



# ENCOR

## Lab Guide

350-401

Labs powered by





# ENCOR Lab Guide

350-401



25 Century Blvd., Ste. 500, Nashville, TN 37214 | [Boson.com](http://Boson.com)

To perform the labs referenced in this book, please download and install the necessary files (refer to your purchase receipt for the download link), navigate to the appropriate lab in the lab menu in the Boson NetSim, and load the lab; all labs should work in NetSim 11 or later. To learn more about the Boson NetSim or to purchase and download the software, please visit [www.boson.com/netsim](http://www.boson.com/netsim).

Copyright © 2020 Boson Software, LLC. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review. This book is designed to provide information about the Implementing Cisco Enterprise Network Core Technologies (ENCOR) exam. Every effort has been made to make this book as complete and as accurate as possible.

All rights reserved. Boson, Boson NetSim, Boson Network Simulator, and Boson Software are trademarks or registered trademarks of Boson Software, LLC. Catalyst, Cisco, and Cisco IOS are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. The Python Software Foundation is the organization behind Python. Media elements, including images and clip art, are the property of Microsoft. All other trademarks and/or registered trademarks are the property of their respective owners. Any use of a third-party trademark does not constitute a challenge to said mark. Any use of a product name or company name herein does not imply any sponsorship of, recommendation of, endorsement of, or affiliation with Boson, its licensors, licensees, partners, affiliates, and/or publishers.

<b>Boson NetSim Overview.....</b>	<b>1</b>
Using NetSim to Prepare for Your Certification .....	2
Using NetSim at Home – Single User.....	3
Downloading and Installing NetSim.....	3
Activating NetSim – Single User .....	3
Loading a Lab.....	3
<b>Module 4: Wired Infrastructure.....</b>	<b>5</b>
Lab 4.1 – Exploring Trunking .....	7
Lab Tasks .....	8
Lab Solutions.....	11
Lab 4.2 – Exploring VLANs .....	21
Lab Tasks .....	22
Lab Solutions.....	24
Lab 4.3 – Understanding VTP .....	33
Lab Tasks .....	35
Lab Solutions .....	38
Lab 4.4 – Understanding Layer 2 EtherChannel .....	57
Lab Tasks .....	58
Lab Solutions.....	60
Lab 4.5 – Understanding Layer 3 EtherChannel .....	70
Lab Tasks .....	72
Lab Solutions.....	75
Lab 4.6 – Exploring Rapid PVST+ .....	90
Lab Tasks .....	92
Lab Solutions.....	93
Lab 4.7 – Exploring MSTP .....	103
Lab Tasks .....	104
Lab Solutions.....	107
Lab 4.8 – Configuring NetSim .....	117
Lab Tasks .....	118
Lab Solutions.....	119
Lab 4.9 – Configuring OSPF .....	126
Lab Tasks .....	127
Lab Solutions.....	129
Lab 4.10 – Configuring EIGRP in Named Mode .....	140
Lab Tasks .....	141
Lab Solutions.....	144
Lab 4.11 – Configuring Single-Area OSPF .....	153
Lab Tasks .....	154
Lab Solutions.....	157
Lab 4.12 – Configuring Multi-Area OSPF .....	168

A couple sample labs are included in this document to display the quality, format, and content of labs that are included in the Boson NetSim and the Boson Courseware products. However, you will not be able to work through the labs in NetSim without purchasing both Boson NetSim and the Boson Courseware Lab Pack.

Please visit [www.boson.com](http://www.boson.com) for more information.

Lab Tasks .....	169
Lab Solutions.....	170
Lab 4.13 – Configuring OSPFv3 .....	178
Lab Tasks .....	179
Lab Solutions.....	181
Lab 4.14 – Configuring eBGP .....	192
Lab Tasks .....	194
Lab Solutions.....	196
<b>Module 5: Service</b> .....	<b>205</b>
Lab Tasks .....	207
Lab Solutions.....	209
Lab 6.2 – Exploring NTP .....	216
Lab Tasks .....	219
Lab Solutions .....	222
Lab 6.3 – Configuring NAT .....	232
Lab Tasks .....	234
Lab Solutions.....	235
Lab 6.4 – Understanding HSRP .....	240
Lab Tasks .....	242
Lab Solutions.....	245
Lab 6.5 – Configuring HSRP Load Sharing .....	258
Lab Tasks .....	260
Lab Solutions .....	263
<b>Module 7: Network Assurance</b> .....	<b>275</b>
Lab 7.1 – Troubleshooting a Network Topology .....	276
Lab Tasks .....	276
Lab Solutions.....	277
Lab 7.2 – Network Troubleshooting .....	286
Lab Tasks .....	288
Lab Solutions.....	288
Lab 7.3 – debug and traceroute Commands .....	297
Lab Tasks .....	299
Lab Solutions.....	300
Lab 7.4 – Network Troubleshooting with the OSI Model.....	304
Lab Tasks .....	306
Lab Solutions.....	308
Lab 7.5 – Configuring System Message Logging .....	318
Lab Tasks .....	319
Lab Solutions.....	319
Lab 7.6 – Basic Debugging .....	324

Lab Tasks .....	324
Lab Solutions.....	325
Lab 7.7 – Configuring SNMP .....	327
Lab Tasks .....	328
Lab Solutions.....	329
Lab 7.8 – Configuring NetFlow.....	332
Lab Tasks .....	333
Lab Solutions.....	334
Lab 7.9 – Configuring Flexible NetFlow.....	339
Lab Tasks .....	340
Lab Solutions.....	342
Lab 7.10 – Configuring Cisco Express Forwarding.....	348
Lab Tasks .....	348
Lab Solutions.....	350
<b>Module 8: Security .....</b>	<b>357</b>
Lab 8.1 – Configuring Passwords .....	358
Lab Tasks .....	359
Lab Solutions.....	360
Lab 8.2 – Router Remote Access via Telnet .....	365
Lab Tasks .....	366
Lab Solutions.....	367
Lab 8.3 – AAA Login Authentication and Exec Authorization .....	371
Lab Tasks .....	373
Lab Solutions.....	375
Lab 8.4 – Configuring SSH.....	382
Lab Tasks .....	383
Lab Solutions.....	385
Lab 8.5 – Troubleshooting Access Lists Part I .....	389
Lab Tasks .....	391
Lab Solutions.....	392
Lab 8.6 – Troubleshooting Access Lists Part II – Extended ACLs .....	396
Lab Tasks .....	397
Lab Solutions.....	399
Lab 8.7 – Troubleshooting Access Lists Part III – Standard ACLs .....	404
Lab Tasks .....	405
Lab Solutions.....	407
Lab 8.8 – Troubleshooting Access Lists Part IV – Named ACLs .....	411
Lab Tasks .....	412
Lab Solutions.....	414
Lab 8.9 – Troubleshooting Access Lists Part V – Named ACLs.....	420
Lab Tasks .....	421
Lab Solutions.....	424

A couple sample labs are included in this document to display the quality, format, and content of labs that are included in the Boson NetSim and the Boson Courseware products. However, you will not be able to work through the labs in NetSim without purchasing both Boson NetSim and the Boson Courseware Lab Pack.

Please visit [www.boson.com](http://www.boson.com) for more information.

Lab 8.10 – Exploring Control Plane Policing.....	430
Lab Tasks .....	432
Lab Solutions .....	434
<b>Module 9: Automation.....</b>	<b>441</b>
Lab 9.1 – Basic Python Scripting.....	442
Lab Tasks .....	443
Lab Solutions.....	447
Lab Solutions.....	447
Lab 9.2 – Python Dictionaries and JSON.....	461
Lab Tasks.....	463
Lab Solutions.....	466
Lab 9.3 – Exploring EEM Applets.....	477
Lab Tasks.....	478
Lab Solutions.....	480

A couple sample labs are included in this document to display the quality, format, and content of labs that are included in the Boson NetSim and the Boson Courseware products. However, you will not be able to work through the labs in NetSim without purchasing both Boson NetSim and the Boson Courseware Lab Pack.

