INSTALLATION AND CONFIGURATION GUIDE

Multi-Purpose Academy Pod with ASA

Document Version: 2015-12-08

For Cisco Networking Academy® courses, including:

CCNA ROUTING AND SWITCHING
CCNA SECURITY
CCNP ROUTING AND SWITCHING
Multi-Purpose Academy Pod with ASA Installation and Configuration Guide

1 Introduction ............................................................................................................. 3
1.1 Deviations ............................................................................................................ 4
1.2 Remote PC Support .............................................................................................. 4
1.3 Dynamic Topologies ........................................................................................... 4
2 Lab Device Requirements ..................................................................................... 5
2.1 Lab Device Requirements for CCNPv7 ................................................................ 5
2.2 Lab Device Requirements for CCNA Security v2.0 ............................................ 7
   2.2.1 Required software for CCNA Security v2.0 ............................................... 8
   2.2.2 Cisco Adaptive Security Appliance (ASA) for CCNA Security v2.0 ....... 9
2.3 Lab Device Requirements for CCNA Routing and Switching, Security v1.2 ..... 10
   2.3.1 Required software for CCNA Security v1.2 ............................................. 11
   2.3.2 Cisco Adaptive Security Appliance (ASA) for CCNA Security v1.2 ...... 13
2.4 PCs and Servers .................................................................................................. 13
3 Control Device Requirements ............................................................................... 14
3.1 Control Switch Overview .................................................................................... 14
3.2 Access Server Ports ............................................................................................ 16
3.3 Switched Outlets ................................................................................................. 16
4 Pre-requisites ........................................................................................................ 17
4.1 Understanding VMware Virtualization and Virtual Machines ......................... 17
4.2 Setup Control Devices ....................................................................................... 17
4.3 Upload IOS Images ............................................................................................. 17
4.4 Disable User Logins (optional) ........................................................................... 17
5 Adding the Pod ....................................................................................................... 18
5.1 Start the New Pod Wizard .................................................................................. 18
5.2 Add a Multi-Purpose Academy Pod with ASA .................................................. 18
5.3 Select Control Switch and Ports ......................................................................... 18
5.4 Select Access Server(s) and Ports ...................................................................... 19
5.5 Select Switched Outlets ..................................................................................... 22
5.6 Select Device Types ........................................................................................... 23
5.7 Select Software Images and Recovery Options .................................................. 23
5.8 Select a Pod ID .................................................................................................... 25
5.9 Select a Pod Name ............................................................................................... 25
5.10 Verify Your Settings ......................................................................................... 25
6 Cable the Pod ......................................................................................................... 27
7 Switch Configuration Tasks .................................................................................... 30
   7.1 Verify Control Switch IOS Version ................................................................... 30
   7.2 Configure Control Switch Ports ......................................................................... 30
   7.3 Initial Lab Switch Setup ..................................................................................... 33
8 Testing the Pod (Test 1 – Before PC Implementation) ........................................... 35
9 Select PC Type ....................................................................................................... 36
10 VMware Settings .................................................................................................. 37
11 Testing the Pod (Test 2 – After PC Implementation) ........................................... 38
12 Finishing Up ........................................................................................................... 40
   12.1 Bring the Pod(s) Back Online .......................................................................... 40
   12.2 Enable Multi-Purpose Academy Pod with ASA Exercises .......................... 41
   12.3 Schedule a Lab Reservation for Your New Pod ............................................ 42
PART 1 – PLANNING

1 Introduction

The NETLAB+ Multi-Purpose Academy Pod with ASA is a versatile pod, which includes 3 routers, 3 switches, and an ASA. This pod is designed to be compatible with Basic Router Pod Version 2 and the LAN Switching Pod; therefore, it supports many CCNA Discovery and Exploration Labs. The Multi-Purpose Academy Pod with ASA also supports CCNA Security Labs (including ASA labs) and CCNPv6.0 TSHOOT, ROUTE and SWITCH labs.

The Multi-Purpose Academy Pod with ASA features direct access to router, switch and ASA consoles. Integration with a separate VMware server supports up to 3 virtual PCs. NETLAB+ can provide remote access to the keyboard, video, and mouse of the VMware virtual machines in the pod.

NETLAB+ users in a team or instructor-led class can share access to a device console or PC.
1.1 Deviations

Remote users may get confused by local deviations from the standard curriculum and labs. The curriculum is relatively complex and offers many opportunities to “make adjustments to the labs”. If your NETLAB+ pods will be made accessible outside your local Academy, you should carefully consider the impact of deviations and substitutions.

Even if your user community is local or relatively small, we recommend that you (1) document the specifics of your pods and (2) use the NETLAB+ News and Announcements feature to point users to your documentation.

1.2 Remote PC Support

A Multi-Purpose Academy Pod with ASA supports up to 3 remote PCs implemented using VMware. NETLAB+ allows several settings for each:

- Users can control the keyboard, video, and mouse.
- Users can power on, shutdown, reboot, and revert to a clean state.
- Users can have administrator rights.

The [NETLAB+ Remote PC Guide Series](http://www.netdevgroup.com/support/remote_pc.html) provides detailed, version-specific information on the implementation of VMware products and virtual machines.

