This support document is intended for users with an active VMware vSphere license. If you do not have a VMware vSphere license, you will need to purchase one to operate NETLAB+ until our team releases a version utilizing Proxmox.

NETLAB+® VE

Virtual Edition

Real Equipment Pod Installation Guide For Cisco Networking Academy

Document Version: 2021-10-12

This guide provides guidance for NETLAB+ VE setup and installation tasks specifically required for Cisco Networking Academy courses that include physical ***lab devices*** (also known as ***real equipment***).

This guide documents features related to supporting real equipment, available in **NETLAB+ VE version 21.1.2** and later.

Contents

Introduction

This guide provides specific guidance for planning, installing, and supporting Cisco Networking Academy courses that contain real lab equipment (i.e., routers, switches, and firewall devices).

> Cisco Networking Academy topologies and labs can be obtained through the NETLAB+ VE course manager, provided your institution is a member of the Cisco Networking Academy.

NETLAB+ VE supports the following Cisco Networking Academy courses utilizing real equipment:

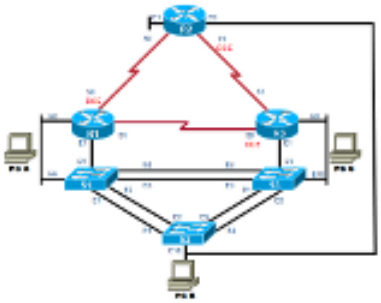
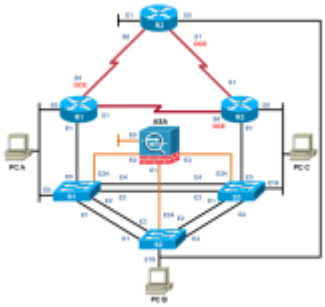
- CCNA Routing and Switching - 6.0
  - Bridging
  - Introduction to Networks
  - Routing & Switching Essentials
  - Scaling Networks
  - Connecting Networks
- CCNA Routing and Switching - 5.1
  - Introduction to Networks
- CCNA Routing and Switching - 5.0
  - Network Basics
  - Introduction to Networks
  - Routing Protocols
  - Routing and Switching Essentials
  - Switched Networks
  - Scaling Networks
  - Connecting Networks
- CCNA Security – 2.0, 1.2, 1.1
- CCNP – 7.0
  - SWITCH
  - ROUTE
  - TSHOOT
- CCNP – 6.0
  - SWITCH
  - ROUTE
  - TSHOOT

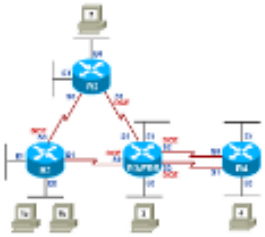
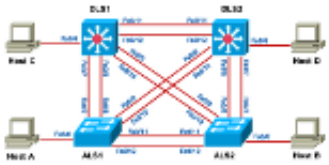
1 Cisco Networking Academy Standard Topologies

NETLAB+ provides scheduled, shared access to lab equipment. A single instance or set of lab equipment that may be reserved and accessed is referred to as a *topology*.

Cisco Networking Academy courses mentioned in the previous section utilize four *standard topologies* that are detailed in this guide.

The standard topologies are implemented as pods in NETLAB+ VE and contain both virtual machines and real lab equipment. Users interacting with the lab equipment through NETLAB+ need not be concerned with whether they are interacting with real or virtualized equipment; NETLAB+ facilitates access to both in the same manner.

Cisco Networking Academy Standard Topologies	
Topology	**Resources**
Multi-purpose Academy Pod (MAP) 	• Quick Reference Page • Planning and Installation Guide
Multi-purpose Academy Pod with ASA (MAPASA) 	• Quick Reference Page • Planning and Installation Guide

Cuatro Router Pod (CRP) 	• Quick Reference Page • Planning and Installation Guide
Cuatro Switch Pod (CSP) 	• Quick Reference Page • Planning and Installation Guide

Custom pods with real equipment are possible. The NETLAB+ VE Pod Designer tool can be used to create topologies that contain both virtual machines and real equipment. This advanced topic is best suited for those who are experienced with the installation of standard pods and all aspects of administrating a NETLAB+ system.

1.1 NETLAB+ VE Maximums

The table below shows the maximum number of pods using standard topologies supported by NETLAB+ VE when conforming to the prescribed rack layouts.

NETLAB+ VE License	Maximum Pods Using Standard Topologies	Number of Racks (Approximate)
VE 16	16	4
VE 32 or higher	28	7

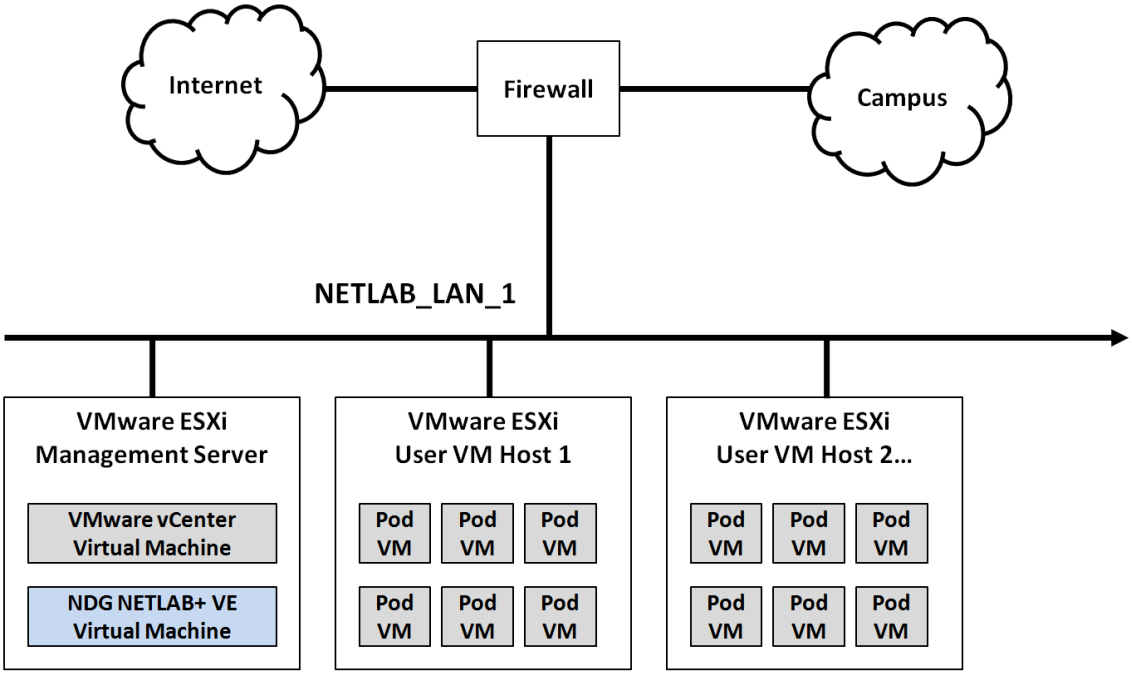
The combination of topologies and specific lab equipment deployed will depend on the Cisco courses you wish to teach.

2 Overview of Real Equipment Support

In this section, we will discuss the concepts and infrastructure requirements for supporting real equipment on your NETLAB+ system.

2.1 Standard NETLAB+ VE Installation

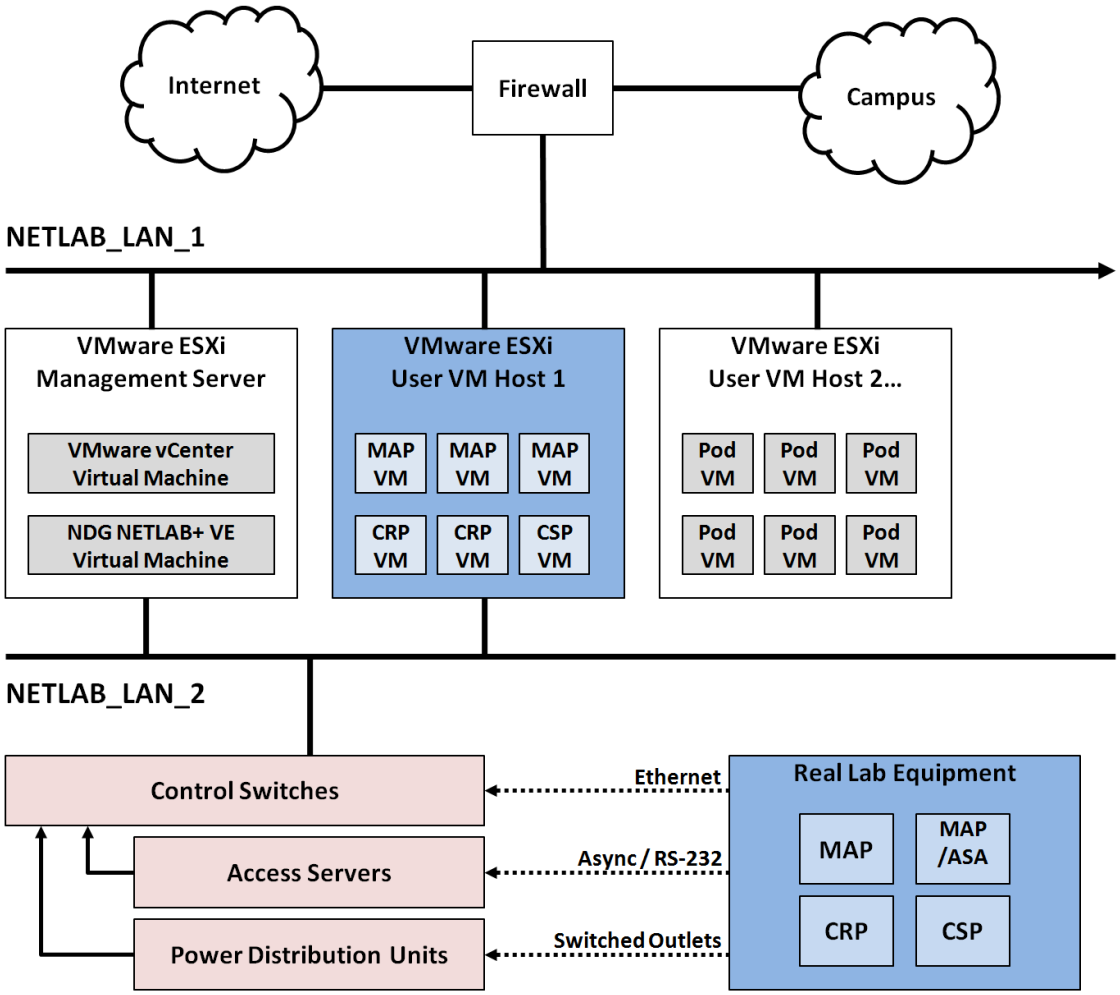
This guide assumes that you already have a working NETLAB+ VE installation with virtual machine infrastructure (as depicted below).



The *NETLAB+ VE Installation Guide* documents the standard installation.

2.2 Real Equipment NETLAB+ VE Installation

A NETLAB+ VE system with real lab equipment extends the standard NETLAB+ VE system by adding additional devices and networks:



The additional devices include:

- **Lab Devices:** real lab equipment that students will access, organized into pods (the standard topologies, MAP, MAPASA, CRP, and CSP)

- **Control Devices:** infrastructure equipment that provides internal connectivity, console access, and managed power. Control devices are managed by NETLAB+ and are not accessible or configurable by lab users

NETLAB_LAN_2 provides a non-routable network for:

- Communication between lab devices and virtual machines.
- Management traffic between NETLAB+ VE and control devices.

3 Standard Rack Layouts

To simplify planning, purchasing, and support, we have introduced four standard rack layouts:

- **MAP - 1U**
  - 4 MAP or 4 MAPASA pods
  - For the latest equipment bundles with all 1U hardware
- **MAP - 2U**
  - 4 MAP or MAPASA pods
  - For older equipment bundles containing 2U Cisco 1941 routers
- **Cuatro - 1U**
  - 4 Cuatro Router pods and 4 Cuatro Switch pods
  - For the latest equipment bundles with all 1U hardware
- **Cuatro - 2U**
  - 3 Cuatro Router pods and 3 Cuatro Switch pods
  - For older equipment bundles containing 2U Cisco 1941 routers

Rack Layout	MAP or MAPASA	CRP	CSP	Total Pods
MAP – 1U	4			**4**
MAP – 2U	4			**4**
Cuatro – 1U		4	4	**8**
Cuatro – 2U		3	3	**6**

The standard rack layouts prescribe:

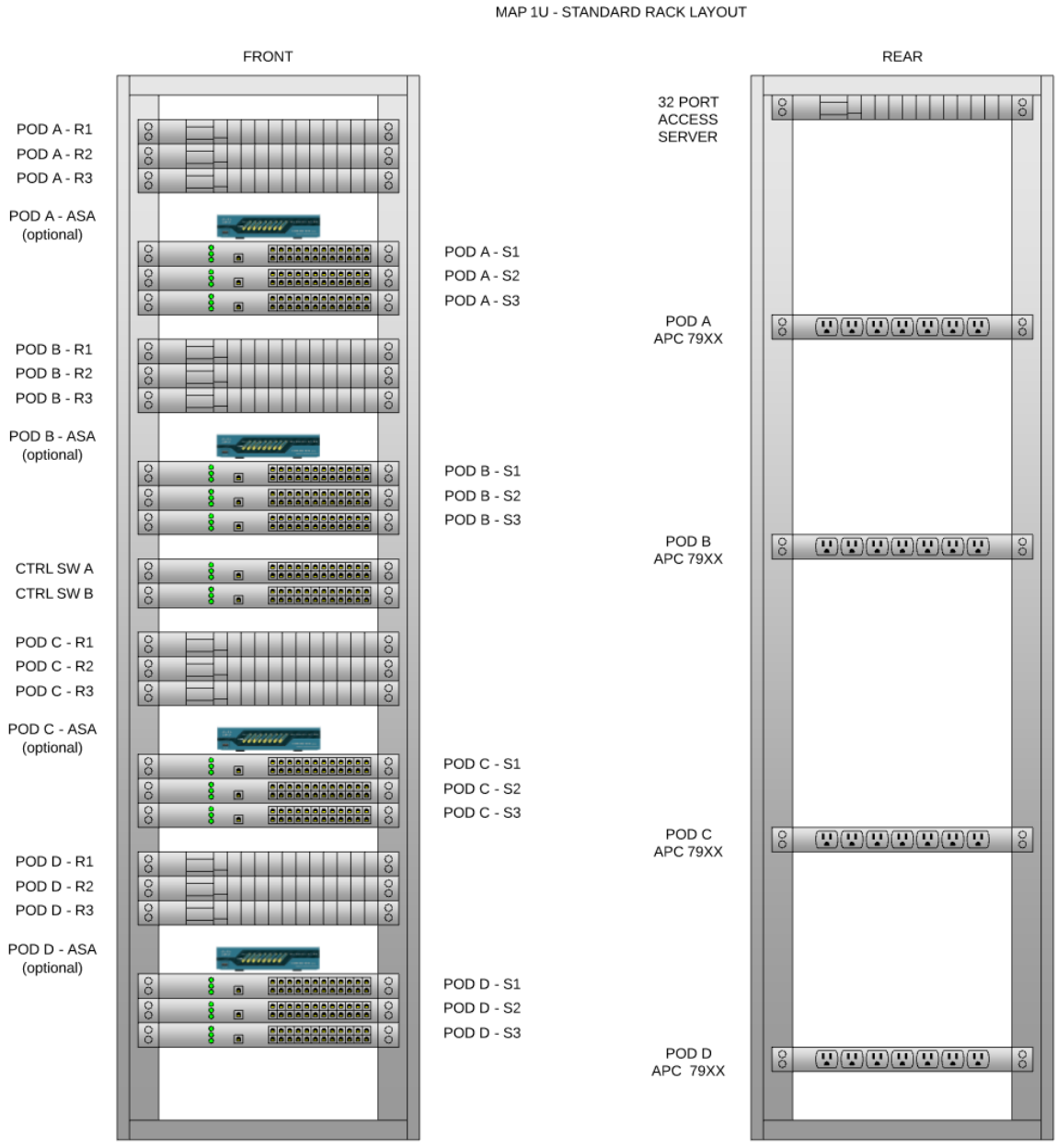
- Equipment to purchase
- Arrangement of equipment within a standard 42U equipment rack
- Cabling between devices
- Standardized port assignments

Adhering to the standard rack layout to support Cisco Networking Academy courses is highly encouraged. Standard racks embody best practices learned from years of support and onsite installations.

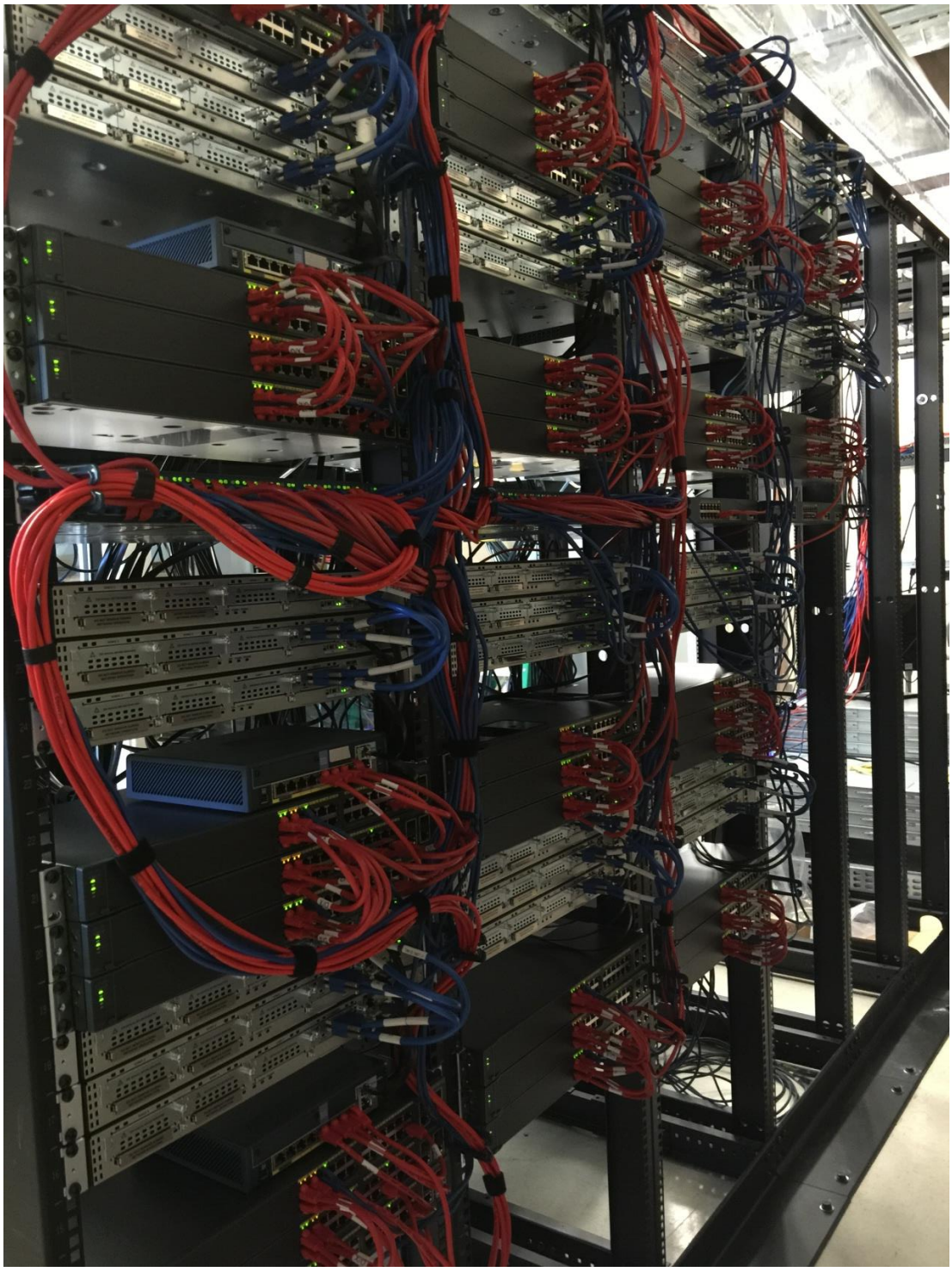
Keep in mind this advice from the NDG development team: *"Do not sweat the gory details. Use the standard racks!"*

3.1 MAP 1U Rack

Total Pods	4
Topology	MAP or MAPASA
Rack Dimensions	Standard Rack – Height 42U, Depth 29” or higher
Access Server	1 X [32 Lines]
Control Switch	1 X [48 ports, 2 Uplinks] OR 2 X [24 ports, 2 Uplinks]
PDU	4 X [8 outlets] (standard cabling) OR 3 X [8 outlets] (alternate cabling)
Applicability	For new hardware purchases using the latest Cisco bundles.



Example: MAP 1U



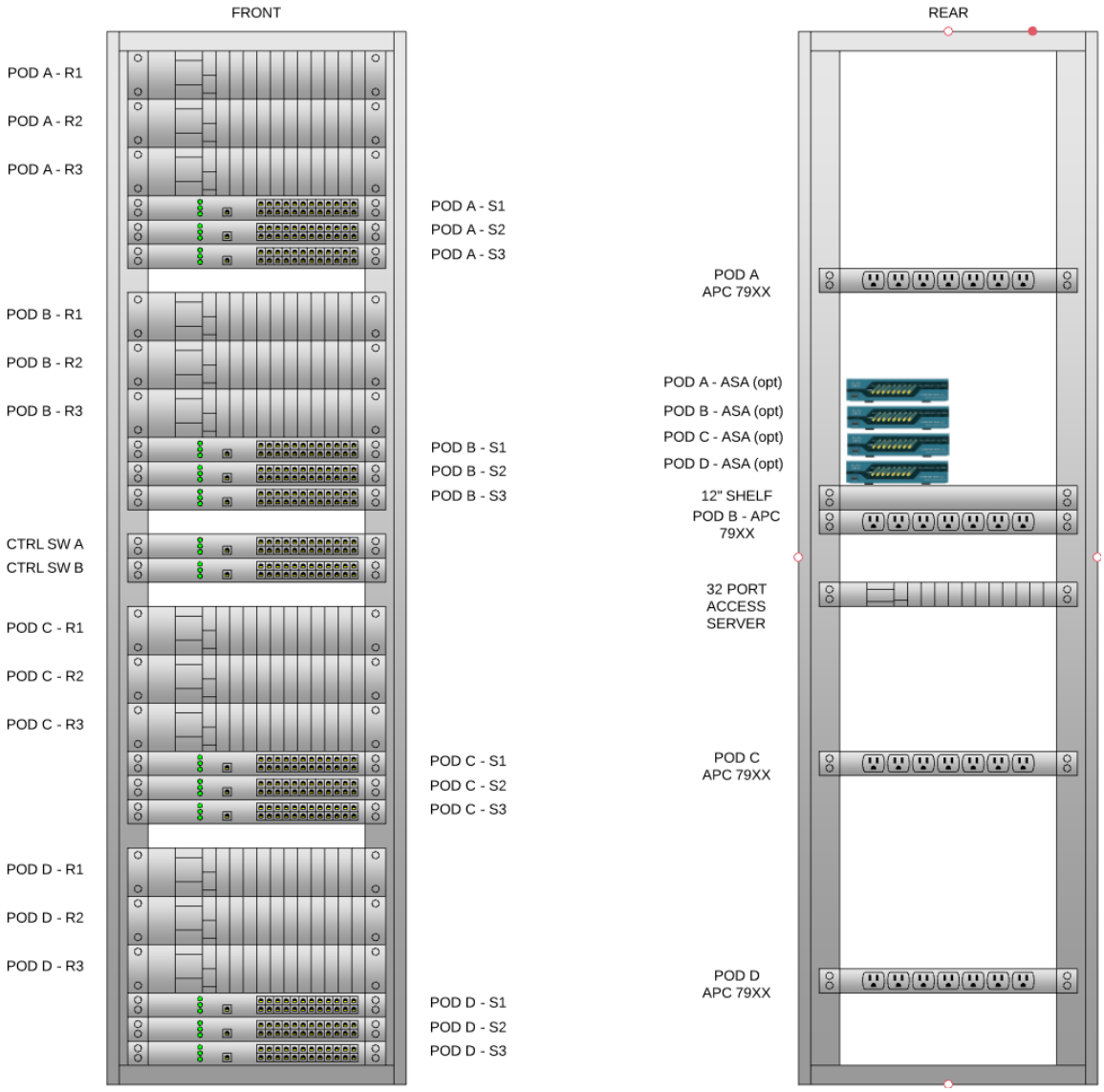
(PHOTO CREDIT TO BE ADDED)

Notice in the picture above:

1. The picture shows the use of a 48-port control switch (middle).
2. ASA devices shown are optional but required in some Cisco courses.
3. Follow router switch, and ASA orientation as shown.
4. Two rack units (2U) allocated for ASA spacing and airflow.

3.2 MAP 2U Rack

Total Pods	4
Topology	MAP or MAPASA
Rack Dimensions	Standard Rack – Height 42U, Depth 29” or higher
Access Server	1 X [32 Lines]
Control Switch	1 X [48 ports, 2 Uplinks] OR 2 X [24 ports, 2 Uplinks]
PDU	3 X [8 outlets]
Applicability	For use with older bundles containing Cisco 1941 routers.



Example: MAP 2U

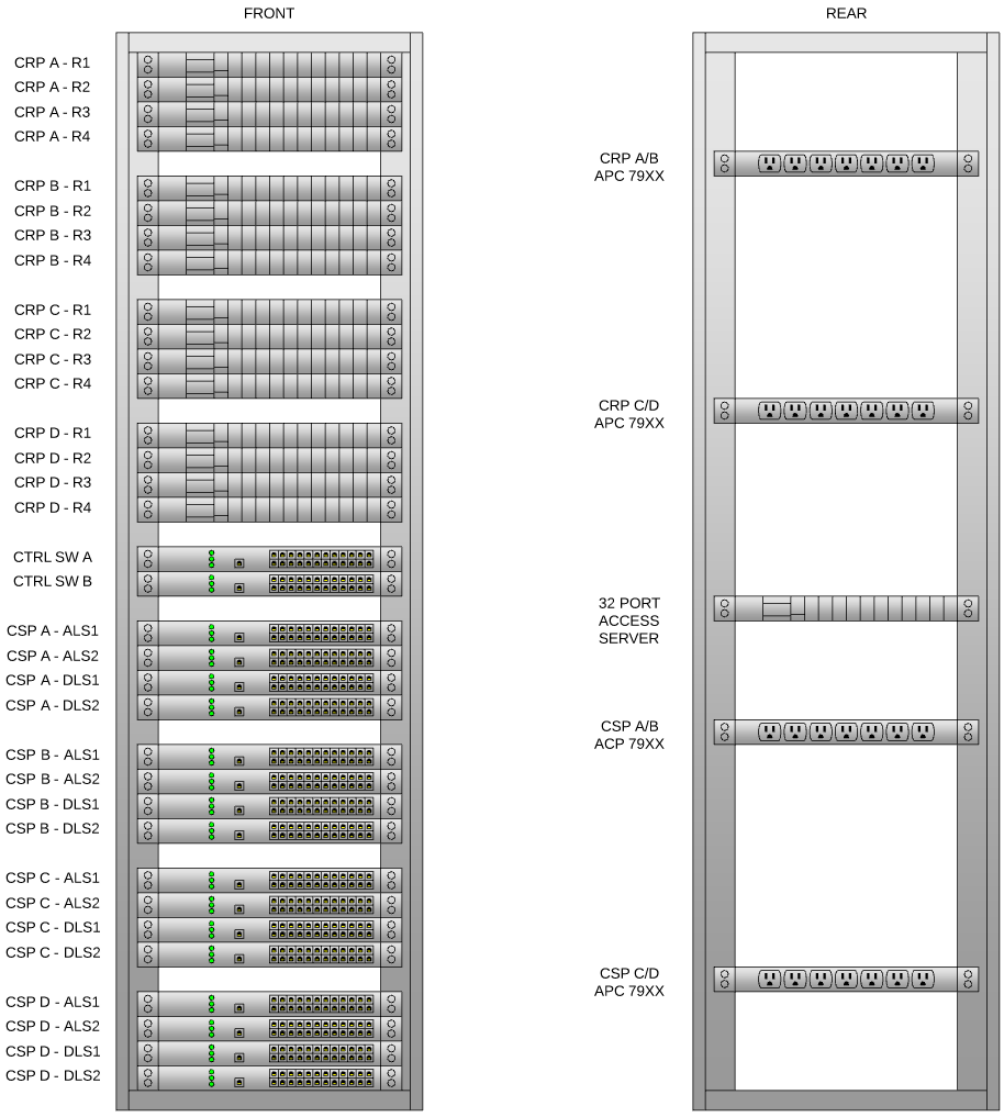
(PHOTO CREDIT TO BE ADDED)

Notice in the picture above:

1. Picture shows the use of a 48-port control switch (middle).
2. Optional ASA devices not shown; stack on the rear shelf if implemented.
3. Follow router and switch orientation as shown.

3.3 Cuatro 1U Rack

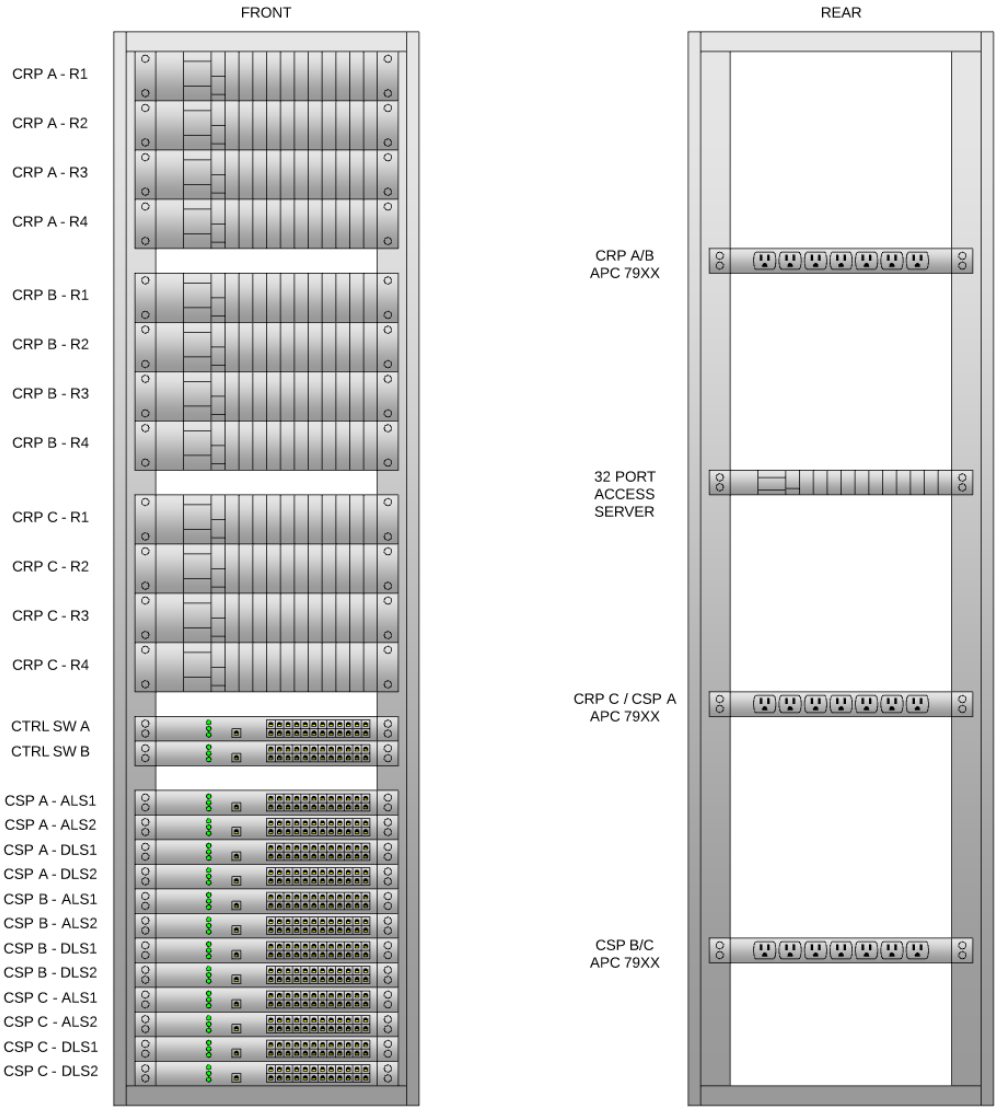
Total Pods	8
Topology	[4 X Cuatro Router Pod] + [4 X Cuatro Switch Pod]
Rack Dimensions	Standard Rack – Height 42U, Depth 29” or higher
Access Server	1 X [32 Lines]
Control Switch	1 X [48 ports, 2 Uplinks] OR 2 X [24 ports, 2 Uplinks]
PDU	4 X [8 outlets]
Applicability	For new hardware purchases using the latest Cisco bundles.



If space for power strip needed at bottom, coalesce open slots as needed.

3.4 Cuatro 2U Rack

Total Pods	6
Topology	[3 X Cuatro Router Pod] + [3 X Cuatro Switch Pod]
Rack Dimensions	Standard Rack – Height 42U, Depth 29” or higher
Access Server	1 X [32 Lines]
Control Switch	1 X [48 ports, 2 Uplinks] OR 2 X [24 ports, 2 Uplinks]
PDU	3 X [8 outlets]
Applicability	For use with older bundles containing Cisco 1941 routers.



If space for power strip needed at bottom, coalesce open slots as needed.

4 Lab Device Equipment Selection

This section provides guidance for new lab equipment purchases.

The lab equipment required for each standard pod is derived from the Cisco Networking Academy Standard Bundle spreadsheets, which are updated periodically. This section will review in detail how to calculate lab device requirements for planning and purchasing.

The latest equipment and/or system software in the latest Standard Bundle may not yet be supported by NETLAB+ VE. Please use the information in this guide for planning.

To simplify purchasing, we have organized equipment requirements by pod type. Since these requirements change over time, we further categorized them as Configuration A, Configuration B, Configuration C, etc.

- Configurations are presented in descending alphabetical order. For example, Configuration D is the most recent configuration among A, B, C, and D. Configuration A contains hardware from the earliest bundle supported by NETLAB+ VE.
- The latest configuration is typically recommended for new purchases. Your selection of courses and equipment budget should also be considered when choosing a configuration.
- Earlier configurations are supported for reference until the equipment no longer supports the requirements of the Cisco Networking Academy.

4.1 MAPASA Pod Configurations

See the specifications for MAPASA pod configurations.

4.2 MAP Pod Configurations

See the specifications for MAP pod configurations.

4.3 CRP Pod Configurations

See the specifications for CRP pod configurations.

4.4 CSP Pod Configurations

See the specifications for CSP pod configurations.

5 Control Device Equipment Selection

The number of control switches, access servers, and power distribution units needed for your system will vary, depending on the type and number of racks containing real equipment that you will be installing. There are three types of control devices.

- **Control Switches**: Provide connectivity to real lab equipment from NETLAB+ and the virtual infrastructure.
- **Access Servers:** Asynchronous terminal servers that provide console access to real lab equipment.
- **Power Distribution Units (PDUs):** Provide switched outlets for real lab equipment.

5.1 Control Switch Requirements

Control switches are used to implement NETLAB_LAN_2 and provide several functions:

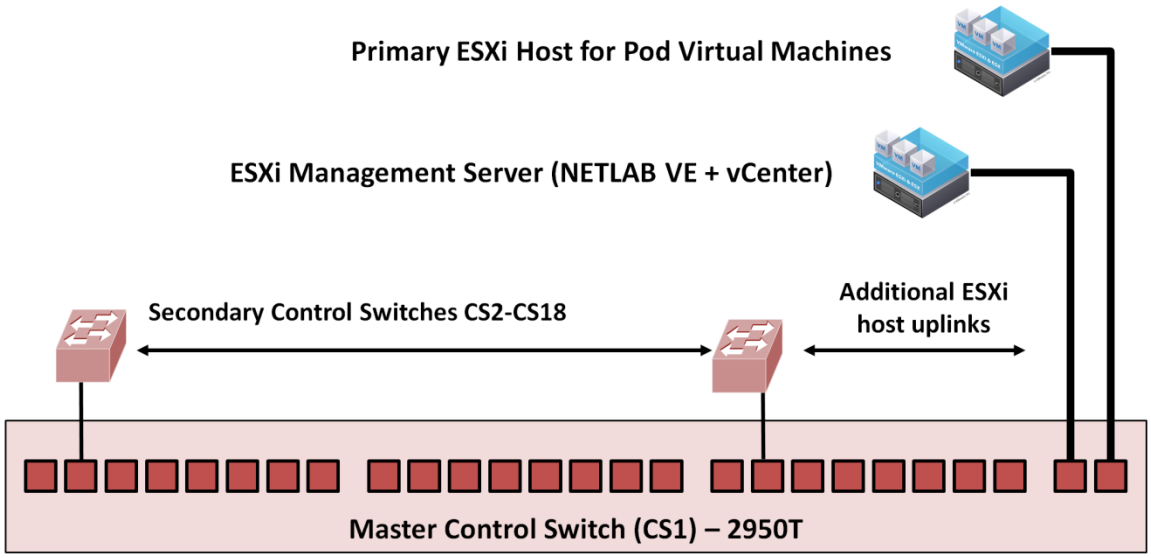
- Connect real lab equipment to virtual machines.
- Simulate networks and dynamic topologies per lab exercise.
- Provide a management path between NETLAB+ and control devices.