Please visit [www.boson.com](http://www.boson.com) for more information.



## Boson NetSim Overview

The Boson NetSim® Network Simulator®, which includes the Boson Router Simulator®, is unique compared to all others on the market because of the functionality it supports and its features. NetSim utilizes Boson's proprietary Network Simulator, Router Simulator®, and ERROUTER® software technologies, along with the Boson Virtual Packet Technology® engine, to create individual packets. These packets are routed and switched through the simulated network, allowing NetSim to build an appropriate virtual routing table and simulate true networking. Other simulation products on the market do not support this level of functionality.

NetSim simulates a wide variety of Cisco® routers, including the 2500 series, 2600 series, 2800 series, and 3600 series routers, as well as the Cisco Catalyst 1900 series, 2900 series, and 3500 series switches. NetSim supports multiple routing protocols, including RIP, IGRP, EIGRP, BGP, and OSPF. It supports different LAN/WAN protocols, including PPP/CHAP, ISDN, and Frame Relay. The labs in NetSim require only the devices and functionality included with NetSim—they do not require access to any external router or switch hardware. NetSim supports many, but not all, of the IOS commands available on a physical router or switch. All of the commands referenced in the available labs are supported by NetSim. The labs included in this book have been selected as companions to the Boson Curriculum. However, for additional practice, you can perform any labs that are unlocked.

Achieving Cisco CCNA® or CCNP® Enterprise-level certification is the goal of many people who use this product. The Boson NetSim product covers many of the new Cisco certifications, including CCNA (200-301), ENCOR (350-401), and ENARSI (300-410). The included labs guide you through the configuration of routers, switches, and workstations in a variety of scenarios.

Activation keys unlock labs and increase the number of available commands. Beginning with the Demo version of NetSim, the command set is limited to those necessary to perform the steps in the lab. For example, if you start your studies with a CCNA activation key, you will have the command set and labs available that are necessary to study for that exam. When you are ready to study for a CCNP exam, you will need to purchase a new activation key and then activate with the new activation key; then, more labs and a larger command set become available.

Each activation key unlocks a selection of labs. A small lock icon (🔒) is displayed next to unavailable labs. Some lab packs are delivered by NetSim to support other products that are sold separately. If you have questions about locked labs, please contact [support@boson.com](mailto:support@boson.com).

After you load and complete an unlocked lab, you can use the grading function in NetSim to grade the lab so that you can determine whether you completed it correctly (click **Lab** > **Grade Lab**). As you progress through the labs, you can master the skills needed to pass the simulation questions in the Cisco certification exams. NetSim has the ability to guide and grade, and using it for practice can actually be more helpful than using real routers and switches. NetSim allows you to gain experience without requiring you to purchase expensive equipment.

You can use the Boson NetSim to work through labs, but you can also use it for additional purposes. For example, you can create your own logical topology to practice designing and planning a network. This tool's functionality goes beyond that of most tools because you can actually create the device configurations that are going to be used, save those configurations, and practice using them on simulated devices.

Routing protocol implementation is one of the more challenging tasks you might encounter. Troubleshooting a production network can be a frustrating experience. Fortunately, you can create a virtual copy of your network by creating a new topology in NetSim and troubleshoot the problems without interfering with your production network. Because NetSim is designed as a study tool for Cisco certification, you should not rely only on NetSim to make decisions about a production network, but you might find it useful in your troubleshooting efforts.

In summary, Boson NetSim is a flexible and powerful product that can help you become certified and, in some cases, can be used to create a simulation of the topology of your corporate network and help you practice troubleshooting without using devices on the production network.

### Using NetSim to Prepare for Your Certification

By using NetSim to help you achieve a Cisco certification, you can learn and master the skills necessary to help you successfully complete your certification track. The purpose of NetSim is to help you with the practical, hands-on portion of your education and to ensure that you not only understand the concepts of routing but can actually configure and implement routing on Cisco devices.

Mastering Cisco networking involves two fundamental tasks:

1. Learn the theory of routers and switches.
2. Gain the hands-on experience of implementing that theory by configuring the devices in a network and testing them in a lab.

Self-studying for a Cisco certification can be a daunting task. The amount of information a CCNA candidate is required to know and the skills that candidate is required to possess are quite extensive. To begin learning the theory of configuring a network, you can find a good reference book or listen to an instructor. (Boson Training, [www.boson.com/boson-training](http://www.boson.com/boson-training), offers a full slate of classes and Bootcamps.) But a reference book might not be enough. The book will not give you the practical, hands-on experience of routing and switching that you can learn from NetSim—experience that will help you build on the theoretical knowledge you learned from the reference book.

Real equipment gives you the ability to practice on actual routers and switches, but it also is a very costly way to practice and leaves a lot of room for error. The Boson NetSim, on the other hand, is an excellent tool to help you prepare for the CCNA-level ([www.boson.com/certification/CCNA](http://www.boson.com/certification/CCNA)) and CCNP-level ([www.boson.com/certification/CCNP](http://www.boson.com/certification/CCNP)) exams. NetSim simulates the behavior of a network and does not just return preprogrammed responses to expected command inputs. It allows you to create virtual packets and virtual frames that will be routed and switched through the simulated network. Aside from physically plugging in the cables and listening to the fan noise, your experience with the simulated network will be much the same as your experience with a fully functional lab rack without the expense of the hardware. NetSim will enable you to practice various configurations and master helpful skills.

Once you feel you have mastered both the theory ([www.boson.com/boson-training](http://www.boson.com/boson-training)) and the practical labs, ([www.boson.com/netsim-cisco-network-simulator](http://www.boson.com/netsim-cisco-network-simulator)) you can test your knowledge by using the Boson ExSim-Max practice exam products available at the ExSim-Max home page ([www.boson.com/exsim-max-practice-exams](http://www.boson.com/exsim-max-practice-exams)). Boson ExSim-Max products include complex multiple-choice questions, drag-and-drop questions, and Boson NetSimX simulation questions.

The Boson NetSim Network Simulator is the most comprehensive product on the market for learning how to configure a Cisco router. The Boson NetSim will not only help you become certified, it will help you learn and understand how to configure routers, switches, and networks.

For more information on how to use NetSim, please read the NetSim User Manual by clicking **Help > Users Manual** from within NetSim or by downloading the User Manual from the following link:

<http://www.boson.com/Files/Support/NetSim-13-User-Manual.pdf>

### Using NetSim at Home – Single User

The following steps are for installation and activation for a single user license and should not be performed on a classroom workstation.

#### Downloading and Installing NetSim

You can download NetSim from the Boson.com downloads page (account required):

<http://www.boson.com/download>

You must have a Boson account to download the NetSim Demo. To create a free account, visit the Boson Online Account page (<https://www.boson.com/account/default.aspx>) and enter a valid email address to begin creating an account.

You should download the NetSim installer to your computer before beginning the installation. It is recommended that you disable antivirus and firewall software while installing and activating NetSim and then reactivate when the installation is complete. Double-click the downloaded installation file to begin the installation, and perform the steps described in the prompts during installation.

#### Activating NetSim – Single User

When you first open NetSim, you will be presented with a NetSim Login dialog box. When prompted, enter the email address and password associated with your Boson.com account. If you have not previously created a Boson.com account, you will need to create one first on Boson.com. If you have any NetSim 13–related products, NetSim will automatically activate those items for you; otherwise, NetSim will launch in Demo mode. If you are using a proxy server to connect to the internet, you must configure the appropriate settings via the Settings icon and click the **Proxy Settings** button.

