



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.



Pod Designer Guide

Document Version: **2024-02-06**



This guide documents pod design features available in **NETLAB+ version 22.7.0** and later.

Current NETLAB+ users of version 21.X.X and earlier: Please see the [NETLAB+ Pod Designer Guide](#) for guidance.

1	Introduction	5
1.1	Prerequisite Knowledge	5
1.2	Pod Types.....	6
1.2.1	Pure Virtual Machine Pods	7
1.2.2	Real Equipment Pods	8
1.2.3	Hybrid Design.....	9
1.3	Pod Design Best Practices.....	10
1.4	Pod Designer.....	11
1.5	Pod Designer Workflow	13
1.6	Granting Instructor Access to Pod Designer.....	14
1.7	Accessing Pod Designer	15
1.8	Viewing Pod Designs.....	16
1.9	Creating a New Pod Design	18
1.10	Pod Designer Tabbed Interface	20
1.10.1	Enabling Password Protection	21
1.11	Closing a Pod Design.....	22
2	Working with Graphical Images.....	23
2.1	Default Topology Image	23
2.1.1	Adding a Default Topology Image.....	23
2.1.2	Hotspots	25
2.1.3	Clearing the Default Topology Image	28
2.2	Scheduler Image	29
2.2.1	Adding a Scheduler Image	29
2.2.2	Clearing the Scheduler Image	31
3	Control Settings.....	32
3.1	Modifying Control Settings.....	33
3.2	Real Equipment Installation on a NETLAB+ VE System	35
3.3	Access Servers	37
3.4	Power Distribution Units	37
3.5	Control Switches.....	37
3.5.1	Control Ports	38
3.5.2	Lab Device Ports.....	38
3.5.3	Control Switch VLAN Numbers	42
3.5.4	VLAN Mapping	42
4	Lab Device Settings	47
4.1	Managed Lab Devices and Generic Console Devices	47
4.1.1	NETLAB+ Automation Features for Managed Lab Devices.....	48
4.1.2	Lab Routers	49
4.1.3	Lab Switches.....	51
4.1.3.1	Special Configuration for Pods Containing Lab Switches	53
4.1.3.2	VLAN Map Special Rule for Pods Containing Lab Switches	56
4.1.4	Lab Firewalls.....	59
4.1.5	Adding a Lab Device	61
4.1.6	Adding Hotspots.....	63
4.1.7	Cable Guidance	63
4.1.8	Modifying a Managed Lab Device.....	64

4.1.9	Deleting a Managed Lab Device.....	65
5	Remote PC.....	66
5.1	Managing Remote PCs.....	67
5.1.1	Adding a Remote PC	67
5.1.2	Setting Hotspots.....	68
5.1.3	Modifying a Remote PC	68
5.1.4	Removing a Remote PC.....	69
6	Advanced Settings.....	70
6.1	Modifying Advanced Settings.....	71
6.2	Advanced Configuration Directive Reference	72
6.2.1	Pod Requirement Configuration Directives	72
6.2.1.1	pod.requires.vm_same_host.....	72
6.2.1.2	pod.requires.vm_types.....	72
6.3	Automatic Networking Configuration Directives	74
6.3.1	pod.auto.net (category).....	74
6.3.1.1	pod.auto.net.supported	74
6.3.1.2	pod.auto.net.host.setup.supported	74
6.3.1.3	pod.auto.net.host.teardown.supported	75
6.3.2	Automatic Networking Support for Hybrid Pods.....	76
6.3.3	pod.auto.net.control_switch.VLANs.....	79
6.3.4	vswitch (category).....	81
6.4	Automatic Networking Configuration Directives	81
6.4.1	Automatic Networking for Pure Virtual Machine Pods	81
6.4.2	PC-Only Pod Designs	82
6.4.3	Hybrid Pod Designs	82
6.5	Virtual Machine Deferred Booting	82
6.5.1	pc.<x>.boot.delay=<seconds>	82
6.5.2	pc.<x>.boot.after_pc_index=<j>.....	83
6.5.3	pc.<x>.boot.after_pc_extra=<seconds>	84
6.6	Remote PCs.....	85
6.6.1	Adding a Remote PC	86
6.6.2	Modifying a Remote PC	87
6.6.3	Removing a Remote PC.....	87
7	Working With Pod Design Files and Builds	88
7.1	The Build Tab	89
7.2	Modifying a Build	89
7.3	Committing a Build	91
7.4	Installing a Build.....	93
7.5	Adding Pods	94
7.6	Creating Lab Exercises for Pods.....	95
7.7	Exporting and Backing Up Pod Design Files.....	96
7.8	Importing and Restoring Pod Design Files.....	97
7.9	Viewing a List of Installed Pod Designs	98
7.10	Uninstalling a Pod Design From the NETLAB+ Database.....	99



7.11 Creating a New Build 100

7.12 Retooling a Build..... 101

7.13 Cloning a Build 103

7.14 Deleting a Pod Design..... 104

1 Introduction

Pod Designer is used to create a custom pod layout. A *pod design* is a template used to create one or more actual pods on a NETLAB+ system.

1.1 Prerequisite Knowledge

Pod design is an advanced NETLAB+ topic. A comprehensive understanding of the core NETLAB+ components is required for pod design.

Pod design requires a working knowledge of the topics presented in the following guides:

- [NETLAB+ VE Designated Operating Environment Guide](#)
- [NETLAB+ VE Installation Guide](#)
- [NETLAB+ VE Administrator Guide](#)
- [NETLAB+ VE Instructor Guide](#)

For pods using physical lab devices such as routers, switches, and firewalls:

- [NETLAB+ VE Real Equipment Pod Management Guide](#)

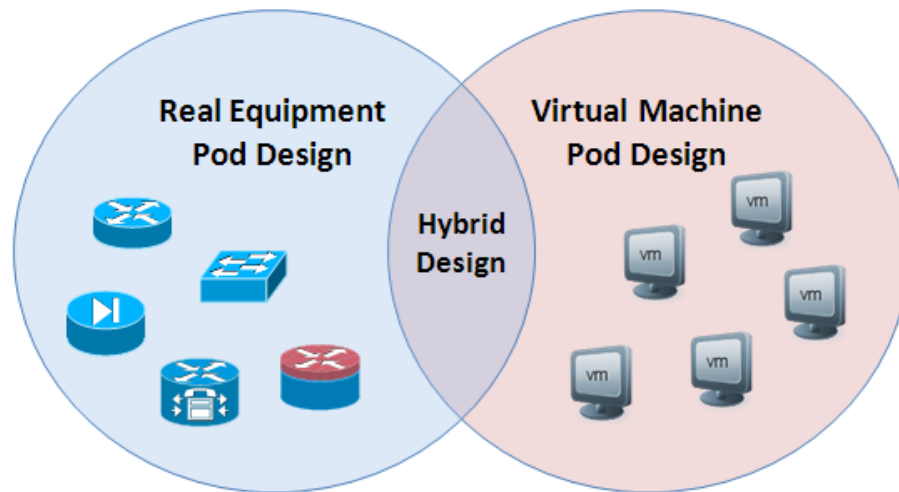
NDG provides a variety of standard pod types for NETLAB+ (which may vary depending on your membership in our curriculum partners' academic programs). We recommend standing up some NDG standard pods as a first step, allowing you to gain experience as a NETLAB+ administrator or instructor before exploring custom pod design.

Normal NDG support does not include custom pod design services. We offer Enhanced Services if you would like assistance with custom pod design.

1.2 Pod Types

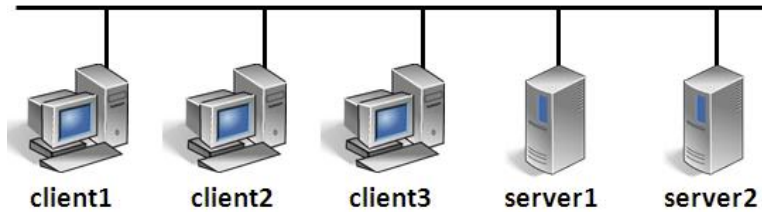
A pod is a single instance of a set of interconnected real equipment and/or virtual machines that students and instructors interact with during their training via the NETLAB+ system. A pod is reserved as a single resource from the scheduler. Each pod is normally isolated from all other pods and the internet, creating a safe sandbox for users.

Every pod derives from a pod design. A pod design can accommodate topologies that include real equipment, virtual machines, or both.



1.2.1 Pure Virtual Machine Pods

A *pure virtual machine pod* contains one or more virtual machines and no real equipment.



Pure virtual machine pods have some special properties:

- Virtual machine pods can be easily cloned using the NETLAB+ pod cloning tool.
- Virtual machines in the pod may be connected using virtual networking.
 - Virtual networks can be created and removed automatically.
 - No external networking is required.
 - All network traffic is confined to the pod.
 - Pods can be "air-gapped" from campus, providing a safe sandbox.
 - Pods do not need unique IP address schemes!

NETLAB+ provides mouse, keyboard, and screen (MKS) access to each VM through its built-in Remote PC viewers. The communication endpoint for viewer sessions is the NETLAB+ server, not the virtual machines in the pod. Therefore, the "air-gap" between the pod network and the campus network is still preserved.

To learn more about the NETLAB+ MKS Remote PC viewer, refer to the videos below:

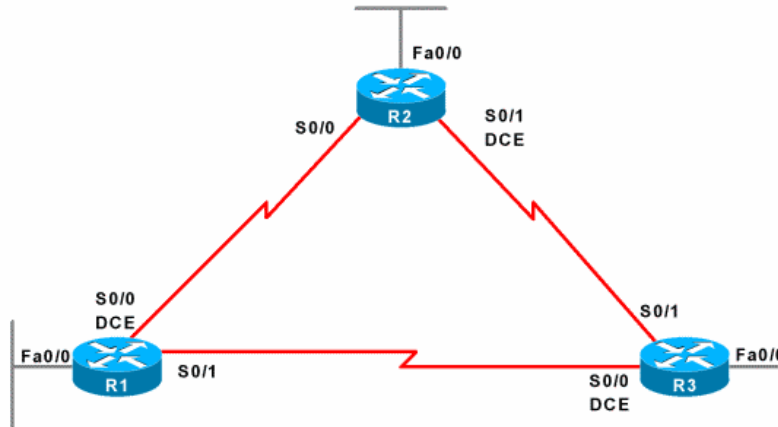
Part 1 - Overview and Resize Mode Demo: <https://youtu.be/7XE-zpOGPc>

Part 2 - Administrator Setup: https://youtu.be/l1r9_aMevl0

1.2.2 Real Equipment Pods

A *real equipment pod* contains one or more lab routers, switches, or firewalls.

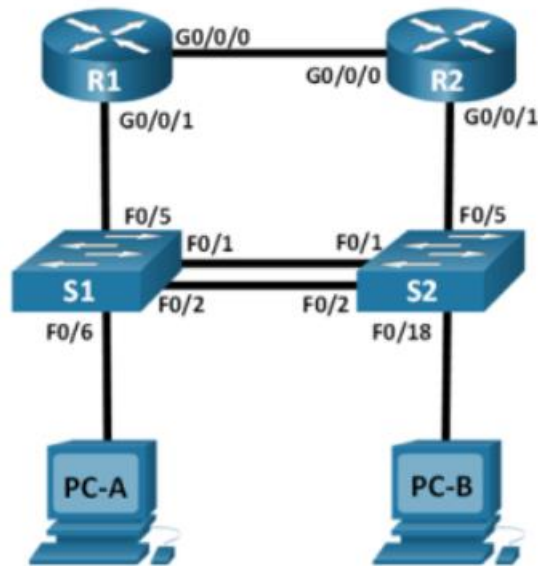
NETLAB+ provides console access to real equipment using its built-in CLI Terminal application and an Asynchronous Terminal Server (ATS). This provides an “air-gap” between equipment pods and campus networks. No routing between pod networks and campus is required.



Internal connectivity between lab devices can be made with direct physical connections or through NETLAB+ control switches. The latter provides dynamic network flexibility for labs. In either case, the real equipment pods are isolated from the campus to maintain a safe sandbox for learners.

1.2.3 Hybrid Design

You may build hybrid pod designs that contain both virtual machines and real equipment.



It is important to understand how real devices and virtual machines communicate with each other. Despite the interconnection of real and virtual, NETLAB+ provides the technology and methodology to isolate the entire pod from production networks while providing remote access to both real equipment and virtual machine consoles.

Recent versions of NETLAB+ support automatic networking support for hybrid pods to make the pod setup process significantly easier and less error-prone.

1.3 Pod Design Best Practices

The following pod design practices are highly recommended, particularly if you are creating pod designs that will be redistributable to other organizations. These practices are strictly followed by NDG during the planning and design of our "standard" pods.

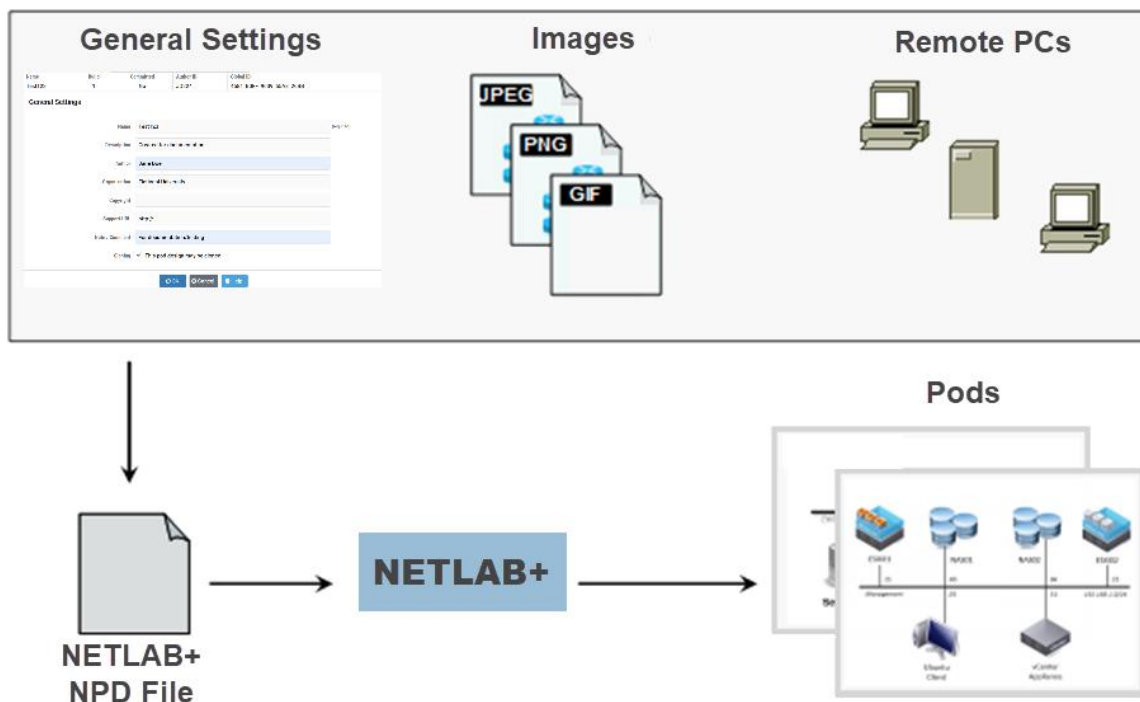
- Study all lab requirements carefully before pod design. Design pods that can service many labs and work across multiple curriculums if possible. Fewer pod types will increase adoption.
- Minimize the number of physical devices and virtual machines in a pod. Leverage the NETLAB+ VLAN map feature with real equipment pods to do more labs with fewer devices in the pod. Smaller pods:
 - Consume fewer system resources and physical devices
 - Tend to have a much higher adoption
 - Are better suited for asynchronous self-paced learning, which is the predominant modality for lab delivery using NETLAB+
- Create self-contained pods that do not require external or inter-pod network connectivity. This creates a safe sandbox for both users and host locations. It also allows labs to use a simple IP addressing scheme that is the same across all pods. Remember that NETLAB+ remote PC viewer and CLI terminal applications provide an out-of-band "air-gap" between real networks in pods. This feature should be leveraged in most cases.
- Create a pod guide (or web page) to assist others in setting up your pod design.

1.4 Pod Designer

Pod Designer is used to gather and store information about the layout of a pod. This data is stored in a *Pod Design File*.

Pod design files are portable. They can be shared, exported, and installed on other NETLAB+ systems. A set of options and passwords control how the pod design can be used.

Once a pod design is installed on a NETLAB+ system, you can add pods to the system based on the pod design.



A NETLAB+ pod design file contains all the information needed to represent a pod. The following items are contained within the pod design file.

- **General Settings**
 - Name
 - Description
 - Author
 - Organization
 - Copyrights
 - Support URL
 - Comments
 - Passwords
 - Cloning options
- **Images**
 - Topology image and clickable hotspots
 - Scheduler image
- **Control Plane (for systems that include real lab equipment)**
 - Access server port requirements
 - Switched outlet requirements
 - Control switch port requirements
 - Size of VLAN pool
 - Default VLAN map
- **Lab Devices**
 - Routers
 - Switches
 - Firewalls
- **Remote PCs**
 - Desktops
 - Servers
- **Advanced Settings**
 - Configuration directives for advanced networking


1.5 Pod Designer Workflow

The following steps outline the typical workflow of the pod design process.

1. Enter **General Information**.
2. **Add Default Topology Image.** Upload a graphic that will depict the pod's default topology.
3. **Define Hotspots.** Hotspots are rectangular areas on the topology image. When a user clicks on a hotspot, NETLAB+ opens the appropriate viewer and connects to the device.
4. **Add Scheduler Image.** Upload an optional small image that will appear in the scheduler. This icon graphically identifies the pod design.
5. **Specify Control Device Requirements.** If your pod design contains managed lab devices, the pod design must define certain control device resources. This includes the number of access server ports, switched outlets, and consecutive control switch ports.
6. **Specify VLAN Pool Size and Default VLAN Map.** A pod design containing managed lab devices will typically allocate a VLAN pool and default VLAN map.
7. **Add Managed Lab Devices.** Specify the lab devices NETLAB+ will manage.
8. **Add Remote PCs.** Specify the names of remotely accessible PCs.
9. **Commit Build.** When all the changes have been made, the *build* is committed. This prevents further changes to the current version of the pod design file and allows the pod design to be installed into the NETLAB+ database.
10. **Install Build.** Pod designer produces NPD files, which behave like software source code. To use the pod design, the administrator must install (compile) the NPD file into the NETLAB+ database.
11. **Add Pods.** The NETLAB+ administrator creates one or more pods based on the installed build.

1.6 Granting Instructor Access to Pod Designer

Pod Designer can be used from the NETLAB+ administrator account or from an instructor account. To use Pod Designer from an instructor account, the NETLAB+ administrator must specifically grant Pod Designer access to the instructor's account by selecting the **Pod Designer** privilege checkbox. Account management is described in detail in the [NETLAB+ VE Instructor Guide](#).

 **testteacher**

Username

testteacher

Full Name

Test Teacher

Display Name

Test Teacher

Sorted Name

Teacher, Test

Email

testteacher@example.edu

Enable Logins

☒ enabled

Type

Instructor ▼

Privileges

☐ Community Administrator

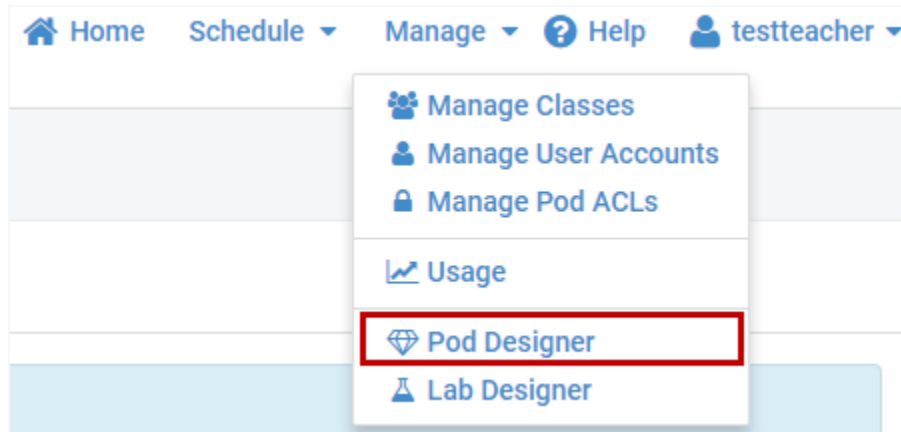
☒ Pod Designer

☒ Lab Designer

1.7 Accessing Pod Designer


The NETLAB+ administrator may access the Pod Designer by simply clicking on the Pod Designer icon on the administrator home page; instructors access Pod designer as shown below.

1. To access the Pod Designer, click **Manage** in the upper-right corner of the Home page and select the **Pod Designer** dropdown option.



Instructors have access to the Pod Designer if the NETLAB+ Administrator has enabled their instructor account with access to the tool. Contact your NETLAB+ Administrator if an error message indicates that you do not have access.

2. If this is your first time accessing the Pod Designer, you will be required to accept the terms and conditions. Review the notice and then click **Accept**.

 **Terms and Conditions**

NOTICE OF TERMS REGARDING POD AND LAB DESIGN COMPONENTS

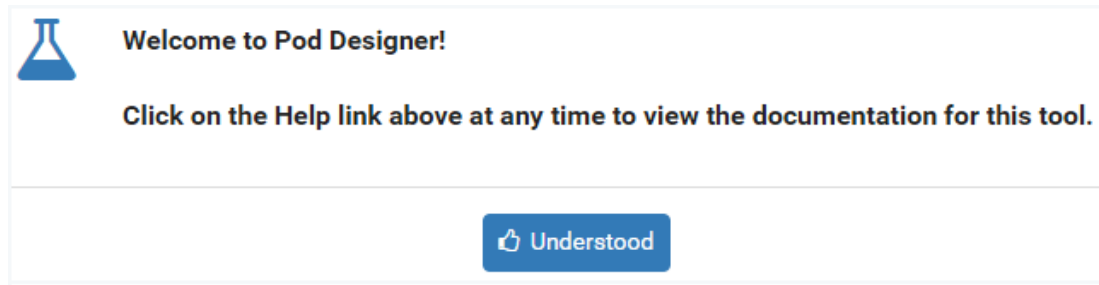
This Notice contains binding terms regarding use of features included in the Pod Designer and Lab Designer components of the NETLAB+ software provided to you (Customer) by Network Development Group, Inc. ("NDG"). By using these tools, you agree that you are authorized to bind and do hereby bind your employer to the terms of this Notice. This Notice supplements the existing agreement terms (Agreement) between NDG and Customer regarding use of NDG software. The Agreement is hereby modified and supplemented by mutual consent with the terms of this Notice.