*A typical NETLA*B+ setup for real equipment includes a master control switch plus one or more secondary control switches that trunk to the master control switch.

> A NETLAB+ VE system will support up to 20 control switches. Using standard rack layouts, the number of control switches including master control switch will not exceed 16.

5.1.1 Master Control Switch

The master control switch is a core switch that provides connectivity between lab equipment racks, the virtual machine infrastructure, and the NETLAB+ VE virtual machine.



Best practice is to locate the master control switch in the same rack as virtual machine servers.

The master control switch is always Control Switch 1 (CS1). NETLAB+ VE always assumes CS1 is the master control switch and the configuration instructions for CS1 provided by NETLAB+ prompts will vary slightly from other control switches.

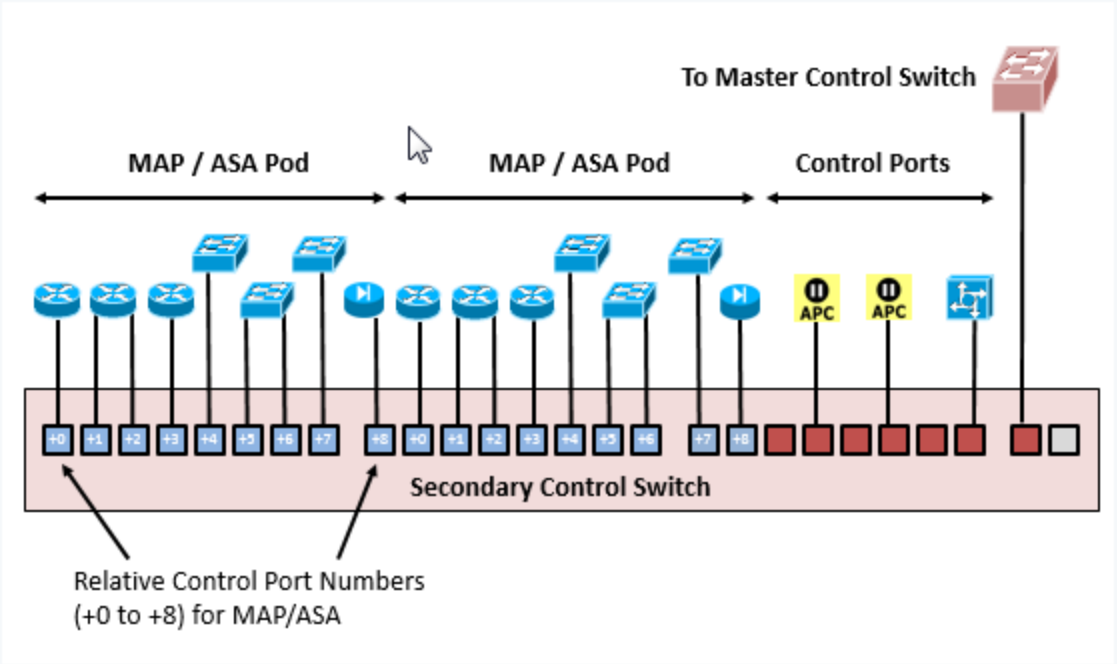
The following switch models are supported for the master control switch.

Type	Minimum Required Image	Ports	Uplinks	Max VLANs	Comments
Cisco WS-C2960+24TC-L	12.2.25	24	2	250	Recommended as master control switch in new installations.
Cisco WS-C2950T-24	12.1(22)EA2 (EI)	24	2	250	Recommended if already on-hand "T" model with uplinks required.
Cisco WS-C3650-24-TS-E	03.06.05.E	24	4	1000	OK as master control switch in Large Installation (5-7 racks).

Please be aware that Lenovo servers' 1 gig ports do not support 10/100 ports on the control switch. They will need to use a 2960-24 with gig uplinks and use one of those gig ports on the 2960-24 master control switch.

5.1.2 Secondary Control Switches

Your NETLAB+ system will include one or more secondary control switches; the number of control switch ports needed depends on the type and number of standard racks you will be adding to your system.



The following table shows the supported switch models and quantity required per standard rack.

Type	Minimum Required Image	Ports	Uplinks	# Per Rack	Comments
Cisco WS-C2960+48TC-L	12.2.25	48	2	1	Recommended for new installations in standard racks. “Plus” model and LAN Base image required.
Cisco WS-C2960+24TC-L	12.2.25	24	2	2	Recommended if already on-hand.
Cisco WS-C2950T-24	12.1(22)EA2 (EI)	24	2	2	OK if already on-hand. "T" model with uplinks required.

5.2 Access Server Requirements

An access server is an asynchronous terminal server that provides console access to real lab equipment. Using this approach, users can access lab gear even when no configurations have been loaded in the lab devices. NETLAB+ proxies all connections through the access server. This special proxy allows simultaneous sharing of console ports and allows all users to access the lab environment using a built-in HTML5 CLI terminal.

Your NETLAB+ system will require one or more access servers, depending on the number and type of real equipment pods you add to your system. Using the standard rack layouts, there will be one access server with 32 lines (ports) per rack.

The following hardware configurations are supported for 32-port access server configurations in a standard rack. Other combinations that are not 32-ports are possible in NETLAB+, but not listed here.

When using a HWIC-16A on a router (2901 or 2811) with IOS 15, you must use version **15.1.4M4(MD)**, due to a Cisco bug. NDG has tested **15.1.4M4(MD**) on all platforms. Please refer to the table below.

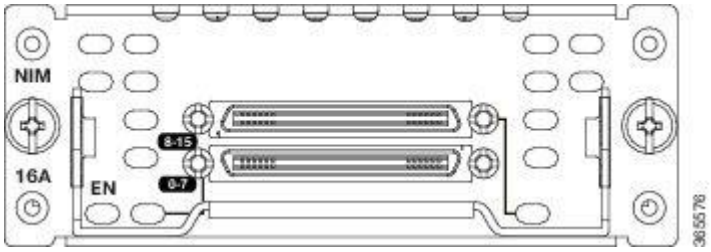
Router	Async Line Card(s) Qty X Type	Cables Qty X Type	Notes
Cisco 4321 ISR	2 X NIM-16A	4 X CAB-ASYNC-8 (10 foot)	1,3
Cisco 2901	2 X HWIC-16A	4 X CAB-HD8-ASYNC (10 foot)	3,4
Cisco 2811	2 X HWIC-16A	4 X CAB-HD8-ASYNC (10 foot)	3,4,5
Cisco 2801	2 X HWIC-16A	4 X CAB-HD8-ASYNC (10 foot)	3
Cisco 2600	1 X NM-32A	4 X CAB-OCTAL-ASYNC (10 foot)	2

1. Recommended for new purchases.
2. End-of-sale.
3. Cuatro 2U rack only requires 3 octal cables per rack.
4. When using an HWIC-16A on a router (2901, or 2811) with IOS 15, you must use an IOS version that has been tested by NDG, due to a Cisco bug. NDG has tested **15.1.4M4(MD)** on all platforms.
5. For Cisco 2811 only: Using HWIC-16A on a router with IOS 12 does not exhibit the bug mentioned in the note above.

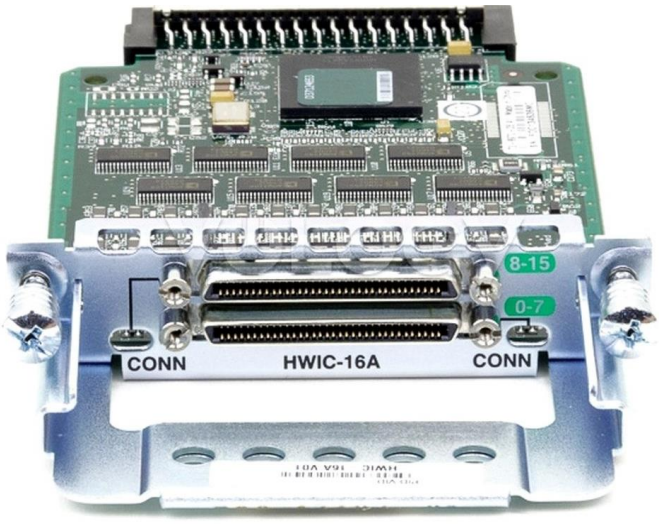
When using a HWIC-16A on a 28*xx* router, please refer to the table below for slot placement (reverse populate as shown, Slot 3 is the first slot that gets the first HWIC-16A module).

Access Server	Slot 3	Slot 2	Slot 1	Slot 0
2801 w/ 1x HWIC-16A	X			
2801 w/ 2x HWIC-16A	X		X	
2811 w/ 1x HWIC-16A	X			
2811 w/ 2x HWIC-16A	X	X		
2811 w/ 3x HWIC-16A	X	X	X	
2811 w/ 4x HWIC-16A	X	X	X	X

Option 1. Two (2) Cisco NIM-16A modules in a Cisco 4321 ISR can be used to provide 32 async lines in a standard rack. Configuration requires four (4) CAB-ASYNC-8 cables (3 for Cuatro 2U rack).



Option 2. Two (2) Cisco HWIC-16A modules in a Cisco 2901/2811/2801 can be used to provide 32 async lines in a standard rack. Configuration requires four (4) CAB-HD8-ASYNC cables (3 for Cuatro 2U rack).



Option 3. One (1) Cisco NM-32A module can be used in a Cisco 2600 router to provide 32 async lines in a standard rack. This configuration requires 4 CAB-OCTAL-ASYNC cables (3 for Cuatro 2U rack).

> This hardware in this configuration has reached end-of-sale. It is only recommended for those sites that may already have them.

"Octopus" cables are used to connect between the access server module and the console port of each lab device. CAB-HD8-ASYNC is the cable shown here.

> Each supported line card type uses a different octopus cable type. Cisco octopus cables are 10 feet, which is required for standard rack layout (access server at top of rack). Third party cables may be shorter. Be sure to specify 10 foot cables.

Line Card	Cable Type
NIM-16A	CAB-ASYNC-8
HWIC-16A	CAB-HD8-ASYNC
NM-32A	CAB-OCTAL-ASYNC

5.3 Power Distribution Unit Requirements

The power of each managed device in a NETLAB+ real equipment pod is connected to a power distribution unit (PDU).

The PDU provides three functions:

- Reboot devices during NETLAB+ automated operations
- Allow users to control the power of a lab device (making password recovery possible)
- Power off devices when not in use to reduce energy and cooling requirements

Your NETLAB+ system will require one or more power distribution units, depending on the number and type of real equipment pods you add to your system.

NETLAB+ supports the following PDU devices for use with the standard rack layouts.

Model	Outlets	Voltage	Input (Plug)	Output (Receptacles)	Notes
APC AP7900	8	115 VAC	NEMA 5-15P	(8) NEMA 5-15R	1,2
APC AP7920	8	208-230 VAC	IEC-320 C14	(8) IEC 320 C13	1,2
APC AP9211	8	115 VAC	NEMA 5-15P	(8) NEMA 5-15R	3
APC AP9212	8	208-230 VAC	IEC-320 C14	(8) IEC 320 C13	3
APC AP7902	16	100-120 VAC	NEMA L5-30P	16) NEMA 5-20R	3
APC AP7922	16	220-240 VAC	IEC 309 32A 2P+E	(16) IEC 320 C13	2,3
APC AP7954	24	220-240 VAC	EC 309 16A 2P+E	(21) IEC 320 C13 (3) IEC 320 C19	3
CyberPower PDU41001	8	115 VAC	NEMA 5-15P	(8) NEMA 5-15R	4

1. Recommended for new purchases.
2. APC 79*XX*B Users: Please see configuration details specific to APC 79XXB from APC on page 5.
3. Older version, end-of-sale.
4. Unsupported.

APC AP7900 supports 120 VAC and provides NEMA-5-15P outlets.

APC AP7912 supports 208-230 VAC and provides IEC 320 C13 outlets.

6 Preparing NETLAB+ VE for Cisco Courses

In this section, we discuss the steps needed to enable Cisco content on your NETLAB+.

6.1 Enabling Cisco Networking Academy Content

Contact NDG technical support to enable support for Cisco Networking Academy Content. NDG will perform the following actions:

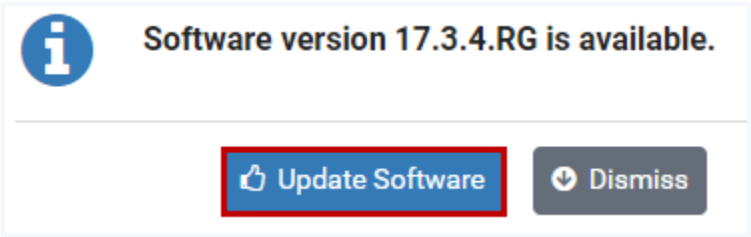
1. Verify your institution's membership in the Cisco Networking Academy.
2. Enable a NETLAB+ VE software upgrade that supports real lab equipment (17.3.0 or higher)
3. Enable Cisco Networking Academy courses to be installed on

6.2 Update NETLAB+ Software

Once NDG has confirmed completion of the tasks from the previous section, you should check for the availability of an updated NETLAB+ VE software version (an updated software version is necessary for the support of real equipment).

Verify NETLAB+ is running 17.3.0 or higher. Version 17.3.0 is required to support real lab equipment. If no upgrade to 17.3.0 or higher is available, contact NDG to ensure the software update for real equipment is enabled on your system.

1. Select **Software Updates** on the panel located on the right side of the Administrator Home page.
2. If your NETLAB+ system does not have the latest available software, a message will alert you that a new version is available. Select the option to **Update Software** to perform the upgrade.

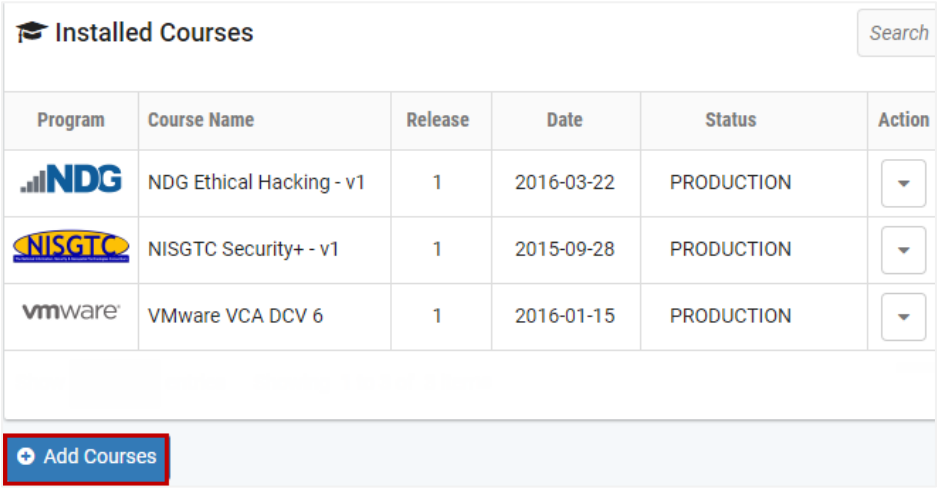


As always, make a backup or take a snapshot of the NETLAB+ VE virtual machine before upgrading software.

6.3 Loading Cisco Content from the Course Catalog

The NETLAB+ Course Manager acts as a course catalog, listing all courses (topic-based lab libraries) that are available from NDG. Installing the courses you plan to use is necessary in order to make available on your NETLAB+ system, the lab designs and pod designs needed in order to install your pods.

1. From the Administrator Home page, select **Course Manager**.
2. The courses currently installed, if any, will be displayed. Click **Add Courses**.



3. The Add Course list will be displayed. This list includes a variety of courses available through NETLAB+. Continue to the subsections below, where we will demonstrate the process of adding courses.

> The Course Manager displays all lab libraries available. Some of the course materials listed, developed in partnership with a vendor, require your organization to join the vendor's academy program in order to be eligible to access the course.

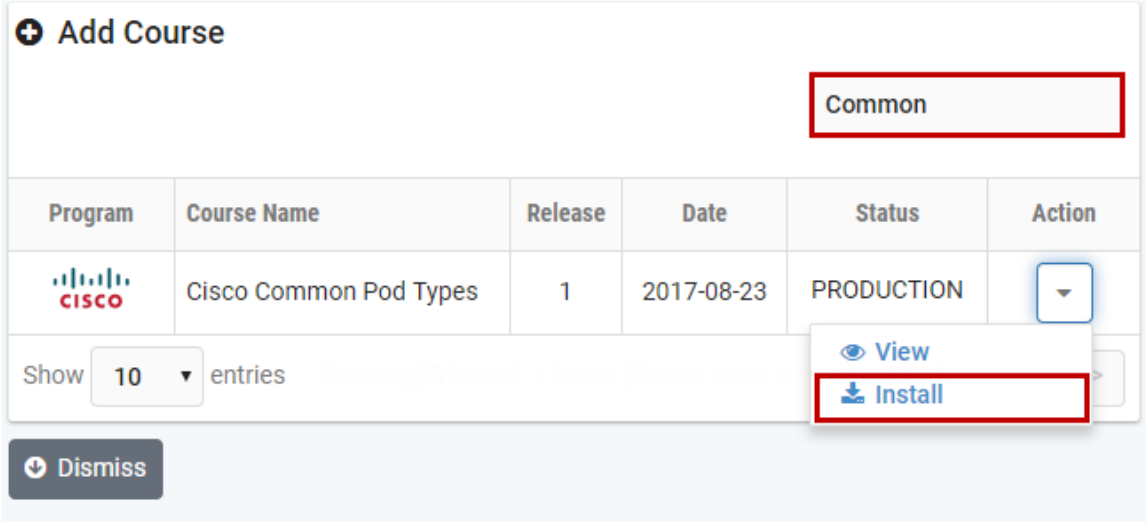
6.3.1 Adding the Cisco Common Pod Types Course

If this is your first time adding real equipment to your NETLAB+ system, you must install the *Cisco Common Pod Types* course. This course provides:

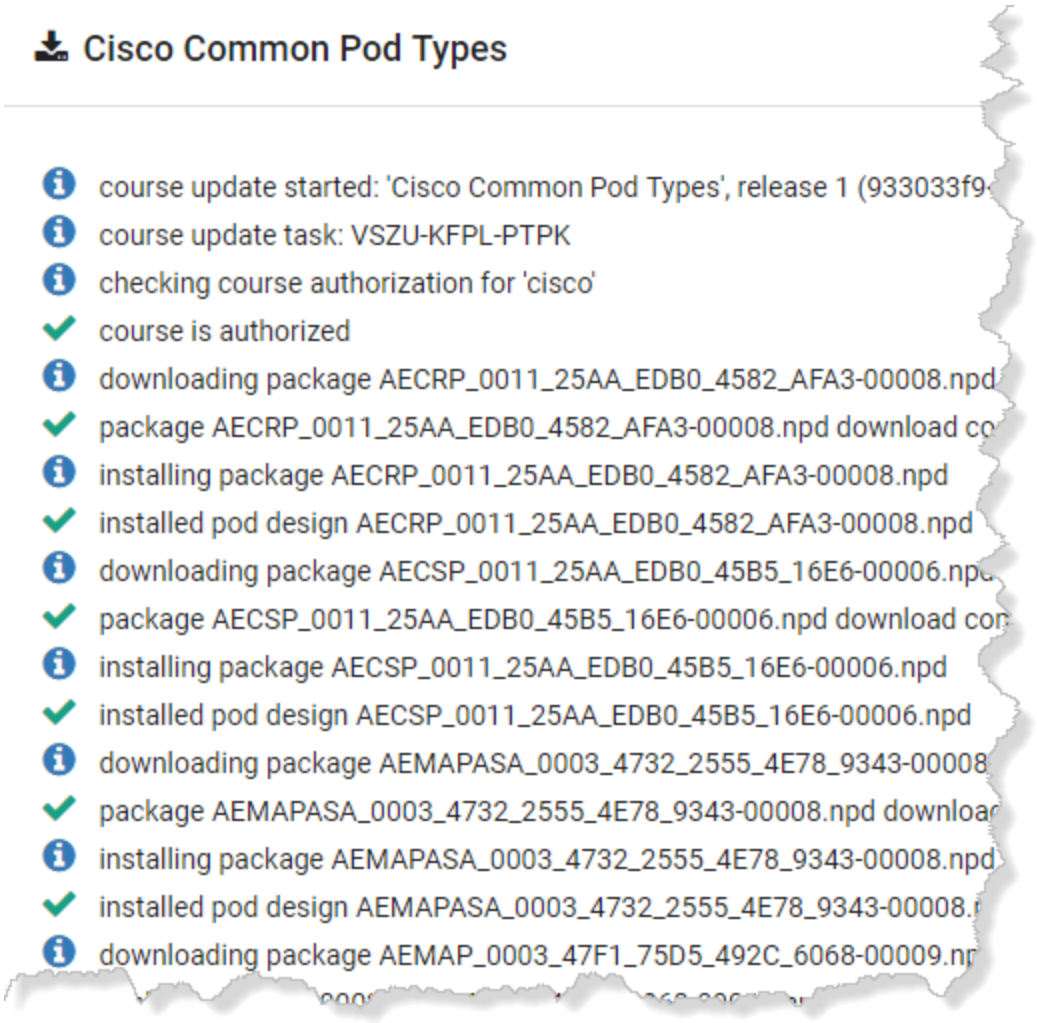
- The four standard topologies for real equipment (MAP, MAPASA, CRP, CSP).
- Four generic lab designs that contain non-specific lab exercises for each of the topologies.

1. From the Add Course page, enter the word **"Common"** into the search box to locate the *Cisco Common Pod Types* course.
2. On the Action dropdown, select **Install**.

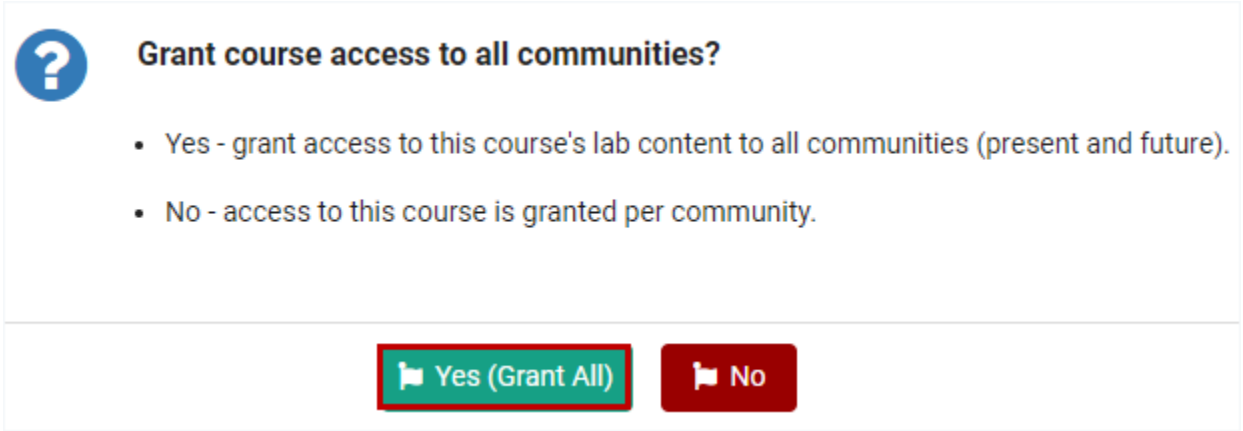
The option to install the *Cisco Common Pod Types* course is available only to organizations who are members of the Cisco Networking Academy. Contact NDG Support to verify your organization's membership if the Install option is not available on your system.



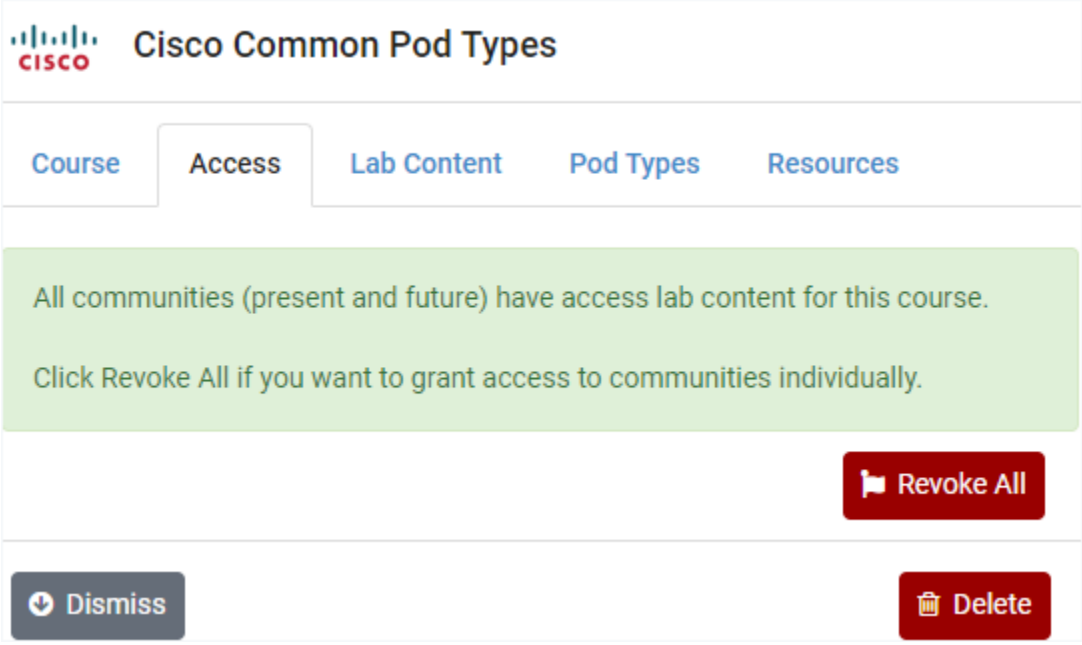
3. You will see the course installation in progress. This will include verification of course authorization and installation of packages, lab designs, and pod designs. When the course installation is complete, click **Next**.



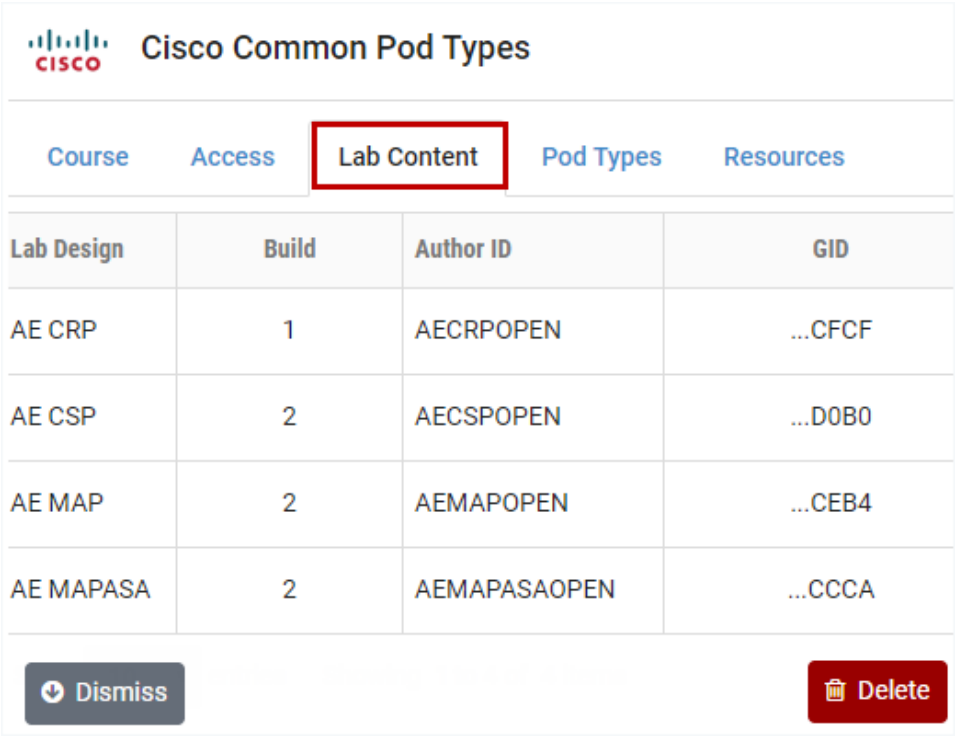
4. You will be prompted to grant access to this course to all communities or per community. If your system has only one community (as in this example), select **Yes (Grant All)**.



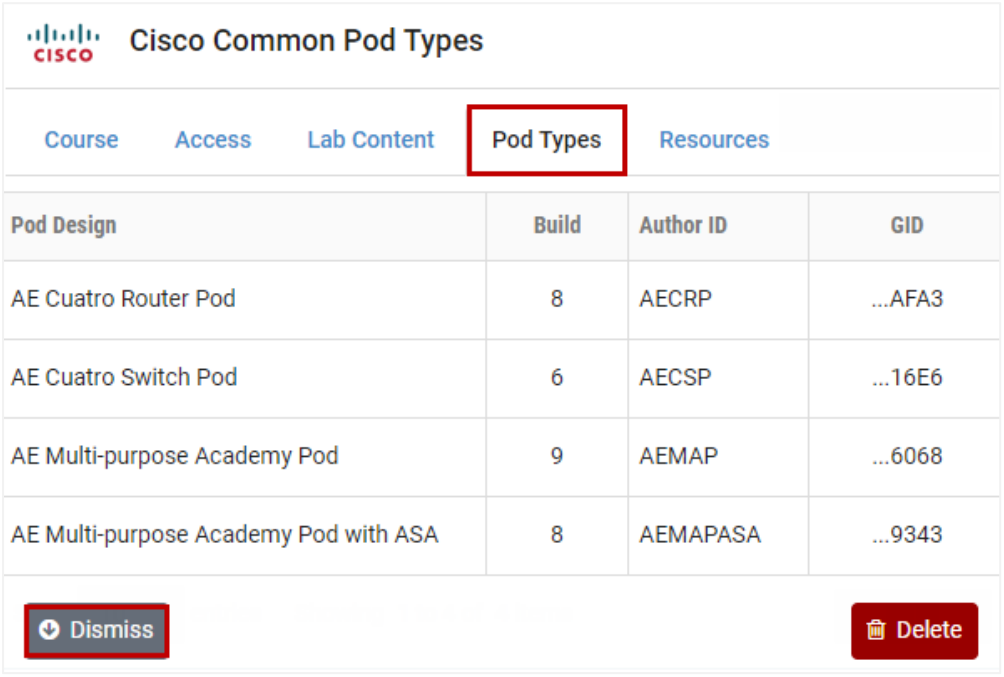
5. The course page will be displayed, where you can modify your course access selection if needed or select a different tab to view more information about the course. You can return to this page any time by selecting the course in the list of installed courses.



6. For your reference, let's take a look at the **Lab Content** tab. Notice the four lab designs included, one for each of the real equipment topology types. These may be used by instructors to enable lab reservations not tied to a specific exercise. For example, if an instructor enables “AE MAP” content for a class, the students of that class can reserve a MAP pod with no content-specific lab exercise.



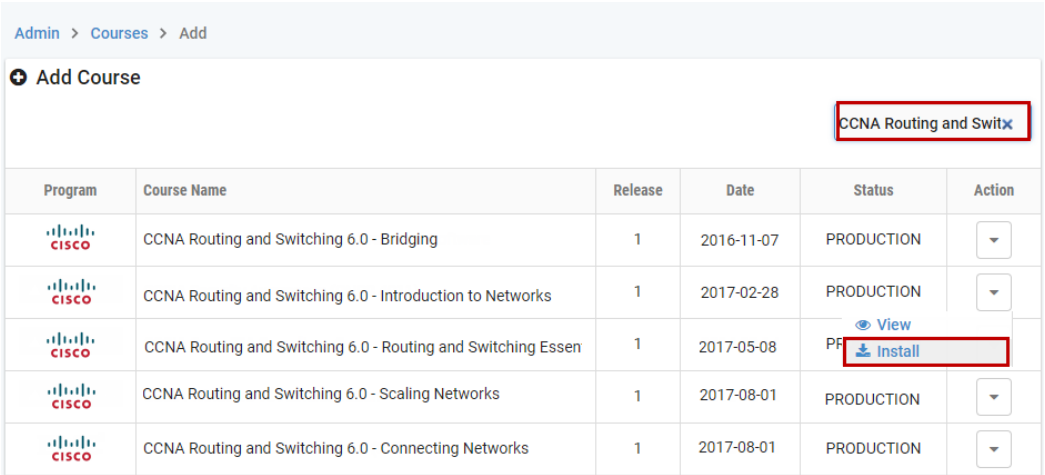
7. We will also take a quick look at the four real equipment pod types included with this course by selecting the **Pod Types** tab. Click **Dismiss**.



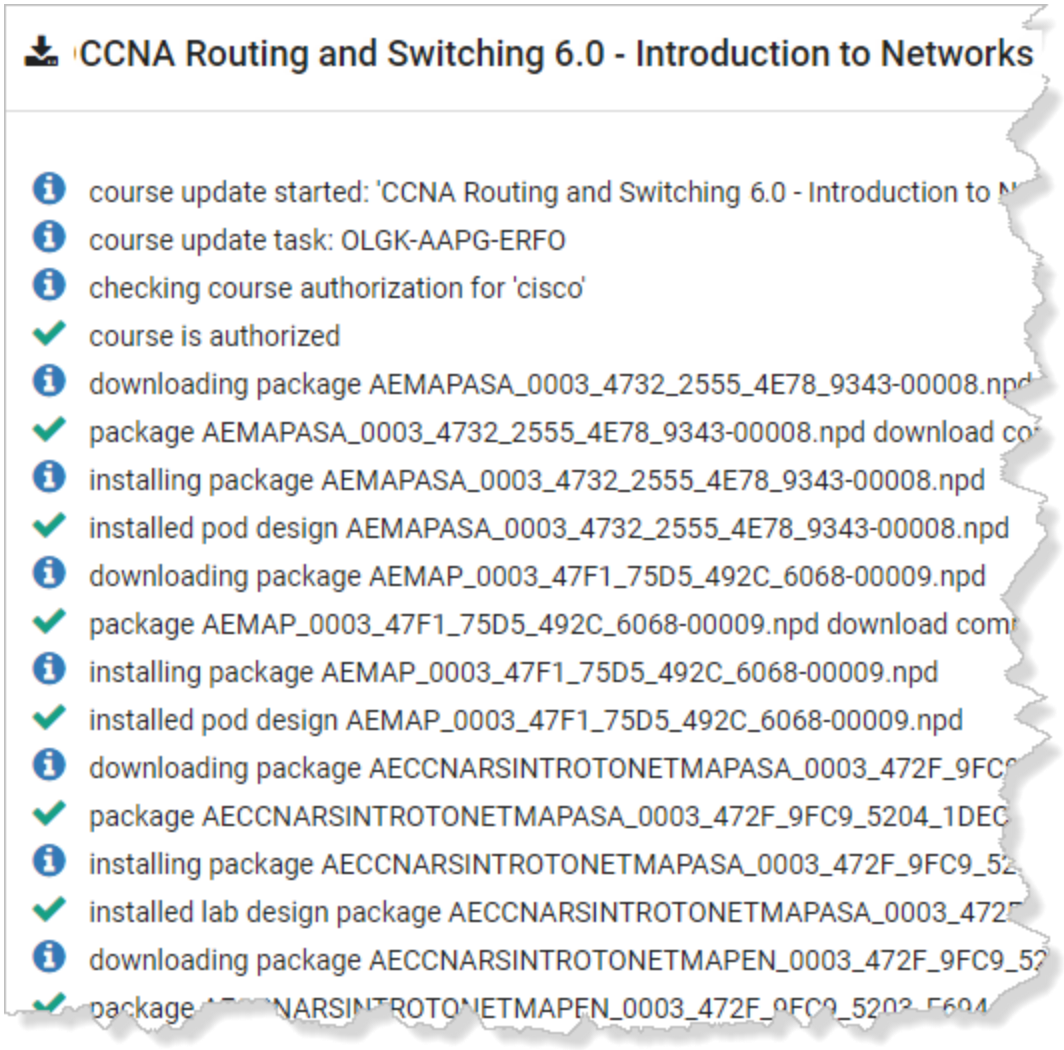
6.3.2 Adding a Course

We will add one of the Cisco courses supported by the Multi-purpose Academy Pod with ASA (MAPASA), following the same process shown in the previous section to add the *Cisco Common Pod Types* course.

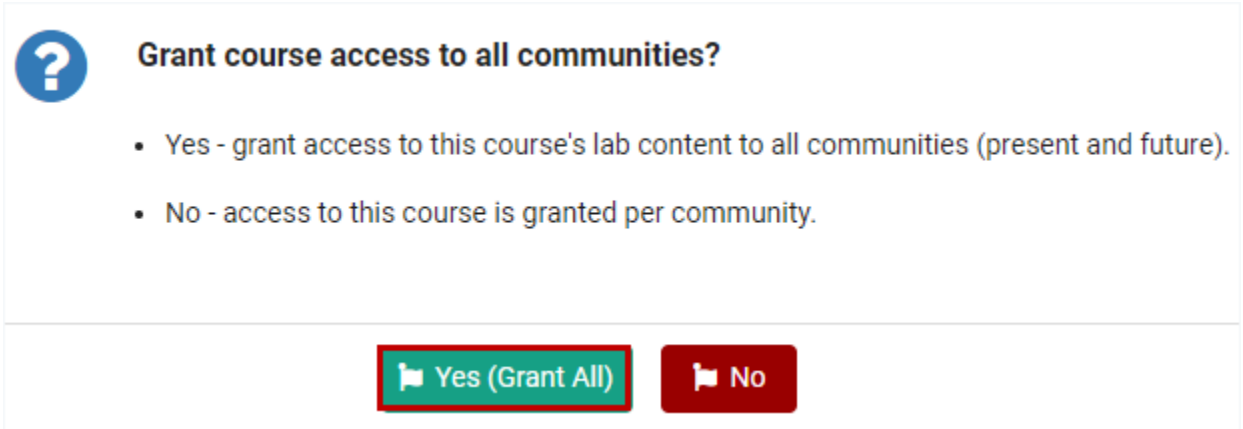
1. Select the Add Courses page, **Admin > Courses > Add**.
2. To make the course we want easier to locate in the course list, enter "**CCNA Routing and Switching 6.0"** in the search box.
3. Select **Install** on the Action dropdown for the *CCNA Routing and Switching 6.0 - Introduction to Networks* course.