To learn more about VMware virtualization products, please visit:
http://www.netdevgroup.com/support/remote_pc.html

1.3 Dynamic Topologies

The Multi-Purpose Academy Pod with ASA features dynamic topologies. NETLAB+ can alter the topology and reposition PCs by manipulating VLANs on the control switch. This is done automatically based on the selected lab exercise. Instructors can change exercises and topologies during instructor led class reservations.
2 Lab Device Requirements

Lab devices are part of the topology and users can interact with them either directly or indirectly. The lab device requirements vary for the Multi-purpose Academy Pod with ASA, depending on the courses you plan to teach.

Please also refer to the NDG website for the latest information: 
https://www.netdevgroup.com/content/cnap/topologies/multipurpose_academy_pod_asa.html

- If you plan to use your Multi-purpose Academy Pod with ASA for the CCNPv7.0 TSHOOT, ROUTE and SWITCH courses, please refer to the lab device requirements in Section 2.1.

- If you plan to use your Multi-purpose Academy Pod with ASA to teach CCNA Security v2.0, you may follow the requirements in Section 2.2 below.

- If you plan to use your Multi-purpose Academy Pod with ASA to teach CCNA Security v1.2 and/or CCNA Routing and Switching, you may follow the requirements in Section 2.3 below.

Other equipment may work if it is supported by NETLAB+ and can meet the minimum requirements for feature sets, interfaces, IOS, RAM, and Flash. A list of NETLAB+ supported lab equipment can be found on the NDG website. Please note, compatibility with NETLAB+ does not guarantee compatibility with the Academy labs.

2.1 Lab Device Requirements for CCNPv7

Details on requirements are provided on the lab pages for each course:

TSHOOT: http://www.netdevgroup.com/content/cnap/labs/ccnp_v7_tshoot.html
ROUTE: http://www.netdevgroup.com/content/cnap/labs/ccnp_v7_route.html
SWITCH: http://www.netdevgroup.com/content/cnap/labs/ccnp_v7_switch.html

Only two (2) SWITCH labs are supported using the MAPASA.

<table>
<thead>
<tr>
<th>Router / Switch</th>
<th>Recommended Model(s)</th>
<th>Minimum DRAM</th>
<th>Minimum Flash</th>
<th>Minimum IOS</th>
<th>Feature Set/Technology Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Cisco 1941</td>
<td>256 MB</td>
<td>256 MB</td>
<td>15.4(3)</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>Router / Switch</td>
<td>Recommended Model(s)</td>
<td>Minimum DRAM</td>
<td>Minimum Flash</td>
<td>Minimum IOS</td>
<td>Feature Set/Technology Packages</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>-------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>R2</td>
<td>Cisco 1941</td>
<td>256 MB</td>
<td>256 MB</td>
<td>15.4(3)</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>R3</td>
<td>Cisco 1941</td>
<td>256 MB</td>
<td>256 MB</td>
<td>15.4(3)</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>S1</td>
<td>Cisco 3650&lt;sup&gt;1,2&lt;/sup&gt;</td>
<td>4096 MB</td>
<td>2048 MB</td>
<td>3.3.5 SE</td>
<td>Universal</td>
</tr>
<tr>
<td>S2</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>15.0(2)SE7</td>
<td>LAN Base</td>
</tr>
<tr>
<td>S3</td>
<td>Cisco 3650&lt;sup&gt;1,2&lt;/sup&gt;</td>
<td>4096 MB</td>
<td>2048 MB</td>
<td>3.3.5 SE</td>
<td>Universal</td>
</tr>
</tbody>
</table>

<sup>1</sup> Requires minimum NETLAB+ version 2015.R2.beta.5.

<sup>2</sup> CCNA Routing and Switching and CCNA Security v2.0 have not been tested with the Cisco 3650 switch.

The global command **boot enable-break** must be enabled on all switches for proper operation. Please refer to Section 7.
## 2.2 Lab Device Requirements for CCNA Security v2.0

<table>
<thead>
<tr>
<th>Router / Switch</th>
<th>Recommended Model(s)</th>
<th>Minimum DRAM</th>
<th>Minimum Flash</th>
<th>Minimum IOS</th>
<th>Feature Set/Technology Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>CISCO1941</td>
<td>512 MB</td>
<td>256 MB</td>
<td>15.4(3)M2</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>R2</td>
<td>CISCO1941</td>
<td>512 MB</td>
<td>256 MB</td>
<td>15.4(3)M2</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>R3</td>
<td>CISCO1941</td>
<td>512 MB</td>
<td>256 MB</td>
<td>15.4(3)M2</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>S1</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>15.0(2)SE7</td>
<td>LAN Base</td>
</tr>
<tr>
<td>S2</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>15.0(2)SE7</td>
<td>LAN Base</td>
</tr>
<tr>
<td>S3</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>15.0(2)SE7</td>
<td>LAN Base</td>
</tr>
</tbody>
</table>

The global command **boot enable-break** must be enabled on all switches for proper operation. Please refer to Section 7.
### 2.2.1 Required software for CCNA Security v2.0

