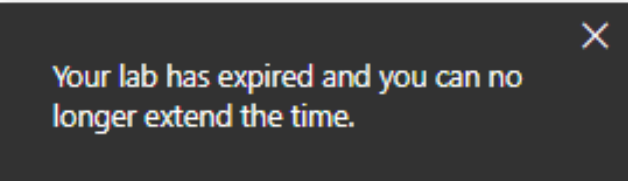


Lab Objectives-Network+ N10-008

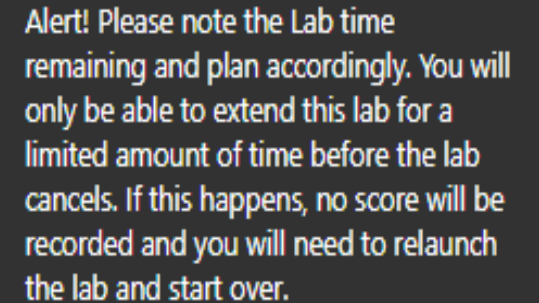
You have access to the lab environment for 6 months past the last day of class. If you End an individual lab once you complete it, you get a little checkmark in the labs list. Labs also have a Save option which allows you to save the lab state for up to 7 days. You can save a maximum of 2 labs at a time. These choices are present when you click the navigation menu in the upper right (hamburger menu).

If your lab time gets to less than 10 minutes remaining, you will see a prompt asking if you want to extend your lab time by 15 minutes. Just click Yes to extend your time. You can only do this a few times. Once that happens your lab will use the remaining time and end anyway. When you can no longer extend the lab, you will see this message:




Your lab has expired and you can no longer extend the time.

Another popup you may see →



Alert! Please note the Lab time remaining and plan accordingly. You will only be able to extend this lab for a limited amount of time before the lab cancels. If this happens, no score will be recorded and you will need to relaunch the lab and start over.

Per CompTIA labs policy of Feb 2022: Once the user reaches the lab duration + all extension times, the lab will cancel (all work will be gone). However, you can launch the lab again from the beginning if desired, until overall lab access expires. Labs are scored. You may change your answers on the Assisted labs, but not the Applied labs.

Note: You may use the Menu  to end (cancel) a lab. This means that no score will be recorded and that the next time you launch the lab it will be reset to its starting conditions

If you need help from CompTIA

To submit a ticket online:

<https://help.comptia.org/hc/en-us/requests/new>

To call for assistance:

Call us: (630) 678-8300 or

(866) 835-8020. You can reach us Monday through Friday from 7:00 a.m. to 7:00 p.m. U.S. Central Time.

To see the list of labs:

On the page

<https://www.comptialabs.com/CourseAssignment/xxxxxxx>

You must scroll down to see the list of labs.

Network+ N10-008 Device info

DEVICE	Username	Password	Platform/OS
DC10 (JOIN)	Administrator	Pa\$\$w0rd	Server 2019 Standard
MS10 (JOIN)	Administrator	Pa\$\$w0rd	Server 2016 Standard
PC10 (JOIN)	Administrator	Pa\$\$w0rd	Server 2019 Standard*
SMB10 (JOIN)	root / smb	Pa\$\$w0rd	Fedora (Linux)
LAMP10	lamp	Pa\$\$w0rd	Ubuntu Server (Linux)
rLAN10	vyos	Pa\$\$w0rd	VyOS 1.4 (Linux)
OpenWRT	root	Pa\$\$w0rd**	
Ubuntu Desktop 18.04	labadmin	Pa\$\$w0rd	
Kali Linux 2020.3	kali	Pa\$\$w0rd	Kali (Linux)
KMS	10.1.0.22:1688	Pa\$\$w0rd	pfSense
pfSense	admin	Pa\$\$w0rd	pfSense
NSIM10	nsim	Pa\$\$w0rd	Ubuntu (Linux) [GNS3]
CUMULUSVX-1	cumulus	Pa\$\$w0rd	White box switch NOS [GNS3]

* - PC10 (JOIN) is acting as a client PC.

** - Configured in Lab 01

If Pa\$\$w0rd is rejected, try again with the RIGHT SHIFT key on your keyboard.

Devices available in the lab environment



vLAN_SERVERS



vLAN_CLIENTS



vLAN_BRANCH



vLOCAL



vCLUSTER



vSAN



INTERNET



vBORDER

Virtual Switches



LAMP10



SMB10 (JOIN)
Fedora Server



KMS
(pfSense)



Kali
Linux
2020.3



NSIM10



Ubuntu
Desktop 18.04



DC10 (JOIN)



MS10 (JOIN)



PC10 (JOIN)
Emulating a client PC

Network nodes (IP endpoints)



pfSense



rLAN10

Router (VyOS)

If you are exploring the Help tab, don't click [Click here to Submit a Support Request](#) because it ends your lab and opens a page to submit a support ticket.

Lab 00: Assisted Lab-Exploring the Lab Environment

15 minutes



vLAN_SERVERS



vLAN_CLIENTS



vBORDER

Virtual Switches



NSIM10



LAMP10



SMB10 (JOIN)



DC10 (JOIN)



MS10 (JOIN)



PC10 (JOIN)
Emulating a client PC

Network nodes (IP endpoints)



rLAN10

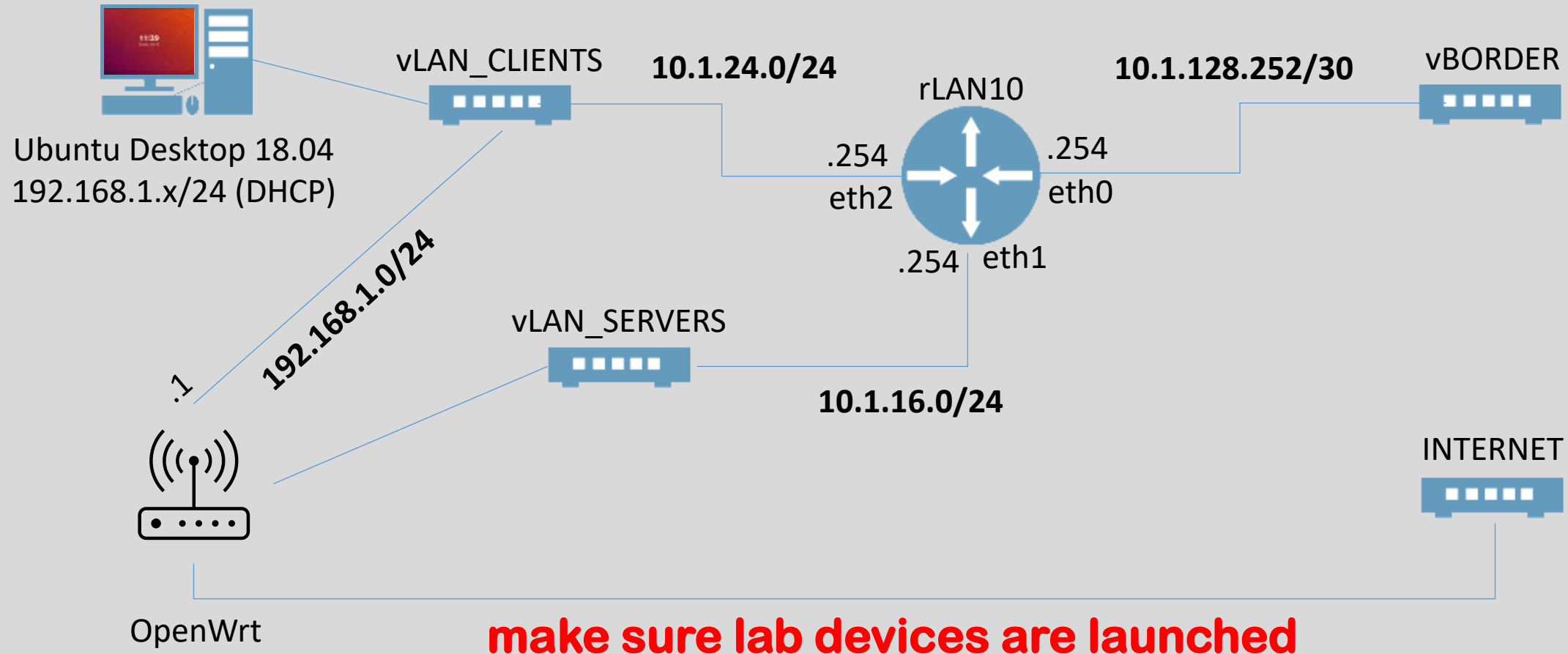
Router (VyOS)

To access the lab environment:
<https://login.comptia.org/training-products>

If you are exploring the Help tab, don't click [Click here to Submit a Support Request](#) because it ends your lab and opens a page to submit a support ticket.