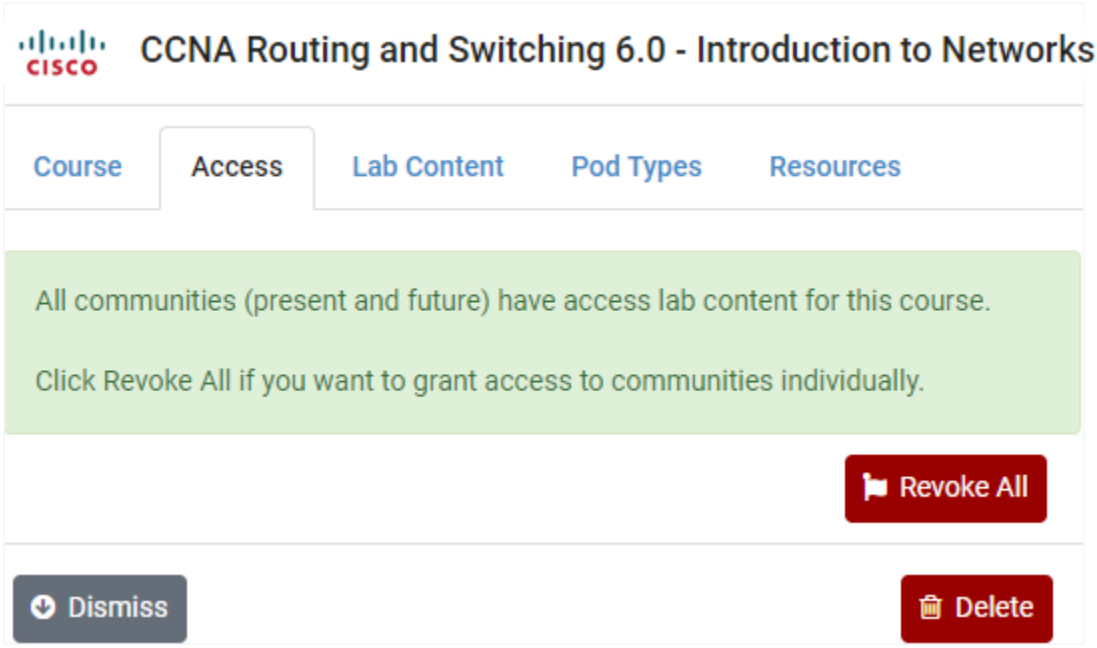
4. You will see the course installation in progress. This will include verification of course authorization and installation of packages, lab designs, and pod designs.



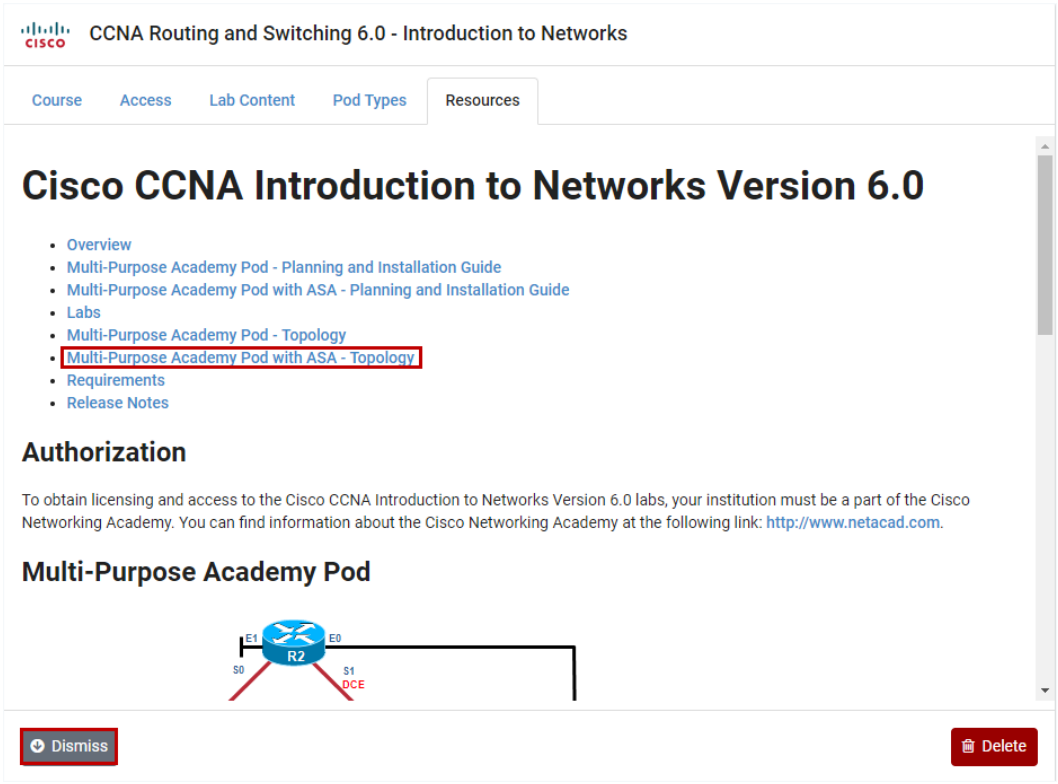
5. You will be prompted to grant access to the course's lab content to all communities or to grant access per community. For this example, we will select **Yes (Grant All).**



6. The course page will be displayed, where you can modify your course access selection if needed or select a different tab to view more information about the course. You can return to this page any time by selecting the course in the list of installed courses.

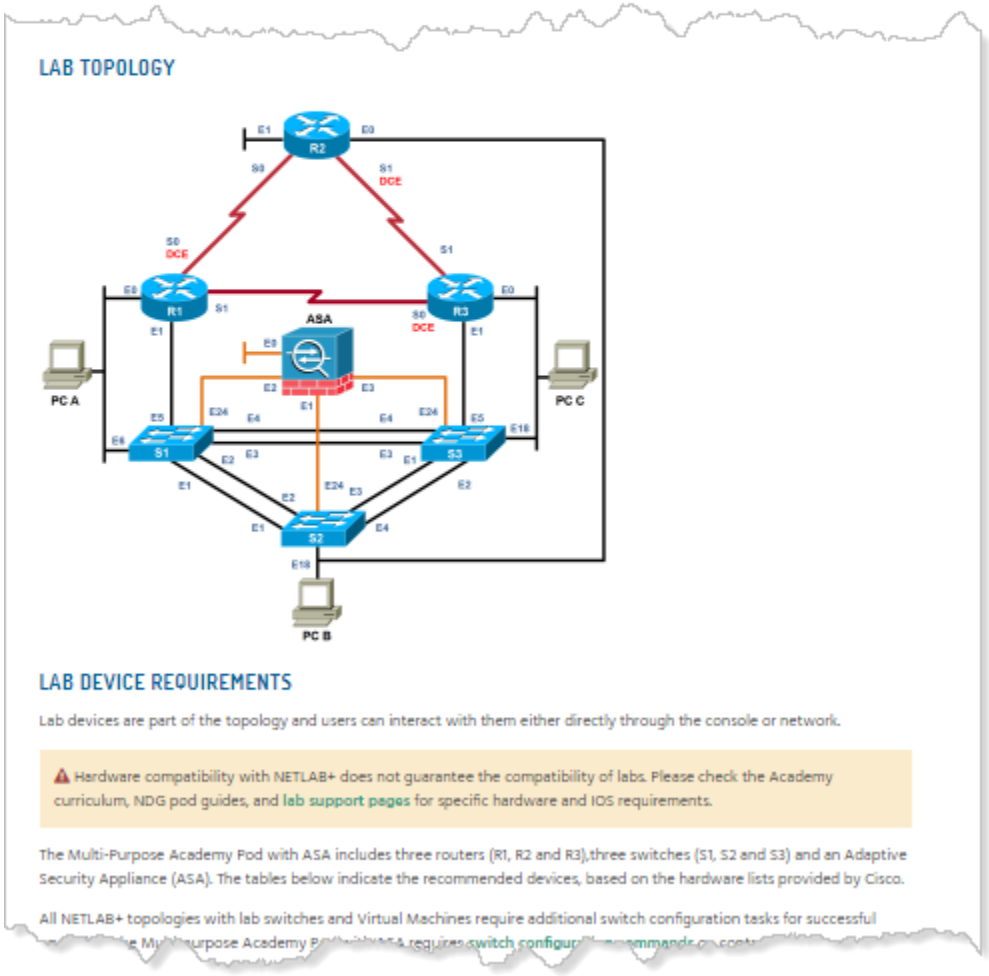


7. For your reference, we will examine the information available on the **Resources** tab. This page includes details on the compatible topologies for the course. We will be installing the MAPASA. Click the link to display the quick reference page for the MAPASA.



8. The quick reference page includes information on supported courses, lab devices, control devices, and the topology diagram. As we have discussed in the first section of this guide, the MAPASA includes several physical lab devices, including 3 routers (R1, R2, and R3), 3 switches (S1, S2, and S3), and an ASA security device. The PCs shown are virtualized.

Be aware that some courses have specific requirements for compatible lab devices and minimum IOS. These details may be found on the pod quick reference page and in the pod installation guide (linked on the quick reference page).

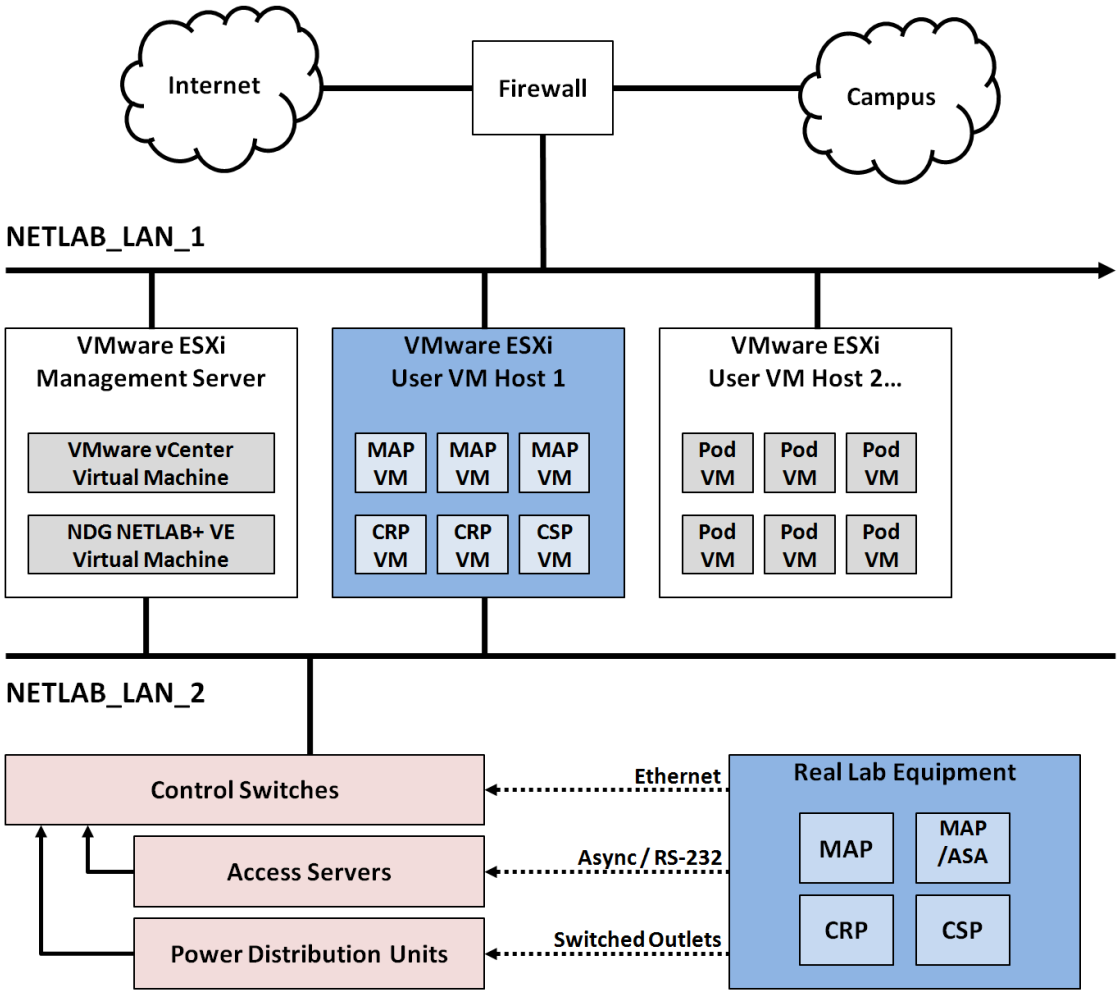


7 Preparing Infrastructure to Support Real Equipment

In a standard NETLAB+ VE installation, each VMware host server attaches to a routable network NETLAB_LAN_1. This is also referred to as the *outside network*.

In a real equipment installation, a second non-routable network NETLAB_LAN_2. This is also called the *inside network*.

	Outside Network	Inside Network
LAN Name	NETLAB_LAN_1	NETLAB_LAN_2
Virtual Switch Names	vSwitch0	vSwitch1
Network Addresses	Customer specified	169.254.0.0 / 24 169.254.1.0 / 24
NETLAB+ VE IP Address	Customer specified	169.254.1.1 (primary) 169.254.0.254 (secondary)



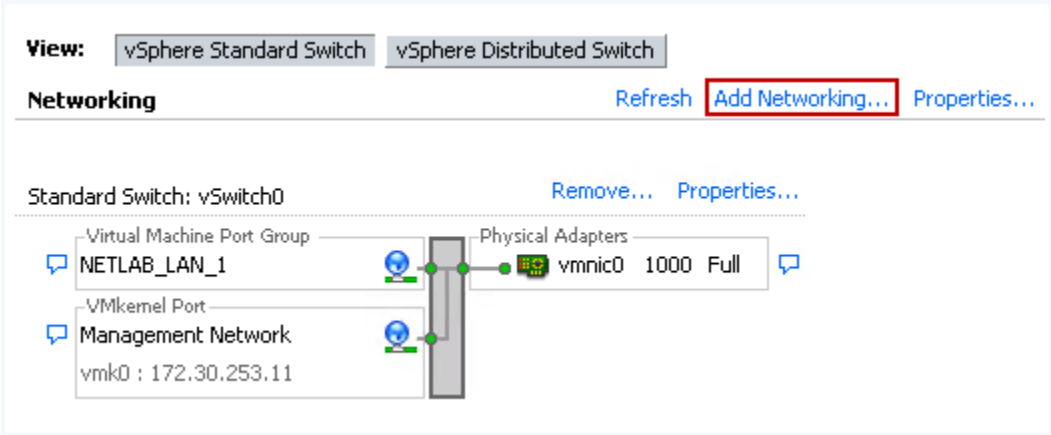
7.1 Create Inside Network on Management Server and ESXi Hosts

Create a virtual network **NETLAB_LAN_2** on a new virtual switch named **vSwitch1** on the following VMware ESXi hosts:

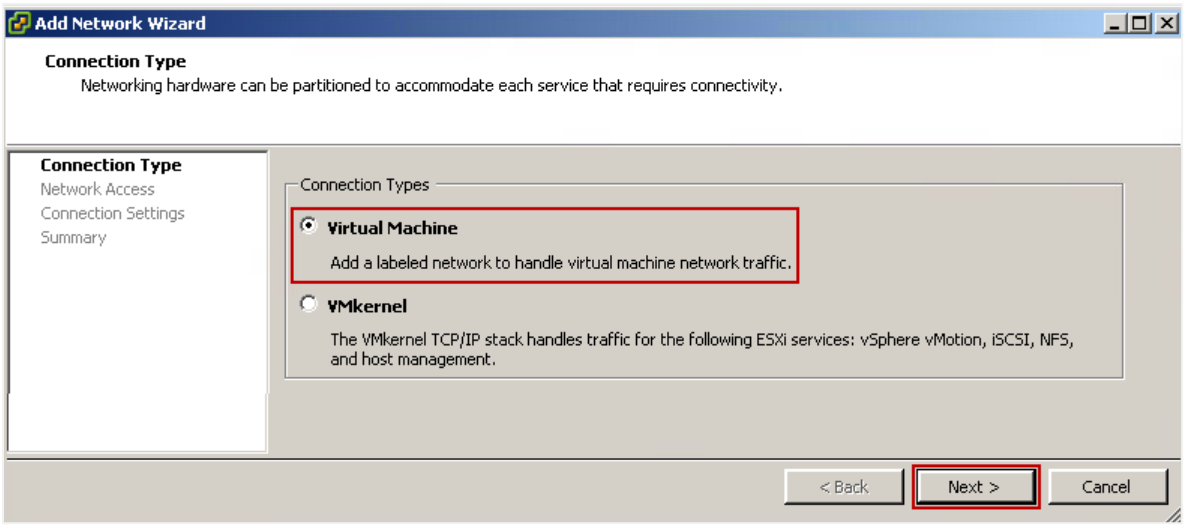
- The ESXi host designated as the VMware Management Server.
- Any ESXi host that runs virtual machines for real equipment pods.

Step 1. Create vSwitch1.

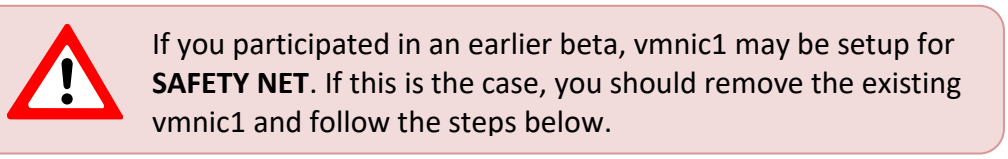
1. Click on **Add Networking**…



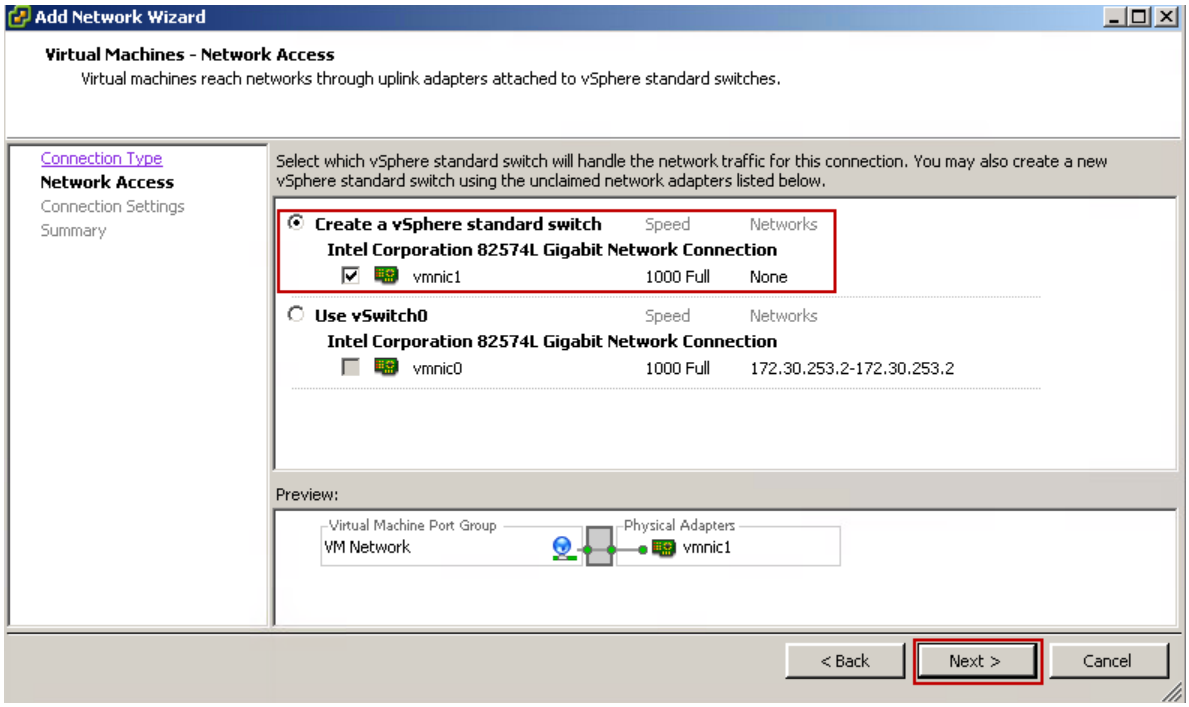
2. Make sure **Virtual Machine** is selected and click **Next**.



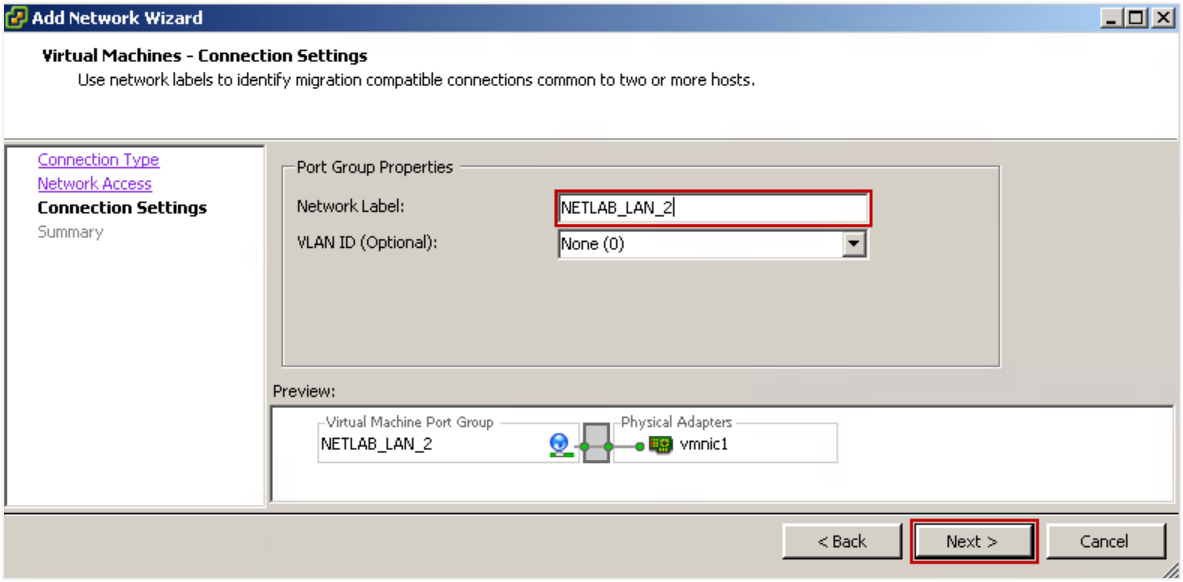
3. Make sure **Create a vSphere standard switch** is selected, along with the checkbox for **vmnic1**. Click **Next** to continue.



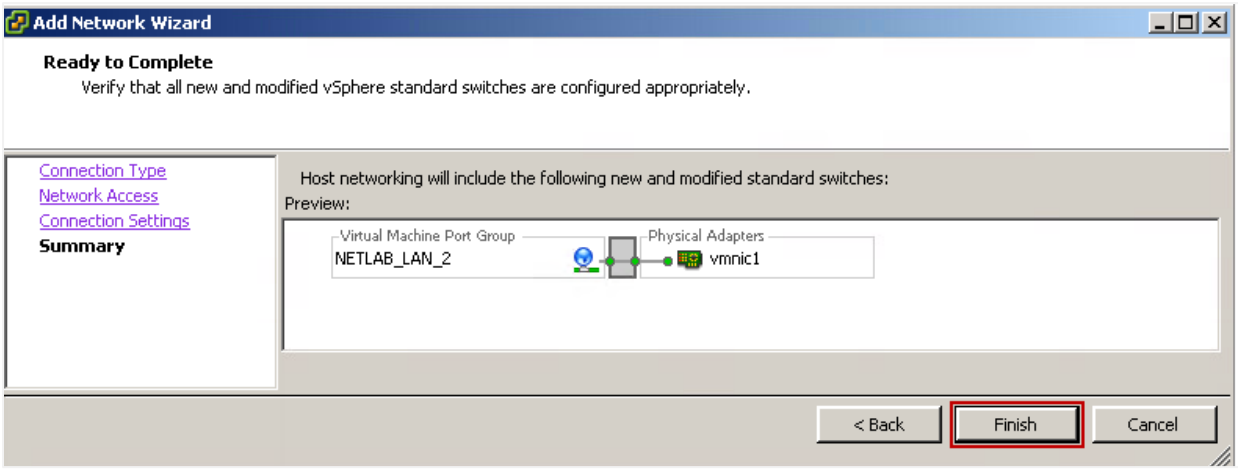
If you participated in an earlier beta, vmnic1 may be setup for **SAFETY NET**. If this is the case, you should remove the existing vmnic1 and follow the steps below.



4. Set the Network Label to **NETLAB_LAN_2**. Click **Next** to continue.



5. Review the information and click **Finish**.

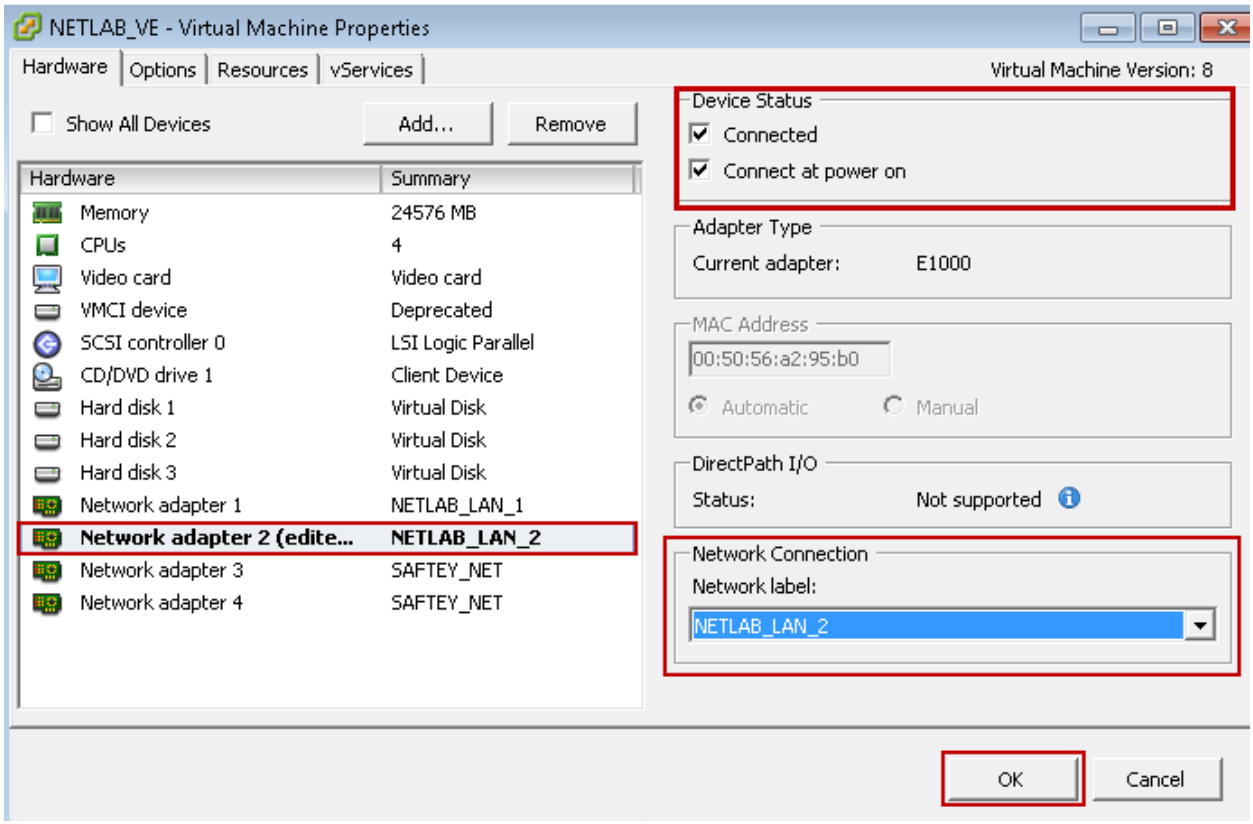


If you removed **vSwitch1** earlier for **SAFETY NET**, be sure to add **vSwitch2** with a name of **SAFETY NET.**

7.2 Attach NETLAB+ VE to NETLAB_LAN_2

On the management server, bind Network Adapter 2 on the NETLAB+ VE virtual machine to NETLAB_LAN_2.

1. Select **NETLAB_VE** on the management server and click **Edit Settings.**
2. Select **Network Adapter 2**, and make sure the Network Connection is set to **NETLAB_LAN_2**.
3. Make sure that the Device Status checkboxes for **Connected** and **Connect at power on** are selected.
4. Click **OK** to save changes.



7.3 Install Master Control Switch

Physically rack the master control switch (Control Switch 1). This is typically placed in the server rack in proximity to the ESXi hosts. The master control switch is preferably powered by a UPS power source. For master control switch requirements, see *Master Control Switch*.

> Erase the configuration and vlan.dat of a control switch before connecting Ethernet ports to other devices or servers. Once the configuration is clean, the master control switch can be safely connected to ESXi host servers.

7.4 Add Master Control Switch to NETLAB+ VE

Using the procedure in *Control Switches*, add the master control switch to NETLAB+ VE.

> The master control switch is always Control Switch 1 (CS1).

NETLAB+ VE automatically configures control switch ports based on role. This differs from NETLAB+ AE/PE, where control ports are configured manually.

Port	Peer Name	Role
GigabitEthernet0/1	Management Server	Virtual Machine Server
GigabitEthernet0/2	Primary ESXi Hosts	Virtual Machine Server
FastEthernet0/22	Secondary ESXi Hosts (opt)	Virtual Machine Server
FastEthernet0/23	Secondary ESXi Hosts (opt)	Virtual Machine Server
FastEthernet0/24	Secondary ESXi Hosts (opt)	Virtual Machine Server
FastEthernet0/1	(not used)	Unmanaged
FastEthernet0/2	Control Switch 2	Other Control Switch
FastEthernet0/3	Control Switch 3	Other Control Switch
FastEthernet0/4	Control Switch 4	Other Control Switch
FastEthernet0/5	Control Switch 5	Other Control Switch
FastEthernet0/6	Control Switch 6	Other Control Switch
FastEthernet0/7	Control Switch 7	Other Control Switch
FastEthernet0/8	Control Switch 8	Other Control Switch
FastEthernet0/9	Control Switch 9	Other Control Switch
FastEthernet0/10	Control Switch 10	Other Control Switch
FastEthernet0/11	(not used)	Unmanaged
FastEthernet0/12	Control Switch 12	Other Control Switch
FastEthernet0/13	Control Switch 13	Other Control Switch
FastEthernet0/14	Control Switch 14	Other Control Switch
FastEthernet0/15	Control Switch 15	Other Control Switch
FastEthernet0/16	Control Switch 16	Other Control Switch
FastEthernet0/17	Control Switch 17	Other Control Switch
FastEthernet0/18	Control Switch 18	Other Control Switch
All others	(not used)	UNMANAGED

Control switch ports may be set to UNMANAGED if they are not used.

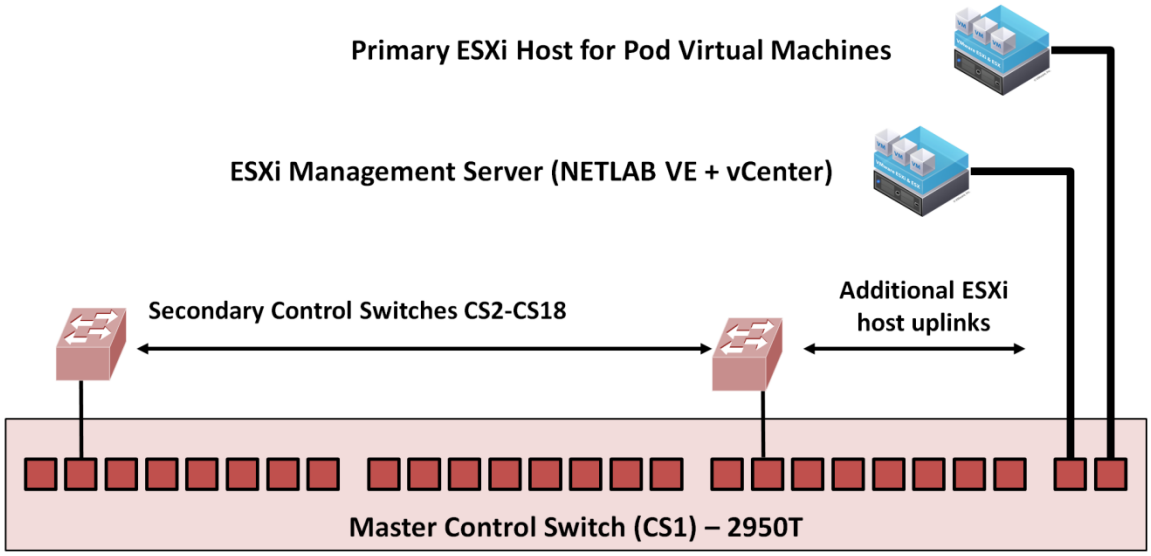
7.5 Connect ESXi Host Servers to Inside Network

Physically cable the master control switch to the relevant ESXi servers as follows.

ESXi Host	Master Control Switch Interface
Management Server	GigabitEthernet0/1
Virtual Machine Host 1	GigabitEthernet0/2
Virtual Machine Host 2 (if required)	FastEthernet0/22
Virtual Machine Host 3 (if required)	FastEthernet0/23
Virtual Machine Host 4 (if required)	FastEthernet0/24

Each connected ESXi hosts server will now have two network connections: one connection to the outside network and one connection to the inside network via the master control switch.

Typically, you will be able to place all virtual machines for real equipment pods on one host server (Virtual Machine Host 1 in the table). If you have a large installation (5 or more standard racks), virtual machines may be spread across two or more hosts.



8 Adding Equipment Racks

This section describes the procedures for adding standard equipment racks.

8.1 Common Rack Procedures and Considerations

The four standard rack layouts all share the same setup procedures and considerations.

8.2 Rack Numbering Scheme

Each rack should be labeled as follows:

Rack Name	Type	Contains
Rack 1	Master Rack	ESXi Management Server ESXi Hosts Servers Master Control Switch
Rack 2 **...** **Rack 8**	One of... MAP 1U MAP 2U CUATRO 1U CUATRO 2U	Lab Equipment Access Server Secondary Control Switch(es) PDUs

8.2.1 Power Requirements

There should be one or two dedicated circuits in each rack with a suitable capacity to power the equipment in the rack. These circuits should have feeder power strips with several outlets for control devices. The following balanced layout with two circuits is recommended.

Circuit 1	Circuit 2
Access Server	
Control Switch 1	Control Switch 2 (when using 24 port switches)
PDU 1	PDU 3
PDU 2	PDU 4

An Uninterrupted Power Supply (UPS) is recommended, particularly in areas where blackouts are common. If UPS is not feasible for the entire rack, consider a small UPS to power access servers and control switches.

If feeder power strips are mounted vertically, the standard rack layouts should work as depicted. If feeder power strips are mounted horizontally and consume rack space, you can do one of the following:

- Place power strips in the designated open rack spaces in the layout.
- Create 2U for power strips at the bottom of the rack by moving equipment up into the designated empty spaces.

8.3 Clear Configuration of Access Server and Control Switches

When reusing equipment such as access servers and control switches, it is recommended that any previous configuration is cleared before connecting to other devices. This can be done by issuing the IOS commands, **write erase** and **reload.**

8.4 Mount Equipment

At this time, you can mount both control equipment and lab devices as depicted in the selected rack layout. Specific details for each layout will be provided in subsequent sections.

8.5 Secondary Control Switches

Connect and configure secondary control switches in standard racks according to the following best practices. Recall that rack 1 is the master rack and control switch 1 is the master control switch.

When using **one 48-port control switch** per standard rack:

Rack	Control Switch ID	Uplink Port on Any Secondary Control Switch	Uplink Port on Master Control Switch
2	2	GigabitEthernet0/1	FastEthernet0/2
3	3	GigabitEthernet0/1	FastEthernet0/3
4	4	GigabitEthernet0/1	FastEthernet0/4
5	5	GigabitEthernet0/1	FastEthernet0/5
6	6	GigabitEthernet0/1	FastEthernet0/6
7	7	GigabitEthernet0/1	FastEthernet0/7
8	8	GigabitEthernet0/1	FastEthernet0/8

When using **two 24-port control switches** per standard rack:

Rack	Control Switch ID	Uplink Port on Any Secondary Control Switch	Uplink Port on Master Control Switch
2	2	GigabitEthernet0/1	FastEthernet0/2
	12	GigabitEthernet0/1	FastEthernet0/12
3	3	GigabitEthernet0/1	FastEthernet0/3
	13	GigabitEthernet0/1	FastEthernet0/13
4	4	GigabitEthernet0/1	FastEthernet0/4
	14	GigabitEthernet0/1	FastEthernet0/14
5	5	GigabitEthernet0/1	FastEthernet0/5
	15	GigabitEthernet0/1	FastEthernet0/15
6	6	GigabitEthernet0/1	FastEthernet0/6
	16	GigabitEthernet0/1	FastEthernet0/16
7	7	GigabitEthernet0/1	FastEthernet0/7
	17	GigabitEthernet0/1	FastEthernet0/17
8	8	GigabitEthernet0/1	FastEthernet0/8
	18	GigabitEthernet0/1	FastEthernet0/18

Once the secondary control switches for the rack are cabled, add them to NETLAB+ VE, per Section 9.1.1.