The pod and lab tools components of Network Development Group's (NDG's) Software allows you to import network designs, lab exercises, curriculum, and other content (Content). All such Content shall remain the intellectual property of Customer or of its suppliers. However, if such Content is made available to NDG as part of the service(s) provided by NDG, then Customer grants to NDG the royalty-free, perpetual, non-exclusive, and transferable right to use the Content and to publish the Content to Authorized Users, in connection with NDG's delivery of the Software and related services under this Agreement, along with internal operational and product development activities.

Customer represents and warrants that: (a) the Content is owned by Customer, or to the extent owned by a third-party Customer has obtained the written agreement of such third party to provide the Content to NDG for access, use and copying under the license in this Agreement; (b) the Content does not violate any third-party copyright, trademark, trade secret or other intellectual property right; and (c) the Content does not include and will not transmit any information, software, or other materials constituting a virus, trojan horse, worm or other harmful computer programming routine that might damage the Software or any NDG service. Customer further acknowledges and agrees that NDG shall have no responsibility for any access or use by Authorized Users of the Content, including but not limited to any reverse engineering by Authorized Users of the Content.

Customer agrees to indemnify and hold harmless NDG and its employees, agents, affiliates, officers and directors against suits, claims, loss, damage, expense, penalty or liability arising from any breach of the above warranties or otherwise relating to the Content, unless due to the gross negligence or intentional misconduct of NDG.

3. A welcome message will be displayed; click **Understood**.



1.8 Viewing Pod Designs

The administrator and each instructor share a common pod design folder on the server. Therefore, you may see pod design files created by other users. This is different from lab designer, where each user has a personal folder. The pod design folder is shared because instructors and the administrator must work closely together to ensure that the NETLAB+ environment has adequate resources to accommodate the pod design. This is also why instructors must be explicitly authorized to use the pod designer.

Although the pod design files are located in the same folder, a set of passwords can be assigned to each pod design file to control modification, installation, and derivative works.

Pod and lab content provided by NDG is installed directly from the Course Manager. The underlying pod designs used to create this content do not appear in the Pod Designer tool.

To see a list of the pod designs available on your NETLAB+ system:

1. The **Pod Design List** is displayed when the Pod Designer option is selected on the Manage dropdown (see the previous section for info on first-time access).
2. To see the pod designs that have been installed in the local NETLAB+ pod-type database on this system, click **Show Installed Pod Designs**.

Pod Designer								
Search								
Name	Build	Commit	Author ID	GID	Author	Size	Modified	
NISGTC Network+	12	Yes	DOLNETP	...15D6	NDGTH	124K	2014-02-10	
NISGTC Security+	9	Yes	DOLSECPV2	...5A23	NDGJJ	35K	2015-08-21	
RHSA7	3	Yes	RHSA7	...A22E	NDGJJ	37K	2016-01-13	
VMware VCA DCV 6	4	Yes	VMVCADC6V6	...F6DE	NDGJJ	32K	2016-01-15	
VMware vSphere ICM 6	4	Yes	VCPICM6F1	...78BE	NDGTK	72K	2016-01-14	


Dismiss
Create New Pod Design
Show Installed Pod Designs
Import Pod Design

- The currently installed pod designs will be displayed. The **Used** column indicates the number of instantiated pods of each type. Click on a pod for additional details and management options. Select the **View** option on the Action dropdown to see additional details for any of the pods displayed.


Manage Installed Pod Designs						
Search						
Name	Build	Author/Org	Used	Icon/Type	Action	
NISGTC Network+	12	NDGTH NISGTC	4	n/a		
NISGTC Security+	9	NDGJJ NISGTC	3		View Uninstall	
RHSA7	3	NDGJJ NDG	0	n/a		
VMware VCA DCV 6	4	NDGJJ NDG	0	n/a		
VMware vSphere ICM 6	4	NDGTK NDG	0	n/a		

Dismiss

- Details of the pod design are displayed. Click **Dismiss** to return to the list of installed pod designs.

 **NISGTC Network+**

Name	NISGTC Network+
Build	12
Author ID	DOLNETP
Global ID	0025_9015_B226_519E_15D6
Description	NISGTC Network+ Pod
Author	NDGTH
Organization	NISGTC
Copyright	2014
Support URL	http://netdevgroup.com/content/networkplus/
Note / Comment	
Origin	Academy Edition
Used	0
Can Uninstall	Yes, by administrator

 Dismiss

1.9 Creating a New Pod Design

Follow the steps below to create a new pod design.

1. To add a new pod design, select the **Create New Pod Design** button at the bottom of the Pod Designer page.



2. Enter the class information into the **General Settings** (refer to the field descriptions below or click the **Help** button to display descriptions). Click **OK**.

Name	Build	Committed	Author ID	Global ID
NDG Advanced Ethical Hacking	1	No	NDGKL	0050_56BF_5E52_5EFE_0F59

General

Image

Control


Device

Remote PC

Advanced

Build

Name	NDG Advanced Ethical Hacking		
Description	Advanced Ethical Hacking		
Author	Jane Doe		
Organization	Fictional University		
Copyright	Copyright (c) 2020, Fictional University		
Support URL	https://fictionaluniversity.edu		
Note / Comment	Created for Jane Doe's Advanced Class		
Modification Password	not required	<input type="checkbox"/> Require a Password	
Installation Password	not required	<input type="checkbox"/> Require a Password	
Cloning Permitted	Yes		
Cloning Password	not required	<input type="checkbox"/> Require a Password	

 Modify General Settings

Field Descriptions – General Settings

- **Name:** This required field is used to assign a name to the Pod Design. It may be helpful to indicate the course with which the lab will be used as part of the name or description.
- **Author's Pod Design ID:** A unique, human-readable identifier. Only the characters **A-Z** and **0-9** can be used. This value is appended to the Global Pod Design ID to create a worldwide unique identifier for the Pod design. **Please note, you cannot modify this value later.** Tip: Use a combination of organization, course, and version. Examples:

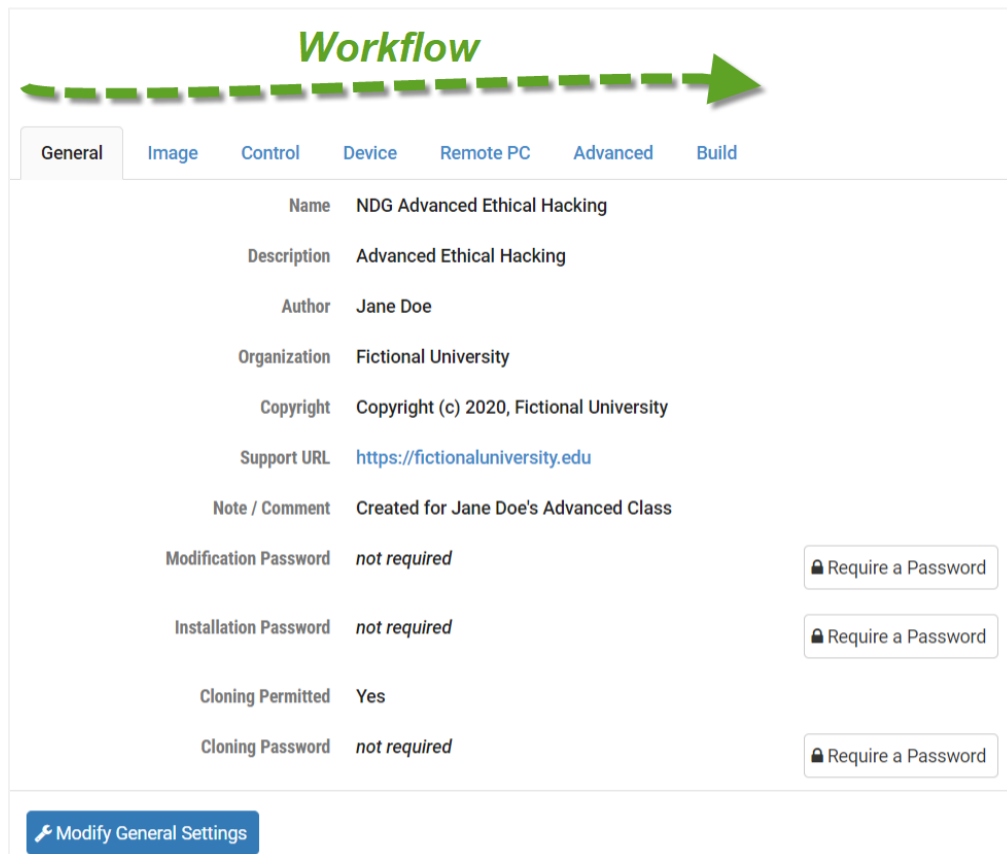
UCCBGP200	University of Central Calendonia, BGP, version 2.0.0
FSUSECP101	Fredrick State University, Security Plus, version 1.0.1
URIOT11	University of Redmond, Internet of Things, version 1.1

- **Description:** This optional field is used to describe the lab content. It may be helpful to indicate the number and types of devices in the pod.
- **Author:** Optional field to indicate the author of the lab content.
- **Organization:** Name of school or organization associated with the lab content.

- **Copyright:** A place for a copyright notice (optional).
- **Support URL:** A website URL containing additional information about the lab content. This is strongly recommended if you publish your pod design. Each topology has a link to “Specifications and Requirements”, which follow a consistent format for each topology.
- **Note/Comment:** Place to indicate any additional information about the pod design file, such as indicating what curriculum the pod design is being used to support.
- **Cloning:** Enable the cloning checkbox to allow derivative works to be created from your pod design.

1.10 Pod Designer Tabbed Interface

Once the general settings are entered, NETLAB+ will create a pod design file in the system’s shared folder. All of the remaining tasks will be performed using the pod designer tabbed interface. The tabs are organized from left to right in the same workflow order described in the previous section.



The screenshot shows the Pod Designer Tabbed Interface. At the top, a green dashed arrow labeled "Workflow" points from left to right. Below it are tabs for General, Image, Control, Device, Remote PC, Advanced, and Build. The General tab is active, displaying the following fields:

Name	NDG Advanced Ethical Hacking		
Description	Advanced Ethical Hacking		
Author	Jane Doe		
Organization	Fictional University		
Copyright	Copyright (c) 2020, Fictional University		
Support URL	https://fictionaluniversity.edu		
Note / Comment	Created for Jane Doe's Advanced Class		
Modification Password	not required	<input type="checkbox"/> Require a Password	
Installation Password	not required	<input type="checkbox"/> Require a Password	
Cloning Permitted	Yes		
Cloning Password	not required	<input type="checkbox"/> Require a Password	

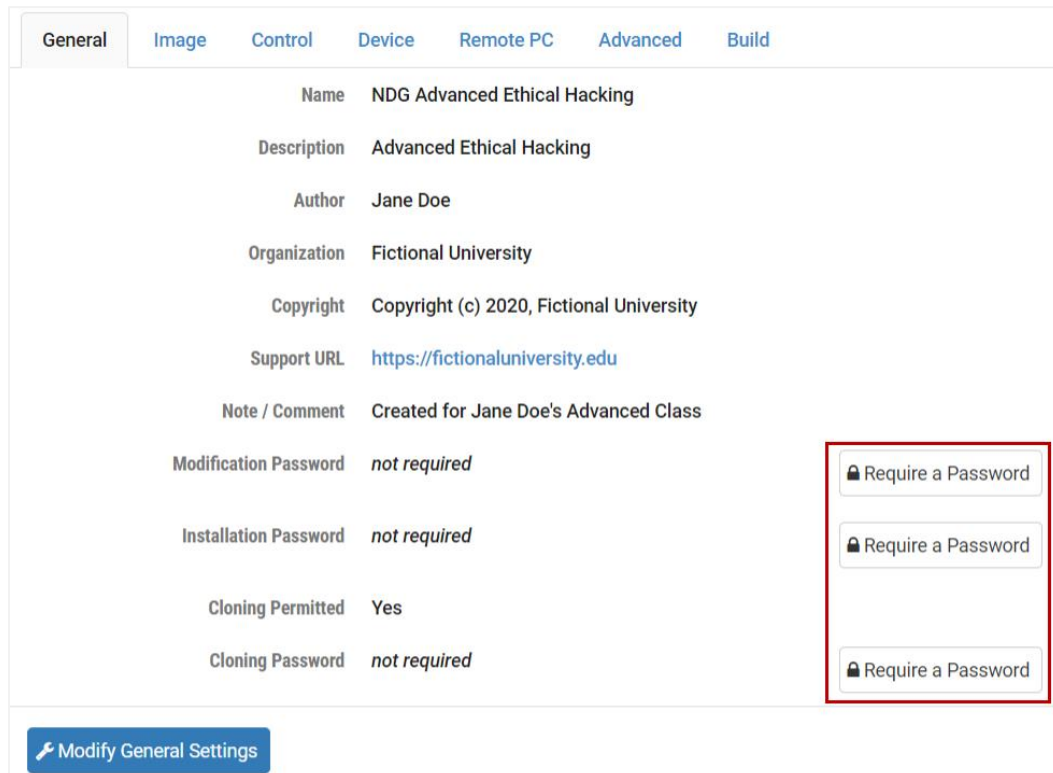
At the bottom left, there is a button labeled "Modify General Settings".

Tip: You may skip the Control and Device sections for Pure Virtual Machine Pods (i.e., there are no physical lab devices).

1.10.1 Enabling Password Protection

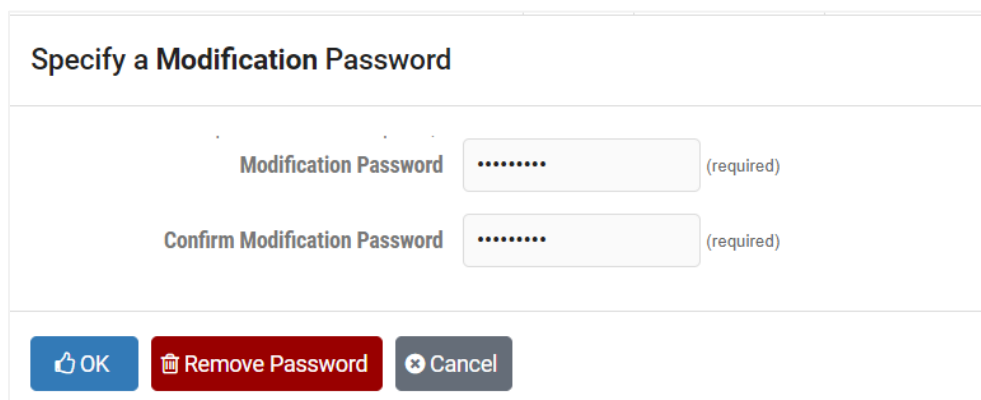
Password protection may be set for the pod design file. A Modification Password, Installation Password, and/or a Cloning Password may be set as a requirement. Select the appropriate **Require a Password** button on the General page of the tabbed interface.

To prevent simultaneous modifications, only one person can modify a pod design file at a time. If the file is being modified, a yellow notice will appear, indicating the file is in use.



	General	Image	Control	Device	Remote PC	Advanced	Build
Name	NDG Advanced Ethical Hacking						
Description	Advanced Ethical Hacking						
Author	Jane Doe						
Organization	Fictional University						
Copyright	Copyright (c) 2020, Fictional University						
Support URL	https://fictionaluniversity.edu						
Note / Comment	Created for Jane Doe's Advanced Class						
Modification Password	not required						<input type="button" value="Require a Password"/>
Installation Password	not required						<input type="button" value="Require a Password"/>
Cloning Permitted	Yes						
Cloning Password	not required						<input type="button" value="Require a Password"/>

Here, a **Modification Password** is set. A modification password protects the design from being changed. Entering the correct password will be required before any changes to the pod design can be made.



Specify a Modification Password

Modification Password (required)

Confirm Modification Password (required)

Setting an **Installation Password** will require the user to enter the password when installing the pod design.

Specify a Installation Password

Installation Password	<input type="password" value="....."/>	(required)
Confirm Installation Password	<input type="password" value="....."/>	(required)

OKRemove PasswordCancel

Setting a **Cloning Password** will require the user to enter the password in order to create derivative works based on this pod design. The user will be prompted to enter the password when selecting the Cloning option on the Build tab. The option to set a cloning password is only available if the setting to permit cloning has been selected.

Specify a Cloning Password

Cloning Password	<input type="password" value="....."/>	(required)
Confirm Cloning Password	<input type="password" value="....."/>	(required)

OKRemove PasswordCancel

1.11 Closing a Pod Design

When you are done making changes to a pod design, click on the Close Pod Design button at the bottom of the tabbed interface. This will ensure that all changes are saved and the file is unlocked. The pod design is also closed if you log out.

Close Pod Design

2 Working with Graphical Images

2.1 Default Topology Image

Each pod design may have one *default topology image* associated with the pod. A topology image is a GIF, JPEG, or PNG file that users see during a lab reservation. Each lab exercise can specify a topology image or use the default image. For best results, the width of a topology image should not exceed 600 pixels.

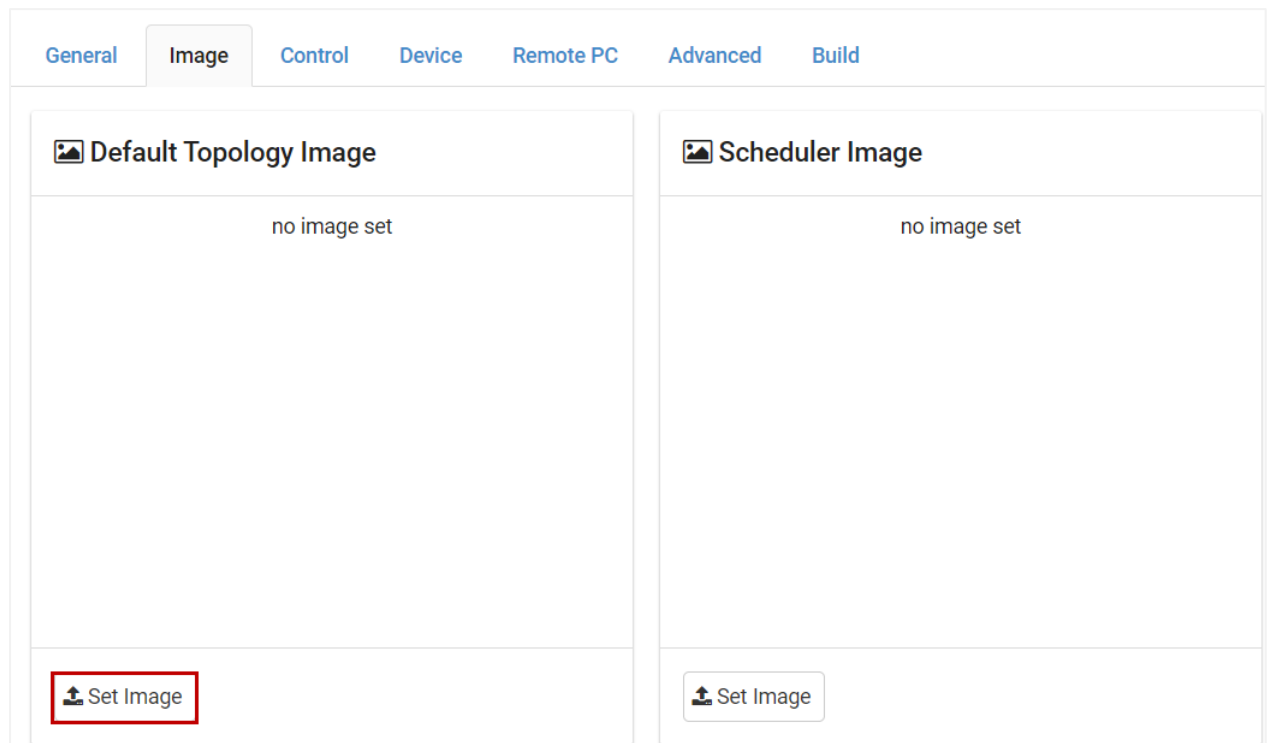
The default topology image is used when a lab exercise does not explicitly specify a topology image. To import a default topology image for this pod design, specify the path of a GIF, JPEG, or PNG file on your PC or workstation or click the browse/choose button.

This image is displayed in the lab access topology tab during a lab reservation. If you omit the default topology image, the lab access topology tab will not display an image unless the user has selected a lab exercise that provides one.

2.1.1 Adding a Default Topology Image

Follow the steps below to set the default topology image for a pod design.

1. Select the **Set Image** button on the left side of the page to upload a default topology image from your PC to the pod design file.



2. Enter the complete path and file name, which must end with one of the supported extensions (GIF, JPEG, or PNG), or click the browse/choose button to traverse your PC's directory structure and select the file to upload. Select the **OK** button to upload the specified image.

In most cases, the PNG format provides error-free image quality with good compression for faster downloads. Do not use PNG format for photo imagery and/or images with gradients as this will compress poorly and decrease page load times. JPEG provides better compression for complex photo imagery and gradients, but at the expense of image quality.



For best results, the width of a topology image should not exceed 600 pixels. Rectangular "hotspots" can be defined for each lab device (see subsections below). When the user clicks on a hotspot, NETLAB+ will launch the appropriate viewer and connect the user to the lab device. the PNG format provides error-free image quality with good compression for faster downloads.

Default Topology Image

Path to Default Topology Image

advanced_ethical_hacking_topology.png

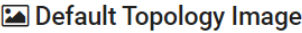
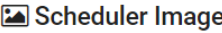


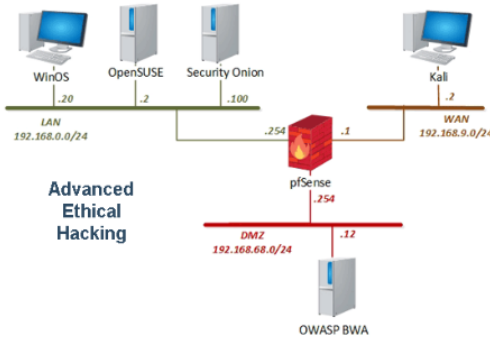
OK

Cancel

The default topology image will now be displayed on the left side of the image screen.