20 minutes (+2x15ext)

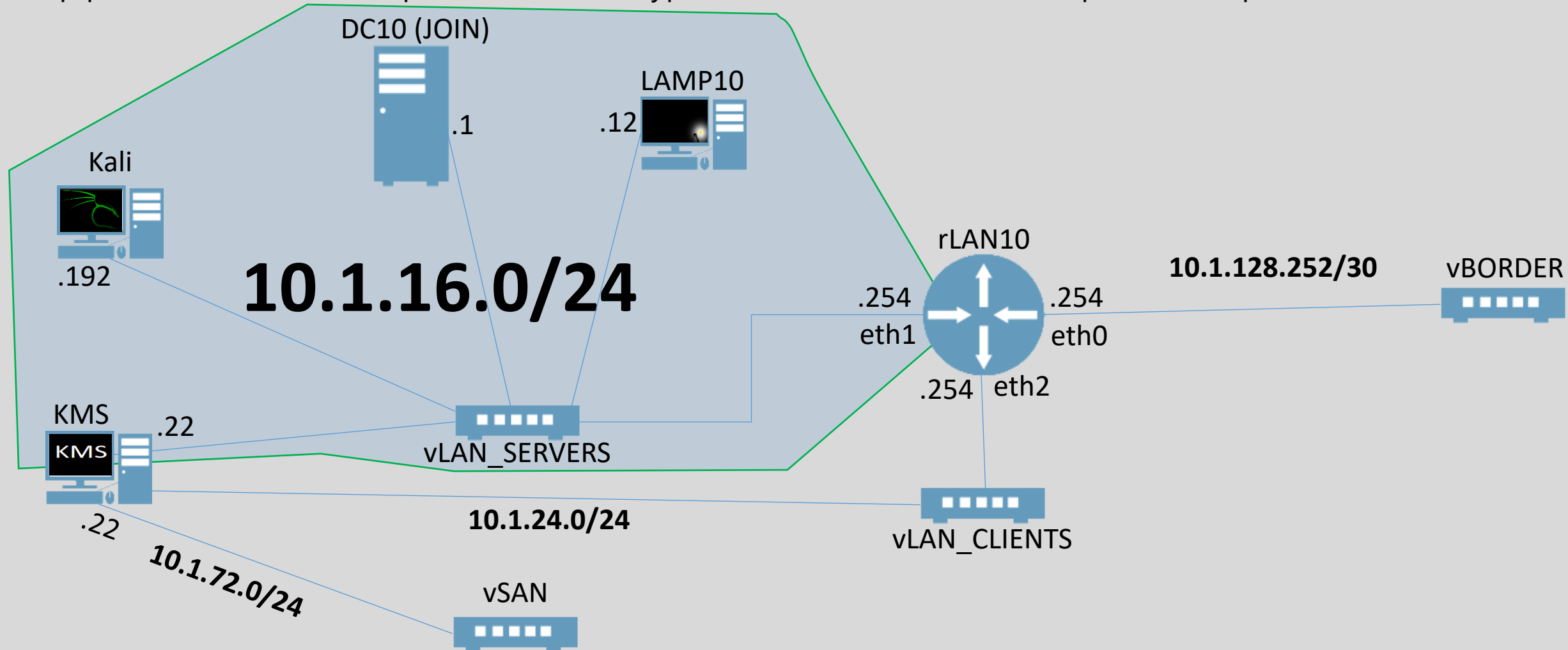
Scenario: You have purchased a router for your work-from-home office and you need to display common settings and set basic configurations.



Lab 02: Assisted Lab: Capture Network Traffic

30 minutes (+1x15ext)

Scenario: You will scan a target server to determine likely types of network traffic to intercept. Next, you will use the tcpdump packet sniffer to intercept three different types of network traffic and interpret the output.



Lab 03: Assisted Lab: Configure Interface Settings

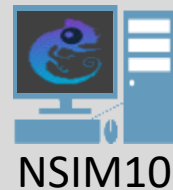
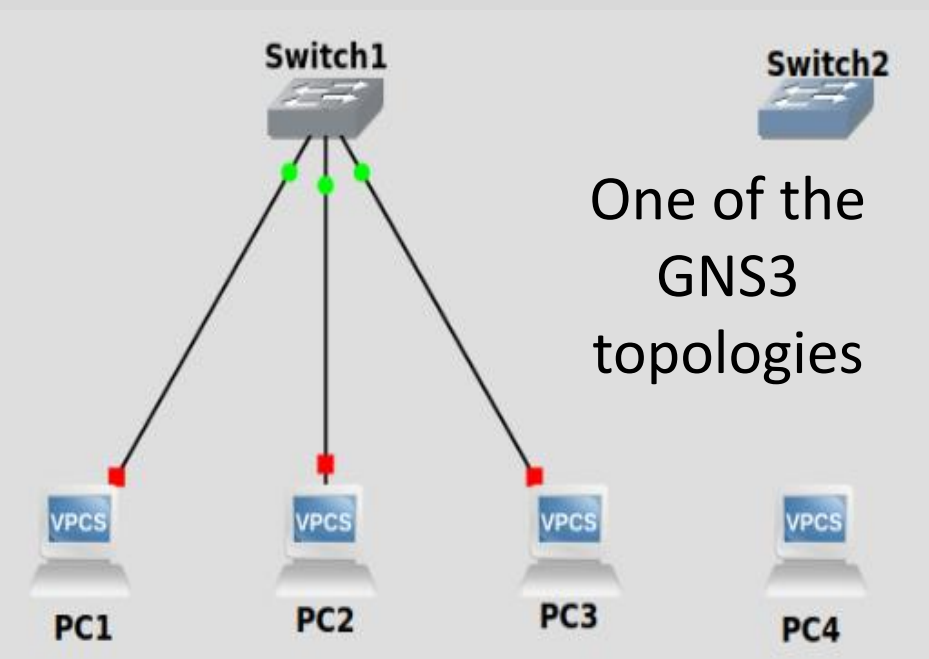
20 minutes (+1x15ext)

Scenario: At layers 1 and 2, the majority of networks are built by connecting end system interfaces to intermediate system interfaces. While networks of this type are now mostly built using Ethernet switches as the intermediate system, it is important to understand legacy technologies, such as hubs.

To complete this activity, use the GNS3 network simulator [GNS3](#) to investigate the properties of local networks built using hubs, unmanaged switches, and managed switches.

Note: The [T] method of pasting into the lab environment from the lab instructions works in the console sessions inside GNS3.

On step 4, when you access the Console of PC1 inside GNS3, after a pause, you may have to click inside the window that appears and then hit the Enter key - to “wake it up.”



Challenge question: In the section **Investigate switch-based Ethernet**, after PC1 pings 10.0.0.2 and 10.0.0.3, an ARP reply is seen in Wireshark in response to the ARP query to 10.0.0.3, but there is no ARP reply in response to the ARP query to 10.0.0.2. Why not?