<table>
<thead>
<tr>
<th>Software Name</th>
<th>Purpose</th>
<th>Requirements</th>
<th>Comments / Links</th>
</tr>
</thead>
</table>
| AnyConnect Secure Mobility Client release 4.1.00028 | Installed on the ASA 5505. | Supported Microsoft Windows O/S:  
  - Windows 7  
  - Windows 8.1 | |
| Kiwi Syslog | This software will be used as the syslog server. Tftpd32 can also be used as the syslog server. | Supported O/S:  
  - Windows XP or Higher | [www.kiwisyslog.com](http://www.kiwisyslog.com) |
| WinRadius | WinRadius is a standard RADIUS server for network authentication and accounting. | Windows/Linux | [sourceforge.net/projects/winradius/](http://sourceforge.net/projects/winradius/) |
| NMAP/ZENMAP | This software is used to test the lab configuration. | Windows/Linux | [www.insecure.org](http://www.insecure.org) |
| TFTP32 | DHCP, TFTP, SMTP, Syslog servers, and TFTP client. |  | [http://tftpd32.jounin.net/tftpd32_download.html](http://tftpd32.jounin.net/tftpd32_download.html) |
| IOS-S855-CLI.pkg | This file is used with Lab 5.4.1.1. |  | To obtain instructions on the file version and how to download, please see Lab 5.4.1.1. |
| realm-cisco.pub.key | This file is used with Lab 5.4.1.1. |  | To obtain instructions on the file version and how to download, please see Lab 5.4.1.1. |
### 2.2.2 Cisco Adaptive Security Appliance (ASA) for CCNA Security v2.0

A Multi-Purpose Academy Pod with ASA adds the additional functionality of a Cisco Adaptive Security Appliance (ASA) to complete the CCNA Security v2.0 labs.

<table>
<thead>
<tr>
<th>Device</th>
<th>Recommended Model(s)</th>
<th>Minimum DRAM</th>
<th>Minimum Flash</th>
<th>Minimum IOS Feature Set</th>
</tr>
</thead>
</table>
### 2.3 Lab Device Requirements for CCNA Routing and Switching, Security v1.2

<table>
<thead>
<tr>
<th>Router / Switch</th>
<th>Recommended Model(s)</th>
<th>Minimum DRAM</th>
<th>Minimum Flash</th>
<th>Minimum IOS</th>
<th>Feature Set/Technology Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Cisco 1941</td>
<td>512 MB</td>
<td>256 MB</td>
<td>15.3(3)M2</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>R2</td>
<td>Cisco 1941</td>
<td>512 MB</td>
<td>256 MB</td>
<td>15.3(3)M2</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>R3</td>
<td>Cisco 1941</td>
<td>512 MB</td>
<td>256 MB</td>
<td>15.3(3)M2</td>
<td>IP Base, Security</td>
</tr>
<tr>
<td>S1</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>150-2.EZ.bin</td>
<td>LAN Base</td>
</tr>
<tr>
<td>S2</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>150-2.EZ.bin</td>
<td>LAN Base</td>
</tr>
<tr>
<td>S3</td>
<td>WS-C2960+24TC-L</td>
<td>128 MB</td>
<td>64 MB</td>
<td>150-2.EZ.bin</td>
<td>LAN Base</td>
</tr>
</tbody>
</table>

1 Other router and switch models may be used. Please consult your Cisco NetAcad support contact for more information.

2 DRAM memory requirements when used to support the CCNA Security course.

The global command **boot enable-break** must be enabled on all switches for proper operation. Please refer to Section 7.
### 2.3.1 Required software for CCNA Security v1.2

<table>
<thead>
<tr>
<th>Software Name</th>
<th>Purpose</th>
<th>Requirements</th>
<th>Comments / Links</th>
</tr>
</thead>
</table>
| **Cisco Configuration Professional (CCP) V2.5** | CCP is installed in the PCs. | Supported Microsoft Windows O/S:  
  - Windows 7  
  Minimum 1GB of RAM for all OSs (2GB recommended). | When using CCP:  
  - The web browser needs Sun JRE 1.5.0_11 up to 1.6.0_16 and Adobe Flash Player Version 10.0.12.36 and later.  
  - The recommended screen size for the virtual PCs is 1024 x 768.  
  - See lab 0.0.0.0 in the CCNA Security V1.2 Instructor's Lab Manual for more information. |
| **Kiwi Syslog**                        | This software will be used as the syslog server. Tftpd32 can also be used as the syslog server. | Supported O/S:  
  - Windows XP or Higher | Known working platform:  
  - Windows 7 Professional, SP1  
  - 2GB of RAM  
  - Java 7 Update 67 - 7.0.670  
  - Adobe Flash Player 11.9.900.117 |
<p>| <strong>Wireshark</strong>                         | This software will be used as the sniffer and packet analyzer. | Windows/Linux | <a href="http://www.wireshark.org">www.wireshark.org</a> |
| <strong>WinRadius</strong>                         | WinRadius is a standard RADIUS server for network authentication and accounting. | Windows/Linux | <a href="http://sourceforge.net/projects/winradius/">sourceforge.net/projects/winradius/</a> |
| <strong>NMAP/ZENMAP</strong>                      | This software is used to test the lab configuration. | Windows/Linux | <a href="http://www.insecure.org">www.insecure.org</a> |
| <strong>Cisco VPN Client</strong>                  | This software is used to | | <a href="http://www.cisco.com">www.cisco.com</a> |</p>
<table>
<thead>
<tr>
<th>Software Name</th>
<th>Purpose</th>
<th>Requirements</th>
<th>Comments / Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tera Term Pro V2.3</td>
<td>Software terminal emulator for Windows.</td>
<td></td>
<td><a href="http://www.ayera.com/teraterm/">www.ayera.com/teraterm/</a></td>
</tr>
<tr>
<td>TFTP32</td>
<td>DHCP, TFTP, SMTP, Syslog servers, and TFTP client.</td>
<td></td>
<td><a href="http://tftpd32.jounin.net/tftpd32_download.html">http://tftpd32.jounin.net/tftpd32_download.html</a></td>
</tr>
<tr>
<td>IOS-Sxxx-CLI.pkg</td>
<td>This file is used with Lab 5.5.1.1.</td>
<td></td>
<td>To obtain instructions on the file version and how to download, please see Lab 5.5.1.1.</td>
</tr>
<tr>
<td>realm-cisco.pub.key.txt</td>
<td>This file is used with Lab 5.5.1.1.</td>
<td></td>
<td>To obtain instructions on the file version and how to download, please see Lab 5.5.1.1.</td>
</tr>
<tr>
<td>PuTTY SSH Client</td>
<td>Used as an SSH Client</td>
<td>Windows/Linux</td>
<td><a href="http://www.chiark.greenend.org.uk/~sgtatham/putty/">www.chiark.greenend.org.uk/~sgtatham/putty/</a></td>
</tr>
</tbody>
</table>
### 2.3.2 Cisco Adaptive Security Appliance (ASA) for CCNA Security v1.2