General
Image
Control
Device
Remote PC
Advanced
Build



no image set

File Name	Type	Width	Height
advanced_ethical_hacking_topology.png	PNG	580	400

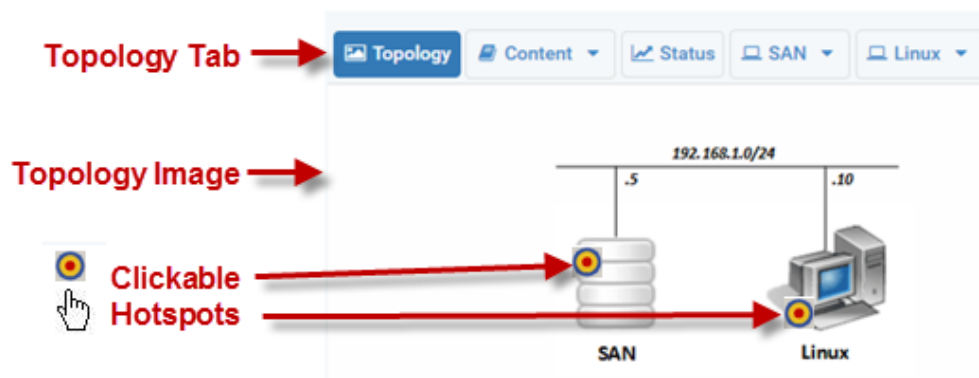
Change Image
Clear Image

Set Image











2.1.2 Hotspots

You may define clickable hotspots for devices and PCs shown on the default topology image. A hotspot is an invisible rectangular area placed on top of a router, switch, firewall, or PC in the image. When a user clicks on a hotspot, NETLAB+ will launch the appropriate viewer and connect to the device.

In order to set hotspots, at least one device or remote PC must be defined in the pod design. The process for adding devices and remote PCs is documented in subsequent sections.



To set hotspots on the topology image, select the Device section or the Remote PC section (as shown below) of the tabbed interface and click the **Set Hotspots** button.

Name	Build	Committed	Author ID	Global ID
NDG Advanced Ethical Hacking	1	No	NDGKL	0050_56BF_5E52_5EFE_0F59
<div> General Image Control Device Remote PC Advanced Build </div>				
Index	Icon	Name	Hotspot	Actions
1		WinOS	Not set	
2		OpenSUSE	Not set	
3		Security Onion	Not set	
4		Kali	Not set	
5		OWASP BWA	Not set	
<div> + Add PC ⦿ Set Hotspots </div>				

The page will display available hotspots for the lab devices and remote PCs in the topology at the top of the page. Highlighted hotspots have not yet been placed on the image. You may elect to set some or all of the hotspots on the image.

Lab routers, switches, and firewall hotspots are red. PC hotspots are green.



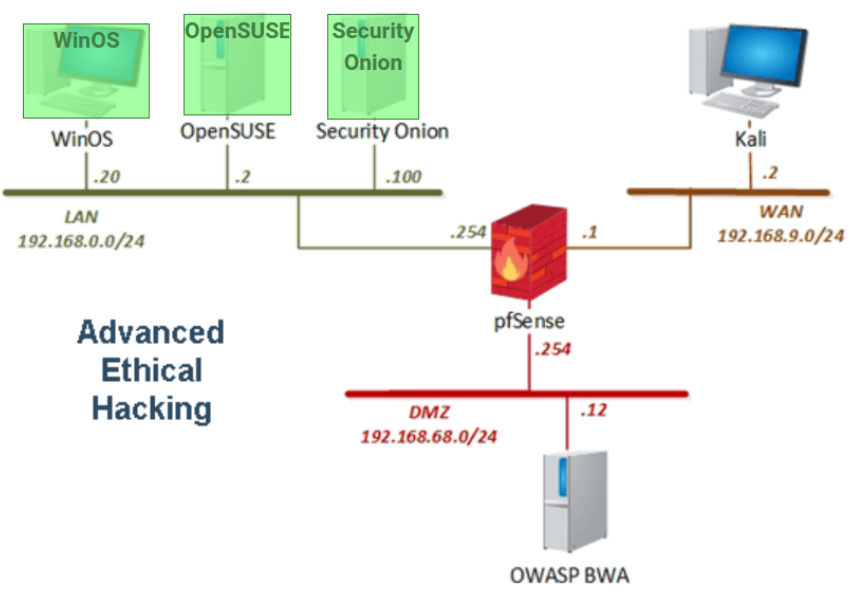
To set a hotspot for a device or remote PC, drag its square from the hotspot tray to the desired location on the image. Drag the lower-right corner or edges to resize the hotspot. To clear a hotspot, drag its square off of the image or back to the hotspot tray. You may elect to set some or all of the hotspots on an image.

In this example, hotspots have been set for the first three remote PCs. Hotspots have not yet been set for the pfSense lab device, the Kali remote PC, and the OWASP BWA remote PC.

Name	Build	Committed	Author ID	Global ID
NDG Advanced Ethical Hacking	1	No	NDGKL	0050_56BF_5E52_5EFE_0F59

Set Hotspots

pfSense WinOS OpenSUSE Security Onion Kali OWASP BWA



Advanced Ethical Hacking

LAN 192.168.0.0/24

WAN 192.168.9.0/24

DMZ 192.168.68.0/24

WinOS .20

OpenSUSE .2

Security Onion .100

Kali .2

OWASP BWA .12

pfSense .254

OK Cancel

2.1.3 Clearing the Default Topology Image

To remove the default topology image from the pod design, select the **Clear Image** button. If you clear the default topology image, the lab access topology tab will not display an image unless the user has selected a lab exercise that provides one.

Name	Build	Committed	Author ID	Global ID
NDG Advanced Ethical Hacking	1	No	NDGKL	0050_56BF_5E52_5EFE_0F59

General

Image


Control

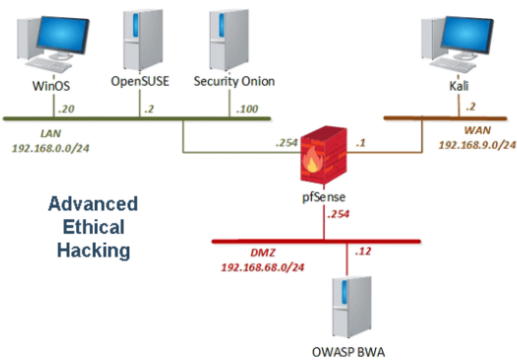
Device

Remote PC

Advanced

Build


Default Topology Image




Advanced Ethical Hacking

File Name	Type	Width	Height
advanced_ethical_hacking_topology.png	PNG	580	400

Change Image

Clear Image


Scheduler Image

no image set

Set Image

Select **OK** to proceed with clearing the image.

Are you sure you want to clear this image?

OK

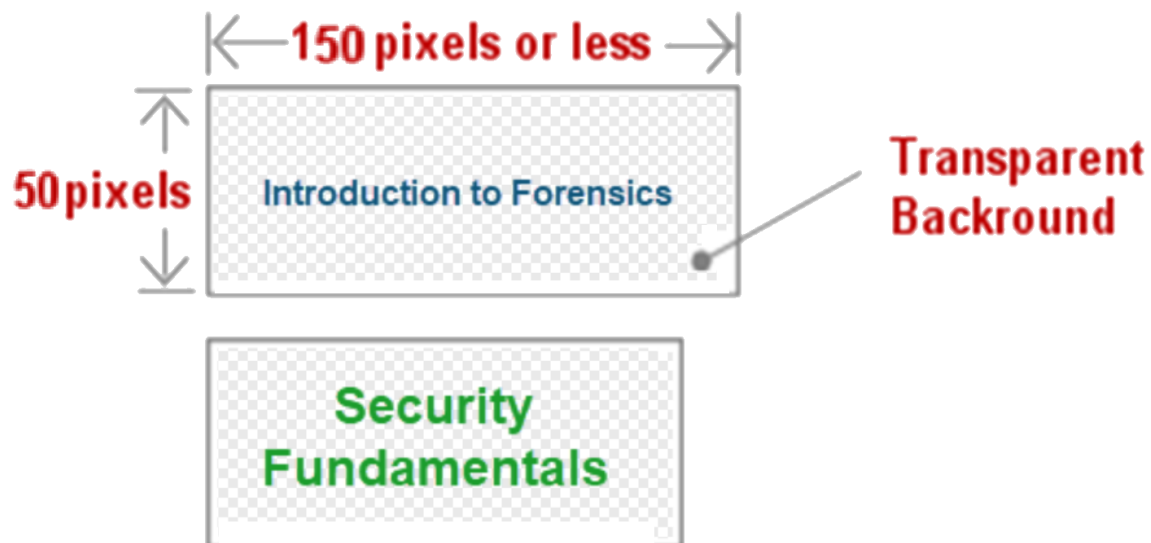
Cancel

2.2 Scheduler Image

A scheduler image is a small rectangular image that uniquely identifies the pod design and appears in various scheduling functions. If you do not define a scheduler image, NETLAB+ will display the Pod Name and Pod Description values from the general settings. A scheduler image must conform to the following specifications:

File Format	GIF, PNG, or JPEG. A transparent GIF is recommended.
Width	150 pixels or less
Height	50 pixels exactly
Background Color	Transparent


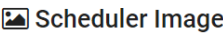
The following examples are valid scheduler images:

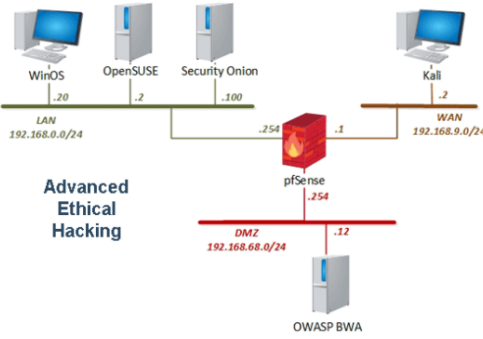


2.2.1 Adding a Scheduler Image

Select the **Set Image** button on the right side of the page to upload a scheduler image from your PC to the pod design file.

General
Image
Control
Device
Remote PC
Advanced
Build



no image set

File Name	Type	Width	Height
advanced_ethical_hacking_topology.png	PNG	580	400


Change Image
Clear Image

Set Image

Enter the complete path and file name, which must end with one of the supported extensions (GIF, JPEG, or PNG). Select the **OK** button to upload the specified image.

A scheduler image is an optional GIF, JPEG, or PNG thumbnail image that visually identifies this pod design. Users see this image in the scheduler. The scheduler image must be **exactly 50 pixels in height** and **no more than 150 pixels in width**.

Scheduler Image

Path to Scheduler Image
adv_eth_hack_sch.png


OK
Cancel

The default scheduler image will now be displayed on the right side of the image screen.

This example shows that a Default Topology Image has also been set.

General

Image


Control

Device

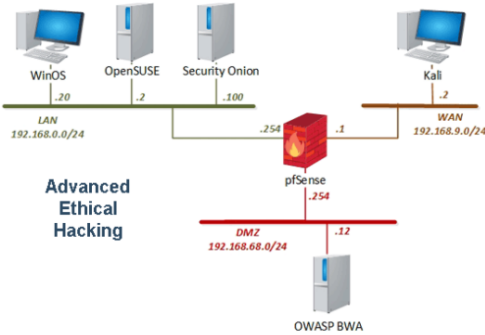
Remote PC

Advanced

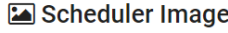
Build




Default Topology Image



Advanced Ethical Hacking



Scheduler Image



Advanced Ethical Hacking

File Name	Type	Width	Height
advanced_ethical_hacking_topology.png	PNG	580	400

Change Image

Clear Image

File Name	Type	Width	Height
adv_eth_hack_sch.png	PNG	120	50

Change Image

Clear Image

2.2.2 Clearing the Scheduler Image

To remove the scheduler image from the pod design, select the **Clear Image** button. If you clear the scheduler image, NETLAB+ will display the Pod Name and Pod Description values from the general settings.

Select **OK** to proceed with clearing the image.

Are you sure you want to clear this image?

OK

Cancel

3 Control Settings

The control tab is used to specify the control device resources required by real equipment pods or hybrid designs. This only quantifies the resources that are required to support the pod design. Actual resource allocation takes place when the administrator creates an instance of the pod.

Control settings do not apply to Pure Virtual Machine Pods. You may skip this section if your pod design does not include real equipment.

In the subsections below, we'll first describe the process of modifying the control settings for a pod design and then also take a more in-depth look at the technical considerations for designing custom real equipment pods in NETLAB+ VE.

[Admin](#) > [Pod Designer](#) > [Advanced Cyber Concepts](#)

To prevent simultaneous modifications, no other users can modify this file until you close the pod design or log out.

Name	Build	Committed	Author ID	Global ID
Advanced Cyber Concepts	1	No	NDGKL	0050_56BF_5E52_5F07_2E97

[General](#) [Image](#) [Control](#) [Device](#) [Remote PC](#) [Advanced](#) [Build](#)

Access Server Ports

Switched Outlets

Consecutive Control Switch Ports

VLAN Pool

Default VLAN Map


None


None

None

None

n/a

 Modify Control Settings

 Close Pod Design

3.1 Modifying Control Settings

Follow the steps in this section to modify the control settings for your pod design.

1. On the Control tab, select **Modify Control Settings** (see picture on previous page).
2. Control Settings page will be displayed. Select the appropriate settings (refer to the field descriptions below) and then click **OK**.

Control Settings

Access Server Ports

4

Switched Outlets

4

Consecutive Control Switch Ports

5

VLAN Pool Size

3

Default VLAN Map

+0	+1	+2	+3
OFF	OFF	VLAN A	VLAN B
+4			
VLAN C			

OK

Cancel

Help

Field Descriptions – Control Settings

- **Access Server Ports:** The number of access server ports required to support this pod design. Typically, one port for each user-accessible lab device is required. Remote PCs do not use access ports. This value may be 0 for pods that only contain remote PCs.
- **Switched Outlets:** The number of switched power outlets required to support this pod design. Typically, one switched outlet for each managed lab device is required. Remote PCs (virtual machines) do not use switched outlets. This value may be 0 for pods that only contain remote PCs.
- **Control Switch Ports:** The number of control switch pod ports required to support this pod design. Typically, each managed lab device will use one control switch port. However, it may be desirable to allocate more than one port per lab device to provide flexible connectivity using *VLAN maps*. You may also allocate pod ports for unmanaged devices. The layout and usage of each port are

arbitrary as long as you are consistent. This value may be 0 for pods that only contain remote PCs, and all networking is achieved externally and/or using virtual networking. Prior to NETLAB+ Virtual Edition, control switch ports must be consecutive. This is recommended but not required in NETLAB+ VE.

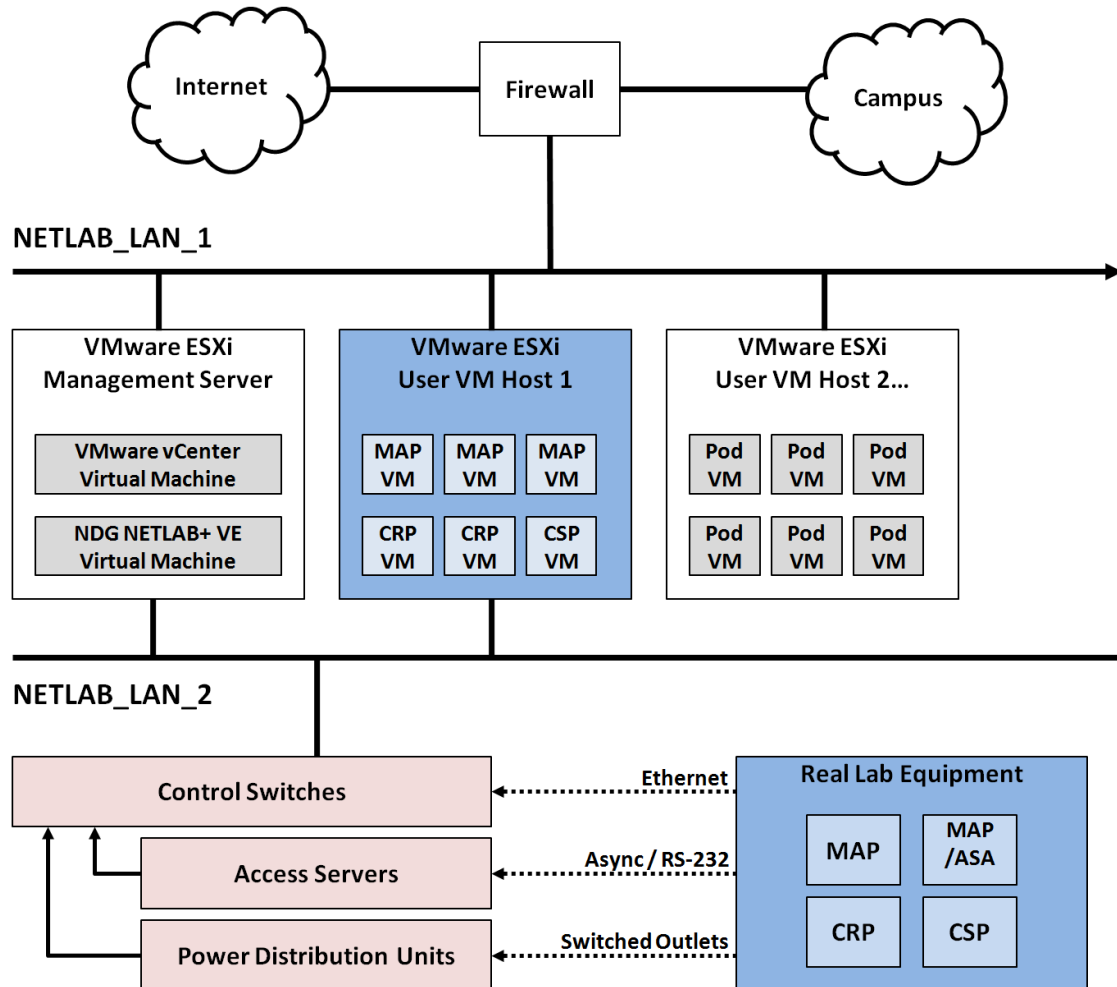
- **VLAN Pool Size:** This value determines the number of unique VLANs that will be created and maintained on control switches for each instance of this pod design. For example, if the VLAN pool value is 5 and 4 pods of this type are added by the administrator, then 20 unique VLANs will be created on the control switches. How these VLANs are used is determined by VLAN maps.

Each VLAN runs a spanning tree instance on the control switch unless the administrator configures MSTP (which is recommended after 48 VLANs). Therefore, a smaller VLAN pool is desired.

- **Default VLAN Map:** This VLAN map is applied to the pod at the beginning of a lab reservation. Each lab exercise may also specify an optional VLAN map that overrides the default VLAN map. Each control switch port used by the pod is given a relative port number (+0, +1, etc.) since the actual control switch ports cannot be determined at design time. Each port can have one of the following settings:
 - **VLAN (*letter*):** At the beginning of the lab exercises, the control switch port will be turned on and set to the VLAN indicated by the letter. The actual VLAN number used cannot be determined at design time; therefore, letters are used.
 - **OFF:** This value causes the control switch port to be turned off at the beginning of the lab exercise. It may be turned on if NETLAB+ needs to recover an erased software image.
 - **STATIC:** This value indicates that the control switch port is statically configured by the administrator. NETLAB+ will not change the administrative state (on/off), will not change the VLAN, or any other setting on the port. This setting can be used to allocate a pod port for trunking to an unmanaged static router or VMware server. However, it is often more desirable to use a reserved port for this purpose.

3.2 Real Equipment Installation on a NETLAB+ VE System

In this section, we'll discuss the technical considerations for designing custom real equipment pods in NETLAB+ VE. 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_1 is the primary network adapter that connects to your campus LAN.

NETLAB_LAN_2 provides a non-routable network for:

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



Network Adapter 2 is used in setups that include physical lab devices. Please refer to the [*NETLAB+ VE Real Equipment Pod Installation Guide for Cisco Networking Academy*](#).

3.3 Access Servers



Access servers provide console connections to managed lab devices (lab routers, lab switches, and lab firewalls) so that users can access these devices from NETLAB+. Each lab device in your pod design that requires console access by the pod user will consume one access server port. The access server provides an air gap between lab devices and the production network. The details of the access server are handled by NETLAB+ and are completely transparent to the user. When a user clicks on a lab device on the topology image, NETLAB+ makes all the necessary connections through the NETLAB+ server and the access server automatically. The NETLAB+ console sharing feature allows simultaneous access by multiple users to a lab device's console port in multi-user reservations (team and ILT).

3.4 Power Distribution Units



Power Distribution Units (PDUs) provide managed electrical power, allowing NETLAB+ and users to turn lab equipment ON and OFF. Each managed lab device in your pod design will consume one switched outlet on a PDU. Switched outlets also allow NETLAB+ to cycle power when required by automation, such as automatic password recovery of a Cisco lab device.

3.5 Control Switches



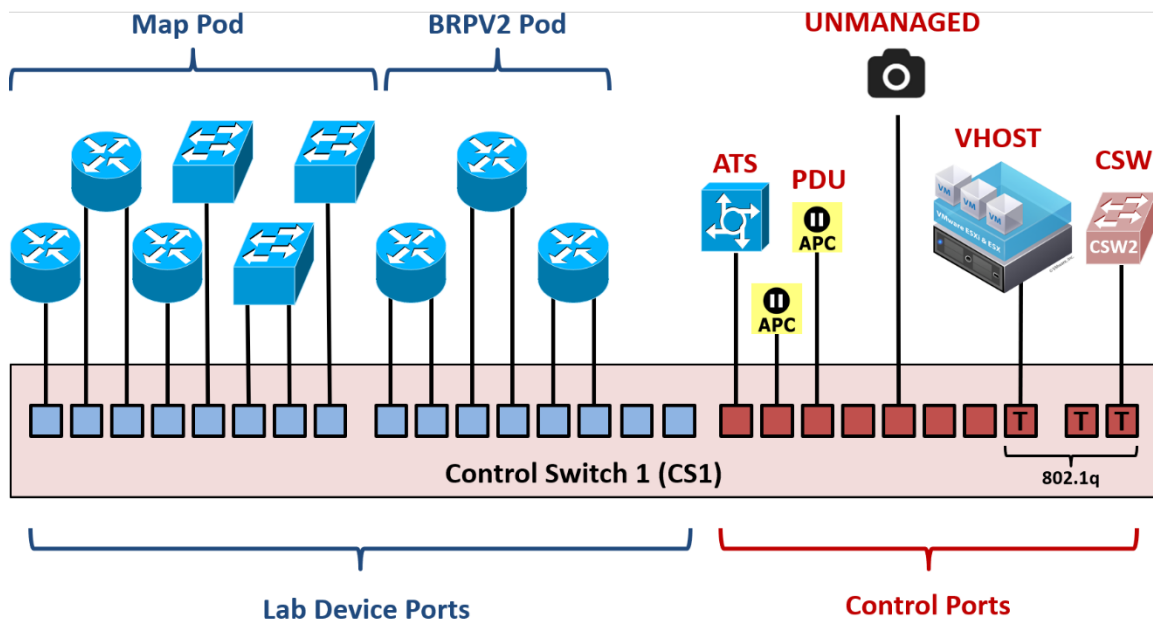
Control switches provide four types of network connectivity:

1. Internal network connectivity between the NETLAB+ server, access servers, power distribution units, and other control switches.
2. Flexible connectivity between lab devices using VLANs.
3. A network path between real equipment and virtual machines running on VMware host servers.