See next slide for answer

Lab 03: Challenge question

Challenge question: In the section **Investigate switch-based Ethernet**, after PC1 pings 10.0.0.2 and 10.0.0.3, an ARP reply is seen in Wireshark in response to the ARP query to 10.0.0.3, but there is no ARP reply in response to the ARP query to 10.0.0.2. Why not?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 10.0.0.2? Tell 10.0.0.1
2	3.491928	Private_66:68:00	Broadcast	ARP	64	Who has 10.0.0.3? Tell 10.0.0.1
3	3.492898	Private_66:68:02	Private_66:68:00	ARP	64	10.0.0.3 is at 00:50:79:66:68:02
4	3.492893	10.0.0.1	10.0.0.3	ICMP	98	Echo (ping) request id=0x44ec,
5	3.493007	10.0.0.3	10.0.0.1	ICMP	98	Echo (ping) reply id=0x44ec,

4	Frame 3: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
	Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Private_66:68:00 (00:50:79:66:68:00)
	Address Resolution Protocol (reply)
	Hardware type: Ethernet (1)
	Protocol type: IPv4 (0x0800)
	Hardware size: 6
	Protocol size: 4
	Opcode: reply (2)
	Sender MAC address: Private_66:68:02 (00:50:79:66:68:02)
	Sender IP address: 10.0.0.3

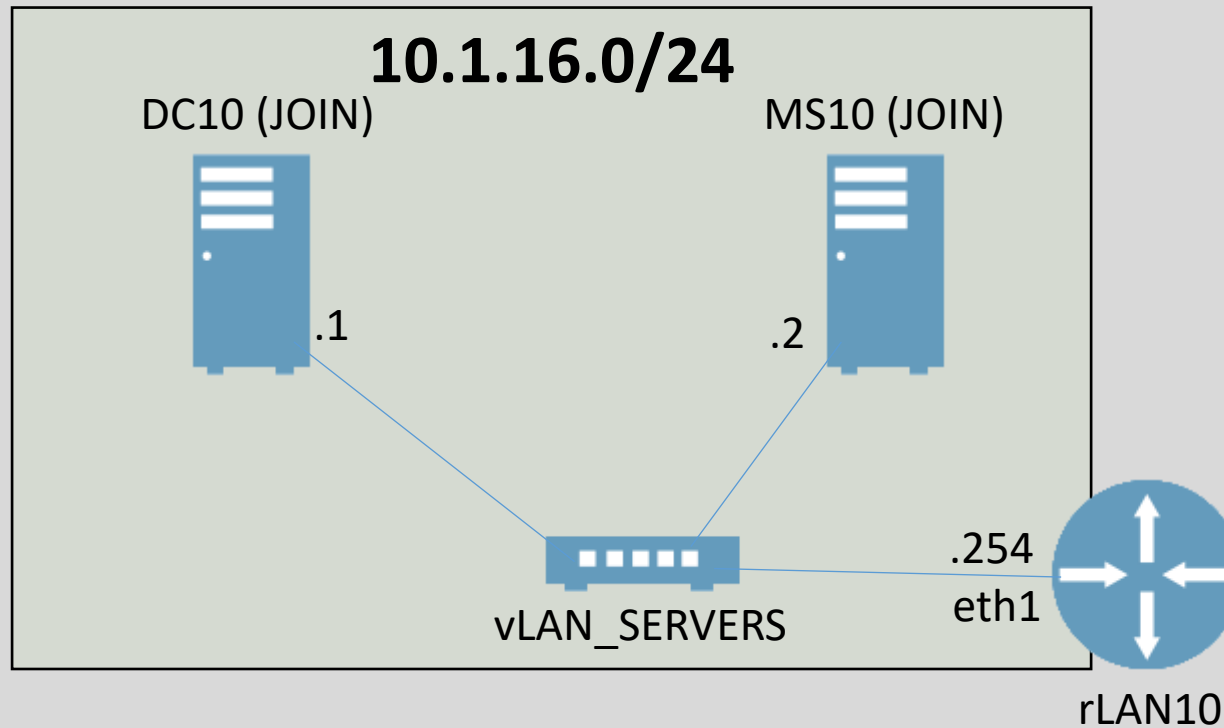
Answer: The packet capture is occurring on the link between the switch and PC3. Since the reply from PC2 (10.0.0.2) has a destination MAC address that is known to the switch, no traffic is generated on the link to PC3.

Lab 04: Assisted Lab: Configure IPv4 Static Addressing

15 minutes (+1x15ext)

Scenario: In this activity, you will discover the effect on connectivity when you adjust the subnet mask applied to an IP configuration.

This topology diagram shows the devices that are relevant in this lab.



Lab 05: Assisted Lab: Analyze ARP Traffic

20 minutes (+2x15ext)

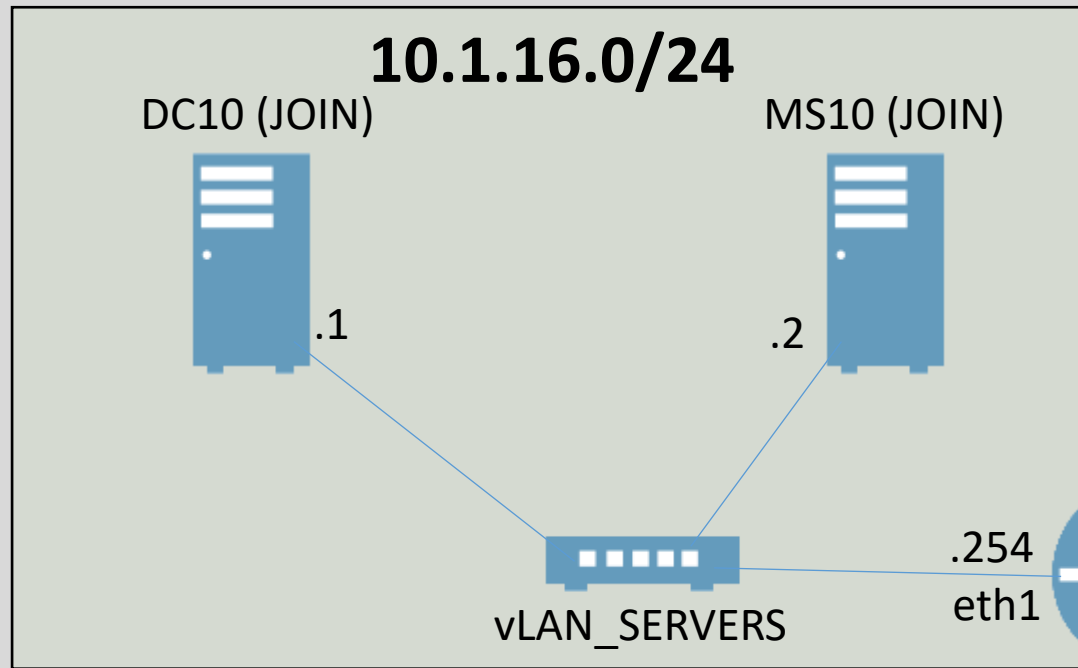
Scenario: In this activity, you will discover several ways of gathering network configuration information by using both Windows Server and a Linux-based router. First, you will examine network adapter properties on a Windows server. Next, you will gather IP address configuration information at the Windows CLI. Your next task will be to analyze ARP traffic by using the Wireshark packet analyzer. Finally, you will collect network information for the VyOS-based router at 10.1.16.254.

This topology diagram shows the devices that are relevant in this lab.

You can SSH from DC10 to the loopback address on rLAN10 if you want to paste text successfully. They did not use the [T] method, so you will have to copy and use the lightning bolt method to paste.

