to any pods

P*n* Port is assigned to equipment pod with pod ID of *n*

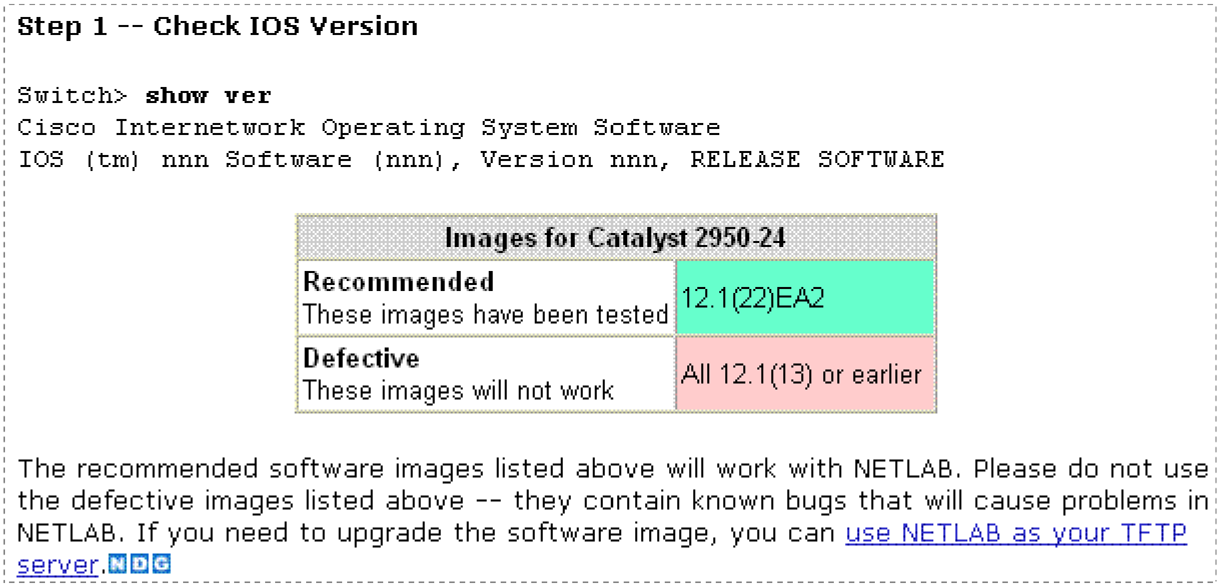
R Port is reserved for connections to NETLAB, control switches, access servers, and switched outlet devices

# Configure You must configure the IOS software on the control switch before it can be used by NETLAB+. To perform this task, we assume that:

- Your NETLAB+ server and control switches are turned on
- Everything is cabled correctly, see section 4.12
- All ports in the path between the control switch and the NETLAB+ server are up (green)
- You have connected a PC or terminal to the console port of the control switch and you are at the Switch> prompt

Carefully follow the steps listed on the configure control switch screen.

The specific settings depicted may differ from the settings for your site.

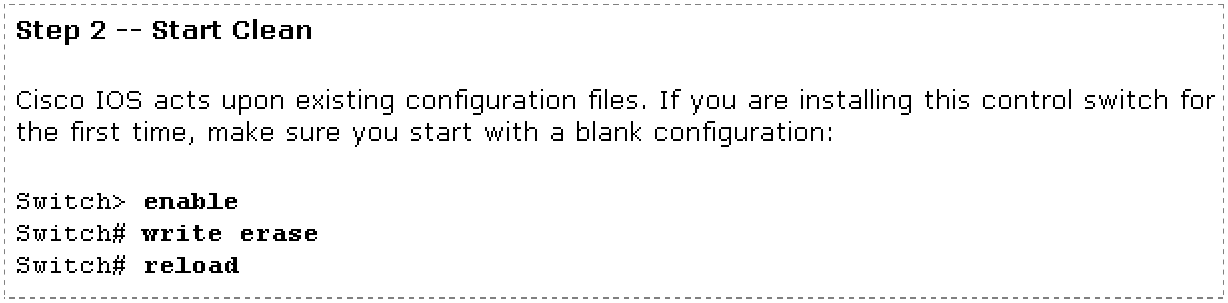


Step 1 -- Check IOS Version

```
Switch> show ver
Cisco Internetwork Operating System Software
IOS (tm) nnn Software (nnn), Version nnn, RELEASE SOFTWARE
```

Images for Catalyst 2950-24	
Recommended These images have been tested	12.1(22)EA2
Defective These images will not work	All 12.1(13) or earlier

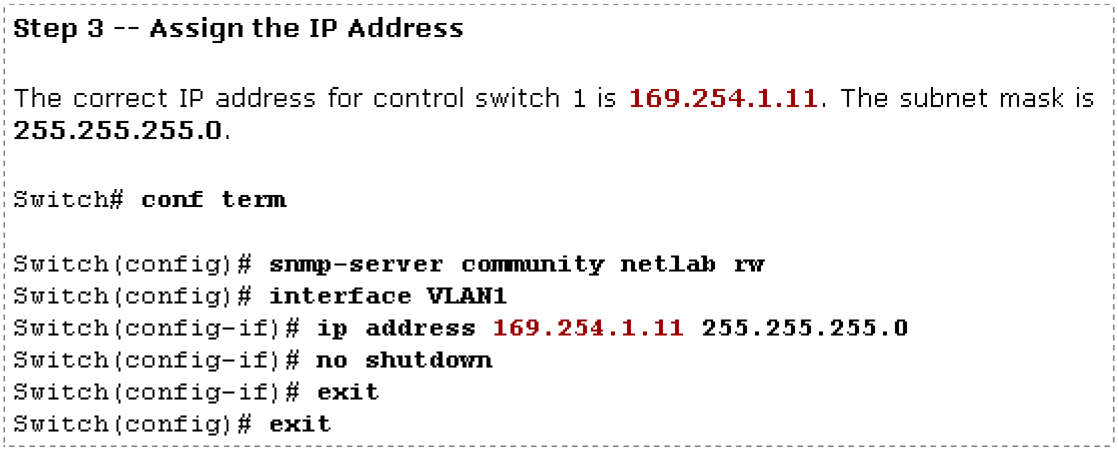
The recommended software images listed above will work with NETLAB. Please do not use the defective images listed above -- they contain known bugs that will cause problems in NETLAB. If you need to upgrade the software image, you can use NETLAB as your TFTP server.



Step 2 -- Start Clean

Cisco IOS acts upon existing configuration files. If you are installing this control switch for the first time, make sure you start with a blank configuration:

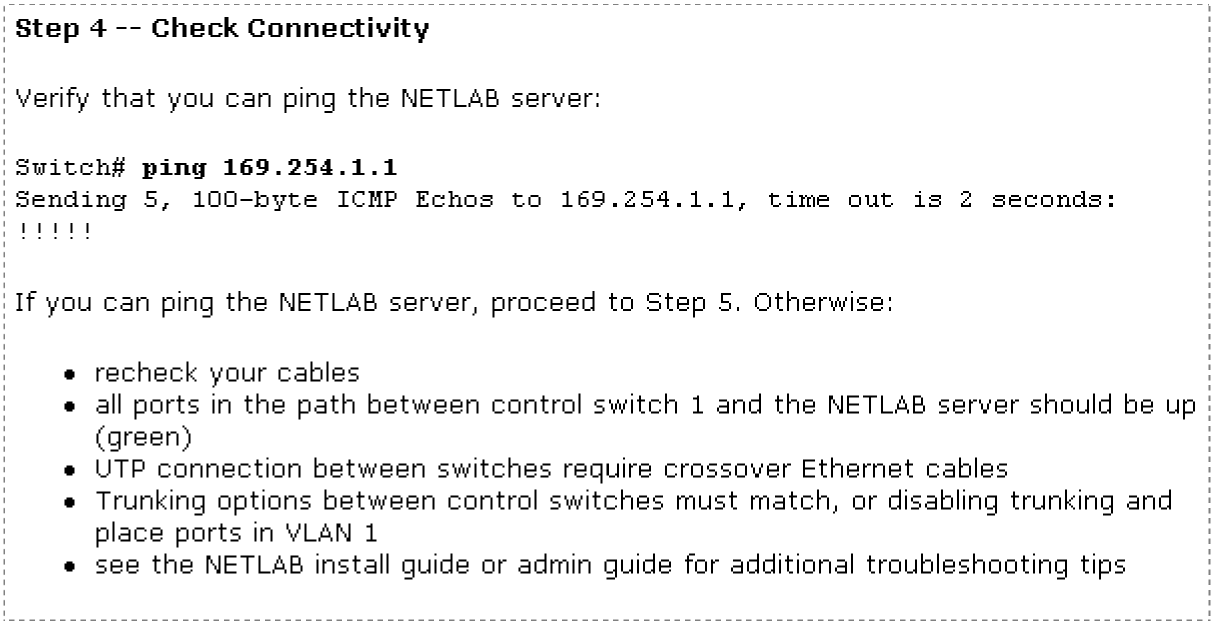
```
Switch> enable
Switch# write erase
Switch# reload
```



Step 3 -- Assign the IP Address

The correct IP address for control switch 1 is **169.254.1.11**. The subnet mask is **255.255.255.0**.

```
Switch# conf term

Switch(config)# snmp-server community netlab rw
Switch(config)# interface VLAN1
Switch(config-if)# ip address 169.254.1.11 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# exit
```



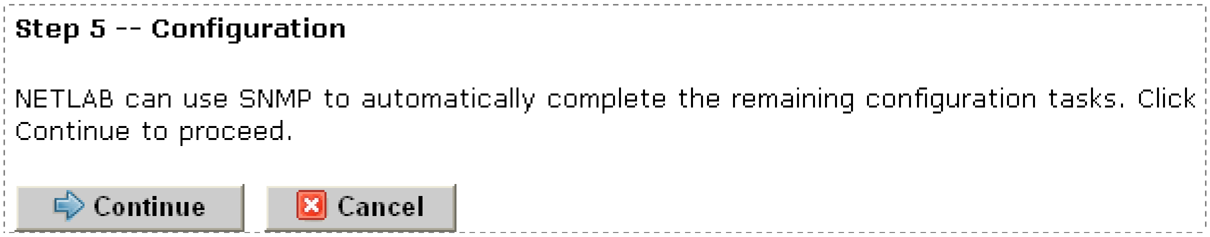
Step 4 -- Check Connectivity

Verify that you can ping the NETLAB server:

```
Switch# ping 169.254.1.1
Sending 5, 100-byte ICMP Echos to 169.254.1.1, time out is 2 seconds:
!!!!!
```

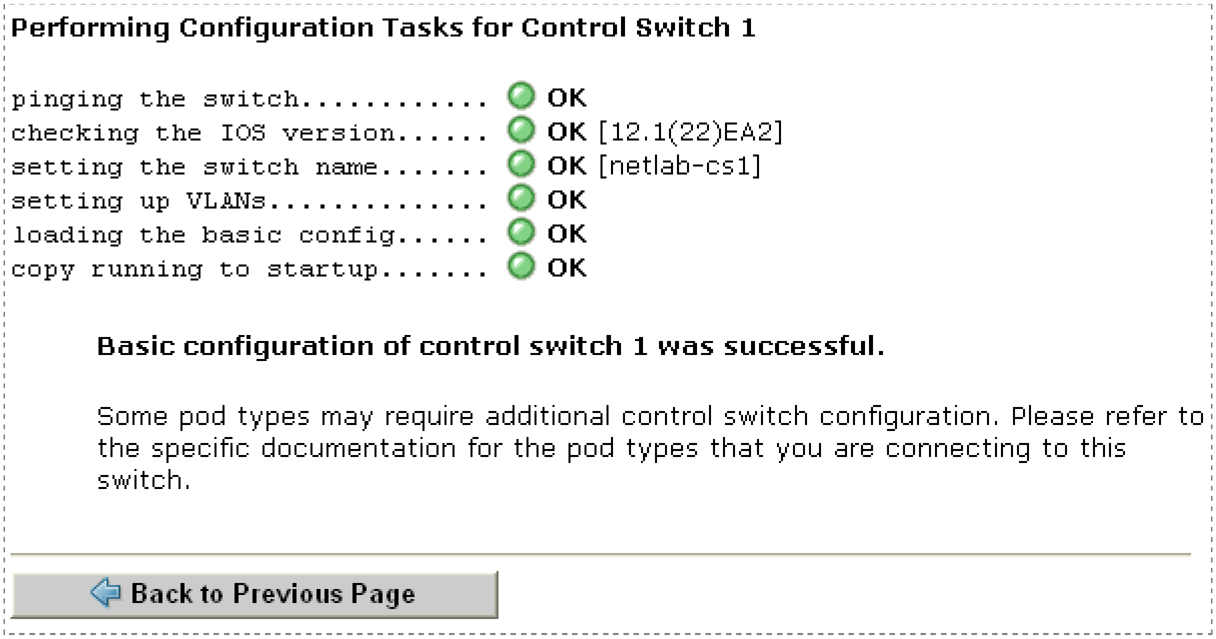
If you can ping the NETLAB server, proceed to Step 5. Otherwise:

- recheck your cables
- all ports in the path between control switch 1 and the NETLAB server should be up (green)
- UTP connection between switches require crossover Ethernet cables
- Trunking options between control switches must match, or disabling trunking and place ports in VLAN 1
- see the NETLAB install guide or admin guide for additional troubleshooting tips



Step 5 -- Configuration

NETLAB can use SNMP to automatically complete the remaining configuration tasks. Click Continue to proceed.



Performing Configuration Tasks for Control Switch 1

```
pinging the switch............ ● OK
checking the IOS version...... ● OK [12.1(22)EA2]
setting the switch name....... ● OK [netlab-cs1]
setting up VLANs.............. ● OK
loading the basic config...... ● OK
copy running to startup....... ● OK
```

Basic configuration of control switch 1 was successful.

Some pod types may require additional control switch configuration. Please refer to the specific documentation for the pod types that you are connecting to this switch.

NETLAB+ automatically sets control switch passwords as shown. You will need to enter these passwords if you wish to access the command line interface of the device at a later time.

Console Password: **router**
Enable Password: **cisco**

See the Control Switches section of the *NETLAB+ Administrator Guide* for more information on control switches.

3.2 Install Access Server

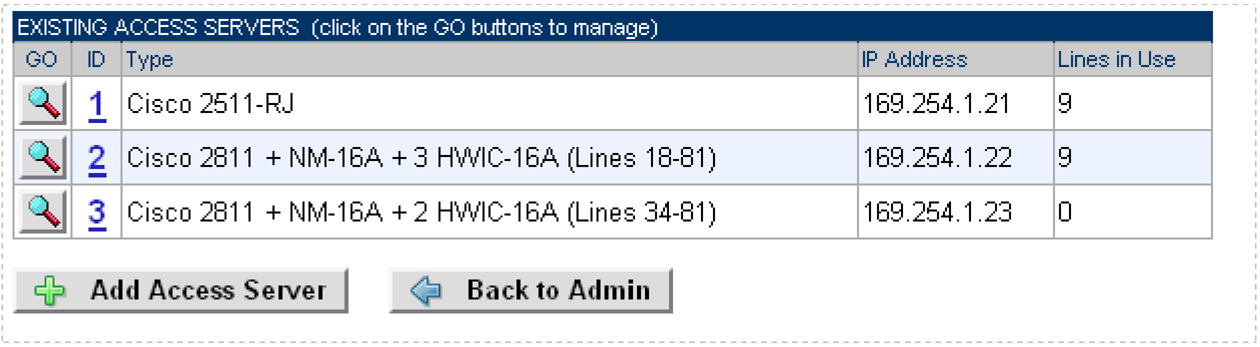
Select **Access Server** from the Manage Control Devices page.

If this is not the first access server to be installed on the system, the existing access servers will be displayed.

Line Number is now used as a unique identifier for access server ports.
Beginning with NETLAB+ version 2010.R3, NETLAB+ supports an expanded selection of access servers,   Since several models include multiple modules, port number is no longer a unique identifier. Instructions for adding/modifying pods and access servers throughout this guide use access server line numbers for identification.

You can easily view the line number of any access server port. Examples are provided below.

Details on supported access server configurations and general usage guidelines can be found at: http://www.netdevgroup.com/ae/controldevices.htm#accessservers

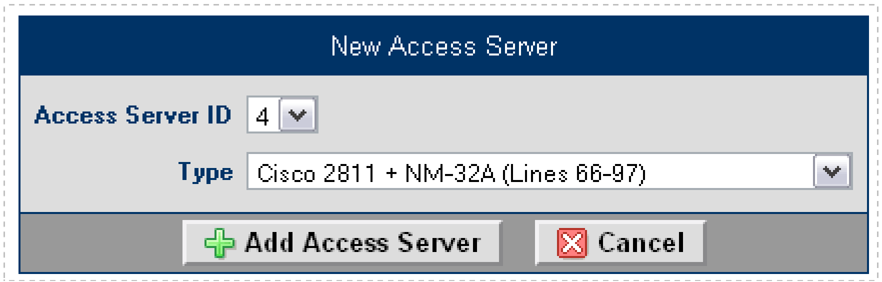


EXISTING ACCESS SERVERS (click on the GO buttons to manage)

GO	ID	Type	IP Address	Lines in Use
🔍	1	Cisco 2511-RJ	169.254.1.21	9
🔍	2	Cisco 2811 + NM-16A + 3 HWIC-16A (Lines 18-81)	169.254.1.22	9
🔍	3	Cisco 2811 + NM-16A + 2 HWIC-16A (Lines 34-81)	169.254.1.23	0

Select **Add an Access Server** from the Configure Access Server screen. The New Access Server screen will be displayed.

Select an access server ID and type, and then click **Add Access Server**.



New Access Server

Access Server ID: 4

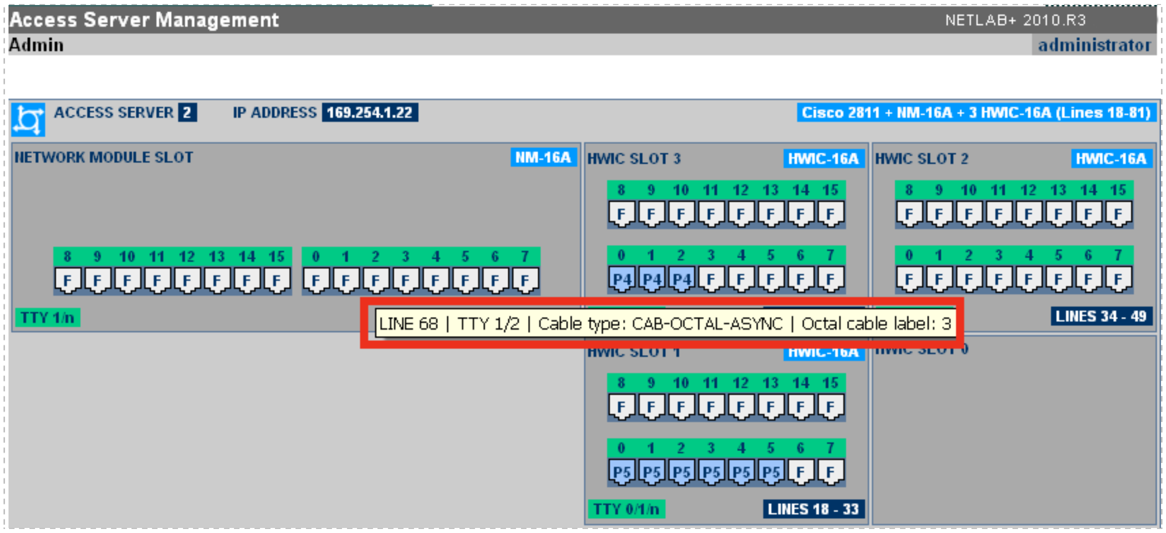
Type: Cisco 2811 + NM-32A (Lines 66-97)

You may change the access server's type as needed, only if the same line numbers in use exist on the new access server.

The Access Server Management screen displays a diagram showing the port assignments and line numbers for the selected access server. As shown below, you can easily view the line number by hovering your mouse over any port.

The specific settings depicted here may differ from the settings at your site.

For access servers using octal cables, the octal cable label is displayed with the line number.



Access Server Management

NETLAB+ 2010.R3

Admin

administrator

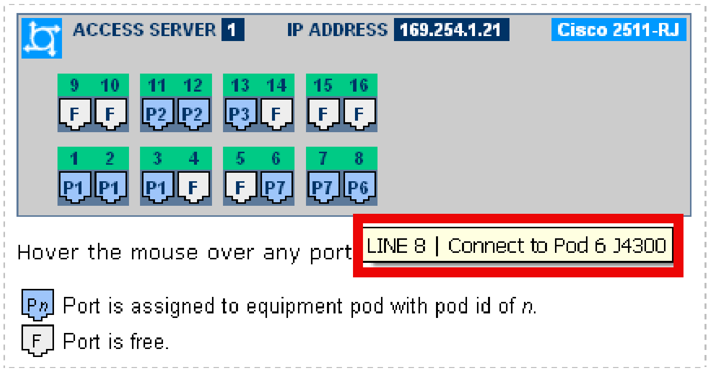
ACCESS SERVER 2

IP ADDRESS 169.254.1.22

Cisco 2811 + NM-16A + 3 HWIC-16A (Lines 18-81)

LINE 68 | TTY 1/2 | Cable type: CAB-OCTAL-ASYNC | Octal cable label: 3

Another example of viewing line numbers by hovering the mouse over a port.



Hover the mouse over any port

Pn Port is assigned to equipment pod with pod id of *n*.

F Port is free.

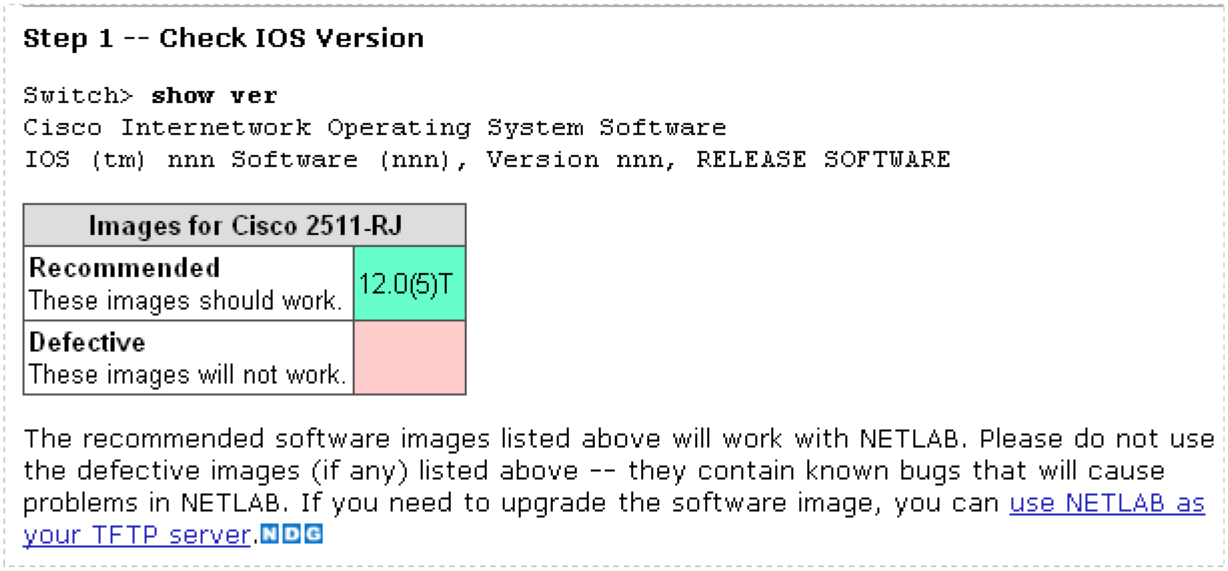
Several management options are accessed from this screen.

Configure You must configure the IOS software on the access server before it can be used by NETLAB+. To perform this task, it is assumed that:

- Your NETLAB+ server, access server, and control switches are turned on
- Everything is cabled correctly.
- All control switch ports in the path between the access server and the NETLAB+ server are up (green)
- You have connected a PC or terminal to the console port of the access server and you are at the Router> prompt

Carefully follow the steps listed on the configure access server screen:

The specific settings depicted may differ from the settings for your site.

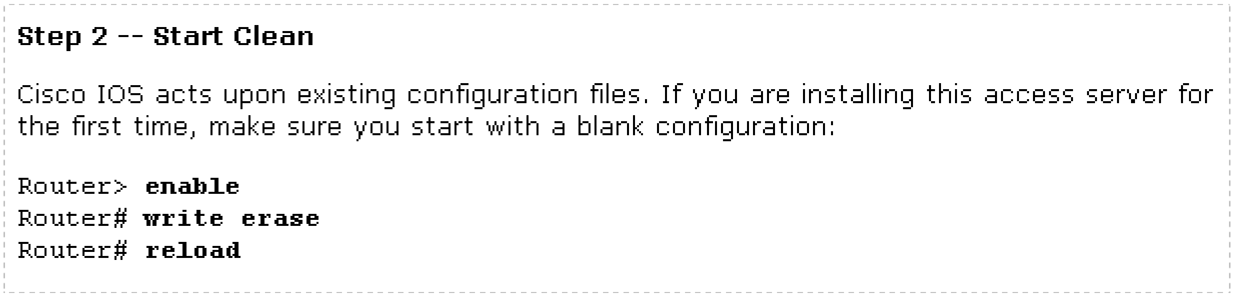


Step 1 -- Check IOS Version

```
Switch> show ver
Cisco Internetwork Operating System Software
IOS (tm) nnn Software (nnn), Version nnn, RELEASE SOFTWARE
```

Images for Cisco 2511-RJ	
Recommended These images should work.	12.0(5)T
Defective These images will not work.	

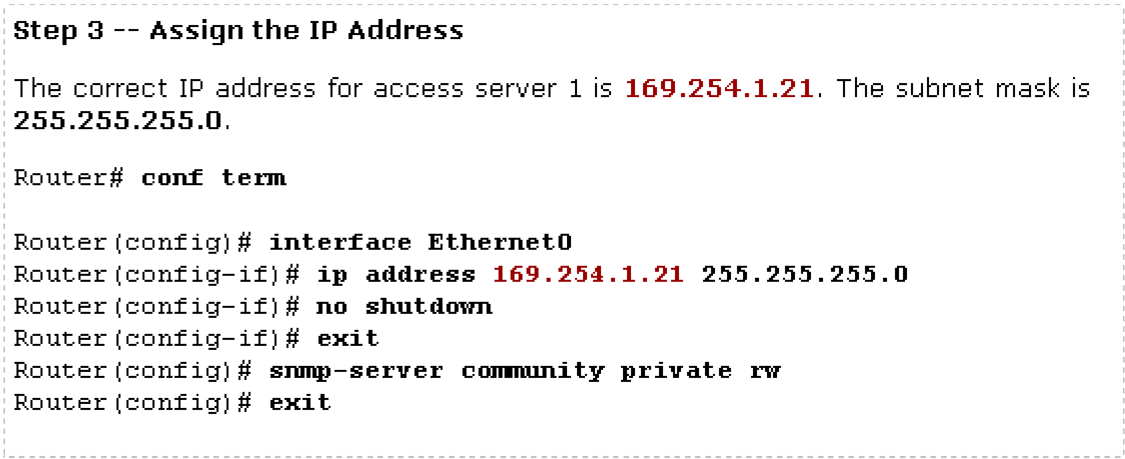
The recommended software images listed above will work with NETLAB. Please do not use the defective images (if any) listed above -- they contain known bugs that will cause problems in NETLAB. If you need to upgrade the software image, you can use NETLAB as your TFTP server.