A temporary network path for NETLAB+ to download IOS images to older Cisco lab devices in the event flash has been erased (or the correct image is not installed). This is not supported on newer Cisco devices, as they can recover images from read-only flash storage.

Control switch ports are categorized into lab device ports and control ports.

- *Lab device ports* provide connectivity to user-accessible lab devices that are typically configured with an RS-232 async console connection.
- *Control ports* connect to supporting infrastructure that is not accessible to the user.



3.5.1 Control Ports

Control ports on a control switch provide the framework to interconnect NETLAB+, control devices, and other shared resources. These ports are designated by the administrator as one of the following roles:

- Connection to an async terminal server (ATS)
- Connection to another control switch (CSW)
- Connection to a power distribution unit (PDU)
- Connection to a virtual machine host (VHOST)
 - The NETLAB+ virtual appliance runs on a VHOST and communicates with the control switch via this type of control port.
- Connection to an unmanaged device (manually configured)

Once the administrator designates a control port role, the port is configured by NETLAB with the proper settings for that role. For example, virtual host (VHOST) and control switch (CSW) port roles are automatically configured with 802.1Q and VLAN tags. Async terminal server (ATS) and power distribution unit (PDU) port roles are configured as non-trunking access ports in VLAN 1.

3.5.2 Lab Device Ports

Lab device ports connect real lab equipment to the NETLAB+ control switch. A single control switch can have pod ports for several pods. You may allocate more than one pod port for a lab device in order to simulate additional LAN segments. Both managed and unmanaged lab devices can be connected to pod ports.

Managed lab devices are device types that NETLAB+ can automate by temporarily taking over the console connection and issuing configuration commands. For example, NETLAB+ can perform a password recovery on certain types of Cisco devices. For a list of supported managed lab devices, please see the NDG website.

Unmanaged lab devices are physical devices that can be configured by the user through an asynchronous terminal server (RS-232) port but are not automated by NETLAB+. For example, a non-Cisco router can be configured using an RS-232 console port.

The pod design author determines how many control ports are required for each pod design and how those ports will connect to lab devices.

The NETLAB+ administrator may locate the lab device ports anywhere on a control switch.



In NETLAB+ version 22 and later, lab device ports can span multiple control switches and do not have to be consecutive, as long as the ports are consecutive and do not overlap reserved ports. Earlier versions of NETLAB+ required consecutive ports confined to a single control switch.

Since the actual ports that will be used on the control switch are not known at design time, all control switch ports in a pod design are specified using *relative port numbers* (+0, +1, ..., +5, etc.).

During normal operation, pod ports can be set to OFF or placed in unique or common VLANs to simulate one or more Ethernet segments required by the topology of the pod. This feature is called *VLAN mapping* and can be used to maximize the flexibility of a statically wired pod.

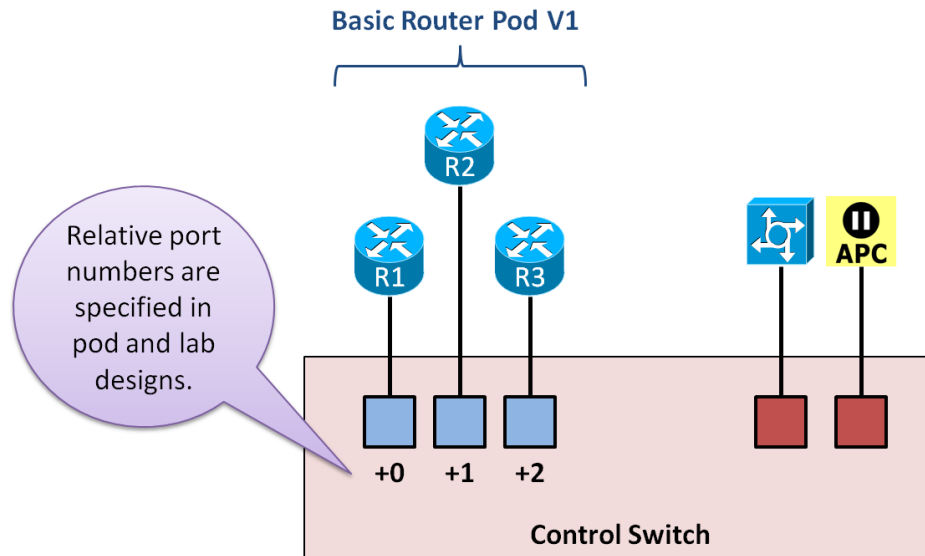
On older Cisco devices, NETLAB+ may temporarily place the device in VLAN 1 so that it can access the NETLAB+ internal TFTP server to obtain IOS images.



Pod ports on the control switch do not support ISL or 802.1q trunks. When lab devices require trunking, a direct connection between devices is required.

Pod Ports Example 1. NDG Basic Router Pod V1

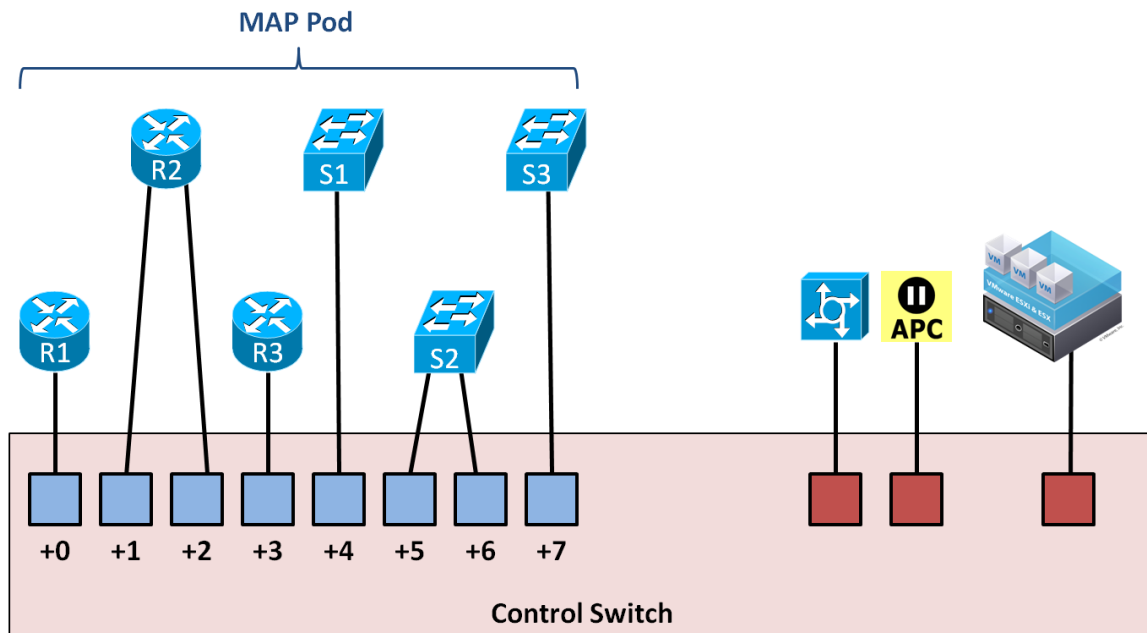
The NDG Basic Router Pod V1 is a simple pod design with one control switch connection per router. The pod design associates R1 with relative port +0, R2 with relative port +1, and R3 with relative port +2 (the blue ports). The actual port numbers cannot be determined at design time; these are determined when the NETLAB+ administrator creates an instance of the pod design and designates a control switch port for each of the three lab device ports.



The pod also uses access server ports and switched outlets. Control ports (red) are used for the corresponding control devices, and no lab device ports (blue) are consumed in the pod design for these connections.

Example 2. NDG Multipurpose Academy Pod

The NDG MAP pod provides 8 control switch ports for its lab devices. Router R2 and S2 were given two control switch connections. This decision was made after carefully looking through all the labs required to run on the pod and determining how LAN segments would best be simulated.



In addition to access server ports and switched outlets, the MAP pod also provides 3 virtual machines. The VMware host server for the 3 VMs connects to a VHOST port on the control switch; no lab device ports are consumed for the VMware host connection.

3.5.3 Control Switch VLAN Numbers

The following table shows the control switch VLAN numbering scheme used by NETLAB+.

VLAN(s)	Purpose in NETLAB+
1	Management VLAN. Used for internal communication between the NETLAB+ server, control devices, and VMware servers.
2-99	Reserved for NETLAB+. NETLAB+ may add or delete VLANs in this range.
100-899	Used for pod dynamic VLAN maps. The maximum number of dynamic VLANs is 26 per pod and 800 per system.
900-999	Reserved for customer special needs. NETLAB+ will NOT add or delete VLANs in this range.
1000+	Reserved for Cisco. Do not use.

Control switches do not run the Cisco VLAN Trunking Protocol (VTP). NETLAB+ sets each control switch to *VTP transparent* mode during the initial switch configuration. It then uses SNMP to maintain a consistent VLAN database on each control switch. This method avoids VTP conflicts and other problems that can arise when lab switches are connected to control switches.



NETLAB+ version 22 transparently assigns and manages the pool of 800 VLANs available for pod designs. Previous versions of NETLAB+ required additional understanding and configuration of VLAN allocation.

3.5.4 VLAN Mapping

VLAN mapping is a NETLAB+ feature that can significantly increase the number of labs that can be performed on a single pod design, thereby decreasing the overall cost of lab equipment.

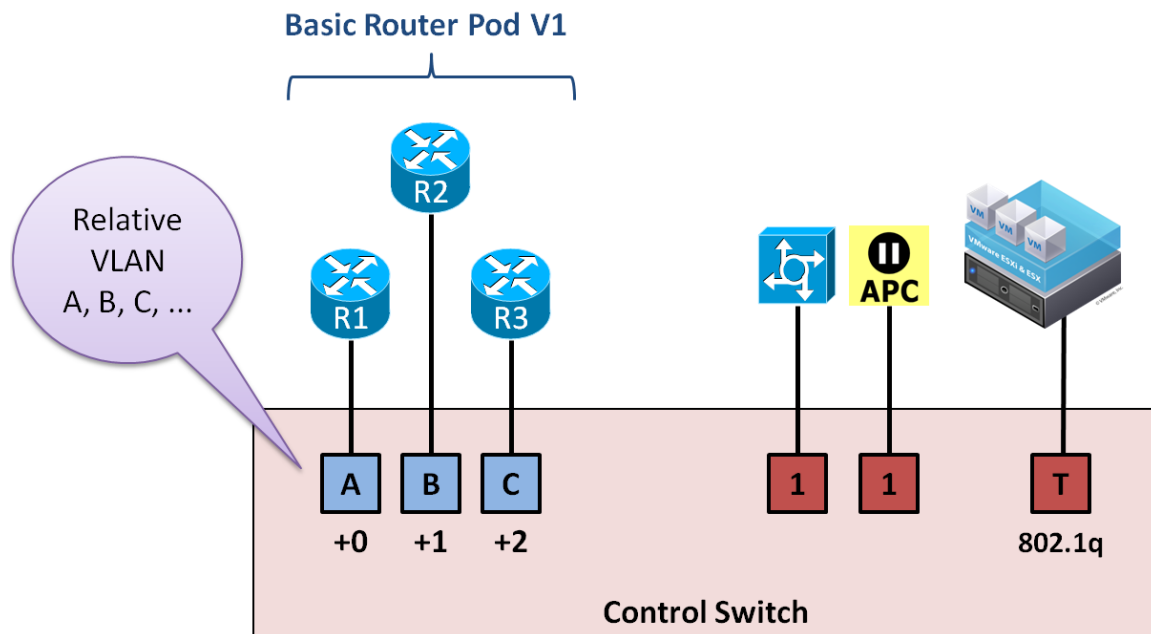
During normal operation, pod ports can be set to OFF or placed in a VLAN to simulate one or more Ethernet segments required by the topology of the pod.

A VLAN map tells NETLAB+ which VLAN to assign to each control switch port at the beginning of a lab reservation.

- A VLAN map can be provided for each lab exercise (these VLAN maps are specified in Lab Designer).

- If a lab exercise does not provide a VLAN map, the *default VLAN map* specified in the pod design is used.

The actual VLAN numbers used by a pod are based on a pod's ID, which is assigned by the NETLAB+ administrator. Since pod IDs cannot be determined at design time, the pod designer uses *relative VLANs* (A, B, C..., etc). The maximum number of VLANs per pod is 26. The maximum number of managed VLANs per NETLAB+ system is 800.



Recall that control switch port numbering in a pod design is also relative (+0, +1, +2, etc.). These ports are assigned to designated lab device ports on control switches by the NETLAB+ administrator. These ports need not be consecutive or confined to the same control switch in NETLAB+ version 22.

The number of VLANs allocated for the pod is the *VLAN pool size*. This value is set by the pod design author based on how many unique LAN segments are required.

Ports in a VLAN map do not need to be assigned to a VLAN. Alternatively, the port may be turned OFF or STATIC. A setting of STATIC instructs NETLAB+ not to manipulate the port. A static port might be configured as a trunk to a special unmanaged router or other special device.

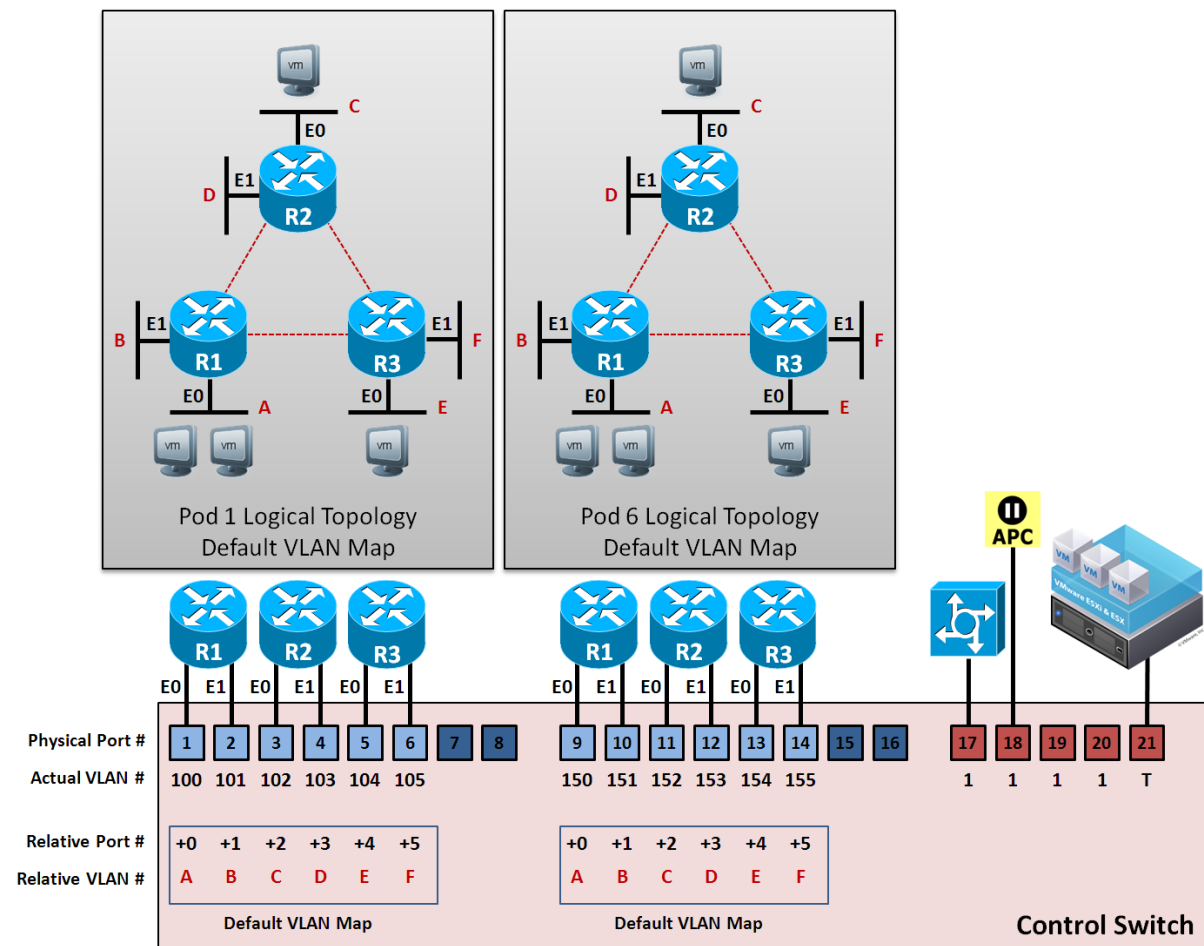
VLAN maps may be easier to understand by example, so we have provided a few below.

VLAN Map Example 1

This example below shows the default VLAN map for a NETLAB+ Basic Router Pod (version 2). The VLAN pool size for this pod design is 6 (VLAN A to VLAN F). This provides enough VLANs so that each router port can be attached to a stub network.

Because each control switch port is placed in a unique VLAN, each LAN segment behaves as a separate routed segment, as shown in the Topology diagrams.

The PCs in these pods are virtual machines on a VMware host server. Discussed in the next section.

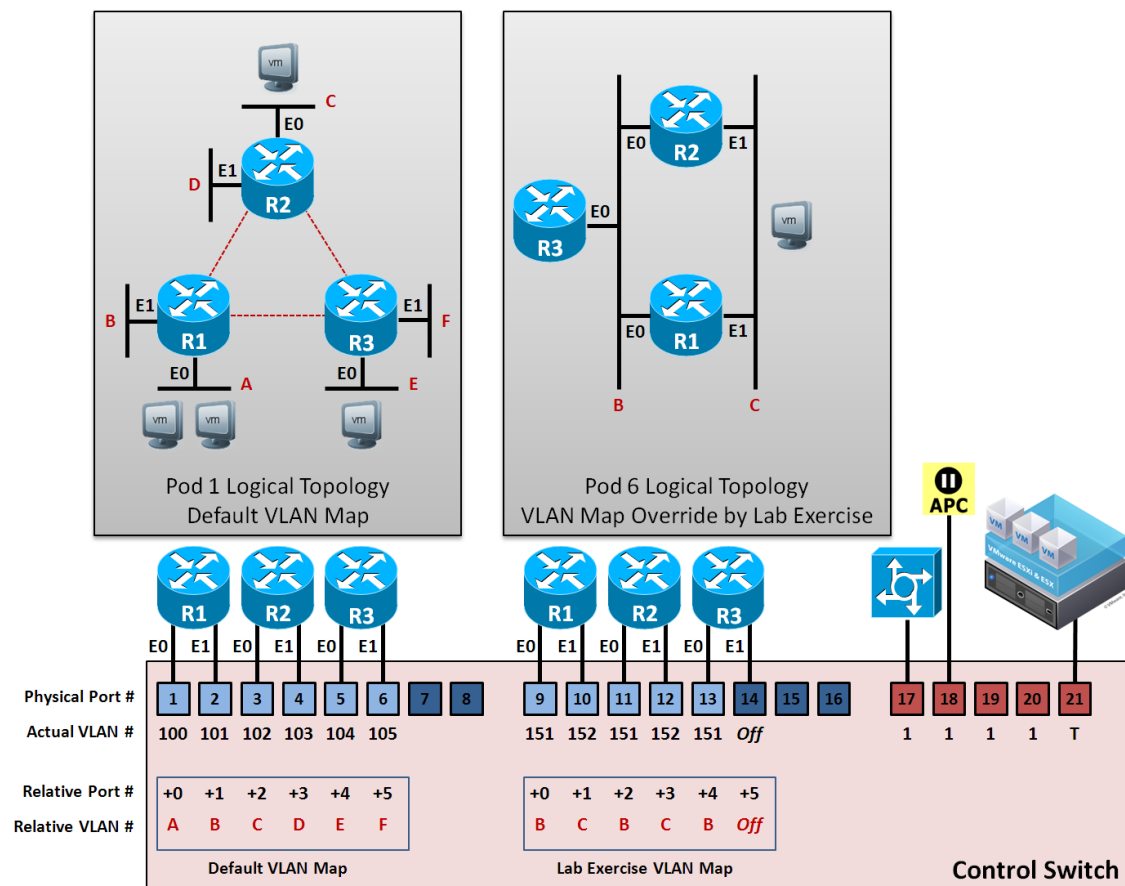


VLAN Map Example 2

The default VLAN map is normally applied to the pod at the beginning of a lab reservation. However, you may also create VLAN maps for each lab exercise (using Lab Designer). Each exercise may specify its own VLAN map or simply use the default VLAN map specified in the pod design.

By using VLAN maps in your lab exercises, you can make logical alterations to the lab topology without changing the cabling of the pod (which is always fixed). If the pod and lab designs utilize VLAN maps, it may be possible to perform many more labs than could be done with static mapping and/or direct connections between lab devices. By decreasing the number of physical lab topologies required, the potential cost of lab equipment to teach a curriculum is greatly reduced.

Consider the two pods below. Both pods are Basic Router Pod Version 2 pods and are physically wired as such. However, pod 6 has loaded an “HSRP” lab exercise that uses a dynamic VLAN map. The pod 6 topology will behave much differently than its pod 1 counterpart for the duration of the lab exercise. The lab exercise also presents the topology picture shown for pod 6, so the user actually sees the modified topology.



4 Lab Device Settings

This section applies to real equipment pods and hybrid pods.

Lab device settings do not apply to Pure Virtual Machine Pods. You may skip this section if your pod design does not include real equipment.

Lab devices can be classified into 3 categories.

- **Managed Lab Devices:** Real equipment that users can connect to and configure, automated by NETLAB+.
- **Generic Console Device:** Real equipment that users can connect to and configure but is not automated by NETLAB+ (except for user control over power).
- **Supporting Lab Devices:** Supporting real equipment that is not visible or configurable by the user.

4.1 Managed Lab Devices and Generic Console Devices

Managed lab devices are real devices that lab users will actually configure during the lab. NETLAB+ automation drivers are provided for a variety of Cisco routers, switches, and firewalls.

Each managed lab device uses a NETLAB+ device driver. Managed lab devices must be specifically supported by NDG. A list of supported lab devices can be found in the support section of the NDG website.

Generic Console Devices are real equipment that users can connect to and configure but are not automated by NETLAB+ (except for user control over power). This allows devices that are not supported (or automated) by NDG to be used without an automation driver, provided they have a serial console port and can be accessed via an access server connection.

The decision to use a managed device or generic console device is made on a per-pod basis. The pod design settings are the same for either.

4.1.1 NETLAB+ Automation Features for Managed Lab Devices

The following table shows the automation features provided for supported managed lab devices. The table does not apply if the administrator chooses a Generic Console Device setting for the given lab device.