From a Command Prompt on DC10, type this:

ssh vyos@10.1.254.254



In the “Run tcpdump” section step 5, if you are running this command from an SSH connection to rLAN10, here is the command to filter out the SSH traffic, so it doesn’t fill the screen

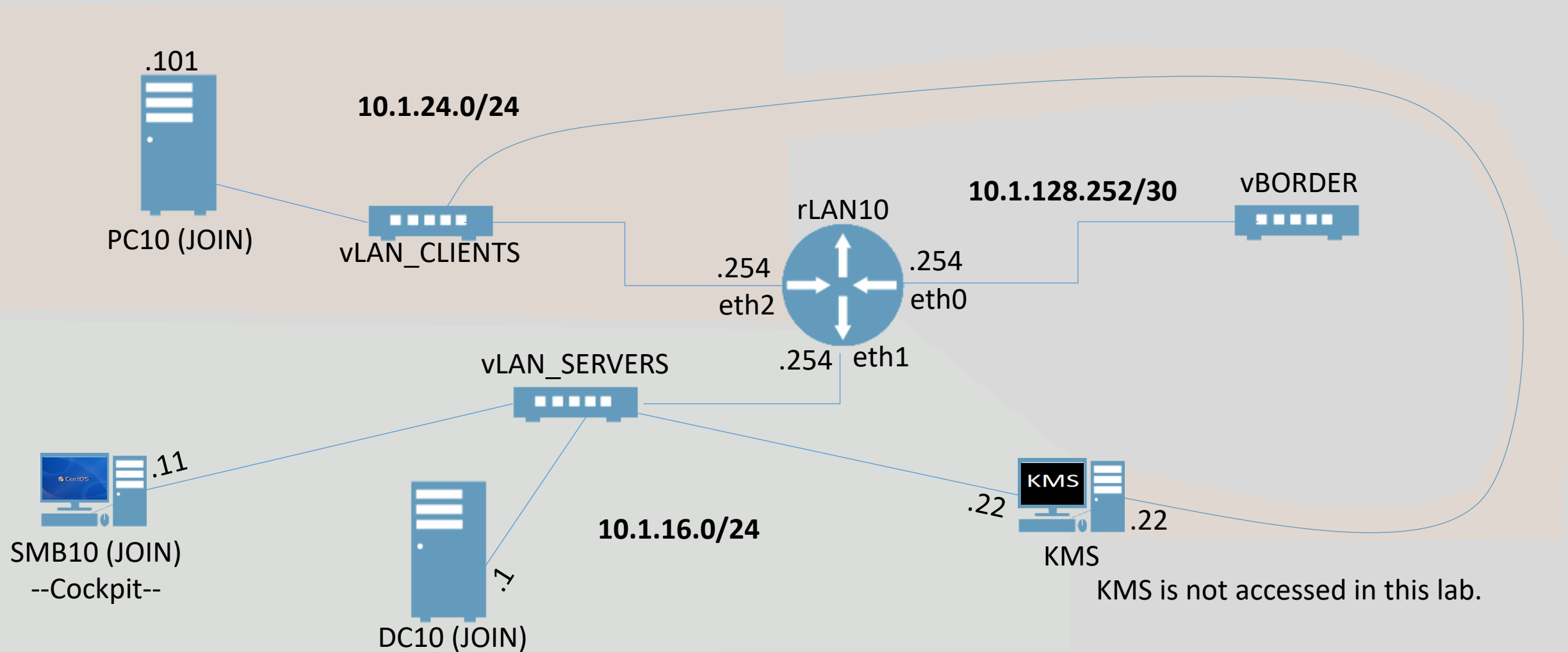
tcpdump -i eth1 ip and not port 22

Loopback:
10.1.254.254/32

Lab 06: Assisted Lab: Use Tools to Test IP Configuration

15 minutes (+2x15ext)

Scenario: You will verify several network address settings in Windows and Linux. First, you will review and configure a network interface for a Windows device. Next, you will remotely administer a Linux server by using Cockpit. Finally, you will manage name resolution configurations on a remote Linux server.

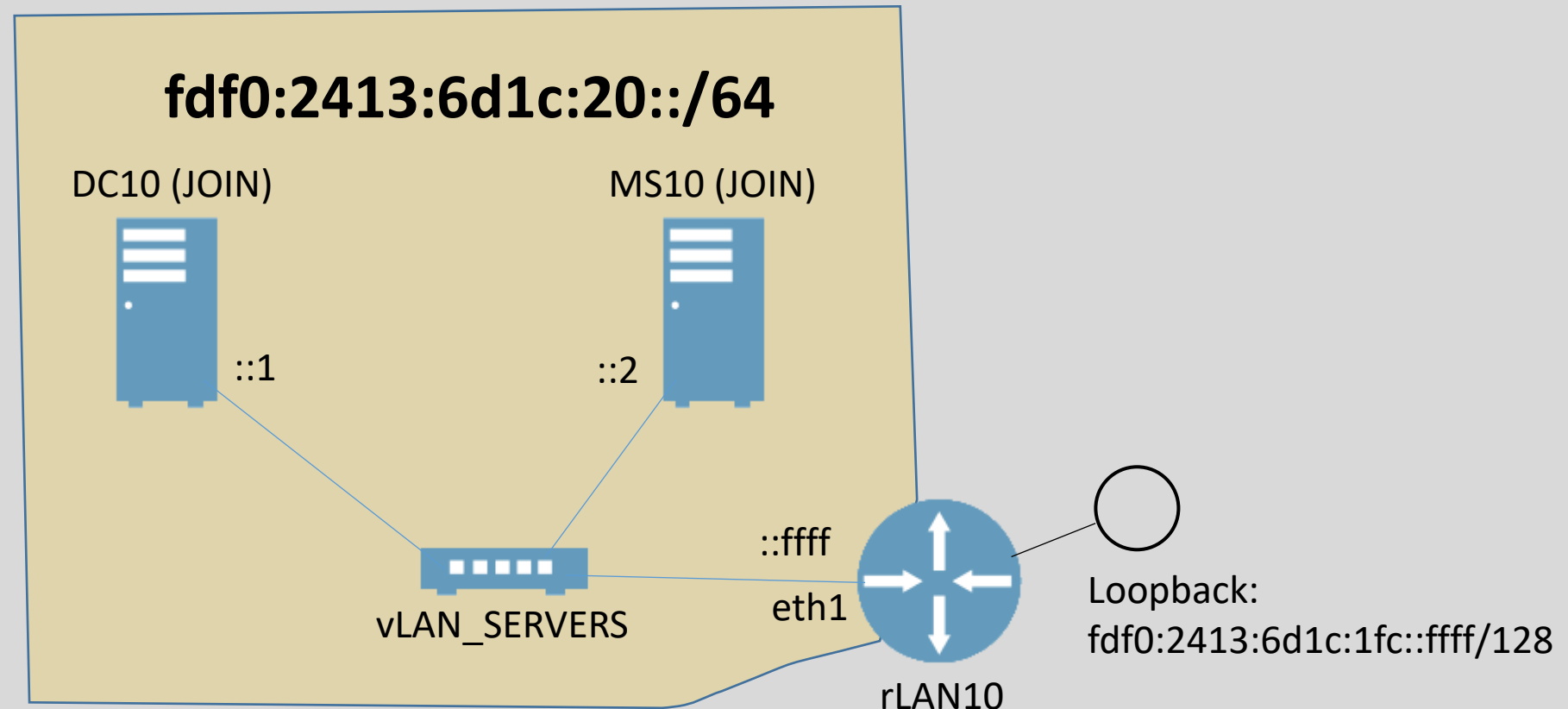


Lab 07: Assisted Lab: Configure IPv6 Static Addressing

15 minutes (+2x15ext)

Scenario: In this activity, you will observe the use of IPv6 configurations in your VMs by using IP commands and Wireshark.