Step 2 -- Start Clean

Cisco IOS acts upon existing configuration files. If you are installing this access server for the first time, make sure you start with a blank configuration:

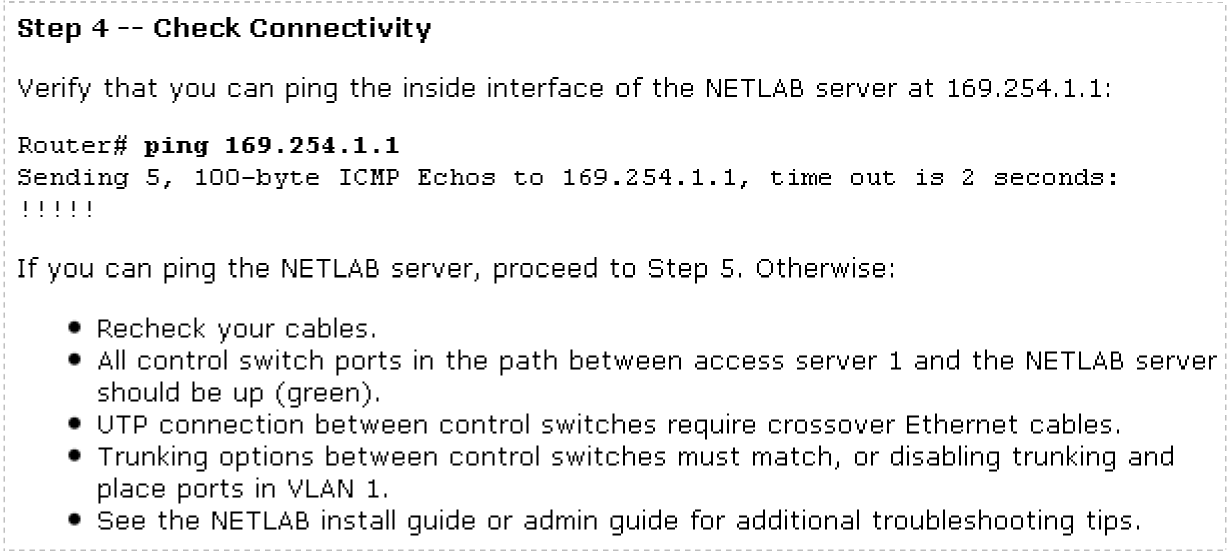
```
Router> enable
Router# write erase
Router# reload
```



Step 3 -- Assign the IP Address

The correct IP address for access server 1 is **169.254.1.21**. The subnet mask is **255.255.255.0**.

```
Router# conf term

Router(config)# interface Ethernet0
Router(config-if)# ip address 169.254.1.21 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# snmp-server community private rw
Router(config)# exit
```



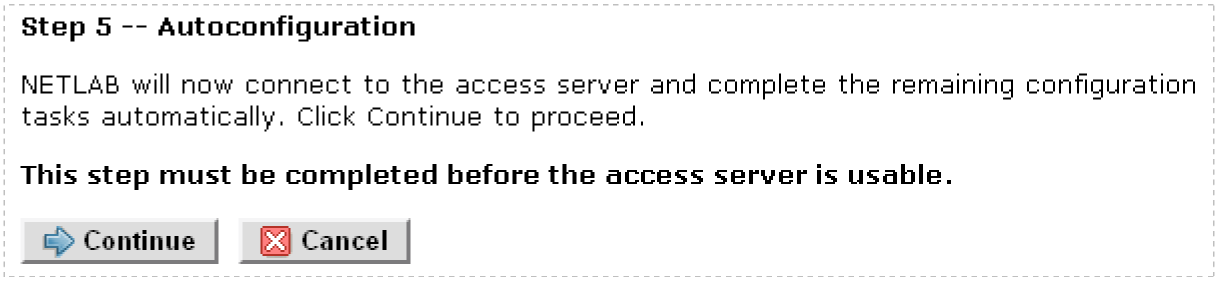
Step 4 -- Check Connectivity

Verify that you can ping the inside interface of the NETLAB server at 169.254.1.1:

```
Router# ping 169.254.1.1
Sending 5, 100-byte ICMP Echos to 169.254.1.1, time out is 2 seconds:
!!!!!
```

If you can ping the NETLAB server, proceed to Step 5. Otherwise:

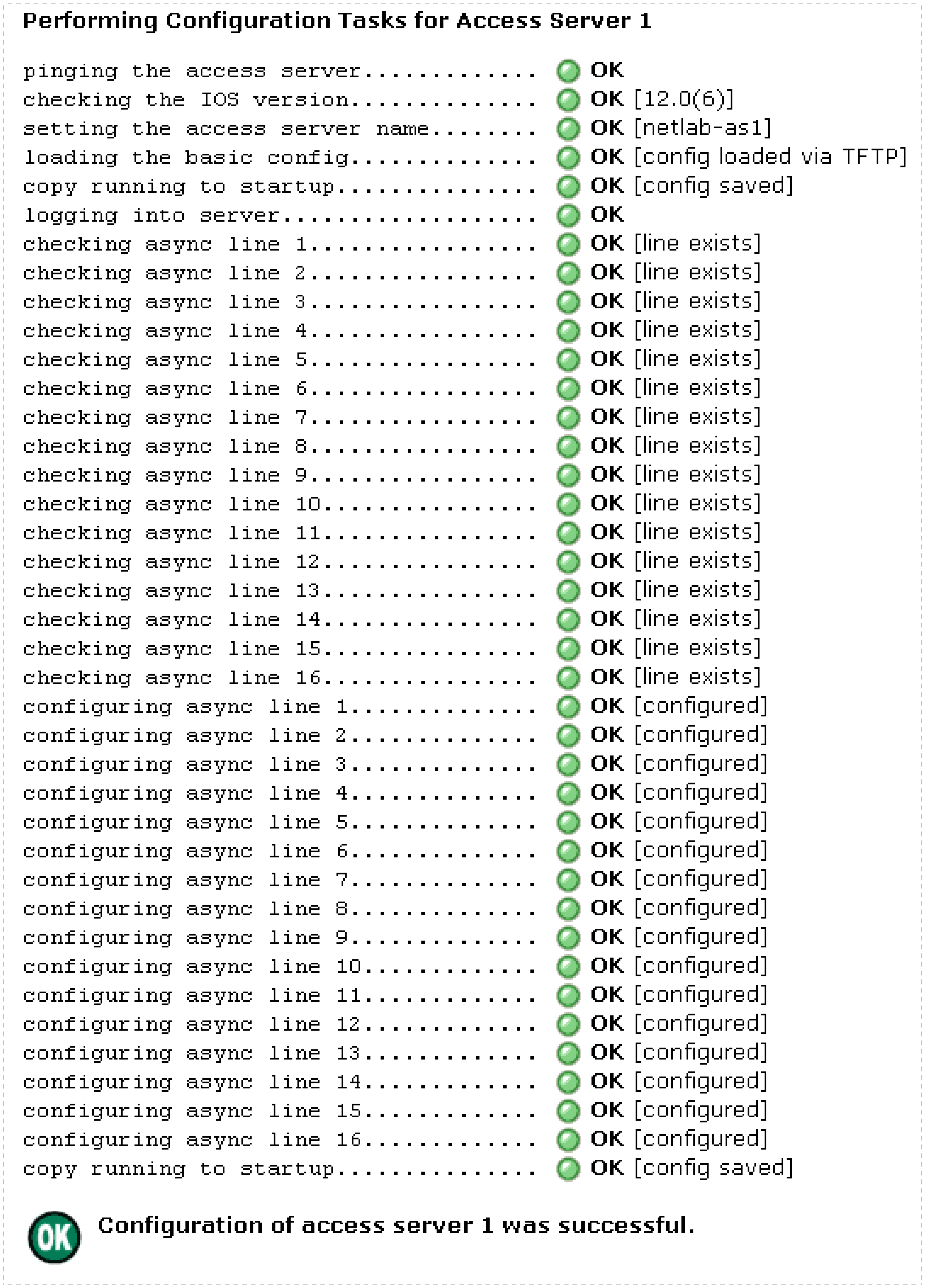
- Recheck your cables.
- All control switch ports in the path between access server 1 and the NETLAB server should be up (green).
- UTP connection between control switches require crossover Ethernet cables.
- Trunking options between control switches must match, or disabling trunking and place ports in VLAN 1.
- See the NETLAB install guide or admin guide for additional troubleshooting tips.



Step 5 -- Autoconfiguration

NETLAB will now connect to the access server and complete the remaining configuration tasks automatically. Click Continue to proceed.

This step must be completed before the access server is usable.

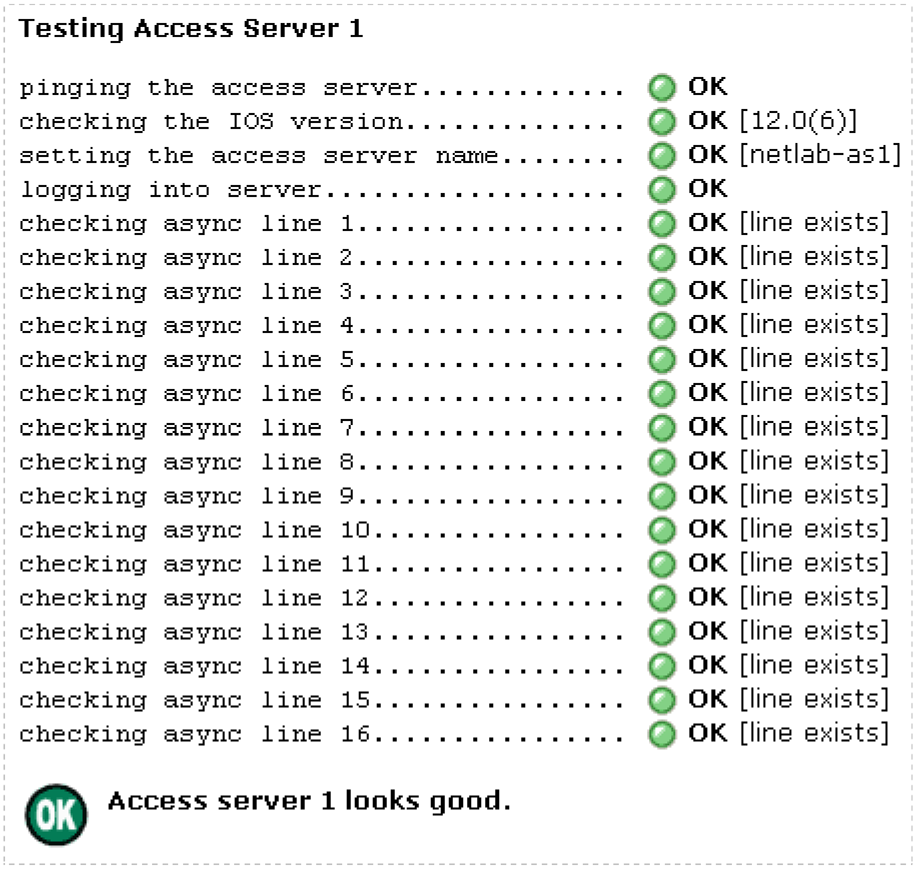


Performing Configuration Tasks for Access Server 1

```
pinging the access server............. ● OK
checking the IOS version.............. ● OK [12.0(6)]
setting the access server name........ ● OK [netlab-as1]
loading the basic config.............. ● OK [config loaded via TFTP]
copy running to startup............... ● OK [config saved]
logging into server................... ● OK
checking async line 1................. ● OK [line exists]
checking async line 2................. ● OK [line exists]
checking async line 3................. ● OK [line exists]
checking async line 4................. ● OK [line exists]
checking async line 5................. ● OK [line exists]
checking async line 6................. ● OK [line exists]
checking async line 7................. ● OK [line exists]
checking async line 8................. ● OK [line exists]
checking async line 9................. ● OK [line exists]
checking async line 10................ ● OK [line exists]
checking async line 11................ ● OK [line exists]
checking async line 12................ ● OK [line exists]
checking async line 13................ ● OK [line exists]
checking async line 14................ ● OK [line exists]
checking async line 15................ ● OK [line exists]
checking async line 16................ ● OK [line exists]
configuring async line 1.............. ● OK [configured]
configuring async line 2.............. ● OK [configured]
configuring async line 3.............. ● OK [configured]
configuring async line 4.............. ● OK [configured]
configuring async line 5.............. ● OK [configured]
configuring async line 6.............. ● OK [configured]
configuring async line 7.............. ● OK [configured]
configuring async line 8.............. ● OK [configured]
configuring async line 9.............. ● OK [configured]
configuring async line 10............. ● OK [configured]
configuring async line 11............. ● OK [configured]
configuring async line 12............. ● OK [configured]
configuring async line 13............. ● OK [configured]
configuring async line 14............. ● OK [configured]
configuring async line 15............. ● OK [configured]
configuring async line 16............. ● OK [configured]
copy running to startup............... ● OK [config saved]
```

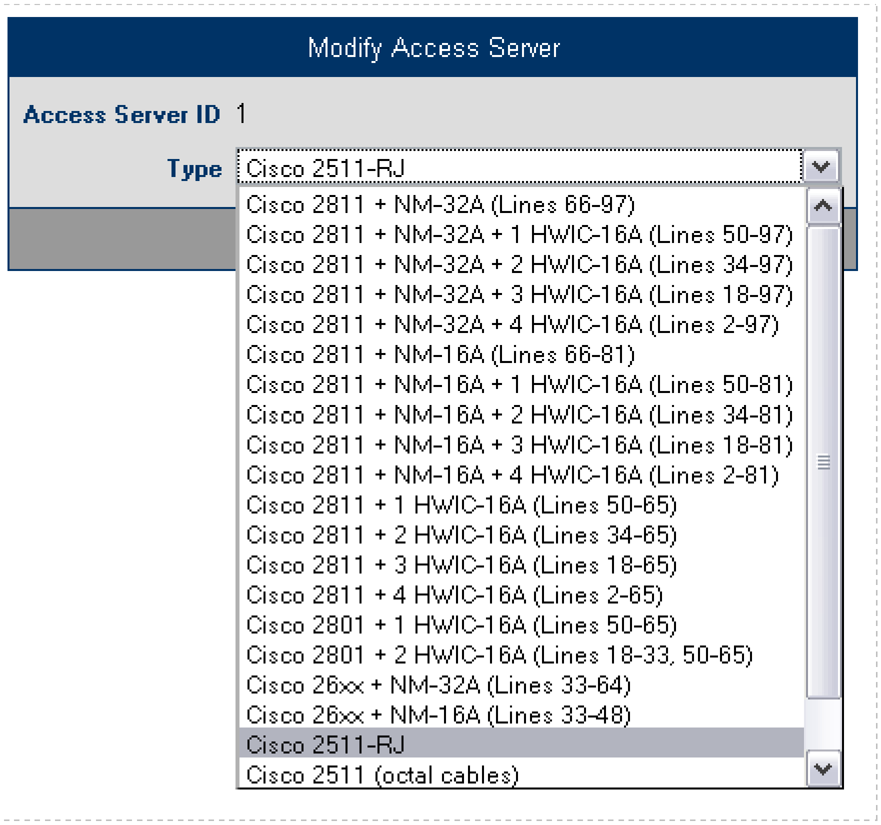
OK **Configuration of access server 1 was successful.**

Test Tell me if this access server is configured and working properly.



```
Testing Access Server 1

pinging the access server............. ● OK
checking the IOS version.............. ● OK [12.0(6)]
setting the access server name........ ● OK [netlab-as1]
logging into server................... ● OK
checking async line 1................. ● OK [line exists]
checking async line 2................. ● OK [line exists]
checking async line 3................. ● OK [line exists]
checking async line 4................. ● OK [line exists]
checking async line 5................. ● OK [line exists]
checking async line 6................. ● OK [line exists]
checking async line 7................. ● OK [line exists]
checking async line 8................. ● OK [line exists]
checking async line 9................. ● OK [line exists]
checking async line 10................ ● OK [line exists]
checking async line 11................ ● OK [line exists]
checking async line 12................ ● OK [line exists]
checking async line 13................ ● OK [line exists]
checking async line 14................ ● OK [line exists]
checking async line 15................ ● OK [line exists]
checking async line 16................ ● OK [line exists]

OK  Access server 1 looks good.
```

Modify Change the access server type. You may change the access server's type only if the same line numbers in use exist on the new access server.



Modify Access Server

Access Server ID 1

Type Cisco 2511-RJ

Cisco 2811 + NM-32A (Lines 66-97)
Cisco 2811 + NM-32A + 1 HWIC-16A (Lines 50-97)
Cisco 2811 + NM-32A + 2 HWIC-16A (Lines 34-97)
Cisco 2811 + NM-32A + 3 HWIC-16A (Lines 18-97)
Cisco 2811 + NM-32A + 4 HWIC-16A (Lines 2-97)
Cisco 2811 + NM-16A (Lines 66-81)
Cisco 2811 + NM-16A + 1 HWIC-16A (Lines 50-81)
Cisco 2811 + NM-16A + 2 HWIC-16A (Lines 34-81)
Cisco 2811 + NM-16A + 3 HWIC-16A (Lines 18-81)
Cisco 2811 + NM-16A + 4 HWIC-16A (Lines 2-81)
Cisco 2811 + 1 HWIC-16A (Lines 50-65)
Cisco 2811 + 2 HWIC-16A (Lines 34-65)
Cisco 2811 + 3 HWIC-16A (Lines 18-65)
Cisco 2811 + 4 HWIC-16A (Lines 2-65)
Cisco 2801 + 1 HWIC-16A (Lines 50-65)
Cisco 2801 + 2 HWIC-16A (Lines 18-33, 50-65)
Cisco 26xx + NM-32A (Lines 33-64)
Cisco 26xx + NM-16A (Lines 33-48)
Cisco 2511-RJ
Cisco 2511 (octal cables)

Delete Remove the access server from NETLAB+.

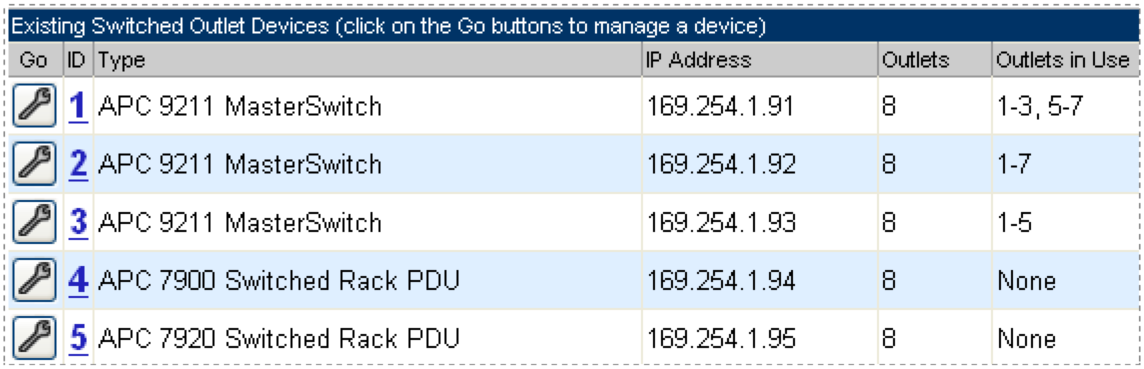
See the Access Servers section of the *NETLAB+ Administrator Guide*, for more information on access servers.

3.3 Install Switched Outlet Device

Select **Switched Outlets** from the Manage Control Devices page.

If this is not the first switched outlet device to be installed on the system, the existing switched outlet devices will be displayed.

The specific settings depicted may differ from the settings for your site.

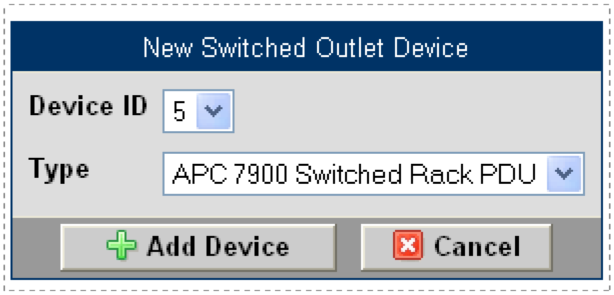


Existing Switched Outlet Devices (click on the Go buttons to manage a device)

Go	ID	Type	IP Address	Outlets	Outlets in Use
	1	APC 9211 MasterSwitch	169.254.1.91	8	1-3, 5-7
	2	APC 9211 MasterSwitch	169.254.1.92	8	1-7
	3	APC 9211 MasterSwitch	169.254.1.93	8	1-5
	4	APC 7900 Switched Rack PDU	169.254.1.94	8	None
	5	APC 7920 Switched Rack PDU	169.254.1.95	8	None

Select **Add Switched Outlet Device**, the New Switched Outlet Device page will be displayed.

Select an ID and Type, and then click **Add Device**.

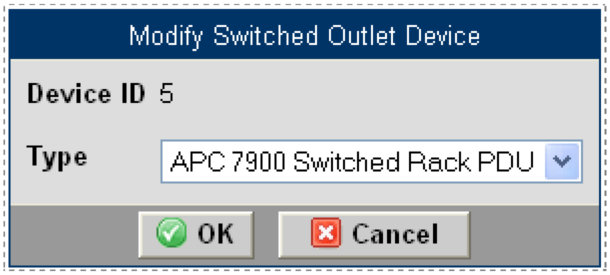


New Switched Outlet Device

Device ID: 5

Type: APC 7900 Switched Rack PDU

You may change the switched outlet device's type.



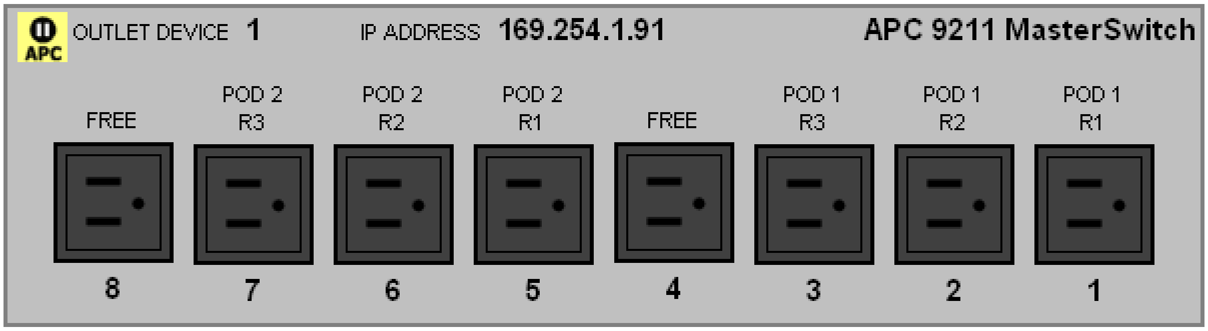
Modify Switched Outlet Device

Device ID 5

Type APC 7900 Switched Rack PDU

The Switched Outlet Device Management screen displays a diagram showing the assignments to each outlet.

Please Note: The specific settings depicted here may differ from the settings at your site.



OUTLET DEVICE 1 IP ADDRESS 169.254.1.91 APC 9211 MasterSwitch

8	7	6	5	4	3	2	1
FREE	POD 2 R3	POD 2 R2	POD 2 R1	FREE	POD 1 R3	POD 1 R2	POD 1 R1

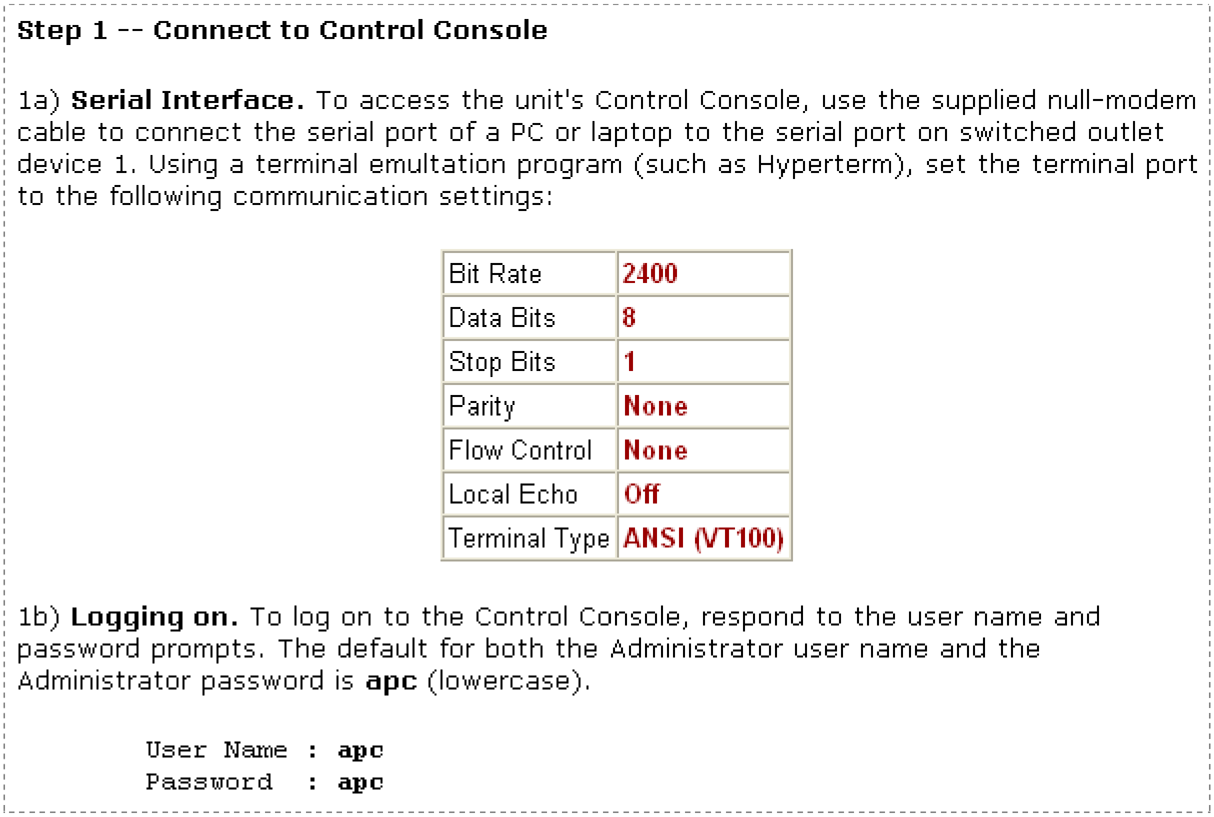
Several management options are accessed from this screen.

You must configure the TCP/IP settings on a switched outlet device before it can be used by NETLAB+. To perform this task, we assume that:

- Your NETLAB+ server, switched outlet device, and control switches are turned on
- Everything is cabled correctly, see section 4.12
- All control switch ports in the path between the switched outlet device and the NETLAB+ server are up (green)

Carefully follow the steps listed on the Configure Switched Outlet Device screen.

The specific settings depicted may differ from the settings for your site.



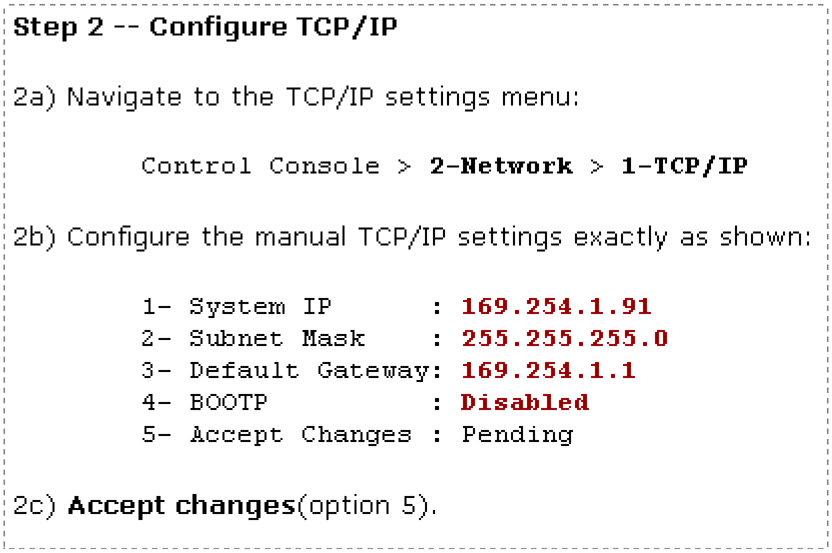
Step 1 -- Connect to Control Console

1a) **Serial Interface.** To access the unit's Control Console, use the supplied null-modem cable to connect the serial port of a PC or laptop to the serial port on switched outlet device 1. Using a terminal emultation program (such as Hyperterm), set the terminal port to the following communication settings:

Bit Rate	**2400**
Data Bits	**8**
Stop Bits	**1**
Parity	**None**
Flow Control	**None**
Local Echo	**Off**
Terminal Type	**ANSI (VT100)**

1b) **Logging on.** To log on to the Control Console, respond to the user name and password prompts. The default for both the Administrator user name and the Administrator password is **apc** (lowercase).

```
User Name  : apc
Password   : apc
```



Step 2 -- Configure TCP/IP

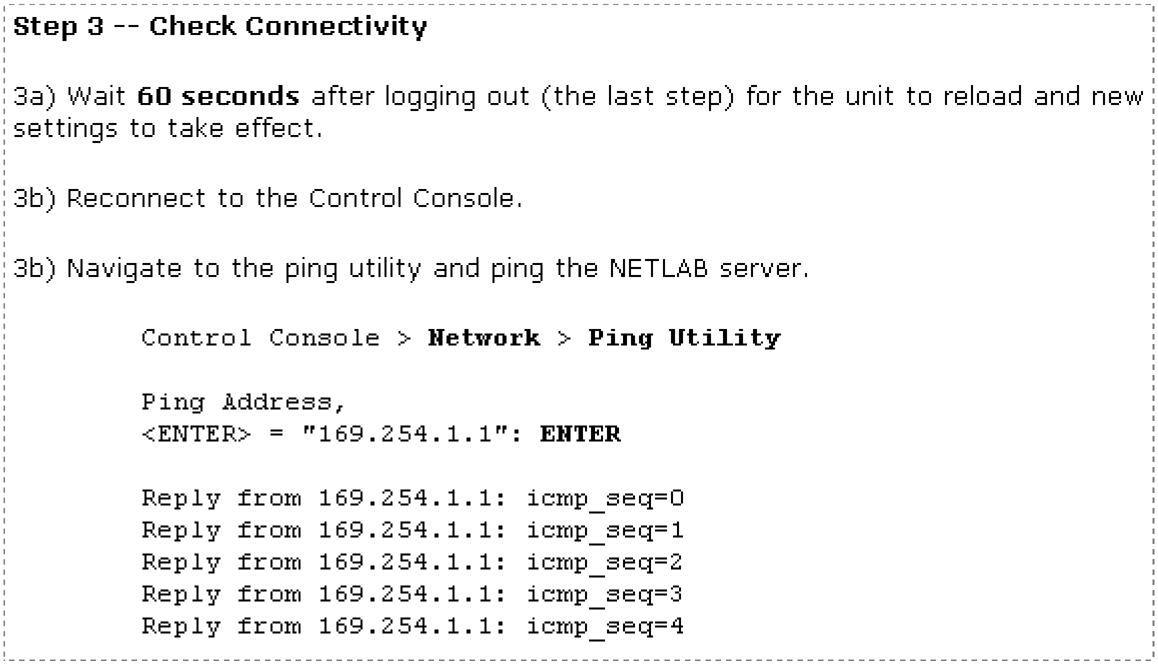
2a) Navigate to the TCP/IP settings menu:

```
Control Console > 2-Network > 1-TCP/IP
```

2b) Configure the manual TCP/IP settings exactly as shown:

```
1- System IP       : 169.254.1.91
2- Subnet Mask     : 255.255.255.0
3- Default Gateway: 169.254.1.1
4- BOOTP           : Disabled
5- Accept Changes  : Pending
```

2c) **Accept changes**(option 5).