#### Loading a Lab

1. You can begin a preloaded Boson NetSim lab by performing one of the following tasks:
  - On the navigation pane, select the appropriate lab tree from the drop-down box; then, double-click the lab you want to open.
  - Click to highlight a lab on the **Labs** pane, then click **Lab > Load lab**.
  - Click to highlight a lab on the **Labs** pane, then click **Load Lab** on the **Lab Preview** pane.
  - Select a lab from the list of **Recent Labs** or **Saved Labs** on the **Home** pane.
2. After you have loaded a lab, click the **Lab Instructions** tab and read through the lab instructions.

3. From the **Devices** drop-down menu on the **Consoles** section, select the device(s) that you need to configure in order to complete the lab and follow the steps in the lab. You can also select the device you want to configure by clicking the **Lab Topology** tab, right-clicking the device, and clicking **Console**.
4. When you have completed the lab, click **Lab > Grade Lab** to ensure that you have completed it successfully.
5. You can choose to save your single device configuration or multiple device configurations by selecting the appropriate option in the **File** menu.

You might also be instructed to open labs from a custom lab pack. If any custom labs are available, you should select **Custom** from the drop-down box. To open a custom lab, double-click the lab you want to load.

# Module 4

---

**Lab 4.1** – Exploring Trunking

**Lab 4.2** – Exploring VLANs

**Lab 4.3** – Understanding VTP

**Lab 4.4** – Understanding Layer 2 EtherChannel

**Lab 4.5** – Understanding Layer 3 EtherChannel

**Lab 4.6** – Exploring Rapid PVST+

**Lab 4.7** – Exploring MSTP

Labs powered by



# Module 4

**Lab 4.8** – Configuring EIGRP

**Lab 4.9** – Configuring EIGRP for IPv6

**Lab 4.10** – Configuring EIGRP in Named Mode

**Lab 4.11** – Configuring Single-Area OSPF

**Lab 4.12** – Configuring Multi-Area OSPF

**Lab 4.13** – Configuring OSPFv3

**Lab 4.14** – Configuring eBGP

## Lab 4.1 – Exploring Trunking

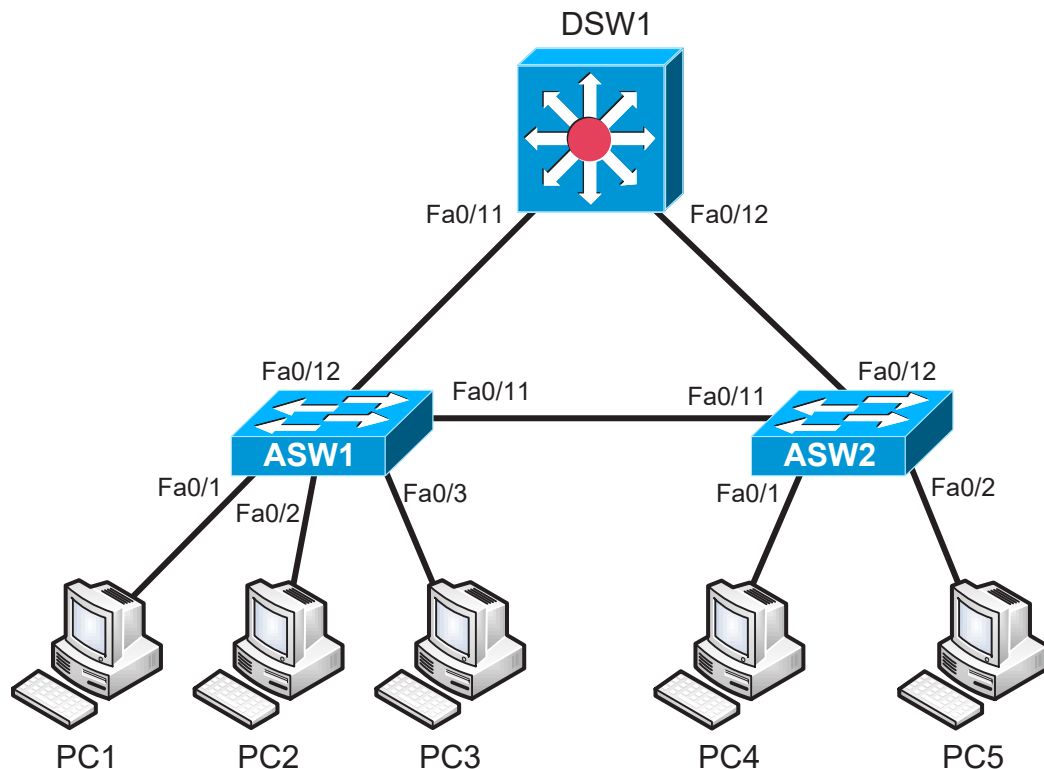
To perform this lab in Boson NetSim, please use the link in your purchase receipt to download and install NetSim and then use the key from your purchase receipt to activate the Courseware Lab Tree. After NetSim is activated, navigate to the appropriate lab in the CCNP Courseware Lab Tree and load the lab.

### Objective

This lab corresponds to Module 4: Wired Infrastructure of Boson’s ENCOR Curriculum. In this lab, you will explore the trunking capabilities of Cisco Catalyst 2900 and 3500 series switches. You will configure trunk links, modify Dynamic Trunking Protocol (DTP) behavior, and control virtual LAN (VLAN) access to trunk links.

### Lab Topology

The topology diagram below represents the NetMap in the Simulator.



### Command Summary

Command	Description
<b>configure terminal</b>	enters global configuration mode from privileged EXEC mode
<b>enable</b>	enters privileged EXEC mode
<b>end</b>	ends and exits configuration mode
<b>exit</b>	exits one level in the menu structure

Command	Description
<b>interface range fastethernet</b> <i>slot/starting-port - ending-port</i>	configures a range of interfaces
<b>interface</b> <i>type number</i>	changes from global configuration mode to interface configuration mode
<b>ping</b> <i>ip-address</i>	sends an Internet Control Message Protocol (ICMP) Echo Request to the specified address
<b>show interfaces</b> [ <i>interface-id</i> ] <b>switchport</b>	shows the switchport configuration
<b>show interfaces trunk</b>	displays port and module interface-trunk information
<b>show running-config</b>	displays the active configuration file
<b>switchport mode</b> { <b>access</b>   <b>dynamic</b>   <b>auto</b>   <b>desirable</b> }   <b>trunk</b> }	configures the VLAN membership mode of a port
<b>switchport nonegotiate</b>	disables DTP
<b>switchport trunk allowed vlan</b> <i>vlan-list</i>	sets the list of allowed VLANs
<b>switchport trunk encapsulation dot1q</b>	sets the trunk encapsulation format to 802.1Q

The IP addresses and subnet masks used in this lab are shown in the tables below:

## IP Addresses

Device	Interface	IP Address	Subnet Mask
ASW1	VLAN 1	1.1.1.2	255.255.0.0
ASW2	VLAN 1	1.1.1.3	255.255.0.0
DSW1	VLAN 1	1.1.1.1	255.255.0.0

Device	IP Address	Subnet Mask
PC1	1.1.1.4	255.255.0.0
PC2	1.1.10.1	255.255.0.0
PC3	1.1.11.1	255.255.0.0
PC4	1.1.10.2	255.255.0.0
PC5	1.1.11.2	255.255.0.0

## Lab Tasks

### Task 1: Examine the Topology

In this task, you will examine the current state of the topology and verify connectivity between various network devices.