A Multi-Purpose Academy Pod with ASA adds the additional functionality of a Cisco Adaptive Security Appliance (ASA) to complete the CCNA Security V1.2 labs.

<table>
<thead>
<tr>
<th>Device</th>
<th>Recommended Model(s)</th>
<th>Minimum DRAM</th>
<th>Minimum Flash</th>
<th>Minimum IOS Feature Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA</td>
<td>Cisco ASA5505-BUN-K9</td>
<td>512 MB</td>
<td>128 MB</td>
<td>Cisco (ASA) Software Version 8.4(2) Base License Cisco ASDM Version 7.2(1)</td>
</tr>
</tbody>
</table>

### 2.4 PCs and Servers

A Multi-Purpose Academy Pod supports 3 VMware virtual machines. Your selection of NETLAB+ supported VMware virtualization product is installed on a separate server.

The following operating system choices are typical. These choices are not mandatory; you can make substitutions, provided:

- The VMware virtualization product supports the operating system (as a “guest”).
- Your choices are compatible with the curriculum.

<table>
<thead>
<tr>
<th>Virtual Machine</th>
<th>Recommended O/S</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC A</td>
<td>Windows XP</td>
<td>Student PC, client activities</td>
</tr>
<tr>
<td>PC B</td>
<td>Windows XP</td>
<td>Student PC, client activities</td>
</tr>
<tr>
<td>PC C</td>
<td>Windows XP</td>
<td>Student PC, client activities</td>
</tr>
</tbody>
</table>
3 Control Device Requirements

NETLAB+ control devices provide internal connectivity, console access, and managed power. Control devices are dynamically managed by NETLAB+ and are not accessible or configurable by lab users.

The NETLAB+ Administrator Guide explains how to add, change, or delete control devices.

A Multi-Purpose Academy Pod with ASA requires the following control device resources:

<table>
<thead>
<tr>
<th>Control Device Resource</th>
<th>Quantity Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Switch</td>
<td>9 consecutive ports</td>
</tr>
<tr>
<td></td>
<td>1 reserved port (VMware)</td>
</tr>
<tr>
<td>Access Server</td>
<td>7 lines</td>
</tr>
<tr>
<td>Switched Outlet Devices</td>
<td>7 outlets</td>
</tr>
</tbody>
</table>

3.1 Control Switch Overview

NETLAB+ uses a control switch to provide connectivity between devices in a Multi-Purpose Academy Pod with ASA and VMware server(s). This pod requires 9 consecutive ports on a supported control switch (other than a Catalyst 1900 series).

Ports are labeled +0 to +8 in the diagram and are relative to the base port. These ports must be consecutive on the same control switch. As with all pods, you choose a base port for the pod during pod installation (Section 5). A control switch can support
multiple pods. To determine the actual port numbers used for this pod, add the base port number to the relative port numbers shown in the diagram. For example, if the base port is 5, the actual port numbers will be 5 to 13.

Using SNMP, NETLAB+ will automatically setup VLANs and configure ports on the control switch. These VLANs are depicted as letters “A” through “H” and represent one subnet in the topology. Each NETLAB+ pod has a unique VLAN pool and the actual VLAN numbers will be unique for each NETLAB+ pod. This is to avoid conflict between pods.

One “reserved” port on the control switch connects to an 802.1q NIC card on the VMware server. This allows devices in the pod to communicate with virtual machines.

The reserved port may be located on a different control switch, provided that all links between control switches are also configured as 802.1q trunks and all VLANs are allowed. You may also have more than one VMware server and virtual machines in the pod can be located on different VMware servers.
3.2 Access Server Ports

Access servers provide console connections to lab routers so that users can access them from NETLAB+. Users do not communicate directly with the access server. Rather, all connections are proxied through NETLAB+.

A Multi-Purpose Academy Pod with ASA requires 7 access server ports.

These ports do not have to be consecutive, and can span multiple access servers.

3.3 Switched Outlets

Switched outlets provide managed electrical power, allowing NETLAB+ and users to turn lab equipment on and off. A Multi-Purpose Academy Pod with ASA requires 7 switched outlets, one for each router and switch.

Outlets do not have to be consecutive and may span multiple switched outlet devices (i.e. APC7900 or APC7920).
PART 2 – IMPLEMENTATION

4 Pre-requisites

This section covers tasks that should be executed prior to adding a Multi-Purpose Academy Pod with ASA.