> The port assignments and roles for secondary control switches vary by rack type. Specific guidance for each rack type is provided in subsequent sections.

8.6 Setup for MAP 1U or MAP 2U Racks

The following section is specific to MAP 1U or MAP 2U racks, containing MAP or MAPASA pods. The following steps should already be completed.

- MAP pod lab equipment racked according to MAP 1U or MAP 2U layout (described earlier).
- Secondary control switches added and configured in NETLAB+ VE.
- Access server added and configured in NETLAB+ VE.

8.6.1 MAP Rack - Control Switch Configuration

Connect MAP or MAPASA pods to the rack's secondary control switch(es) and configure control switch port roles per the following tables.

When using a single 48-port control switch in the rack:

Control Switch		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD A	
1	Lab Device	R1	0/0
2	Lab Device	R2	0/0
3	Lab Device	R2	0/1
4	Lab Device	R3	0/0
5	Lab Device	S1	6
6	Lab Device	S2	11
7	Lab Device	S2	18
8	Lab Device	S3	18
9	Lab Device	ASA (optional)	0
10	Unmanaged	*No connection*	
		POD B	
11	Lab Device	R1	0/0
12	Lab Device	R2	0/0
13	Lab Device	R2	0/1
14	Lab Device	R3	0/0
15	Lab Device	S1	6
16	Lab Device	S2	11
17	Lab Device	S2	18
18	Lab Device	S3	18

Control Switch		Peer Device	
19	Lab Device	ASA (optional)	0
20	Unmanaged	*No connection*	
		POD C	
21	Lab Device	R1	0/0
22	Lab Device	R2	0/0
23	Lab Device	R2	0/1
24	Lab Device	R3	0/0
25	Lab Device	S1	6
26	Lab Device	S2	11
27	Lab Device	S2	18
28	Lab Device	S3	18
29	Lab Device	ASA (optional)	0
30	Unmanaged	*No connection*	
		POD D	
31	Lab Device	R1	0/0
32	Lab Device	R2	0/0
33	Lab Device	R2	0/1
34	Lab Device	R3	0/0
35	Lab Device	S1	6
36	Lab Device	S2	11
37	Lab Device	S2	18
38	Lab Device	S3	18
39	Lab Device	ASA (optional)	0
40	Unmanaged	*No connection*	
		Control Devices	
41	PDU	PDU A	0
42	PDU	PDU B	0
43	PDU	PDU C	0
44	PDU	PDU D	0
45	Unmanaged	*No connection*	
46	Unmanaged	*No connection*	
47	Unmanaged	*No connection*	
48	Access Server	Access Server	0/0
GigabitEthernet0/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet0/1	Unmanaged	*No connection*	

When using two (2) 24-port control switches in the rack:

Control Switch A		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD A	
1	Lab Device	R1	0/0
2	Lab Device	R2	0/0
3	Lab Device	R2	0/1
4	Lab Device	R3	0/0
5	Lab Device	S1	6
6	Lab Device	S2	11
7	Lab Device	S2	18
8	Lab Device	S3	18
9	Lab Device	ASA (optional)	0
10	Unmanaged	*No connection*	
		POD B	
11	Lab Device	R1	0/0
12	Lab Device	R2	0/0
13	Lab Device	R2	0/1
14	Lab Device	R3	0/0
15	Lab Device	S1	6
16	Lab Device	S2	11
17	Lab Device	S2	18
18	Lab Device	S3	18
19	Lab Device	ASA (optional)	0
20	Unmanaged	*No connection*	
		Control Devices	
21	PDU	PDU A	Ethernet
22	PDU	PDU B	Ethernet
23	PDU	PDU C	Ethernet
24	PDU	PDU D	Ethernet
GigabitEthernet0/0	Control Switch	Control Switch 1	2 – 18
GigabitEthernet0/1	Access Server	Access Server	0/0

Control Switch B		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD C	
1	Lab Device	R1	0/0
2	Lab Device	R2	0/0
3	Lab Device	R2	0/1
4	Lab Device	R3	0/0
5	Lab Device	S1	6
6	Lab Device	S2	11
7	Lab Device	S2	18
8	Lab Device	S3	18
9	Lab Device	ASA (optional)	0
10	Unmanaged	*No connection*	
		POD D	
11	Lab Device	R1	0/0
12	Lab Device	R2	0/0
13	Lab Device	R2	0/1
14	Lab Device	R3	0/0
15	Lab Device	S1	6
16	Lab Device	S2	11
17	Lab Device	S2	18
18	Lab Device	S3	18
19	Lab Device	ASA (optional)	0
20	Unmanaged	*No connection*	
		Control Devices	
21	Unmanaged	*No connection*	
22	Unmanaged	*No connection*	
23	Unmanaged	*No connection*	
24	Unmanaged	*No connection*	
GigabitEthernet0/0	Control Switch	Control Switch 1	2 – 18
GigabitEthernet0/1	Unmanaged	*No connection*	

8.6.2 MAP Rack – Normal PDU Configuration

Each MAP or MAPASA pod uses one 8-outlet PDU in a normal configuration. Connect each lab device to the PDU as follows. See also the alternate configuration for normal MAP pods.

Outlet	Lab Device
1	R1
2	R2
3	R3
4	S1
5	S2
6	S3
7	ASA (optional)
8	*Not connected*

8.6.3 MAP Rack – Alternate PDU Configuration

It is possible to eliminate one of the PDU devices in the rack if all four ASA devices are omitted. In this case, MAP pods A, C, and D are cabled normally per the previous section, and MAP Pod B can be split across three PDUs on outlets 7 and 8 as follows:

PDU/Outlet	POD B / Lab Device
A / 7	R1
A / 8	R2
B / 7	R3
B / 8	S1
C / 7	S2
C / 8	S3

The alternate PDU configuration assumes power cords for Pod B will reach the three PDU devices. Check cable length and adjust PDU placement accordingly.

8.6.4 MAP Rack - Access Server Configuration

Connect lab devices to the access server per the following table.

- Port numbers represent physical connections.
- Line numbers represent logical connections and will be used later in the pod setup process.

	Cisco 4321 (2) NIM-16A		Cisco 2901 (2) HWIC-16A		Cisco 2600 (1) NM-32A	
Lab Device	**Port**	**Line**	**Port**	**Line**	**Port**	**Line**
POD A						
R1	0/1/0	2	0/0/0	3	1/0	33
R2	0/1/1	3	0/0/1	4	1/1	34
R3	0/1/2	4	0/0/2	5	1/2	35
S1	0/1/3	5	0/0/3	6	1/3	36
S2	0/1/4	6	0/0/4	7	1/4	37
S3	0/1/5	7	0/0/5	8	1/5	38
ASA (optional)	0/1/6	8	0/0/6	9	1/6	39
Not connected	0/1/7	9	0/0/7	10	1/7	40
POD B						
R1	0/1/8	10	0/0/8	11	1/8	41
R2	0/1/9	11	0/0/9	12	1/9	42
R3	0/1/10	12	0/0/10	13	1/10	43
S1	0/1/11	13	0/0/11	14	1/11	44
S2	0/1/12	14	0/0/12	15	1/12	45
S3	0/1/13	15	0/0/13	16	1/13	46
ASA (optional)	0/1/14	16	0/0/14	17	1/14	47
Not connected	0/1/15	17	0/0/15	18	1/15	48

POD C						
R1	0/2/0	26	0/1/0	18	1/16	49
R2	0/2/1	27	0/1/1	20	1/17	50
R3	0/2/2	28	0/1/2	21	1/18	51
S1	0/2/3	29	0/1/3	22	1/19	52
S2	0/2/4	30	0/1/4	23	1/20	53
S3	0/2/5	31	0/1/5	24	1/21	54
ASA (optional)	0/2/6	32	0/1/6	25	1/22	55
Not connected	0/2/7	33	0/1/7	26	1/23	56
POD D						
R1	0/2/8	34	0/1/8	27	1/24	57
R2	0/2/9	35	0/1/9	28	1/25	58
R3	0/2/10	36	0/1/10	29	1/26	59
S1	0/2/11	37	0/1/11	30	1/27	60
S2	0/2/12	38	0/1/12	31	1/28	61
S3	0/2/13	39	0/1/13	32	1/29	62
ASA (optional)	0/2/14	40	0/1/14	33	1/31	63
Not connected	0/2/15	41	0/1/15	34	1/31	64

8.6.5 Intra-Pod Cabling for MAP Pods

The following additional connections are made between **lab devices** in a MAP or MAPASA pod. Ignore ASA connections in the table for regular MAP pod (without ASA).

> Control device connections are not included in this table.

From Device	From Interface	From Cable	To Cable	To Device	To Interface
Required Intra-pod Cabling					
R1	Serial0/0	V.35 Female DCE	V.35 Male DTE	R2	Serial0/0
R2	Serial0/1	V.35 Female DCE	V.35 Male DTE	R3	Serial0/1
R3	Serial0/0	V.35 Female DCE	V.35 Male DTE	R1	Serial0/1
S1	Port 1	Cat5e		S2	Port 1
S1	Port 2	Cat5e		S2	Port 2
S1	Port 5	Cat5e		R1	Ethernet0/1
S2	Port 3	Cat5e		S3	Port 1
S2	Port 4	Cat5e		S3	Port 2
S3	Port 3	Cat5e		S1	Port 3
S3	Port 4	Cat5e		S1	Port 4
S3	Port 5	Cat5e		R3	Ethernet0/1
Optional Intra-pod Cabling					
ASA	Ethernet1	Cat5e		S2	Port 24
ASA	Ethernet2	Cat5e		S1	Port 24
ASA	Ethernet3	Cat5e		S3	Port 24

8.7 Setup for Cuatro 1U Rack

The following section is specific to the Cuatro 1U rack layout, containing CRP and CSP pods. The following steps should already be completed.

- Lab equipment racked according to CUATRO 1U layout (described earlier).
- Secondary control switches added and configured in NETLAB+ VE.
- Access server added and configured in NETLAB+ VE.

8.7.1 Cuatro 1U Rack - Control Switch Configuration

Connect CRP pods and CSP pods to the rack's secondary control switch(es) and configure control switch port roles per the following tables.

When using a single 48-port control switch in the rack:

Control Switch		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD CRP A	
1	Lab Device	R1	0/0
2	Lab Device	R1	0/1
3	Lab Device	R2	0/0
4	Lab Device	R2	0/1
5	Lab Device	R3	0/0
6	Lab Device	R3	0/1
7	Lab Device	R4	0/0
8	Lab Device	R4	0/1
		POD CRP B	
9	Lab Device	R1	0/0
10	Lab Device	R1	0/1
11	Lab Device	R2	0/0
12	Lab Device	R2	0/1
13	Lab Device	R3	0/0
14	Lab Device	R3	0/1
15	Lab Device	R4	0/0
16	Lab Device	R4	0/1
		POD CRP C	
17	Lab Device	R1	0/0
18	Lab Device	R1	0/1
19	Lab Device	R2	0/0
20	Lab Device	R2	0/1
21	Lab Device	R3	0/0
22	Lab Device	R3	0/1
23	Lab Device	R4	0/0
24	Lab Device	R4	0/1

		POD CRP D	
25	Lab Device	R1	0/0
26	Lab Device	R1	0/1
27	Lab Device	R2	0/0
28	Lab Device	R2	0/1
29	Lab Device	R3	0/0
30	Lab Device	R3	0/1
31	Lab Device	R4	0/0
32	Lab Device	R4	0/1
		POD CSP A	
33	Lab Device	ALS1	Port 6
34	Lab Device	ALS2	Port 6
35	Lab Device	DLS1	Port 6
36	Lab Device	DLS2	Port 6
		POD CSP B	
37	Lab Device	ALS1	Port 6
38	Lab Device	ALS2	Port 6
39	Lab Device	DLS1	Port 6
40	Lab Device	DLS2	Port 6
		POD CSP C	
41	Lab Device	ALS1	Port 6
42	Lab Device	ALS2	Port 6
43	Lab Device	DLS1	Port 6
44	Lab Device	DLS2	Port 6
		POD CSP D	
45	Lab Device	ALS1	Port 6
46	Lab Device	ALS2	Port 6
47	Lab Device	DLS1	Port 6
48	Lab Device	DLS2	Port 6
		Control Devices	
GigabitEthernet1/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet1/1	Access Server	Access Server	0/0

When using two (2) 24-port control switches in the rack:

Control Switch A		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD CRP A	
1	Lab Device	R1	0/0
2	Lab Device	R1	0/1
3	Lab Device	R2	0/0
4	Lab Device	R2	0/1
5	Lab Device	R3	0/0
6	Lab Device	R3	0/1
7	Lab Device	R4	0/0
8	Lab Device	R4	0/1
		POD CRP B	
9	Lab Device	R1	0/0
10	Lab Device	R1	0/1
11	Lab Device	R2	0/0
12	Lab Device	R2	0/1
13	Lab Device	R3	0/0
14	Lab Device	R3	0/1
15	Lab Device	R4	0/0
16	Lab Device	R4	0/1
		POD CRP C	
17	Lab Device	R1	0/0
18	Lab Device	R1	0/1
19	Lab Device	R2	0/0
20	Lab Device	R2	0/1
21	Lab Device	R3	0/0
22	Lab Device	R3	0/1
23	Lab Device	R4	0/0
24	Lab Device	R4	0/1
		Control Devices	
GigabitEthernet1/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet1/1	Access Server	Access Server	0/0

Control Switch B		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD CRP D	
1	Lab Device	R1	0/0
2	Lab Device	R1	0/1
3	Lab Device	R2	0/0
4	Lab Device	R2	0/1
5	Lab Device	R3	0/0
6	Lab Device	R3	0/1
7	Lab Device	R4	0/0
8	Lab Device	R4	0/1
		POD CSP A	
9	Lab Device	ALS1	Port 6
10	Lab Device	ALS2	Port 6
11	Lab Device	DLS1	Port 6
12	Lab Device	DLS2	Port 6
		POD CSP B	
13	Lab Device	ALS1	Port 6
14	Lab Device	ALS2	Port 6
15	Lab Device	DLS1	Port 6
16	Lab Device	DLS2	Port 6
		POD CSP C	
17	Lab Device	ALS1	Port 6
18	Lab Device	ALS2	Port 6
19	Lab Device	DLS1	Port 6
20	Lab Device	DLS2	Port 6
		POD CSP D	
21	Lab Device	ALS1	Port 6
22	Lab Device	ALS2	Port 6
23	Lab Device	DLS1	Port 6
24	Lab Device	DLS2	Port 6
		Control Devices	
GigabitEthernet1/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet1/1	Unmanaged	*Not implemented*	

8.7.2 Cuatro 1U Rack - Control Switch Ports for PDU Devices

Due to the high density of lab devices in the Cuatro 1U rack, there are no control switch ports in the Cuatro 1U rack allocated to PDU devices. The PDU devices for a Cuatro 1U rack can be connected to a control switch in a different rack. This can be the master control switch or any secondary control switch with unused ports. Be sure to configure the PDU role on the control switch ports you choose.

8.7.3 Cuatro 1U Rack - PDU Configuration

Cable the PDU outlets per the following table.

Outlet	Lab Device
PDU A	
1	POD CRP A - R1
2	POD CRP A – R2
3	POD CRP A – R3
4	POD CRP A – R4
5	POD CRP B – R1
6	POD CRP B – R2
7	POD CRP B – R3
8	POD CRP B – R4
PDU B	
1	POD CRP C – R1
2	POD CRP C – R2
3	POD CRP C – R3
4	POD CRP C – R4
5	POD CRP D – R1
6	POD CRP D – R2
7	POD CRP D – R3
8	POD CRP D – R4

PDU C	
1	POD CSP A – ALS1
2	POD CSP A – ALS2
3	POD CSP A – DLS1
4	POD CSP A – DLS2
5	POD CSP B – ALS1
6	POD CSP B – ALS2
7	POD CSP B – DLS1
8	POD CSP B – DLS2
PDU D	
1	POD CSP C – ALS1
2	POD CSP C – ALS2
3	POD CSP C – DLS1
4	POD CSP C – DLS2
5	POD CSP D – ALS1
6	POD CSP D – ALS2
7	POD CSP D – DLS1
8	POD CSP D – DLS2

8.7.4 Cuatro 1U Rack - Access Server Configuration

Connect lab devices to the access server per the following table.

- Port numbers represent physical connections.
- Line numbers represent logical connections and will be used later in the pod setup process.

	Cisco 4321 (2) NIM-16A		Cisco 2901 (2) HWIC-16A		Cisco 2600 (1) NM-32A	
Lab Device	**Port**	**Line**	**Port**	**Line**	**Port**	**Line**
POD CRP A						
R1	0/1/0	2	0/0/0	3	1/0	33
R2	0/1/1	3	0/0/1	4	1/1	34
R3	0/1/2	4	0/0/2	5	1/2	35
R4	0/1/3	5	0/0/3	6	1/3	36
POD CRP B						
R1	0/1/4	6	0/0/4	7	1/4	37
R2	0/1/5	7	0/0/5	8	1/5	38
R3	0/1/6	8	0/0/6	9	1/6	39
R4	0/1/7	9	0/0/7	10	1/7	40
POD CRP C						
R1	0/1/8	10	0/0/8	11	1/8	41
R2	0/1/9	11	0/0/9	12	1/9	42
R3	0/1/10	12	0/0/10	13	1/10	43
R4	0/1/11	13	0/0/11	14	1/11	44
POD CRP D						
R1	0/1/12	14	0/0/12	15	1/12	45
R2	0/1/13	15	0/0/13	16	1/13	46
R3	0/1/14	16	0/0/14	17	1/14	47
R4	0/1/15	17	0/0/15	18	1/15	48
POD CSP A						
ALS1	0/2/0	26	0/1/0	18	1/16	49
ALS2	0/2/1	27	0/1/1	20	1/17	50
DLS1	0/2/2	28	0/1/2	21	1/18	51
DLS2	0/2/3	29	0/1/3	22	1/19	52

POD CSP B						
ALS1	0/2/4	30	0/1/4	23	1/20	53
ALS2	0/2/5	31	0/1/5	24	1/21	54
DLS1	0/2/6	32	0/1/6	25	1/22	55
DLS2	0/2/7	33	0/1/7	26	1/23	56
POD CSP C						
ALS1	0/2/8	34	0/1/8	27	1/24	57
ALS2	0/2/9	35	0/1/9	28	1/25	58
DLS1	0/2/10	36	0/1/10	29	1/26	59
DLS2	0/2/11	37	0/1/11	30	1/27	60
POD CSP D						
ALS1	0/2/12	38	0/1/12	31	1/28	61
ALS2	0/2/13	39	0/1/13	32	1/29	62
DLS1	0/2/14	40	0/1/14	33	1/31	63
DLS2	0/2/15	41	0/1/15	34	1/31	64

8.8 Setup for Cuatro 2U Rack

The following section is specific to the Cuatro 2U rack layout, containing CRP and CSP pods. The following steps should already be completed.

- Lab equipment racked according to CUATRO 2U layout (described earlier).
- Secondary control switches added and configured in NETLAB+ VE.
- Access server added and configured in NETLAB+ VE.

8.8.1 Cuatro 2U Rack - Control Switch Configuration

Connect CRP pods and CSP pods to the rack's secondary control switch(es) and configure control switch port roles per the following tables.

When using a single 48-port control switch in the rack:

Control Switch		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD CRP A	
1	Lab Device	R1	0/0
2	Lab Device	R1	0/1
3	Lab Device	R2	0/0
4	Lab Device	R2	0/1
5	Lab Device	R3	0/0
6	Lab Device	R3	0/1
7	Lab Device	R4	0/0
8	Lab Device	R4	0/1
		POD CRP B	
9	Lab Device	R1	0/0
10	Lab Device	R1	0/1
11	Lab Device	R2	0/0
12	Lab Device	R2	0/1
13	Lab Device	R3	0/0
14	Lab Device	R3	0/1
15	Lab Device	R4	0/0
16	Lab Device	R4	0/1
		POD CRP C	
17	Lab Device	R1	0/0
18	Lab Device	R1	0/1
19	Lab Device	R2	0/0
20	Lab Device	R2	0/1
21	Lab Device	R3	0/0
22	Lab Device	R3	0/1
23	Lab Device	R4	0/0
24	Lab Device	R4	0/1
		Placeholder for POD CRP D Not Implemented in Cuatro 2U Rack	

Control Switch		Peer Device	
25	Unmanaged	*Not implemented*	
26	Unmanaged	*Not implemented*	
27	Unmanaged	*Not implemented*	
28	Unmanaged	*Not implemented*	
29	Unmanaged	*Not implemented*	
30	Unmanaged	*Not implemented*	
31	Unmanaged	*Not implemented*	
32	Unmanaged	*Not implemented*	
		POD CSP A	
33	Lab Device	ALS1	Port 6
34	Lab Device	ALS2	Port 6
35	Lab Device	DLS1	Port 6
36	Lab Device	DLS2	Port 6
		POD CSP B	
37	Lab Device	ALS1	Port 6
38	Lab Device	ALS2	Port 6
39	Lab Device	DLS1	Port 6
40	Lab Device	DLS2	Port 6
		POD CSP C	
41	Lab Device	ALS1	Port 6
42	Lab Device	ALS2	Port 6
43	Lab Device	DLS1	Port 6
44	Lab Device	DLS2	Port 6
		Control Devices	
45	PDU	PDU CRP A/ CRP B	Ethernet Mgt.
46	PDU	PDU CRP C / CSP A	Ethernet Mgt.
47	PDU	PDU CSP B / CSP C	Ethernet Mgt.
48	Unmanaged	*Not implemented*	
GigabitEthernet1/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet1/1	Access Server	Access Server	0/0

When using two (2) 24-port control switches in the rack:

Control Switch A		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD CRP A	
1	Lab Device	R1	0/0
2	Lab Device	R1	0/1
3	Lab Device	R2	0/0
4	Lab Device	R2	0/1
5	Lab Device	R3	0/0
6	Lab Device	R3	0/1
7	Lab Device	R4	0/0
8	Lab Device	R4	0/1
		POD CRP B	
9	Lab Device	R1	0/0
10	Lab Device	R1	0/1
11	Lab Device	R2	0/0
12	Lab Device	R2	0/1
13	Lab Device	R3	0/0
14	Lab Device	R3	0/1
15	Lab Device	R4	0/0
16	Lab Device	R4	0/1
		POD CRP C	
17	Lab Device	R1	0/0
18	Lab Device	R1	0/1
19	Lab Device	R2	0/0
20	Lab Device	R2	0/1
21	Lab Device	R3	0/0
22	Lab Device	R3	0/1
23	Lab Device	R4	0/0
24	Lab Device	R4	0/1
		Control Devices	
GigabitEthernet1/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet1/1	Access Server	Access Server	0/0

Control Switch B		Peer Device	
Port	**Role**	**Name**	**Interface or Port**
		POD CSP A	
1	Lab Device	ALS1	Port 6
2	Lab Device	ALS2	Port 6
3	Lab Device	DLS1	Port 6
4	Lab Device	DLS2	Port 6
5	Unmanaged	*Not implemented*	
6	Unmanaged	*Not implemented*	
7	Unmanaged	*Not implemented*	
8	Unmanaged	*Not implemented*	
		POD CSP B	
9	Lab Device	ALS1	Port 6
10	Lab Device	ALS2	Port 6
11	Lab Device	DLS1	Port 6
12	Lab Device	DLS2	Port 6
13	Unmanaged	*Not implemented*	
14	Unmanaged	*Not implemented*	
15	Unmanaged	*Not implemented*	
16	Unmanaged	*Not implemented*	
		POD CSP C	
17	Lab Device	ALS1	Port 6
18	Lab Device	ALS2	Port 6
19	Lab Device	DLS1	Port 6
20	Lab Device	DLS2	Port 6
21	Unmanaged	*Not implemented*	
22	Unmanaged	*Not implemented*	
23	Unmanaged	*Not implemented*	
24	Unmanaged	*Not implemented*	
		Control Devices	
GigabitEthernet1/0	Control Switch	Control Switch 1	2 - 18
GigabitEthernet1/1	Unmanaged	*Not implemented*	

8.8.2 Cuatro 2U Rack - PDU Configuration

Cable the PDU outlets per the following table.

Outlet	Lab Device
PDU CRP A/B	
1	POD CRP A - R1
2	POD CRP A – R2
3	POD CRP A – R3
4	POD CRP A – R4
5	POD CRP B – R1
6	POD CRP B – R2
7	POD CRP B – R3
8	POD CRP B – R4
PDU CRP B/CSP A	
1	POD CRP C – R1
2	POD CRP C – R2
3	POD CRP C – R3
4	POD CRP C – R4
5	POD CSP A – ALS1
6	POD CRP A – ALS2
7	POD CRP A – ALS3
8	POD CRP A – ALS4
PDU CSP B/C	
1	POD CSP B – ALS1
2	POD CSP B – ALS2
3	POD CSP B – DLS1
4	POD CSP B – DLS2
5	POD CSP C – ALS1
6	POD CSP C – ALS2
7	POD CSP C – DLS1
8	POD CSP C – DLS2

8.8.3 Cuatro 2U Rack - Access Server Configuration

Connect lab devices to the access server per the following table.

- Port numbers represent physical connections.
- Line numbers represent logical connections and will be used later in the pod setup process.

	Cisco 4321 (2) NIM-16A		Cisco 2901 (2) HWIC-16A		Cisco 2600 (1) NM-32A	
Lab Device	**Port**	**Line**	**Port**	**Line**	**Port**	**Line**
POD CRP A						
R1	0/1/0	2	0/0/0	3	1/0	33
R2	0/1/1	3	0/0/1	4	1/1	34
R3	0/1/2	4	0/0/2	5	1/2	35
R4	0/1/3	5	0/0/3	6	1/3	36
POD CRP B						
R1	0/1/4	6	0/0/4	7	1/4	37
R2	0/1/5	7	0/0/5	8	1/5	38
R3	0/1/6	8	0/0/6	9	1/6	39
R4	0/1/7	9	0/0/7	10	1/7	40
POD CRP C						
R1	0/1/8	10	0/0/8	11	1/8	41
R2	0/1/9	11	0/0/9	12	1/9	42
R3	0/1/10	12	0/0/10	13	1/10	43
R4	0/1/11	13	0/0/11	14	1/11	44
POD CSP A						
ALS1	0/1/12	14	0/0/12	15	1/12	45
ALS2	0/1/13	15	0/0/13	16	1/13	46
DLS1	0/1/14	16	0/0/14	17	1/14	47
DLS2	0/1/15	17	0/0/15	18	1/15	48
POD CSP B						
ALS1	0/2/0	26	0/1/0	18	1/16	49
ALS2	0/2/1	27	0/1/1	20	1/17	50
DLS1	0/2/2	28	0/1/2	21	1/18	51
DLS2	0/2/3	29	0/1/3	22	1/19	52

POD CSP C						
ALS1	0/2/4	30	0/1/4	23	1/20	53
ALS2	0/2/5	31	0/1/5	24	1/21	54
DLS1	0/2/6	32	0/1/6	25	1/22	55
DLS2	0/2/7	33	0/1/7	26	1/23	56
Unused Ports on Line Card (Octopus Cable Not Required)						
Not used	0/2/8	34	0/1/8	27	1/24	57
Not used	0/2/9	35	0/1/9	28	1/25	58
Not used	0/2/10	36	0/1/10	29	1/26	59
Not used	0/2/11	37	0/1/11	30	1/27	60
Not used	0/2/12	38	0/1/12	31	1/28	61
Not used	0/2/13	39	0/1/13	32	1/29	62
Not used	0/2/14	40	0/1/14	33	1/31	63
Not used	0/2/15	41	0/1/15	34	1/31	64

8.9 Intra-pod Cabling for CRP Pods

The following additional connections are made between **lab devices** in a Cuatro Router Pod (CRP).

> Control device connections are not shown in this table.

From Device	From Interface	From Cable	To Cable	To Device	To Interface
Required Intra-pod Cabling					
R1	Serial0/0	V.35 Female DCE	V.35 Male DTE	R2	Serial0/0
R2	Serial0/1	V.35 Female DCE	V.35 Male DTE	R3	Serial0/1
R3	Serial0/0	V.35 Female DCE	V.35 Male DTE	R1	Serial0/1
R4	Serial0/0	V.35 Male DTE	V.35 Female DCE	R3	Serial0/2
	Serial0/1	V.35 Male DTE	V.35 Female DCE	R3	Serial0/3

8.10 Intra-pod Cabling for CSP Pods

The following additional connections are made between **lab devices** in a Cuatro Switch Pod (CSP).

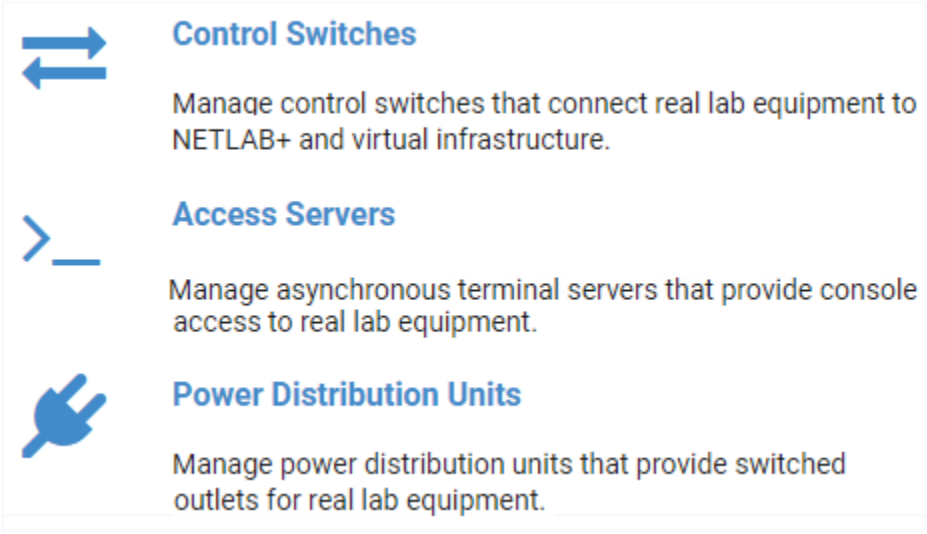
> Control device connections are not included in this table.

From Device	From Interface	Cable	To Device	To Interface
ALS1	Port 7	Cat5e	DLS1	Port 7
	Port 8	Cat5e	DLS1	Port 8
	Port 11	Cat5e	ALS2	Port 11
	Port 12	Cat5e	ALS2	Port 12
ALS2	Port 7	Cat5e	DLS2	Port 7
	Port 8	Cat5e	DLS2	Port 8
DLS1	Port 9	Cat5e	ALS2	Port 9
	Port 10	Cat5e	ALS2	Port 10
	Port 11	Cat5e	DLS2	Port 11
	Port 12	Cat5e	DLS2	Port 12
DLS2	Port 9	Cat5e	ALS1	Port 9
	Port 10	Cat5e	ALS1	Port 10

9 Adding Control Devices to the Infrastructure

In this section, we document the procedures for adding the control devices using the NETLAB+ VE user interface. These procedures are referenced at various steps in this guide.

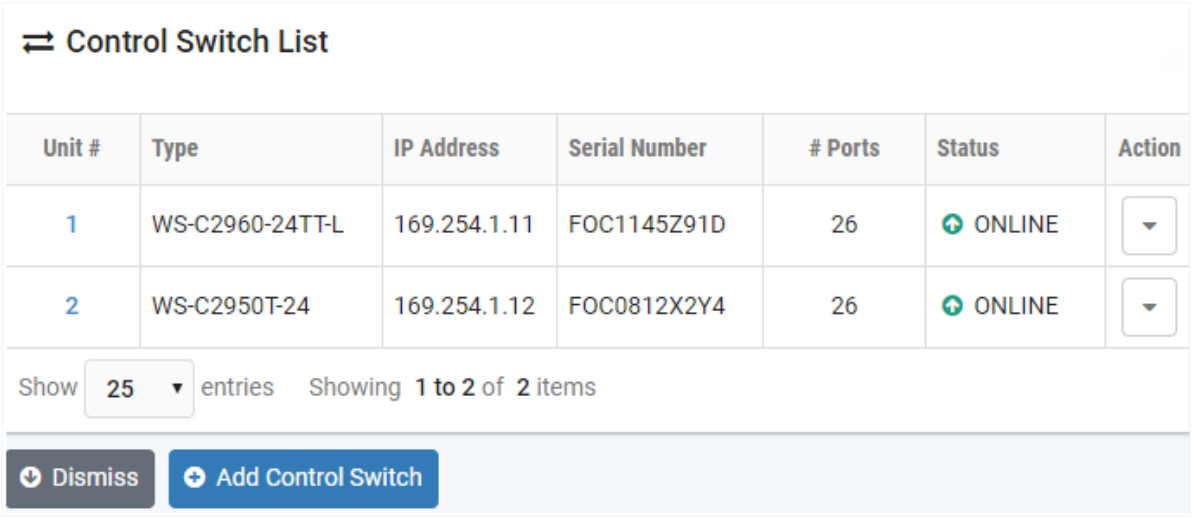
To manage control devices, select **Control Devices** from the Pods and Infrastructure section of the Administrator Home page. The control devices page will be displayed, listing the 3 types of control devices. Each type of control device is described in detail in the subsections below.



9.1 Control Switches

Control switches are used to connect real lab equipment to NETLAB+ and the virtual infrastructure. Control switches can provide a temporary TFTP path for automated management of IOS images in lab devices. Control switches function as virtual Ethernet hubs in lab topologies when the lab is active. Control switches provide internal connectivity between NETLAB+, access servers, remote PCs, and PDUs.

To access control switches, select **Control Switches** on the Control Devices page. The control switches currently defined on your system (if any) will be displayed.

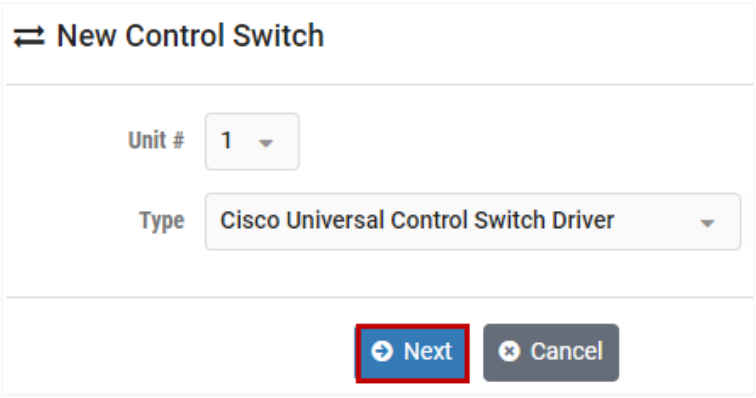


See the subsections below for information on adding a control switch and viewing/configuring control switch settings.

9.1.1 Adding a Control Switch

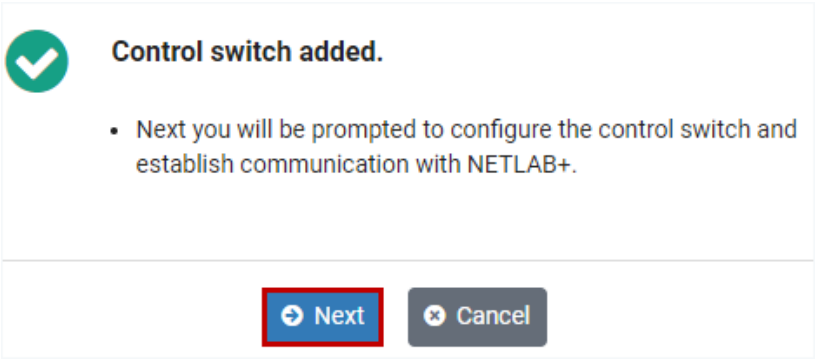
Follow the steps below to add a control switch to your NETLAB+ system.

1. Select the option to **Add a Control Switch**, from the **Admin > Control Devices > Control Switches** page.
2. The New Control Switch Screen will be displayed. Select a Unit # and Type, and then click **Next**.



All currently supported control switches should be added using the **Cisco Universal Control Switch Drive**r, which will allow NETLAB+ to recognize the specific switch model and automate configuration of the switch. For supported control switches, see *Control Switch Requirements*.

3. The control switch has been added. Click **Next** to configure the switch and establish communication with NETLAB+, as described in the next section.



Power off any lab devices connected to this switch until the control switch is configured and the pods in which they belong have been added to NETLAB+.

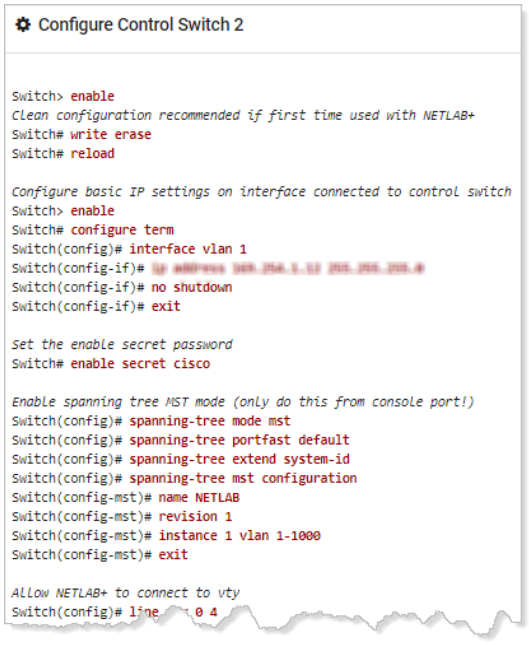
9.1.2 Configuring a Control Switch

Those who are familiar with the setup of NETLAB AE and PE will recall the requirement that pod port numbers be consecutive. NETLAB+ VE does not require port numbers to be consecutive; you may use any ports available. The use of consecutive pod ports is however considered best practice and will aid in simplifying the design, cabling, and troubleshooting of your system.