This topology diagram shows the devices that are relevant in this lab.

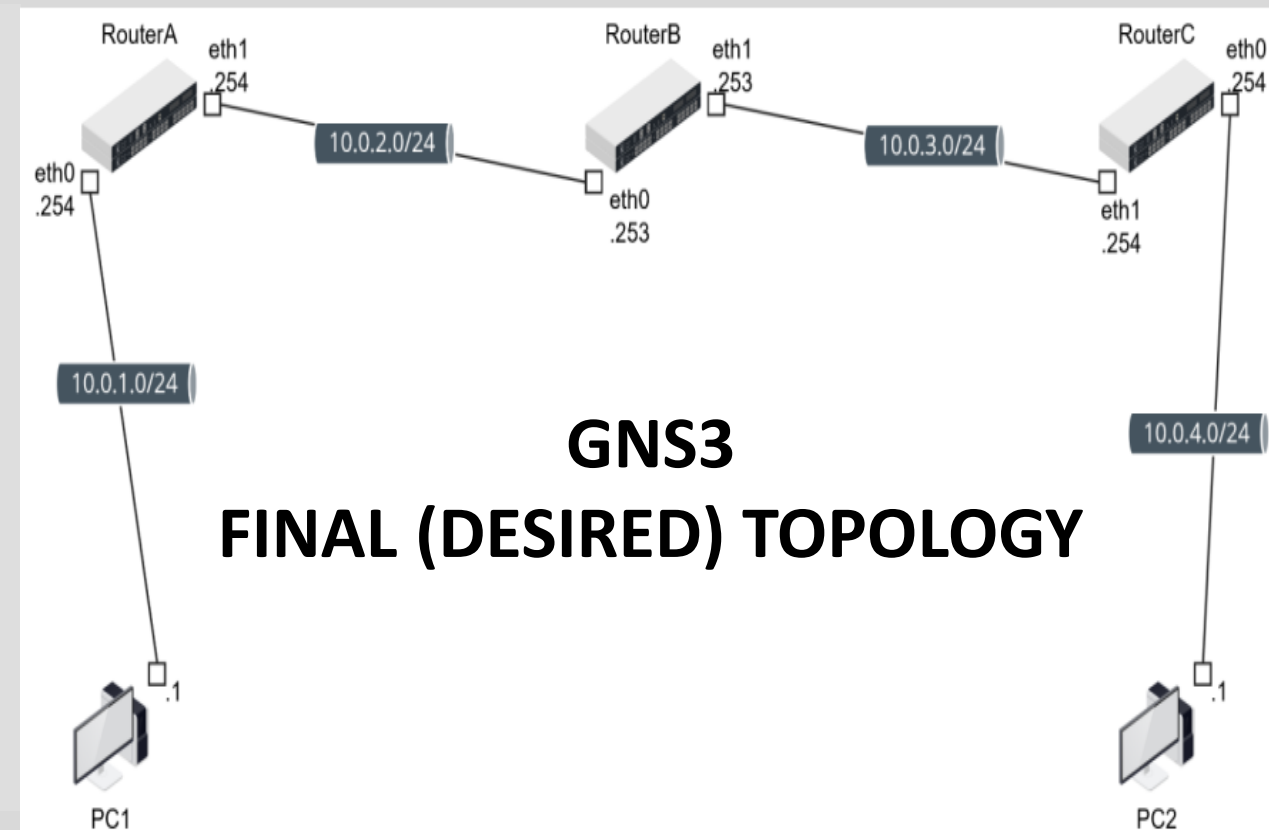
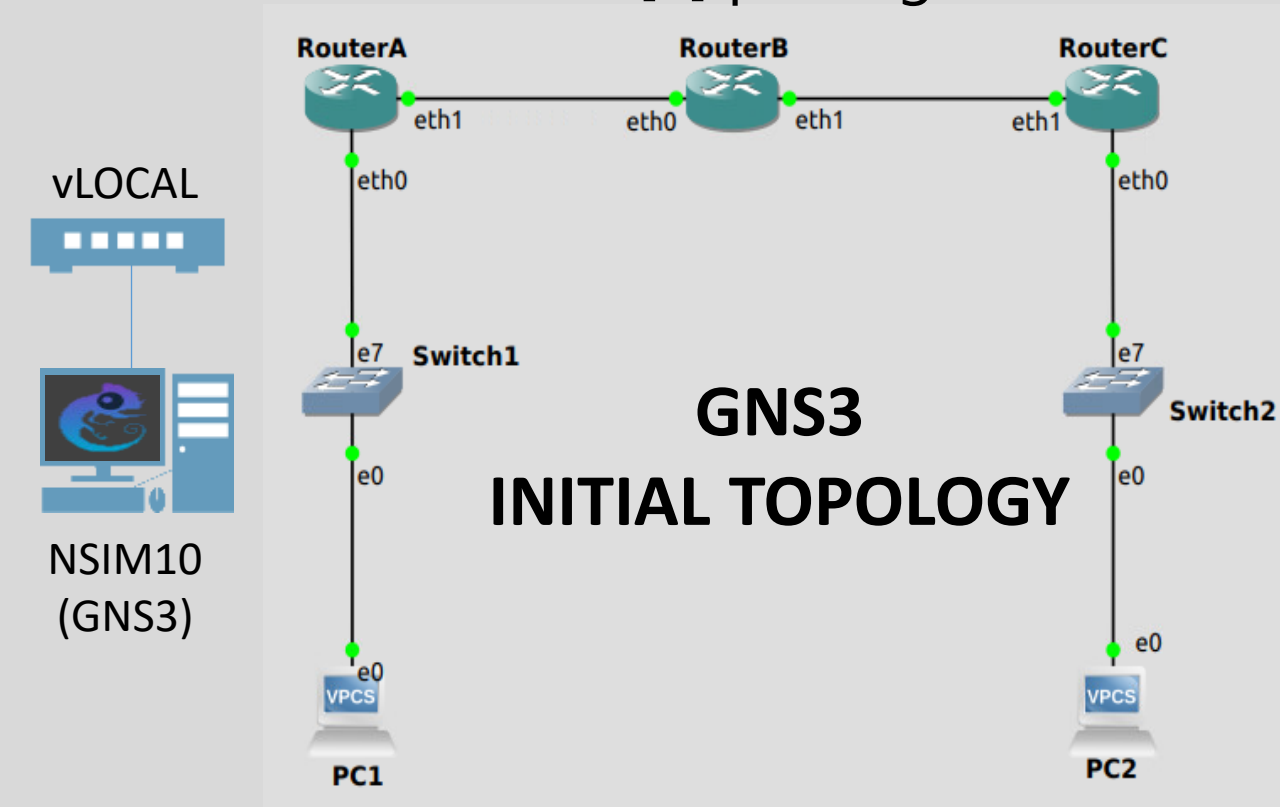


Lab 08: Assisted Lab: Configure Static Routing

30 minutes (+2x15ext)

Scenario: Being able to analyze documentation and use command-line tools to implement dynamic routing protocols quickly and accurately are essential competencies. To complete this activity, use the GNS3 network simulator gns3.com to configure an internetwork running the RIP dynamic routing protocol.

This topology diagram shows the devices that are relevant in this lab. Note that the [T] pasting method works on the console windows in GNS3.