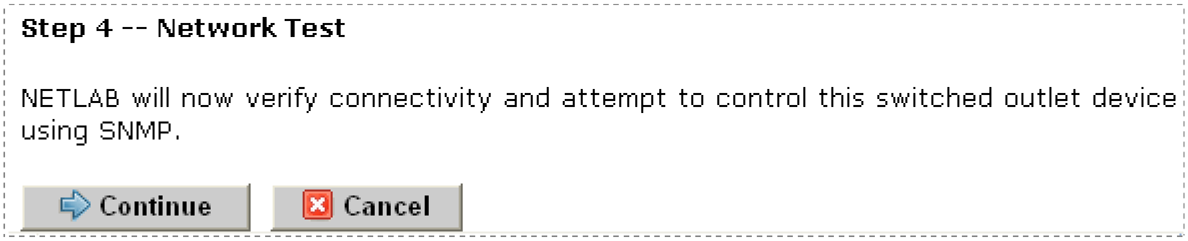
Step 3 -- Check Connectivity

3a) Wait **60 seconds** after logging out (the last step) for the unit to reload and new settings to take effect.

3b) Reconnect to the Control Console.

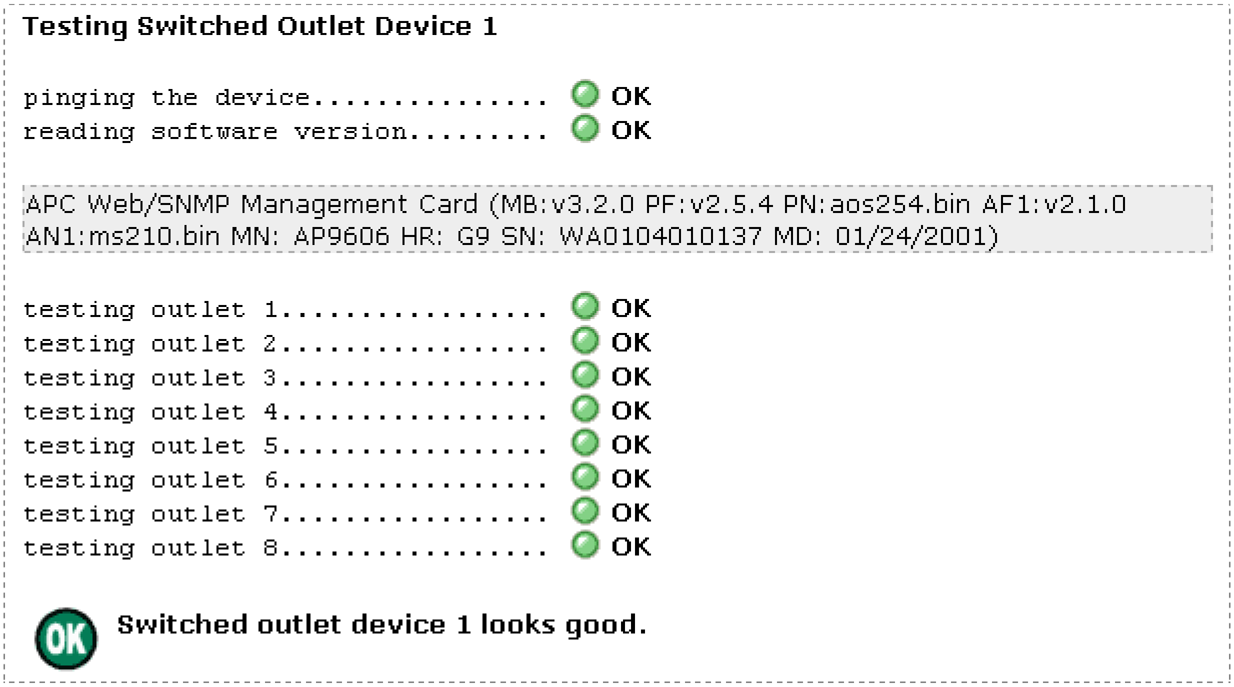
3b) Navigate to the ping utility and ping the NETLAB server.

```
        Control Console > Network > Ping Utility

        Ping Address,
        <ENTER> = "169.254.1.1": ENTER

        Reply from 169.254.1.1: icmp_seq=0
        Reply from 169.254.1.1: icmp_seq=1
        Reply from 169.254.1.1: icmp_seq=2
        Reply from 169.254.1.1: icmp_seq=3
        Reply from 169.254.1.1: icmp_seq=4
```



Step 4 -- Network Test

NETLAB will now verify connectivity and attempt to control this switched outlet device using SNMP.



```
Testing Switched Outlet Device 1

pinging the device...............  ● OK
reading software version.........  ● OK

APC Web/SNMP Management Card (MB:v3.2.0 PF:v2.5.4 PN:aos254.bin AF1:v2.1.0
AN1:ms210.bin MN: AP9606 HR: G9 SN: WA0104010137 MD: 01/24/2001)

testing outlet 1.................  ● OK
testing outlet 2.................  ● OK
testing outlet 3.................  ● OK
testing outlet 4.................  ● OK
testing outlet 5.................  ● OK
testing outlet 6.................  ● OK
testing outlet 7.................  ● OK
testing outlet 8.................  ● OK

OK  Switched outlet device 1 looks good.
```

See the Switched Outlets section of the , *NETLAB+ Administrator Guide* for more information on switched outlets.

3.4 Download System Images

The NETLAB+ TFTP server must contain IOS images compatible with your equipment in order to perform the automated procedures essential to the proper operation of the NETLAB+ system. These image files will be used by NETLAB+ to perform automated recovery when flash has been erased or the image has been corrupted.

Even if your routers are currently running the appropriate IOS image, you must download image files for each router type to the PC that you will be using to set up the NETLAB+ system. The files must have a .bin extension in order to be updated to the TFTP server. You will need to download an image for each type of router hardware in your lab pods.
If you do not have the necessary image files, they may be obtained from the appropriate source
(i.e. log into Cisco CCO and go to the Software Center)

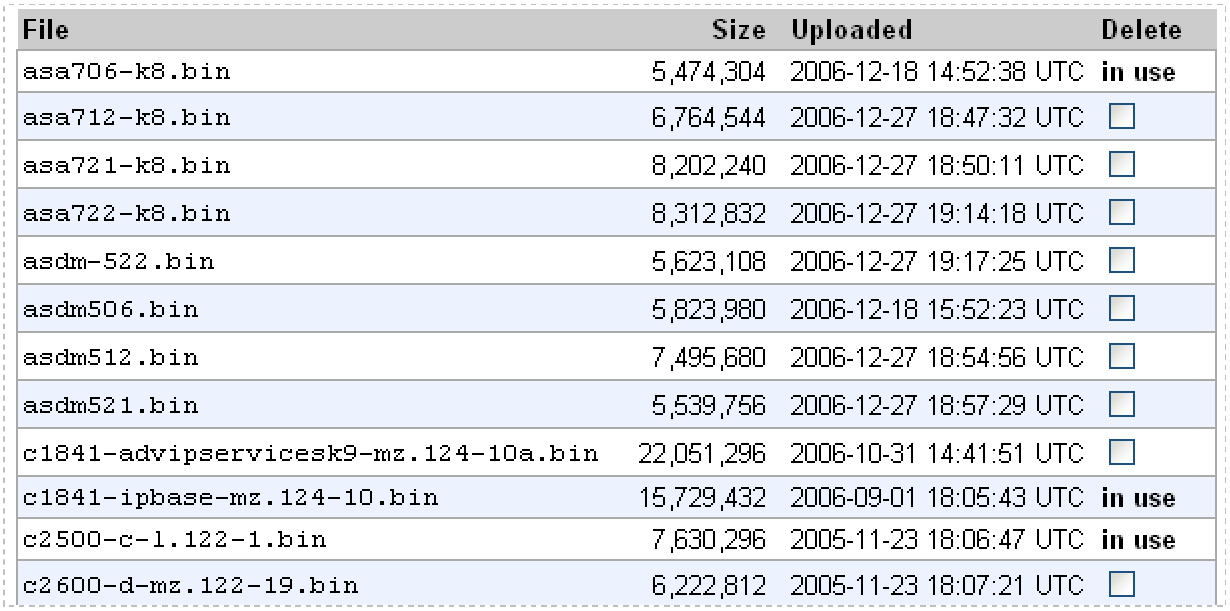
Once these files have been downloaded to the PC, the files may then be uploaded to the TFTP server. Proceed to the next section.

3.5 Upload System Images to TFTP Directory

With the necessary system images downloaded to your PC, (see previous section) you may proceed to upload system images to the TFTP directory.

During the process of adding a pod, you will specify an image file to be used with each router in your lab pods. If you have not uploaded these images to the NETLAB+ TFTP directory, you will be unable to choose a compatible image. Therefore, it is critical that you download a compatible image for each router type in your lab pods.

Select the IOS & PIX Images administrator function. The top of the page displays the list of files currently in the directory.



File	Size	Uploaded	Delete
asa706-k8.bin	5,474,304	2006-12-18 14:52:38 UTC	in use
asa712-k8.bin	6,764,544	2006-12-27 18:47:32 UTC	☐
asa721-k8.bin	8,202,240	2006-12-27 18:50:11 UTC	☐
asa722-k8.bin	8,312,832	2006-12-27 19:14:18 UTC	☐
asdm-522.bin	5,623,108	2006-12-27 19:17:25 UTC	☐
asdm506.bin	5,823,980	2006-12-18 15:52:23 UTC	☐
asdm512.bin	7,495,680	2006-12-27 18:54:56 UTC	☐
asdm521.bin	5,539,756	2006-12-27 18:57:29 UTC	☐
c1841-advipservicesk9-mz.124-10a.bin	22,051,296	2006-10-31 14:41:51 UTC	☐
c1841-ipbase-mz.124-10.bin	15,729,432	2006-09-01 18:05:43 UTC	in use
c2500-c-l.122-1.bin	7,630,296	2005-11-23 18:06:47 UTC	in use
c2600-d-mz.122-19.bin	6,222,812	2005-11-23 18:07:21 UTC	☐

Follow the instructions at the bottom of the System Images page to upload any image files needed that are not already present in the TFTP directory.

You can upload system images with a .bin extension from your local machine to NETLAB+'s TFTP Directory.

In order to upload a system image to NETLAB+, the image must exist on your local PC. If the image is not on your PC, you will need to obtain it from the appropriate source (i.e. log into Cisco CCO and go to the Software Center)

Do not rename Cisco software images. NETLAB+ examines the file name to determine compatibility during pod configuration.

Specify the file name on your PC machine (example: C:\My Documents\c2500-d-l.120-5.T.bin) or click the Browse button to bring up a file dialog box.

Upload File Select after you have specified a file name. Repeat as needed.

Refresh List Refresh the list after adding image files and verify that you have every file needed loaded into the TFTP directory.

See the IOS & PIX Images section of the *NETLAB+ Administrator Guide* for more information.

4 Add a Pod

After successful installation of the NETLAB+ control plane, the next step is to install equipment pods.

A pod (or lab topology) is a single instance of a set of lab gear that students and instructors interact with during their training via the NETLAB+ system. It is a logical group of equipment that is physically interconnected and can be reserved as a single resource from the scheduler. In addition, a pod is isolated from other pods during normal operation.

This pod installation process must be repeated for each pod that is installed on the NETLAB+ system.

Please complete the tasks in the sub-sections below in order. Do not physically connect your pod to a control switch until the pod has been added to your NETLAB+ system by following the instructions below. This is necessary in order for the control switch to be programmed with the proper VLANs.

NETLAB$_{AE}$ users may refer to the guide written specifically for the pod-type they plan to install. Pod-specific guides include:

- NETLAB$_{AE}$ Multi-Purpose Academy Pod (MAP)
- NETLAB$_{AE}$ Network Fundamentals Pod (NFP)
- NETLAB$_{AE}$ Basic Router Pod Version 2 (BRPv2)
- NETLAB$_{AE}$ Basic Router Pod Version 1 (BRPv1)
- NETLAB$_{AE}$ Cuatro Router Pod (CRP)
- NETLAB$_{AE}$ Cuatro Switch Pod (CSP)
- NETLAB$_{AE}$ LAN Switching Pod (LSP)
- NETLAB$_{AE}$ Network Security Pod (NSP)
- NETLAB$_{AE}$ Basic Switch Pod Version 2 (BSPv2)
- NETLAB$_{AE}$ Basic Switch Pod Version 1 (BSPv1)
- NETLAB$_{AE}$ Advanced Router Pod (ARP)
- NETLAB$_{AE}$ Advanced Switch Pod (ASP)
- NETLAB$_{AE}$ Security Router Pod (SRP)
- NETLAB$_{AE}$ Security PIX Pod (SPP

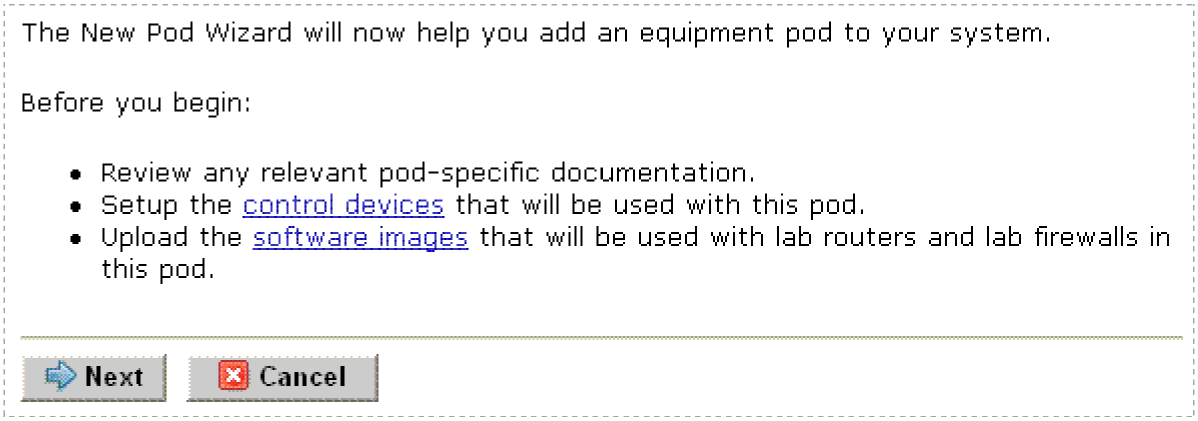
Select the Equipment Pods administrator function.

The instructions for this section should be followed for each pod you wish to add to the NETLAB+ system.

Select Take All OFFLINE if any of the pods are online.

Select ✚ Add a Pod.

The network and hardware settings depicted here are intended to provide an example only. Your system requirements may differ according to your specific hardware selections.

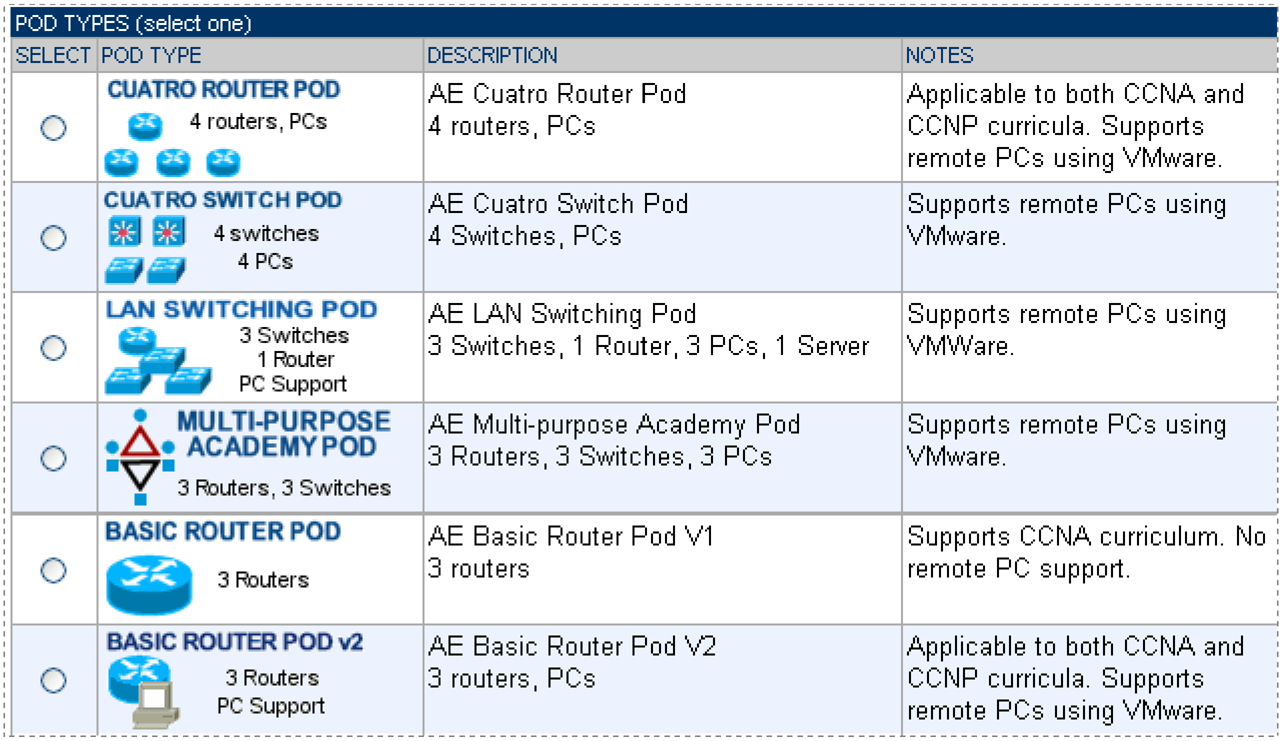


The New Pod Wizard will now help you add an equipment pod to your system.

Before you begin:

- Review any relevant pod-specific documentation.
- Setup the control devices that will be used with this pod.
- Upload the software images that will be used with lab routers and lab firewalls in this pod.

NETLAB$_{AE}$ users may select the pod type they wish to add to their NETLAB+ system from the list of pod types provided.

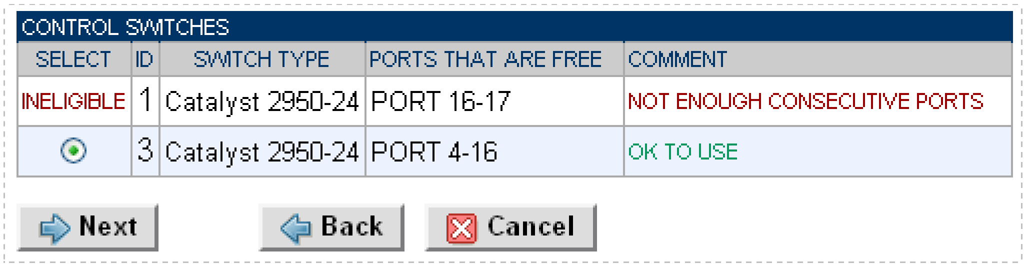


POD TYPES (select one)

SELECT	POD TYPE	DESCRIPTION	NOTES
○	CUATRO ROUTER POD 4 routers, PCs	AE Cuatro Router Pod 4 routers, PCs	Applicable to both CCNA and CCNP curricula. Supports remote PCs using VMware.
○	CUATRO SWITCH POD 4 switches 4 PCs	AE Cuatro Switch Pod 4 Switches, PCs	Supports remote PCs using VMware.
○	LAN SWITCHING POD 3 Switches 1 Router PC Support	AE LAN Switching Pod 3 Switches, 1 Router, 3 PCs, 1 Server	Supports remote PCs using VMWare.
○	MULTI-PURPOSE ACADEMY POD 3 Routers, 3 Switches	AE Multi-purpose Academy Pod 3 Routers, 3 Switches, 3 PCs	Supports remote PCs using VMware.
○	BASIC ROUTER POD 3 Routers	AE Basic Router Pod V1 3 routers	Supports CCNA curriculum. No remote PC support.
○	BASIC ROUTER POD v2 3 Routers PC Support	AE Basic Router Pod V2 3 routers, PCs	Applicable to both CCNA and CCNP curricula. Supports remote PCs using VMware.

4.1 Select Control Switch

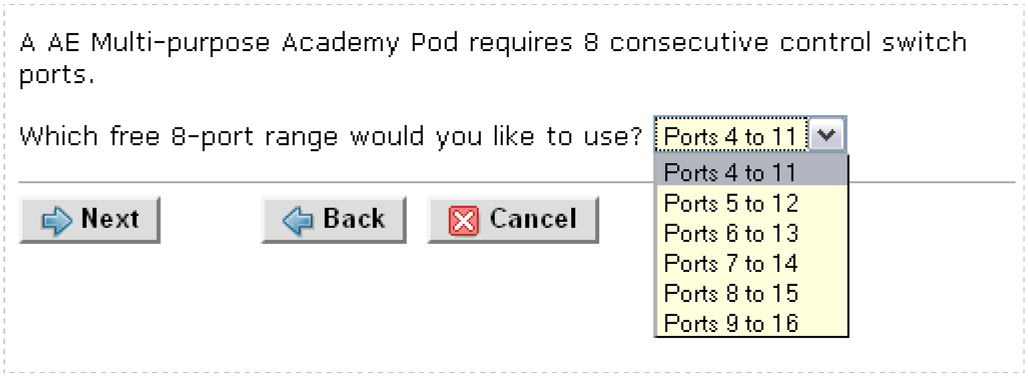
Next, NETLAB+ will present a list of the control switches on your system. Only selections that meet your port requirements can be made.



CONTROL SWITCHES

SELECT	ID	SWITCH TYPE	PORTS THAT ARE FREE	COMMENT
INELIGIBLE	1	Catalyst 2950-24	PORT 16-17	NOT ENOUGH CONSECUTIVE PORTS
●	3	Catalyst 2950-24	PORT 4-16	OK TO USE

Next, select the ports you want to use.



A AE Multi-purpose Academy Pod requires 8 consecutive control switch ports.

Which free 8-port range would you like to use? Ports 4 to 11

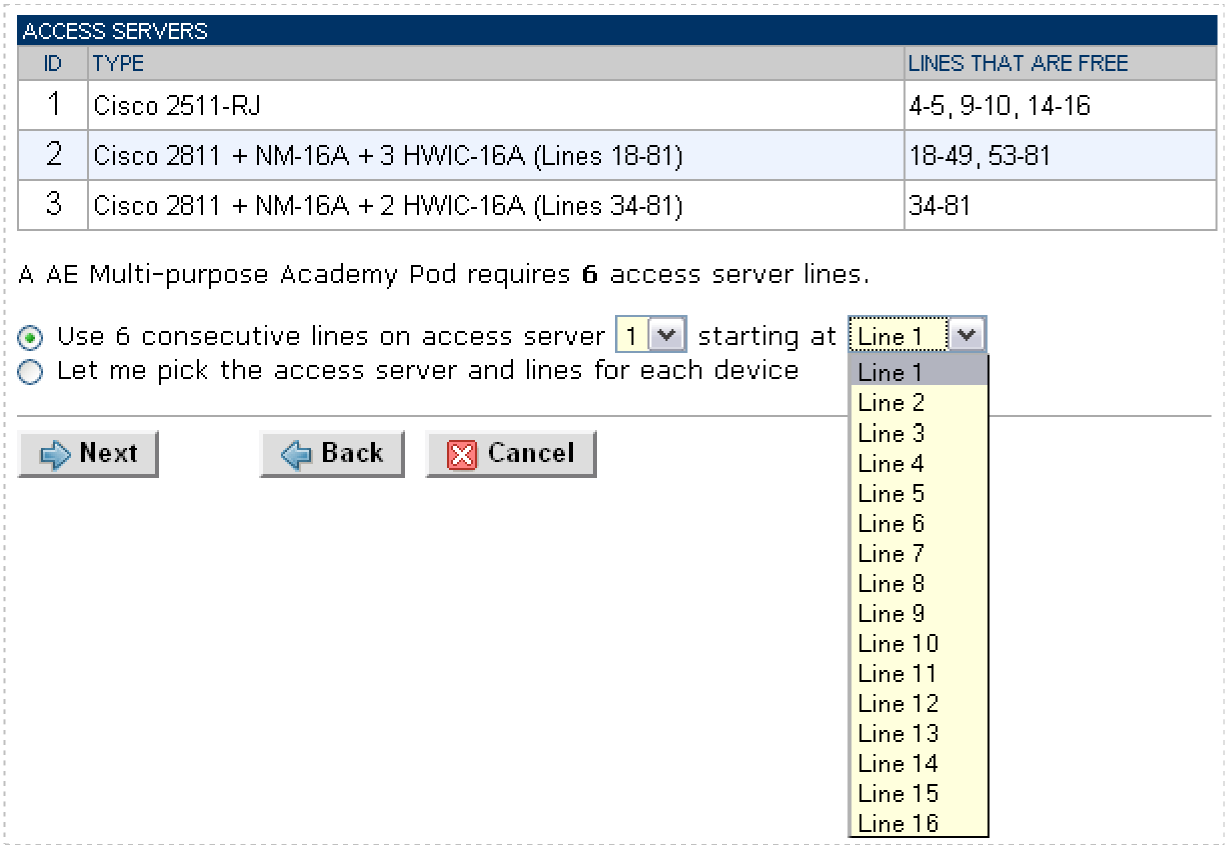
4.2 Select Access Server(s) and Lines

This section is only applicable if there are lab devices in your topology that require asynchronous console access. Such connections are provided by access servers.

Line Number is now used as a unique identifier for access server ports.
Beginning with NETLAB+ version 2010.R3, NETLAB+ supports an expanded selection of access servers. Since several models include multiple modules, port number is no longer a unique identifier.

It is a good idea to use consecutive lines on one access server if possible. This practice will make it easier to cable and troubleshoot. If consecutive lines are not available, you can use non-consecutive lines, spanning multiple access servers if necessary.

NETLAB+ allows you to choose consecutive lines on one access server, or you can choose "Let me pick" to select an access server and line for each router.



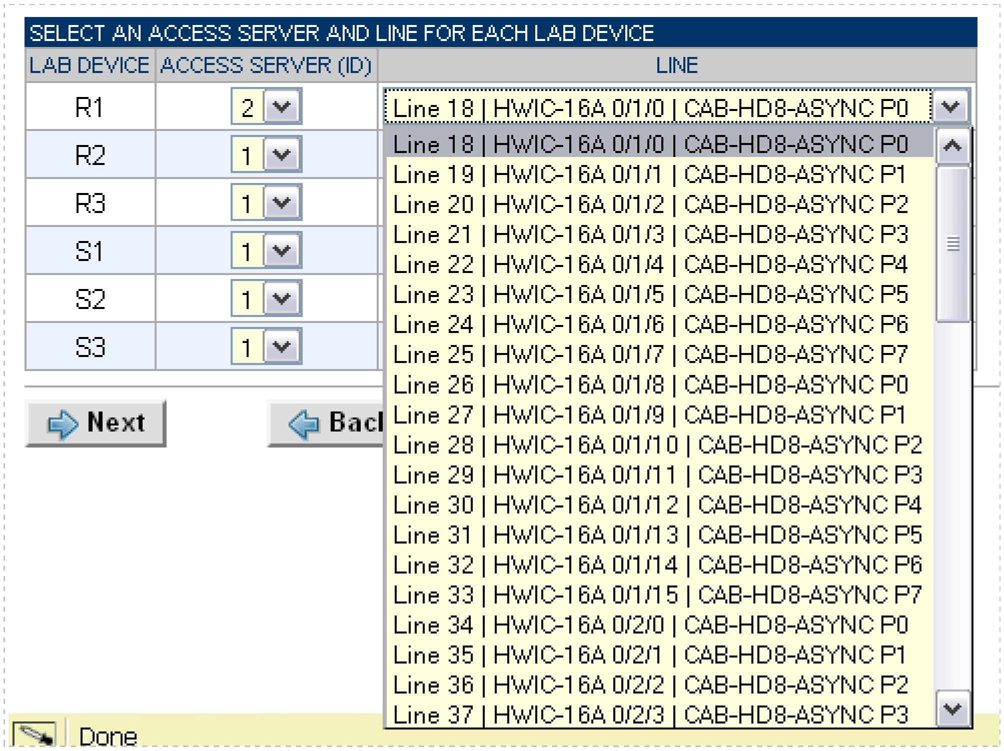
ACCESS SERVERS

ID	TYPE	LINES THAT ARE FREE
1	Cisco 2511-RJ	4-5, 9-10, 14-16
2	Cisco 2811 + NM-16A + 3 HWIC-16A (Lines 18-81)	18-49, 53-81
3	Cisco 2811 + NM-16A + 2 HWIC-16A (Lines 34-81)	34-81

A AE Multi-purpose Academy Pod requires **6** access server lines.

● Use 6 consecutive lines on access server 1 starting at Line 1
○ Let me pick the access server and lines for each device

“Let me pick”, allows you to make granular selections. For access servers using octal cables, both the line number and the cable label are displayed.