The configuration commands required to automate your switch will be generated by NETLAB+ and displayed after adding a new switch or when selecting the option to configure an existing switch.

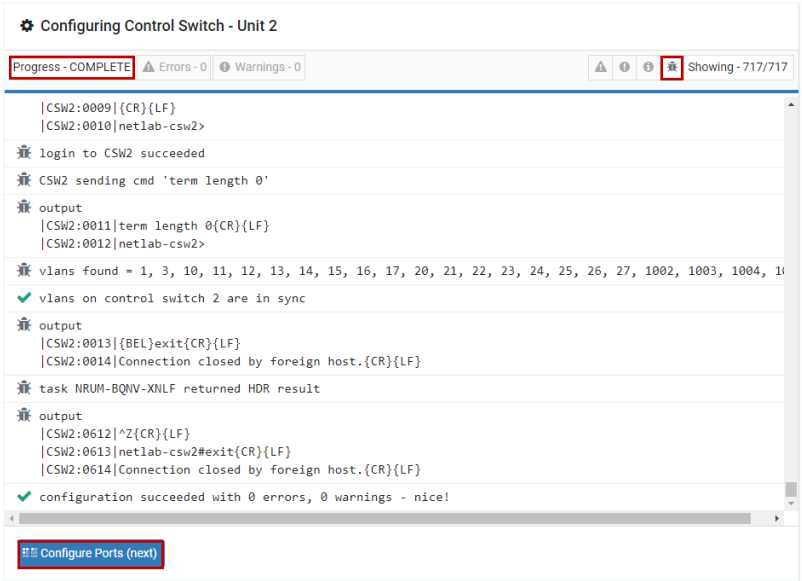
1. Connect a PC with a serial port and terminal software to the control switch console port and enter the IOS commands provided. This will provide enough configuration so that NETLAB+ can manage the control switch.

2. Click **Next** after you have entered the commands (copy the commands generated on *your* system, they will vary from the partial example below).



3. The Configuring Control Switch page will be displayed, showing the configuration in progress. If errors occur, it may be necessary to troubleshoot the errors, enter the commands again (select Configure to view the IOS commands again), and retry the configuration. Upon successful completion, click **Configure Ports (next**), and continue to the next section.

Notice the bug icon  in the upper-right corner of the picture below. Selecting the bug icon allows you to see all available debug output, which can be very helpful when troubleshooting.



9.1.3 Control Switch Port Roles

Each port on a control switch is assigned one of the following roles:

Port Role	Description
LAB:FREE	Port is available for lab device connection.
LAB:ROUTER	Port is connected to a lab router.
LAB:SWITCH	Port is connected to a lab switch.
LAB:FIREWALL	Port is connected to a lab firewall.
CONTROL:SWITCH	Port is connected to another control switch.
CONTROL:ACCESS	Port is connected to an access server.
CONTROL:PDU	Port is connected to a power distribution unit.
CONTROL:VMS	Port is connected to a VM host server.
UNMANAGED	Port is not configured or managed by NETLAB+ VE.

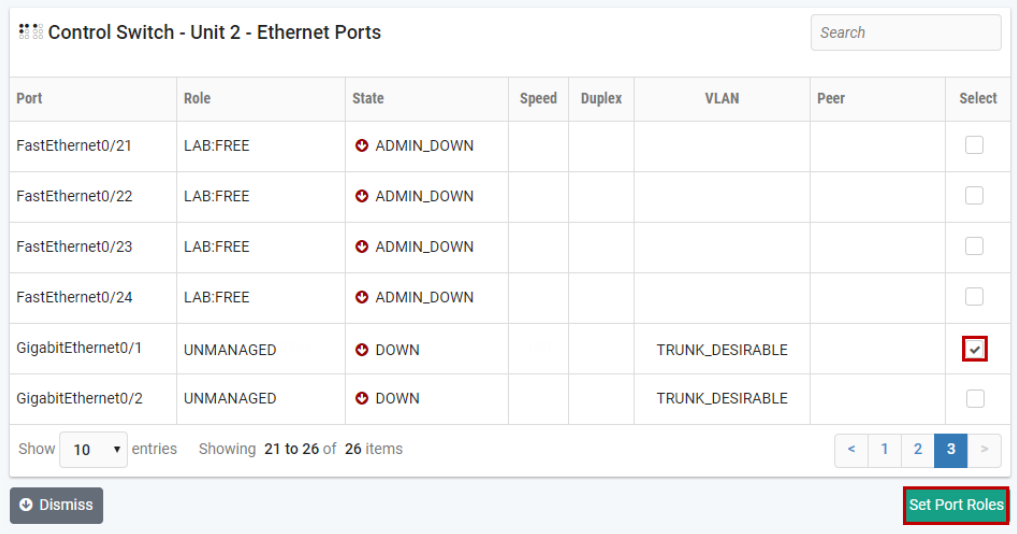
- *Ports designated with LAB roles* connect to lab devices. During normal operation, these ports are automatically placed in unique or common VLANs to simulate one or more Ethernet segments required by the topology of the pod, and to connect the real equipment and virtual machines in a pod. A single control switch can have LAB ports for several pods. LAB ports are automatically configured based on the peer device type and lab exercise requirements.

- *Ports designated with CONTROL roles* are used to provide the framework to interconnect NETLAB+ and control devices. CONTROL ports are automatically configured based on the peer device. For example, a CONTROL:VMS port will be configured with 802.1q trunking turned on.

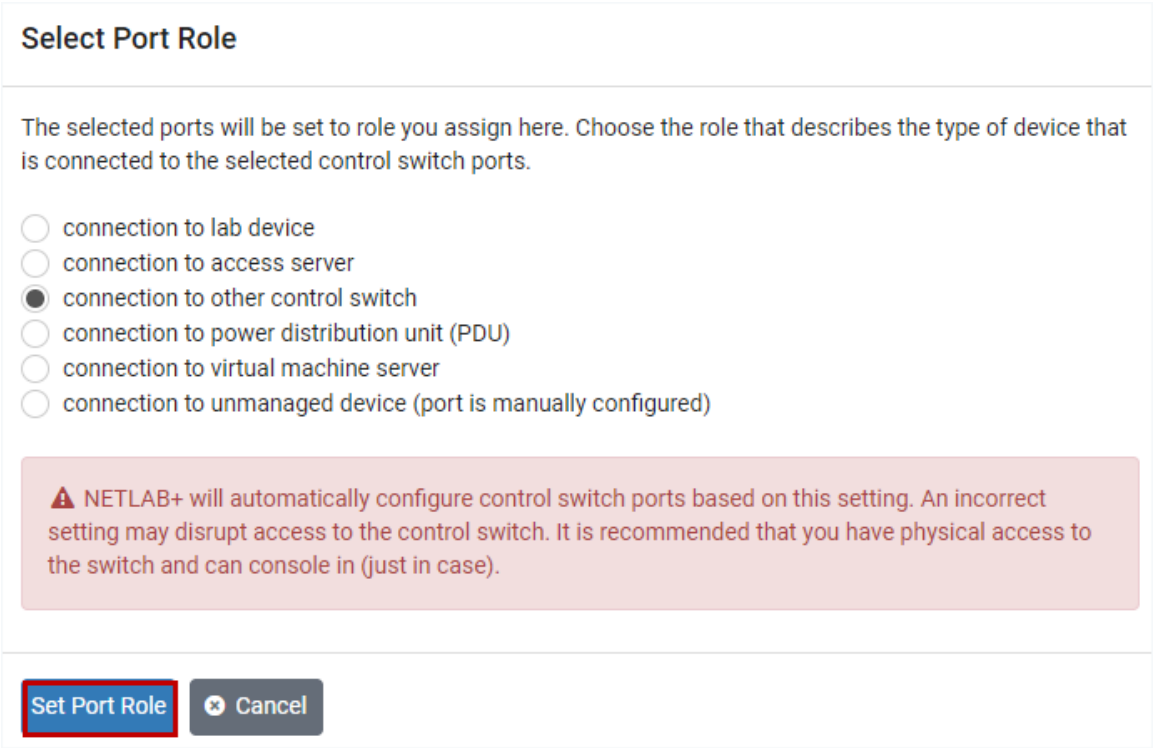
- Ports designated with the UNMANAGED role are not configured by NETLAB+ VE. They may be used by advanced custom pod designs requiring specialized external connectivity.

The Ethernet Ports page is displayed after configuring a new switch or by selecting the Ports option on the Control Switch detail page for an existing switch.

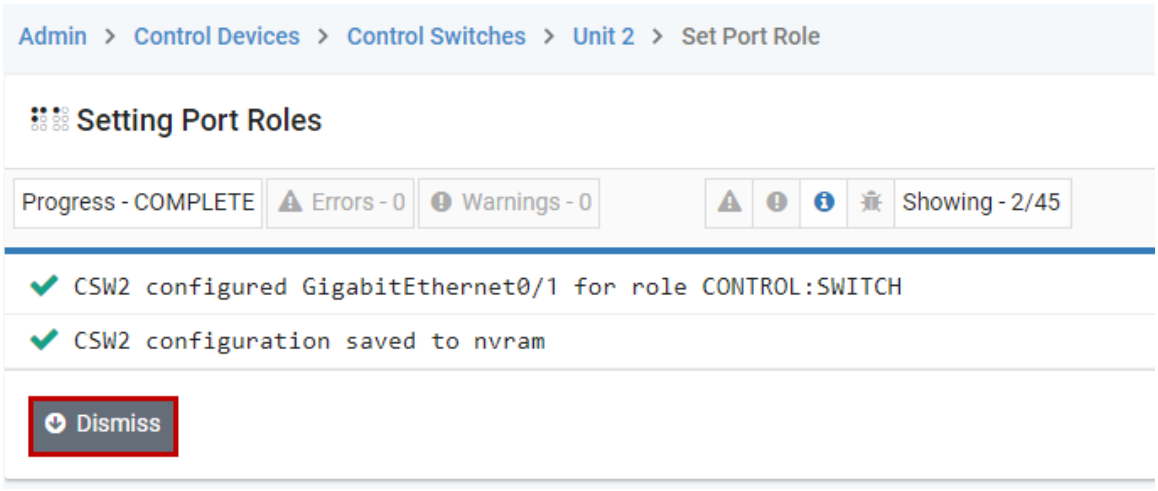
1. You will select the role to assign to the ports. The role of an Ethernet port refers to the type of device that you intend to connect to the port. You may select multiple Ethernet ports that you wish to assign the same role, using the Select checkbox and then clicking the option to **Set Port Rules**.



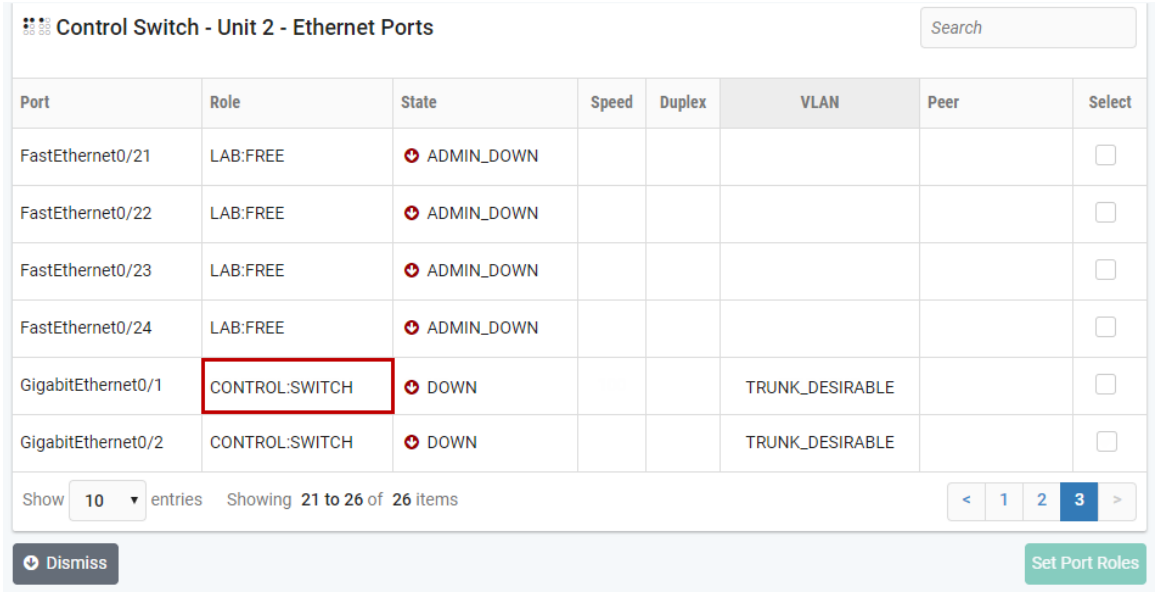
2. You will be prompted to make a selection on the Select Port Role pop-up page. The port role will be applied to all Ethernet ports selected. In the example below, we have chosen to set the selected port for **connection to other control switch.** Click **Set Port Role**.



3. The Setting Port Roles page will display the configuration in progress of the port(s) to the selected role. Select **Dismiss** when the process is completed.



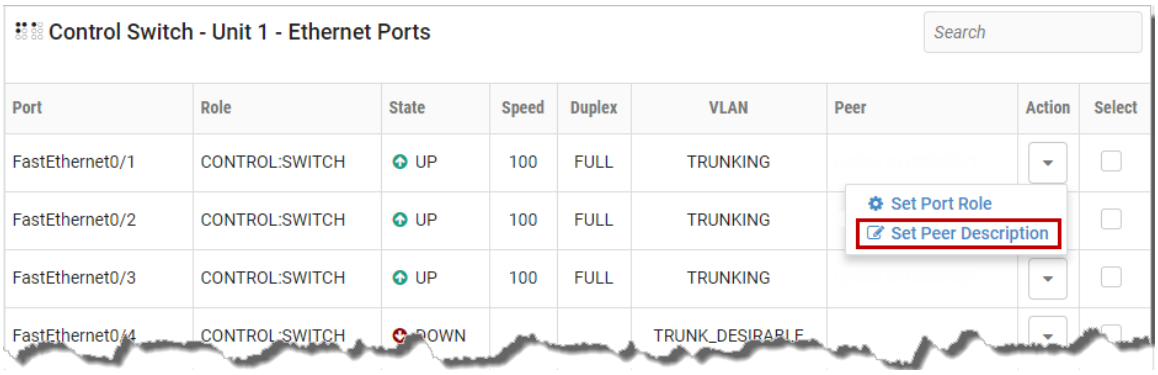
4. The Ethernet Ports page now shows the selected port assigned to the role of **CONTROL: SWITCH**, indicating that the port has been configured to use as a connection to another control switch. In this example, we are configuring this port on Control Switch 2 as a connection to the Master Control Switch.



9.1.4 Control Switch Port Peer Description

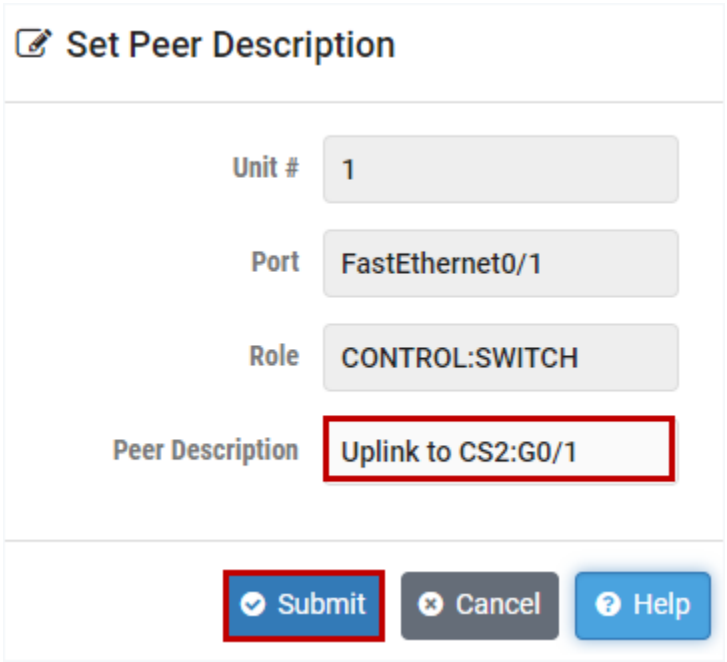
You may find it helpful to make a note of the location of the server, control switch, access server, or PDU that is connected to a control switch port by setting a Peer Description.

1. On the Ethernet Ports page, click the Action dropdown for a port and select **Set Peer Description.**

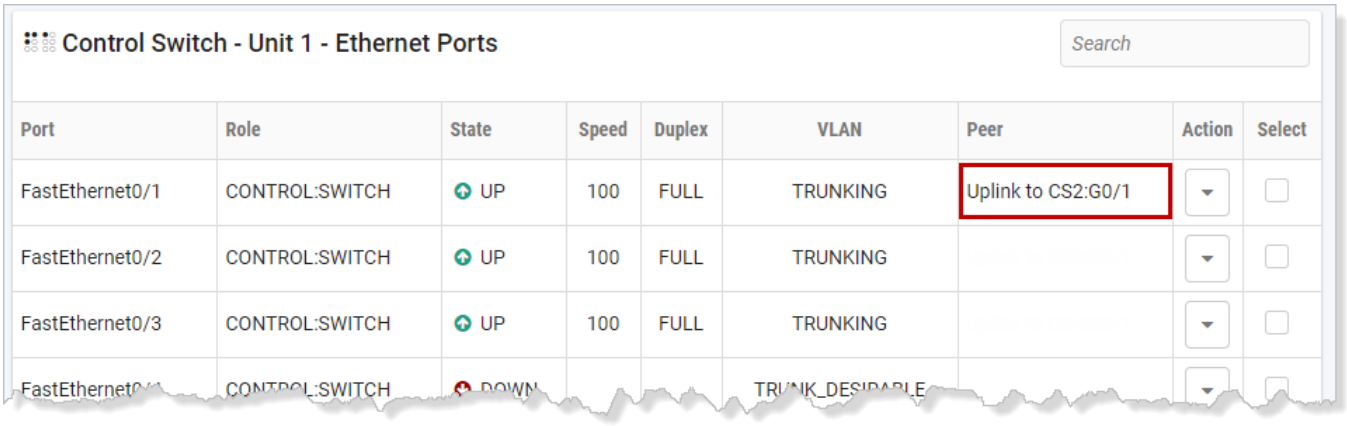


2. Enter a Peer Description. In this example, we note that this port is an uplink to Control Switch 2, connected to G0/1. Click **Submit**.

The peer description of a *lab device* is automatically set when bound to a pod and may overwrite information previously entered.



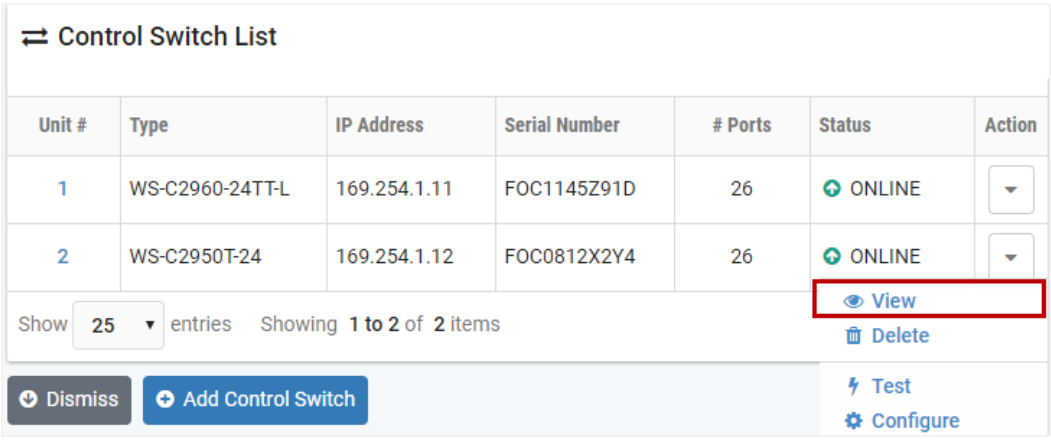
In the screenshot below, we can see that the peer description is now displayed.



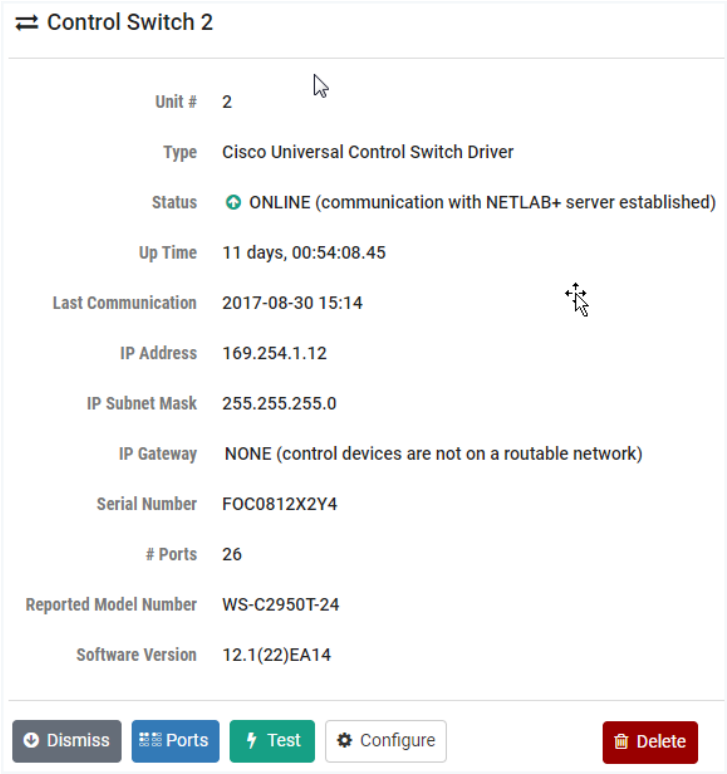
9.1.5 Viewing Control Switch Details

To see the details of a control switch, follow the steps below.

1. Select **View** on the Action dropdown for any of the switches on the Control Switch List page (or simply click anywhere on the row of the desired switch in the list).



2. The Control Switch detail page will be displayed. Several options described in previous sections are available from this page, including the options to configure the switch and the control switch port, along with the option to delete the control switch.

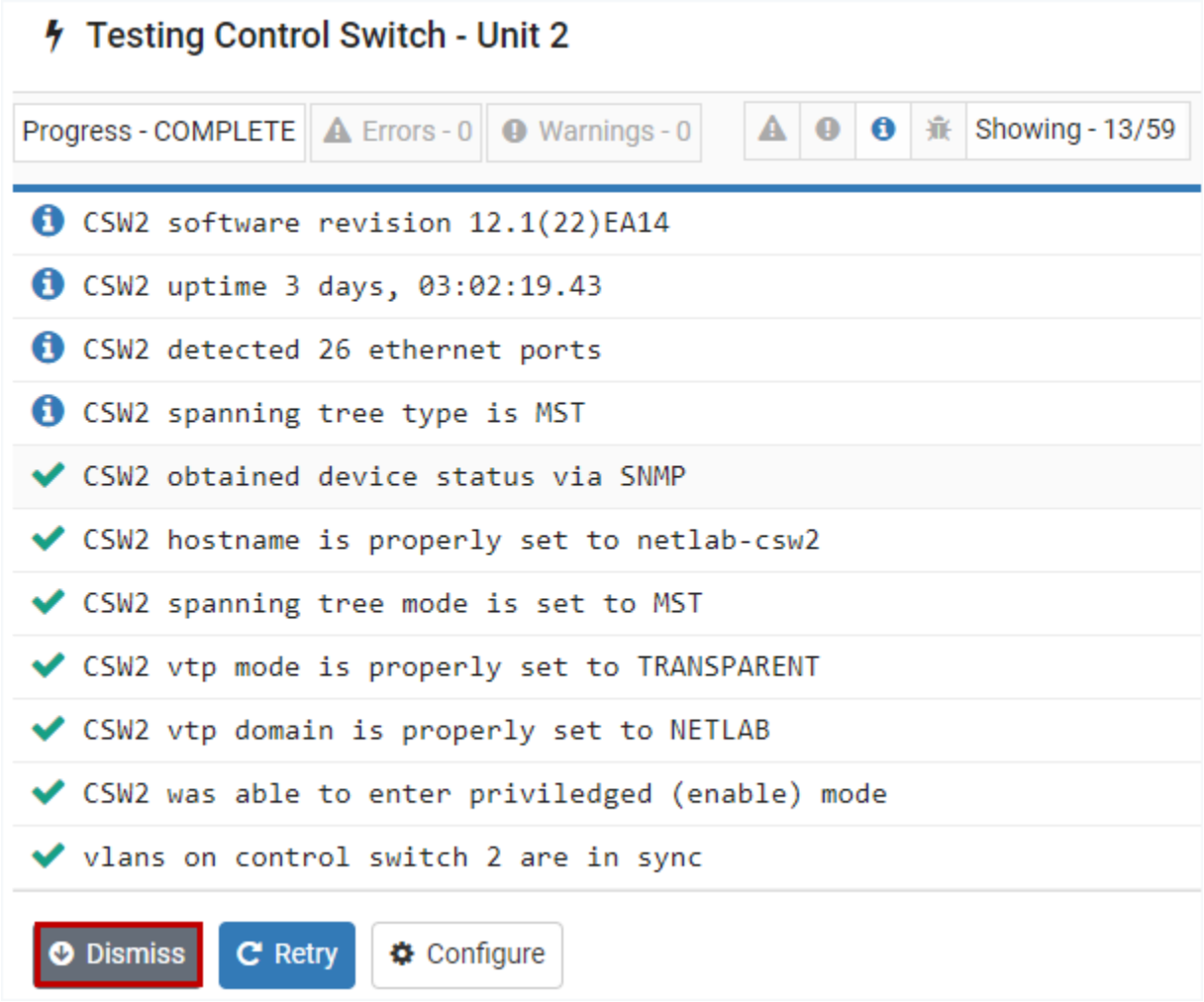


> The options to Test, Configure and Delete are also available from the Action dropdown on the Control Switch List page.

9.1.6 Testing a Control Switch

Follow the steps below to test the configuration of a control switch.

1. Select the **Test** option from the control switch detail page (see above).
2. The Testing Control Switch page will be displayed, showing the test in progress. Click **Dismiss** to return to the Control Switch detail page.



9.2 Access Servers

An access server is an asynchronous terminal server that provides console access to real lab equipment. Using this approach, users can access lab gear even when no configurations have been loaded in the lab devices. NETLAB+ proxies all connections through the access server. This special proxy allows simultaneous sharing of console ports and allows all users to access the lab environment using a built-in HTML5 CLI terminal.

When using a HWIC-16A on a router (2901 or 2811) with IOS 15, you must use version **15.1.4M4(MD)**, due to a Cisco bug. NDG has tested **15.1.4M4(MD**) on all platforms (see *Access Server Requirements*).

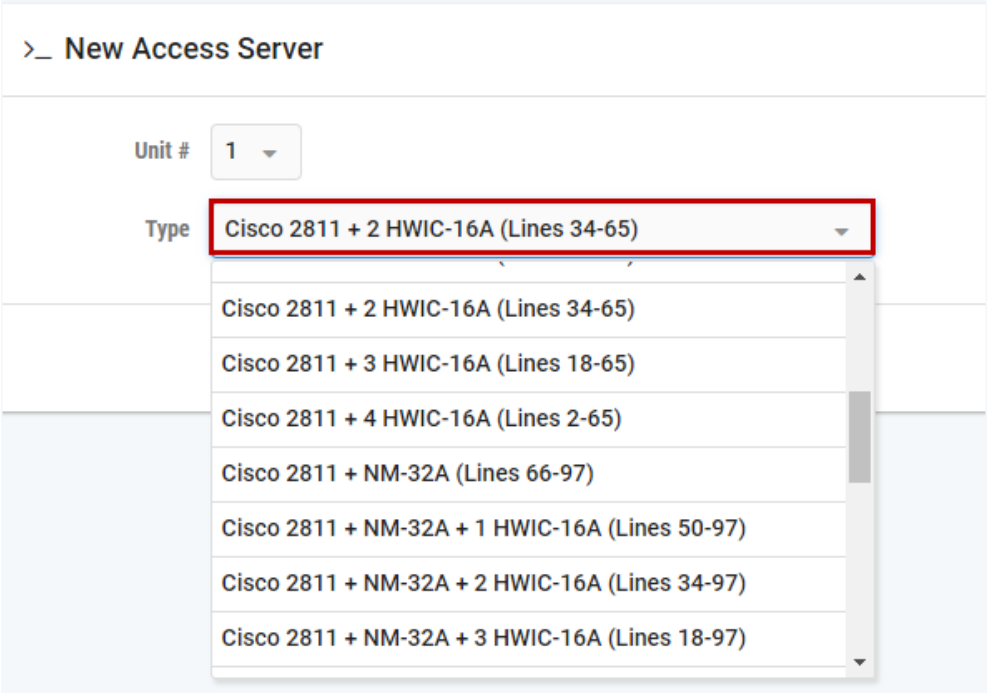
Line Number is used as a unique identifier for access server ports. Since several models include multiple modules, port number is not a unique identifier. Instructions for adding/modifying pods and access servers throughout this guide use access server line numbers for identification.

Select **Access Servers** on the Control Devices page. The access servers currently defined on your system (if any) will be displayed.

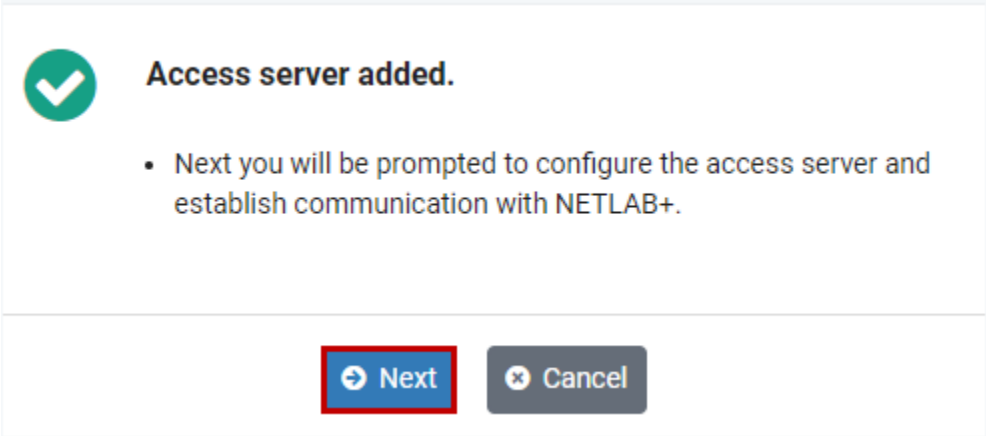
9.2.1 Adding an Access Server

Follow the steps below to add an access server to your NETLAB+ system.

1. Select the option to **Add Access Server**, from the **Admin > Control Devices > Access Servers** page.
2. The New Access Server paged will be displayed. Select a Unit # and Type, and then click **Next**.



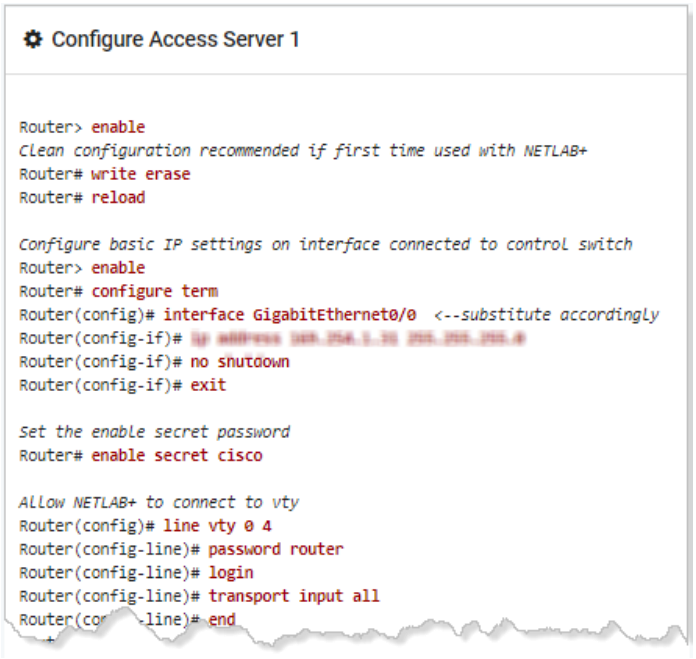
4. The access server has been added. Click **Next** to configure the access server and establish communication with NETLAB+, as described in the next section.



9.2.2 Configuring an Access Server

The configuration commands required to automate your access server will be generated by NETLAB+ and displayed after adding a new access server (see the previous section) or when selecting the option to configure an existing access server.

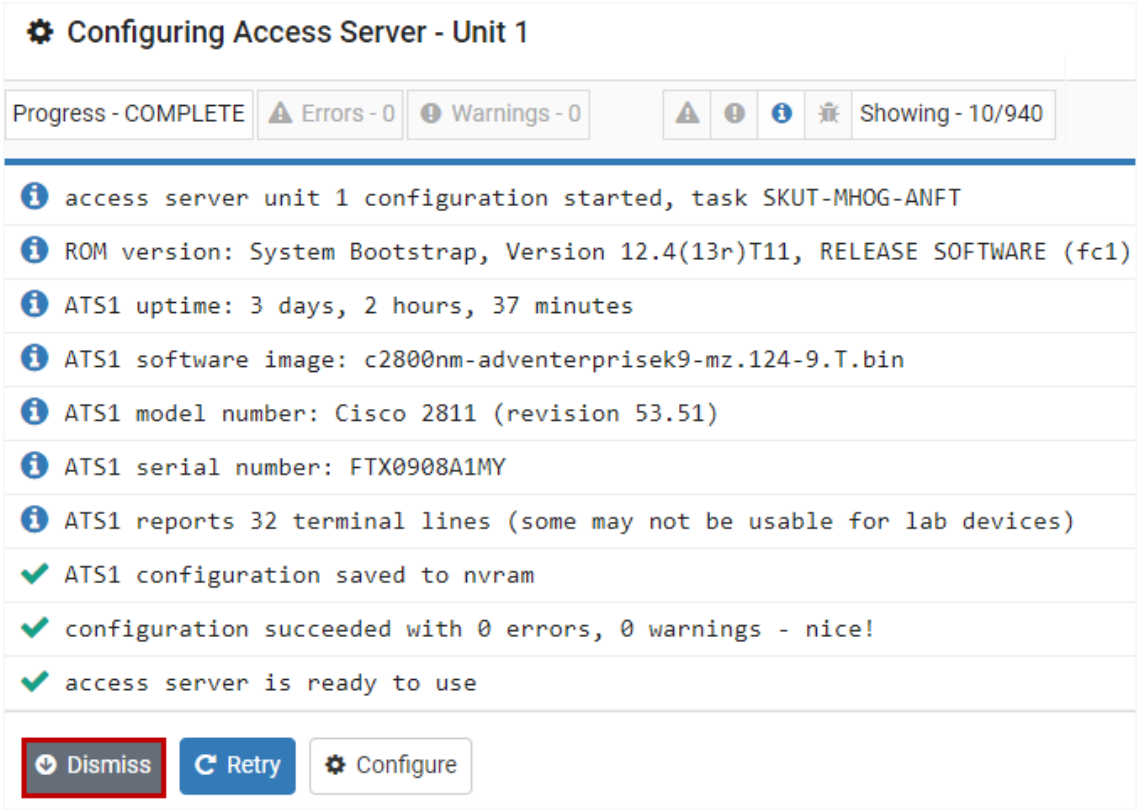
1. At this time, the access server should be connected to a reserved control switch port. This will provide a communication path to the NETLAB+ server.
2. Connect a PC with a serial port and terminal software to the access server console port and enter the IOS commands provided. This will provide enough configuration so that NETLAB+ can manage the access server.
3. Click **Next** after you have entered the commands (copy the commands generated on *your* system, they will vary from the partial example below).



The configuration commands include setting the Console and Enable passwords as shown below. You will need to enter these passwords if you wish to access the command line interface of the device.

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

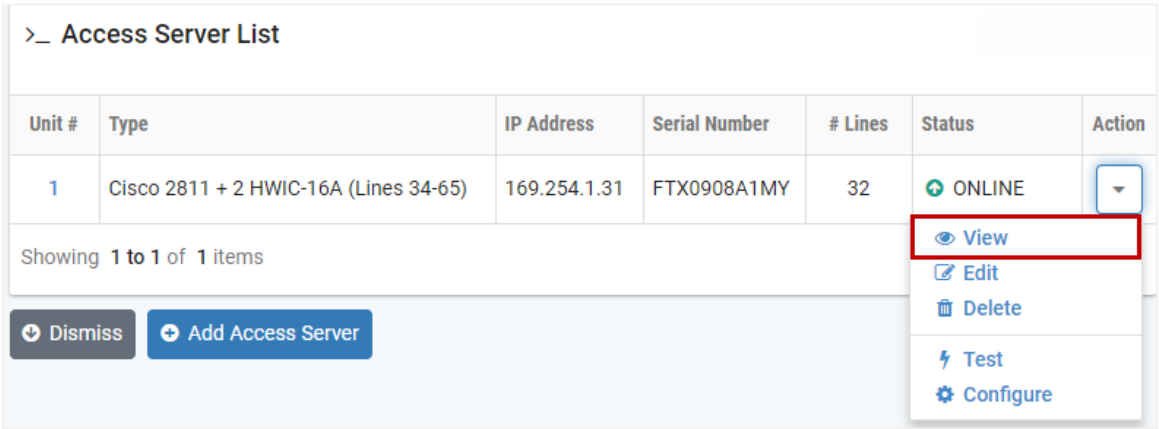
4. The Configuring Access Server page will be displayed, showing the configuration in progress. If errors occur, it may be necessary to enter the commands again (select Configure to view the IOS commands again) or retry the configuration. Upon successful completion, click **Dismiss**.