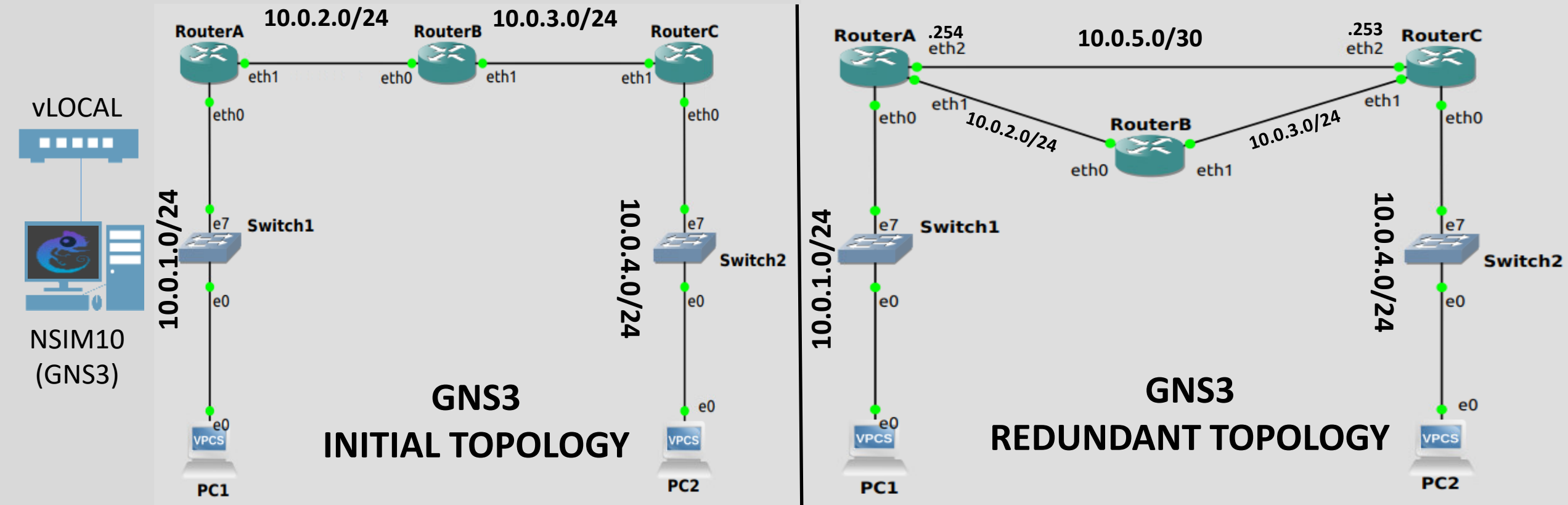


Lab 09: Assisted Lab: Configure Dynamic Routing

20 minutes (+2x15ext)

Scenario: Being able to use command-line tools to implement router configuration quickly and accurately is an essential competency. To complete this activity, use the GNS3 network simulator gns3.com to configure an internetwork based on static routing.

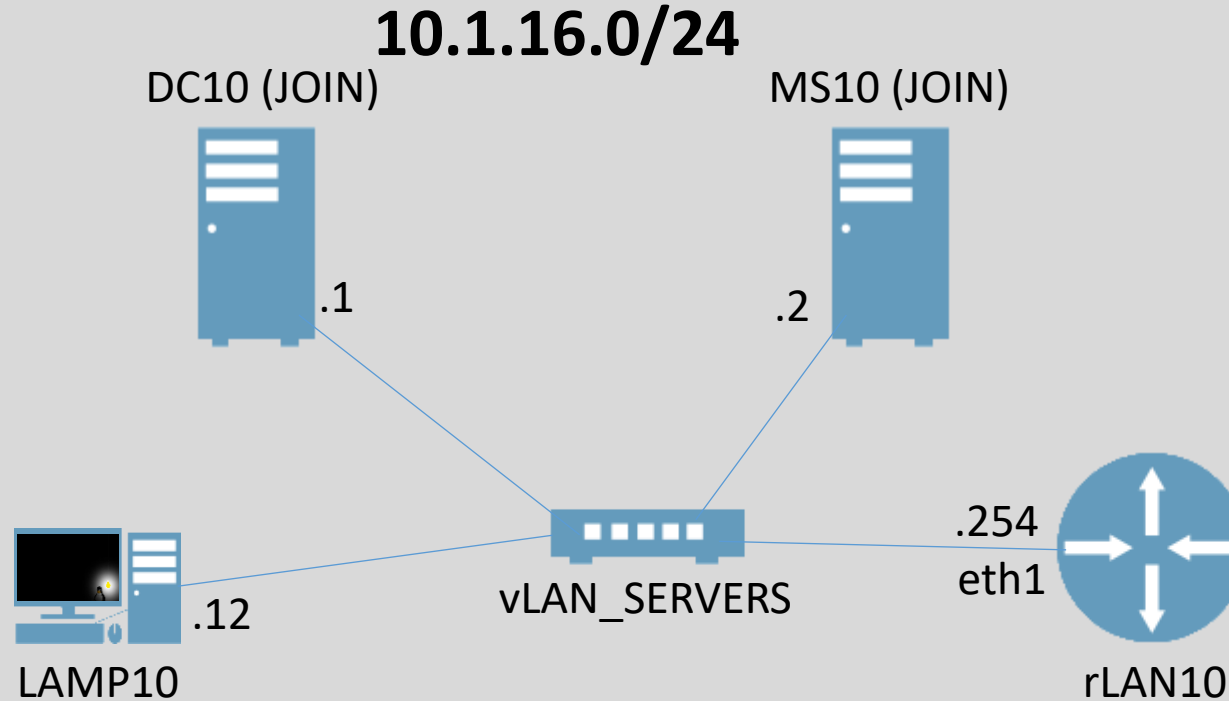
This topology diagram shows the devices that are relevant in this lab. Note that the [T] pasting method works on the console windows in GNS3.



Lab 10A: Applied Lab: Troubleshoot IP Networks

20 minutes (+2x15ext) Labs 10A & 10B can be done in either order

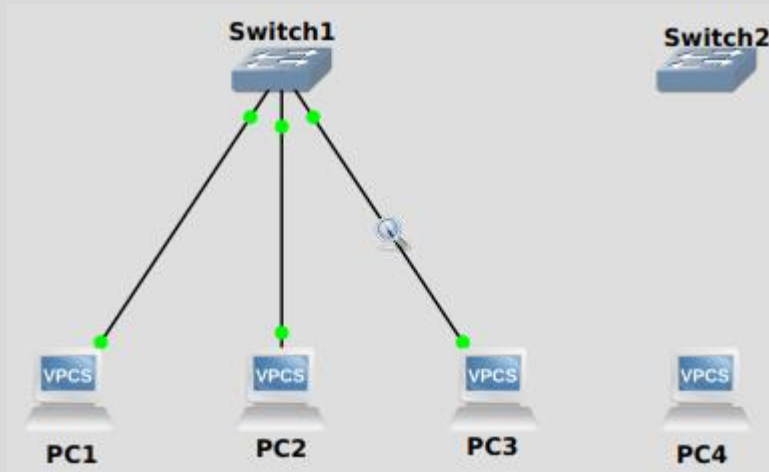
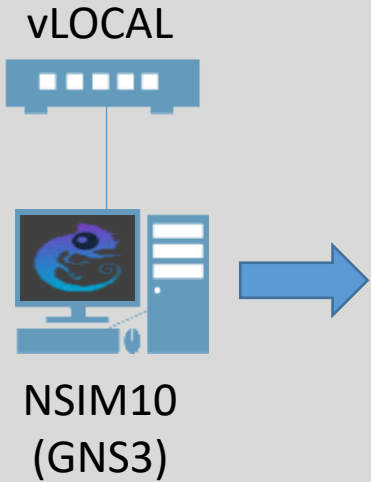
This topology diagram shows the devices that are relevant in this lab.