NETLAB+ Feature	Cisco Routers	Cisco Switches	Cisco Firewalls
Connect directly to the console port	Yes	Yes	Yes
Built-in terminal application to access device console ports	Yes	Yes	Yes
Share console with several users at the same time	Yes	Yes	Yes
Turn the device ON or OFF	Yes	Yes	Yes
Automatically load or save configuration files via the console port (does not rely on networking and TFTP)	Yes	Yes	Yes
Automatically perform password recovery	Yes	Yes	Yes
Reset device to a clean configuration upon request or at the end of the lab reservation	Yes	Yes	Yes
Automatically recover an image that has been erased from flash memory	Partial	No	No

See the [NETLAB+ Supported Lab Devices](#) page for a list of supported managed equipment.

4.1.2 Lab Routers

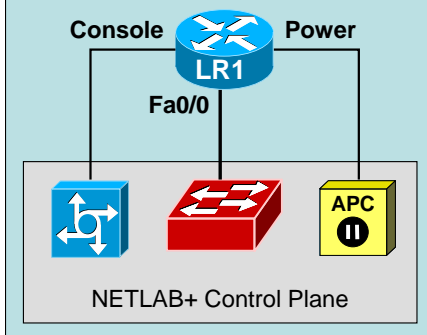


The following connections are typical for each lab router.

- One connection to an access server port.
- One connection to a switched outlet (i.e., APC device)
- One or more connections to a control switch.

Refer to the three configuration scenarios below. LR1 is a lab router. LR1 has connections to the NETLAB+ control plane: access server (left), control switch (middle), and switch outlet device (right).

1: Minimum Configuration

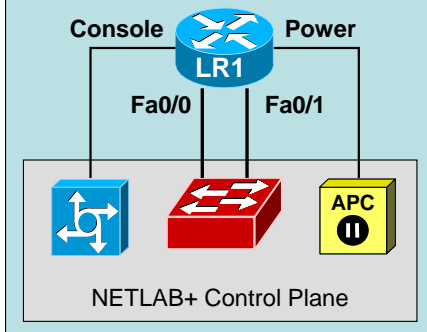


Configuration 1 depicts the minimum connection requirement for each lab router.

The lowest numbered Ethernet (typically Fa0/0) port may be used to recover the router's image should it be erased from flash on previously supported Cisco routers. Currently supported routers recover images from a read-only USB storage device, if capable.

During the lab, this port may be turned off or mapped dynamically to a VLAN on the control switch to simulate a LAN segment. Dynamic VLAN mapping is a powerful feature that may be used to alter the lab topology. This can be done for each lab exercise.

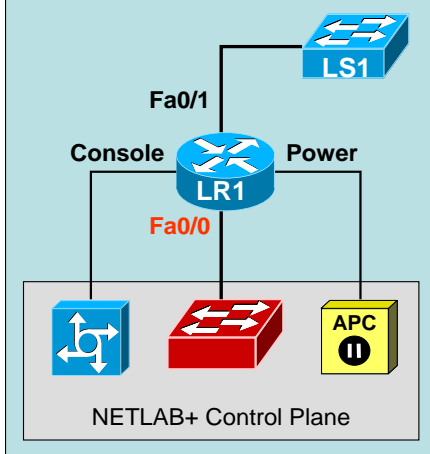
2: Multiple C/S Connections



Configuration 2 depicts both built-in Ethernet ports connected to the control switch.

Each Ethernet port connected to the control switch may participate in dynamic VLAN mapping. This technique can be used to create very flexible lab topologies from a single statically cabled pod.

3: Lab Switch Connection



Configuration 3 shows a direct connection between a lab router (RT1) and a lab switch (LS1).

Direct connections between lab devices are required to teach core switching concepts such as trunking, VTP, CDP, inter-VLAN routing, and port channeling. Direct connections preserve the nature of these protocols. A path through the control switch will not work in these scenarios.

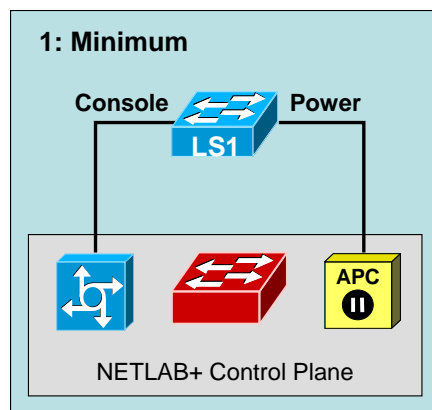
4.1.3 Lab Switches



The following connections are required for each lab switch.

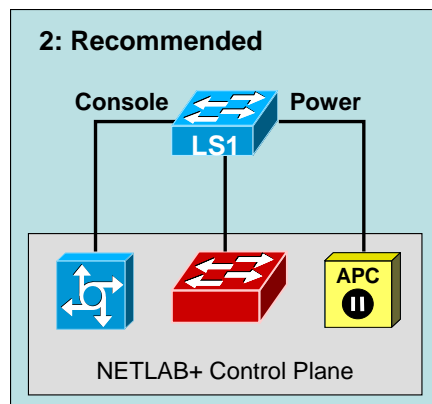
- One console connection to an access server port.
- One power connection to a switched outlet (i.e., APC device).
- One connection to a control switch for every VMware virtual machine will appear as a directly attached PC.

Refer to the four configuration scenarios below. LS1 is a lab switch. LS1 has connections to the NETLAB+ control plane: access server (left), control switch (middle, recommended), and switch outlet device (right).



Configuration 1 depicts the minimum connection requirement for each lab switch.

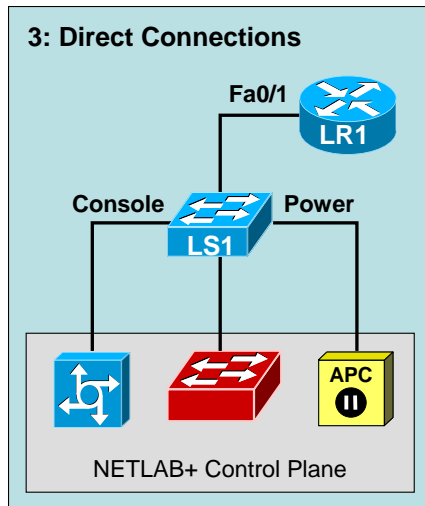
Please note this configuration will not support flash recovery, should this feature be implemented for lab switches in the future. Therefore, we recommend one of the other configuration options below.



Configuration 2 depicts the recommended configuration. If LS1 does not connect to other devices (such as VMware PCs) through the control switch, then the control switch connection can be turned off during the lab exercise. This connection also enhances NDG's ability to perform diagnostics and troubleshooting on the lab switch.

Whenever a lab switch is connected to a control switch, additional configuration commands are required on the control switch to prevent unwanted spanning tree, trunking, and VTP side effects. This is explained in the following section.

3: Direct Connections



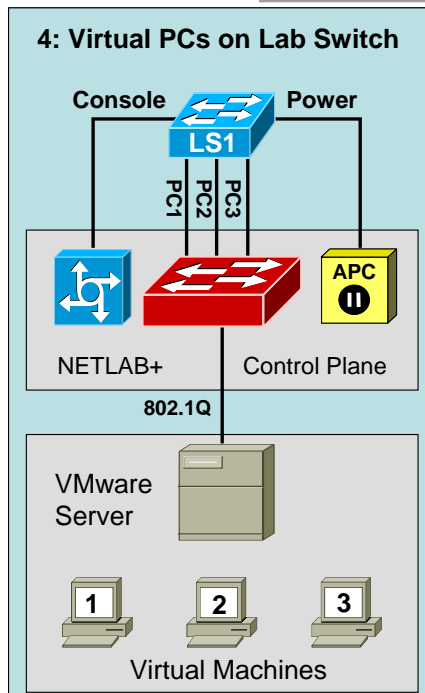
Configuration 3 shows a direct connection between a lab switch (LS1) and a lab router (RT1).

Direct connections between lab devices are required to teach core switching concepts such as trunking, VTP, CDP, inter-VLAN routing, and port channeling. Direct connections preserve the nature of these protocols. A path through the control switch will not work in these scenarios.

The connection between LS1 and the control switch is turned OFF during the lab. As in configuration 2, this is a management connection.

Whenever a lab switch is connected to a control switch, additional configuration commands are required on the control switch to prevent unwanted spanning tree, trunking, and VTP side effects. This is explained in the following section.

4: Virtual PCs on Lab Switch



Configuration 4 shows how virtual PCs can be tied to a lab switch via the control switch. To the lab user, each PC appears to be directly connected to ports on the lab switch.

Whenever a lab switch is connected to a control switch, additional configuration commands are required on the control switch to prevent unwanted spanning tree, trunking, and VTP side effects. This is explained in the following section.

4.1.3.1 Special Configuration for Pods Containing Lab Switches



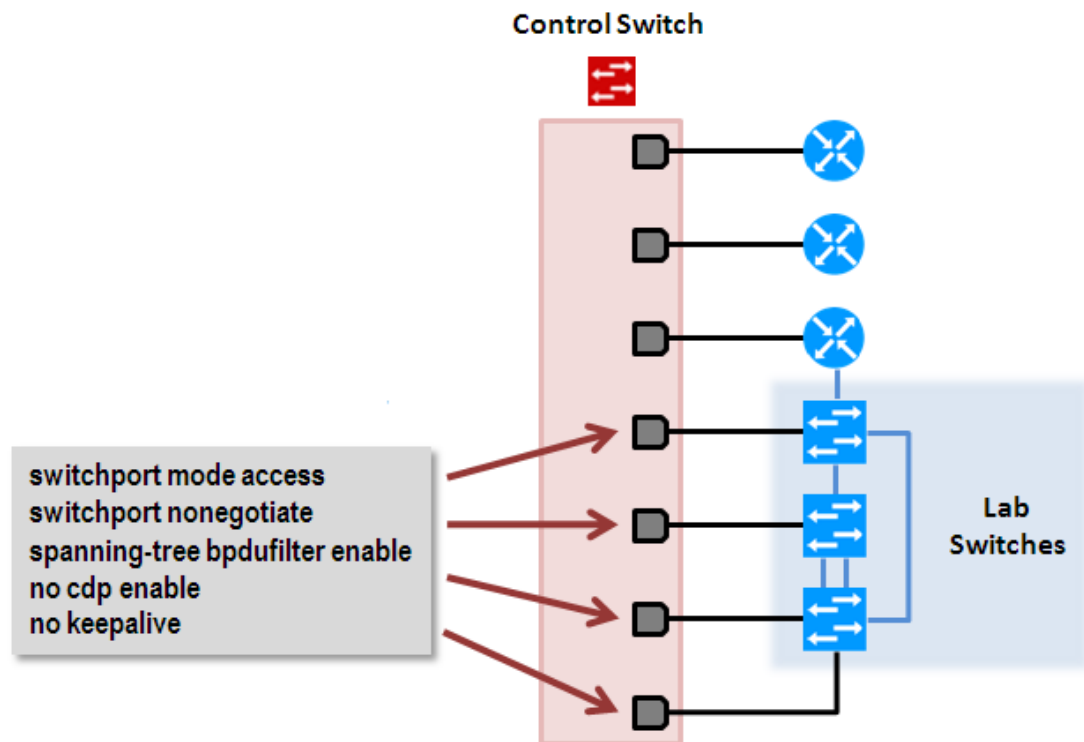
Whenever a pod contains lab switches and ports on the lab switch connect to a control switch, NETLAB+ will apply additional commands to the control switch ports to prevent adverse interactions between the lab switch and control switches.



When setting up a pod containing lab switches, be sure to add the pod to NETLAB+ and configure control switch lab ports physically attaching the equipment to the pod.

BEFORE CONNECTING LAB EQUIPMENT: the system administrator should perform the following steps in this order to prevent packet loops between control switches and lab switches.

1. Determine which access server (ATS) lines, control switch (CSW) lab ports, and power distribution outlets (PDU) will be assigned to the pod.
2. Ensure that all ATS, CSW, and PDU units are configured in NETLAB+.
3. Designate the control switch lab ports and configure them into the NETLAB+ free lab port pool. This step applies the necessary commands to the control switch lab ports to prevent packet loops. In NETLAB+ version 22, these commands are configured automatically.



4. Add the pod in NETLAB+.
5. Assign access server lines (ATS) to the pod.

6. Assign power distribution outlets (PDU) to the pod.
7. Assign control switch lab ports to the pod.
8. Now lab devices for the pod equipment can be safely connected to the designated control switch(es).



If lab equipment is connected (step 3) before configuration steps 1 or 2, serious side effects will likely occur. These include packets loops, spanning tree problems, VTP problems, and trunking problems. These issues can cause high CPU utilization, error-disabled ports, on all control switches leading to complete connectivity loss for all pods. Be sure to include this guidance in any support documentation for pod designs containing lab switches that you make available to others.

The following special commands (step 2) are configured on each control switch port that connects to a lab switch. They are provided for reference. You do not need to configure them manually on NETLAB+ version 22 systems.

- **switchport mode access**
 - Prevents the link from becoming a trunk port.
 - The labs will not work as designed if the link between the control switch and the lab switch is trunking.
 - Trunking on ports that should be access ports, combined with BPDU filtering, creates loops that are not prevented by spanning trees.
- **switchport nonegotiate**
 - Prevents the interface from sending DTP messages.
 - Disabling DTP messages is not critical but will hide the control switch's MAC address from lab switches when users perform commands to see the CAM table.
- **spanning-tree bpduguard enable**
 - Instructs control switch port not to send and receive spanning tree BPDU frames to and from the lab switch.
 - Spanning tree in the lab must not mangle with the spanning tree on the control switch. This would cause several undesirable effects in both the lab and on the control switches.
- **no cdp enable**
 - Disabling CDP is not critical but will hide the control switch from lab switch users performing CDP commands.
- **no keepalive**
 - Prevents the interface from sending L2 keepalive messages.
 - Disabling L2 keepalives messages is not critical but will hide the control switch's MAC address from lab switches when users performing commands to see the CAM table.

Here is an example configuration for a control switch control port that is connected to a lab switch:

```
interface FastEthernet0/X
  description control port to lab switch LS1 port 7
  switchport mode access
  switchport nonegotiate
  spanning-tree bpdu filter enable
  no cdp enable
  no keepalive
```



These commands are now automatically configured by NETLAB+ version 22 and later. Without them, serious side effects will likely occur.

4.1.3.2 VLAN Map Special Rule for Pods Containing Lab Switches

When connecting lab switches to control switches, special care must be taken not to create loops and other side effects. The commands and rules outlined in the previous help prevent this, but there is another rule that pod and lab design authors must follow to avoid trouble.



When specifying VLAN maps, place pod ports connecting to lab switches in unique VLANs. Pod ports that connect to lab switches should NEVER share a common VLAN, unless there is absolutely no possibility of loop formation.

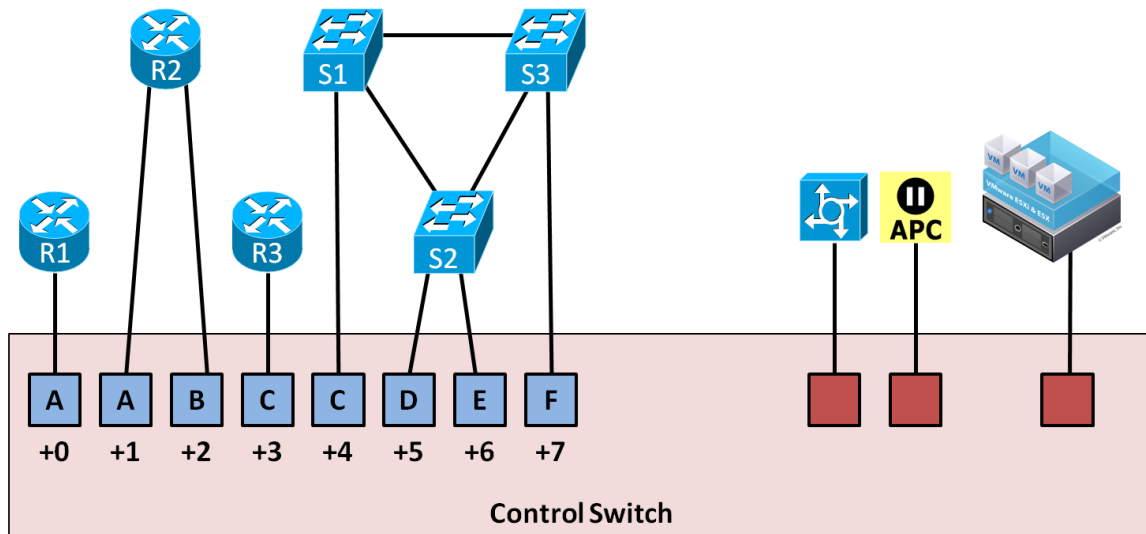
Explanation

1. Recall from the previous section that the spanning tree is intentionally disabled between the control switch (BPDU disabled) and lab switches. This creates a barrier between spanning tree domains.
 - a. Connections between lab switches and control switches are always non-trunking (switchport mode access, nonegotiate). Thus, VTP information is also isolated. That is, VLANs used on control switches are completely independent of VLANs that users may create on lab switches.
 - b. All packets between control switch and lab switches have no VLAN tagging.
2. By default, all lab switches ports will be placed in VLAN 1.
 - a. Any physical loops between lab switches will be prevented by the lab switch spanning tree domain.
 - b. However, spanning tree does not run between lab switch and control switch. Loop potential exists here.

These factors create the potential for loops to form between lab switches and control switches unless VLAN maps are properly constructed by pod and lab designers. By ensuring that control switch ports are placed on unique VLANs, you can ensure that interaction between control and lab switches will be loop-free, regardless of the configuration that takes place on the lab switches.

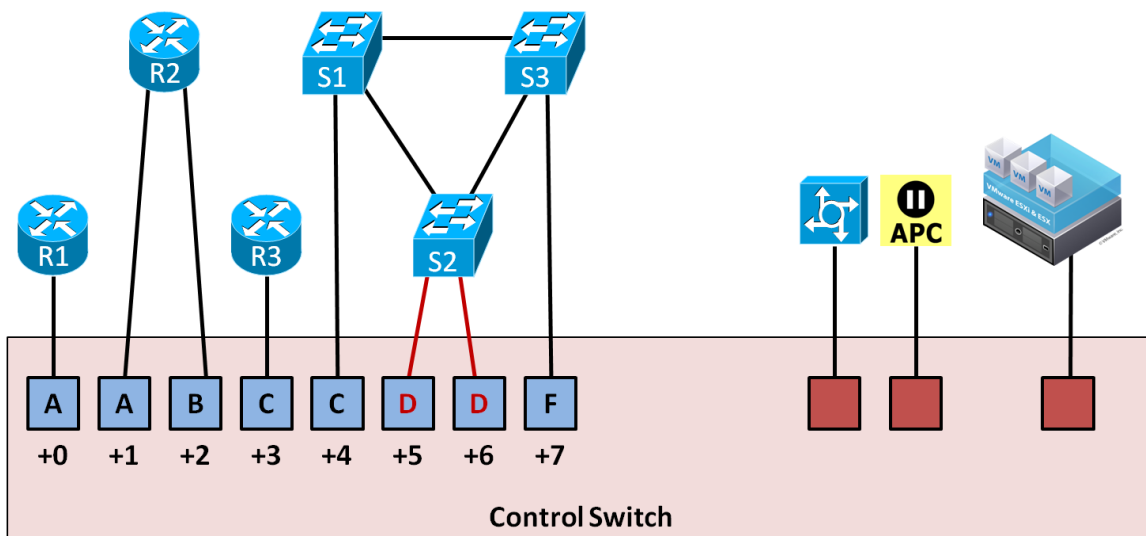
Example 1.

Our first example (below) shows a **valid** configuration. Each pod port connection on the control switch is placed in a unique VLAN (C, D, E, F). There is no possibility of looping through the control switch, regardless of how the user configures the lab switches.



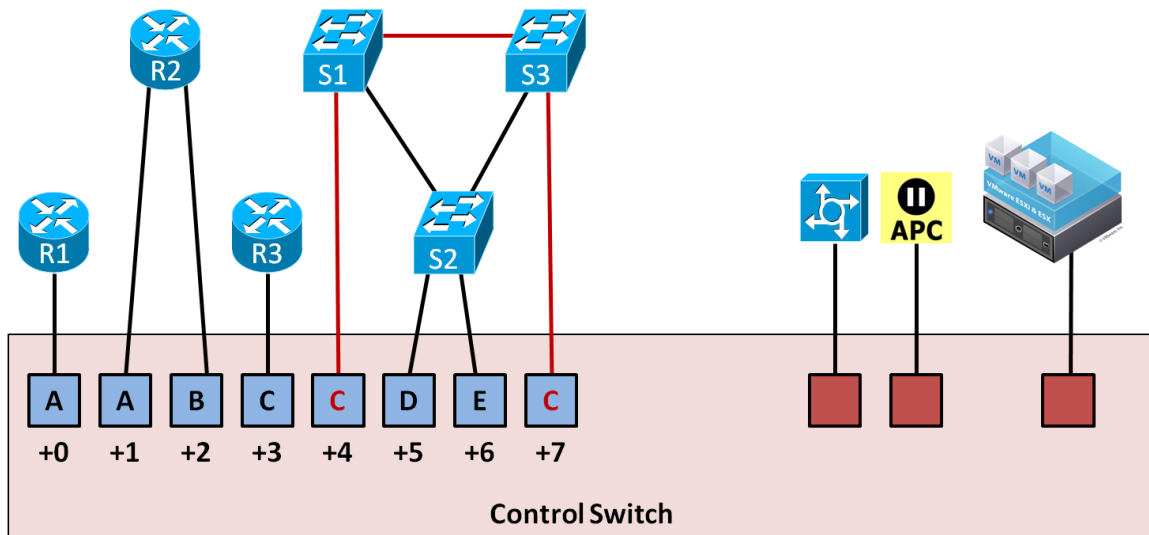
Example 2.

Our second example (below) shows an invalid VLAN map. Two ports share VLAN D. A loop will form between S2 and control switch. Broadcast traffic will quickly multiply and consume all the lab switches in this pod. More importantly, it will also consume the control switches with broadcast traffic.



Example 3.

This scenario is also invalid for the same reason as example 2.

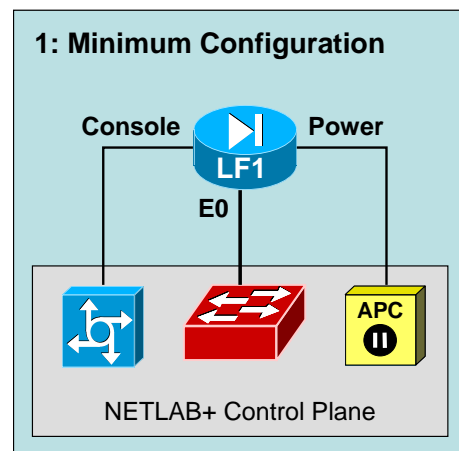


4.1.4 Lab Firewalls

The following connections are required for each lab firewall.