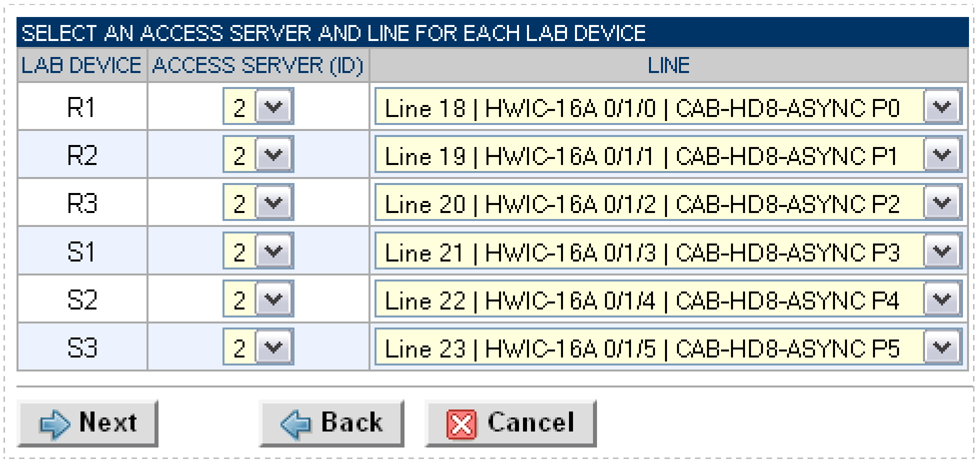


SELECT AN ACCESS SERVER AND LINE FOR EACH LAB DEVICE

LAB DEVICE	ACCESS SERVER (ID)	LINE
R1	2	Line 18 | HWIC-16A 0/1/0 | CAB-HD8-ASYNC P0
R2	1	
R3	1	
S1	1	
S2	1	
S3	1	

Line 18 | HWIC-16A 0/1/0 | CAB-HD8-ASYNC P0
Line 19 | HWIC-16A 0/1/1 | CAB-HD8-ASYNC P1
Line 20 | HWIC-16A 0/1/2 | CAB-HD8-ASYNC P2
Line 21 | HWIC-16A 0/1/3 | CAB-HD8-ASYNC P3
Line 22 | HWIC-16A 0/1/4 | CAB-HD8-ASYNC P4
Line 23 | HWIC-16A 0/1/5 | CAB-HD8-ASYNC P5
Line 24 | HWIC-16A 0/1/6 | CAB-HD8-ASYNC P6
Line 25 | HWIC-16A 0/1/7 | CAB-HD8-ASYNC P7
Line 26 | HWIC-16A 0/1/8 | CAB-HD8-ASYNC P0
Line 27 | HWIC-16A 0/1/9 | CAB-HD8-ASYNC P1
Line 28 | HWIC-16A 0/1/10 | CAB-HD8-ASYNC P2
Line 29 | HWIC-16A 0/1/11 | CAB-HD8-ASYNC P3
Line 30 | HWIC-16A 0/1/12 | CAB-HD8-ASYNC P4
Line 31 | HWIC-16A 0/1/13 | CAB-HD8-ASYNC P5
Line 32 | HWIC-16A 0/1/14 | CAB-HD8-ASYNC P6
Line 33 | HWIC-16A 0/1/15 | CAB-HD8-ASYNC P7
Line 34 | HWIC-16A 0/2/0 | CAB-HD8-ASYNC P0
Line 35 | HWIC-16A 0/2/1 | CAB-HD8-ASYNC P1
Line 36 | HWIC-16A 0/2/2 | CAB-HD8-ASYNC P2
Line 37 | HWIC-16A 0/2/3 | CAB-HD8-ASYNC P3

Select a line number for each device.



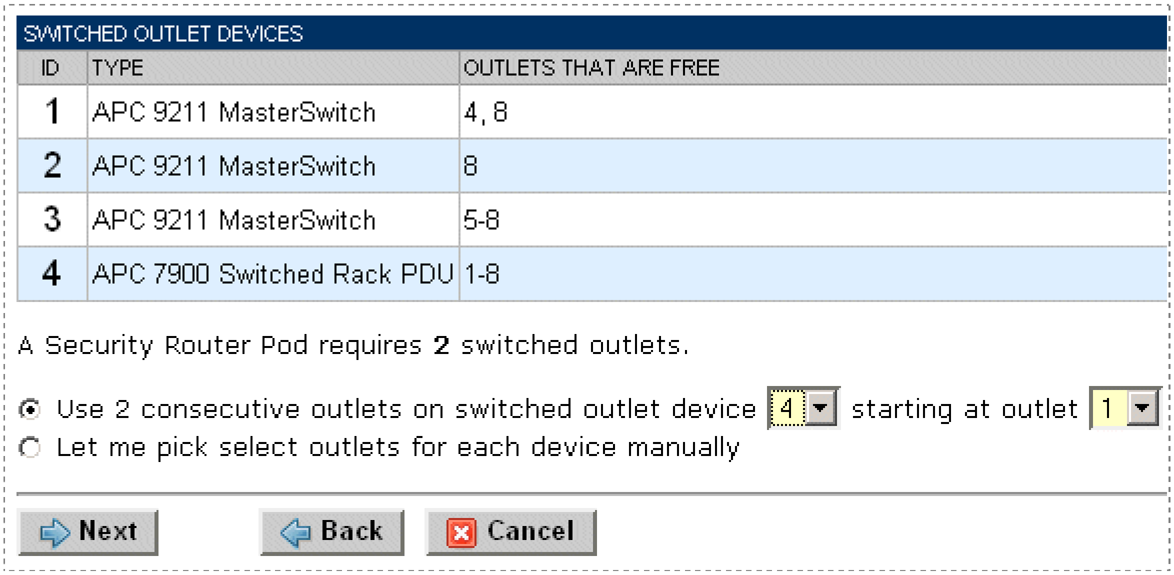
SELECT AN ACCESS SERVER AND LINE FOR EACH LAB DEVICE

LAB DEVICE	ACCESS SERVER (ID)	LINE
R1	2	Line 18 | HWIC-16A 0/1/0 | CAB-HD8-ASYNC P0
R2	2	Line 19 | HWIC-16A 0/1/1 | CAB-HD8-ASYNC P1
R3	2	Line 20 | HWIC-16A 0/1/2 | CAB-HD8-ASYNC P2
S1	2	Line 21 | HWIC-16A 0/1/3 | CAB-HD8-ASYNC P3
S2	2	Line 22 | HWIC-16A 0/1/4 | CAB-HD8-ASYNC P4
S3	2	Line 23 | HWIC-16A 0/1/5 | CAB-HD8-ASYNC P5

4.3 Select Switched Outlet Devices

This section is only applicable if there are lab devices in your topology that require managed electrical power. Such connections are provided by switched outlet devices.

It is a good idea to use consecutive outlets on one switched outlet device (SOD) if possible. This practice will make it easier to cable and troubleshoot. If consecutive outlets are not available, you may use non-consecutive outlets, spanning multiple Sods if necessary.



SWITCHED OUTLET DEVICES

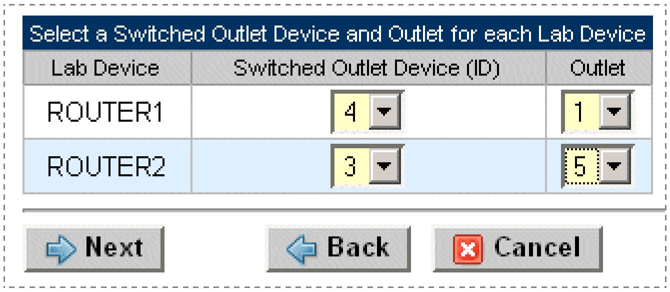
ID	TYPE	OUTLETS THAT ARE FREE
1	APC 9211 MasterSwitch	4, 8
2	APC 9211 MasterSwitch	8
3	APC 9211 MasterSwitch	5-8
4	APC 7900 Switched Rack PDU	1-8

A Security Router Pod requires **2** switched outlets.

● Use 2 consecutive outlets on switched outlet device 4 starting at outlet 1

○ Let me pick select outlets for each device manually

"Let me Pick", will allow you to make granular selections.



Select a Switched Outlet Device and Outlet for each Lab Device

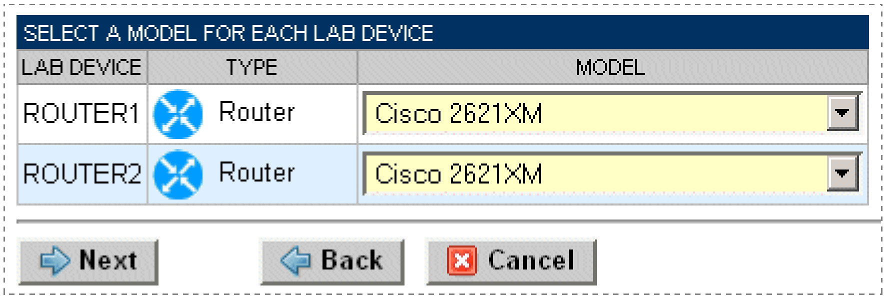
Lab Device	Switched Outlet Device (ID)	Outlet
ROUTER1	4	1
ROUTER2	3	5

4.4 Select Device Types

This section is only applicable if there are network devices in your lab topology. Please specify a device model for each device displayed. All statically configured routers may not appear in the router selection process.

- Your selections are used to assign the appropriate NETLAB+ device driver.
- Improper selections may cause errors.

NETLAB+ may offer selections that meet the port requirements, but do not support your curriculum. NETLAB$_{AE}$ administrators may refer to the pod specific guides for more information.



SELECT A MODEL FOR EACH LAB DEVICE

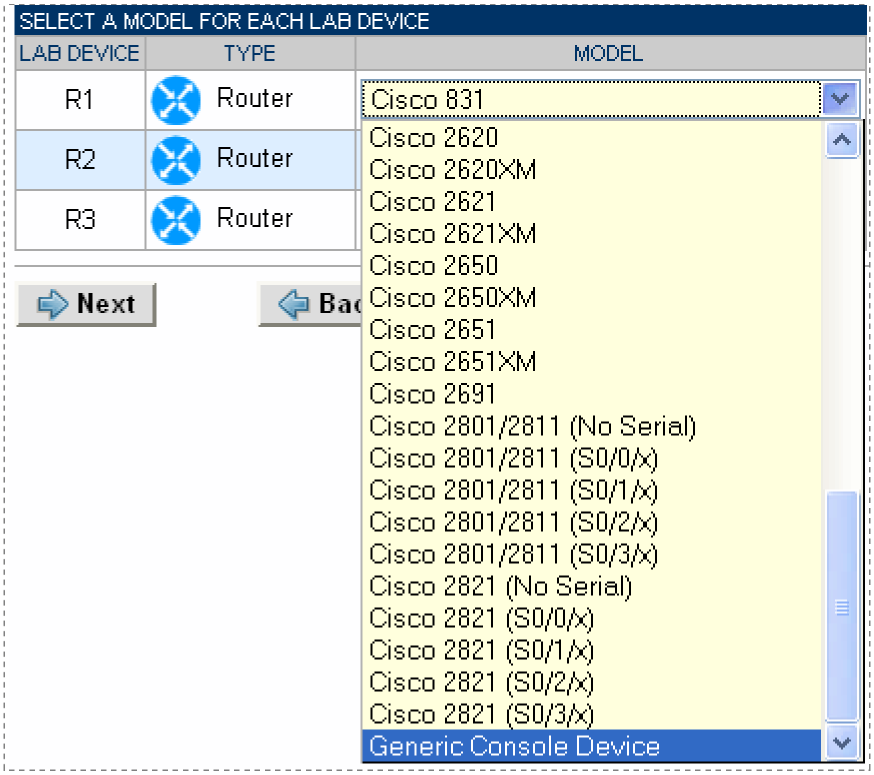
LAB DEVICE	TYPE	MODEL
ROUTER1	Router	Cisco 2621XM
ROUTER2	Router	Cisco 2621XM

If the device model you wish to install is not available for selection, proceed to the next section for guidance on installing generic console devices.

4.5 Generic Console Devices

This section is only applicable if there are network devices in your lab topology. NETLAB+ supports a wide range of devices. Selecting the appropriate device type is important to ensure that the full range of NETLAB+ features is available to users. Automation drivers have been created for all supported lab devices that enable the use of NETLAB+'s automation features.

If however, you wish to install a device in your pod that is not included among the supported devices (for example, an older model that has reached EOL and is no longer supported by the vendor) you may do so by selecting **Generic Console Device** as the device model.



SELECT A MODEL FOR EACH LAB DEVICE

LAB DEVICE	TYPE	MODEL
R1	Router	Cisco 831
R2	Router	
R3	Router	

Cisco 2620
Cisco 2620XM
Cisco 2621
Cisco 2621XM
Cisco 2650
Cisco 2650XM
Cisco 2651
Cisco 2651XM
Cisco 2691
Cisco 2801/2811 (No Serial)
Cisco 2801/2811 (S0/0/x)
Cisco 2801/2811 (S0/1/x)
Cisco 2801/2811 (S0/2/x)
Cisco 2801/2811 (S0/3/x)
Cisco 2821 (No Serial)
Cisco 2821 (S0/0/x)
Cisco 2821 (S0/1/x)
Cisco 2821 (S0/2/x)
Cisco 2821 (S0/3/x)
Generic Console Device

Generic Console Devices have the following limited capabilities:

- Console access
- Ability to share connections to CLI devices.
- Powered off at the end of a lab reservation (if connected to a switched outlet device).
- Powered on at the beginning of a lab reservation (if connected to a switched outlet device.).
- Automation options available for user selection during a lab reservation include power on, power off and power recycle (if connected to a switched outlet device).

There are several considerations to keep in mind when adding a generic console device to a pod:

- Automation features such as such as scrubbing the device and password recovery are not available for use on generic console devices.

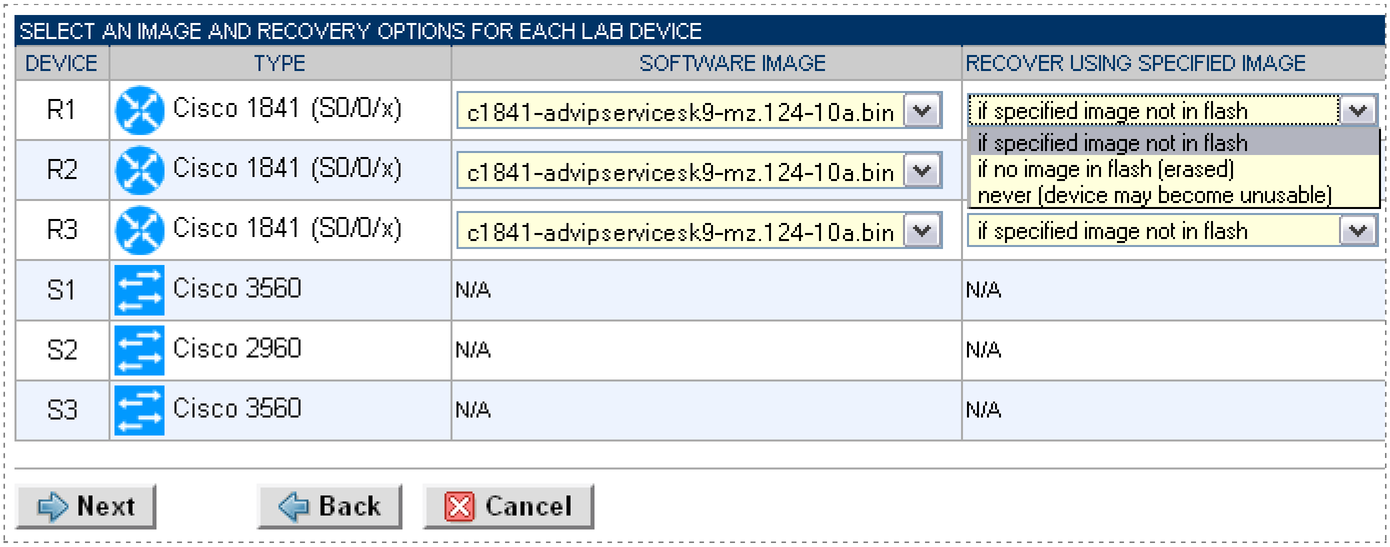
- Since password recovery is not supported on the device, you must use discretion in allowing user access to the pod. It is recommended allowing use by only a trusted group of users who will not perform password changes or other actions that may render the pod unavailable for subsequent reservations without intervention.

- Use of the NETLAB+ CLI Terminal with a generic console device will function only with devices using a command line interface. The applet does not provide terminal emulation such as VT100. You do have the option of using an alternate terminal application of your choice, if your selection is compatible with the device.

For detailed information, please refer to 5.4 for details.

4.6 Select Software Images and Recovery Options

This section is only applicable if there are network devices in your lab topology. NETLAB+ scrubs the devices at the end of lab reservations or upon request. During a scrub, NETLAB+ can recover an IOS image if it has been erased from flash.



SELECT AN IMAGE AND RECOVERY OPTIONS FOR EACH LAB DEVICE

DEVICE	TYPE	SOFTWARE IMAGE	RECOVER USING SPECIFIED IMAGE
R1	Cisco 1841 (S0/0/x)	c1841-advipservicesk9-mz.124-10a.bin	if specified image not in flash
R2	Cisco 1841 (S0/0/x)	c1841-advipservicesk9-mz.124-10a.bin	
R3	Cisco 1841 (S0/0/x)	c1841-advipservicesk9-mz.124-10a.bin	if specified image not in flash
S1	Cisco 3560	N/A	N/A
S2	Cisco 2960	N/A	N/A
S3	Cisco 3560	N/A	N/A

if specified image not in flash
if no image in flash (erased)
never (device may become unusable)
Next
Back
Cancel

You have three choices for flash recovery:

Recovery Using Specified Image	During A Scrub Operation…
If specified image not in flash	Restores the selected software image if that image is not in flash.
If no image in flash (erased)	Restores the selected software image if there are no .bin images in flash. No action is taken if flash contains a .bin image (even if it is not the specified one).
Never (device may become unusable)	NETLAB+ will take no action if the flash does not contain a bootable image. In this case, NETLAB+ automated boot process will fail and manual restoration of IOS will be required.

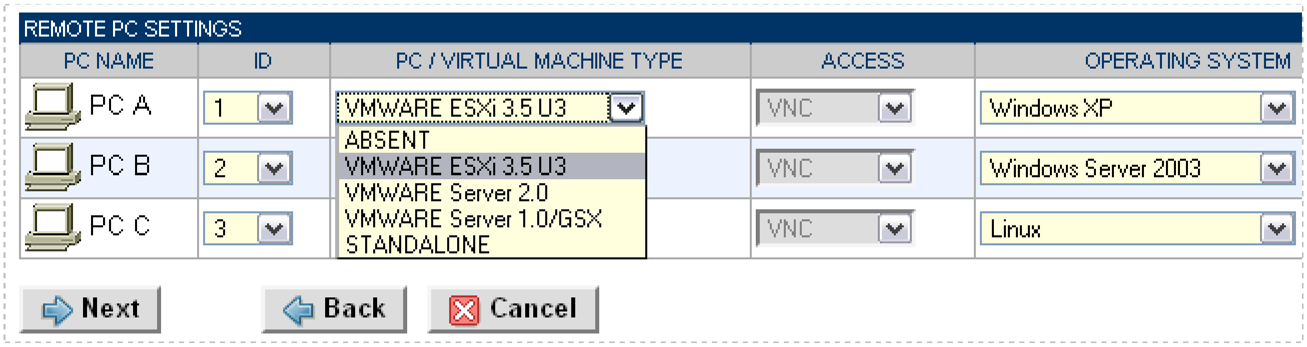
If you select an automatic recovery option, you must also select a software image supported by the curriculum. NETLAB$_{AE}$ users may refer to the guide specific for their selected pod-type.

If you select a Cisco ASA security device, additional management options become available in the device manager. These additional settings do not appear in the New Pod Wizard and must be made separately from a new pod install. Please see section 5.3 for details.

There is an additional image management setting for routers to support Pagent IOS images. A license key must be entered in order for NETLAB+ automation to function with routers using Pagent IOS. This setting does not appear in the New Pod Wizard and must be made separately from a new pod installation. For information on upgrading a router to use Pagent IOS, please see Appendix B of the NETLAB+ Administrator Guide.

4.7 Select PC Options

This section is only applicable if there are PCs in your lab topology. Select an ID, type, access method, and operating system for your PCs and servers.



REMOTE PC SETTINGS

PC NAME	ID	PC / VIRTUAL MACHINE TYPE	ACCESS	OPERATING SYSTEM
PC A	1	VMWARE ESXi 3.5 U3	VNC	Windows XP
PC B	2		VNC	Windows Server 2003
PC C	3		VNC	Linux

ID. Select a unique numeric identifier for this PC. The ID you choose is also appended to 169.254.0.X to become IP address assigned to the PC's control path network interface. You should accept the defaults unless you want to influence the last octet of the IP address (i.e. you already setup the PC and assigned an address)

PC/Virtual Machine Type

- VMWARE ESXi 3.5 U3 provides direct access to a VMware virtual machine and enables automation through the VMware API. This is the correct setting if you are using VMware ESXi.

- VMWARE Server 2.0 provides direct access to a VMware virtual machine and enables automation through the VMware API. This is the correct setting if you are using VMware Server version 2.x.

- VMWARE Server 1.0/GSX provides direct access to a VMware virtual machine and enables automation through the VMware API. This is the correct setting for VMware virtual machines if you are using VMware Server version 1.x or GSX.

- STANDALONE provides indirect access to a real PC or server resource.

- 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.

If you have not yet set up VMware and installed virtual machines on your NETLAB+ system, you may use the ABSENT setting for now, and modify the setting after installing your virtual machines.

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.

- INDIRECT specifies a static PC or server resource. Users will not have access to the keyboard, video, or mouse. This option is only available when PC type is STANDALONE.

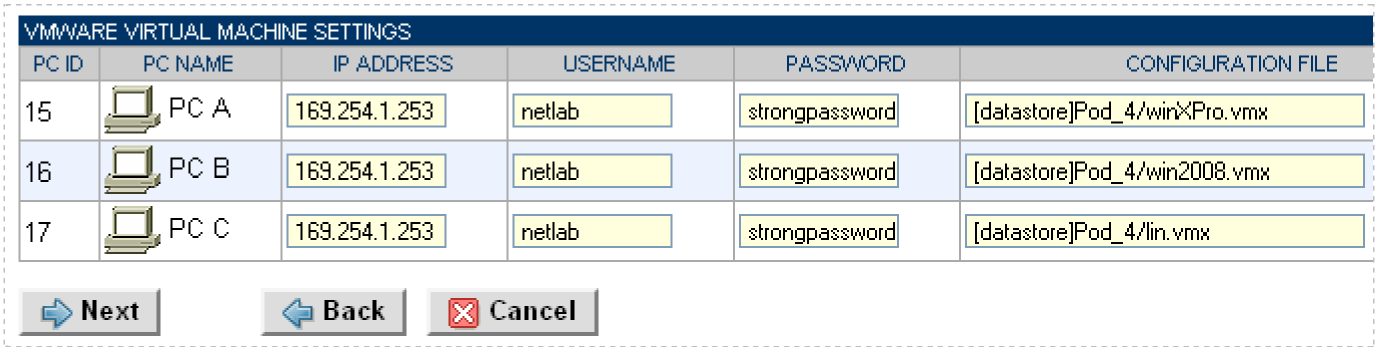
The **Operating System** setting specifies an OS for this PC. The availability of a selection does not guarantee compatibility with all labs.

The following table depicts the type and access settings that are available for selection:

To implement…	Set TYPE to…	Set ACCESS to…
VMware	Select the VMware virtualization product you are using. Selections include, **VMWARE ESXi 3.5 U3, VMWARE Server 2.0** and **VMWARE Server 1.0/GSX**.	VNC
Standalone	Does not apply to VMware implementations.	
Indirect	STANDALONE	INDIRECT
Absent (no PC)	**ABSENT**	**(not applicable)**

4.8 VMware Settings

If you select one of the VMware settings for any of the PCs, NETLAB+ will prompt for additional settings on the next page.



VMWARE VIRTUAL MACHINE SETTINGS

PC ID	PC NAME	IP ADDRESS	USERNAME	PASSWORD	CONFIGURATION FILE
15	PC A	169.254.1.253	netlab	strongpassword	[datastore]Pod_4/winXPro.vmx
16	PC B	169.254.1.253	netlab	strongpassword	[datastore]Pod_4/win2008.vmx
17	PC C	169.254.1.253	netlab	strongpassword	[datastore]Pod_4/lin.vmx

Each virtual machine requires four VMware-specific settings. Please refer to the *NETLAB+ Remote PC Guide* specific to your VMware server virtualization product selection for version-specific details regarding these settings.

- The **IP Address** setting is used to connect to the VMware host system. This is the IP address used for KVM and API traffic flow.

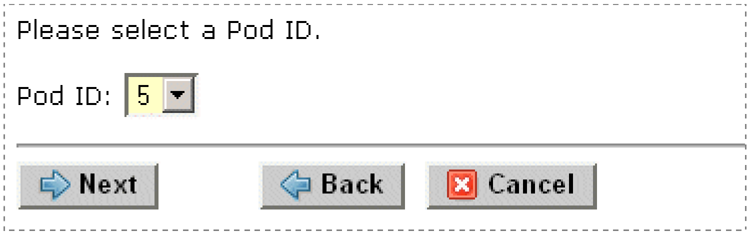
- **Username** specifies an operating system account on the VMware host system. NETLAB+ will use this account to login to the VMware host and control virtual machines through the VMware API (se

- **Password** specifies the password associated with the host account (see section

- **Configuration File** Enter the path of the virtual machine configuration file on the VMware host.

4.9 Select a Pod ID

Each pod is assigned a unique numeric ID.

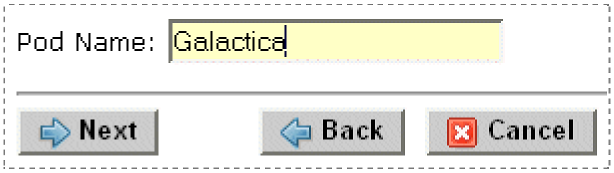


Please select a Pod ID.

Pod ID: 5

4.10 Select a Pod Name

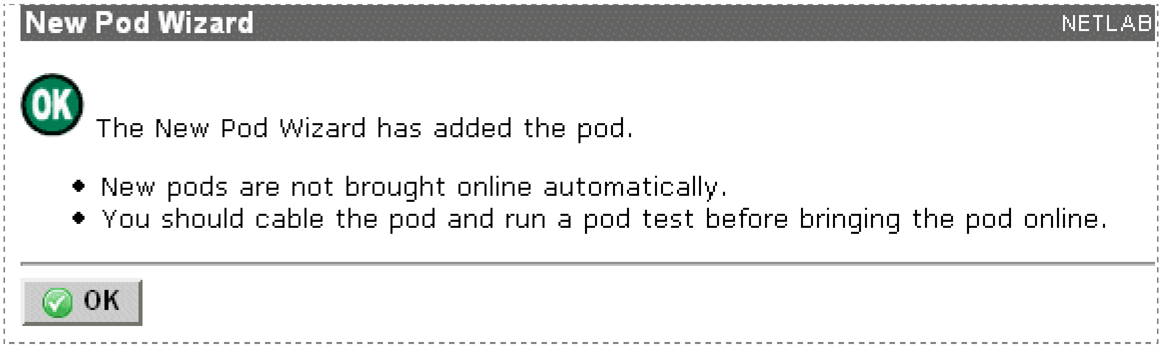
Each pod can have a unique name. This name will appear in the scheduler, along with the pod type.



Pod Name: Galactica

4.11 Verify Your Settings

At this point NETLAB+ has added the pod to its database. However, the pod has not been brought online yet. You will want to cable up the pod, and configure PCs (if any), and run a pod test before bringing the pod online.



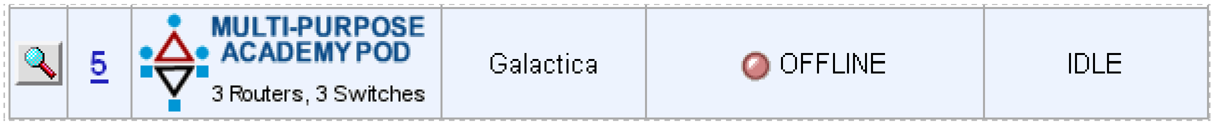
New Pod Wizard

The New Pod Wizard has added the pod.

- New pods are not brought online automatically.
- You should cable the pod and run a pod test before bringing the pod online.