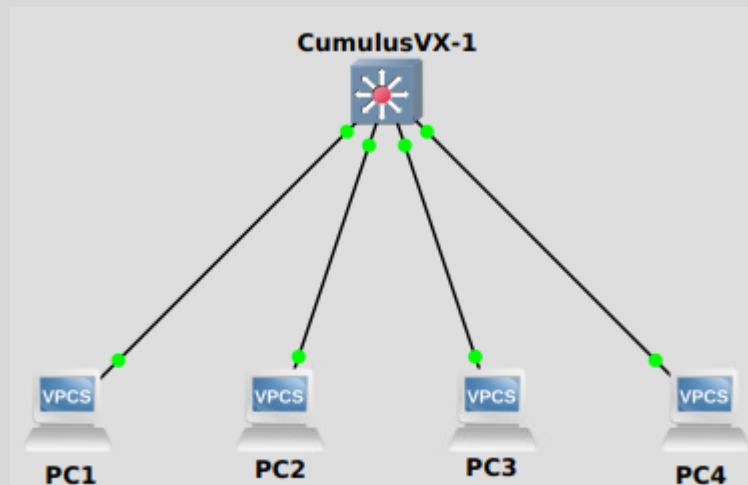
Lab 10B: Applied Lab: Troubleshoot IP Networks

20 minutes (+3x15ext) Labs 10A & 10B can be done in either order

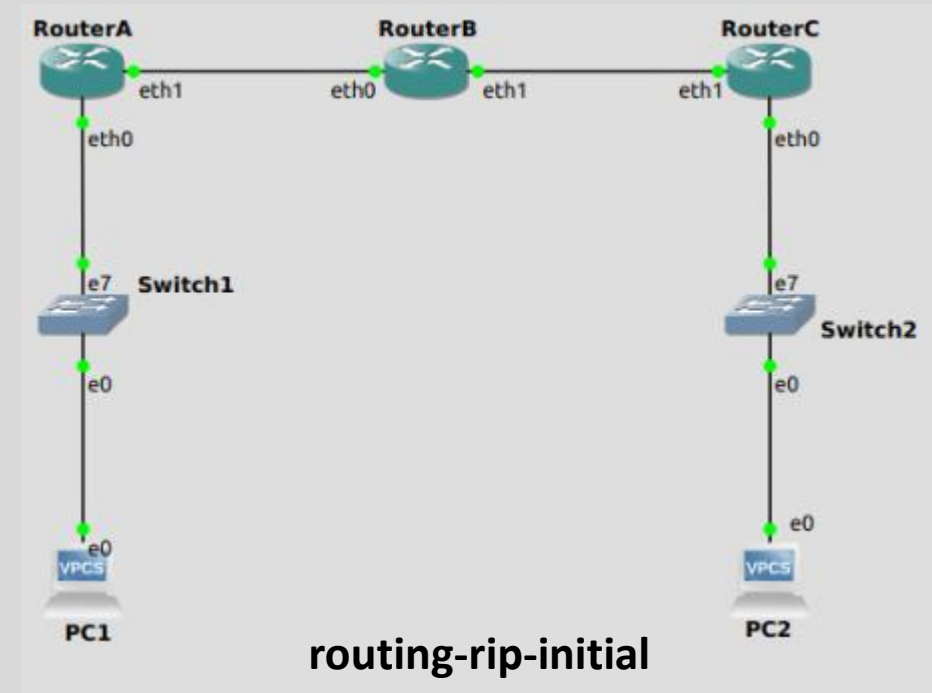
These topologies are within GNS3 on NSIM10..



interfaces-switch-unmanaged-initial



interfaces-switch-managed-initial

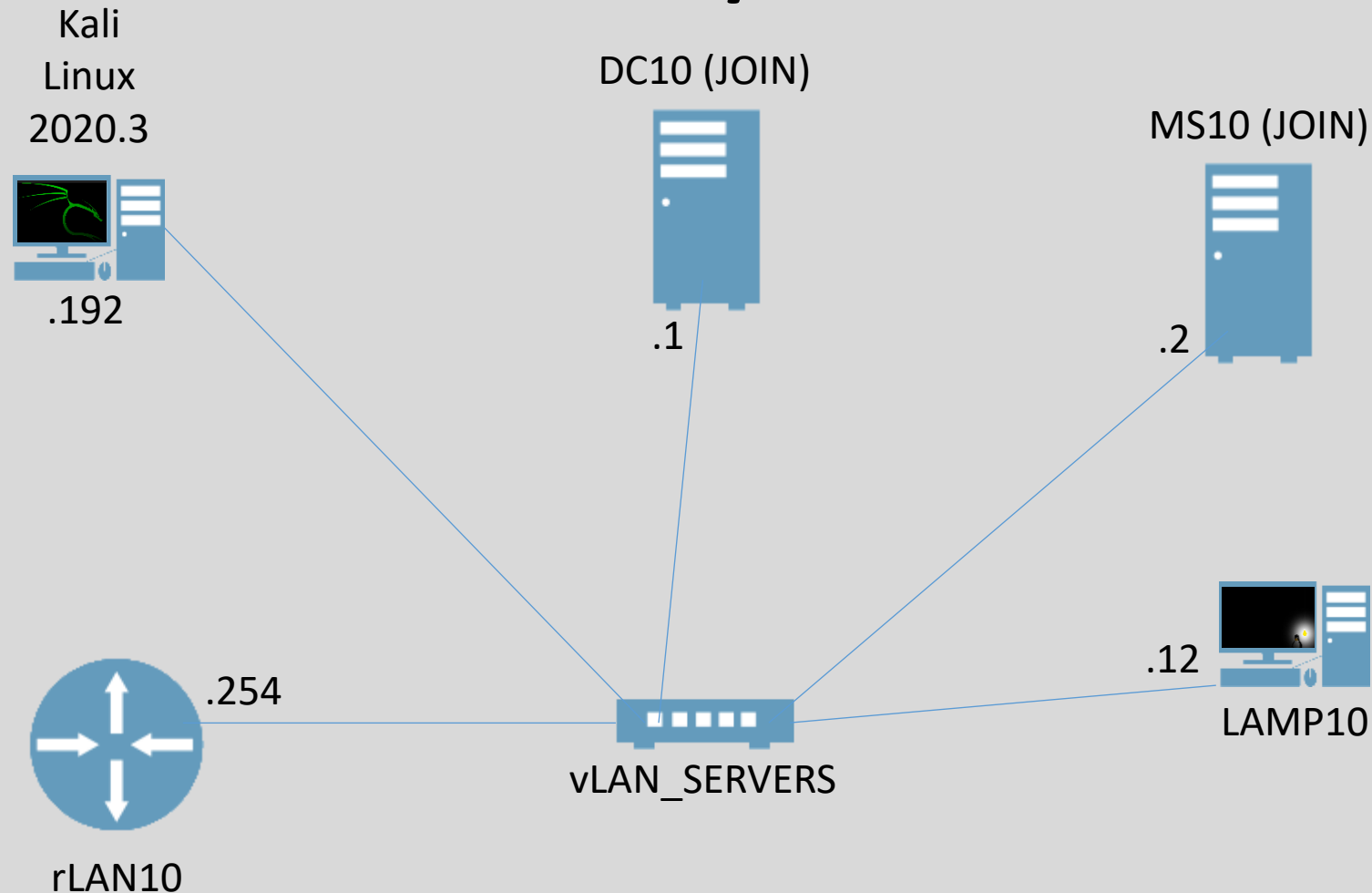


Lab 11: Assisted Lab: Use Network Scanners

20 minutes (+2x15ext)

You will use two different network scanners (nmap and Netdiscover) to investigate network hosts, including discovering available hosts, network services, and port. You will also analyze TCP and UDP traffic by using Wireshark to display packet headers.