- One connection to an access server port.
- One connection to a switched outlet (i.e., APC device)
- One connection from the lowest numbered built-in Ethernet port to the control switch (i.e., Ethernet0).

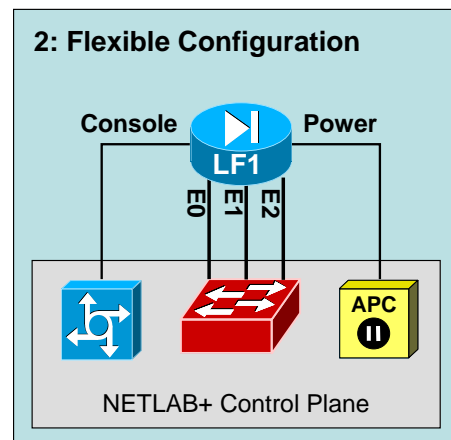
Refer to the three configuration scenarios below. LF1 is a lab firewall. LF1 has connections to the NETLAB+ control plane: access server (left), control switch (middle, recommended), and switch outlet device (right).



Configuration 1 depicts the minimum connection requirement for each lab firewall.

The lowest numbered port (typically Ethernet0) is used to manage the IOS image.

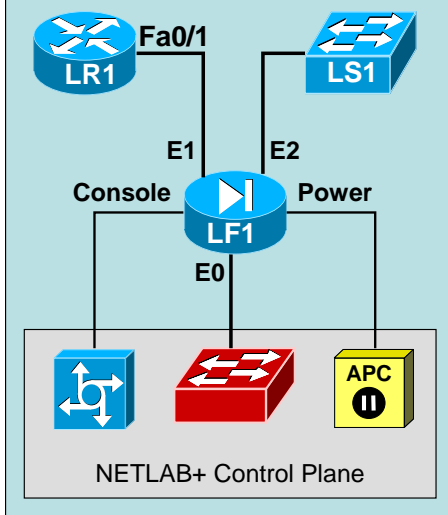
During the lab, this port may be turned off or mapped dynamically to a VLAN on the control switch to simulate a LAN segment. Dynamic VLAN mapping is a powerful feature that may be used to alter the lab topology. This can be done for each lab exercise.



Configuration 2 depicts all built-in Ethernet ports connected to the control switch.

Each Ethernet port connected to the control switch may participate in dynamic VLAN mapping. This technique can be used to create very flexible lab topologies from a single statically cabled pod.

3: Direct Connections



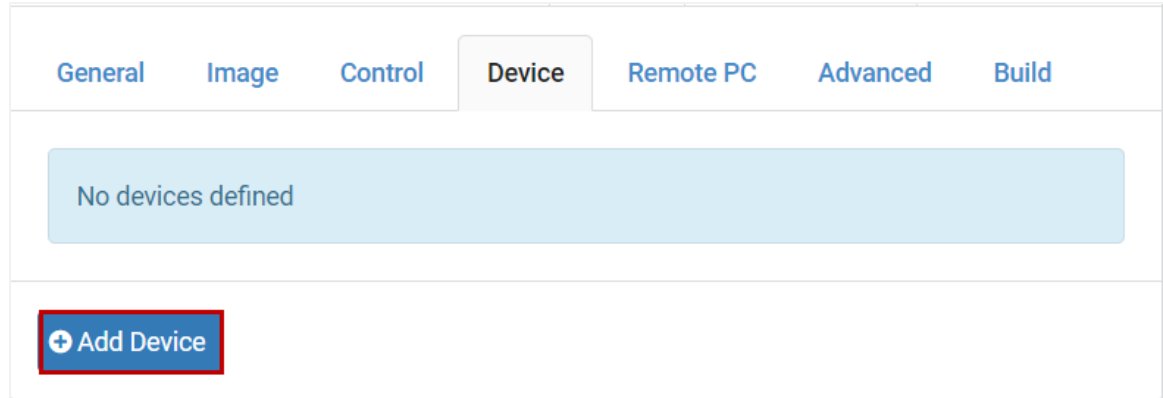
Configuration 3 shows a direct connection between a lab firewall (LF1) and two other lab devices (LR1, LS1).

Direct connections between firewalls and other devices may be required if the control switch would interfere with protocols that must be preserved to teach the core concepts (i.e., CDP). This is not usually the case with firewalls, as they typically are simple Ethernet ports.

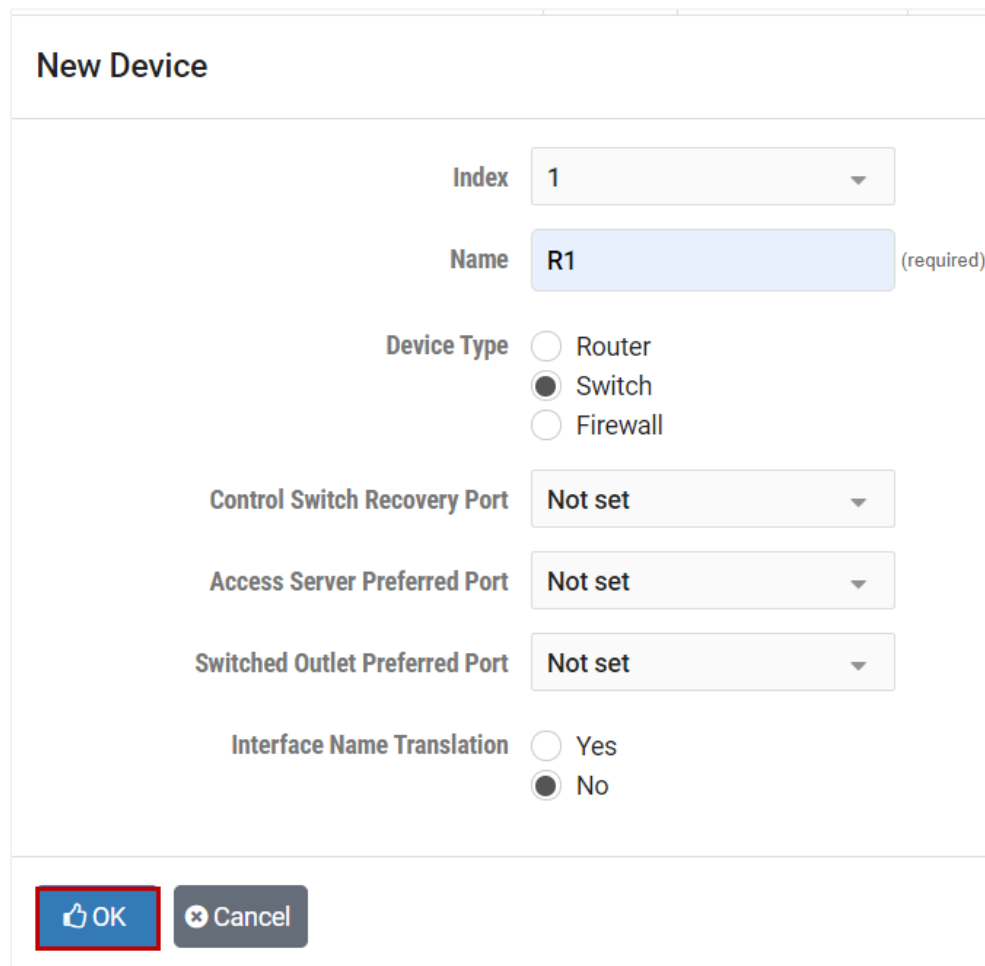
4.1.5 Adding a Lab Device

Follow the steps in this section to add a lab device to the pod design.

1. On the Device tab, click **Add Device** to add a new managed device.



2. The New Device page is displayed. On the Device tab, click **Add Device** to add a new managed device. Enter a name for the device and select the appropriate settings (refer to the field descriptions below). Click OK.



Field Descriptions – New Device

- **Index:** This value determines the order in which the device will appear in the various lab access tabs.
- **Name:** The default name of the device. This may be overridden by lab exercises.
- **Device Type:** The type of managed device required: router, switch, or firewall. This will determine the icon displayed on NETLAB+ screens.
- **Control Switch Recovery Port:** The relative control switch port that will be used to recover an IOS image that has been erased flash. This port is always connected to the lowest-numbered Ethernet port on the lab device. A value of “not set” can be specified to save a control switch port and/or if the NETLAB+ device driver does not support image recovery. This feature only applies to older Cisco devices that are no longer supported. Newer models will recover from USB and/or flash if recovery is supported.
- **Access Server Preferred Port:** The suggested port on the access server the lab device should use relative to the first port. This value will be used if the administrator requests consecutive ports. However, the administrator may override this value and explicitly choose an access server and port.
- **Switched Outlet Preferred Port:** The suggested port on the switched outlet device this lab device should use relative to the first port. This value will be used if the administrator requests consecutive ports. However, the administrator may override this value and choose any switched outlet device and port.
- **Interface Name Translation:** The feature allows configuration files saved by NETLAB+ to be loaded, without errors, on a different pod with different router types. This setting is currently supported on managed routers and ignored by managed switches and firewalls. As a configuration is loaded, NETLAB+ will substitute the correct interface names for the actual router types being used (if necessary). To do this, NETLAB+ maintains a fixed table of interface names that should be present on each supported router model. Currently, this table supports two Ethernet and two serial interfaces.

If possible, you should always use the same hardware models on a similar pod type. This way, the interface names will not be a factor during automated load and save operations.

4.1.6 Adding Hotspots

You may define clickable hotspots for devices shown on the default topology image. A hotspot is an invisible rectangular area placed on top of a device in the image. When a user clicks on a device, NETLAB+ will launch a terminal application and connect to the console of the device.




Please see section [2.1.2](#) for instructions on adding hotspots.

4.1.7 Cable Guidance

Each managed device can provide cabling guidance for the administrator. This feature is currently used by NDG for NETLAB+ pods. This feature is not yet documented for general use.

4.1.8 Modifying a Managed Lab Device

To modify a managed lab device, select the device by clicking **Edit** on the Action dropdown.

General Image Control Device Remote PC Advanced Build								
Index	Type	Name	Hotspot	CS	AS	SO	INX	Action
1		pfSense	322,136,382,196				No	▼
<div> <div>+ Add Device</div> <div>⦿ Set Hotspots</div> <div>  Edit  View Cables </div> </div>								

See section 4.1.5 for a description of each field on the page.

Device [pfSense]

Index

1 ▼

Name

pfSense (required)

Device Type

☐ Router
☐ Switch
☒ Firewall

Control Switch Recovery Port

Not set ▼

Access Server Preferred Port

Not set ▼

Switched Outlet Preferred Port

Not set ▼

Interface Name Translation

☐ Yes
☒ No

OK

Remove Device

Cancel

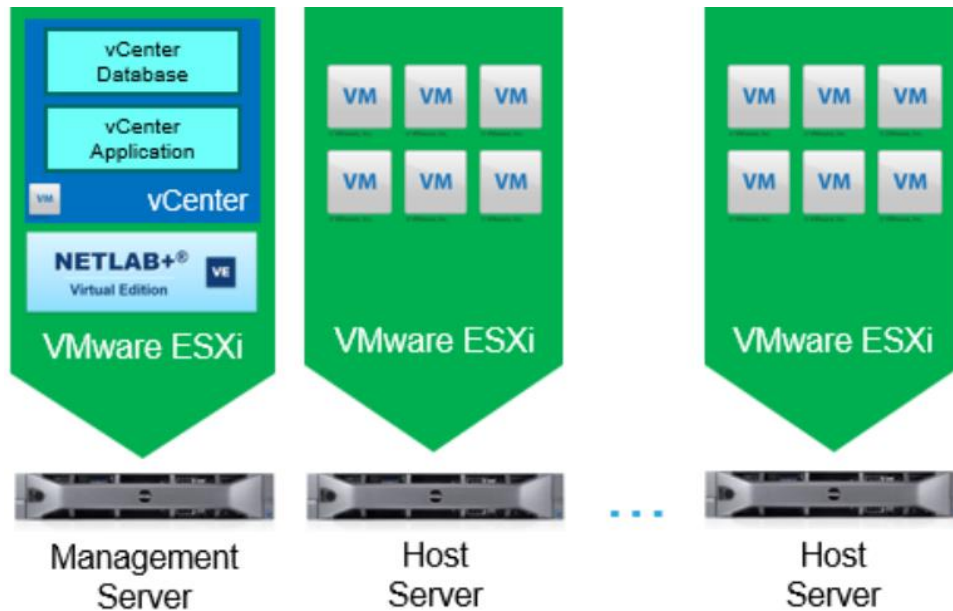
Select **OK** to save your modifications.

4.1.9 Deleting a Managed Lab Device

To delete a managed lab device, select the device from the Device tab by clicking **Edit** on the Action dropdown (see section [4.1.8](#)) and then select the **Remove Device** button.

5 Remote PC

A *remote PC* is a virtualized PC or virtualized server that is remotely accessible and configurable by lab users. Virtual machines are implemented using supported third-party virtualization products such as VMware ESXi.











The flexibility and broad selection of operating systems and configurations that may be provisioned on a virtual machine offer great potential to support IT training in a wide range of disciplines using NETLAB+.

Non-virtualized "physical" PCs and servers are no longer supported as Remote PCs.

5.1 Managing Remote PCs

Adding remote PCs using Pod Designer is fairly straightforward. Each remote PC is given a name and an icon designation of “PC” or “server”. A pod may contain very little information about remote PCs. Most of the remote PC settings are determined by the administrator when an actual pod is added to the system. Remote PCs are added and managed from the Remote PC tab.

General	Image	Control	Device	Remote PC	Advanced	Build
Index	Icon	Name	Hotspot	Actions		
1		PC1	Not set			
2		PC2	Not set			
3		PC3	Not set			



5.1.1 Adding a Remote PC

Click on the Add PC button. NETLAB+ will display the New Remote PC dialog.




Name	Build	Committed	Author ID	Global ID
Test123	1	No	TEST123	___6501_C07C

New Remote PC

Index

Display Icon ☒  ☐ 

Name (required)

Index. Determines the order in which the PC will appear in the various lab access tabs.

Display Icon. Determines which icon (PC or server) will be associated with the PC and displayed on various pages. This setting only affects the icon that is shown. It does not affect functionality.

Name. The name of the PC.




5.1.2 Setting Hotspots

You may define clickable hotspots for PCs shown on the default topology image. A hotspot is an invisible rectangular area placed on top of a remote PC in the image. When a user clicks on a hotspot, NETLAB+ will launch the appropriate remote PC viewer and connect to the virtual machine.

Please see section 2.1.2 for instructions on adding hotspots.

5.1.3 Modifying a Remote PC

To modify the settings for a Remote PC, select **Edit** on the Actions dropdown.

General	Image	Control	Device	Remote PC	Advanced	Build
Index	Icon	Name	Hotspot		Actions	
1		PC1	Not set		<div>⌵</div>	
2		PC2	Not set		<div>⚙ Edit</div>	
3		PC3	Not set		<div>⌵</div>	
<div>+ Add PC</div>		<div>⦿ Set Hotspots</div>				

Please refer to the previous section for descriptions of each field.

Name	Build	Committed	Author ID	Global ID
Test123	1	No	TEST123	__6501_C07C

Remote PC [PC1]

Index

1

⌵

Display Icon

☒

☐

Name

PC1

(required)

OK

Remove PC

Cancel

Help

After completing modifications, select the **OK** button.

5.1.4 Removing a Remote PC

To delete a Remote PC, select the device by clicking Edit on the Actions dropdown and then select the **Remove PC** button.


Name	Build	Committed	Author ID	Global ID
Test123	1	No	TEST123	___6501_C07C


Remote PC [PC1]

Index

1

Display Icon

☒ 

☐ 

Name

PC1

(required)

OK

Remove PC

Cancel

Help

6 Advanced Settings

NETLAB+'s Advanced configuration settings are based on simple "key=value" strings. Advanced settings allow pod designers to take advantage of new features and capabilities that are still evolving and have not been backed by a final user interface in NETLAB+.

Advanced settings for a pod design can be accessed and viewed from the Advanced tab.

Name	Build	Committed	Author ID	Global ID
Test123	1	No	JD224	4581_B0FF_9639_65A8_26BB

[General](#) [Image](#) [Control](#) [Device](#) [Remote PC](#) [Advanced](#) [Build](#)

Advanced Settings

```
pod.requires.vm_same_host=1
pod.requires.vm_types=AVMI,ABSENT

pod.auto.net.supported=1
pod.auto.net.enabled.default=1
pod.auto.net.host.setup.supported=1
pod.auto.net.host.setup.enabled.default=1
pod.auto.net.host.teardown.supported=1
pod.auto.net.host.teardown.enabled.default=1

# vmware virtual switches created on host
vswitch.0.name.include.pod_id=1
vswitch.0.name.suffix=VS1
```

[Modify Advanced Settings \(NDG\)](#)

[Close Pod Design](#)

6.1 Modifying Advanced Settings

To modify Advanced settings:

1. Click the Advanced tab.
2. Click the Modify Design button.
3. Enter the pod modification password, if any.
4. Click the Modify Advanced Settings Button.
5. Enter configuration directives, one per line in the text area. Each line may contain one of the following elements:
 - a. A *key=value* configuration directive. Supported directives are discussed in the next section.
 - b. A blank line.
 - c. A comment beginning with the pound symbol (#) in the first column.

Name	Build	Committed	Author ID	Global ID
Test123	1	No	JD224	4581_B0FF_9639_65A8_26BB

Advanced Settings (NDG)

Advanced Settings

```

pod.requires.vm_same_host=1
pod.requires.vm_types=AVMI,ABSENT

pod.auto.net.supported=1
pod.auto.net.enabled.default=1
pod.auto.net.host.setup.supported=1
pod.auto.net.host.setup.enabled.default=1
pod.auto.net.host.teardown.supported=1
pod.auto.net.host.teardown.enabled.default=1

# vmware virtual switches created on host
vswitch.0.name.include.pod_id=1
vswitch.0.name.suffix=VS1
vswitch.0.ports=6

vswitch.0.portgroup.0.id=common
vswitch.0.portgroup.0.name.include.pod_id=1
vswitch.0.portgroup.0.name.suffix=PG1
vswitch.0.portgroup.0.vlan.mode=UNTAGGED
vswitch.0.portgroup.0.vlan.id=1
          
```

Avoid trailing whitespace at the end of a line.

6.2 Advanced Configuration Directive Reference

The following configuration directives are currently supported. These may be complemented or replaced by user interface elements in future versions. Please see subsequent sections for examples; it may be easier to learn from examples than to return to the reference.

6.2.1 Pod Requirement Configuration Directives

Pod requirement configuration directives allow the pod designer to ensure certain requirements are met by the NETLAB+ administrator.

6.2.1.1 `pod.requires.vm_same_host`

When enabled, it will force the administrator to place all VMs for this pod on the same virtual host system. VMs on the same host can communicate with each other using virtual networking on the host and do not require external networking. This should generally be enabled on any pod that supports automatic networking.

Synopsis

```
pod.requires.vm_same_host=1
```

Values

- 1** enabled
- 0** disabled (default)

Deprecated. This setting should always be set to enabled (1). Virtual machines of a single pod should be run on the same host system. Future versions of NETLAB+ may ignore this setting.

6.2.1.2 `pod.requires.vm_types`

This directive enforces the types of virtual machines that can be used with this pod. The primary use of this directive is to indicate that the pod relies on the advanced features of the NETLAB+ Virtual Machine Inventory, ESXi 4.X+, and VMware vCenter.

You would typically use this setting for Pure Virtual Machine Pods, which would be difficult to replicate and stand up without pod cloning and automatic networking support. For example, NDG uses this setting on the VMware ICM pod to ensure that the proper virtual machine host environment will support pod cloning and automatic networking; it would be difficult to configure and support an ICM pod on a standalone VMware host without the help of VMware vCenter. NDG omits this setting on its

standard hybrid pods to allow all older versions and/or standalone versions of VMware to be used.

Synopsis

```
pod.requires.vm_types=AVMI,ABSENT
```

Values

These are the intended values to be used by this directive.

AVMI	pod may contain virtual machine inventory / vCenter VMs
ABSENT	pod may contain missing VMs

Example

```
pod.requires.vm_types=AVMI,ABSENT
```

This directive requires that each VM in the pod must be registered in the NETLAB+ Virtual Machine Inventory, which also implies that it is supported by vCenter and the advanced automation capabilities of NETLAB+. Alternatively, the administrator may choose ABSENT on any particular VM. Any other virtual machine host platforms will be disallowed for pods of this type. For example, VMware Server 2 or standalone ESXi virtual machines would not be a configurable option for pods of this type.



Deprecated. This setting is ignored in NETLAB+ VE version 22.X.X and higher.

6.3 Automatic Networking Configuration Directives

The following scenarios are currently supported by automatic networking:

- Pure Virtual Machines Pods with no external networking
- Hybrid pods with no external networking

The following scenarios are not currently supported by automatic networking but may be in future software versions:

- Pods connecting to external networks or the internet.

6.3.1 pod.auto.net (category)

The pod.auto.net configuration directives specify which automatic networking features are supported by the pod. The administrator may choose to disable these features if manual networking is desired.

6.3.1.1 pod.auto.net.supported

Enables or disabled automatic networking features for the pod design. Requires other directives if enabled. The administrator may disable automatic networking on a per-pod basis if manual networking is desired.

Synopsis

```
pod.auto.net.supported=1
```

Values

- 1** enable automatic networking support for pod design
- 0** disable automatic networking support for pod design (default)

6.3.1.2 pod.auto.net.host.setup.supported

If enabled, it allows virtual switches and/or portgroups to be automatically created on the virtual machine host per the pod design specifications. Switches and portgroups are created when a pod reservation starts. The administrator may disable this feature on a per-pod basis if manual setup is preferred.

Synopsis

```
pod.auto.net.host.setup.supported=1
```

Values

- 1** enable automatic vswitch/portgroup setup for pod design
- 0** disable automatic vswitch/portgroup setup for pod design (default)

6.3.1.3 pod.auto.net.host.teardown.supported

If enabled, it allows virtual switches and/or portgroups to be automatically removed from the virtual machine host when the pod reservation ends. This frees networking resources from the host when they are not being used by the pod. The administrator may disable this feature on a per-pod basis if manual teardown (or persistent networking) is preferred.