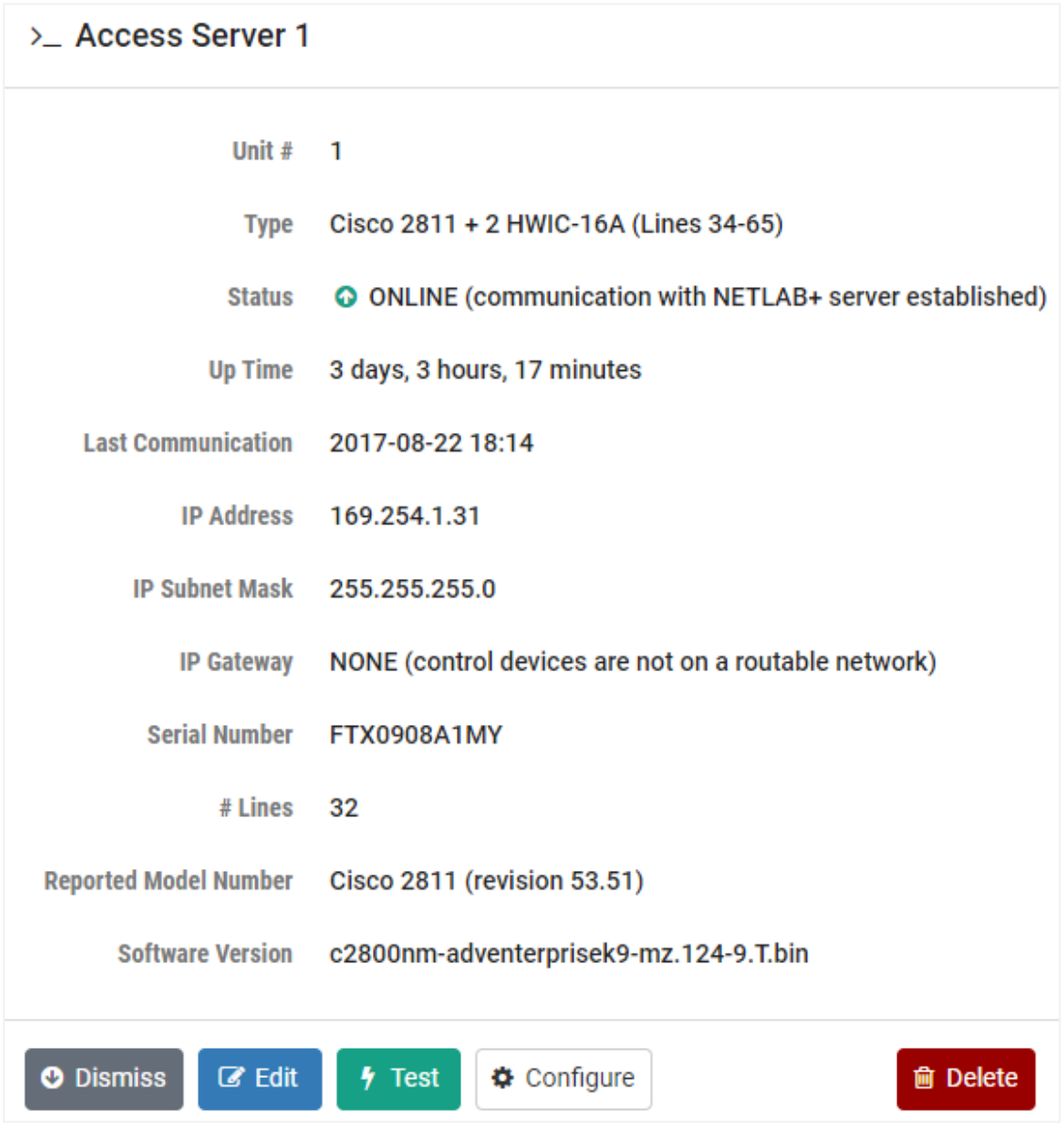
9.2.3 Viewing Access Server Details

To see the settings for an access server, follow the steps below.

1. Select **View** on the Action dropdown for any of the access servers on the Access Server List page (or simply click anywhere on the row of the desired access server in the list).



2. The Access Server detail page will be displayed. The option to configure the access server (described in a previous section) and the options to edit and delete the access server are available from this page.



As you may have noticed, the options to Test, Configure and Delete are also available from the Action dropdown on the Access Server List page.

9.2.4 Editing Access Server Type

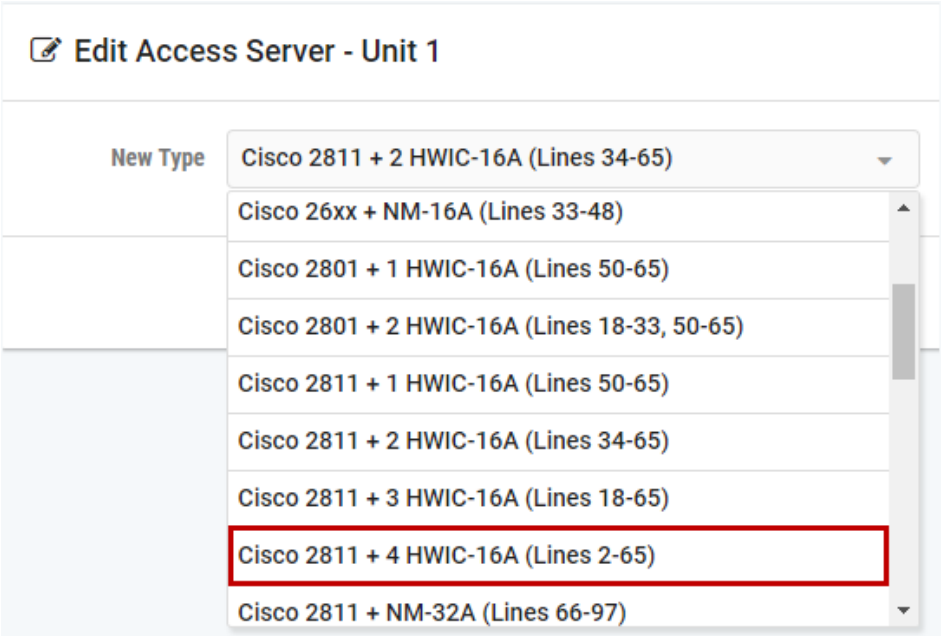
Follow the steps below to change the access server type.

To change access server types, the new access server type must have the same async line numbers that are assigned to lab devices on the currently selected access server. For example, if a lab device is configured to use async line 33 on the current access server, then line 33 must also exist on the new access server.

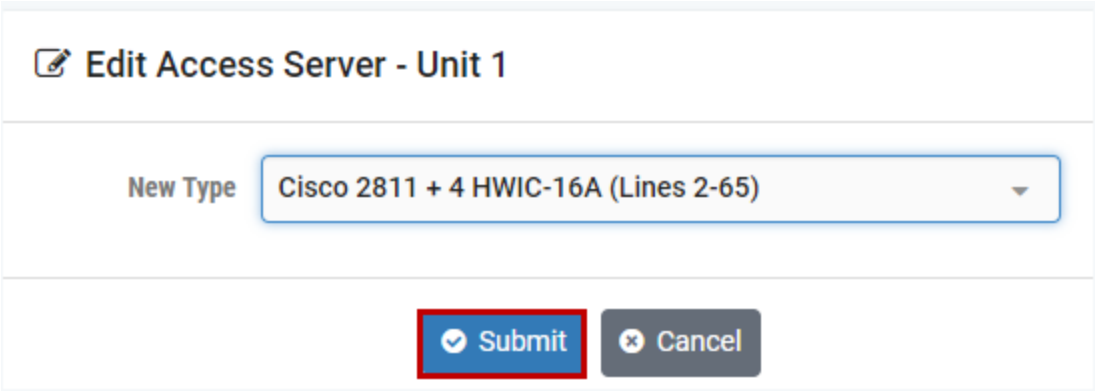
If it is necessary to change to an access server with a range of line numbers not inclusive of the original access server, you will need to unbind any lab devices and re-attach to available line numbers.

1. Select the **Edit** option from the Access Server detail page (see the section above). The Edit Access Server page will be displayed. Be sure to keep in mind that the new access server type must have the same async line numbers that are assigned to lab devices on the currently selected access server.

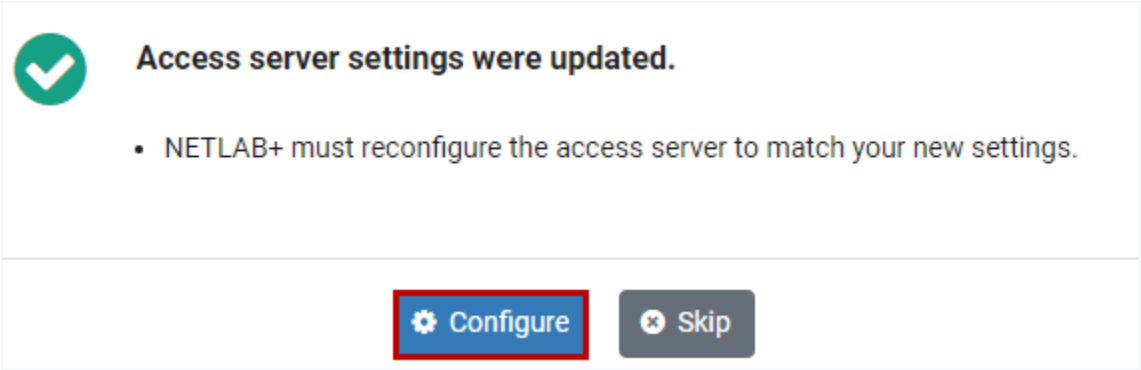
   In the example below, let us imagine that we are swapping out an access server due to equipment failure. Our Cisco 2811 + HWIC-16A (Lines 34-65) may be replaced with a Cisco 2811 + 4 HWIC-16A (Lines 2-65) since all line numbers on our original access server (34-65) are available on our replacement server (2-65). So, any lab devices bound to a line on the original access server will have a place on the new access server.



2. After selecting an appropriate replacement access server type, click **Submit**.



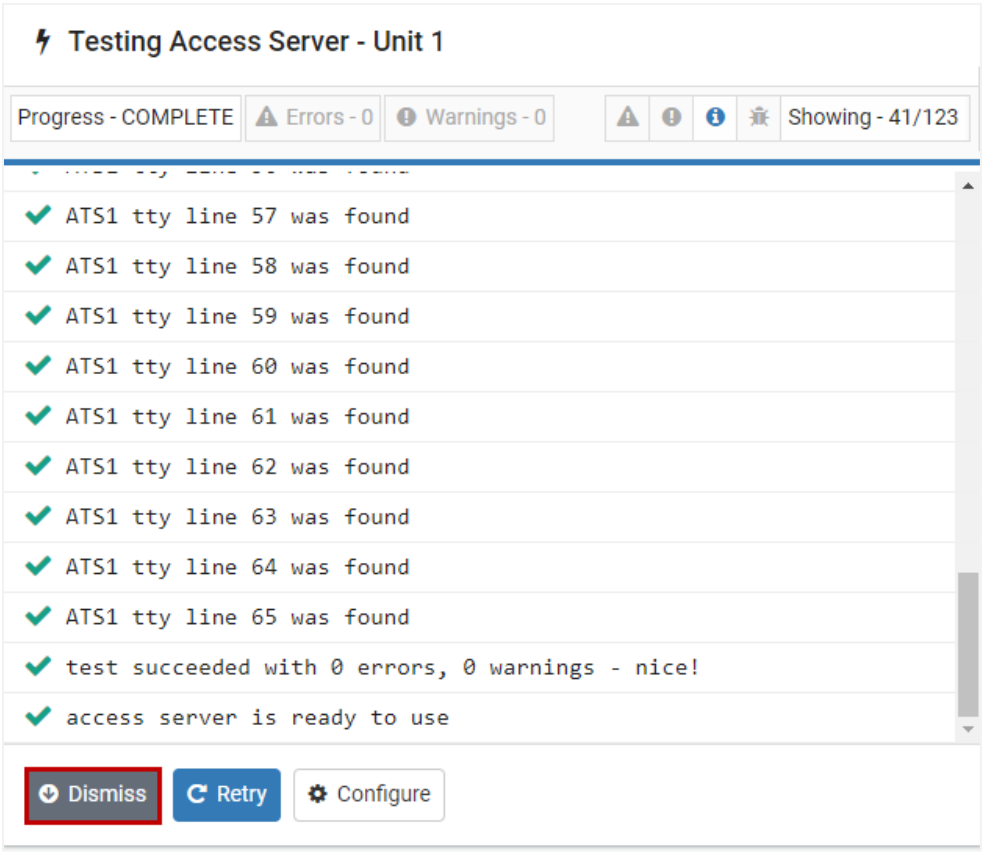
3. A message will indicate that the access server settings were updated. Select **Configure** to allow NETLAB+ to reconfigure the access server to match your new settings (see *Configuring an Access Server*).



9.2.5 Testing an Access Server

Follow the steps below to test the configuration of an access server.

1. Select the **Test** option from the Access Server detail page (shown above).
2. The Testing Access Server page will be displayed, showing the test in progress. Click **Dismiss** to return to the Access Server detail page.



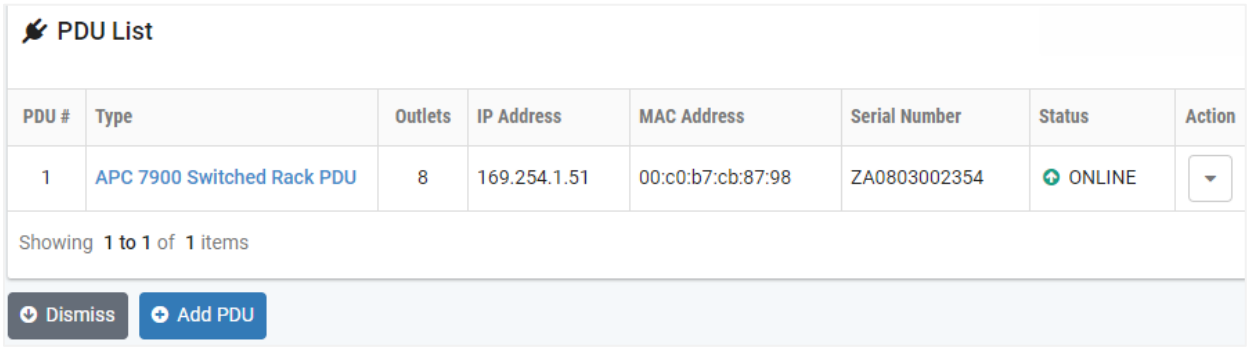
9.3 Power Distribution Units

The power of each managed device in a NETLAB+ equipment pod is connected to a power distribution unit (PDU).

The device provides three functions:

- Reboot devices during NETLAB+ automated operations.
- Allow users to control the power of a lab device (making password recovery possible).
- Power off devices when not in use to reduce energy and cooling requirements.

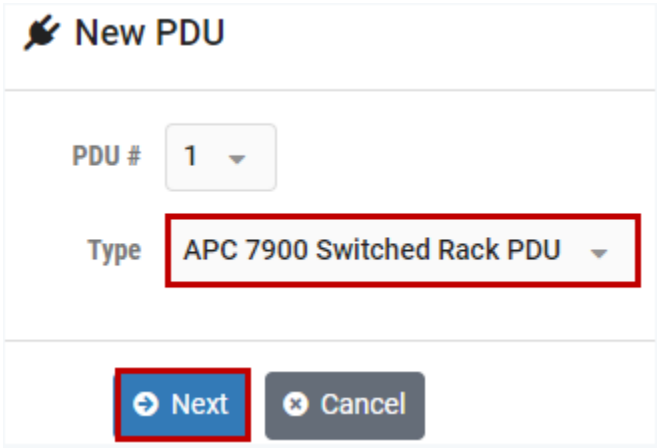
Select **Power Distribution Units** on the Control Devices page. The PDUs currently defined on your system (if any) will be displayed.



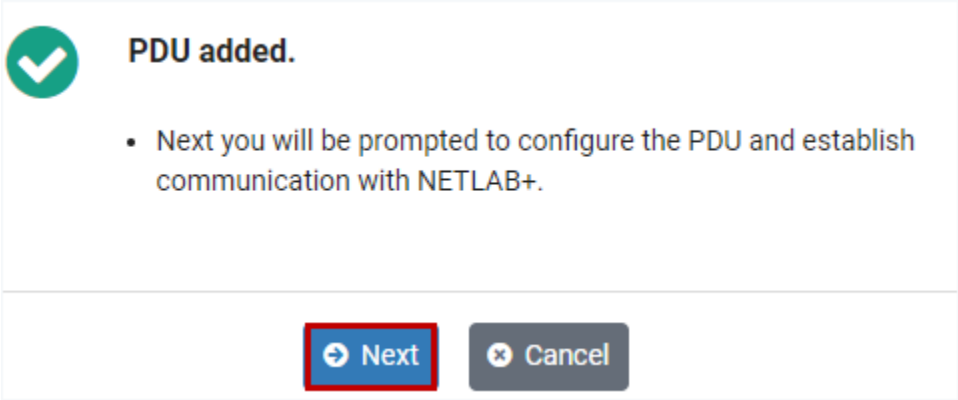
9.3.1 Adding a Power Distribution Unit

Follow the steps below to add a Power Distribution Unit (PDU) to your NETLAB+ system.

1. Select the option to **Add PDU**, from the **Admin > Control Devices > Power Distribution Units** page.
2. The New PDU page will be displayed. Select a Unit # and Type, and then click **Next**.



3. The PDU has been added. Click **Next** to configure the PDU and establish communication with NETLAB+, as described in the next section.



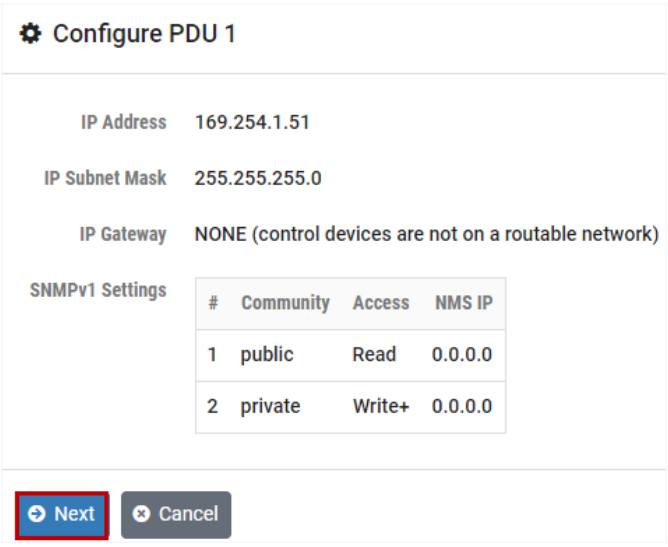
9.3.2 Configuring a Power Distribution Unit

At this time, the PDU should be connected to a reserved control switch port. This will provide a communication path to the NETLAB+ server.

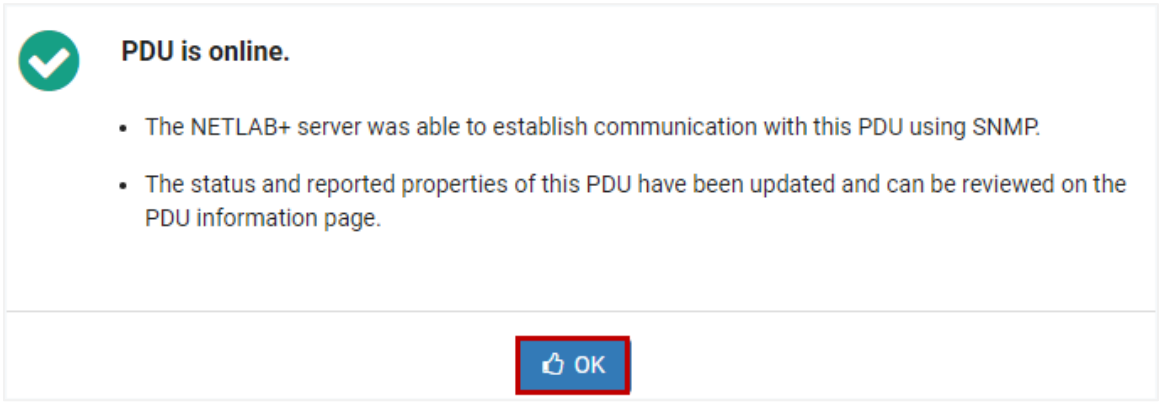
1. Connect to the PDU console port and configure the SNMP settings shown on the Configure PDU page.
2. To configure APC® devices, connect using the serial port and cable supplied with the PDU. If the serial port does not respond at 9600 bps, try 2400 bps (used by older APC models).

> The factory default username is **apc**. The default password is also **apc**. NDG expects these credentials for support, so please do not change them.

3. Click **Next** after you have configured the PDU.



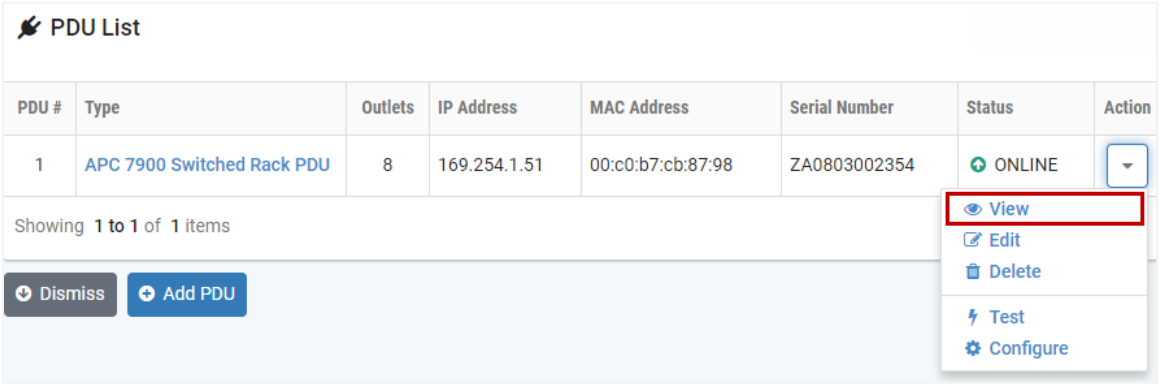
4. A message will indicate the PDU is online. Click **OK**.



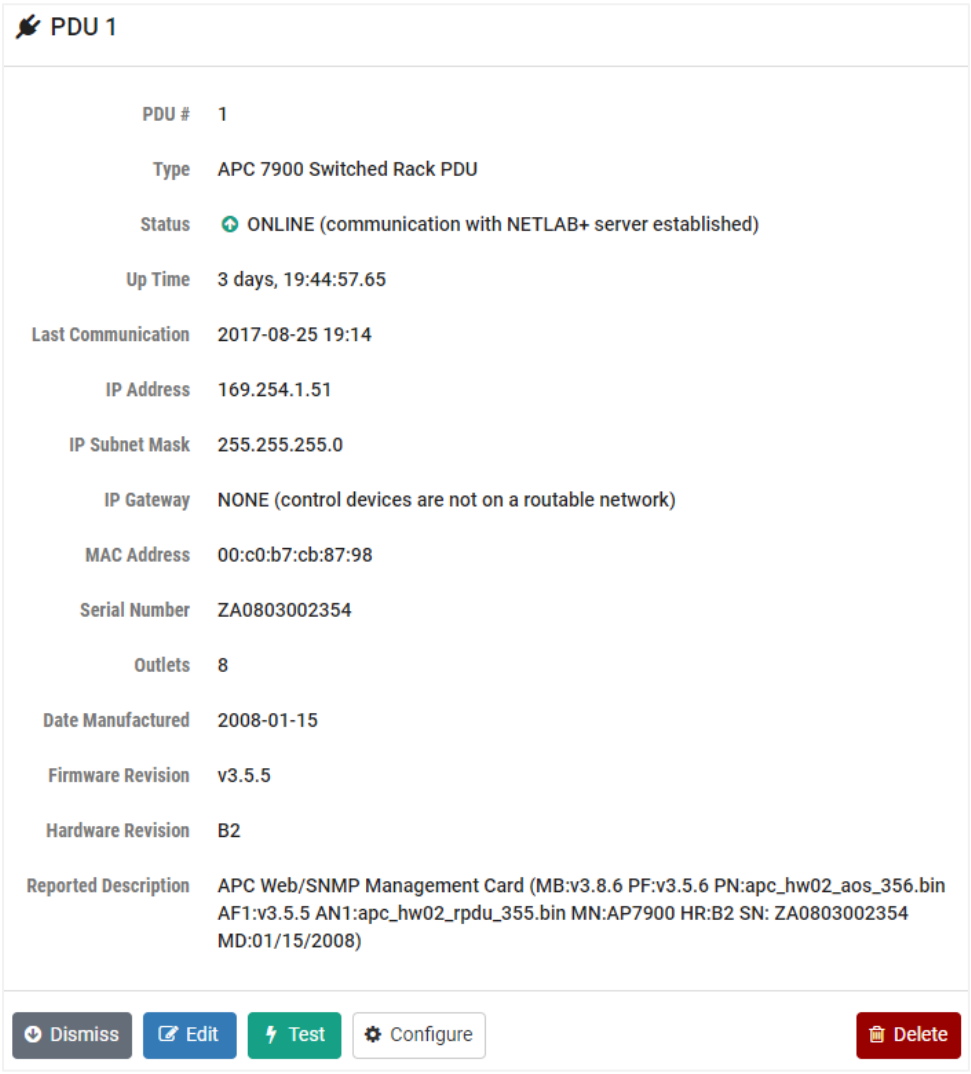
9.3.3 Viewing Power Distribution Unit Details

To see the settings for a PDU, follow the steps below.

1. Select **View** on the Action dropdown for any of the PDUs on the PDU List page (or simply click anywhere on the row of the desired PDU in the list).



2. The PDU detail page will be displayed. The option to configure the PDU (see *Configuring a Power Distribution Unit*) and the options to edit and delete the PDU are available from this page.

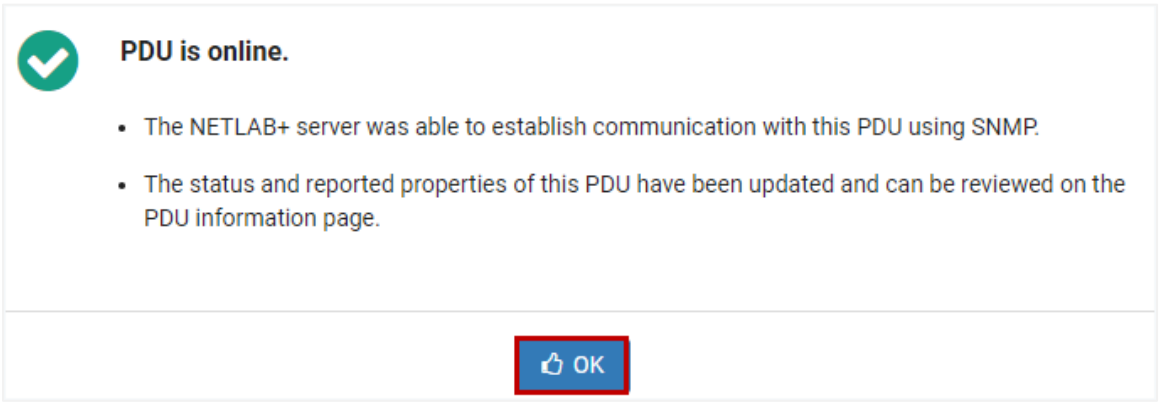


> As you may have noticed, the options to Test, Configure and Delete are also available from the Action dropdown on the PDU List page.

9.3.4 Testing a Power Distribution Unit

Follow the steps below to test the configuration of a PDU.

1. Select the **Test** option from the PDU detail page (shown above).
2. A message will indicate that the PDU is online. Click **OK**.



10 Adding Pods with Real Equipment

In this section, go through the process of adding a Multi-purpose Academy with ASA to a NETLAB+ system.

NETLAB+ may be used to facilitate access to lab equipment. Lab equipment is used for actual coursework and includes routers, switches, and firewalls. Lab devices are part of a topology (also referred to as a pod).

10.1 Real Equipment Pod Types

The table below lists the real equipment pod types available in NETLAB+ VE. Click on any of the pod types to view a quick reference page on the NDG website with details of the topology.

The quick reference pages (links below) include topology diagrams and links to the pod installation guides, which include pod-specific requirements for installing the pod. You may find it helpful to refer to the appropriate install guide as you go through the setup tasks discussed in this section.

Real Equipment Pod Types in NETLAB+ VE:

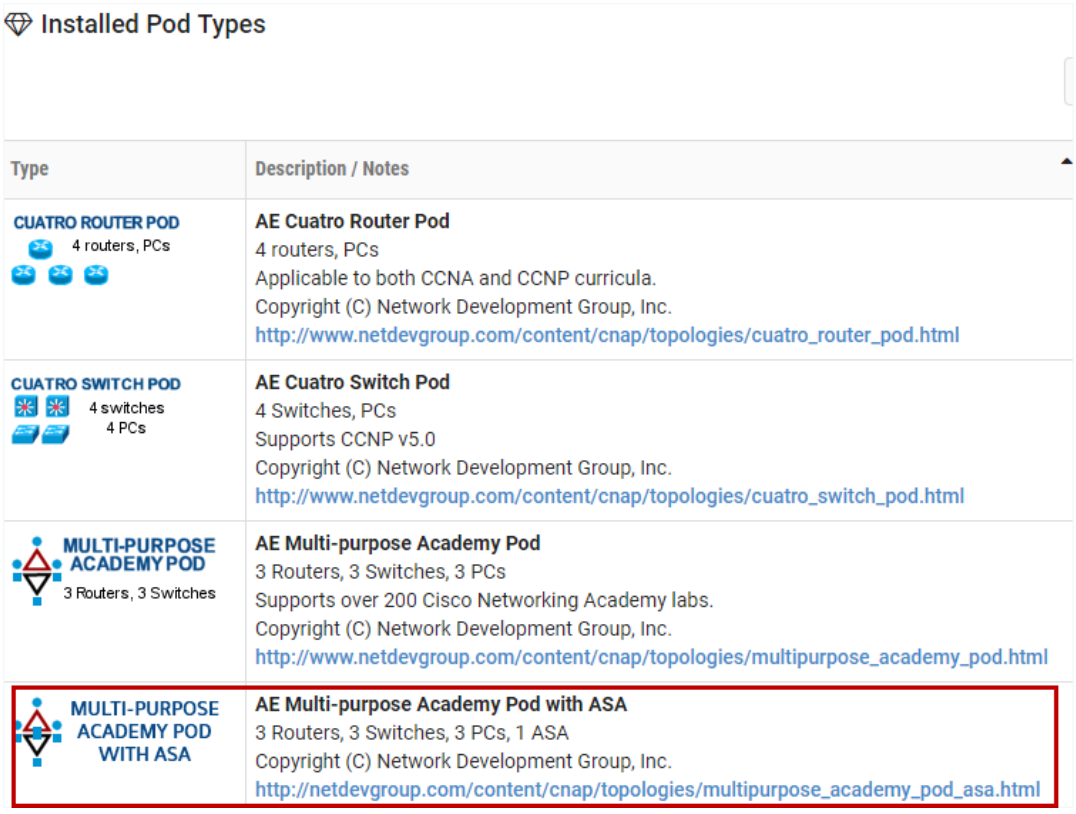
- Multi-purpose Academy Pod
- Multi-purpose Academy Pod with ASA
- Cuatro Router Pod
- Cuatro Switch Pod

10.2 Creating a Pod

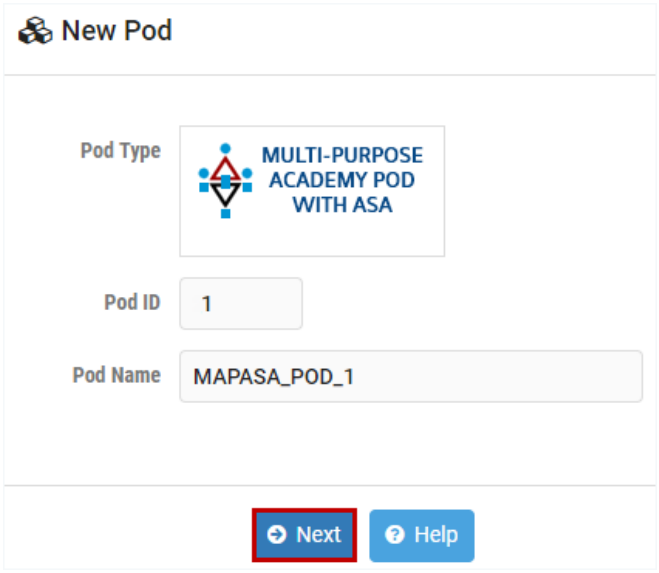
Follow the steps below to create a Multi-purpose Academy Pod with ASA.

1. From the Administrator Home Page, select Pods and then click the **Create New Pod** button.

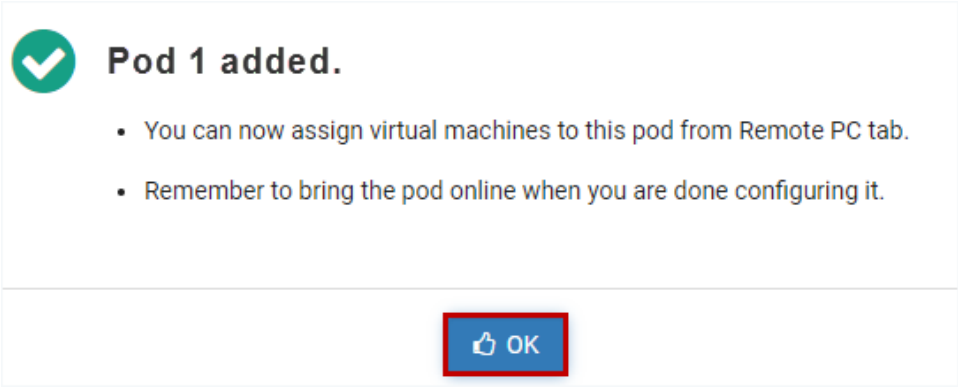
2. The list of Installed Pod Types is displayed (recall that these pod types were installed as part of the *Cisco Common Pod Types* course). Select the **MAPASA** by clicking anywhere on the row.



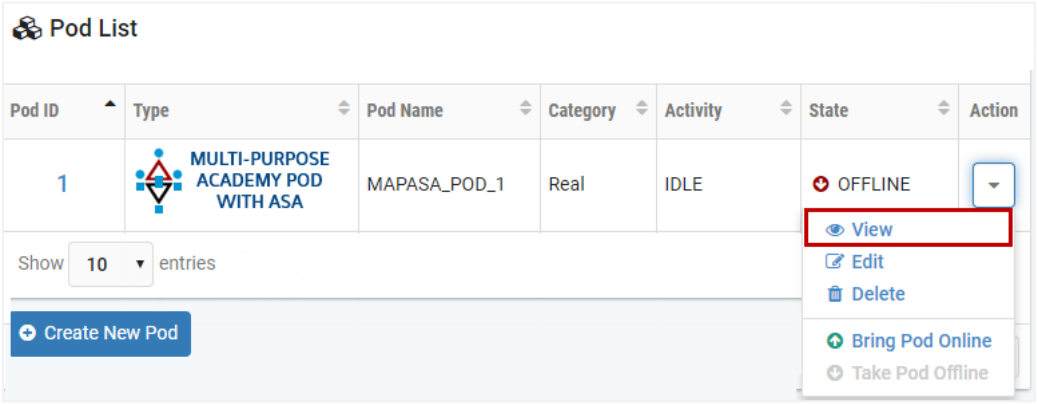
3. Enter values for Pod ID and Pod Name (or accept defaults) and then click **Next.**



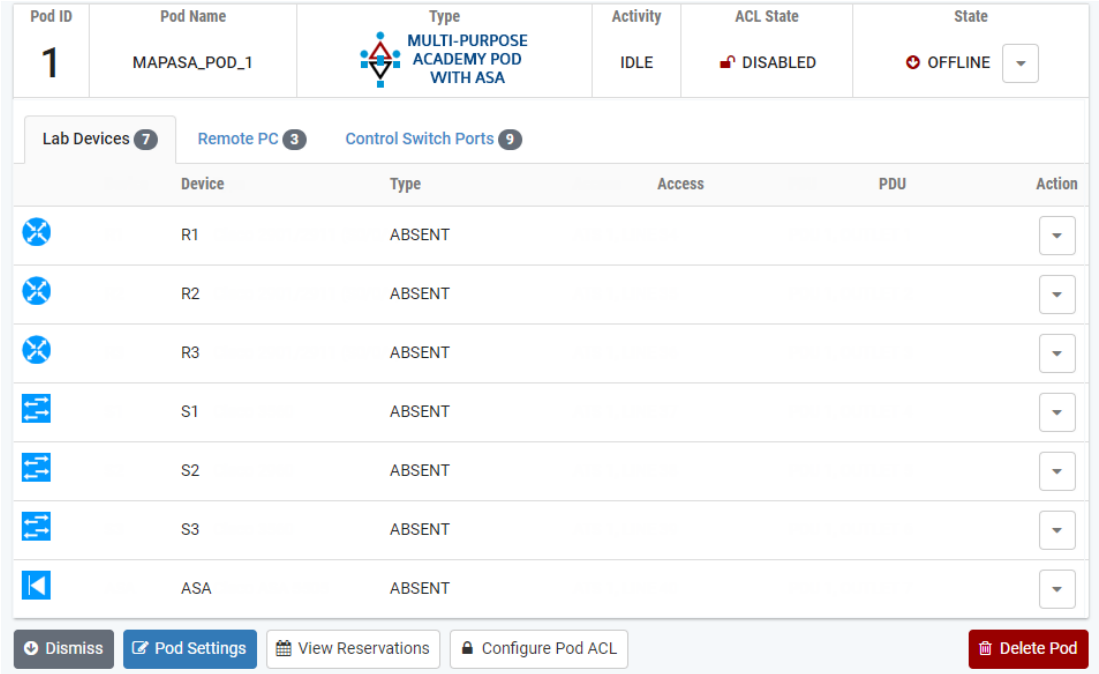
4. A message will confirm the pod has been added. Click **OK**.