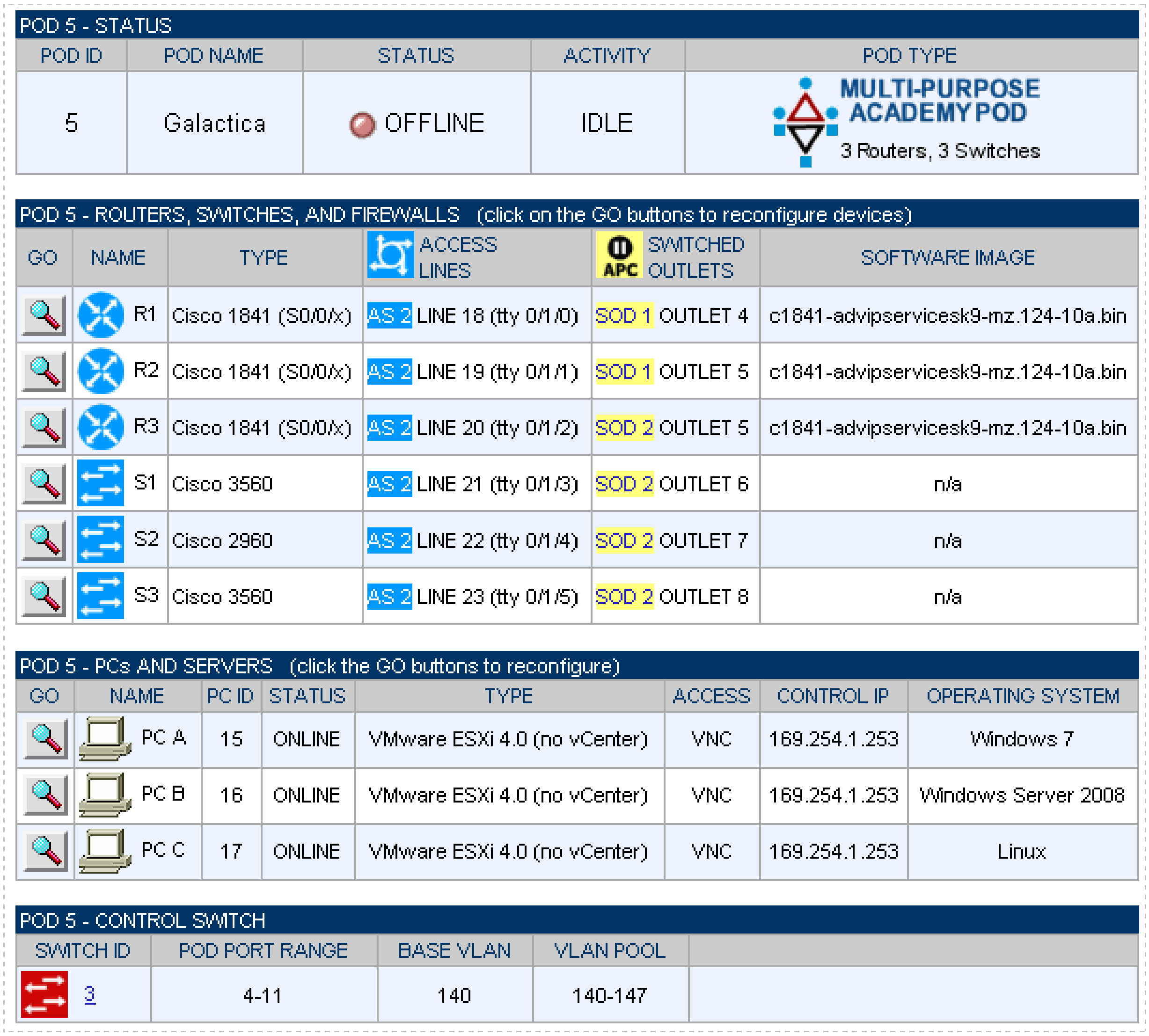
After you click **OK**, the new pod will appear in the list of equipment pods.

Click on the magnifier button or pod ID to manage you new pod.



🔍	5	MULTI-PURPOSE ACADEMY POD 3 Routers, 3 Switches	Galactica	● OFFLINE	IDLE

NETLAB+ will display the status of the pod and the high-level settings for each device, PC, and control switch.



POD 5 - STATUS

POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
5	Galactica	● OFFLINE	IDLE	MULTI-PURPOSE ACADEMY POD 3 Routers, 3 Switches

POD 5 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS LINES	SWITCHED OUTLETS	SOFTWARE IMAGE
🔍	R1	Cisco 1841 (S0/0/x)	AS 2 LINE 18 (tty 0/1/0)	SOD 1 OUTLET 4	c1841-advipservicesk9-mz.124-10a.bin
🔍	R2	Cisco 1841 (S0/0/x)	AS 2 LINE 19 (tty 0/1/1)	SOD 1 OUTLET 5	c1841-advipservicesk9-mz.124-10a.bin
🔍	R3	Cisco 1841 (S0/0/x)	AS 2 LINE 20 (tty 0/1/2)	SOD 2 OUTLET 5	c1841-advipservicesk9-mz.124-10a.bin
🔍	S1	Cisco 3560	AS 2 LINE 21 (tty 0/1/3)	SOD 2 OUTLET 6	n/a
🔍	S2	Cisco 2960	AS 2 LINE 22 (tty 0/1/4)	SOD 2 OUTLET 7	n/a
🔍	S3	Cisco 3560	AS 2 LINE 23 (tty 0/1/5)	SOD 2 OUTLET 8	n/a

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

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
🔍	PC A	15	ONLINE	VMware ESXi 4.0 (no vCenter)	VNC	169.254.1.253	Windows 7
🔍	PC B	16	ONLINE	VMware ESXi 4.0 (no vCenter)	VNC	169.254.1.253	Windows Server 2008
🔍	PC C	17	ONLINE	VMware ESXi 4.0 (no vCenter)	VNC	169.254.1.253	Linux

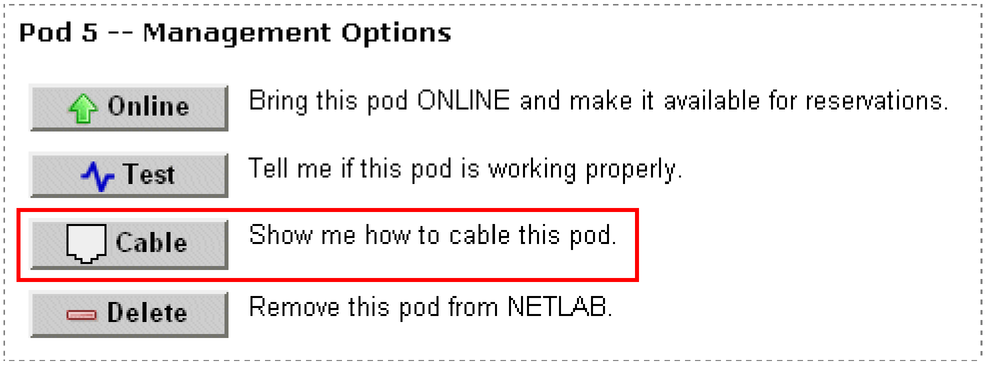
POD 5 - CONTROL SWITCH

SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL	
3	4-11	140	140-147	

4.12 Cable the Pod

NETLAB$_{AE}$ has a cable chart feature to help you connect the lab devices in your pod. The chart is generated in real-time and contains port-specific information based on your current lab device and control device settings.

The cable chart function is accessed from the pod management page.



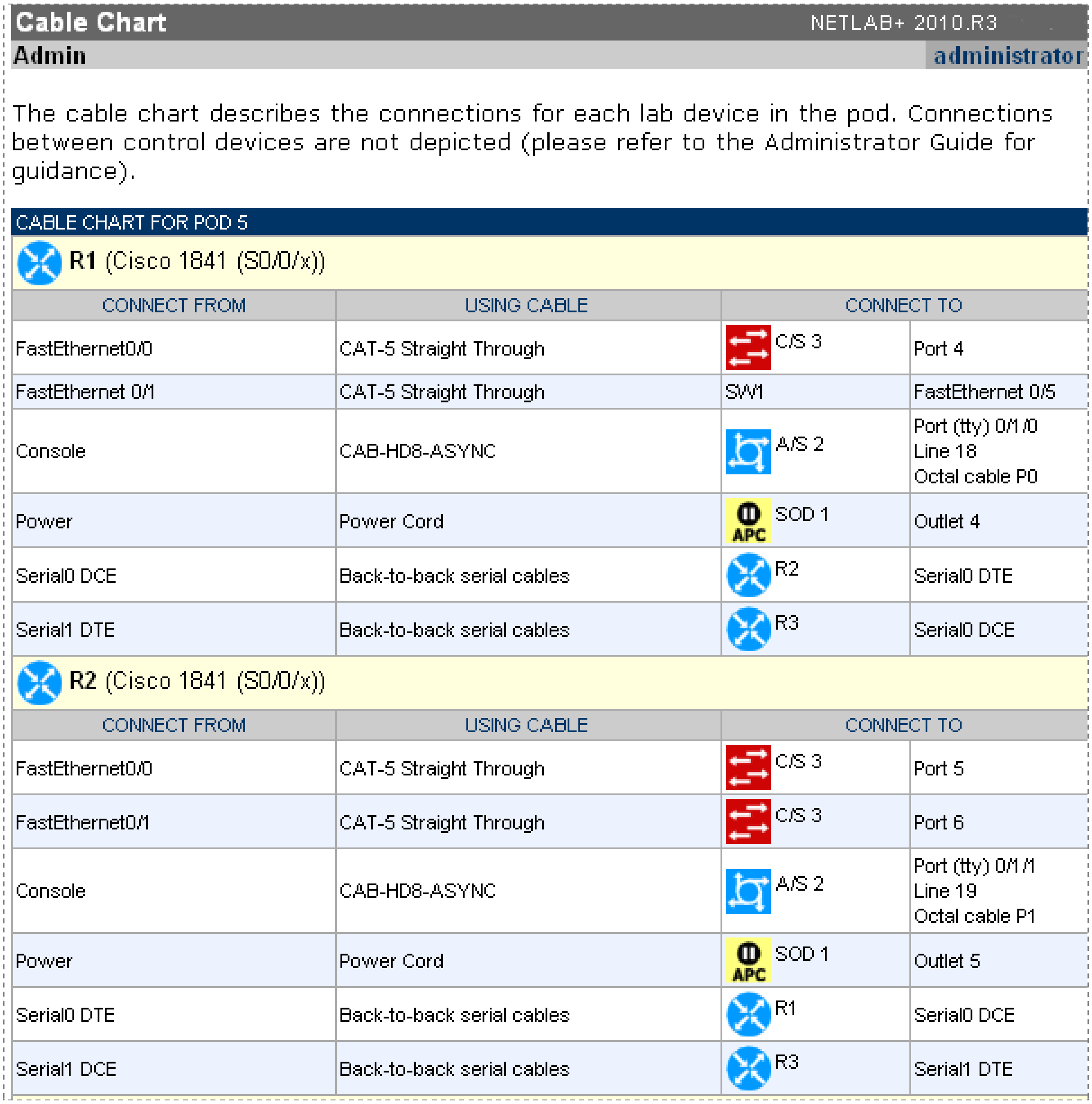
Pod 5 -- Management Options

Online — Bring this pod ONLINE and make it available for reservations.

Test — Tell me if this pod is working properly.

Cable — Show me how to cable this pod.

Delete — Remove this pod from NETLAB.



Cable Chart

NETLAB+ 2010.R3

Admin administrator

The cable chart describes the connections for each lab device in the pod. Connections between control devices are not depicted (please refer to the Administrator Guide for guidance).

CABLE CHART FOR POD 5

R1 (Cisco 1841 (S0/0/x))

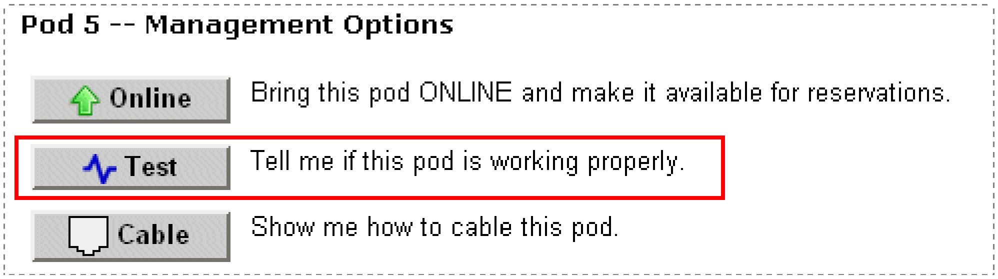
CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet0/0	CAT-5 Straight Through	C/S 3	Port 4
FastEthernet 0/1	CAT-5 Straight Through	SW1	FastEthernet 0/5
Console	CAB-HD8-ASYNC	A/S 2	Port (tty) 0/1/0 Line 18 Octal cable P0
Power	Power Cord	SOD 1	Outlet 4
Serial0 DCE	Back-to-back serial cables	R2	Serial0 DTE
Serial1 DTE	Back-to-back serial cables	R3	Serial0 DCE

R2 (Cisco 1841 (S0/0/x))

CONNECT FROM	USING CABLE	CONNECT TO	
FastEthernet0/0	CAT-5 Straight Through	C/S 3	Port 5
FastEthernet0/1	CAT-5 Straight Through	C/S 3	Port 6
Console	CAB-HD8-ASYNC	A/S 2	Port (tty) 0/1/1 Line 19 Octal cable P1
Power	Power Cord	SOD 1	Outlet 5
Serial0 DTE	Back-to-back serial cables	R1	Serial0 DCE
Serial1 DCE	Back-to-back serial cables	R3	Serial1 DTE

4.13 Test the Pod

After all routers and PCs have been installed, you should run a pod test to verify that your pod is working. The pod test will detect common configuration and cabling problems.



Pod 5 -- Management Options

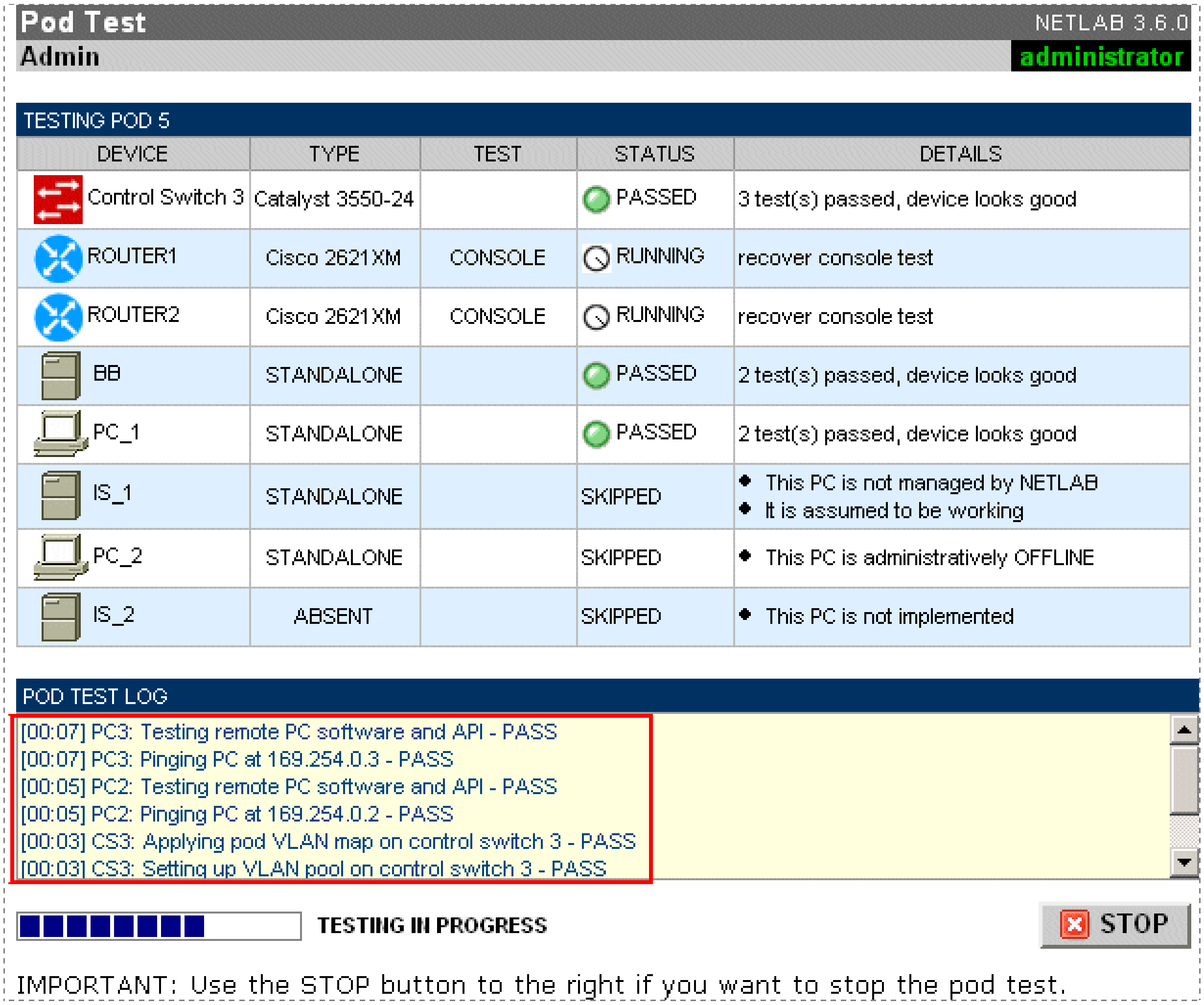
Online Bring this pod ONLINE and make it available for reservations.

Test Tell me if this pod is working properly.

Cable Show me how to cable this pod.

Some tests may take a long time. During the BOOTIOS test, NETLAB+ may have to load the specified IOS image if it is not in flash. The IOS images can be very large and can take up to 30 minutes to program into flash memory.

If you cannot resolve an issue and decide to contact technical support, please cut and paste the text from the POD TEST LOG and include with your e-mail.



Pod Test	NETLAB 3.6.0
Admin	administrator

TESTING POD 5

DEVICE	TYPE	TEST	STATUS	DETAILS
Control Switch 3	Catalyst 3550-24		● PASSED	3 test(s) passed, device looks good
ROUTER1	Cisco 2621XM	CONSOLE	RUNNING	recover console test
ROUTER2	Cisco 2621XM	CONSOLE	RUNNING	recover console test
BB	STANDALONE		● PASSED	2 test(s) passed, device looks good
PC_1	STANDALONE		● PASSED	2 test(s) passed, device looks good
IS_1	STANDALONE		SKIPPED	◆ This PC is not managed by NETLAB ◆ It is assumed to be working
PC_2	STANDALONE		SKIPPED	◆ This PC is administratively OFFLINE
IS_2	ABSENT		SKIPPED	◆ This PC is not implemented

POD TEST LOG

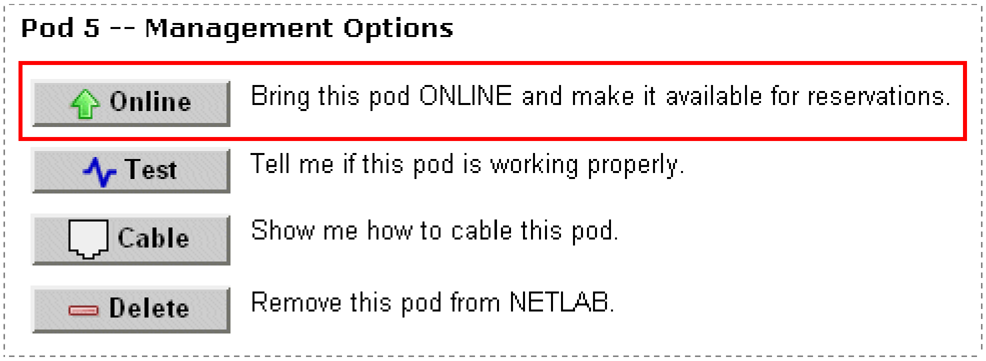
```
[00:07] PC3: Testing remote PC software and API - PASS
[00:07] PC3: Pinging PC at 169.254.0.3 - PASS
[00:05] PC2: Testing remote PC software and API - PASS
[00:05] PC2: Pinging PC at 169.254.0.2 - PASS
[00:03] CS3: Applying pod VLAN map on control switch 3 - PASS
[00:03] CS3: Setting up VLAN pool on control switch 3 - PASS
```

TESTING IN PROGRESS

IMPORTANT: Use the STOP button to the right if you want to stop the pod test.

4.14 Bring the Pod(s) Back Online

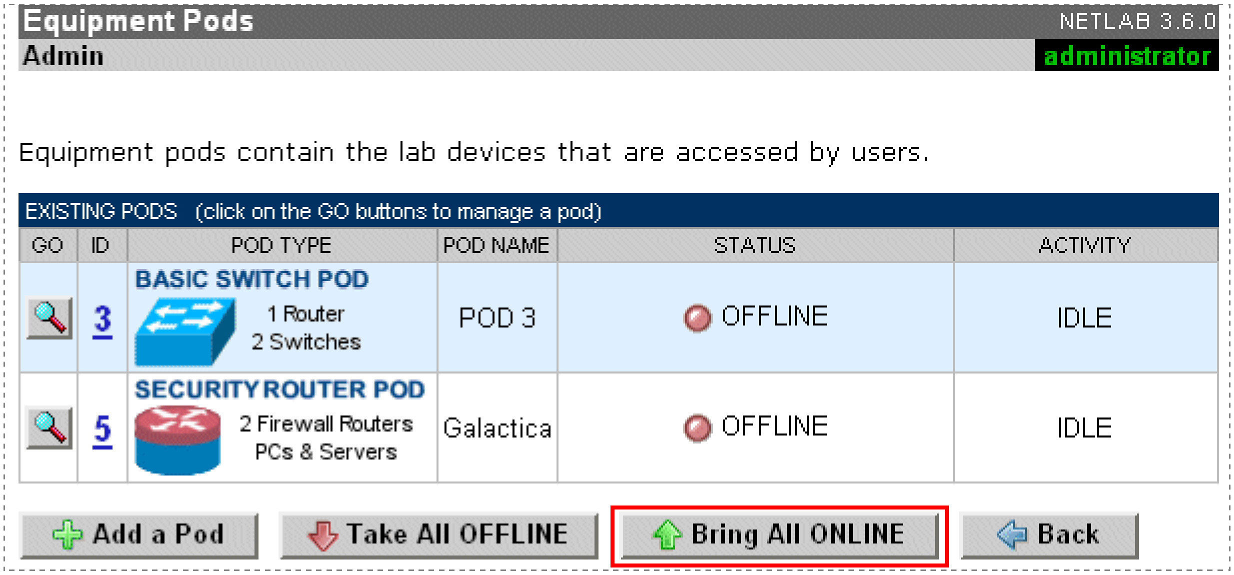
Now you can bring the pod online and make it available for lab reservations. You can bring just this pod online by clicking the Online button under Management Options.



Pod 5 -- Management Options

Online	Bring this pod ONLINE and make it available for reservations.
Test	Tell me if this pod is working properly.
Cable	Show me how to cable this pod.
Delete	Remove this pod from NETLAB.

Alternatively, you can click Bring All ONLINE on the Equipment Pods page. Choose this option when you have no more additions or modifications to pods or control devices and you wish to put all pods into service.



Equipment Pods NETLAB 3.6.0

Admin administrator

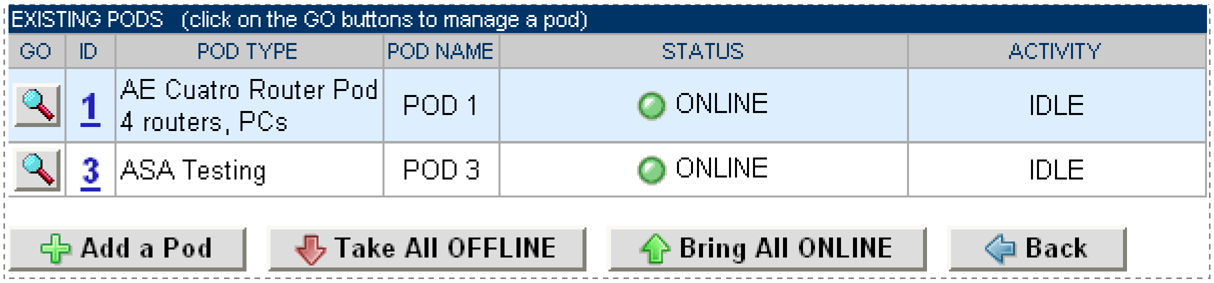
Equipment pods contain the lab devices that are accessed by users.

EXISTING PODS (click on the GO buttons to manage a pod)

GO	ID	POD TYPE	POD NAME	STATUS	ACTIVITY
	3	BASIC SWITCH POD 1 Router 2 Switches	POD 3	OFFLINE	IDLE
	5	SECURITY ROUTER POD 2 Firewall Routers PCs & Servers	Galactica	OFFLINE	IDLE

5 Modifying Device Settings

If it is necessary to make modifications to device settings that were selected during the pod installation, select the appropriate pod on the Equipment Pods page.



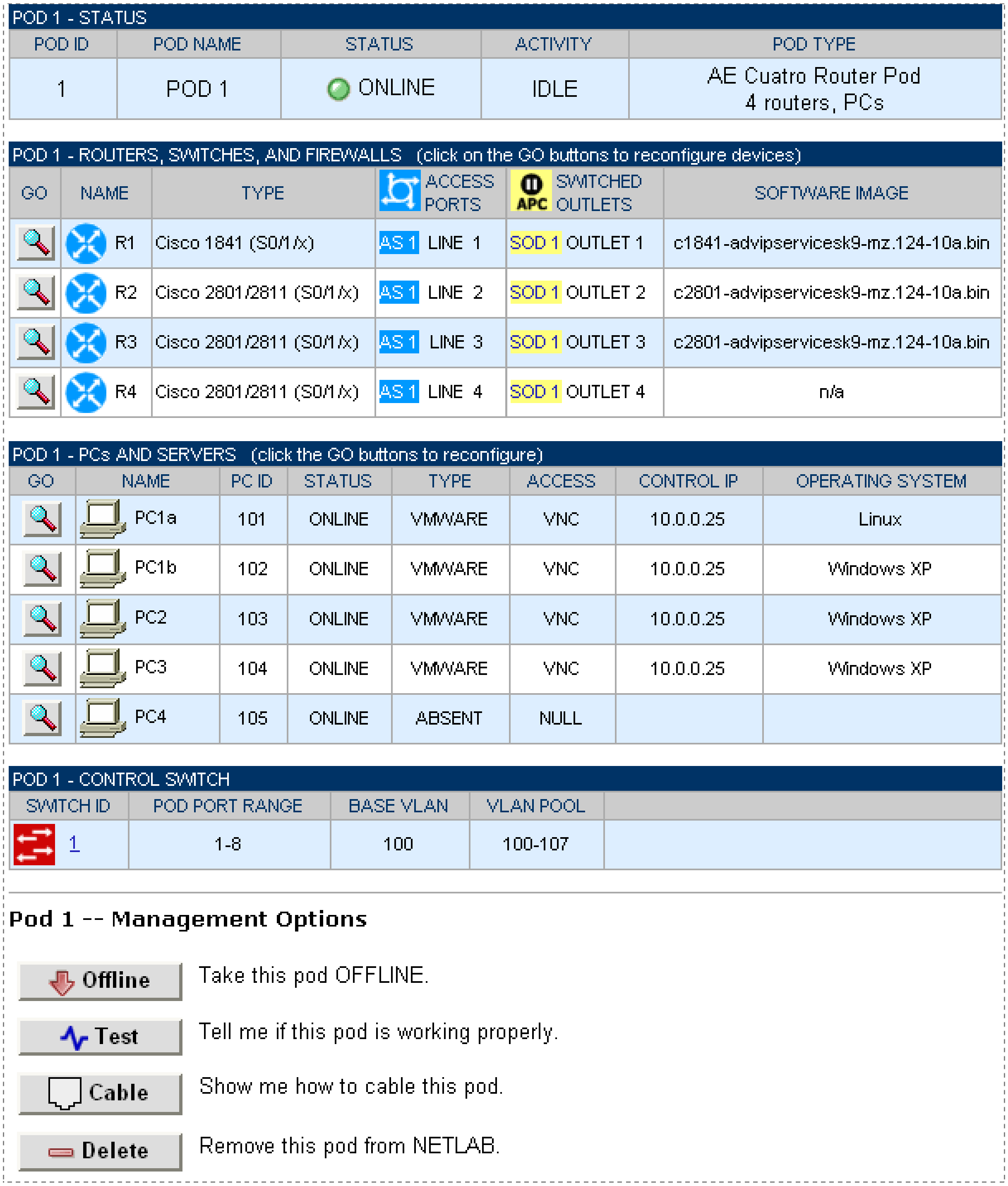
EXISTING PODS (click on the GO buttons to manage a pod)

GO	ID	POD TYPE	POD NAME	STATUS	ACTIVITY
🔍	1	AE Cuatro Router Pod 4 routers, PCs	POD 1	● ONLINE	IDLE
🔍	3	ASA Testing	POD 3	● ONLINE	IDLE

In order to modify settings, the pod must be offline. You have the option to select Take All OFFLINE to bring all the pods offline or select a single pod and take the pod offline on the pod specific page.

The network and hardware settings depicted here are intended to provide an example only. Your system requirements may differ according to your specific hardware selections.

Select the pod, which contains the device(s) requiring setting modifications using the magnify button 🔍 to the left of Pod Id. In this example, we have selected Pod 1.