4.1 Understanding VMware Virtualization and Virtual Machines

The NETLAB+ Remote PC Guide Series provides detailed, version-specific information on the implementation of VMware virtualization products and virtual machines. A NETLAB+ Remote PC Guide should be used in conjunction with this guide. Use the guide appropriate for the VMware virtualization product you have chosen to implement on your NETLAB+ system in order to support remote PCs in your pod. To select the Remote PC Guide appropriate for your installation, please refer to the Remote PC Support page.

4.2 Setup Control Devices

Using the guidelines in Section 2, decide which control switch ports, access server ports, and switched outlets you will use for your Multi-Purpose Academy Pod with ASA. Add control devices if necessary. Control device configuration is documented in the NETLAB+ Administrator Guide.

4.3 Upload IOS Images

Upload the IOS images for the lab routers. NETLAB+ will recover these images on the devices if they are erased from flash.

4.4 Disable User Logins (optional)

You must take all equipment pods offline to add pods or configure control devices. You may wish to disable user logins during this time.
5 Adding the Pod

This section walks you through the process of adding a Multi-Purpose Academy Pod with ASA using the NETLAB+ New Pod Wizard.

5.1 Start the New Pod Wizard

Login to the administrator account.

Select Equipment Pods.

Select Add a Pod.

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

5.2 Add a Multi-Purpose Academy Pod with ASA

When prompted, select the Multi-Purpose Academy Pod with ASA.

5.3 Select Control Switch and Ports

A Multi-Purpose Academy Pod with ASA requires 9 consecutive control switch ports. NETLAB+ will present a list of the control switches on your system. Switches that meet the port requirement can be selected. Choose one control switch for your new pod.

A Multi-purpose Academy Pod with ASA requires 9 consecutive control switch ports.

Please select a control switch for this pod, then click Next.

Next, select the ports you want to use.
5.4 Select Access Server(s) and Ports

A Multi-Purpose Academy Pod with ASA requires 7 access server lines.

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 ports are not available, you can use non-consecutive ports, on different access servers if necessary.

**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.

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.
A AE Multi-purpose Academy Pod with ASA requires 7 access server lines.

- Use 7 consecutive lines on access server 1 starting at Line 1
- Let me pick the access server and lines for each device

<table>
<thead>
<tr>
<th>ACCESS SERVERS</th>
<th>ID</th>
<th>TYPE</th>
<th>LINES THAT ARE FREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Cisco 2511-RJ</td>
<td>1-16</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Cisco 2901 + 2 HWIC-16A (Lines 3-34)</td>
<td>3-18, 22-34</td>
</tr>
</tbody>
</table>

Line 1
Line 2
Line 3
Line 4
Line 5
Line 6
Line 7
Line 8
Line 9
Line 10
Line 11
Line 12
Line 13
Line 14
Line 15
Line 16
“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 a line number for each device.
5.5 Select Switched Outlets

A Multi-Purpose Academy Pod with ASA requires 7 switched outlets.

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.

<table>
<thead>
<tr>
<th>SWITCHED OUTLET DEVICES (SOD)</th>
<th>OUTLETS THAT ARE FREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>APC 9211 MasterSwitch</td>
</tr>
<tr>
<td>2</td>
<td>APC 9211 MasterSwitch</td>
</tr>
</tbody>
</table>

A Multi-purpose Academy Pod with ASA requires 7 switched outlets.

- Use 7 consecutive outlets on switched outlet device starting at outlet 1
- Let me pick select outlets for each device manually

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

<table>
<thead>
<tr>
<th>SELECT A SWITCHED OUTLET FOR EACH LAB DEVICE</th>
<th>SOD</th>
<th>OUTLET</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>R2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>R3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>S1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>S2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>S3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>ASA</td>
<td>2</td>
<td>7</td>
</tr>
</tbody>
</table>
5.6 Select Device Types

Select the model of each lab device that you will deploy.

⇒ Your selections are used to assign the appropriate NETLAB+ device driver.

⇒ Improper selections may cause errors.
⇒ NETLAB+ may offer selections that do not support the curriculum.

![Select Device Types Table]

5.7 Select Software Images and Recovery Options

NETLAB+ scrubs each router at the end of lab reservation or upon request. During a scrub, NETLAB+ can recover an IOS image if it is erased from flash.

![Select Software Images and Recovery Options Table]
The software images selected in this example support CCNA Security V1.1. For CCNA Exploration and Discovery, R1, R2 and R3 may have IP services, and for CCNPv6.0 R1, R2 and R3 must have Advanced IP Services, furthermore S1 and S3 must be 3560s.

You have three choices for flash recovery:

<table>
<thead>
<tr>
<th>Recovery Using Specified Image</th>
<th>During A Scrub Operation…</th>
</tr>
</thead>
<tbody>
<tr>
<td>If specified image not in flash</td>
<td>Restores the selected software image if that image is not in flash.</td>
</tr>
<tr>
<td>If no image in flash (erased)</td>
<td>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).</td>
</tr>
<tr>
<td>Never (device may become unusable)</td>
<td>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.</td>
</tr>
</tbody>
</table>

If you select an automatic recovery option, you must also select a software image supported by the curriculum.
5.8 Select a Pod ID

Each pod is assigned a unique numeric ID.

Each equipment pod is assigned a unique numeric ID.

Please select a Pod ID.

Pod ID: 4

5.9 Select a Pod Name

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

Each equipment pod is assigned a unique name.