- On DSW1, display information about active trunk links. What trunking mode is configured on each active trunk? \_\_\_\_\_
- Based on the trunking mode configured on DSW1's end of the link to ASW1, what are the possible trunking modes that could be configured on ASW1's end of the link to successfully create a trunk? \_\_\_\_\_




3. Based on the trunking mode configured on DSW1's end of the link to ASW2, what are the possible trunking modes that could be configured on ASW2's end of the link to successfully create a trunk? \_\_\_\_\_  
\_\_\_\_\_
4. On ASW1, display information about active trunk links. What trunking mode is configured on ASW1's end of the link to DSW1? \_\_\_\_\_
5. On ASW2, display information about active trunk links. What trunking mode is configured on ASW2's end of the link to DSW1? \_\_\_\_\_
6. On ASW1, display switchport information for the interface that connects to ASW2. What trunking mode is configured on this interface? Is this interface operating as a trunk? \_\_\_\_\_
7. Based on the trunking mode configured on ASW1's end of the link to ASW2, what are the possible trunking modes that could be configured on ASW2's end of the link to prevent the creation of a trunk? \_\_\_\_\_  
\_\_\_\_\_
8. On ASW2, display switchport information for the interface that connects to ASW1. What trunking mode is configured on this interface? Is this interface operating as a trunk? \_\_\_\_\_
9. From PC1, attempt to ping the VLAN 1 interface on ASW2 (1.1.1.3). Does the ping succeed? Why or why not? \_\_\_\_\_
10. From PC2, attempt to ping PC4 (1.1.10.2). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
11. From PC3, attempt to ping PC5 (1.1.11.2). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_

## Task 2: Modify the Trunking Configuration

In this task, you will configure the trunk interfaces on each switch in the topology. You will also disable DTP and explicitly permit VLANs on specific trunk links.

1. ASW1 and ASW2 are Catalyst 2900 series switches. What trunking encapsulation protocols are supported on this series of switches? Must you specify a trunking protocol before manually configuring a trunk? Is this different from the supported protocols and requirements on DSW1, which is a Catalyst 3500 series switch? \_\_\_\_\_  
\_\_\_\_\_
2. On ASW1 and ASW2, configure static trunking mode for the interfaces that connect to DSW1.
3. On ASW1 and ASW2, disable DTP for the interfaces that connect to DSW1.

4. On ASW1, verify that DTP negotiation is disabled for the interface that connects to DSW1 and that the interface is operating in trunk mode.
5. On ASW1, configure static trunking mode and disable DTP for the interface that connects to ASW2.
6. On ASW2, configure static trunking mode and disable DTP for the interface that connects to ASW1.
7. On ASW2, verify that DTP negotiation is disabled for the interface that connects to ASW1 and that the interface is operating in trunk mode.
8. On ASW1 and ASW2, configure the trunk link between ASW1 and ASW2 to permit traffic only from VLAN 11.
9. On ASW1 and ASW2, configure the trunk link to DSW1 to permit traffic only from VLANs 1 and 10.
10. On DSW1, configure the trunk links to ASW1 and ASW2 to permit traffic from VLANs 1 and 10.
11. On ASW1, display information about active trunk links. Verify that the correct VLANs are allowed on each trunk link.
12. On DSW1, display information about active trunk links. Verify that the correct VLANs are allowed on each trunk link.
13. From PC1, attempt to ping the VLAN 1 interface on ASW2 (1.1.1.3). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
14. From PC2, attempt to ping PC4 (1.1.10.2). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
15. From PC3, attempt to ping PC5 (1.1.11.2). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_

Once you have completed this lab, be sure to check your work by using the grading function. You can do so by clicking the Grade Lab icon () in the toolbar or by pressing Ctrl+G.

## Lab Solutions

### Task 1: Examine the Topology

1. You should issue the following command on DSW1 to display information about active trunk links:

```
DSW1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/11    on        802.1q         trunking    1
Fa0/12    on        802.1q         trunking    1
```

<output omitted>

Based on the output, you can determine that both of the active trunk links are configured to operate in static trunk mode. Cisco workgroup switches, such as the Catalyst 2900, 3500, and 3700 series switches, typically support three trunking modes: static trunk, dynamic desirable, and dynamic auto. In addition, Cisco switchports support a static access mode that places the interface into a nontrunking state. The text `on` in the `Mode` field indicates that a trunk link is operating in static trunk mode. If a trunk link were configured to operate in dynamic desirable mode, the `Mode` field would contain the text `desirable`. Likewise, if a trunk link were configured to operate in dynamic auto mode, the `Mode` field would contain the text `auto`.

2. Because DSW1's end of the link to ASW1 is configured to operate in static trunk mode, the interface will create a trunk if the other end of the link is configured to operate in either dynamic auto, dynamic desirable, or static trunk mode. When an interface is configured to operate in static trunk mode, it will always attempt to form a trunk link.
3. Because DSW1's end of the link to ASW2 is configured to operate in static trunk mode, the interface will create a trunk if the other end of the link is configured to operate in either dynamic auto, dynamic desirable, or static trunk mode.
4. On ASW1, you should issue the following command to display information about active trunk links:

```
ASW1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/12    auto     802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/12    1-4094

Port      Vlans allowed and active in management domain
Fa0/12    1,10,11

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/12    1,10,11
```

Based on the output, you can determine that the active trunk link to DSW1 is configured to operate in dynamic auto mode. The `Mode` field contains the text `auto` to indicate that an interface is configured to operate in dynamic auto trunking mode.

5. On ASW2, you should issue the following command to display information about active trunk links:

```
ASW2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/12    auto      802.1q          trunking    1

Port      Vlans allowed on trunk
Fa0/12    1-4094

Port      Vlans allowed and active in management domain
Fa0/12    1,10,11

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/12    1,10,11
```

6. You should issue the following command on ASW1 to display switchport information for the interface that connects to ASW2:

```
ASW1#show interfaces fastethernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative mode: dynamic auto
Operational mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<output omitted>
```

Based on the output, you can determine that the FastEthernet 0/11 interface is configured to operate in dynamic auto mode. However, the interface is not currently operating as a trunk. Instead, the interface is operating in static access mode. An interface can be in a different operational state from the one configured if the requirements for its configured state are not met. In this case, the interface is operating in static access mode because ASW2 has not negotiated to form a trunk link.

7. Because ASW1's end of the link to ASW2 is configured to operate in dynamic auto mode and a trunk link has not formed, you can surmise that ASW2's end of the link must be configured to operate in either static access or dynamic auto mode. An interface operating in dynamic auto mode will become a trunk port only if the other end of the link is explicitly configured as a trunk port or is set to dynamic desirable mode. The port will not actively negotiate to become a trunk port.
8. You should issue the following command on ASW2 to display switchport information for the interface that connects to ASW1:

```
ASW2#show interfaces fastethernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative mode: dynamic auto
Operational mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<output omitted>
```

The output confirms that ASW2's end of the link is not configured to operate in static trunk or dynamic desirable mode. Instead, the FastEthernet 0/11 interface on ASW2 is configured to operate in dynamic auto mode. Like the interface on ASW1's end of the link, the FastEthernet 0/11 interface will not actively negotiate to form a trunk link. Therefore, the FastEthernet 0/11 remains in static access mode and does not form a trunk.

9. From PC1, you should issue the following command to attempt to ping the VLAN 1 interface on ASW2 (1.1.1.3):

```
C:>ping 1.1.1.3
```

The ping should succeed because PC1 is in VLAN 1 and can reach the VLAN 1 interface on ASW2 through the trunk links on DSW1 or the direct link between ASW1 and ASW2. Note that although the direct link between ASW1 and ASW2 is not operating as a trunk link, traffic from PC1 could use it as a path to the VLAN 1 interface of ASW2. The FastEthernet 0/11 interfaces on ASW1 and ASW2 are operating in static access mode and are considered members of VLAN 1; therefore, traffic from PC1, which is also in VLAN 1, can pass directly from ASW1 to ASW2.

10. From PC2, you should issue the following command to attempt to ping PC4 (1.1.10.2):

```
C:>ping 1.1.10.2
```

The ping should succeed because PC2 and PC4 are both in VLAN 10 and PC2 can reach PC4 through the trunk links on DSW1. Note that even though the direct link between ASW1 and ASW2 is shorter and faster, it is not considered as a path between PC2 and PC4 because it is not currently operating as a trunk link. As a nontrunk link, the direct link between ASW1 and ASW2 is restricted to a single VLAN, VLAN 1, and cannot pass traffic from other VLANs.