Synopsis

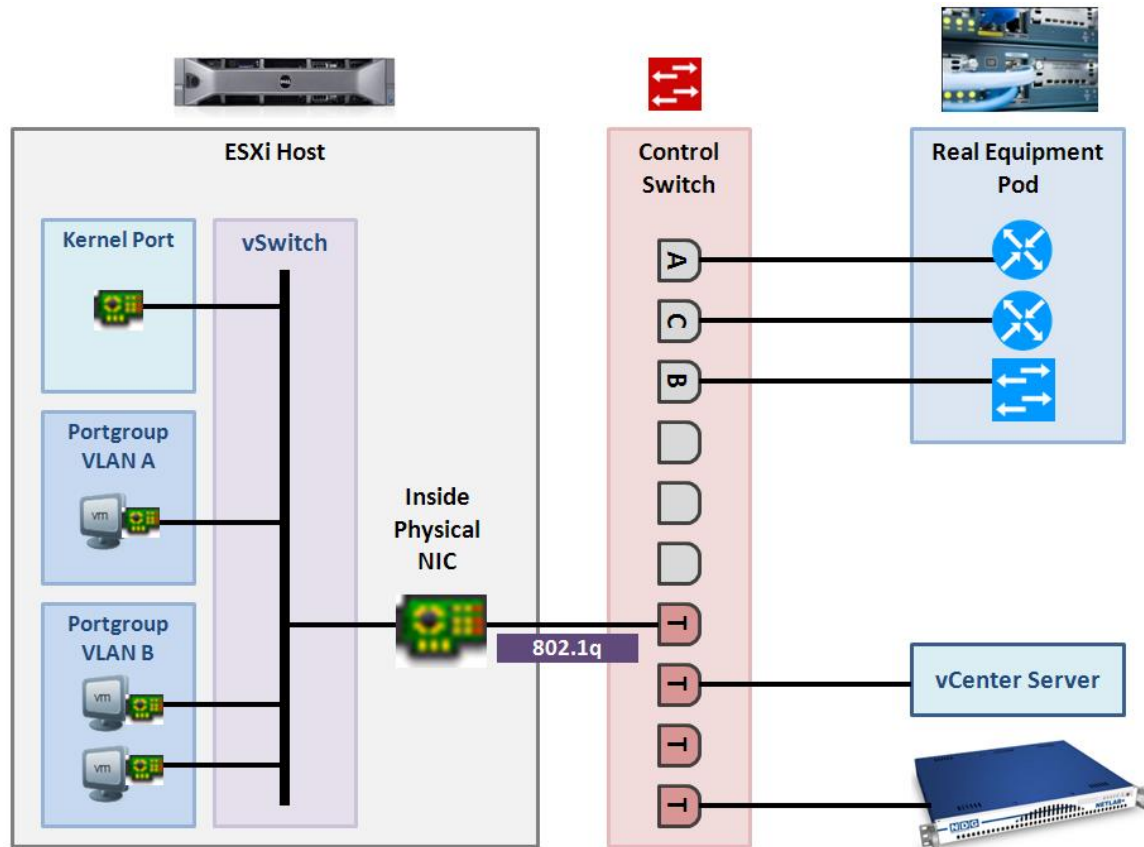
```
pod.auto.net.host.teardown.supported=1
```

Values

- 1** enable automatic vswitch/portgroup teardown for pod design
- 0** disable automatic vswitch/portgroup teardown for pod design (default)

6.3.2 Automatic Networking Support for Hybrid Pods

Hybrid pods contain both real equipment and virtual machines. To transport network traffic between virtual machines and real equipment, each virtual machine host server is connected to a control switch and configured for 802.1q (trunking mode).



The network interface that connects to the control switch on the VM host server is associated with the NETLAB+ inside virtual switch (typically vswitch1). The designated inside vswitch is specified by the NETLAB+ administrator in the Virtual Machine Host Server settings and can be specified on a per-host basis. Each VLAN within the inside vswitch is backed by a virtual portgroup within the virtual switch.

- Using NETLAB+ versions 2011.R2 (and later) with vCenter implementation, VLAN portgroups for hybrid pods can be automatically created and removed from the inside vswitch using the following configuration directives in the pod design:
 - `pod.auto.net.control_switch.vlans`
 - `pc.net.vnic.vlan`
- When using NETLAB+ versions prior to 2011.R2 and/or standalone VMware host server implementations, the NETLAB+ administrator must create these portgroups manually.

The `pod.auto.net.control_switch.vlans` setting is used in conjunction with the `pc.net.vnic.vlan` directive, which bind virtual network adapters (vNIC) to a particular

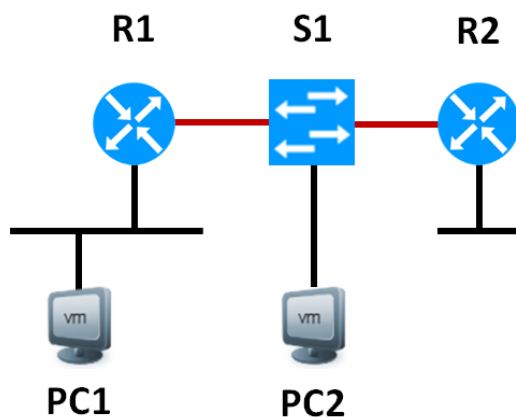
VLAN. VLAN letters are used instead of numbers, because the actual VLAN numbers cannot be determined at design time (as explained in section [3.5.4](#)).

VLAN maps cannot be currently specified for virtual machine networking interfaces. Virtual machine VLANs remain fixed regardless of lab exercise. This is to maintain backward compatibility with a large installed base of standalone VMware host implementations that cannot support this feature. To overcome this limitation, real network device interfaces must move into the same VLANs with virtual machines (which remain fixed regardless of lab exercise).

Deprecated. Virtual machines in a pod always use the same VLAN, regardless of lab exercise. Real lab equipment may change VLANs on a per lab basis.

Example 1

We wish to provide automatic networking for virtual machines in the following hybrid topology.



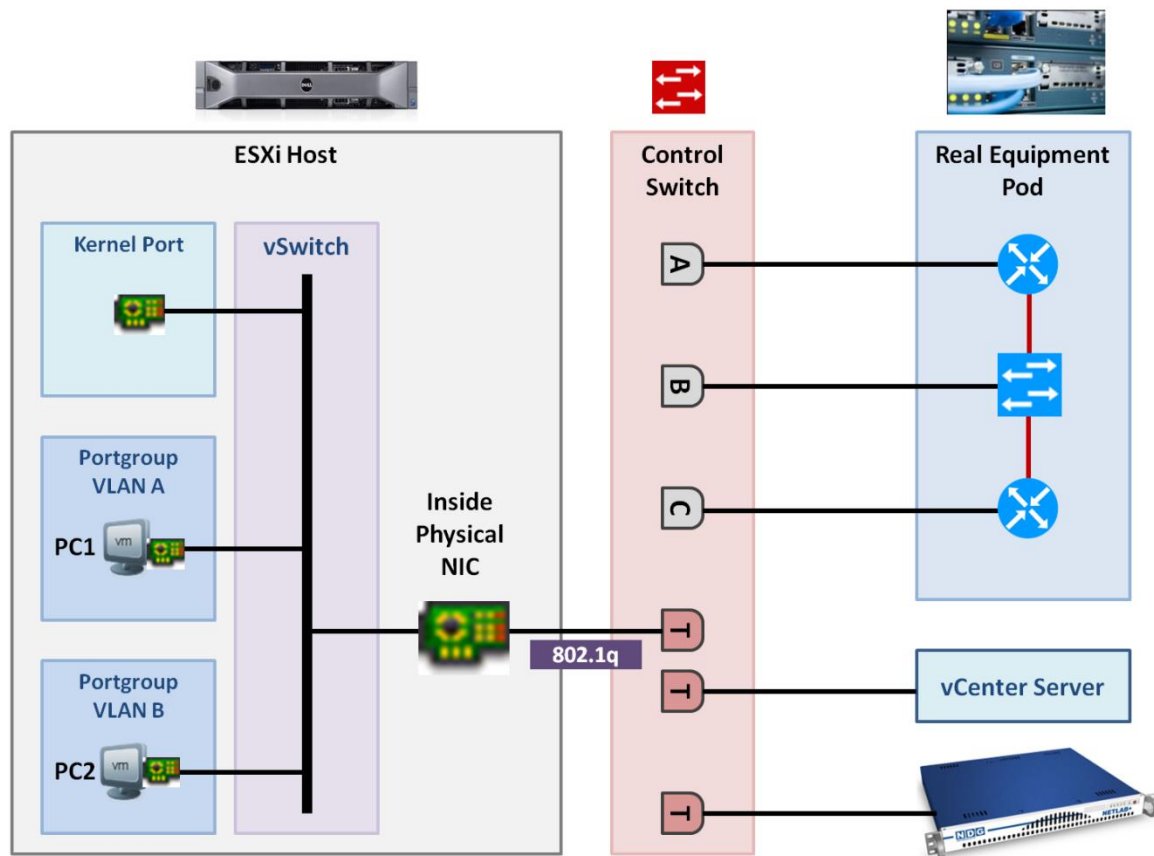
The black Ethernet segments:

- Are implemented through the control switch
- Can participate in VLAN maps
- Can connect to virtual machines
- Cannot use 802.1q

The red Ethernet segments:

- Are direct hard-wired connections between lab routers and lab switch
- Can support 802.1q if configured

The topology is implemented as follows with respect to the VM host server, control switch, and default VLAN map.



The following advanced configuration directives are implemented in the pod design to support automatic networking of the virtual machines.

```
pod.auto.net.supported=1
pod.auto.net.host.setup.supported=1
pod.auto.net.host.teardown.supported=1

pod.auto.net.control_switch.vlans=A,B

pc.1.net.vnic.1.vlan=A
pc.2.net.vnic.1.vlan=B
```

Note that VLAN C is not required in the `pod.auto.net.control_switch.vlans` directive, as there are no virtual machines in VLAN C. This avoids unnecessary setup and teardown of an empty portgroup.

VLAN maps for virtual machines are not currently supported. However, it is still possible to move virtual machines in this topology. For example, if a lab exercise wanted to relocate PC1 from the R1's stub network to R2's stub network, you could change the VLAN map from A-B-C to C-B-A; the router stub network moves to the PC, rather than the PC moving to the router stub network.

When a pod of this type starts up, a port group for VLAN A and VLAN B is created on the inside vswitch. Given a pod ID of 1 and a NETLAB+ global system ID of 1, the portgroups would be named NETLAB001_POD1_VLAN100_A and NETLAB001_POD1_VLAN101_B, respectively.

When the pod reservation is complete, NETLAB+ will remove the two portgroups from the inside vswitch.

6.3.3 pod.auto.net.control_switch.VLANs

This configuration directive specifies which VLANs are used by virtual machines in hybrid pod designs. It is used in conjunction with the pc.net.vnic.vlan directive, which binds virtual network adapters (vNIC) to a particular VLAN.

Synopsis

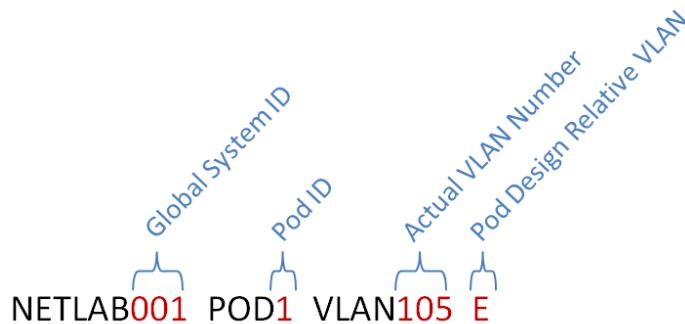
```
pod.auto.net.control_switch.vlans=A, B, C, ..., Z
```

Upon pod startup, a portgroup for each specified VLAN is created on the inside vswitch. These portgroups are removed when the pod reservation ends.

VLAN letters are used instead of numbers since the actual VLAN numbers cannot be determined at design time (as explained in [3.5.4](#)).

Only VLANs that contain virtual machines should be listed. Omit VLAN letters that do not contain virtual machines to avoid setup and teardown of empty portgroups.

The portgroups that are created by NETLAB on the inside vswitch are named as follows.



- **Global System ID:** A unique number assigned to the NETLAB+ system. Normally 001, but can be altered by the administrator when multiple NETLAB+ systems share a virtual host environment.
- **Pod ID:** The numeric ID assigned to the pod by the administrator.

- **Actual VLAN Number:** This is the 802.1q VLAN ID bound to the portgroup. It is automatically calculated from pod ID and relative VLAN letter.
- **Pod Design Relative VLAN:** This is the relative VLAN letter as specified in the pod design. It is shown in the portgroup name for easy association with the pod design VLANs.

Synopsis

```
pod.auto.net.control_switch.vlans=A,B,C,...,Z
```

Values

A comma-separated list of relative VLAN letters that will be used by virtual machines in the pod.

Example

```
pod.auto.net.supported=1
pod.auto.net.host.setup.supported=1
pod.auto.net.host.teardown.supported=1

pod.auto.net.control_switch.vlans=A,D,E

pc.1.net.vnic.1.vlan=A
pc.2.net.vnic.1.vlan=A
pc.3.net.vnic.1.vlan=D
pc.3.net.vnic.2.vlan=E
```

In this example, three portgroups are created for virtual machines residing in VLAN A, VLAN D, and VLAN E. The pod also uses VLAN B and VLAN C, but they are omitted from the configuration directive because they do not contain virtual machines.

Actual network bindings are performed by the pc.net.vnic.vlan directives.

- PC1 and PC2 have one network adapters that are bound to VLAN A.
- PC3 is dual-homed. Network adapter 1 is bound to VLAN D. Network adapter 2 is bound to VLAN E.

6.3.4 vswitch (category)

Synopsis

```
who=dat
```

Values

1 enabled
0 disabled

Example

```
who=date
```

6.4 Automatic Networking Configuration Directives

The following scenarios are currently supported by automatic networking:

- Pure Virtual Machines Pods with no external networking
- Hybrid pods with no external networking

The following scenarios are not currently supported by automatic networking but may be in future software versions:

- Pods connecting to external networks or the internet

6.4.1 Automatic Networking for Pure Virtual Machine Pods

```
pod.auto.net.supported=1  
pod.auto.net.host.setup.supported=1  
pod.auto.net.host.teardown.supported=1
```

```
pod.auto.net.control_switch.vlans=A,C,E
```

```
pc.1.net.vnic.1.vlan=A  
pc.2.net.vnic.1.vlan=A  
pc.3.net.vnic.1.vlan=C  
pc.4.net.vnic.1.vlan=E
```

6.4.2 PC-Only Pod Designs

When a pod design contains only PCs and no managed lab devices, it is not necessary to allocate lab device ports and VLANs for control switches in the pod design. This is generally true if there are no special connectivity requirements and the PCs in the pod just communicate amongst themselves. Simply connect them to one or more virtual switches (VMnets).

If your pod has one PC, or PCs that do not need to communicate, then no virtual switches are required. The NETLAB+ viewers work with the VMware host to display the mouse, keyboard, and screen (MKS); the virtual machine does not require a network adapter or network connection for MKS.

6.4.3 Hybrid Pod Designs

In a hybrid pod design, remote PCs and lab devices communicate with each other. Virtual machines (which are the remote PCs) connect to virtual switches on a virtual machine host (i.e., VMware ESXi). They are bound to real VLAN numbers by NETLAB+ and trunked to a pod's designated lab device ports. In NETLAB+ version 22, this happens automatically.

In NETLAB+ version 22, this is an automated process.

6.5 Virtual Machine Deferred Booting

Sometimes, it is necessary to defer the booting of a virtual machine to allow other virtual machines or resources to become available first. NETLAB+ provides three advanced configuration settings that can control deferred booting.

```
pc.<i>.boot.delay  
pc.<i>.after_pc_index=<j>  
pc.<i>.after_pc_extra=<j>
```

These settings are enforced:

- At the beginning of a lab reservation.
- When a user switches lab exercises during a reservation, if the user chooses to reset virtual machines at that time.

6.5.1 pc.<x>.boot.delay=<seconds>

The directive delays the boot of a virtual machine by a specified number of seconds. The index <i> is the index of the remote PC, as shown in the Pod Designer. The default is 0 seconds (no delay).

Synopsis

```
pc.<i>.boot.delay=<seconds>
```

Example

```
pc.2.boot.delay=30
```

This example will cause the remote PC with index 2, if present, to delay booting of the corresponding virtual machine 30 seconds after a lab reservation is started or lab exercise is switched (with VM resets).

Caveats

- This directive was added in NETLAB+ version 22.7.3 and was ignored in previous versions.
- The specified delay time will be accurate to within 5 seconds.
- Other settings may cause this value to be ignored or adjusted.

6.5.2 pc.<x>.boot.after_pc_index=<j>

This directive causes the remote PC with index <i> to boot after the PC with index <j> boots. Both <i> and <j> are the remote PC indices of the virtual machines, as shown in the Pod Designer. NETLAB+ considers a virtual machine to have booted when the VMware Tools process is running on the virtual machine.

Synopsis

```
pc.<x>.boot.after_index=<j>
```

Example

```
pc.2.boot.after_index=5
```

This example will cause the remote PC with index 2 to delay booting until the remote PC with index 5, if present, has booted.

Caveats

- This directive was added in NETLAB+ version 22.7.3 and was ignored in previous versions.
- This setting is ignored for pc.<i> if pc.<j> is absent, or pc.<j> is not used by a lab exercise.
- If pc.<i>.boot.delay is not specified, a minimum value of 120 seconds is set when pc.<x>.boot.after_index=<j> is specified. This ensures that pc.<i> will eventually

boot, even if VMware Tools on pc.<j> is never detected. This delay may be too long, so it is always best to set boot.delay to a reasonable value when using boot.after_index.

6.5.3 pc.<x>.boot.after_pc_extra=<seconds>

Used in conjunction with boot.after_index, this directive causes the remote PC with index <i> to wait an extra amount of time (in seconds) to boot, after VMware Tools is detected on pc.<j>.

Synopsis

```
pc.<x>.boot.after_extra=<seconds>
```

Example 1

```
pc.2.boot.after_index=5  
pc.2.boot.after_extra=15  
pc.2.boot.delay=60
```

This example will cause the remote PC with index 2 to defer booting until one of the following conditions occurs (whichever comes first):

- VMware Tools is running on the PC with index 5, AND 15 extra seconds have elapsed.
- 60 seconds have elapsed since the pod reservation was started.

Example 2

```
pc.2.boot.after_index=5  
pc.2.boot.after_extra=10
```

This example will cause the remote PC with index 2 to defer booting until one of the following conditions occurs (whichever comes first):

- VMware Tools is running on the PC with index 5, AND 10 extra seconds have elapsed.
- 120 seconds have elapsed since the pod reservation was started. This is the default setting for pc.2.boot.delay if not specified AND pc.2.boot.after_index is set.

Caveats

- This directive was added in NETLAB+ version 22.7.3 and was ignored in previous versions.
- This setting is ignored for pc.<i> if pc.<j> is absent, or pc.<j> is not used by a lab exercise.

- This setting is also ignored if the setting `pc.<i>.boot.after_index=<j>` is omitted.
- If `pc.<i>.boot.delay` is not specified, a minimum value of 120 seconds PLUS the `boot.after_extra` setting. This ensures that `pc.<i>` will eventually boot, even if VMware Tools on `pc.<j>` is never detected. This delay may be too long, so it is always best to set `boot.delay` to a reasonable value when using `boot.after_index`.

6.6 Remote PCs

A pod design contains very little information about remote PCs. Most of the remote PC settings are determined by the administrator when an actual pod is added to the system.

Remote PCs are optional.

General

Image




Control

Device

Remote PC

Advanced

Build

Index	Icon	Name	Hotspot	Actions
1		PC1	Not set	<div></div>
2		PC2	Not set	<div></div>
3		PC3	Not set	<div></div>

+ Add PC

Set Hotspots

6.6.1 Adding a Remote PC

Click on the Add PC button. NETLAB+ will display the New Remote PC dialog.


Name	Build	Committed	Author ID	Global ID
Test123	1	No	TEST123	___6501_C07C


New Remote PC

Index

1

Display Icon

☒ 

☐ 

Name

PC1

(required)

OK







Cancel



Help

- **Index:** Determines the order in which the PC will appear in the various lab access tabs.
- **Display Icon:** Determines which icon (PC or server) will be associated with the PC and displayed on various pages. This setting only affects the icon that is shown. It does not affect functionality.
- **Name:** The name of the PC.

6.6.2 Modifying a Remote PC

To modify the settings for a Remote PC, select **Edit** on the Actions pull-down.

General	Image	Control	Device	Remote PC	Advanced	Build
Index	Icon	Name	Hotspot	Actions		
1		PC1	Not set			
2		PC2	Not set			
3		PC3	Not set			


Please refer to the previous section for descriptions of each field.

Remote PC [PC1]

Index

1

Display Icon

☒ 
☐ 

Name

PC1

(required)

OK


Remove PC

Cancel

Help

After completing modifications, select the **OK** button.

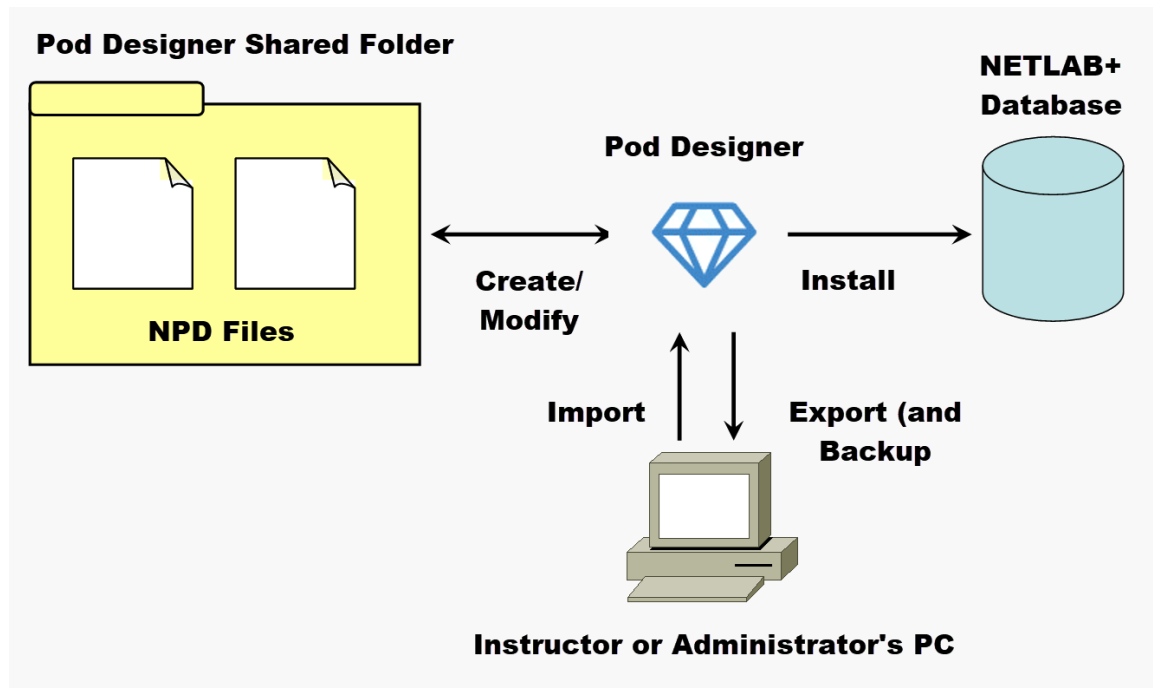
6.6.3 Removing a Remote PC

To delete a Remote PC, select the device by clicking the appropriate  button on the Remote PC tab (See section 6.6.2). The **Remove PC** button is available on the Remote PC page (See previous section).