Pod Name: Atlantic

5.10 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, run a pod test, configure PCs, and run another pod test before bringing the pod online. These tasks are discussed in the next sections.

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.
- Additional management options can be set for Cisco ASA security appliances.

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 your new pod.
NETLAB+ will display the status of the pod and the high-level settings for each device, PC, and control switch. Notice the PCs currently have a type of “ABSENT”. The PCs will be implemented in Section 9.
6 Cable the Pod

Use the NETLAB+ 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 4 -- 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 FOR POD 4

#### R1 (Cisco 1841 (S0/1/x))

<table>
<thead>
<tr>
<th>CONNECT FROM</th>
<th>USING CABLE</th>
<th>CONNECT TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>CAT-5 Straight Through</td>
<td>C/S 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port 1</td>
</tr>
<tr>
<td>FastEthernet 0/1</td>
<td>CAT-5 Straight Through</td>
<td>S/W</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FastEthernet 0/5</td>
</tr>
<tr>
<td>Console</td>
<td>Console Cable</td>
<td>A/S 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port 0</td>
</tr>
<tr>
<td>Power</td>
<td>Power Cord</td>
<td>SOD 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outlet 1</td>
</tr>
<tr>
<td>Serial0 DCE</td>
<td>Back-to-back serial cables</td>
<td>R2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial0 DTE</td>
</tr>
<tr>
<td>Serial1 DTE</td>
<td>Back-to-back serial cables</td>
<td>R3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial1 DCE</td>
</tr>
</tbody>
</table>

#### R2 (Cisco 1841 (S0/1/x))

<table>
<thead>
<tr>
<th>CONNECT FROM</th>
<th>USING CABLE</th>
<th>CONNECT TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>CAT-5 Straight Through</td>
<td>C/S 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port 2</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>CAT-5 Straight Through</td>
<td>C/S 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port 3</td>
</tr>
<tr>
<td>Console</td>
<td>Console Cable</td>
<td>A/S 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port 1</td>
</tr>
<tr>
<td>Power</td>
<td>Power Cord</td>
<td>SOD 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outlet 2</td>
</tr>
<tr>
<td>Serial0 DTE</td>
<td>Back-to-back serial cables</td>
<td>R1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial0 DCE</td>
</tr>
<tr>
<td>Serial1 DCE</td>
<td>Back-to-back serial cables</td>
<td>R3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial1 DTE</td>
</tr>
</tbody>
</table>

The cable chart is continued on the next page.
The cable chart is continued on the next page.
Virtual machine information will not appear on the cable chart. Refer to Section 9 for configuration instructions.

The Ethernet interface names show in the cable guidance will be the actual interface names based on your selected hardware. However, the interface names shown for serial ports are relative, not actual. Please consider this when cabling the pod.
7 Switch Configuration Tasks

The Multi-Purpose Academy Pod with ASA requires additional switch configuration tasks for successful operation. Using Hyperterm or other terminal, connect to the console port of the control switch in which the Multi-Purpose Academy Pod with ASA is connected. The following passwords are used on the control switch.

<table>
<thead>
<tr>
<th>Console login password</th>
<th>router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable secret password</td>
<td>cisco</td>
</tr>
</tbody>
</table>

Please do not change the passwords, they are used by NETLAB+ automation and technical support.

7.1 Verify Control Switch IOS Version

Each control switch should be running **IOS 12.2.25 or later**. Earlier versions may have defects that affect NETLAB+.

7.2 Configure Control Switch Ports

There are several essential commands that must be manually configured on each control switch port that connects to a lab switch (S1, S2, and S3 in this case).

```
switchport mode access
switchport nonegotiate
spanning-tree bpdugenfilter enable
no cdp enable
no keepalive
```
Locate the 4 control switch ports connecting to S1, S2 and S3. Refer to the cabling diagram if necessary (Section 6). The following commands must be manually added to each switch port.

- **switchport mode access**
  - Prevents the link from becoming a trunk port.
  - The labs will not work as designed if the link between control switch and lab switch is trunking.
  - Trunking on ports that should be access ports, combined with BPDU filtering, creates loops that are not prevented by spanning-tree.

- **switchport nonegotiate**
  - Prevents the interface from sending DTP messages.
  - Disabling DTP messages is not critical, but will hide the control switch' MAC address from lab switches when users performing commands to see the CAM table.

- **spanning-tree bpdudfilter enable**
  - Instructs control switch port not to send and receive spanning tree BPDU frames to and from the lab switch.
  - Spanning tree in the lab must not mingle with spanning tree on the control switch. This would cause several undesirable effects in both the lab and on the control switches.

- **no cdp enable**
  - Disabling CDP is not critical, but will hide the control switch from lab switch users performing CDP commands.

- **no keepalive**
  - Prevents the interface from sending L2 keepalive messages.
  - Disabling L2 keepalives messages is not critical, but will hide the control switch' MAC address from lab switches when users performing commands to see the CAM table.