11. From PC3, you should issue the following command to attempt to ping PC5 (1.1.11.2):

```
C:>ping 1.1.11.2
```

The ping should succeed because PC3 and PC5 are both in VLAN 11 and PC3 can reach PC5 through the trunk links on DSW1.

## Task 2: Modify the Trunking Configuration

1. ASW1 and ASW2 are Catalyst 2900 series switches. You can use contextual help to determine which types of trunking encapsulation are supported. For example, you could issue the following commands to determine which types of trunking encapsulation are supported on the FastEthernet 0/12 interface on ASW1:

```
ASW1(config)#interface fastethernet 0/12
ASW1(config-if)#switchport trunk encapsulation ?
dot1q      Interface uses only 802.1q trunking encapsulation when trunking
```

Because this switch platform supports only a single trunking encapsulation type, you are not required to specify a trunking protocol before manually configuring a trunk. However, on other platforms, such as the Catalyst 3500 series switch, you must specify a trunking encapsulation protocol before manually configuring a trunk. You can issue the following commands to determine which types of trunking encapsulation are supported on the FastEthernet 0/12 interface on DSW1:

```
DSW1(config)#interface fastethernet 0/12
DSW1(config-if)#switchport trunk encapsulation ?
dot1q      Interface uses only 802.1q trunking encapsulation when trunking
isl        Interface uses only ISL trunking encapsulation when trunking
```

The Catalyst 3500 series switch supports both Institute of Electrical and Electronics Engineers (IEEE) 802.1Q and Cisco Inter-Switch Link (ISL) encapsulation. Because the Catalyst 2900 series switch supports only IEEE 802.1Q encapsulation, a dynamically formed trunk will negotiate the correct encapsulation type for the link. However, when manually configuring a trunk, you must specify the trunking encapsulation.

2. On ASW1 and ASW2, you should issue the following commands to configure static trunking mode for the interfaces that connect to DSW1:

```
ASW1(config)#interface fastethernet 0/12
ASW1(config-if)#switchport mode trunk
```

```
ASW2(config)#interface fastethernet 0/12
ASW2(config-if)#switchport mode trunk
```

3. On ASW1 and ASW2, you should issue the following commands to disable DTP for the interfaces that connect to DSW1:

```
ASW1(config-if)#switchport nonegotiate
```

```
ASW2(config-if)#switchport nonegotiate
```

When DTP is disabled, an interface no longer originates or responds to DTP messages. Cisco recommends disabling DTP, particularly on Access layer switches where there it provides an additional threat surface for a malicious actor to exploit. Because DTP enables an interface to dynamically form a trunk link with another switch, an attacker could potentially convert an access port to a trunk port and then through that trunk access VLANs that would otherwise be inaccessible.

4. You should issue the following command on ASW1 to verify that DTP negotiation is disabled for the interface that connects to DSW1:

```
ASW1#show interface fastethernet 0/12 switchport
Name: Fa0/12
Switchport: Enabled
Administrative mode: trunk
Operational mode: trunk
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<output omitted>
```

The output verifies that DTP is no longer being used to negotiate trunk links. In addition, the output confirms that the FastEthernet 0/12 interface is operating in trunk mode.

5. On ASW1, you should issue the following commands to configure static trunking mode and disable DTP for the interface that connects to ASW2:

```
ASW1(config)#interface fastethernet 0/11
ASW1(config-if)#switchport mode trunk
ASW1(config-if)#switchport nonegotiate
```

6. On ASW2, you should issue the following commands to configure static trunking mode and disable DTP for the interface that connects to ASW1:

```
ASW2(config)#interface fastethernet 0/11
ASW2(config-if)#switchport mode trunk
ASW2(config-if)#switchport nonegotiate
```

7. On ASW2, you should issue the following command to verify that DTP negotiation is disabled for the interface that connects to ASW1:

```
ASW2#show interface fastethernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative mode: trunk
Operational mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<output omitted>
```

The output verifies that DTP is no longer being used to negotiate trunk links. In addition, the output confirms that the FastEthernet 0/11 interface is operating in trunk mode.

8. On ASW1 and ASW2, you should issue the following commands to configure the trunk link between ASW1 and ASW2 to permit traffic only from VLAN 11:

```
ASW1(config)#interface fastethernet 0/11
ASW1(config-if)#switchport trunk allowed vlan 11

ASW2(config)#interface fastethernet 0/11
ASW2(config-if)#switchport trunk allowed vlan 11
```

You can specify which VLANs are allowed to receive 802.1Q tagged traffic when trunking. You can specify a list of one or more comma-separated VLAN IDs for VLANs that are allowed to receive

tagged traffic. You can also specify a range of VLANs instead of a list by using a dash-separated beginning VLAN ID and end VLAN ID. By default, all VLANs are allowed to send and receive tagged traffic when trunking.

9. On ASW1 and ASW2, you should issue the following commands to configure the trunk link to DSW1 to permit traffic only from VLANs 1 and 10:

```
ASW1(config)#interface fastethernet 0/12
ASW1(config-if)#switchport trunk allowed vlan 1,10
```

```
ASW2(config)#interface fastethernet 0/12
ASW2(config-if)#switchport trunk allowed vlan 1,10
```

When pruning VLANs from trunk links, you should be careful to not exclude the default VLAN. Some vital traffic, such as Spanning Tree Protocol (STP) messages for the Common Spanning Tree (CST) are sent untagged on the default VLAN. Pruning the default VLAN from trunk links can cause unexpected behavior and potential Layer 2 loops.

10. On DSW1, configure the trunk links to ASW1 and ASW2 to permit traffic from VLANs 1 and 10:

```
DSW1(config)#interface range fastethernet 0/11 - 12
DSW1(config-if-range)#switchport trunk allowed vlan 1,10
```

11. On ASW1, you should issue the following command to verify that the correct VLANs are allowed on each trunk link:

```
ASW1#show interfaces trunk
Port          Mode          Encapsulation  Status        Native vlan
Fa0/11        on            802.1q         trunking      1
Fa0/12        on            802.1q         trunking      1
```

Port	Vlans allowed on trunk
Fa0/11	11
Fa0/12	1,10

```
Port          Vlans allowed and active in management domain
Fa0/11        11
Fa0/12        10
```

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/11	11
Fa0/12	10

Based on the output, you can determine that VLAN 11 is the only VLAN allowed on the link to ASW2 and that VLANs 1 and 10 are the only VLANs allowed on the link to DSW1.



12. On DSW1, you should issue the following command to verify that the correct VLANs are allowed on each trunk link.

```
DSW1#show interfaces trunk
Port          Mode          Encapsulation  Status      Native vlan
Fa0/11        on            802.1q         trunking    1
Fa0/12        on            802.1q         trunking    1

Port          Vlans allowed on trunk
Fa0/11        1,10
Fa0/12        1,10

Port          Vlans allowed and active in management domain
Fa0/11        10
Fa0/12        10

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/11        10
Fa0/12        10
```

13. From PC1, you should issue the following command to attempt to ping the VLAN 1 interface on ASW2 (1.1.1.3):

```
C:>ping 1.1.1.3
```

The ping should succeed because PC1 is in VLAN 1 and can still reach the VLAN 1 interface on ASW2 through the trunk links on DSW1.

14. From PC2, you should issue the following command to attempt to ping PC4 (1.1.10.2):

```
C:>ping 1.1.10.2
```

The ping should succeed because PC2 and PC4 are both in VLAN 10 and PC2 can reach PC4 through the trunk links on DSW1. If the link between ASW1 and DSW1 was shut down, PC2 would no longer be able to reach PC4 because the only remaining link to ASW2 is restricted to traffic from VLAN 11.

15. From PC3, you should issue the following command to attempt to ping PC5 (1.1.11.2):

```
C:>ping 1.1.11.2
```

The ping should succeed because PC3 and PC5 are both in VLAN 11 and PC3 can reach PC5 through the trunk link between ASW1 and ASW2. If the link between ASW1 and ASW2 were shut down, PC3 would no longer be able to reach PC5 because the only remaining link to ASW2 is restricted to traffic from VLANs 1 and 10.