5. The pod will now appear in the pod list. On the Action dropdown, select the option to **View** the pod details.



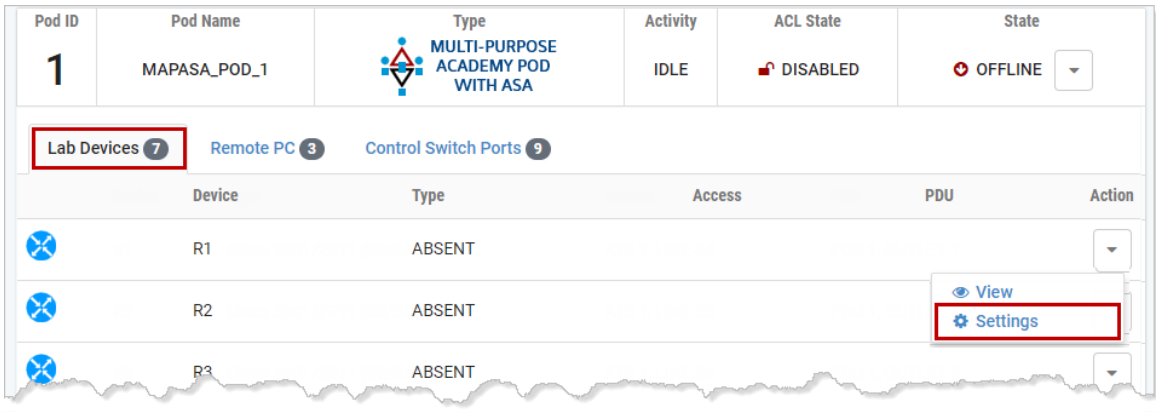
6. The pod detail page will be displayed. Continue to the subsections, where we will configure lab devices, remote PCs, and control switch ports.



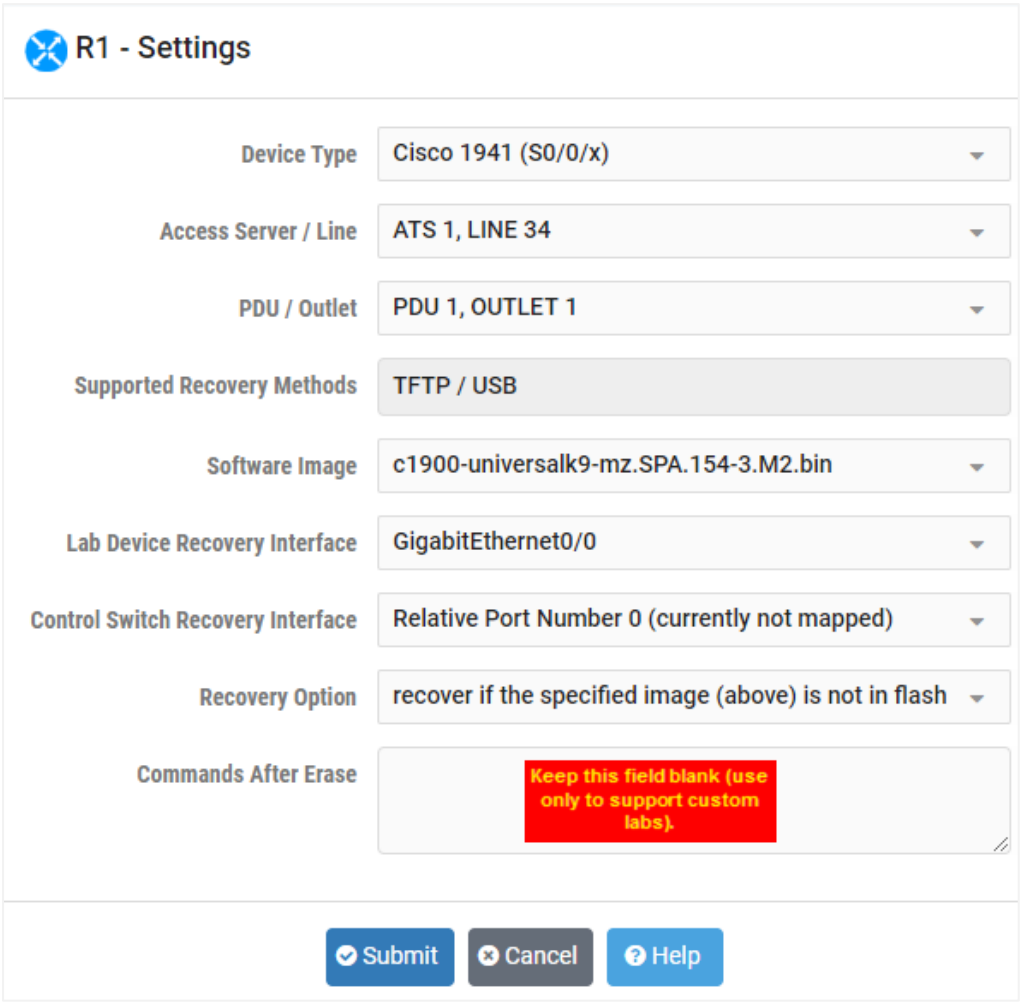
10.2.1 Configuring Lab Device Settings and Device Recovery

We will now configure the lab device settings for the devices shown on the Lab Devices tab of the pod detail page.

1. For the first device, router R1, select **Settings** on the Action dropdown.



2. On the settings page, select the appropriate values and then click **Submit**. For guidance on completing the form, see the field descriptions below or select **Help**.



Field Descriptions - Device Settings and Device Recovery

- **Device Type:** Select device type or ABSENT if the device is not implemented.

- **Access Server/Line:** Select the access server and line that connects to the async console port of this device. If the device does not have a console, select NONE.

- **PDU/Outlet:** Select the power distribution unit (PDU) and outlet that controls power to this device. If the device does not connect to a PDU, select NONE.

- **Supported Recovery Methods:** Supported recovery methods are determined by the selected Device Type and include the following; please also refer to the table in the *Lab Device Images* section for a summary of the methods for supported devices.

    - **NONE:** This device does not support any recovery method.

    - **TFTP:** This device can be recovered over TFTP using NETLAB+. Requirements:
        - The desired software image must be uploaded to NETLAB+ using the Administrator's *Lab Device Images* interface as described in the *Lab Device Images* section and then selected below.
        - An appropriate recovery interface must be selected for the device.
        - An appropriate recovery interface must be selected for the control switch.
        - A suitable recovery option must be selected.

    - **USB:** This device can be recovered from an attached USB storage device. Requirements:
        - The desired software image must be uploaded to NETLAB+ using the Administrator's *Lab Device Images* interface as described in the *Lab Device Images* section and then selected below.
        - The desired software image must be copied onto a USB storage device and inserted into an available USB port on this device. NDG recommends using USB storage devices with a physical write-lock switch. Activating this write lock before installing the USB storage device will ensure that the software image will not be overwritten during lab exercises.
        - Recovery options were tested by NDG using a 16GB physical write protection switcher USB flash drive; using this model or a comparable device is recommended: https://www.amazon.com/gp/product/B07B48H6WL/ref=ppx_yo_dt_b_asin_title_o08__o00_s00?ie=UTF8&psc=1
        - The names of the files on NETLAB+ and the USB storage device must be identical.
        - A suitable recovery option must be selected.

- **TFTP/USB:** This device can be recovered using either the TFTP or USB methods, provided that the respective requirements are met. NETLAB+ will first attempt to recover using USB, then TFTP if necessary.

- **Software Image:** Select the file name of the software image that this device should be running. Depending on the other device recovery settings, NETLAB+ will try to ensure that this device is always running this software image.

- **Lab Device Recovery Interface:** Select the interface on this device that NETLAB+ should use to recover the software image.

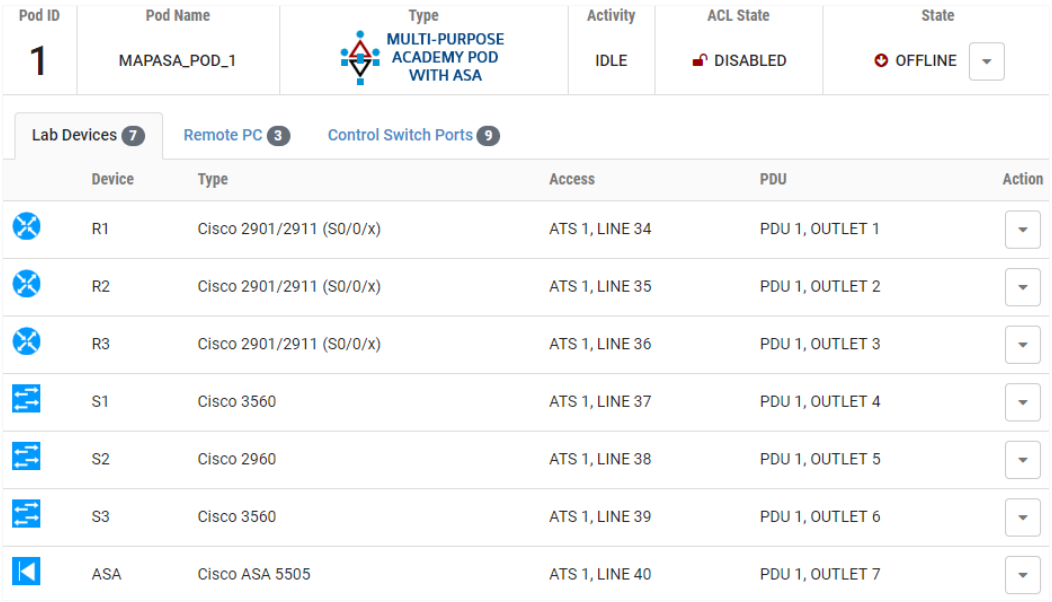
- **Control Switch Recovery Interface:** Select the interface on the control switch that NETLAB+ should use to recover the software image. This interface should be connected directly to the device recovery interface selected above.

- **Recovery Option:** Select the condition in which NETLAB+ will recover this device's software image. Options include:

  - Recover if the specified image is not in flash
  - Recover if there is no image in flash
  - Never recover image (the device may become unusable).

- **Commands After Erase:** This setting currently applies to Cisco devices with command-line interface only and is otherwise ignored. Commands entered here will be sent to the command line interface during lab cleanup after "write erase" has been issued. **This field should be left blank, with the exception of special use cases with custom labs** (described in a subsection below).

3. Select the device settings for the remaining lab devices. The values for Type, Access, and PDU should now be set similar to the picture below.



10.2.1.1 Post-Erase Custom Commands for Lab Device Configurations

This setting is applicable for advanced users who have created custom labs, in circumstances where it is desirable to specify commands to be executed on a device after the "write erase" has been issued during lab cleanup. See the use case below for an example.

If you are using Cisco labs provided by NDG there is no need to add commands, the **Commands After Erase** field should be left blank.

The **Commands After Erase** setting currently applies to Cisco devices with command-line interface only and is otherwise ignored. Commands entered will be sent to the command line interface during lab cleanup after "write erase" has been issued.

Use Case: On a Cisco switch, the *sdm prefer* setting is lost when NETLAB+ issues a *write erase* command at the end of the lab. This setting cannot be easily restored during lab load because it requires a reboot. The following configuration can be specified in the **Commands After Erase** field to set *sdm prefer* for next reload.

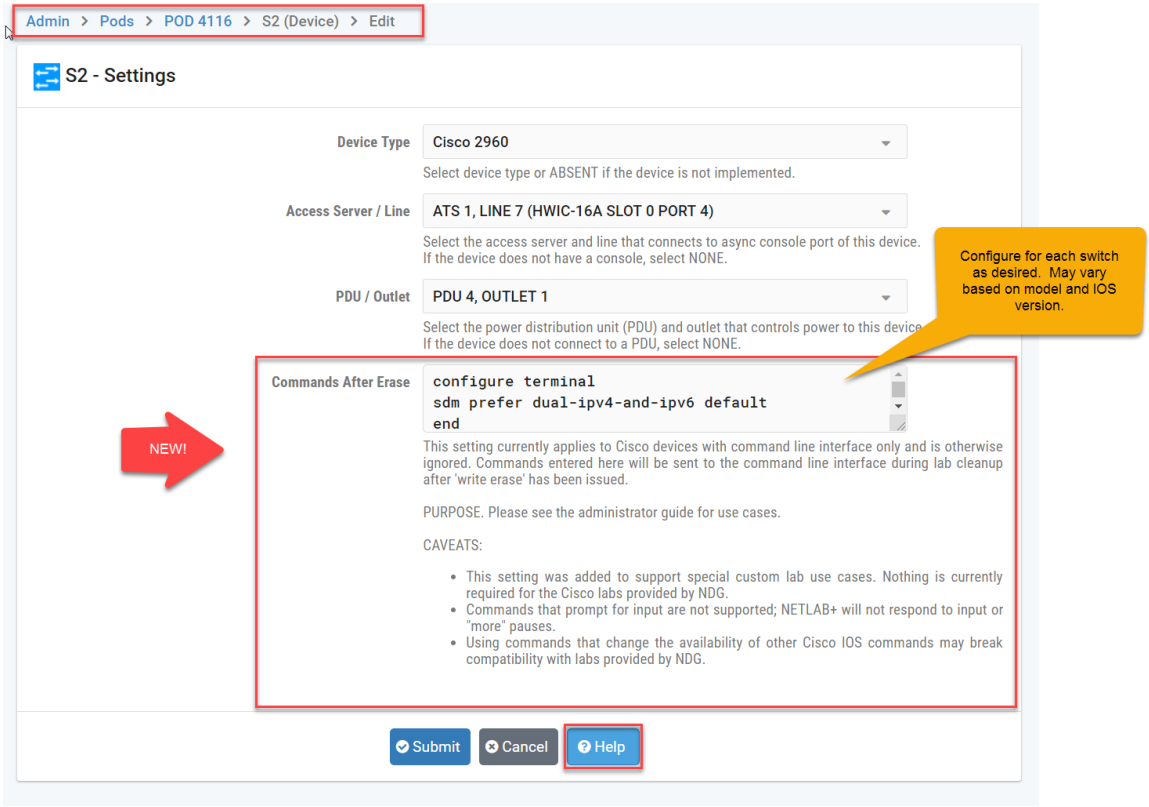
```
configure terminal
sdm prefer both-ipv4-and-ipv6 default
end
```

Be aware that NDG labs do not require the *sdm prefer* setting to be changed and doing so may break labs that require the default settings.

Perform the following steps to specify the commands to be executed after erase:

1. On the Lab Devices tab of the pod detail page, select a lab device to edit the settings.
2. Add the configuration commands to the **Commands After Erase** field and then click Submit.

Commands that prompt for input are not supported; NETLAB+ will not respond to input or "more" pauses. Using commands that change the availability of other Cisco IOS commands may break compatibility with labs provided by NDG.

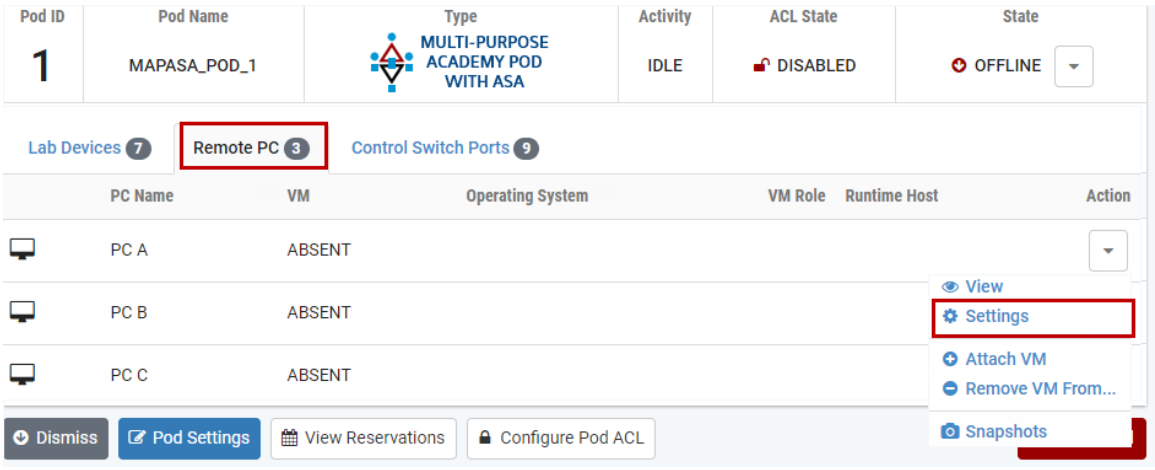


10.2.2 Configuring Remote PCs

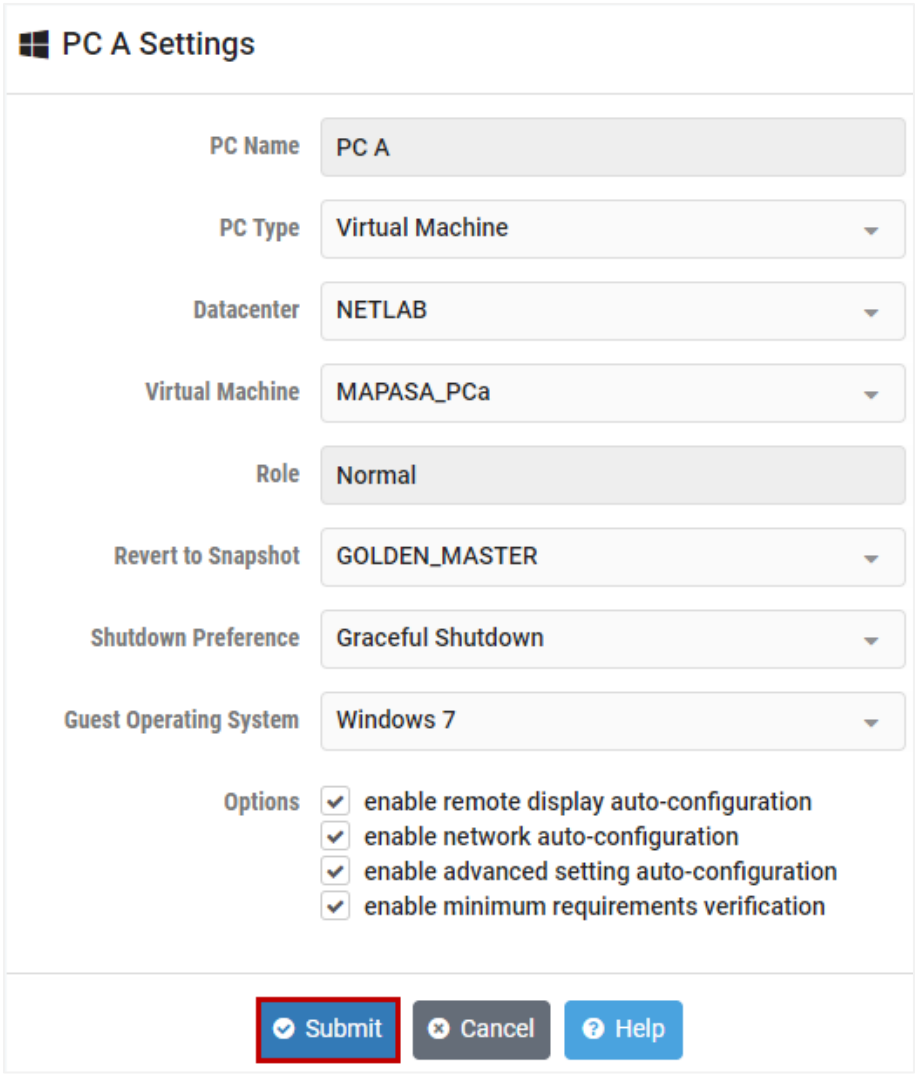
> The remote PCs required for your topology must be imported into the NETLAB+ virtual machine inventory. Please refer to *NETLAB+ Remote PC Guide Volume 3 - Configuring the NETLAB+ Virtual Machine Infrastructure*.

Next, we will configure the remote PCs shown on the Remote PC tab of the pod detail page.

1. For the first remote pc, PC A, select **Settings** on the Action dropdown.



2. On the settings page, select the appropriate values and then click **Submit**. For guidance on completing the form, see the field descriptions below or select **Help**.



Field Descriptions - PC Settings

- **PC Name:** The name of the PC as defined in the pod design.
- **PC Type:** The type of PC.
    - **Absent:** The PC will not be implemented in this pod.
    - **Use Virtual Machine Inventory:** Use a virtual machine defined in the NETLAB+ Virtual Machine Inventory. The VMI offers the most advanced VM configuration and automation capabilities available in NETLAB+.
- **Datacenter:** The virtual datacenter that contains the virtual machine to be used for this PC (unless overridden by a lab).
- **Virtual Machine:** The virtual machine that will be used for this PC.
- **Role:** The role the virtual machine plays in the inventory.

  - **Template:** A pristine virtual machine image used as the basis for cloning many virtual machines. Template VMs cannot be powered on, modified, or assigned to pods.
  - **Master:** A virtual machine used as the basis for cloning other virtual machines. Master VMs can be assigned to pods, modified, and powered on.
  - **Normal**: A virtual machine that can be assigned to a pod. A normal VM will typically revert to a specified snapshot at the start of a lab reservation.
  - **Persistent:** A virtual machine that can be assigned to a pod and retains its state between labs. A persistent VM is typically used in conjunction with Pod ACLs to create long-term personal pods.
  - **Runtime:** A temporary on-demand virtual machine that exists for one lab or lab reservation. These VMs are created and destroyed by NETLAB+ based on pod settings.

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

  This setting does not apply to virtual machines whose role is Persistent.

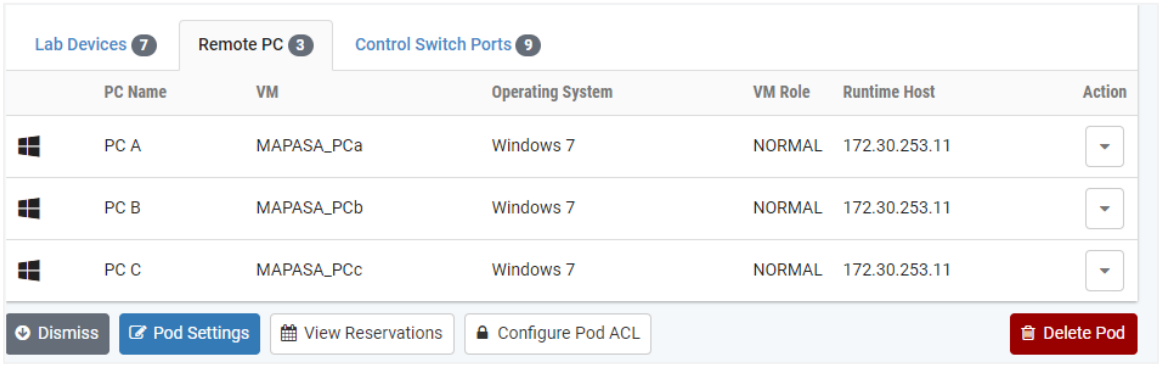
- **Shutdown Preference:** The preferred shutdown sequence if the virtual machine is still powered on at the end of a lab reservation. If Revert to Snapshot is configured (on a non-persistent VM), it is reverted first. If the virtual machine is still powered on after reverting to the snapshot, the preferred shutdown sequence is executed. Otherwise, the final power state will be the same as the snapshot state.

  - **Graceful Shutdown:** Performs an orderly shutdown from the operating system if possible (i.e., VMware Tools is installed on the VM). If an orderly shutdown is not possible, the virtual machine is powered off.
  - **Power Off:** Just like hitting the power button. Does not perform an orderly shutdown of the VM.
  - **Suspend:** Suspend the virtual machine in its current state. When powered on, it will resume in the same state without booting. This option requires a complete disk snapshot of the virtual machine's memory and page files, so you should use the suspend option only if you have plenty of disk storage. Network connection state is not preserved.
  - **Keep Running:** The virtual machine is left in the powered-on state. This is rarely desirable since host resources are not freed. In conjunction with Keep Running, a Revert to Snapshot setting of NONE is probably the right choice.

- **Guest Operating System:** The operating system running on this virtual machine.
- **Options:** Enable or disable automated features.

- **Enable remote display auto-configuration:** If enabled, NETLAB+ will automatically configure remote display parameters on the VM after a power on or revert to snapshot operation. This option allows VMs to be cloned without manual customization of the remote display settings. Therefore, we recommend you enable this setting and be happy about it.
- **Enable network auto-configuration:** If enabled, NETLAB+ will automatically bind the virtual machine's network adapters to the correct port group. This option allows VMs to be cloned without manual customization of networking bindings. This option is ignored if the pod type does not support automatic networking. If this setting is disabled and/or the pod type does not support automatic networking, then the virtual machine network adapters must be manually bound to the correct port group(s) using the vSphere client.
- **Enable advanced setting auto-configuration:** If enabled, NETLAB+ will automatically program advanced virtual machine settings that may be required for a particular pod type. For example, nested VM support for the VMware IT Academy program. It is usually safe to enable this option. It will be ignored if the pod type does not require advanced settings.
- **Enable minimum requirements verification:** If enabled, NETLAB+ will verify that the current settings of the virtual machine meet or exceed any minimum requirements established for the remote PC to which it is assigned. It is usually safe to enable this option. The setting will be ignored if the pod type does not specify a set of minimum requirements for the remote PC.

3. Select the settings for the remaining remote PCs. The settings should now be similar to the picture below.

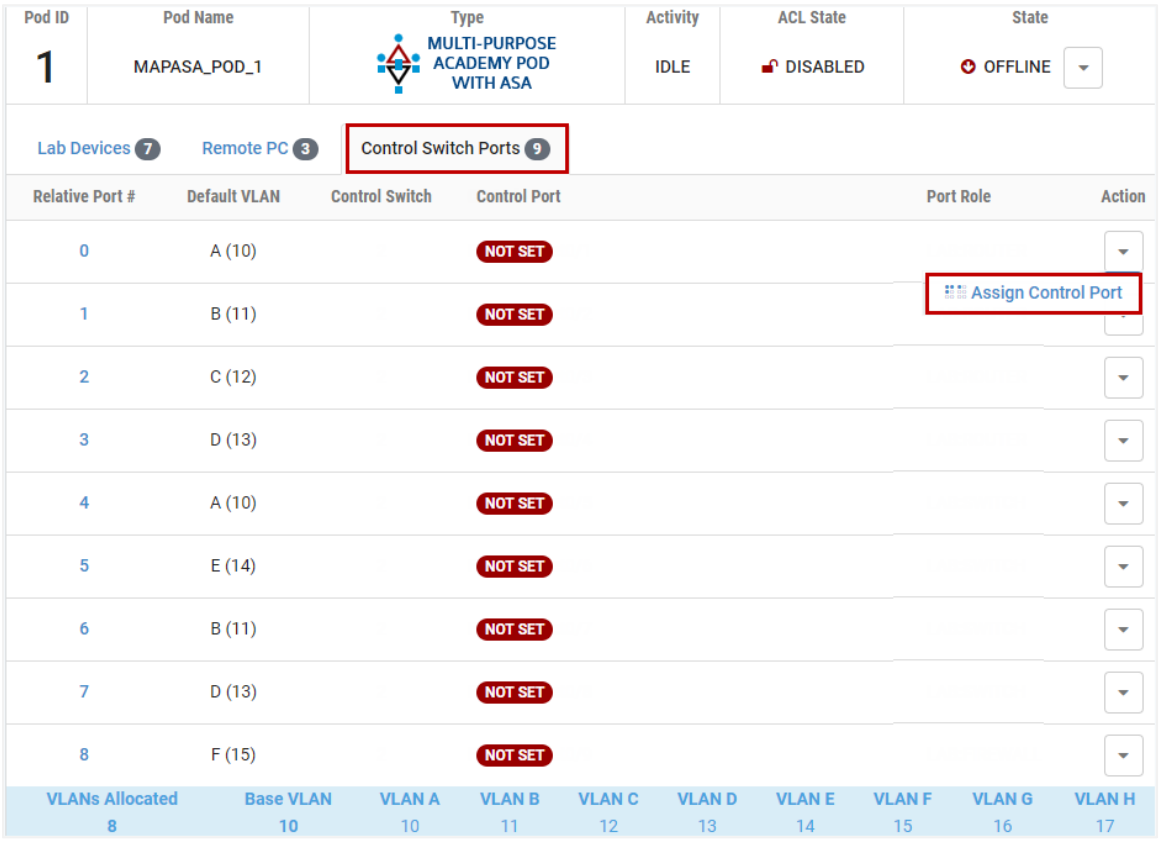


10.2.3 Configuring Control Port Bindings

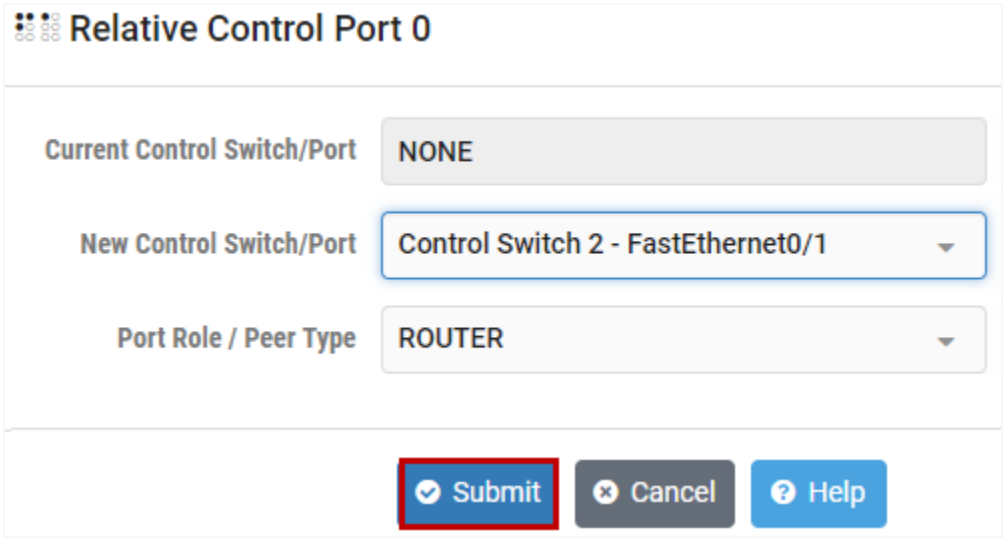
Lab device roles must be set on the control switch ports, as described in *Control Switch Port Roles*, prior to assigning control ports.

Now, we will configure the control switch and port assignment to the pod's relative control port.

1. For the first relative port number, select **Assign Control Port** on the Action dropdown.



2. On the Relative Control Port page, select the appropriate values and then click **Submit**. For guidance on completing the form, see the field descriptions below or select **Help**.



Field Descriptions - Relative Control Port

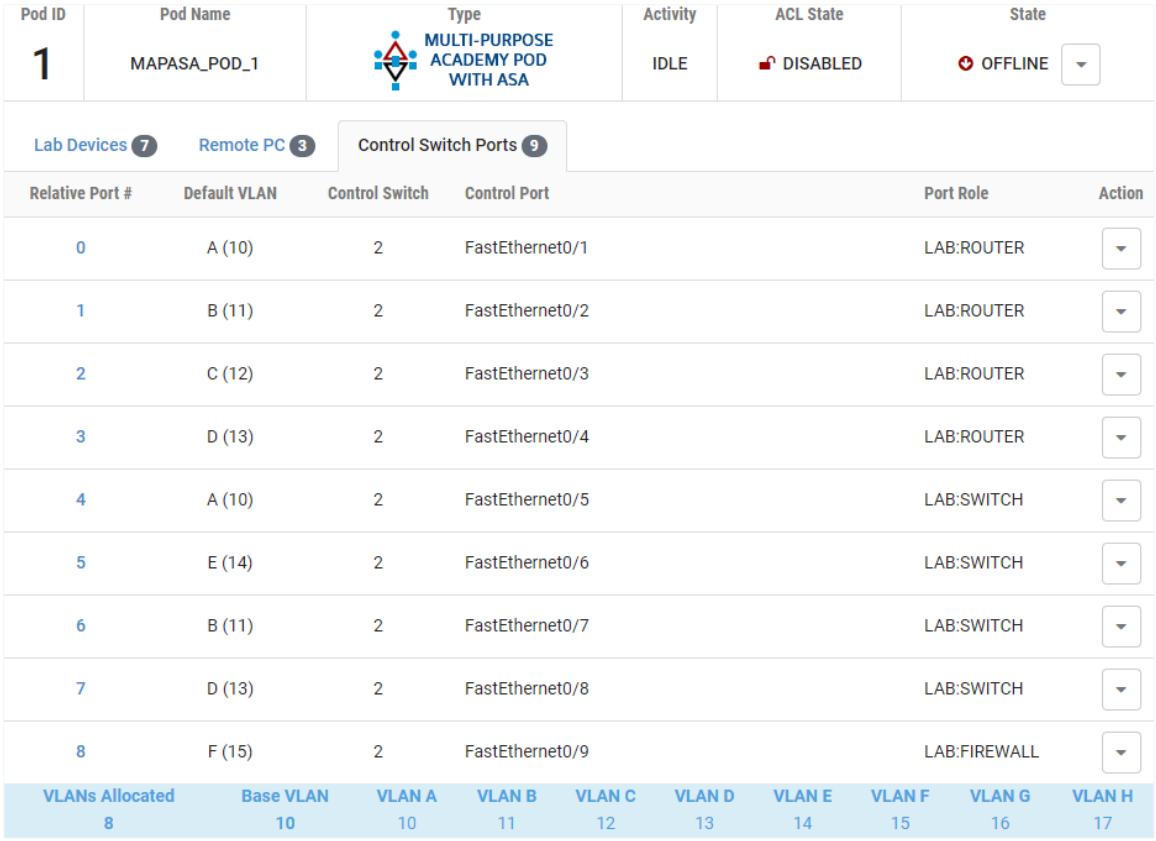
- **Current Control Switch/Port**: The control switch and port currently assigned to the pod's relative control port.

- **New Control Switch/Port:** The new control switch and port to be assigned to the pod's relative control port.

- **Port Role / Peer Type:** Select the role of the port. NETLAB+ will configure the control switch port accordingly.

    - **ROUTER**: The port is connected to a lab router or other non-switch device.
    - **SWITCH**: The port is connected to a lab switch.
    - **FIREWALL**: The port is connected to a lab firewall.
    - **STATIC:** The port will be allocated to this pod, but the control switch port will not be configured by NETLAB+ (i.e., manual configuration).

3. Assign the control ports for the remaining relative port numbers. The settings should now be similar to the picture below.



Pod ID	Pod Name	Type	Activity	ACL State	State
1	MAPASA_POD_1	MULTI-PURPOSE ACADEMY POD WITH ASA	IDLE	DISABLED	OFFLINE

Lab Devices 7 | Remote PC 3 | Control Switch Ports 9

Relative Port #	Default VLAN	Control Switch	Control Port	Port Role	Action
0	A (10)	2	FastEthernet0/1	LAB:ROUTER	
1	B (11)	2	FastEthernet0/2	LAB:ROUTER	
2	C (12)	2	FastEthernet0/3	LAB:ROUTER	
3	D (13)	2	FastEthernet0/4	LAB:ROUTER	
4	A (10)	2	FastEthernet0/5	LAB:SWITCH	
5	E (14)	2	FastEthernet0/6	LAB:SWITCH	
6	B (11)	2	FastEthernet0/7	LAB:SWITCH	
7	D (13)	2	FastEthernet0/8	LAB:SWITCH	
8	F (15)	2	FastEthernet0/9	LAB:FIREWALL	

VLANs Allocated	Base VLAN	VLAN A	VLAN B	VLAN C	VLAN D	VLAN E	VLAN F	VLAN G	VLAN H
8	10	10	11	12	13	14	15	16	17

10.2.4 Boot enable-break on Switches

The following switch models are subject to a common problem when used as a **lab switch**:

- Cisco Catalyst 2900 XL Series Switches
- Cisco Catalyst 2950 Series Switches
- Cisco Catalyst 2960 Series Switches
- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3650 Series Switches

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**.

Symptoms

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.

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. Notice the output below shows that enable-break is disabled.

```
Lab_Sw# show boot

BOOT path-list:      flash:c2950-i6q4l2-mz.121-22.EA4.bin
Config file:         flash:config.text
Private Config file: flash:private-config.text
Enable Break:        no
Manual Boot:         no
```

In the following procedure, enable-break is set to yes, and/or the BOOT path-list is set to an image.