Do not omit these commands! Without them, loops will form causing high CPU utilization, error-disabled ports, and connectivity loss. These commands are specific to switch pods and are not automatically configured.
Example switch port configuration. Interface numbers will vary.

```plaintext
interface FastEthernet0/9
  description port to S1 port 6
  switchport mode access
  switchport nonegotiate
  spanning-tree bpdudfilter enable
  no cdp enable
  no keepalive

interface FastEthernet0/10
  description port to S2 port 11
  switchport mode access
  switchport nonegotiate
  spanning-tree bpdudfilter enable
  no cdp enable
  no keepalive

interface FastEthernet0/11
  description port to S2 port 18
  switchport mode access
  switchport nonegotiate
  spanning-tree bpdudfilter enable
  no cdp enable
  no keepalive

interface FastEthernet0/12
  description port to S3 port 18
  switchport mode access
  switchport nonegotiate
  spanning-tree bpdudfilter enable
  no cdp enable
  no keepalive
```

If the control switch does not recognize the `spanning-tree bpdudfilter` command, make sure the switch is running at least 12.2.25.
7.3 Initial Lab Switch Setup

Several switch models are subject to a common problem when used as a lab switch. These include (but not limited to):

- Cisco Catalyst 2900 XL Series
- Cisco Catalyst 2950 Series
- Cisco Catalyst 2960 Series
- Cisco Catalyst 3550 Series
- Cisco Catalyst 3560 Series

Cisco WS-C3560V2-24PS switches ("V2" models) do not respond to a console break signal, regardless of "enable break" setting, and therefore do not work with NETLAB+ automation (reference Cisco bug CSCsv92241). Although the bug was reported fixed, the problem still persists on the V2 models as of this writing. Workarounds: use WS-C3560-24PS (non-"V2" version) switches if available, or turn off automation by using the Generic Console Device setting.

By default, these switches will not respond to a console break signal the same way routers do. There are two environment variables that affect this: Enable Break and BOOT path-list.

The following procedure explains how to check these variables and set them so that the console port will respond to a break signal.

When to Use

You must initialize the environment variables when:

- Installing a lab switch for the first time.
- The Enable Break environment variable is set to "no".
- The BOOT path-list environment variable is set.

This procedure does not apply to control switches.

Determining the Boot Status

From the enable mode, issue the following IOS command.

```
Lab_Sw# show boot
BOOT path-list:     flash:c2950-i6q412-mz.121-22.EA4.bin
Config file:        flash:config.text
Private Config file: flash:private-config.text
Enable Break:       no
Manual Boot:        no
```

Setting Up the Environment
Follow this procedure if Enable Break is set to “no” and/or the boot path-list is set to an image.

```plaintext
Lab_Sw# configure terminal
Lab_Sw(config)# boot enable-break
Lab_Sw(config)# no boot system
Lab_Sw(config)# end
Lab_Sw# copy run start
Lab_Sw# show boot

BOOT path-list:
Config file: flash:config.text
Private Config file: flash:private-config.text
Enable Break: yes
Manual Boot: no
```

**Verification**

With Enable Break set to "yes" and removal of a BOOT path-list, a pod test should pass.

If the environment variables are not set correctly, you may experience one of the following symptoms:

1. Pod test fails with a message such as "unable to put the switch into monitor mode"
2. Lab automation such as scrub fails
3. Users cannot perform password recovery (automated or manual).

Please keep in mind that Cisco WS-C3560V2-24PS switches ("V2" models) do not respond to a console break signal, regardless of "enable break" setting, and therefore do not work with NETLAB+ automation (reference Cisco bug CSCsv92241). Although the bug was reported fixed, the problem still persists on the V2 models as of this writing. Workarounds: use WS-C3560-24PS (non-"V2" version) switches if available, or turn off automation by using the Generic Console Device setting.
8 Testing the Pod (Test 1 – Before PC Implementation)

We recommend that you run a pod test at this point in the MAP w/ ASA installation process in order to verify that all lab devices (routers, switches and ASA) in the pod have been properly installed, before implementing the PCs as described in the next section. The pod test will detect common configuration and cabling problems. You will also run a second pod test after implementing the PCs in the MAP with ASA pod.

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. Some images are very large and can take up to 30 minutes to program into flash memory.

See Section 11 for additional information on running a pod test, including an example.
9 Select PC Type

It is strongly encouraged that you choose the Use Virtual Machine Inventory. This option combined with automatic networking and VNC configuration, makes deploying pods much easier.

At the time that the MAP w/ ASA was created, the PC Type for each PC in the pod was given the default setting of ABSENT (NETLAB+ version 2011.R1 and later). The appropriate PC options must be set for each remote PC, depending on your selection of virtualization options.

PC Configuration

PC/Virtual Type

1. ABSENT When new pods are created, the PC Type for each PC is initially set to ABSENT. This indicates the PC is not implemented in the pod. A “PC Unavailable” message can be set to display so that users with get a popup message if they try to connect to it, informing them that the PC is not implemented.

   - Use Virtual Machine Inventory (available in NETLAB+ version 2011.R1 and later): Use a virtual machine defined in the NETLAB+ Virtual Machine Inventory (VMI). The VMI offers the most advanced VM configuration and automation capabilities available in NETLAB+. NETLAB+ Remote PC Guide Volume 3 - Configuring the NETLAB+ Virtual Machine Infrastructure includes a section, Assigning Virtual Machines to Pods, which provides step-by-step guidance in the process of assigning a virtual machine in the VMI to a pod.
• Basic virtualization options using VMware products. This option offers basic 'no frills' VM automation.

  o **VMWARE ESXi 4.0 (no vCenter)** provides direct access to a VMware virtual machine and enables automation through the VMware API. Select this option if you are using ESXi 4.0 without vCenter.

NDG strongly recommends using the Virtual Machine Inventory. There is no network and VNC automation without using vCenter. Please refer to the **NETLAB+ Remote PC Guide Series**. Please see also the **Remote PC Support** page for current information on the support status of this and other options.