## Sample Configuration Scripts

DSW1	DSW1 (continued)
<pre> DSW1#show running-config Building configuration... Current configuration : 1248 bytes ! Version 15.b service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname DSW1 ! ip subnet-zero ! ip cef no ip domain-lookup spanning-tree mode pvst spanning-tree vlan 1,10 priority 24576 spanning-tree vlan 11 priority 28672 spanning-tree extend system-id ! interface FastEthernet0/1 ! interface FastEthernet0/2 ! interface FastEthernet0/3 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 ! interface FastEthernet0/8 ! </pre>	<pre> interface FastEthernet0/9 ! interface FastEthernet0/10 ! interface FastEthernet0/11 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,10 ! interface FastEthernet0/12 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk allowed vlan 1,10 ! interface GigabitEthernet0/1 ! interface GigabitEthernet0/2 ! interface Vlan 1 ip address 1.1.1.1 255.255.0.0 no ip route-cache ! vlan 10 name VLAN0010 vlan 11 name VLAN0011 ! ip classless no ip http server ! line con 0 line aux 0 line vty 0 4 login ! no scheduler allocate end </pre>

ASW1	ASW1 (continued)
<pre> ASW1#show running-config Building configuration... Current configuration : 1219 bytes ! Version 15.b service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname ASW1 ! ip subnet-zero ! ip cef no ip domain-lookup spanning-tree mode pvst spanning-tree vlan 11 priority 24576 spanning-tree extend system-id ! interface FastEthernet0/1 ! interface FastEthernet0/2   switchport mode access   switchport access vlan 10 ! interface FastEthernet0/3   switchport mode access   switchport access vlan 11 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 ! </pre>	<pre> interface FastEthernet0/8 ! interface FastEthernet0/9 ! interface FastEthernet0/10 ! interface FastEthernet0/11   switchport mode trunk   switchport trunk allowed vlan 11   switchport nonegotiate ! interface FastEthernet0/12   switchport mode trunk   switchport trunk allowed vlan 1,10   switchport nonegotiate ! interface Vlan 1   ip address 1.1.1.2 255.255.0.0   no ip route-cache ! vlan 10 name VLAN0010 vlan 11 name VLAN0011 ! ip classless no ip http server ! line con 0 line aux 0 line vty 0 15   login ! no scheduler allocate end </pre>

ASW2	ASW2 (continued)
<pre> ASW2#show running-config Building configuration... Current configuration : 1181 bytes ! Version 15.b service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname ASW2 ! ip subnet-zero ! ip cef no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id ! interface FastEthernet0/1  switchport mode access  switchport access vlan 10 ! interface FastEthernet0/2  switchport mode access  switchport access vlan 11 ! interface FastEthernet0/3 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 ! </pre>	<pre> interface FastEthernet0/8 ! interface FastEthernet0/9 ! interface FastEthernet0/10 ! interface FastEthernet0/11  switchport mode trunk  switchport trunk allowed vlan 11  switchport nonegotiate ! interface FastEthernet0/12  switchport mode trunk  switchport trunk allowed vlan 1,10  switchport nonegotiate ! interface Vlan 1  ip address 1.1.1.3 255.255.0.0  no ip route-cache ! vlan 10 name VLAN0010 vlan 11 name VLAN0011 ! ip classless no ip http server ! line con 0 line aux 0 line vty 0 15  login ! no scheduler allocate end </pre>

## Lab 4.2 – Exploring VLANs

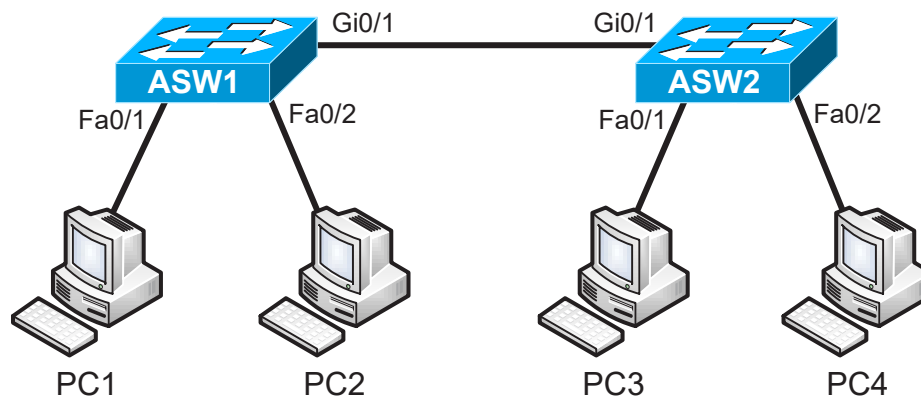
To perform this lab in Boson NetSim, please use the link in your purchase receipt to download and install NetSim and then use the key from your purchase receipt to activate the Courseware Lab Tree. After NetSim is activated, navigate to the appropriate lab in the CCNP Courseware Lab Tree and load the lab.

### Objective

This lab corresponds to Module 4: Wired Infrastructure of Boson’s ENCOR Curriculum. In this lab, you will be introduced to the basic operation of virtual LANs (VLANs). You will create new VLANs, modify their configuration, and explore connectivity both within a VLAN and between VLANs on a single switch and across multiple switches.

### Lab Topology

The topology diagram below represents the NetMap in the Simulator.



### Command Summary

Command	Description
<b>configure terminal</b>	enters global configuration mode from privileged EXEC mode
<b>enable</b>	enters privileged EXEC mode
<b>end</b>	ends and exits configuration mode
<b>exit</b>	exits one level in the menu structure
<b>interface</b> <i>type number</i>	changes from global configuration mode to interface configuration mode
<b>name</b> <i>vlan-name</i>	names a VLAN
<b>ping</b> <i>ip-address</i>	sends an Internet Control Message Protocol (ICMP) Echo Request to the specified address
<b>show interfaces status</b>	displays the line status of all interfaces
<b>show interfaces trunk</b>	displays port and module interface-trunk information
<b>show interfaces</b> [ <i>type number</i> ] <b>switchport</b>	shows the switchport configuration
<b>show running-config</b>	displays the active configuration file

Command	Description
<b>show vlan brief</b>	displays parameters for all VLANs; contains the VLAN's name, status, and ports assigned to it
<b>switchport access vlan <i>vlan-id</i></b>	assigns the default VLAN for a port
<b>switchport mode {access   dynamic {auto   desirable}   trunk}</b>	configures the VLAN membership mode of a port
<b>switchport trunk encapsulation dot1q</b>	sets the trunk encapsulation format to 802.1Q
<b>vlan <i>vlan-id</i></b>	creates a VLAN

The IP addresses and subnet masks used in this lab are shown in the following tables:

## IP Addresses

Device	Interface	IP Address	Subnet Mask
ASW1	VLAN 1	1.1.1.5	255.255.255.0
ASW2	VLAN 1	1.1.1.6	255.255.255.0

Device	IP Address	Subnet Mask	Default Gateway
PC1	1.1.1.10	255.255.255.0	1.1.1.5
PC2	1.1.1.11	255.255.255.0	1.1.1.5
PC3	1.1.1.12	255.255.255.0	1.1.1.5
PC4	1.1.1.13	255.255.255.0	1.1.1.5

## Lab Tasks

### Task 1: Examine the Topology


In this task, you will examine the VLAN and trunking configuration on ASW1 and ASW2. In addition, you will test connectivity between the workstations attached to the same switch and between workstations connected to different switches.

- Examine the VLAN configuration on each switch. How many manually configured VLANs are on each switch? \_\_\_\_\_
- Examine the status of the interfaces on each switch. To which VLAN is each active interface assigned? \_\_\_\_\_
- From PC1, attempt to ping PC2 (1.1.1.11). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
- Examine the trunk configuration on each switch. What kind of link connects ASW1 to ASW2? \_\_\_\_\_
- From PC1, attempt to ping PC3 (1.1.1.12). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_

## Task 2: Explore Basic VLAN Characteristics

In this task, you will create VLANs and examine their impact on inter-device communication on the same switch and across multiple switches.