Setting enable-break and BOOT path-list for 3650 Switches

```
Lab_Sw# configure terminal
Lab_Sw(config)# boot enable-break
Lab_Sw(config)# boot system flash:packages.conf
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
```


Setting enable-break and BOOT path-list (all other switches)

```
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
```

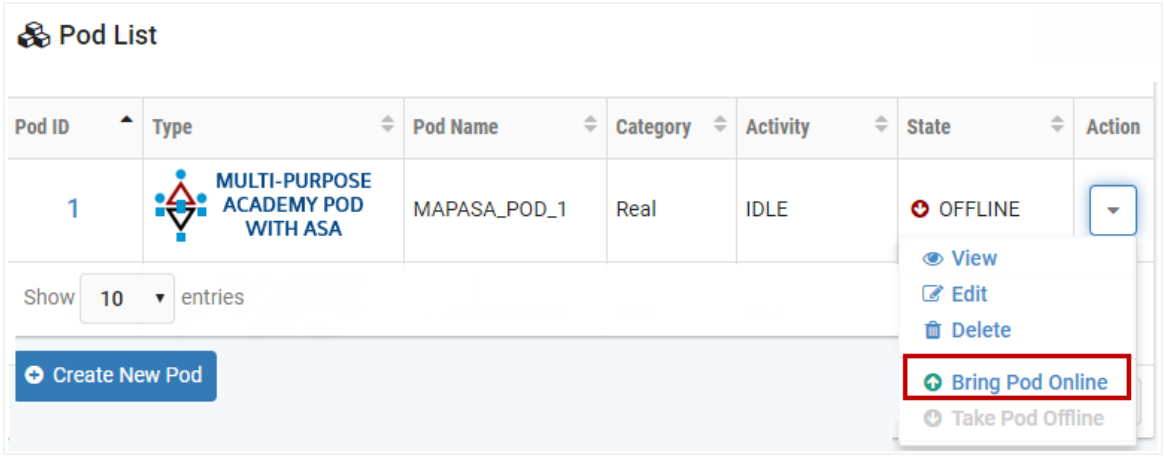
Verification

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

10.3 Bringing a Pod Online

For additional information on pod management, please see the *Equipment Pods section of the NETLAB+ VE Administrator Guide*.

Your pod must be brought online to be available for use. Select the option to **Bring Pod Online** on the Action dropdown.



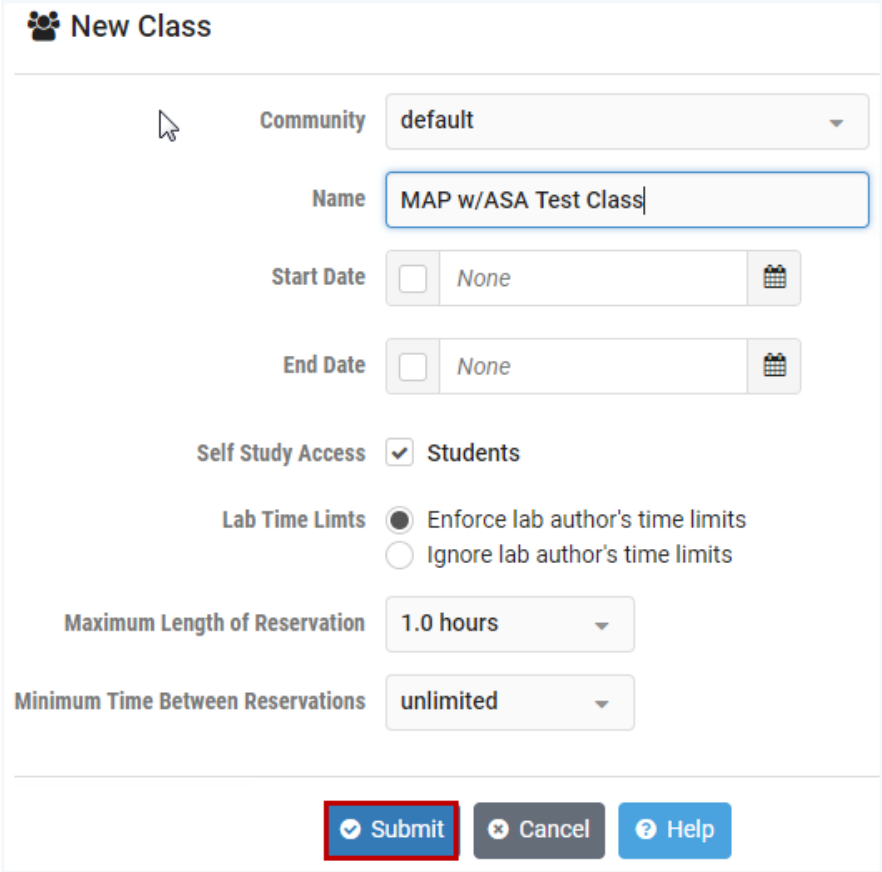
10.4 Testing a Pod

Test the pod to ensure it is operating properly before making it available to your user community. You will create a class and assign a lead instructor to the class in order to test the pod by making a lab reservation.

If you do not already have an instructor account, create an account (see the *Manage Accounts section of the NETLAB+ VE Administrator Guide*).

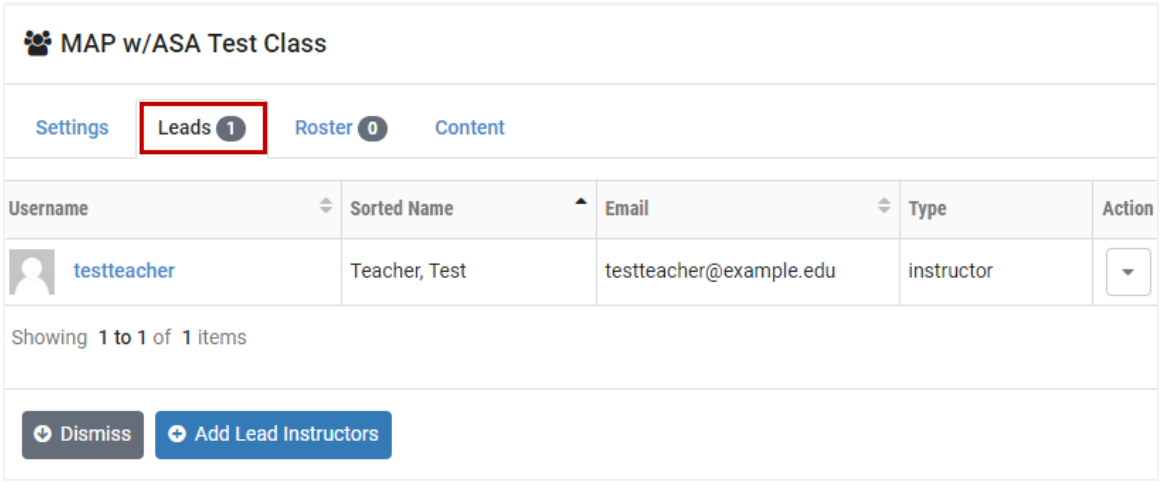
10.4.1 Creating a Class for Testing Purposes

1. From the Administrator Home page, select **Classes > Add Class**.
2. The New Class page will be displayed. Enter a name for your test class (default values are fine for the rest of the fields) and then click **Submit**.

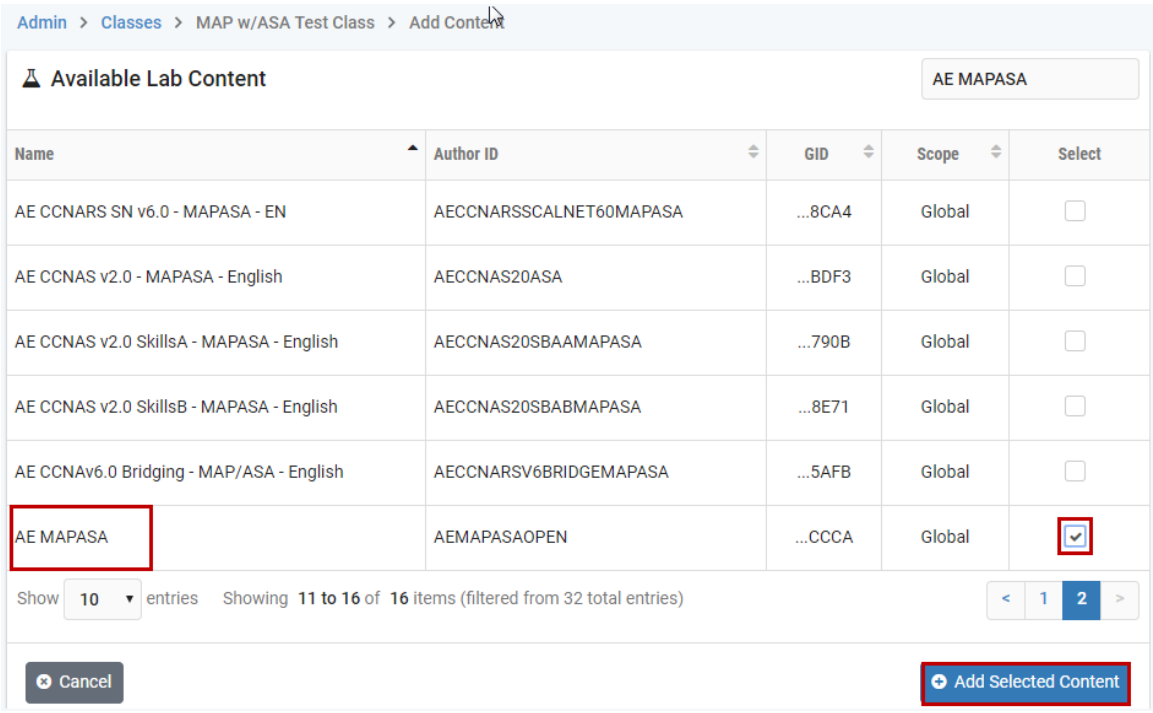


3. The class detail page will be displayed. Select the **Leads** tab and click **Add Lead Instructors**.

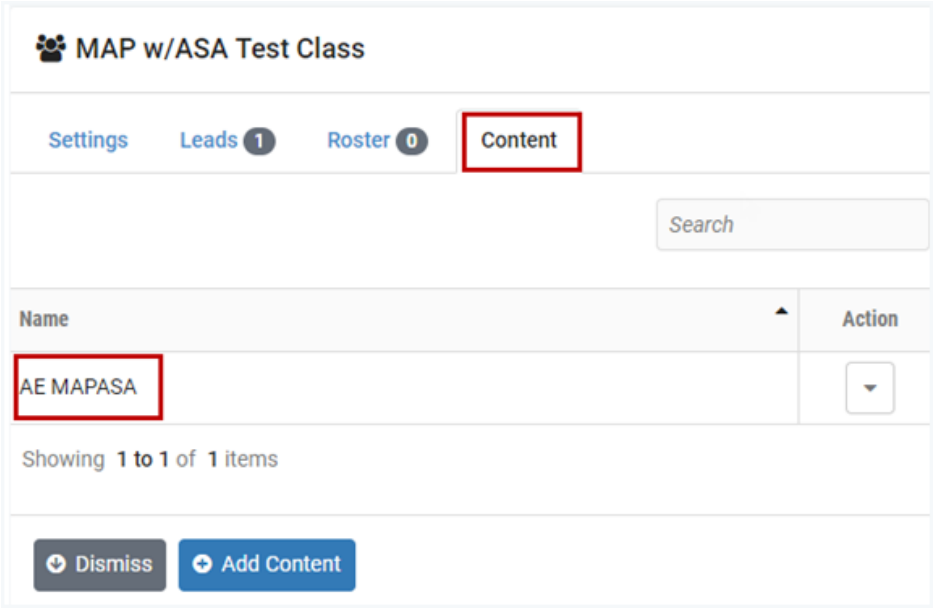
4. Using the Select checkbox, select your instructor account and then click **Add Selected**. Your instructor account is now listed as a lead for your test class.



5. Select the Content tab and click Add Content.
6. The Available Lab Content list will be displayed. The content that we will add is one of the lab designs we installed as part of the *Cisco Common Pod Types* course. Enter "AE MAPASA" in the search box to locate the content that will allow us to make pod-only lab reservations on the MAPASA.
7. Select the **AE MAPASA** content and then click **Add Selected Content**.



8. A message will display, confirming the content was added. Click OK.
9. The **AE MAPASA** content is now listed on the Content tab of the class detail page.



10.4.2 Performing a Lab Reservation and Monitoring the Pod Operation

To perform the functions in this section, you will be playing dual roles:

- An instructor, performing a lab reservation
- The administrator, monitoring the operation of the pod

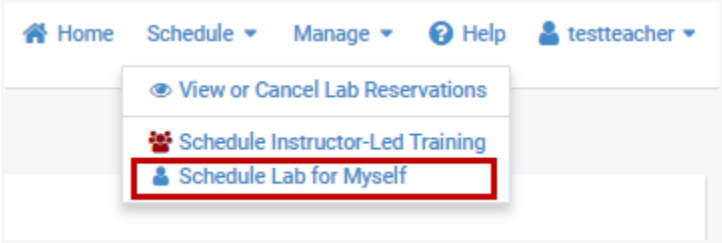
You will need two browser windows open so that you can be logged into both accounts simultaneously. It may be necessary to have one browser window set as incognito (depending on your browser selection and pc settings) to prevent any interference.

Monitoring from the Administrator account:

1. From the Administrator Home page, select Pods > *Your Pod.*
2. You will monitor the event log at the bottom of the pod detail page.

Performing a lab reservation from the Instructor account:

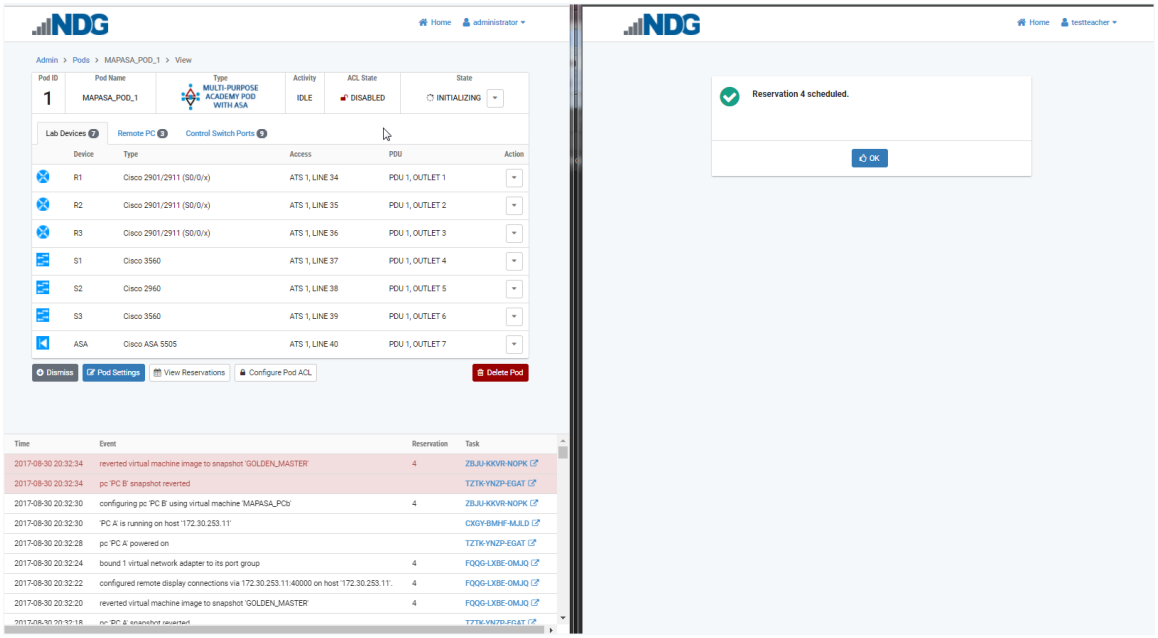
1. Click the Schedule option in the upper-right corner and select **Schedule Lab for Myself**.



2. Select **Reserve Multi-purpose Academy Pod with ASA (no lab exercise)** by selecting **Schedule Lab** on the Action dropdown.
3. Choose a reservation time on the calendar (select immediately below the red line on the calendar to begin the reservation ASAP).

In the Administrator window, notice the events in the pod event log as the pod is being configured for the reservation.

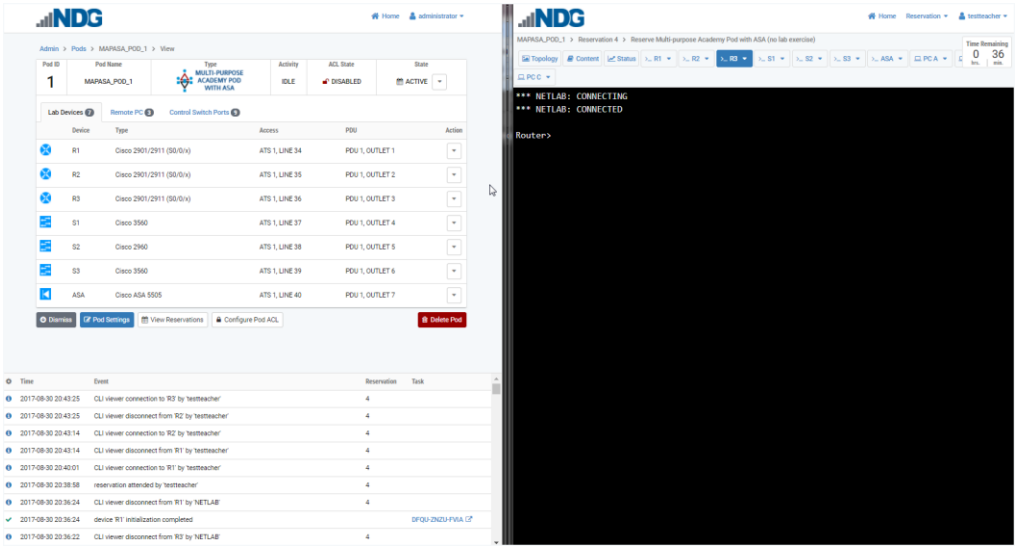
Administrator (watching pod page) **Instructor (reservation scheduled)**



4. The instructor enters the lab when available. The lab devices are listed at the top of the page. Click on each device to connect a viewer.

In the Administrator window, notice the events in the pod event log as a viewer connection is made to the devices.

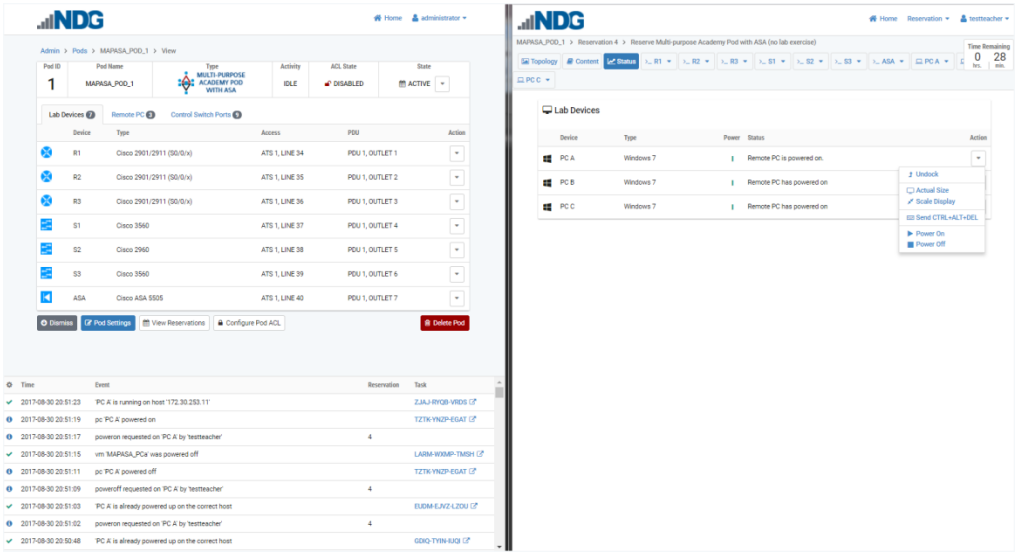
Administrator (watching pod page) **Instructor (connecting to devices)**



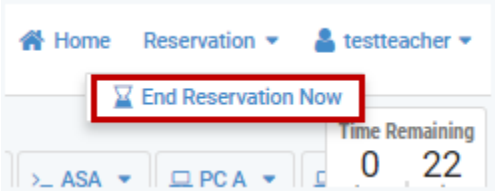
5. The instructor may also test the lab devices in the pod by performing some of the actions available from the Status tab, such as Power On, Power Off and Send CTRL+ALT+DELETE, or by entering commands at the prompt.

In the Administrator window, the event log will show the selected actions taking place on the pod.

Administrator (watching pod page) **Instructor (powering devices on and off)**

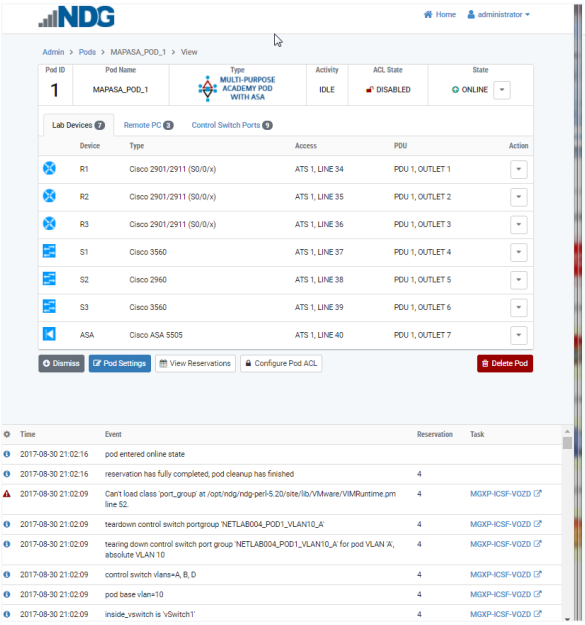


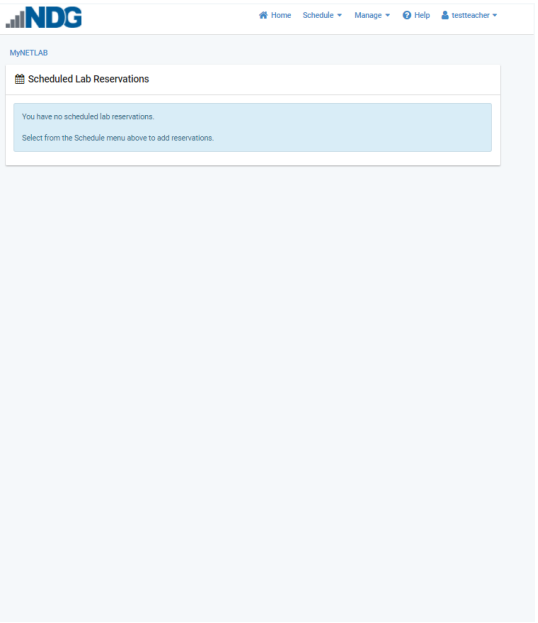
6. When you are finished testing the lab devices in the pod, click the Reservation option in the upper-right corner and select **End Reservation Now.**



In the Administrator window, the event log will show the reservation completed, and the pod cleanup finished.

Administrator (watching pod page) **Instructor (reservation has ended)**



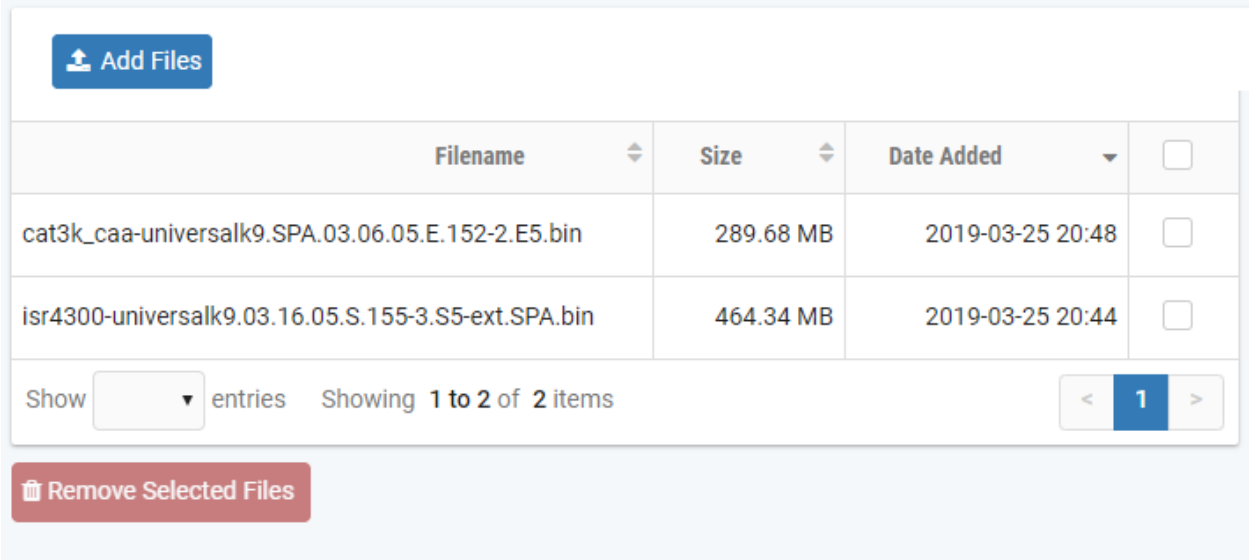


If you have observed no problems during the test lab reservation, you may proceed with making the pod available to your user community.

For details on account management, class management and scheduling lab reservations, please see the *NETLAB+ VE Administrator Guide*.

11 Lab Device Images

To manage lab device software images (i.e., Cisco IOS, SDM, etc.) in NETLAB+'s image repository, select **Lab Device Images** from the Pods and Infrastructure section of the Administrator Home page. Certain automated operations will install the specified images on lab devices via TFTP, as needed. All files must have a .bin or a .pkg extension. The subsections below describe the process of adding and removing image files from your NETLAB+ system.



Please refer to the table below for guidance on the available recovery options for installing the software image for your device. Guidance for setting the appropriate recovery options in NETLAB+ for a device is included in the *Configuring Lab Device Settings and Device Recovery* section.

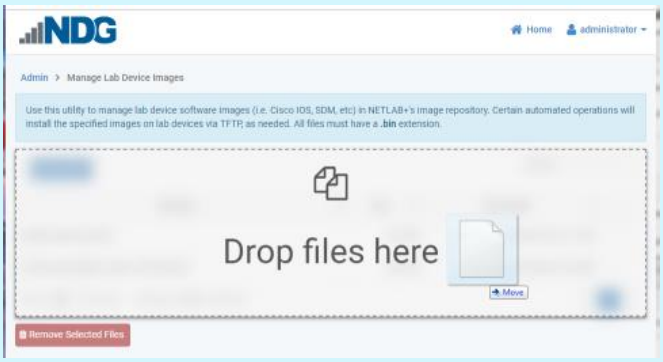
Lab Device Recovery Options

Model	Tested IOS	IOS Recovery Options
Cisco 1841	c1841-advipservicesk9-mz.124-10a.bin	TFTP
Cisco 1941	c1900-universalk9-mz.SPA.154-3.M2.bin	TFTP, USB
Cisco 4221	isr4200-universalk9_ias.16.07.01.SPA.bin	USB
Cisco 4321	isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin	USB
Cisco 4331	isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin	USB

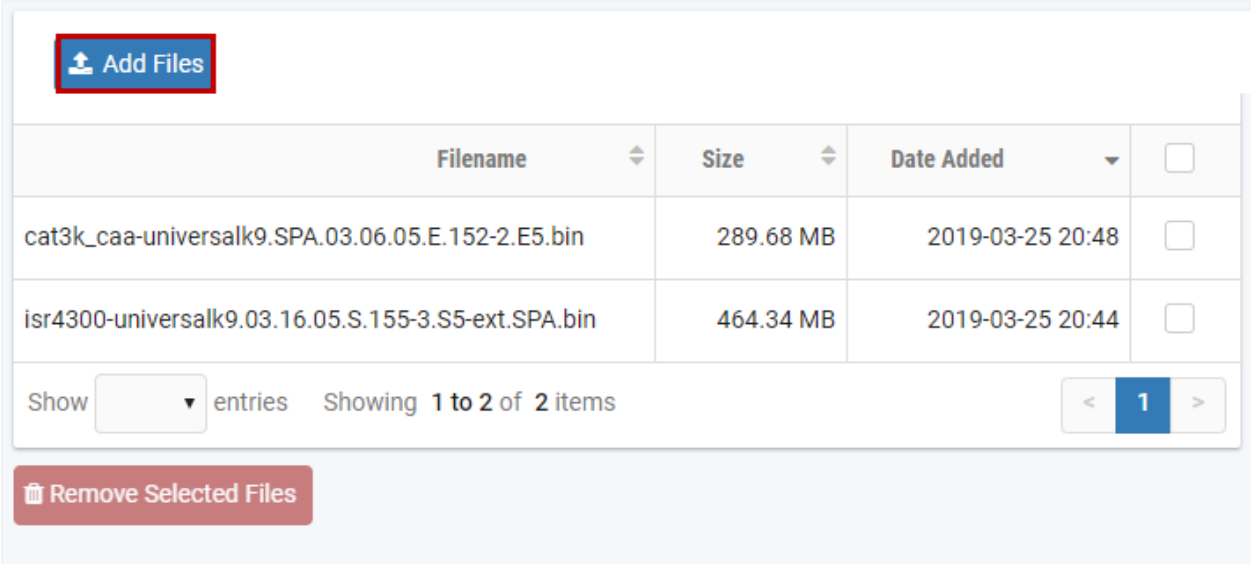
11.1 Add a Lab Device Image

There are two methods you may use for uploading lab device software images. The files can be dragged and dropped (as highlighted below) or by following the steps below:

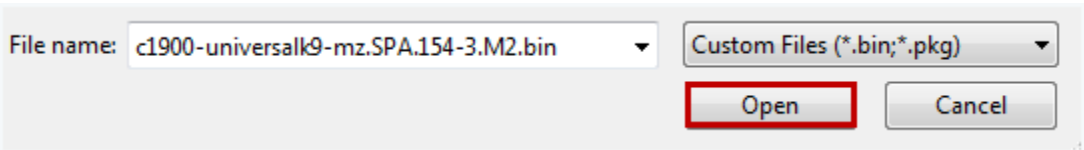
Image files can be dragged and dropped onto the Device Image table to upload.



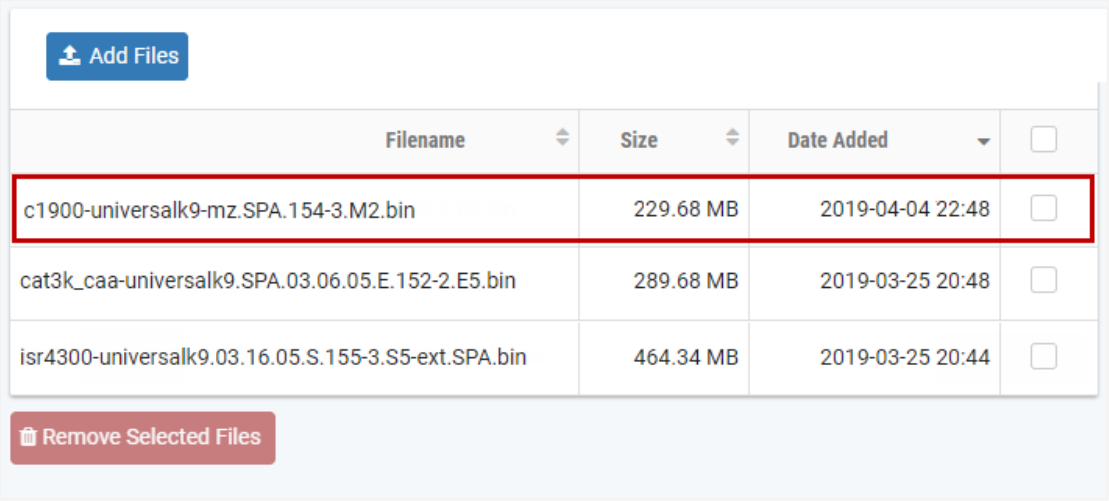
1. On the Manage Lab Device Images page, click the **Add Files** button.



2. Select the location of the file(s) that you want to upload (multiple files can be uploaded at once by selecting multiple files from the file browser), and click **Open**.



3. The file has been added to the list. The file will be available for selection as a device recovery option.

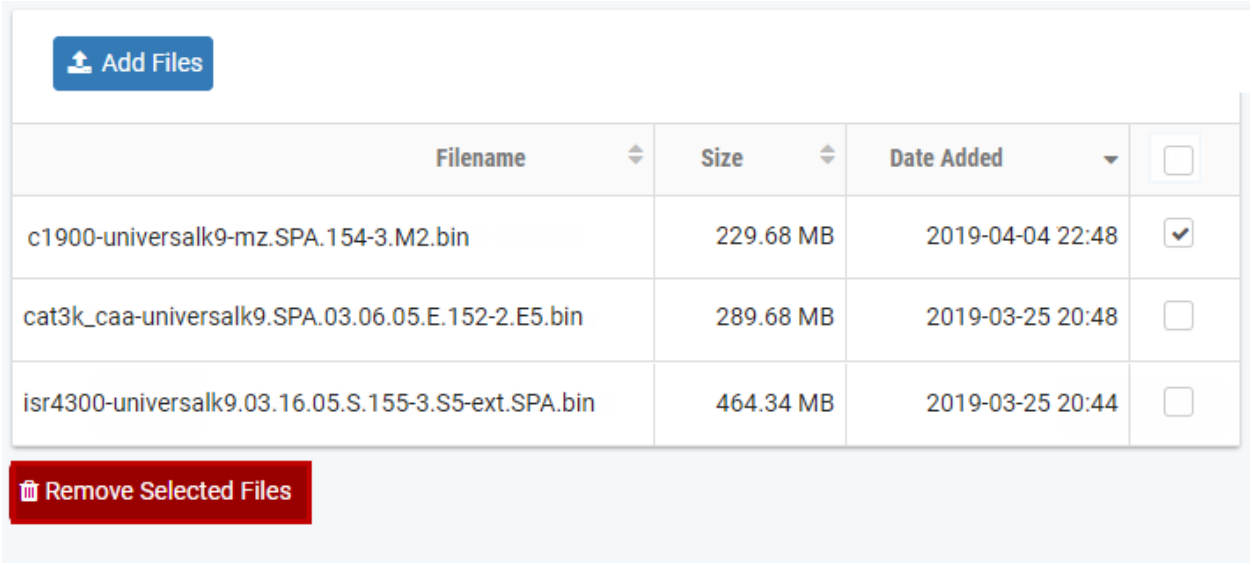


11.2 Remove a Lab Device Image

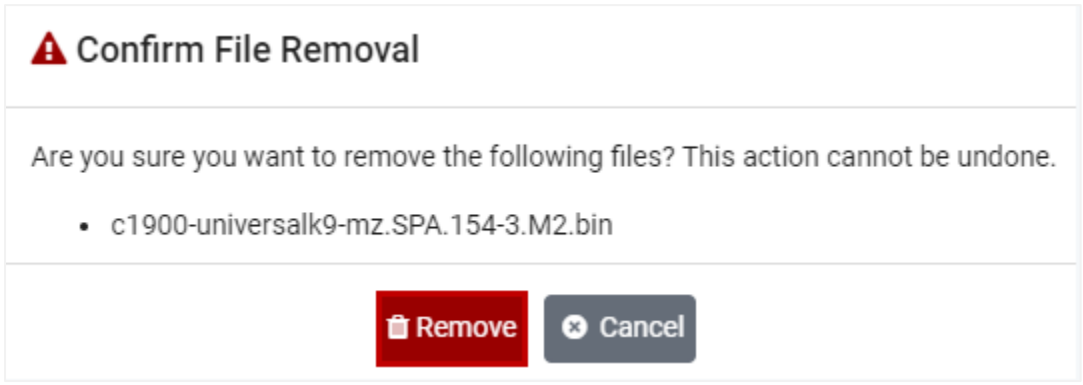
Perform the following steps to remove a lab device image file from your NETLAB+ system.

> Lab device images that are currently assigned for use to recover a device cannot be selected for removal. For these images, the checkbox will be disabled and unavailable for selection. See *Configuring Lab Device Settings and Device Recovery* for details on setting device recovery options.

1. On the Manage Lab Device Images page, click the checkbox at the end of the row of the file you want to delete (or check the box in the top-right column to select all available files).
2. Click **Remove Selected Files**.



3. You will be prompted to confirm that you want to delete the file. Click **Remove**.



12 Troubleshooting Tips and Known Issues

If you were unable to complete your lab reservation or observed problems, please review the items noted in this section.

12.1 Poor Virtual Machine Performance

During a recent installation performed by NDG, a bug was discovered when using VMware ESXi 6.0 **U2** on a Dell 630. The performance issue was resolved by upgrading the ESXi host server to 6.0 **U3**.

At this writing, our recommendation for those who are using a Dell 630 as the VM host server is to install **VMware ESXi 6.0 U3**:

https://downloads.dell.com/FOLDER04388318M/1/VMware-VMvisor-Installer-6.0.0.update03-5224934.x86_64-DellEMC_Customized-A03.iso

12.2 Access Server IOS

When using a HWIC-16A on a router (2901 or 2811) with IOS 15, you must use version **15.1.4M4(MD)**, due to a Cisco bug. NDG has tested **15.1.4M4(MD**) on all platforms (see *Access Server Requirements*).