POD 1 - STATUS

POD ID	POD NAME	STATUS	ACTIVITY	POD TYPE
1	POD 1	● ONLINE	IDLE	AE Cuatro Router Pod 4 routers, PCs

POD 1 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS PORTS	SWITCHED OUTLETS	SOFTWARE IMAGE
🔍	R1	Cisco 1841 (S0/1/x)	AS 1 LINE 1	SOD 1 OUTLET 1	c1841-advipservicesk9-mz.124-10a.bin
🔍	R2	Cisco 2801/2811 (S0/1/x)	AS 1 LINE 2	SOD 1 OUTLET 2	c2801-advipservicesk9-mz.124-10a.bin
🔍	R3	Cisco 2801/2811 (S0/1/x)	AS 1 LINE 3	SOD 1 OUTLET 3	c2801-advipservicesk9-mz.124-10a.bin
🔍	R4	Cisco 2801/2811 (S0/1/x)	AS 1 LINE 4	SOD 1 OUTLET 4	n/a

POD 1 - PCs AND SERVERS (click the GO buttons to reconfigure)

GO	NAME	PC ID	STATUS	TYPE	ACCESS	CONTROL IP	OPERATING SYSTEM
🔍	PC1a	101	ONLINE	VMWARE	VNC	10.0.0.25	Linux
🔍	PC1b	102	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	PC2	103	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	PC3	104	ONLINE	VMWARE	VNC	10.0.0.25	Windows XP
🔍	PC4	105	ONLINE	ABSENT	NULL		

POD 1 - CONTROL SWITCH

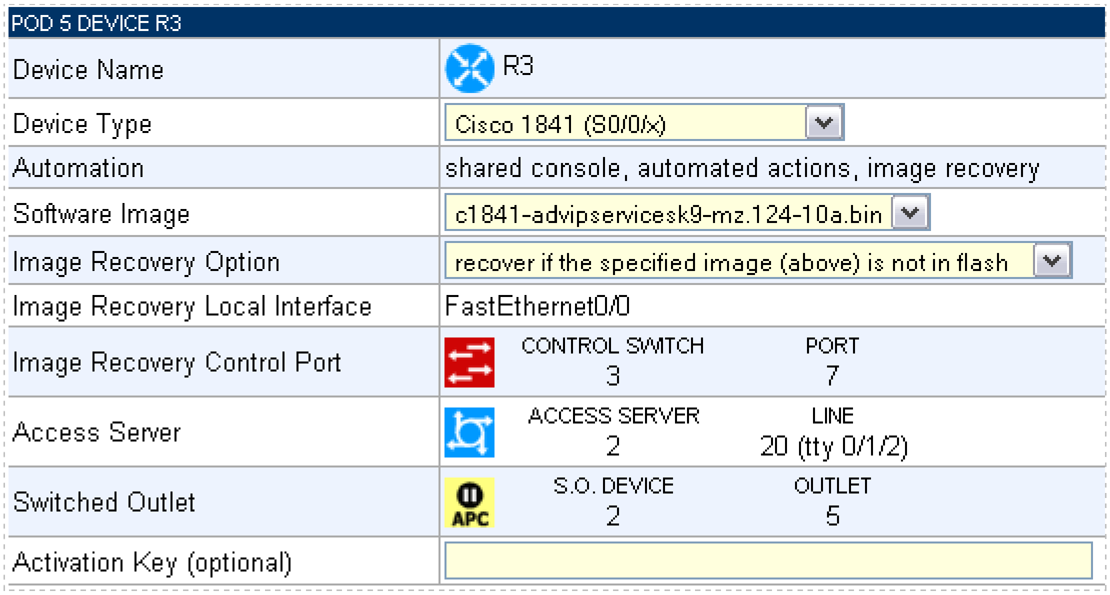
SWITCH ID	POD PORT RANGE	BASE VLAN	VLAN POOL
1	1-8	100	100-107

Pod 1 -- Management Options

Offline	Take this pod OFFLINE.
Test	Tell me if this pod is working properly.
Cable	Show me how to cable this pod.
Delete	Remove this pod from NETLAB.

5.1 Modifying Device Settings for Routers, Switches and Firewalls

Select a device to modify using the magnify button to the left of the device name. In this example, we are examining the settings for R1.

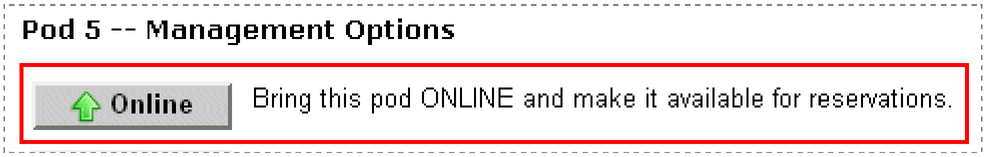


POD 5 DEVICE R3	
Device Name	R3
Device Type	Cisco 1841 (S0/0/x)
Automation	shared console, automated actions, image recovery
Software Image	c1841-advipservicesk9-mz.124-10a.bin
Image Recovery Option	recover if the specified image (above) is not in flash
Image Recovery Local Interface	FastEthernet0/0
Image Recovery Control Port	CONTROL SWITCH 3 PORT 7
Access Server	ACCESS SERVER 2 LINE 20 (tty 0/1/2)
Switched Outlet	APC S.O. DEVICE 2 OUTLET 5
Activation Key (optional)	

See sections 4.4 and 4.6 for details on making device-setting selections for your equipment.

There are additional management settings for Cisco ASA devices and Generic Console Devices that can be set after pod installation has been completed. Please see section 5.3 and 5.4 for details.

Please note that the pod must be offline in order to modify these settings. After completing modifications, remember to select the management option to bring the pod online and make it available for reservations.

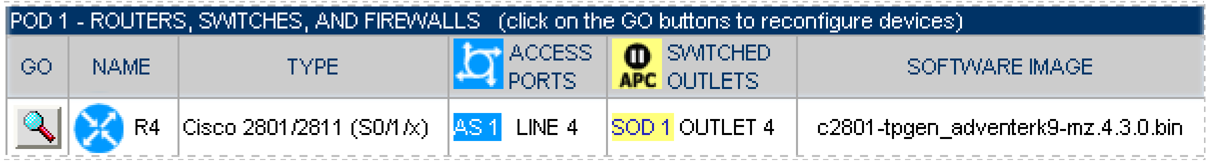


Pod 5 -- Management Options

Online — Bring this pod ONLINE and make it available for reservations.

5.2 Modifying Device Settings for Routers Using Pagent IOS

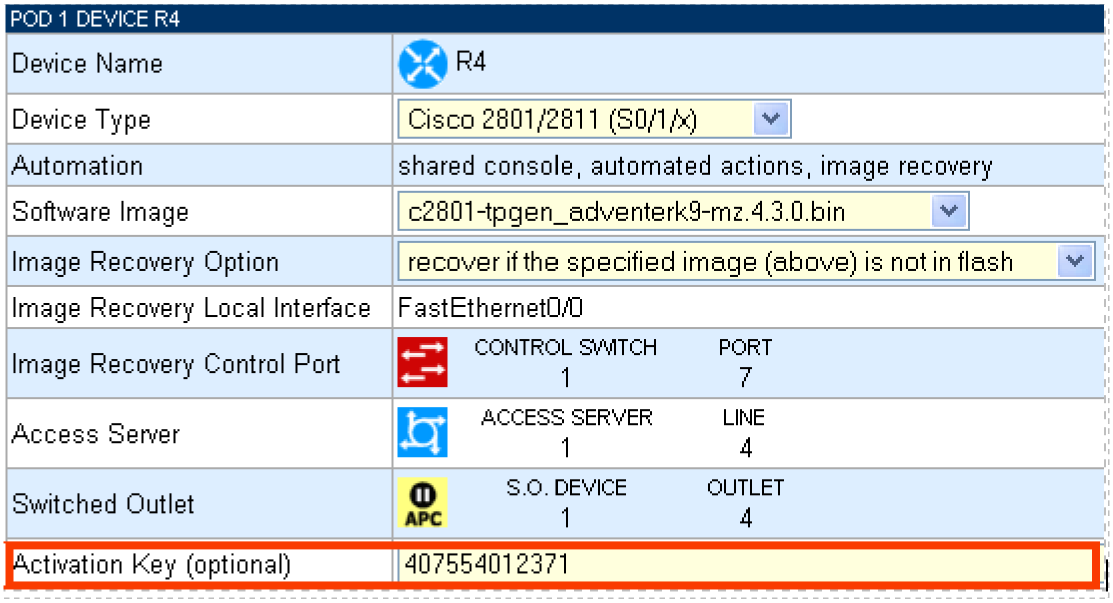
If your device selections include routers using Pagent IOS, it will be necessary to enter the license key for these devices after the pod installation has been completed. This additional management option becomes available for selection when the device is selected on the Equipment Pods page.



POD 1 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS PORTS		SWITCHED OUTLETS		SOFTWARE IMAGE
🔍	R4	Cisco 2801/2811 (S0/1/x)	AS 1	LINE 4	SOD 1	OUTLET 4	c2801-tpgen_adventerk9-mz.4.3.0.bin

Select the router to display the management options.



POD 1 DEVICE R4

Device Name	R4		
Device Type	Cisco 2801/2811 (S0/1/x)		
Automation	shared console, automated actions, image recovery		
Software Image	c2801-tpgen_adventerk9-mz.4.3.0.bin		
Image Recovery Option	recover if the specified image (above) is not in flash		
Image Recovery Local Interface	FastEthernet0/0		
Image Recovery Control Port		CONTROL SWITCH 1	PORT 7
Access Server		ACCESS SERVER 1	LINE 4
Switched Outlet		S.O. DEVICE 1	OUTLET 4
Activation Key (optional)	407554012371		

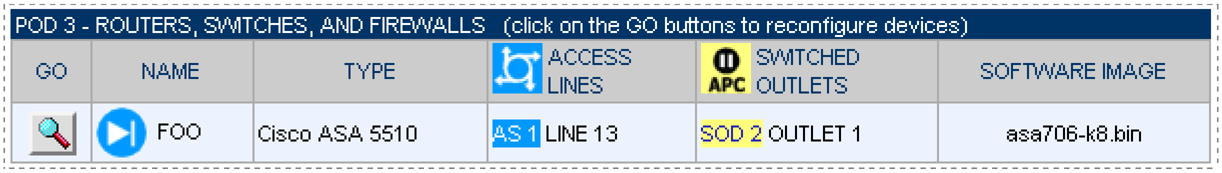
A license key must be entered into the Activation Key field for all routers using Pagent IOS in order for NETLAB+ automation features to function.

For information on upgrading a router to use Pagent IOS, please see Appendix B of the NETLAB+ Administrator Guide.

This optional field may be left blank for routers not using Pagent IOS.

5.3 Modifying Device Settings for Cisco ASA Security Devices

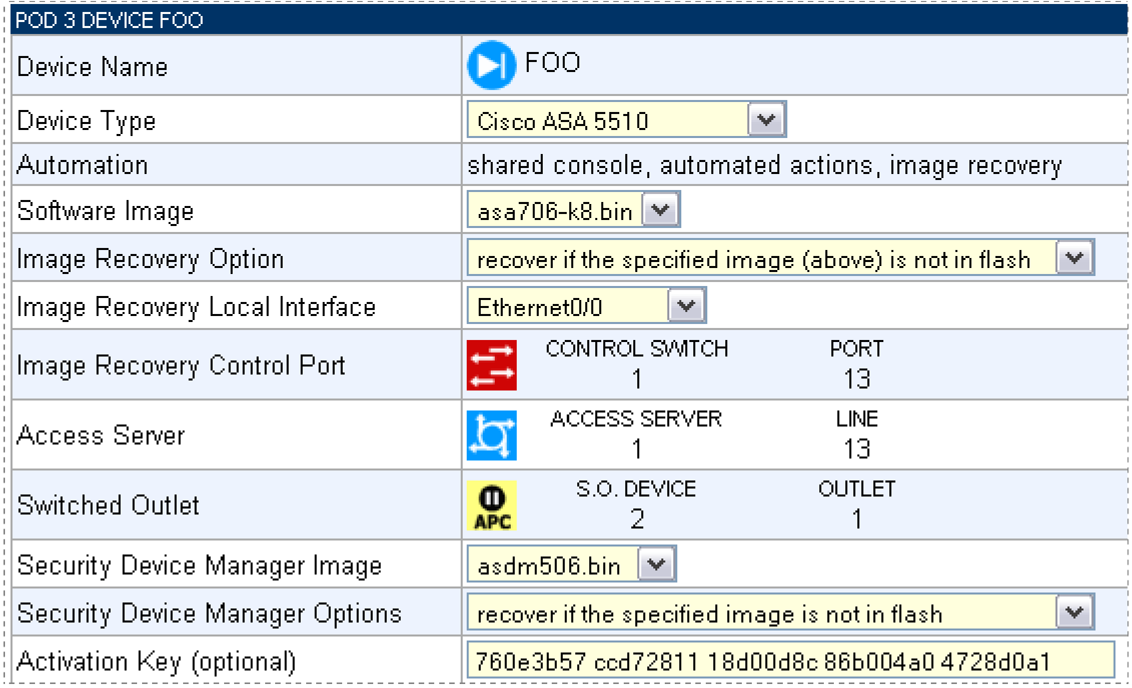
If your device selections include Cisco ASA security appliances, it will be necessary to select device settings for these devices after the pod installation has been completed. These additional management options become available for selection when the device is selected on the Equipment Pods page.



POD 3 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS LINES	SWITCHED OUTLETS	SOFTWARE IMAGE
🔍	FOO	Cisco ASA 5510	AS 1 LINE 13	SOD 2 OUTLET 1	asa706-k8.bin

Select the device to display the management options.



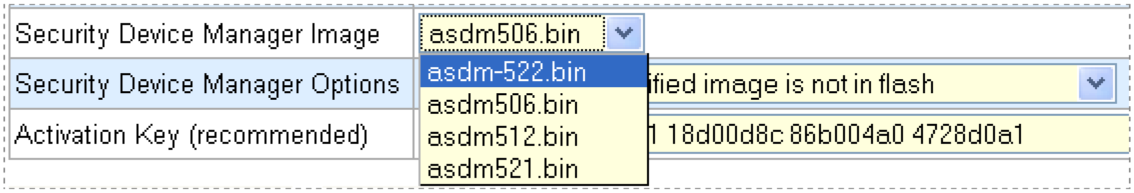
POD 3 DEVICE FOO

Device Name	FOO
Device Type	Cisco ASA 5510
Automation	shared console, automated actions, image recovery
Software Image	asa706-k8.bin
Image Recovery Option	recover if the specified image (above) is not in flash
Image Recovery Local Interface	Ethernet0/0
Image Recovery Control Port	CONTROL SWITCH 1 PORT 13
Access Server	ACCESS SERVER 1 LINE 13
Switched Outlet	S.O. DEVICE 2 OUTLET 1
Security Device Manager Image	asdm506.bin
Security Device Manager Options	recover if the specified image is not in flash
Activation Key (optional)	760e3b57 ccd72811 18d00d8c 86b004a0 4728d0a1

Here, we describe the options that are available for selection for ASA devices, in addition to the other device option settings referred to in the previous section.

Image Recovery Local Interface This setting must match the port, which is connected to the cable, which is connected to the control switch that is defined as the Image Recovery Control Port. The correct setting for this interface is set during pod installation and should not require modification on a $NETLAB_{AE}$ system.

Security Device Manager Image. The software image providing the Security Device Manager software. In order for these image files to be available for selection, they must first be uploaded to the system, see section 3.5 for details. Note that the SDM image is tied to specific versions of the ASA software image. NETLAB+ does not check for compatibility between the two images, administrators should check the vendor's release notes specific to their selected device to insure compatibility.

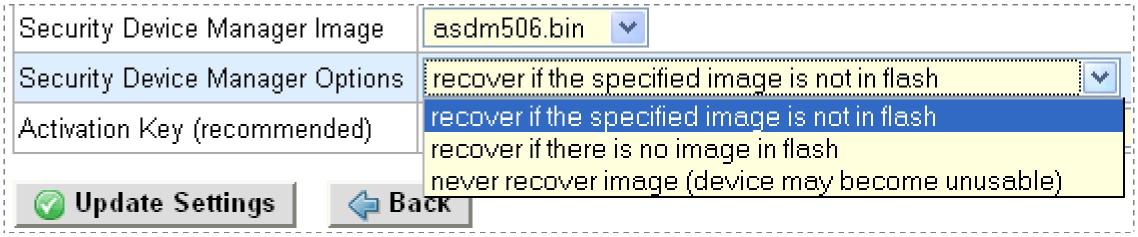


Security Device Manager Image: asdm506.bin

Security Device Manager Options: ified image is not in flash

Activation Key (recommended): 1 18d00d8c 86b004a0 4728d0a1

Security Device Manager Options. This option determines when the SDM image is recovered. A selection of "never" means that the SDM image will not be managed by NETLAB+.



Security Device Manager Image: asdm506.bin

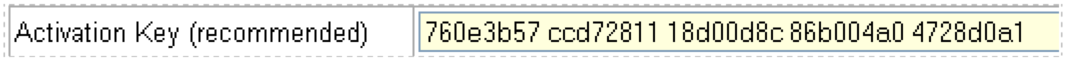
Security Device Manager Options: recover if the specified image is not in flash

Activation Key (recommended)

recover if the specified image is not in flash
recover if there is no image in flash
never recover image (device may become unusable)
Update Settings
Back

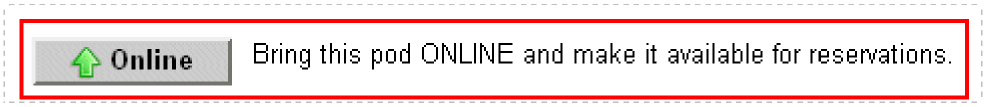
Activation Key. Cisco ASA software requires an activation key. If specified, NETLAB+ will configure the activation key during the scrub process.

As a precaution, administrators should write down their activation keys prior to installing Cisco ASA or PIX devices in NETLAB+.



Activation Key (recommended): 760e3b57 ccd72811 18d00d8c 86b004a0 4728d0a1

Please note that the pod must be offline in order to modify these settings. After completing modifications, remember to select the management option to bring the pod online and make it available for reservations.



Bring this pod ONLINE and make it available for reservations.

5.4 Modifying Device Settings for Generic Console Devices

If you would like to use a lab device that is not supported by NETLAB+, it may be possible by selecting Generic Console Device option in the Device Type pull down menu. This option provides user console access to an unsupported device during a lab reservation. This option also supports the console-sharing feature; therefore, several users could access the console at the same time.

A generic console device has several limitations:

1. Automated scrub, password recovery, and configuration management are not performed. The device will not be reset to a clean configuration between lab reservations. If a user changes a password to an unknown value, a manual password recovery will be necessary.

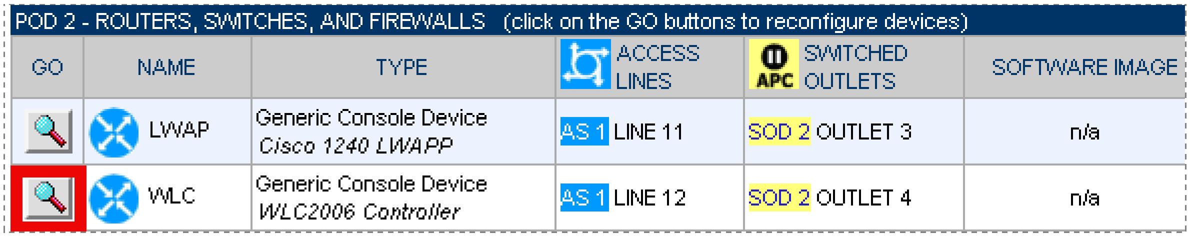
2. The NETLAB+ CLI Terminal is designed for command line interfaces and do not provide terminal emulation. If your device requires terminal emulation (such as VT100), users must use a terminal application that supports the required terminal emulation (this can be set in their profile settings). Because terminal emulation uses screen formatting and invisible control codes, the NETLAB+ console sharing and archive features may exhibit unpredictable behavior.

3. Generic console devices may be controlled by a switched outlet. This is determined by the pod design. See below for details.

Generic console devices are unmanaged. Due to the limitations outlined above, you should only deploy this option in environments where users are experienced and trusted. Users should be briefed on these limitations and the proper procedures for using the device without causing problems for others.

Configuring a Generic Console Device

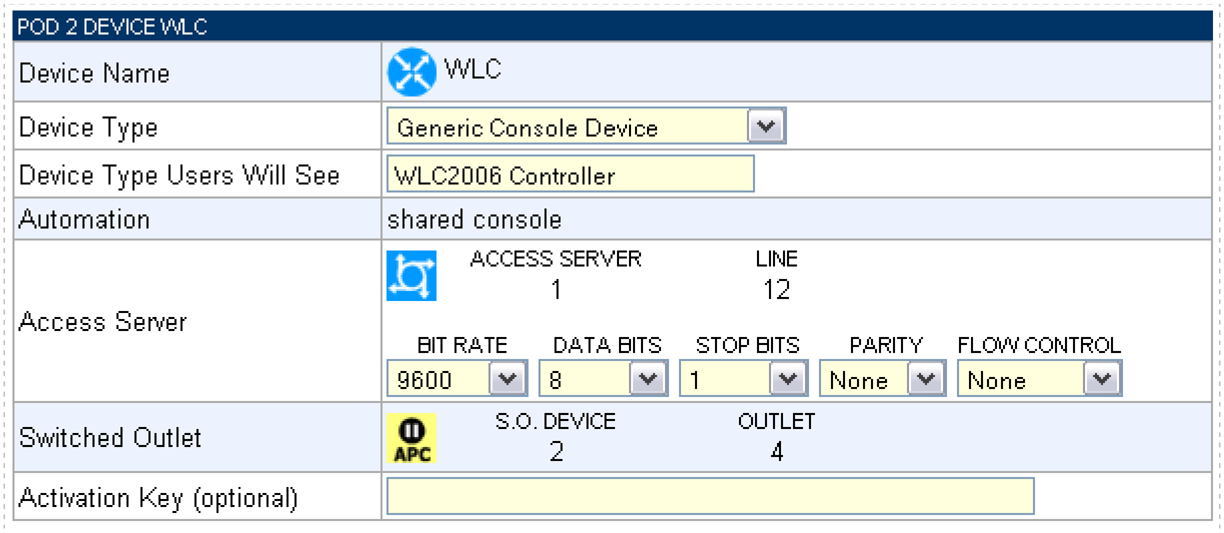
Step 1. Select the desired device from the Equipment Pods page, and click the GO button.



POD 2 - ROUTERS, SWITCHES, AND FIREWALLS (click on the GO buttons to reconfigure devices)

GO	NAME	TYPE	ACCESS LINES	SWITCHED OUTLETS	SOFTWARE IMAGE
🔍	LWAP	Generic Console Device *Cisco 1240 LWAPP*	AS 1 LINE 11	SOD 2 OUTLET 3	n/a
🔍	WLC	Generic Console Device *WLC2006 Controller*	AS 1 LINE 12	SOD 2 OUTLET 4	n/a

Step 2. Select Generic Console Device from the Device Type pull down menu. Click OK on the popup to confirm this change.



POD 2 DEVICE WLC	
Device Name	WLC
Device Type	Generic Console Device
Device Type Users Will See	WLC2006 Controller
Automation	shared console
Access Server	ACCESS SERVER 1, LINE 12 BIT RATE 9600, DATA BITS 8, STOP BITS 1, PARITY None, FLOW CONTROL None
Switched Outlet	S.O. DEVICE 2, OUTLET 4
Activation Key (optional)	

Step 3. In the *Device Type Users Will See* field, type in a brief description of the actual device. This provides a more descriptive name for the device that will be displayed for users when accessing the pod during a lab reservation.

Step 4. Set the asynchronous communication parameters for the access server port. NETLAB+ will initialize the access server port using these parameters at the beginning of each lab reservation.

It is recommended that flow control remain set to none. If hardware flow control is selected and cabling and hardware are not configured correctly for hardware flow control, the access server port may will hang and require and require a manual access to the access server to clear the line.

Switched Outlet

The switched outlet settings are displayed for reference only. The pod design determines whether a switched outlet is allocated for the device. The following table describes switched outlet behavior.

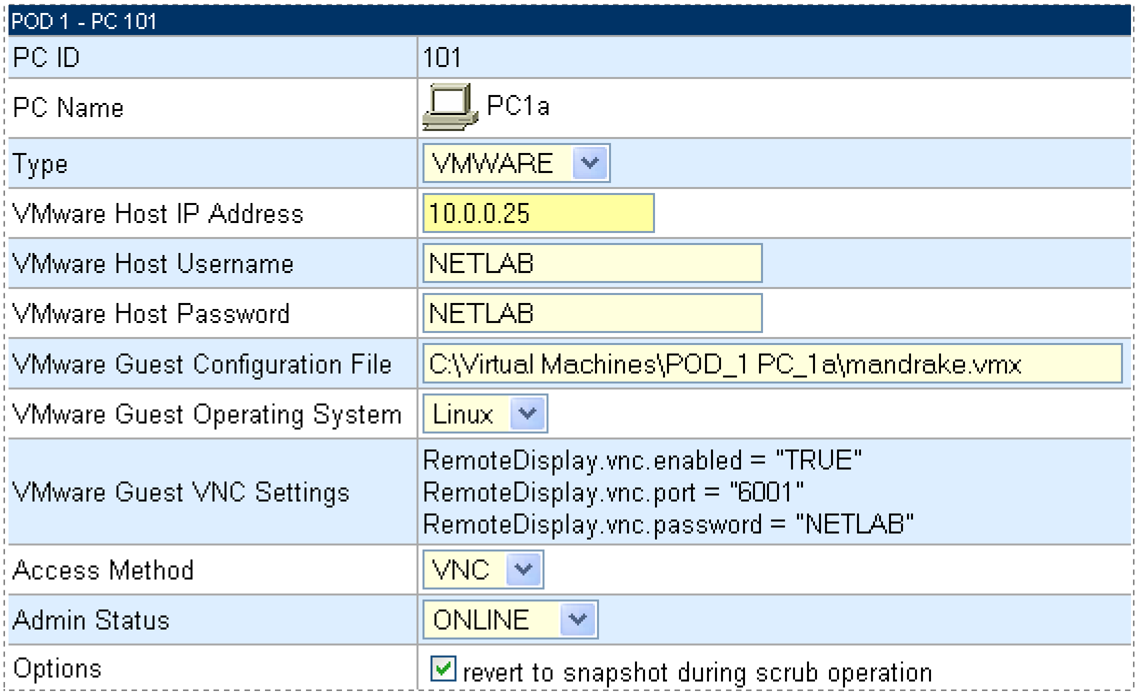
	Pod design allocates a switched outlet:	Pod design DOES NOT allocate switched outlet:
Power Source	Switched Outlet	Uncontrolled Outlet
At beginning of lab	Power On	Always On
At end of lab	Power Off	Always On
During lab	User Controlled	Always On

If this is a custom pod and you have access to the pod design, you may control whether or not a switched outlet is allocated. This setting is a function of pod design. Please refer the *NETLAB+ Pod Design Guide* for details.

If you are using a NETLAB$_{AE}$ standard pod, or you do not have access to the pod design, you may plug the device into an uncontrolled outlet if you do not want switched outlet behavior. However, if a switched outlet is allocated, it cannot be reclaimed.

5.5 Modifying PC Settings

In order to modify the settings for a PC that has been installed in the pod, Select the PC using the magnify button to the left of the PC name. In this example, we are examining the settings for PC1a.



POD 1 - PC 101

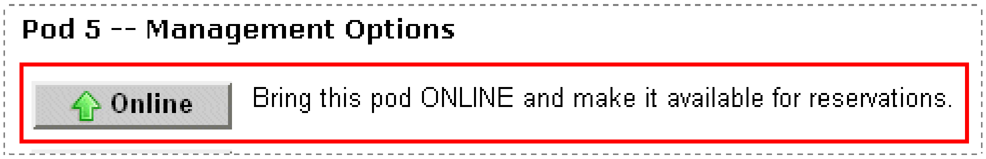
PC ID	101
PC Name	PC1a
Type	VMWARE
VMware Host IP Address	10.0.0.25
VMware Host Username	NETLAB
VMware Host Password	NETLAB
VMware Guest Configuration File	C:\Virtual Machines\POD_1 PC_1a\mandrake.vmx
VMware Guest Operating System	Linux

VMware Guest VNC Settings	RemoteDisplay.vnc.enabled = "TRUE"
	RemoteDisplay.vnc.port = "6001"
	RemoteDisplay.vnc.password = "NETLAB"

Access Method	VNC
Admin Status	ONLINE
Options	☑ revert to snapshot during scrub operation

Refer to section 4.7 for information on selecting PC settings.

Please note that the pod must be offline in order to modify these settings. After completing modifications, remember to select the management option to bring the pod online and make it available for reservations.



Pod 5 -- Management Options

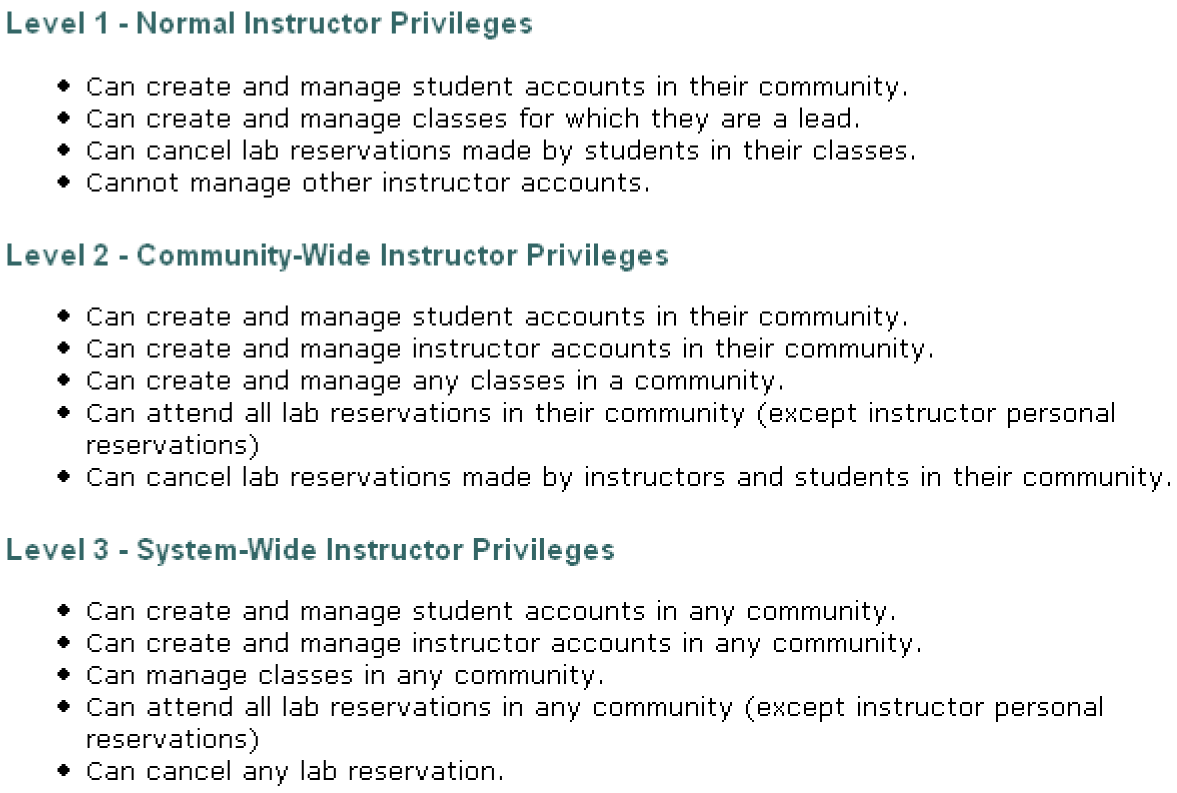
Online — Bring this pod ONLINE and make it available for reservations.