7 Working With Pod Design Files and Builds

Pod Designer does not create actual pods. Rather, it produces an NPD file, which is a pod template. The administrator and each instructor share a common folder where NPD files are stored and manipulated by Pod Designer. NPD files can be exported to your PC, shared with others, and transferred to other NETLAB+ systems.

The NPD file format has built-in version control. Each version is called a *build*. Builds are managed from the build tab. When all desired changes have been made to the NPD file, the build is *committed*. Only a committed build can be *installed* into the NETLAB+ database, which allows the administrator to add actual pods based on the pod design.



A new build must be created to make further changes to the pod design. All changes must be made to the NPD file.

Certain settings cannot be changed once the first build is committed unless the pod design is retooled. Please see section [7.12](#) for discussion.

You cannot modify pod designs directly in the NETLAB+ database. Therefore, it is important to export, backup, and protect your NPD files.

Always keep backup copies of your pod designs. Pod design files are not automatically backed up by the system. The export function is used to make backups and is described in section [7.7](#).

When you are done working with a pod design, always click on the **Close Pod Design** button at the bottom of the tabbed interface. This will ensure that all changes are saved and the file is unlocked.

7.1 The Build Tab

Many of the tasks described in this section are managed from the Build tab. A set of buttons for different actions will appear near the end of the Build tab page. The buttons shown on the build tab will vary depending on the state of the build and if the NPD file is being modified.

Name	Build	Committed	Author ID	Global ID
Test123	2	Yes	TEST123	___6501_C07C

General	Image	Control	Device	Remote PC	Advanced	Build
---------	-------	---------	--------	-----------	----------	-------

Installed	Build #	Description	Retool
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No

Install

New Build

Export

Delete

Close Pod Design

Modify Design

7.2 Modifying a Build

To modify a build, click on the Modify Design Button at the bottom of the tabbed interface. Once you are modifying a build, you can make changes to almost all of the settings contained within the design file.

If you are already modifying, the Modify Design button will not appear. If the current build is committed, you must create a new build as described in section [7.11](#) before changes can be made.

Name	Build	Committed	Author ID	Global ID
Test123	2	Yes	TEST123	__6501_C07C

[General](#)
[Image](#)
[Control](#)
[Device](#)
[Remote PC](#)
[Advanced](#)
[Build](#)


Installed	Build #	Description	Retool
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No

[Install](#)
[New Build](#)
[Export](#)
[Delete](#)

[Close Pod Design](#)
[Modify Design](#)

Button does not appear if the design file is already being modified.

If a modification password is assigned to the design file, you will be asked to provide the correct password before modification is allowed.

 **Password Required**

This file is password protected. Before changes are allowed, you must supply the **current** modification password.

Enter the current modification password: (required)

[OK](#)
[Cancel](#)
[Help](#)

7.3 Committing a Build





The NPD file format has built-in version control. Each version is called a *build*. Builds are managed from the build tab. When all desired changes have been made to the NPD file, the build is *committed*. Only a committed build can be *installed* into the NETLAB+ database. To commit the current build, click on the Commit button in the Build tab.

You must modify the design file in order for the Commit button to appear.


Name	Build	Committed	Author ID	Global ID
Test123	3	No	TEST123	__6501_C07C

General	Image	Control	Device	Remote PC	Advanced	Build
---------	-------	---------	--------	-----------	----------	-------

Installed	Build #	Description	Retool
	3	Modified 2024-01-17 17:03:21 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No



 Commit
 Retool
 Export
 Delete

Confirm that you wish to proceed with the commit action by selecting **Commit** again.

 **Commit Build**

Commit build?

- Once committed, this design cannot be changed without creating a new build.

 Commit
 Cancel

After confirming the commit, further changes to the build will be locked out. You can now install the build in the NETLAB+ database.

All parameters in the pod design can be changed during the initial (first) build. After you commit the initial build, certain settings (see below) cannot be changed unless you *retool* the pod design. Retooling will require you to reinstall any actual pods based on the design. The retooling procedure is explained in section [7.12](#).

Settings that can always be changed:	Settings that cannot be changed without retooling:
Images and Hotspots VLAN Pool Size (partial) Default VLAN Map Cable Guidance	Number of Access Server Ports Number of Switched Outlets Number of Consecutive Control Switch Ports Lab Devices Remote PCs

7.4 Installing a Build


Before a pod design can be used, it must be installed into the NETLAB+ database. If the current build is committed, an install button will appear on the build tab.


To install the current build, click on the install button located on the build tab.


Name	Build	Committed	Author ID	Global ID
Test123	3	Yes	TEST123	__6501_C07C


[General](#) [Image](#) [Control](#) [Device](#) [Remote PC](#) [Advanced](#) **Build**

Installed	Build #	Description	Retool
	3	Committed 2024-01-17 17:10:02 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No

 [+ New Build](#) [Export](#) [Delete](#)

 **Install Build**

 **Install this build?**

 [Cancel](#)

NETLAB+ will not install the current build if it is already installed.

- NETLAB+ will display a warning message if you are about to install a build that is older than the currently installed build.

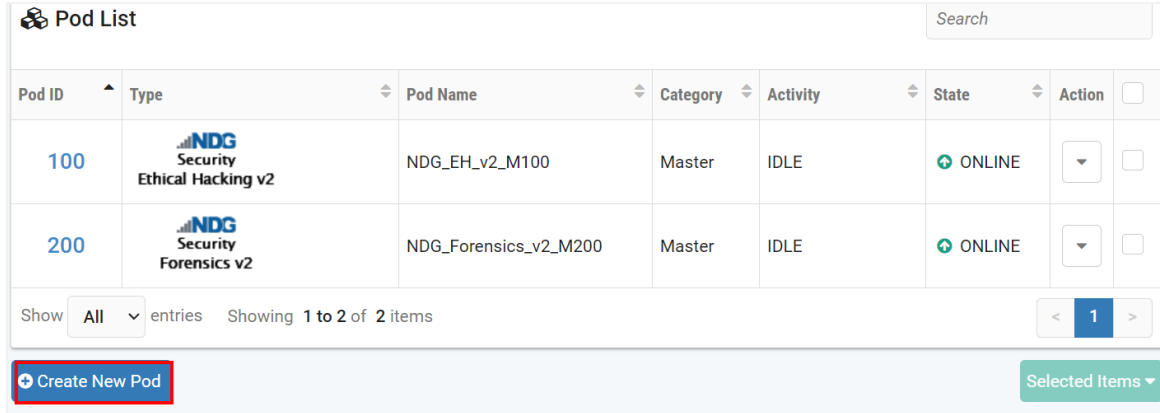
If the pod design requires an installation password, you will be required to enter the correct password at this time.

Once you have installed your pod design, it becomes an asset that your classes can use and rely upon. As always, it is important to keep a backup copy of the pod design. You will need the pod design file if you want to make changes. Please see section [7.2](#).



7.5 Adding Pods

Pods are added to the NETLAB+ system using the Pods administrator function.

1. Select the **Create New Pod** button.



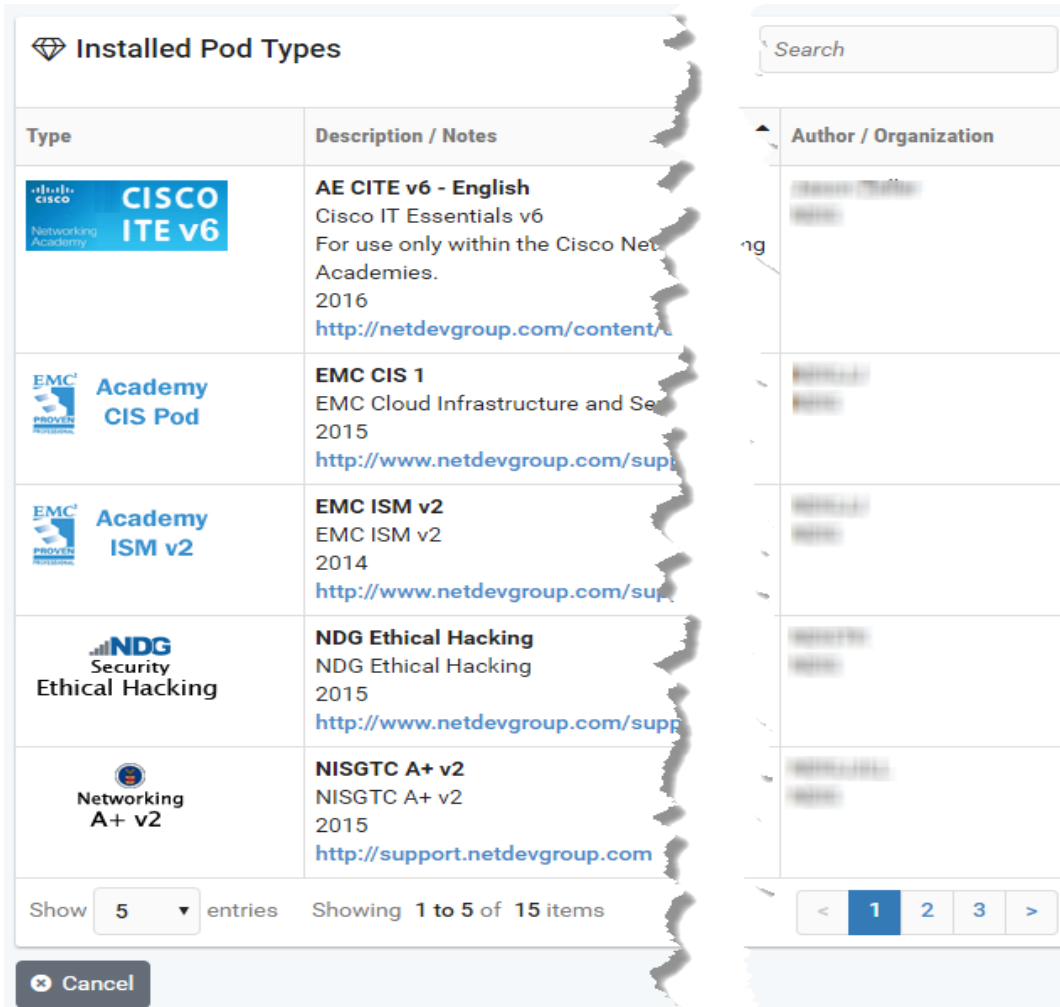
Pod List Search

Pod ID	Type	Pod Name	Category	Activity	State	Action
100	 NDG Security Ethical Hacking v2	NDG_EH_v2_M100	Master	IDLE	ONLINE	<input type="checkbox"/>
200	 NDG Security Forensics v2	NDG_Forensics_v2_M200	Master	IDLE	ONLINE	<input type="checkbox"/>











Show **All** entries Showing 1 to 2 of 2 items < 1 >

+ Create New Pod Selected Items

2. The list shows pod types provided by NDG, along with any installed custom pod designs among the selections. Select a pod type by clicking on any row.



Installed Pod Types Search

Type	Description / Notes	Author / Organization
 CISCO ITE v6	AE CITE v6 - English Cisco IT Essentials v6 For use only within the Cisco Net Academies. 2016 http://netdevgroup.com/content/...	 Cisco
 Academy CIS Pod	EMC CIS 1 EMC Cloud Infrastructure and Se 2015 http://www.netdevgroup.com/sup...	 EMC
 Academy ISM v2	EMC ISM v2 EMC ISM v2 2014 http://www.netdevgroup.com/sup...	 EMC
 NDG Ethical Hacking	NDG Ethical Hacking NDG Ethical Hacking 2015 http://www.netdevgroup.com/sup...	 NDG
 Networking A+ v2	NISGTC A+ v2 NISGTC A+ v2 2015 http://support.netdevgroup.com	 Networking

Show **5** entries Showing 1 to 5 of 15 items < 1 2 3 >

Cancel


3. After selecting the pod type, the New Pod Wizard will prompt for information on control device settings. Please refer to the *Adding New Pods* section of the *NETLAB+ Administrator Guide* for details on continuing this process.

7.6 Creating Lab Exercises for Pods

In order for a pod to be available for use by a class, the pod type must be referenced in at least one lab exercise from a lab design selected for the class. Therefore, it is often desirable to create a lab exercise that allows a class to reserve a particular type of pod. This exercise will typically have no lab activity and will use the settings shown here:

Reserve MAP Pod (no lab exercise specified)





Index	3
Global Lab ID	CCNARS51_0050_56BF_5E52_5A03_37B1_0006
Lab Name	Reserve MAP Pod (no lab exercise specified)
Pod Type	AE Multi-purpose Academy Pod
Time Limit	up to class maximum
Lab Document	none
Lab Image	none
Preset Configuration	none
Assessment Options	<ul style="list-style-type: none">• disable the action tab (AE/PE only)
VLAN Map	use default VLAN map for pod
Device Customizations	none

 Dismiss

At least one lab exercise must be created using Lab Designer in order to make the pod available to classes. Please refer to the *Relationship Between Classes, Lab Exercises, Reservations and Pods* section of the *NETLAB+ Lab Designer Guide*.

7.7 Exporting and Backing Up Pod Design Files

The export function downloads a copy of a pod design from the pod design folder on the NETLAB+ server to your local PC. You can use the export function to make a backup copy of your pod designs. Similarly, you can use the import function (see 0) to restore a pod design. Import and export can be used to share pod designs with other users and/or other NETLAB+ systems. However, only one instance of a pod design can be installed per system (see 7.4).

Name	Build	Committed	Author ID	Global ID	
Test123	3	Yes	TEST123	__6501_C07C	
<div><div>General</div><div>Image</div><div>Control</div><div>Device</div><div>Remote PC</div><div>Advanced</div><div>Build</div></div>					
Installed	Build #	Description			Retool
	3	Committed 2024-01-17 17:10:02 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5			No
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5			No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5			No
<div><div> Install</div><div> New Build</div><div> Export</div><div> Delete</div></div>					

7.8 Importing and Restoring Pod Design Files

The import function uploads a copy of a pod design on your local PC to the pod design folder on the NETLAB+ server. Import is the opposite of export. You can use the import function to restore a backup copy of your pod designs. Import and export can be used to share pod designs with other users and/or other NETLAB+ systems. However, only one instance of a pod design can be installed per system (see 7.4).


1. Select the **Import Design** button located at the bottom of the main Pod Designer page.

Name	Build	Commit	Author ID	GID	Author	Size	Modified
Test123	3	Yes	TEST123	...C07C		4K	2024-01-17

Showing 1 to 1 of 1 items

DismissCreate New Pod DesignShow Installed Pod DesignsImport Pod Design


Select the upload button to browse to the location of the file, which must end with the **NPD** extension. Select the **OK** button to upload the specified pod design.


 **Import Pod Design File**


To import a pod design, specify the path of an NPD file on your PC or workstation, or click the browse/choose button.

Path to Pod Design File (.npd)

VMVJJ_0025_9015_B226_5069_AB6E-00001.npd



 OK

 Cancel

7.9 Viewing a List of Installed Pod Designs

To see a list of the pod designs that are installed on your NETLAB+ system, select the **Show Installed Pod Designs** button located at the bottom of the main Pod Designer page.

1. The **Pod Design List** is displayed when the Pod Designer option is selected on the administrator interface.
2. To see the pod designs that have been installed in the local NETLAB+ pod type database on this system, click **Show Installed Pod Designs**.

Pod Designer Search								
Name	Build	Commit	Author ID	GID	Author	Size	Modified	
NISGTC Network+	12	Yes	DOLNETP	...15D6	NDGTH	124K	2014-02-10	
NISGTC Security+	9	Yes	DOLSECPV2	...5A23	NDGJJ	35K	2015-08-21	
RHSA7	3	Yes	RHSA7	...A22E	NDGJJ	37K	2016-01-13	
VMware VCA DCV 6	4	Yes	VMVCADC6	...F6DE	NDGJJ	32K	2016-01-15	
VMware vSphere ICM 6	4	Yes	VCPICM6F1	...78BE	NDGTK	72K	2016-01-14	
Dismiss Create New Pod Design Show Installed Pod Designs Import Pod Design								

3. The currently installed pod designs will be displayed. The **Used** column indicates the number of instantiated pods of each type. Click on a pod for additional details and management options. Select the **View** option on the Action dropdown to see additional details for any of the pods displayed.

Manage Installed Pod Designs Search						
Name	Build	Author/Org	Used	Icon/Type	Action	
NISGTC Network+	12	NDGTH NISGTC	4	n/a		
NISGTC Security+	9	NDGJJ NISGTC	3		View Uninstall	
RHSA7	3	NDGJJ NDG	0	n/a		
VMware VCA DCV 6	4	NDGJJ NDG	0	n/a		
VMware vSphere ICM 6	4	NDGTK NDG	0	n/a		
Dismiss						


7.10 Uninstalling a Pod Design From the NETLAB+ Database

The option to uninstall a pod is available only to the NETLAB+ administrator. Select the option to **Show Installed Pod Designs** (See section 7.9) and select the file name of the pod design to uninstall. The uninstall button will display if uninstalling is permitted for the pod design. The uninstall button is not displayed for NETLAB+ pods provided by NDG.



Caution: If a pod design has been installed on your system and used to add pods to your NETLAB+ system (using the Equipment Pods administrator function; see the *NETLAB+ Administrator Guide* for details), the pods must first be deleted from the system before uninstalling the pod design. This is necessary to prevent access conflicts to control resources.

The option to uninstall a pod is available only to the NETLAB+ administrator. Select the option to Show Installed Pod Designs (See section 7.9) and select the file name of the pod design to uninstall. The uninstall button will display if uninstalling is permitted for the pod design. The uninstall button is not displayed for NETLAB+ pods provided by NDG.

General	Image	Control	Device	Remote PC	Advanced	Build
Name		Test123				
Description		Created for documentation				
Author						
Organization						
Copyright						
Support URL		http://				
Note / Comment						
Modification Password		not required				
Installation Password		not required				
Cloning Permitted		No				
Cloning Password		not applicable				
						





7.11 Creating a New Build

The NPD file format has built-in version control. Each version is called a *build*. A new build must be created to make further changes to a pod design. All changes must be made to the NPD file. Once a build is committed, no further modifications may be made. In order to make additional changes to the pod design, a new build must be created.

Name	Build	Committed	Author ID	Global ID
Test123	3	Yes	TEST123	___6501_C07C


General	Image	Control	Device	Remote PC	Advanced	Build
---------	-------	---------	--------	-----------	----------	-------

Installed	Build #	Description	Retool
	3	Committed 2024-01-17 17:10:02 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5	No


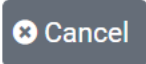
The **New Build** button will be available on the build tab only if the current build has been committed. Select the checkbox to **remove pod design files from previous builds** if you wish to have the previous builds for this pod design deleted from the pod design folder on the NETLAB+ server.

You may wish to keep your previous build should any circumstance cause you to decide not to proceed with the installation of the changes you plan to make to the pod design.

 **New Build**

Create new build?

☒ **remove pod design files from previous builds**

Select **OK** to proceed with the build.





7.12 Retooling a Build

All parameters in the pod design can be changed during the initial (first) build. After you commit the initial build, certain settings (see below) cannot be changed unless you retool the pod design. Retooling will require you to reinstall any actual pods based on the design.

Setting that can always be changed:	Settings that cannot be changed after the first build without retooling:
Images and Hotspots VLAN Pool Size (partial) Default VLAN Map Cable Guidance	Number of Access Server Ports Number of Switched Outlets Number of Consecutive Control Switch Ports Lab Devices Remote PCs


If the settings you must change to the pod design fall into the retooling category in the table above, proceed with the **Retool** option, available on the Build tab.

1. Select the **Retool Design** button to proceed.

General	Image	Control	Device	Remote PC	Advanced	Build	
Installed	Build #	Description					Retool
	4	Created 2024-01-17 18:43:40 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5					No
	3	Committed 2024-01-17 17:10:02 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5					No
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5					No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5					No
<div><div> Commit</div><div> Retool</div><div> Export</div><div> Delete</div></div>							

Keep in mind that it will be necessary to reinstall any pod based on the design. The extent of the modifications that may be performed using the Retool option allow modifications to the pod design which can significantly change it from the previous build. Reinstalling any pods using the design is necessary in order to prevent access conflicts to control resources.


2. Select the **Retool Design** button.

 **Retool Build**

Retooling permits unrestricted modification of the design, but will break compatibility with installed pods.

WARNING: to install a retooled build, you must delete and reinstall any pod based on this design.




Retool Design

 Cancel

After retooling, unrestricted modification of the pod design settings will be permitted.

7.13 Cloning a Build

Use the Clone feature to create derivative works based on a pod design. The cloning feature must be enabled in the general settings.



General	Image	Control	Device	Remote PC	Advanced	Build
Installed	Build #	Description				Retool
	4	Modified 2024-01-17 18:55:18 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5				Yes
	3	Committed 2024-01-17 17:10:02 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5				No
	2	Committed 2024-01-17 15:58:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5				No
	1	Committed 2024-01-16 21:53:58 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5				No
<div><div> Clone</div><div> Export</div><div> Delete</div></div>						

The Clone button does not appear if cloning permitted is not checked in the design.

If a Cloning password requirement has been set, the password must be entered in order to proceed.


Clone build

Clone build?

 Clone  Cancel


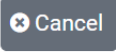
You will be required to enter a new Pod Design ID and modify the pod design name in order to create the clone.

A cloned pod design is a derivative work, not an exact copy. NETLAB+ automatically assigns a new globally unique ID number to the clone.

 **Delete Design**

Delete this design file?

This will only delete the design file. Any installation of this design or pod instances will not be deleted.


 

7.14 Deleting a Pod Design

To delete a pod design file from the folder, select the Delete button located on the build tab.

General	Image	Control	Device	Remote PC	Advanced	Build
Installed	Build #	Description				Retool
	1	Cloned 2024-01-17 19:12:59 UTC by administrator on NDG-VE-2ABB-CEA5-6322-F6D5				No
<div><div>Clone</div><div>Export</div><div>Delete</div></div>						

Please note that deleting the design file does not automatically delete the pod design from your NETLAB+ system database. To proceed with the deletion, select the **Delete File** button.

 **Delete Design**

Delete this design file?

This will only delete the design file. Any installation of this design or pod instances will not be deleted.