You will be prompted to enter additional information for VMware specific settings. These settings are discussed in the next section.

10 VMware Settings

If you are using any of the basic virtualization options (see previous section), you will be prompted to enter VMware-specific settings. Please refer to the **NETLAB+ Remote PC Guide Series** for version-specific details regarding these settings.

Here, we show an example where **Use Virtual Machine Inventory** is the virtualization option selected. The settings are described below.
**Base Datacenter:** The virtual datacenter that contains the virtual machine to be used for this PC (unless overridden by a lab).

**Base Virtual Machine:** The virtual machine that will be used for this PC (unless overridden by a lab).

**Base Snapshot:** The snapshot that will be used to revert the base virtual machine to a clean state during pod initialization, user initiated scrub action, and at the end of a lab reservation.

**VMware Guest Configuration File:** The preferred shutdown sequence if the virtual machine is still powered on at the end of a lab reservation. If a base snapshot is configured, it is reverted first. If the virtual machine is still powered on after reverting to the snapshot, the preferred shutdown sequence is executed. Otherwise, the final power state will be the same as the snapshot state.

**Guest Operating System:** The operating system running on this virtual machine.

**Options:** Enable or disable automated features.

**V2 Maximum Color Depth:** Set the maximum and default color depth for Remote PC Viewer version 2. The client will start up using the color depth set here. The user may select a lower color depth to conserve bandwidth. However, the user may not select a higher color depth than this setting.

**Admin Status:** Set admin status to ONLINE to enable this PC. You can temporarily disable this PC by setting the administrative status to OFFLINE.

### 11 Testing the Pod (Test 2 – After PC Implementation)

After all PCs have been implemented, 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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Online]</td>
<td>Bring this pod ONLINE and make it available for reservations.</td>
</tr>
<tr>
<td>![Test]</td>
<td>Tell me if this pod is working properly.</td>
</tr>
<tr>
<td>![Cable]</td>
<td>Show me how to cable this pod.</td>
</tr>
</tbody>
</table>

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. Some images are 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.

<table>
<thead>
<tr>
<th>POD TEST LOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>[09:43] ASA: scrub test test - PASS</td>
</tr>
<tr>
<td>[08:22] ASA: check switched outlet test - PASS</td>
</tr>
<tr>
<td>[06:08] ASA: boot ASA image test - PASS</td>
</tr>
<tr>
<td>[09:42] ASA: check ethernet connection test - PASS</td>
</tr>
<tr>
<td>[09:21] S3: camosku fueled test - PASS</td>
</tr>
</tbody>
</table>

The pod test has passed with the following warnings:

- WARNING: Automatic virtual machine host networking setup is supported by this pod, but not pod tested in this release.

- WARNING: Automatic virtual machine host networking teardown is supported by this pod, but not pod tested in this release.

If you contact technical support for assistance, please cut and paste the entire pod test log (above) into your e-mail or support request web form. This will expedite resolution.

You are now encouraged to bring the pod online, schedule a lab reservation, and test functionality that NETLAB+ did not test above.
12 Finishing Up

12.1 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.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>Bring this pod ONLINE and make it available for reservations</td>
</tr>
<tr>
<td>Test</td>
<td>Tell me if this pod is working properly</td>
</tr>
<tr>
<td>Cable</td>
<td>Show me how to cable this pod</td>
</tr>
<tr>
<td>Delete</td>
<td>Remove this pod from NETLAB</td>
</tr>
</tbody>
</table>
12.2 Enable Multi-Purpose Academy Pod with ASA Exercises

To make the Multi-Purpose Academy Pod with ASA available to classes and students, you must enable the corresponding lab exercise content.

To avoid configuration management problems, we recommend that the CCNA Security courses be enabled in a separate class from other courses. Likewise, the CCNPv7 TSHOOT course must be enabled in a separate class from other courses. Enabling the courses each within a separate class will allow you to set the appropriate console and enable the secret passwords in the class settings as required.

- If you are using your Multi-Purpose Academy Pod with ASA for CCNA Security v2.0, please note that CCNA Security labs require different console and enable secret password settings from other courses. If CCNA Security and other courses are enabled in the same class, it is likely that the NETLAB+ automation will fail to save configuration files, since the default passwords, “cisco” and “class” are not the correct passwords for CCNA Security.
  
  1. In the Global Labs section of the class settings, select AE CCNA Security v2.0 - MAPASA- English Do not enable any other labs for this class.
  2. Change the Console Password to ciscoconpass
  3. Change the Enable Password to cisco12345

- If you are using your Multi-Purpose Academy Pod for the CCNPv7, please note that CCNP TSHOOT v7 labs require a different Enable Secret Password setting from other courses.
  
  1. In the Global Labs section of the class settings, select AE CCNPv7 TSHOOT - MAP
  2. Do not enable any other labs for this class.
  3. Do not the change the default Console Password, is should remain cisco.
  4. Change the Enable Secret Password to cisco.
12.3 Schedule a Lab Reservation for Your New Pod

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. In this example, we will reserve an equipment pod for your own use.

- 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 selection of pods depicted may be different from the pods available at your site.
Select an available time, and the confirmation page will be displayed.

Review the details of the reservation and select **I'm Done** to confirm the reservation. If you return to the scheduler and select view or cancel reservations, you will see details of the reservation in the reservation listing.
For more information on scheduling reservations, see the Scheduler section of the 
*NETLAB+ Instructor Guide*. 