6 First Steps Using NETLAB+

After successfully installing your pod(s) it is recommended that you try out some of the major features of NETLAB+ in order to become familiar and comfortable using the system.

The duties of the NETLAB+ administrator include the management of communities, accounts and classes on the NETLAB+ system. You have the option to delegate account and class management duties to instructors that you have granted the appropriate privilege level.

A summary of instructor privilege levels is shown here. Please refer to the Modify Instructor Privileges section of *NETLAB+ Administrator Guide* for more details.



Level 1 - Normal Instructor Privileges

- Can create and manage student accounts in their community.
- Can create and manage classes for which they are a lead.
- Can cancel lab reservations made by students in their classes.
- Cannot manage other instructor accounts.

Level 2 - Community-Wide Instructor Privileges

- Can create and manage student accounts in their community.
- Can create and manage instructor accounts in their community.
- Can create and manage any classes in a community.
- Can attend all lab reservations in their community (except instructor personal reservations)
- Can cancel lab reservations made by instructors and students in their community.

Level 3 - System-Wide Instructor Privileges

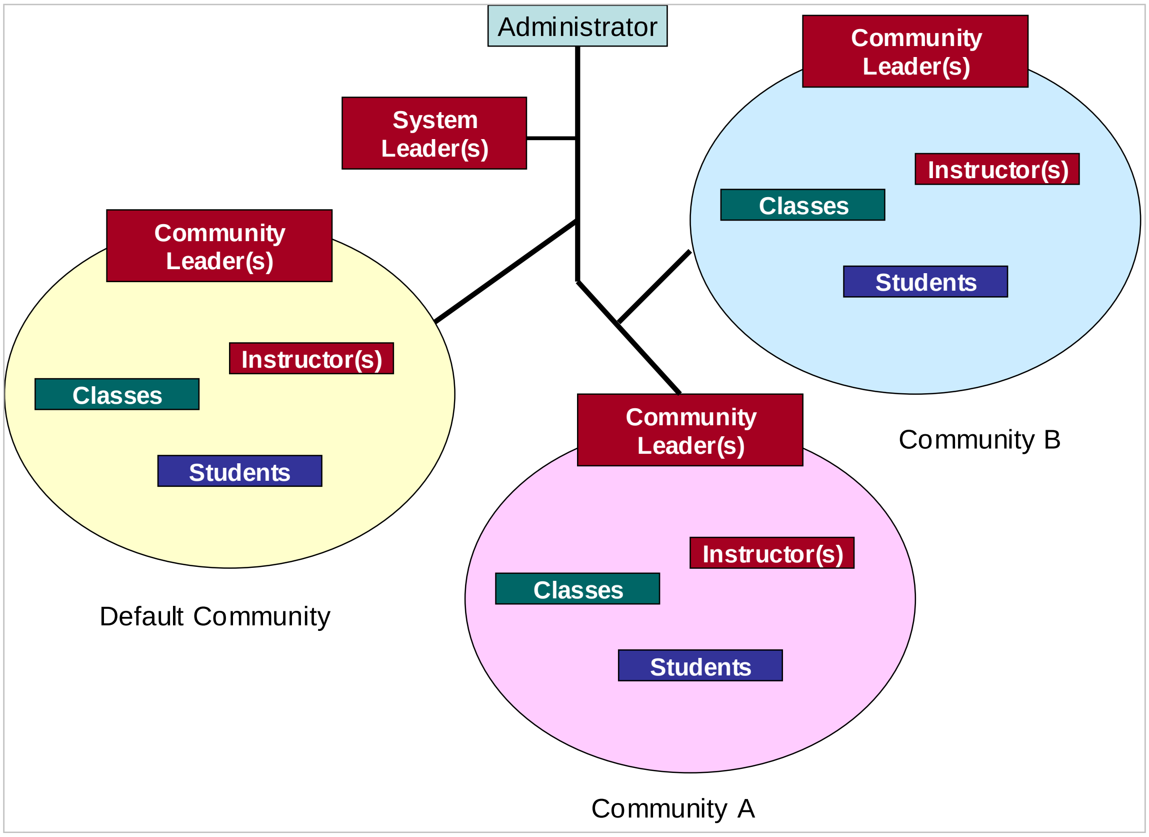
- Can create and manage student accounts in any community.
- Can create and manage instructor accounts in any community.
- Can manage classes in any community.
- Can attend all lab reservations in any community (except instructor personal reservations)
- Can cancel any lab reservation.

Please see the *NETLAB+ Administrator Guide* for detailed information on community management, account management, class management. These topics are introduced briefly in the sections below along with an example of using the lab scheduler.

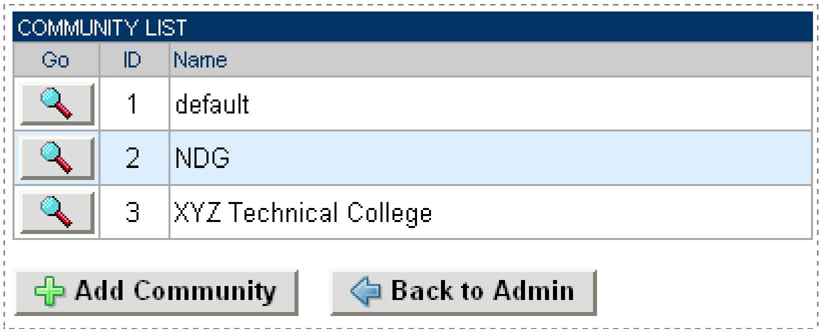
6.1 Add Communities

A *community* is a distinct group of instructors, students, and classes. Instructors may only manage students and classes within their own community (unless they are granted system-wide privileges by the administrator). Each community reflects a separate autonomous group using the NETLAB+ system. There is no sharing of accounts or class records between communities.

Multiple communities are optional. If the system is being used by a single Academy, the default community assignment should be used. Keep in mind that each instructor, student and class can belong to only one community. If you do not wish to use communities, place all accounts and classes in the default community.



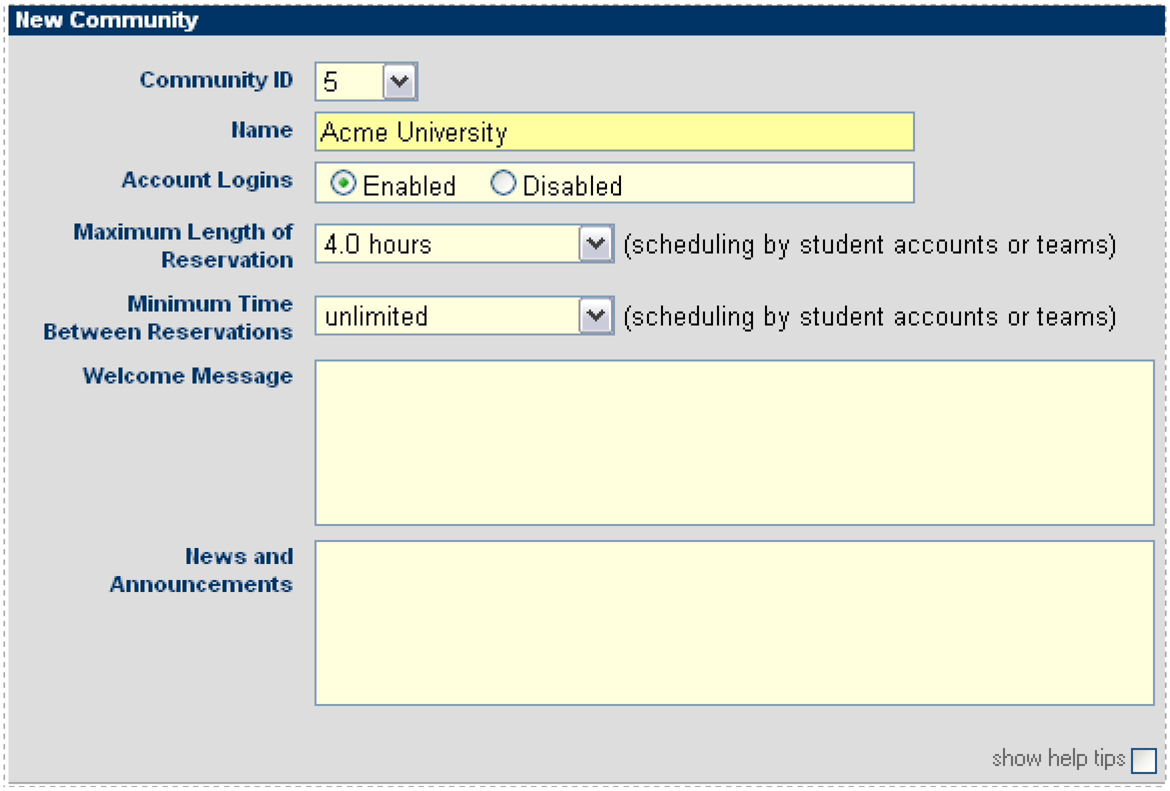
New communities are added using the Manage Communities administrator function.



COMMUNITY LIST

Go	ID	Name
🔍	1	default
🔍	2	NDG
🔍	3	XYZ Technical College

Select **Add Community** to display the Add Community page.



New Community

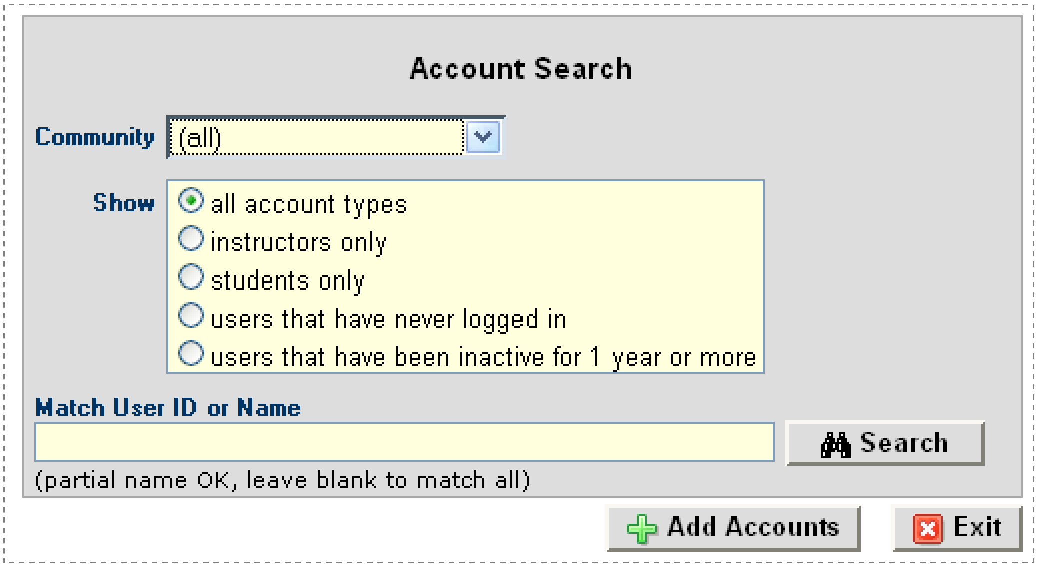
Community ID	5
Name	Acme University
Account Logins	● Enabled ○ Disabled
Maximum Length of Reservation	4.0 hours (scheduling by student accounts or teams)
Minimum Time Between Reservations	unlimited (scheduling by student accounts or teams)
Welcome Message	
News and Announcements	

For more information on communities, see the Manage Communities section of the *NETLAB+ Administrator Guide*.

6.2 Add Accounts

At least one instructor account must be setup by the NETLAB+ Administrator in order to access the scheduler for lab reservations. A student account should be created for each student to allow them to participate in labs as part of an instructor-led session, a team session, or an individual reservation.

Accounts are added to the NETLAB+ system by using the Manage Accounts function.



Account Search

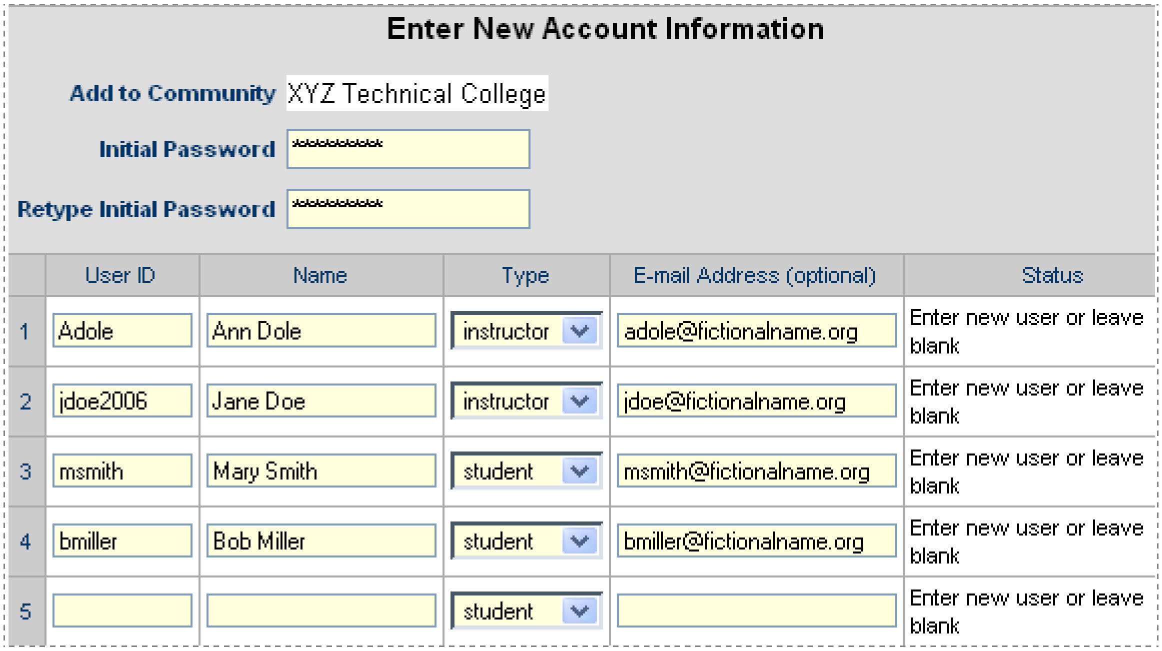
Community (all)

Show
● all account types
○ instructors only
○ students only
○ users that have never logged in
○ users that have been inactive for 1 year or more

Match User ID or Name

(partial name OK, leave blank to match all)

Select the Add Accounts button to display the New Accounts page.



Enter New Account Information

Add to Community XYZ Technical College

Initial Password **********

Retype Initial Password **********

	User ID	Name	Type	E-mail Address (optional)	Status
1	Adole	Ann Dole	instructor	adole@fictionalname.org	Enter new user or leave blank
2	jdoe2006	Jane Doe	instructor	jdoe@fictionalname.org	Enter new user or leave blank
3	msmith	Mary Smith	student	msmith@fictionalname.org	Enter new user or leave blank
4	bmiller	Bob Miller	student	bmiller@fictionalname.org	Enter new user or leave blank
5			student		Enter new user or leave blank

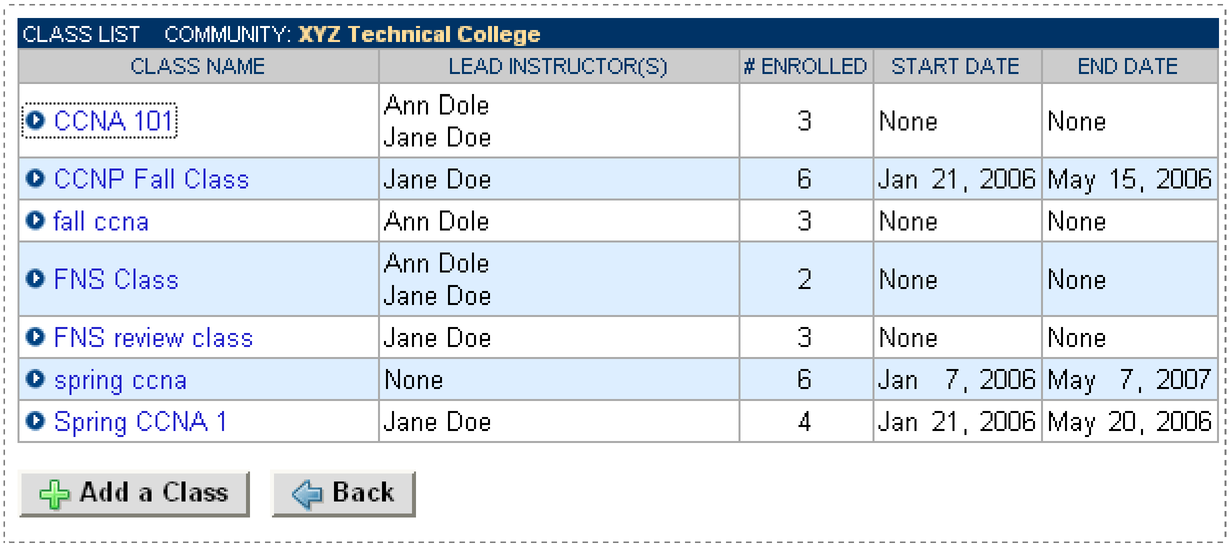
For more information on adding accounts, including a description of each field on the page, see the Manage Accounts section of the *NETLAB+ Administrator Guide*.

6.3 Add Classes

Information for each class using the system must be entered into the Class Manager. As the NETLAB+ administrator, you may manage classes for all the communities you have added to your NETLAB+ system.

Classes are added to the NETLAB+ system by using the Manage Classes function.

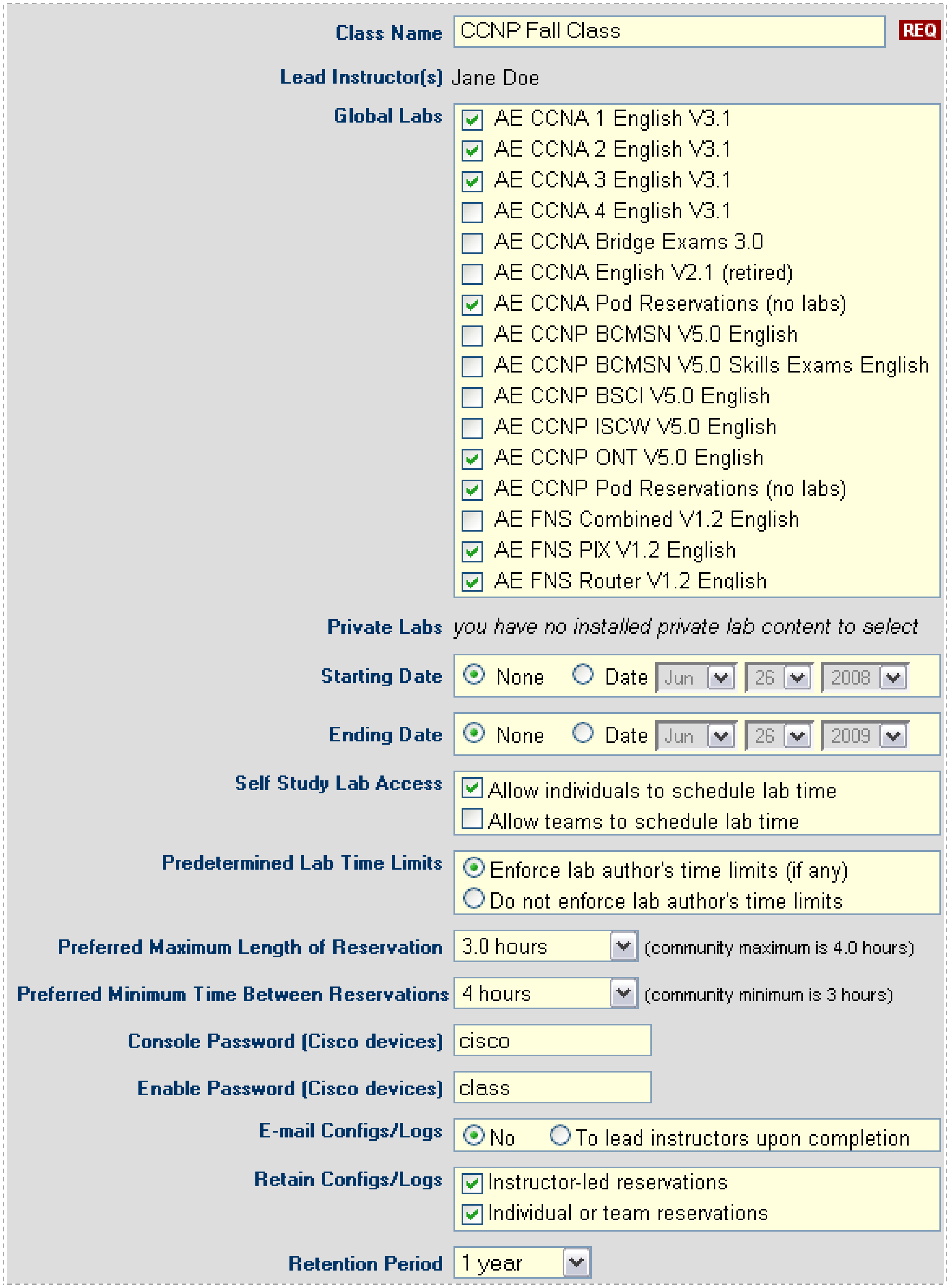
If there have been any classes previously entered into the system, they will be displayed.



CLASS LIST COMMUNITY: **XYZ Technical College**

CLASS NAME	LEAD INSTRUCTOR(S)	# ENROLLED	START DATE	END DATE
CCNA 101	Ann Dole Jane Doe	3	None	None
CCNP Fall Class	Jane Doe	6	Jan 21, 2006	May 15, 2006
fall ccna	Ann Dole	3	None	None
FNS Class	Ann Dole Jane Doe	2	None	None
FNS review class	Jane Doe	3	None	None
spring ccna	None	6	Jan 7, 2006	May 7, 2007
Spring CCNA 1	Jane Doe	4	Jan 21, 2006	May 20, 2006

To add a class to the system, select the **Add a Class** button at the bottom of the Class Manager page and enter the class information into the form.



Class Name	CCNP Fall Class REQ
Lead Instructor(s)	Jane Doe
Global Labs	☑ AE CCNA 1 English V3.1 ☑ AE CCNA 2 English V3.1 ☑ AE CCNA 3 English V3.1 ☐ AE CCNA 4 English V3.1 ☐ AE CCNA Bridge Exams 3.0 ☐ AE CCNA English V2.1 (retired) ☑ AE CCNA Pod Reservations (no labs) ☐ AE CCNP BCMSN V5.0 English ☐ AE CCNP BCMSN V5.0 Skills Exams English ☐ AE CCNP BSCI V5.0 English ☐ AE CCNP ISCW V5.0 English ☑ AE CCNP ONT V5.0 English ☑ AE CCNP Pod Reservations (no labs) ☐ AE FNS Combined V1.2 English ☑ AE FNS PIX V1.2 English ☑ AE FNS Router V1.2 English
Private Labs	*you have no installed private lab content to select*
Starting Date	● None ○ Date Jun 26 2008
Ending Date	● None ○ Date Jun 26 2009
Self Study Lab Access	☑ Allow individuals to schedule lab time ☐ Allow teams to schedule lab time
Predetermined Lab Time Limits	● Enforce lab author's time limits (if any) ○ Do not enforce lab author's time limits
Preferred Maximum Length of Reservation	3.0 hours (community maximum is 4.0 hours)
Preferred Minimum Time Between Reservations	4 hours (community minimum is 3 hours)
Console Password (Cisco devices)	cisco
Enable Password (Cisco devices)	class
E-mail Configs/Logs	● No ○ To lead instructors upon completion
Retain Configs/Logs	☑ Instructor-led reservations ☑ Individual or team reservations
Retention Period	1 year

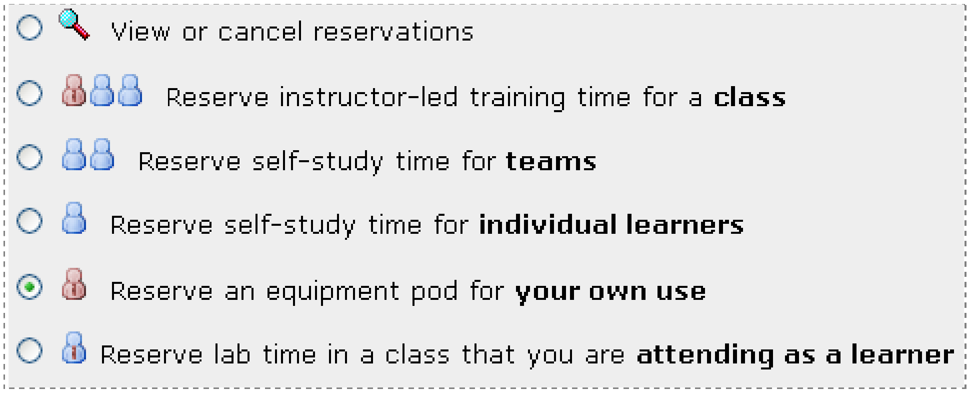
For more information on adding classes, including a description of each field on the page, refer to the Class Management section of the *NETLAB+ Administrator Guide*.

6.4 Schedule a Lab Reservation

The NETLAB+ Lab Scheduler may be accessed using an instructor account or a student account (if enrolled in a class where individual or team lab reservations have been enabled). Log in to the NETLAB+ system using an instructor account (see section 6.2 and the *NETLAB+ Instructor Guide*).

To schedule a lab reservation, select **Scheduler** from the menu bar or the link on the body of the MyNETLAB page.

The Scheduler Options screen will be displayed. Detailed descriptions of the scheduler options are available by selecting Help on the menu bar. Try out the scheduler by reserving an equipment pod for your own use. To reserve an equipment pod for your own use, select the scheduling option shown below and then click the **OK** button**.**



○ View or cancel reservations

○ Reserve instructor-led training time for a **class**

○ Reserve self-study time for **teams**

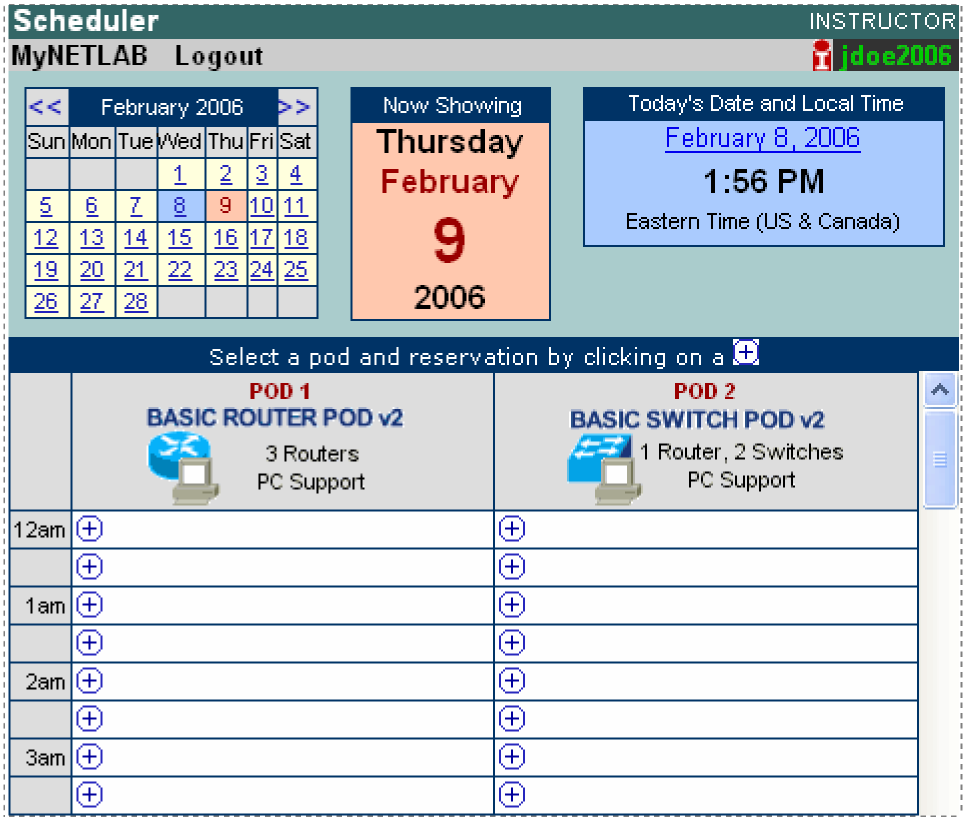
○ Reserve self-study time for **individual learners**

● Reserve an equipment pod for **your own use**

○ Reserve lab time in a class that you are **attending as a learner**

The reservation calendar will be displayed, where a reservation time may be selected. Use the calendar in the upper left corner of the screen to select the date for the reservation by clicking on the date of your choice. You may scroll from month to month by selecting the < and > symbols.