1. On ASW1, create a VLAN named **VLAN 10** with a name of **SALES**.
2. On ASW1, assign the interface to which PC2 is connected (FastEthernet 0/2) to **VLAN 10**.
3. On ASW1, examine the switchport configuration for the FastEthernet 0/2 interface. Verify that the FastEthernet 0/2 interface is operating in access mode.
4. Examine the VLAN configuration on ASW1. How many interfaces are shown to reside in VLAN 10?  
\_\_\_\_\_
5. From PC1, attempt to ping PC2 (1.1.1.11). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
6. On ASW2, assign the interface to which PC3 is connected (FastEthernet 0/1) to **VLAN 10**.
7. On ASW2, assign **VLAN 10** the name **SALES**.
8. From PC2, attempt to ping PC3 (1.1.1.12). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
9. Configure the link between ASW1 and ASW2 as a trunk interface that uses 802.1Q encapsulation.
10. On ASW1, examine the switchport configuration for the GigabitEthernet 0/1 interface. Verify that the GigabitEthernet 0/1 interface is operating in trunk mode.
11. Examine the VLAN configuration on ASW1. Is the trunk interface listed as a member of any VLAN?  
\_\_\_\_\_
12. Examine the trunk configuration on ASW1. What is the native VLAN for the link that connects ASW1 to ASW2? \_\_\_\_\_
13. From PC2, attempt to ping PC3 (1.1.1.12). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_
14. From PC1, attempt to ping PC4 (1.1.1.13). Does the ping succeed? Why or why not? \_\_\_\_\_  
\_\_\_\_\_

Once you have completed this lab, be sure to check your work by using the grading function. You can do so by clicking the Grade Lab icon () in the toolbar or by pressing Ctrl+G.

## Lab Solutions

### Task 1: Examine the Topology

- On ASW1 and ASW2, you should issue the following command to examine the VLAN configuration. Sample output from ASW1 is shown below:

```
ASW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Gi0/1, Gi0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Based on the output, you can determine that there are no manually configured VLANs on each switch. VLAN 1, which is referred to as the default VLAN, is automatically created on the switch. In addition, VLANs 1002 – 1005 are special, reserved VLANs that are automatically created and cannot be removed.

- On ASW1 and ASW2, you should issue the following command to examine the status of the interfaces. Sample output from ASW1 is shown below:

```
ASW1#show interfaces status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		connected	1	a-full	a-100	10/100BaseTX
Fa0/2		connected	1	a-full	a-100	10/100BaseTX
Fa0/3		disabled	1	auto	auto	10/100BaseTX
Fa0/4		notconnect	1	auto	auto	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9		notconnect	1	auto	auto	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX
Fa0/11		notconnect	1	auto	auto	10/100BaseTX
Fa0/12		notconnect	1	auto	auto	10/100BaseTX
Gi0/1		connected	1	a-full	a-100	10/100BaseTX
Gi0/2		notconnect	1	auto	auto	10/100BaseTX

Based on the output, you can determine that there are three active interfaces and they are all members of VLAN 1. An active interface is an interface that is not in a shutdown state and that is connected to a network device, such as a host or another switch. An active interface has a status of `connected`, whereas an interface that is shut down has a status of `disabled`. An interface that is not shut down but that has no network device attached has a status of `notconnect`.



3. On PC1, you should issue the following command to attempt to ping PC2 (1.1.1.11):

```
C:>ping 1.1.1.11
```

The ping should succeed because PC1 and PC2 are both on the same switch, within the same VLAN, and connected to active interfaces.

4. On ASW1 and ASW2, you should issue the **show interfaces trunk** command to examine the trunk configuration:

```
ASW1#show interfaces trunk
ASW1#
```

Based on the output, you can determine that there are no active trunk links on either switch. Therefore, ASW1 and ASW2 are connected by an access link.

5. On PC1, you should issue the following command to attempt to ping PC3 (1.1.1.12):

```
C:>ping 1.1.1.12
```

The ping should succeed because PC1 and PC3 are within the same VLAN and are connected to active interfaces on switches that are connected with an access link residing in the same VLAN as the hosts. Because all of the active interfaces in the topology are members of the same VLAN, they may freely send traffic between them.

## Task 2: Explore Basic VLAN Characteristics

1. On ASW1, you should issue the following commands to create a VLAN named **VLAN 10** with a name of **SALES**:

```
ASW1(config)#vlan 10
ASW1(config-vlan)#name SALES
ASW1(config-vlan)#exit
```

If no name is specified, a VLAN is assigned a default name that is composed of the text **VLAN** and the VLAN ID expresses as a four-digit integer with leading zeroes. For example, creating VLAN 10 without assigning it a name would result in VLAN 10 automatically being assigned the name VLAN0010. From VLAN configuration mode, a VLAN is not created until the mode is exited.

2. On ASW1, you should issue the following commands to assign the interface to which PC2 is connected (FastEthernet 0/2) to **VLAN 10**:

```
ASW1(config)#interface fastethernet 0/2
ASW1(config-if)#switchport mode access
ASW1(config-if)#switchport access vlan 10
```

A switch interface can operate in one of two general, Layer 2 modes: Access mode or Trunking mode. When in access mode, an interface can be assigned to a primary VLAN. Any frames arriving on that interface will be tagged with the VLAN ID to identify the originating VLAN as the frame is processed and traverses the switch backplane.

3. On ASW1, you can issue the following command to verify that the FastEthernet 0/2 interface is operating in access mode that it is a member of the correct VLAN:

```
ASW1#show interfaces fastethernet 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative mode: static access
Operational mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 10 (SALES)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false

Appliance trust: none
```

Based on the output, you can determine that the interface is operating in `static access` mode and it has been assigned to the `SALES` VLAN (VLAN 10). Because an interface can be configured to dynamically negotiate its Layer 2 mode, the output specifies the administrative mode and the operational mode. The administrative mode is the Layer 2 mode that was configured for the interface while the operational mode is the Layer 2 mode that is in use. In this case, the interface is manually configured to operate in access mode; therefore, its administrative mode and operational modes are identical and listed as `static access`.

4. On ASW1, you should issue the following command to examine the VLAN configuration:

```
ASW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Gi0/1 Gi0/2
10	SALES	active	Fa0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Based on the output, you can determine that only the FastEthernet 0/2 interface is listed as a member of VLAN 10.

5. On PC1, you should issue the following command to attempt to ping PC2 (1.1.1.11):

```
C:>ping 1.1.1.11
```

The ping should fail because PC1 and PC2 no longer reside in the same VLAN. A switch treats each VLAN as its own distinct broadcast domain. Layer 2 traffic from one VLAN, such as Address Resolution Protocol (ARP) requests, are not forwarded to other VLANs.

6. On ASW2, you should issue the following commands to assign the interface to which PC3 is connected (FastEthernet 0/1) to **VLAN 10**:

```
ASW2(config)#interface fastethernet 0/1
ASW2(config-if)#switchport mode access
ASW2(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
```

Note that by default, if a VLAN has not already been created on a switch, the VLAN will automatically be created when an interface is assigned to the VLAN. Because VLAN 10 did not already exist on ASW2, the switch automatically created the VLAN the moment the FastEthernet 0/1 interface was assigned to it.

7. On ASW2, you should issue the following commands to assign **VLAN 10** the name **SALES**:

```
ASW2(config)#vlan 10
ASW2(config-vlan)#name SALES
ASW2(config-vlan)#exit
```

Because VLAN 10 was created automatically on ASW2, it was given the default name of VLAN0010. VLAN parameters, such as the VLAN name, can be changed after the VLAN is created by entering VLAN configuration mode.

8. On PC2, you should issue the following command to attempt to ping PC3 (1.1.1.12):