The number of pods available for you to select from will depend upon the number of pods that have been installed on your NETLAB+ server. If more than one community uses your NETLAB+ server, you will be limited to selecting within the timeframes designated for your community. Please see the Pod Rules section of the *NETLAB+ Administrator Guide* for more information.



<<	February 2006					>>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28				

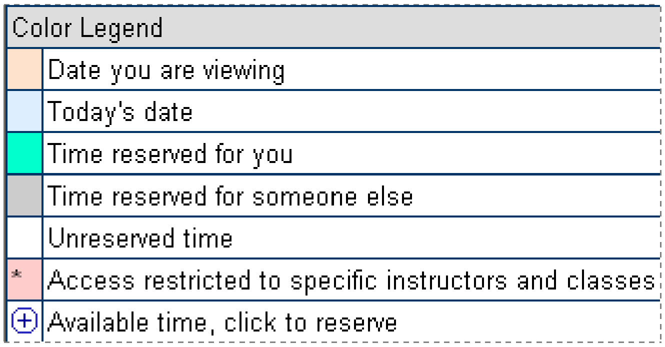
Now Showing
Thursday
February
9
2006

Today's Date and Local Time
February 8, 2006
1:56 PM
Eastern Time (US & Canada)

Select a pod and reservation by clicking on a ⊕

	POD 1 BASIC ROUTER POD v2 3 Routers PC Support	POD 2 BASIC SWITCH POD v2 1 Router, 2 Switches PC Support
12am	⊕	⊕
	⊕	⊕
1am	⊕	⊕
	⊕	⊕
2am	⊕	⊕
	⊕	⊕
3am	⊕	⊕
	⊕	⊕

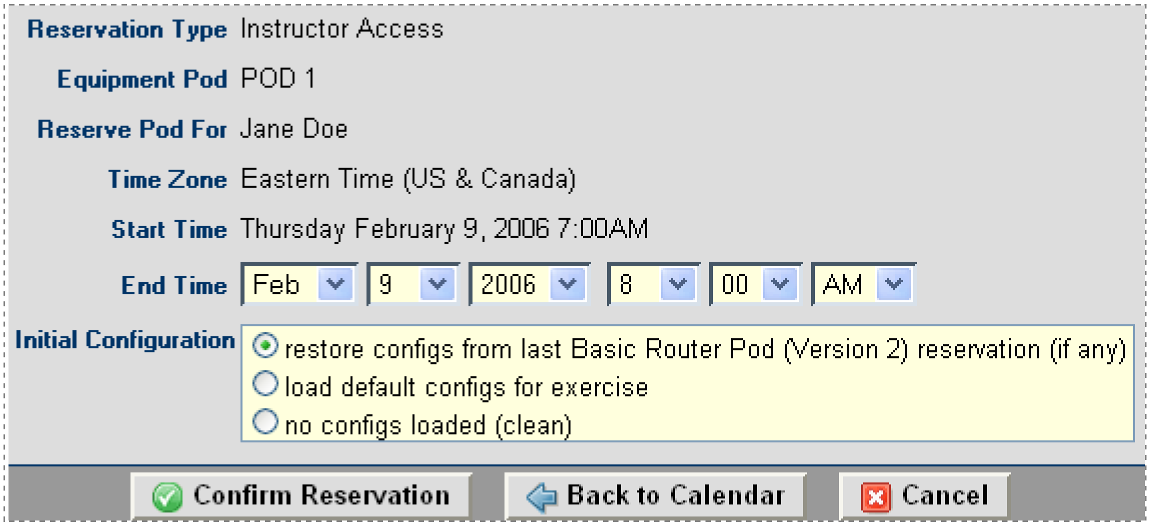
To select the reservation time, scroll the page up and down as needed to display available reservation times. Available times are indicated with an ⊕ symbol. Scrolling to the bottom of the page will display the color legend, designed to make the calendar easy to understand.



Color Legend	
🟧	Date you are viewing
🟦	Today's date
🟩	Time reserved for you
▨	Time reserved for someone else
□	Unreserved time
*	Access restricted to specific instructors and classes
⊕	Available time, click to reserve

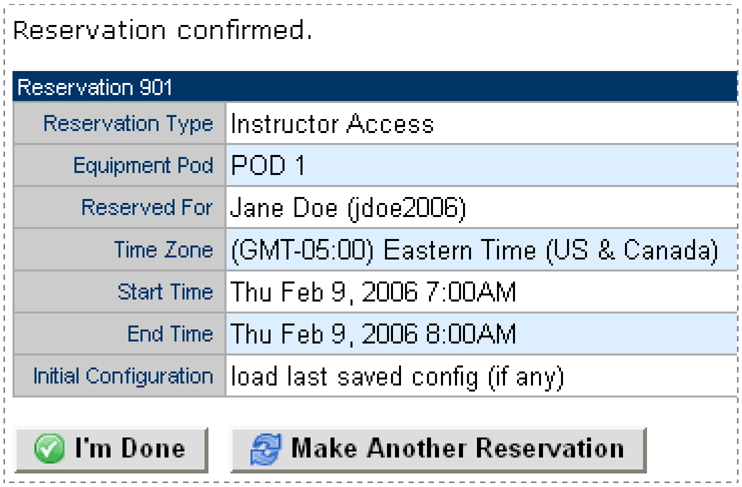
Once a lab reservation time has been selected by selecting an available time ⊕, the confirmation page will be displayed.

Select the appropriate option for initial configuration of the pod equipment. The restore last configuration option will try to restore the lab to the state it was in at the end of the last attended reservation. NETLAB+ maintains a different .LAST_SAVED configuration folder for each type of reservation (classroom, student, team, and instructor).



Reservation Type	Instructor Access
Equipment Pod	POD 1
Reserve Pod For	Jane Doe
Time Zone	Eastern Time (US & Canada)
Start Time	Thursday February 9, 2006 7:00AM
End Time	Feb 9 2006 8 00 AM
Initial Configuration	● restore configs from last Basic Router Pod (Version 2) reservation (if any) ○ load default configs for exercise ○ no configs loaded (clean)

After confirming, a message will be displayed and you may make additional reservations, or select **Done** to return to the MyNETLAB page.



Reservation confirmed.

Reservation 901	
Reservation Type	Instructor Access
Equipment Pod	POD 1
Reserved For	Jane Doe (jdoe2006)
Time Zone	(GMT-05:00) Eastern Time (US & Canada)
Start Time	Thu Feb 9, 2006 7:00AM
End Time	Thu Feb 9, 2006 8:00AM
Initial Configuration	load last saved config (if any)

The reservation for this lab reservation will now be displayed on the instructor's MyNETLAB page. For more information on scheduling reservations, see the Schedule Lab Reservations section of the *NETLAB+ Instructor Guide*.

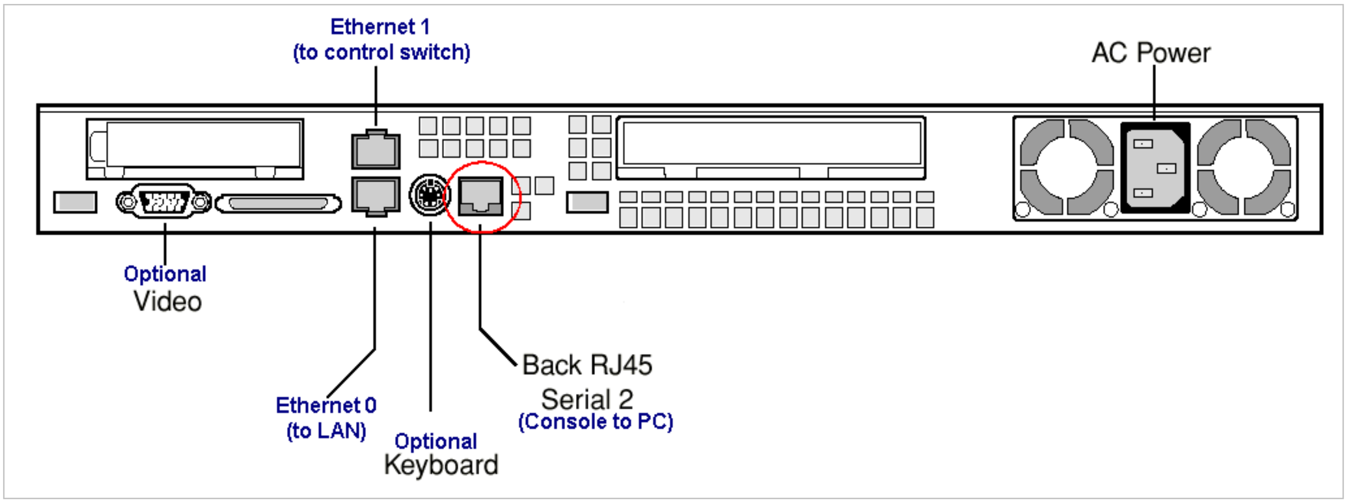
Appendix A Sun LX50

Appendix A.1 Rack Mounting

The Sun LX50 can be mounted in a front-only, front and rear or mid-mount configuration. The instructions for each style are included in a large, fold out diagram in the server box. It is very important that you read and follow these directions carefully, as the server is large and bulky and should be securely affixed to the rack. The chassis handles should be replaced, and the front cover reattached to prevent accidental access to the power switch.

Appendix A.2 Console Connection

The Sun LX50 rear RJ45 port is used to connect a PC using a standard console cable like those used to access Cisco routers. This console connection allows the Administrator to access the **NETLAB+ System Console** menu system to perform IP configuration.
Connect the console cable to the server port indicated. The other end of the console cable should be connected to the PC serial communications port. If your PC has multiple com ports, be sure to choose the correct port in your Hyper Terminal Port Settings.

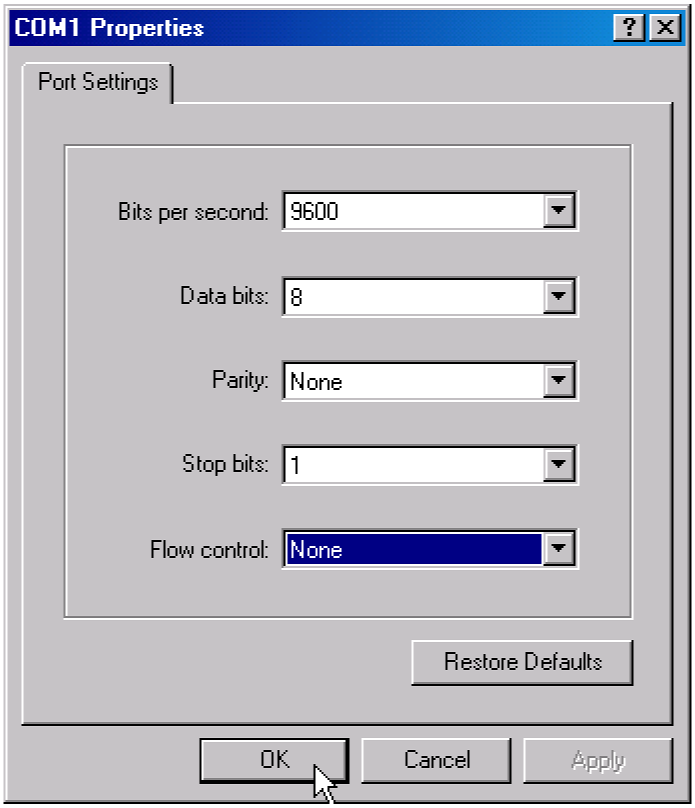


Appendix A.3 Hyper Terminal Settings

The HyperTerminal program on the PC should be configured for the correct serial port for the following settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

Press the “Enter” key to view the login screen. Please note that the initial login prompt may be delayed as much as 1 minute.



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

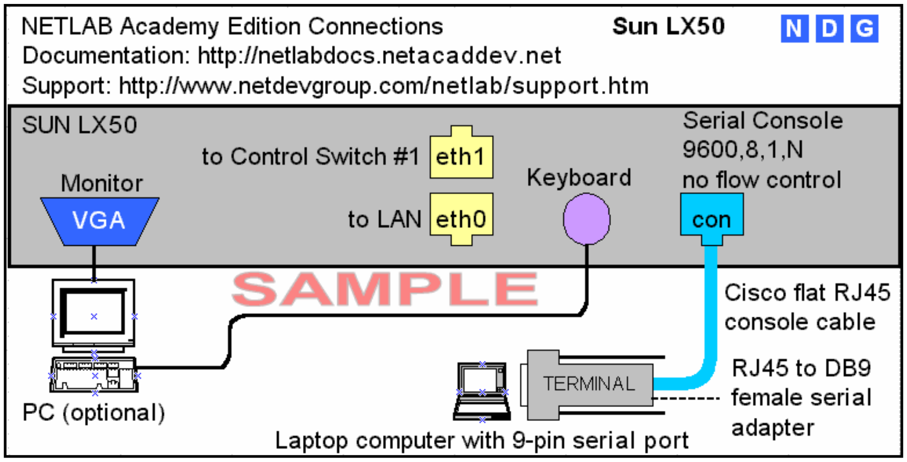
Parity: None

Stop bits: 1

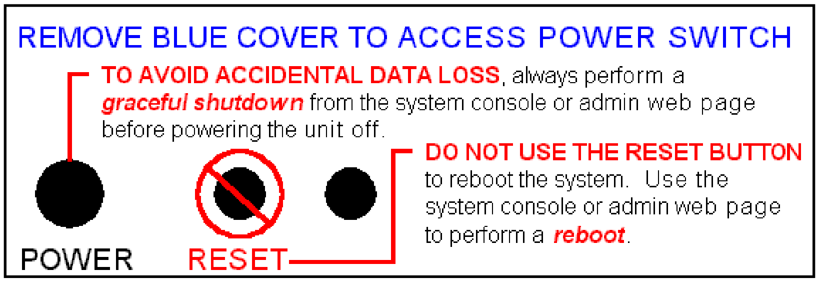
Flow control: None

Appendix A.4 Labels

A printed label attached to the top of the server case can be used to identify the ports and connections for this server.



An additional label identifies the power and reset buttons located under the front cover.


REMOVE BLUE COVER TO ACCESS POWER SWITCH
TO AVOID ACCIDENTAL DATA LOSS, always perform a
graceful shutdown from the system console or admin web page
before powering the unit off.
DO NOT USE THE RESET BUTTON
to reboot the system. Use the
system console or admin web page
to perform a reboot.
POWER
RESET

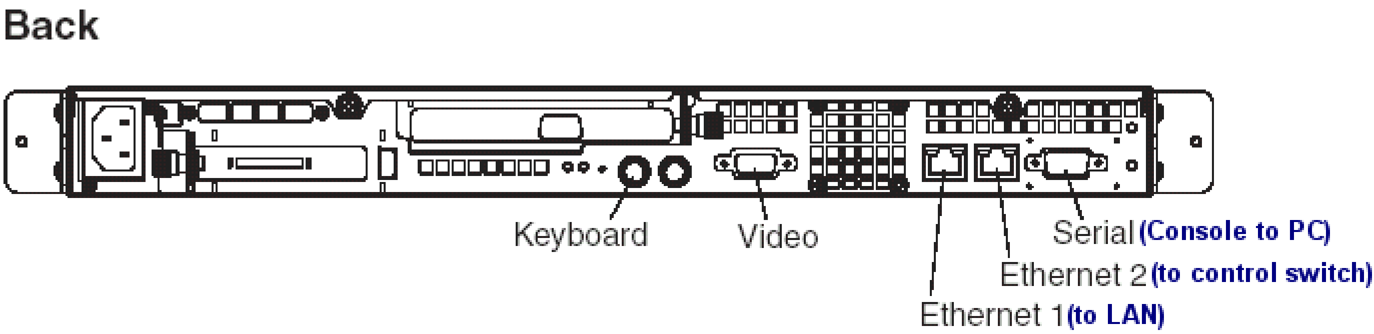
Appendix B IBM xSeries 305

Appendix B.1 Rack Mounting

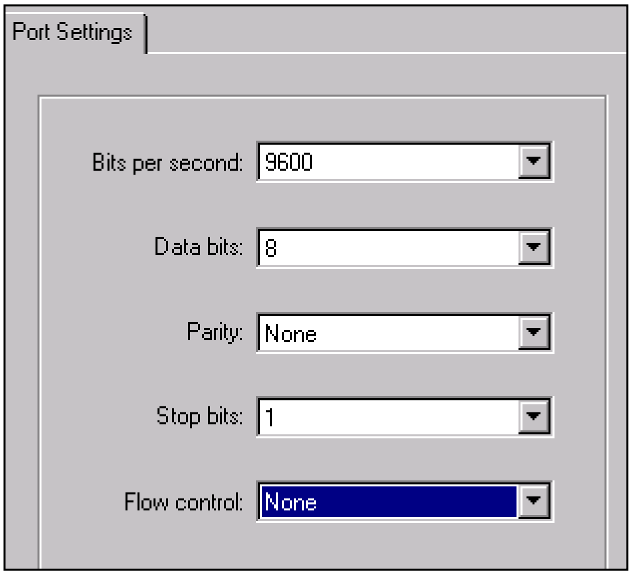
The IBM x305 *Rack Installation Instructions* are included with the documentation that shipped with the server. This printed publication contains the instructions to install your server in a rack. It is very important that you read and follow these directions carefully.

Appendix B.2 Console Connection

The IBM x305 rear serial-port connector is used to connect a PC using a standard serial cable. This console connection allows the Administrator to access the NETLAB+ System Console menu system to perform IP configuration.
Connect the serial cable to the server port indicated. The other end of the serial cable should be connected to the PC serial communications port. If your PC has multiple com ports, be sure to choose the correct port in your Hyper Terminal Port Settings.



Appendix B.3 Hyper Terminal Settings



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

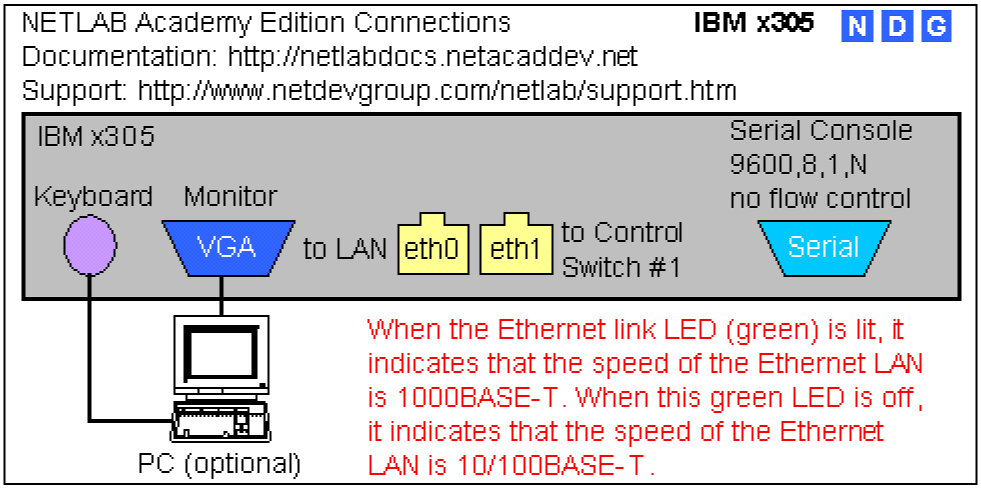
The HyperTerminal program on the PC should be configured for the correct serial port for the following settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

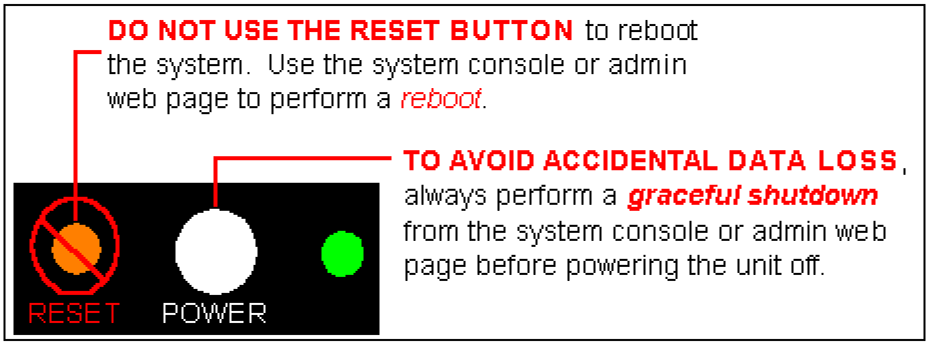
Press the “Enter” key to view the login screen. Please note that the initial login prompt may be delayed as much as 1 minute.

Appendix B.4 Labels

A printed label attached to the top of the server case (rear view) can be used to identify the ports and connections for this server.


NETLAB Academy Edition Connections
IBM x305
N D G
Documentation: http://netlabdocs.netacaddev.net
Support: http://www.netdevgroup.com/netlab/support.htm
IBM x305
Keyboard
Monitor
VGA
to LAN
eth0
eth1
to Control Switch #1
Serial Console 9600,8,1,N no flow control
Serial
PC (optional)
When the Ethernet link LED (green) is lit, it indicates that the speed of the Ethernet LAN is 1000BASE-T. When this green LED is off, it indicates that the speed of the Ethernet LAN is 10/100BASE-T.

An additional label identifies the power and reset buttons located on the front cover.


DO NOT USE THE RESET BUTTON to reboot the system. Use the system console or admin web page to perform a reboot.
TO AVOID ACCIDENTAL DATA LOSS, always perform a graceful shutdown from the system console or admin web page before powering the unit off.
RESET
POWER

Appendix C IBM xSeries 306

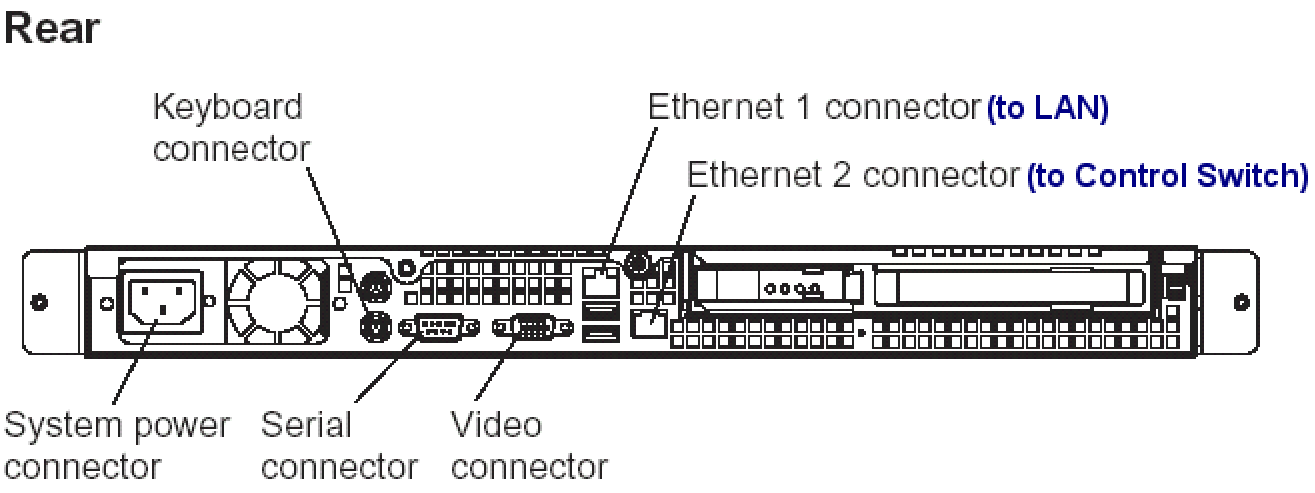
Appendix C.1 Rack Mounting

The IBM x306 *Rack Installation Instructions* are included with the documentation that shipped with the server. This printed publication contains the instructions to install your server in a rack. It is very important that you read and follow these directions carefully.

Appendix C.2 Console Connection

The IBM x306 rear serial-port connector is used to connect a PC using a standard serial cable. This console connection allows the Administrator to access the NETLAB+ System Console menu system to perform IP configuration.

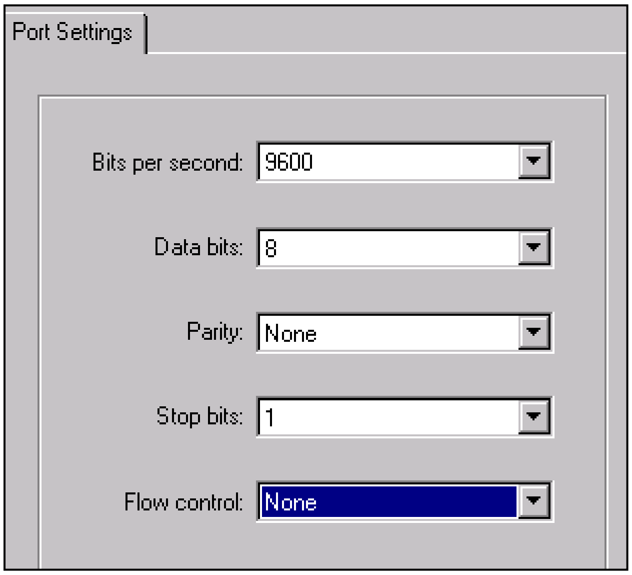
Connect the serial cable to the server port indicated (serial connector port). The other end of the serial cable should be connected to the PC serial communications port. If your PC has multiple com ports, be sure to choose the correct port in your Hyper Terminal Port Settings.



Appendix C.3 Hyper Terminal Settings

The HyperTerminal program on the PC should be configured for the correct serial port for the following settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None



Bits per second: 9600

Data bits: 8

Parity: None

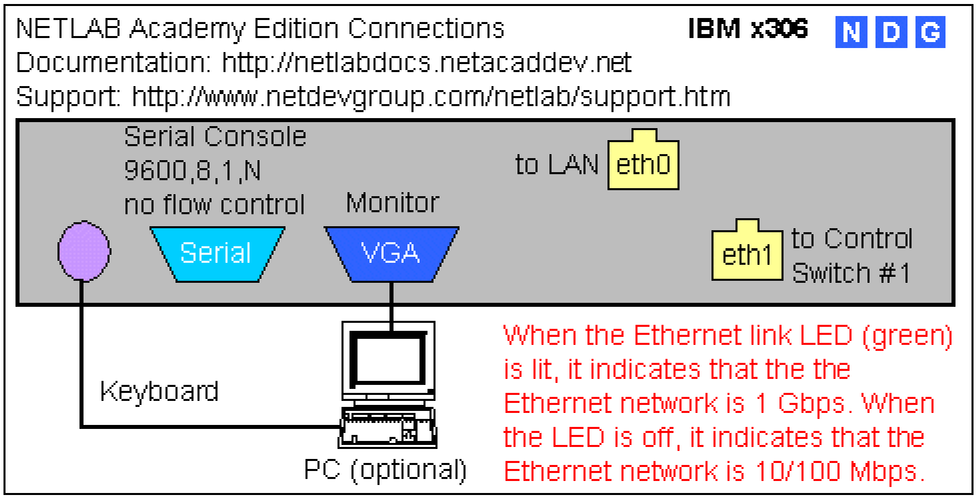
Stop bits: 1

Flow control: None

Press the “Enter” key to view the login screen. Please note that the initial login prompt may be delayed as much as 1 minute.

Appendix C.4 Labels

A printed label attached to the top of the server case (rear view) can be used to identify the ports and connections for this server.


NETLAB Academy Edition Connections

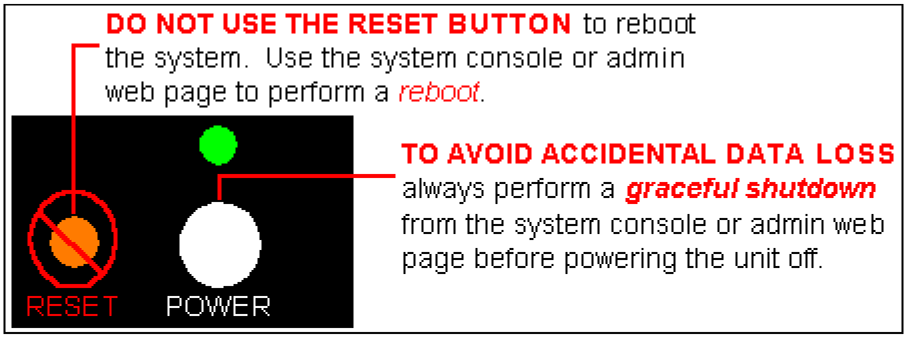
IBM x306

Documentation: http://netlabdocs.netacaddev.net

Support: http://www.netdevgroup.com/netlab/support.htm

When the Ethernet link LED (green) is lit, it indicates that the the Ethernet network is 1 Gbps. When the LED is off, it indicates that the Ethernet network is 10/100 Mbps.

An additional label identifies the power and reset buttons located on the front cover.



DO NOT USE THE RESET BUTTON to reboot the system. Use the system console or admin web page to perform a *reboot*.

TO AVOID ACCIDENTAL DATA LOSS always perform a ***graceful shutdown*** from the system console or admin web page before powering the unit off.