```
C:>ping 1.1.1.12
```

The ping should fail. Although PC2 and PC3 are both configured to reside in the same VLAN, they reside on separate switches. By default, VLAN information is not conveyed between switches unless they are interconnected with a trunk link. The link between ASW1 and ASW2 is currently configured to operate in access mode and to reside in the default VLAN, which is VLAN 1. When ASW1 receives the initial ARP frame from PC2, the switch will broadcast the frame out any other interfaces that reside in PC2's VLAN. However, none of the other ports on ASW2 are configured as members of VLAN 10. Therefore, PC2 is effectively isolated.

9. You should issue the following commands to configure the link between ASW1 and ASW2 as a trunk interface that uses 802.1Q encapsulation:

```
ASW1(config)#interface gigabitethernet 0/1
ASW1(config-if)#switchport trunk encapsulation dot1q
ASW1(config-if)#switchport mode trunk

ASW2(config)#interface gigabitethernet 0/1
ASW2(config-if)#switchport trunk encapsulation dot1q
ASW2(config-if)#switchport mode trunk
```

On a Cisco switch, an interface can be configured to dynamically negotiate a trunking encapsulation or one can be statically configured. In this scenario, you should manually configure the trunking encapsulation as Institute of Electrical and Electronics Engineers (IEEE) 802.1Q encapsulation. In addition, an interface can be configured to dynamically negotiate a trunk link. However, in this scenario you should manually configure the interface to operate as a trunk.

10. On ASW1, you should issue the following command to examine the switchport configuration for the GigabitEthernet 0/1 interface.

```
ASW1#show interfaces gigabitethernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative mode: trunk
Operational mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false

Appliance trust: none
```

Based on the command output, you can determine that the GigabitEthernet 0/1 interface is operating in trunk mode.

11. You should issue the following command to examine the VLAN configuration on ASW1:

```
ASW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Gi0/2
10	SALES	active	Fa0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Based on the output, you can determine that the trunk interface (Gi0/1) is not listed as a member of any VLAN. Trunk interfaces do not reside within any single VLAN; therefore, active trunk interfaces do not appear in the VLAN configuration.

12. You should issue the following command to examine the trunk configuration on ASW1:

```
ASW1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gi0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Gi0/1	1-4094

Port	Vlans allowed and active in management domain
Gi0/1	1,10

Port	Vlans in spanning tree forwarding state and not pruned
Gi0/1	1,10

Based on the output, VLAN 1 is the native VLAN for the link that connects ASW1 to ASW2. Traffic across a trunk link is typically tagged; however, traffic from the native VLAN is transmitted on the link without a tag. The native VLAN configured on each end of a trunk link should match; otherwise, traffic will not pass from one VLAN to another correctly. Cisco switches will issue a warning message on the console if a native VLAN mismatch is detected on a trunk link.

13. On PC2, you should issue the following command to attempt to ping PC3 (1.1.1.12):

```
C:>ping 1.1.1.12
```

The ping should succeed. Because the link between ASW1 and ASW2 is now configured to operate in trunk mode, traffic from VLAN 10 is tagged and sent across the link. For example, when ASW1 receives the initial ARP frame from PC2, the switch will broadcast the frame out any other interfaces that reside in PC2's VLAN. Trunk links are considered to reside in all VLANs that are permitted on the link. Therefore, ASW1 tags the ARP frame and forwards it to ASW2. When ASW2 received the frame, it will identify the ARP frame as belonging to VLAN 10 and will forward the frame to all interfaces that reside in that VLAN. Because PC3 is a member of VLAN 10, it will receive the frame and will be able to continue the process of communication until eventually ping messages are exchanged between PC2 and PC3.

14. On PC1, you should issue the following command to attempt to ping PC4 (1.1.1.13):

```
C:>ping 1.1.1.13
```

The ping should succeed. Because the link between ASW1 and ASW2 is now configured to operate in trunk mode, traffic from VLAN 1 is sent untagged across the link. For example, when ASW1 receives the initial ARP frame from PC1, the switch will broadcast the frame out any other interfaces that reside in PC1's VLAN, which is the default VLAN. Trunk links are considered to reside in all VLANs that are permitted on the link, including the default VLAN. Therefore, ASW1 forwards the ARP frame to ASW2. When ASW2 received the frame, it will identify the ARP frame as being untagged and thus belonging to its default VLAN. ASW2 will forward the frame to all interfaces in VLAN 1 and because PC4 is attached to an interface in the default VLAN, it will receive the frame and will be able to continue the process of communication until eventually ping messages are exchanged between PC1 and PC4.

## Sample Configuration Scripts

ASW1	ASW1 (continued)
<pre> ASW1#show running-config Building configuration... Current configuration : 1098 bytes ! Version 15.b service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname ASW1 ! ip subnet-zero ! ip cef no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id ! interface FastEthernet0/1 ! interface FastEthernet0/2   switchport mode access   switchport access vlan 10 ! interface FastEthernet0/3   shutdown ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 !           </pre>	<pre> interface FastEthernet0/8 ! interface FastEthernet0/9 ! interface FastEthernet0/10 ! interface FastEthernet0/11 ! interface FastEthernet0/12 ! interface GigabitEthernet0/1   switchport trunk encapsulation dot1q   switchport mode trunk   switchport nonegotiate ! interface GigabitEthernet0/2 ! interface Vlan 1   ip address 1.1.1.5 255.255.255.0   no ip route-cache ! vlan 10 name SALES ! ip classless no ip http server ! line con 0 line aux 0 line vty 0 4   login ! no scheduler allocate end           </pre>

ASW2	ASW2 (continued)
<pre> ASW2#show running-config Building configuration... Current configuration : 1087 bytes ! Version 15.b service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname ASW2 ! ip subnet-zero ! ip cef no ip domain-lookup spanning-tree mode pvst spanning-tree extend system-id ! interface FastEthernet0/1   switchport mode access   switchport access vlan 10 ! interface FastEthernet0/2 ! interface FastEthernet0/3 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 ! </pre>	<pre> interface FastEthernet0/8 ! interface FastEthernet0/9 ! interface FastEthernet0/10 ! interface FastEthernet0/11 ! interface FastEthernet0/12 ! interface GigabitEthernet0/1   switchport trunk encapsulation dot1q   switchport mode trunk   switchport nonegotiate ! interface GigabitEthernet0/2 ! interface Vlan 1   ip address 1.1.1.6 255.255.255.0   no ip route-cache ! vlan 10 name SALES ! ip classless no ip http server ! line con 0 line aux 0 line vty 0 4   login ! no scheduler allocate end </pre>



## **Certification Candidates**

Boson Software's ExSim-Max practice exams are designed to simulate the complete exam experience. These practice exams have been written by in-house authors who have over 30 years combined experience writing practice exams. ExSim-Max is designed to simulate the live exam, including topics covered, question types, question difficulty, and time allowed, so you know what to expect. To learn more about ExSim-Max practice exams, please visit [www.boson.com/exsim-max-practice-exams](http://www.boson.com/exsim-max-practice-exams) or contact Boson Software.

## **Organizational and Volume Customers**

Boson Software's outstanding IT training tools serve the skill development needs of organizations such as colleges, technical training educators, corporations, and governmental agencies. If your organization would like to inquire about volume opportunities and discounts, please contact Boson Software at [orgsales@boson.com](mailto:orgsales@boson.com).

## **Contact Information**

E-Mail: support@boson.com  
Phone: 877-333-EXAM (3926)  
615-889-0121  
Fax: 615-889-0122  
Address: 25 Century Blvd., Ste. 500  
Nashville, TN 37214





B o s o n . c o m

8 7 7 . 3 3 3 . 3 9 2 6      s u p p o r t @ b o s o n . c o m

© Copyright 2020 Boson Software, LLC. All rights reserved.