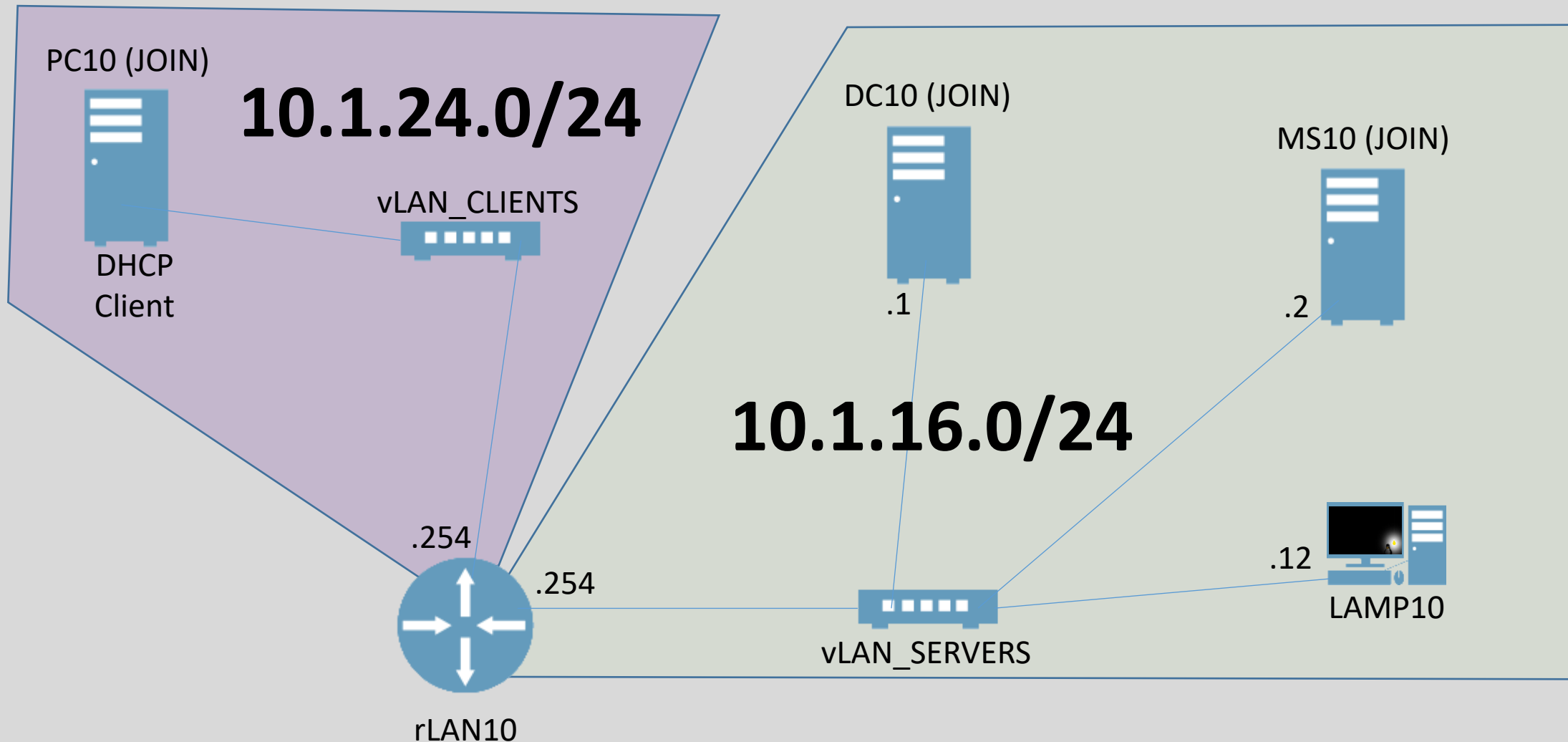
10.1.16.0/24



Lab 12: Assisted Lab: Analyze a DHCP Server Configuration

20 minutes (+2x15ext)

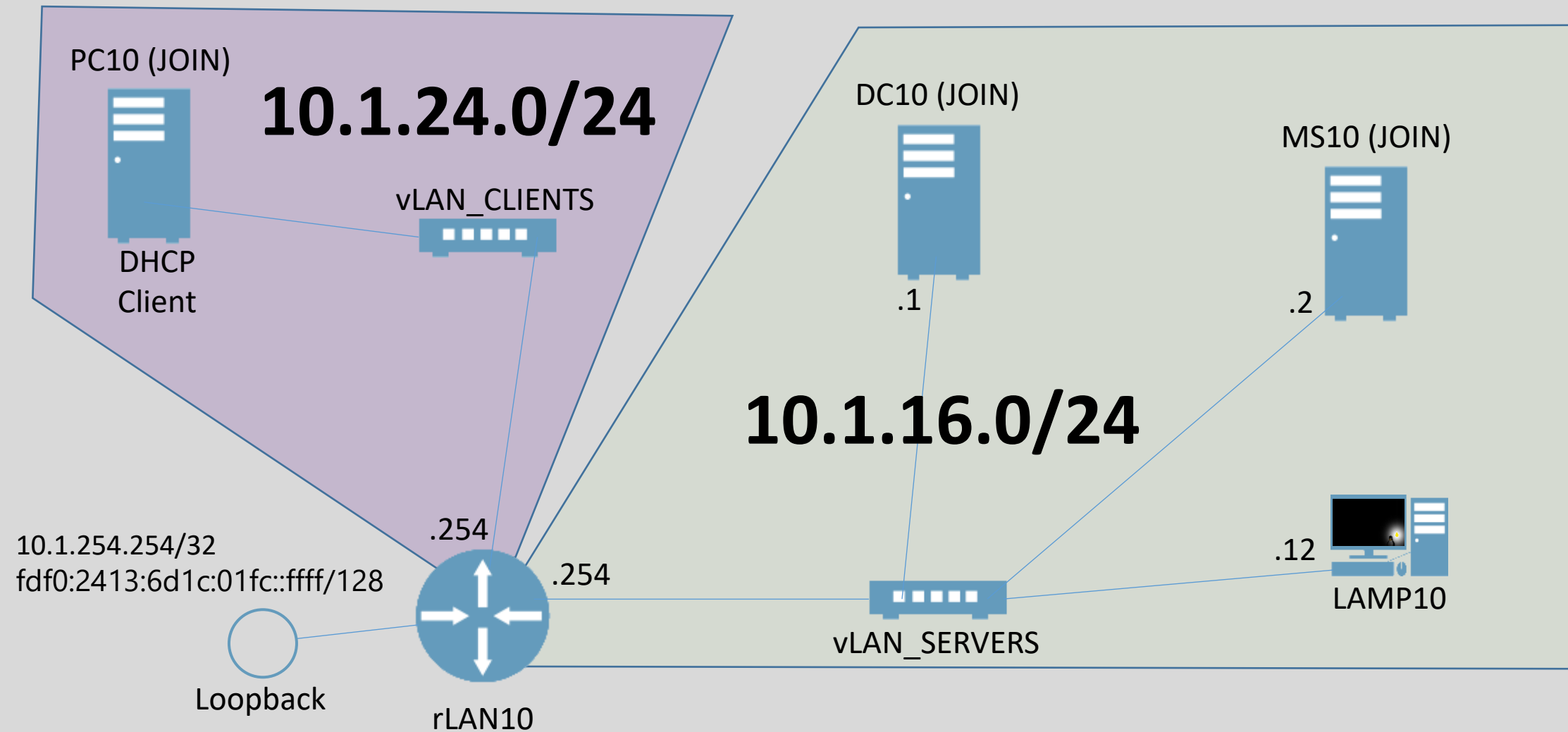
You will examine an existing DHCP implementation for two subnets, including reserved addresses. Next, you will create a new scope of available addresses. You will also configure DHCP replication for fault tolerance. Finally, you will configure a DHCP client to receive IP address settings from the DHCP server.



Lab 13: Assisted Lab: Analyze a DNS Server Configuration

20 minutes (+2x15ext)

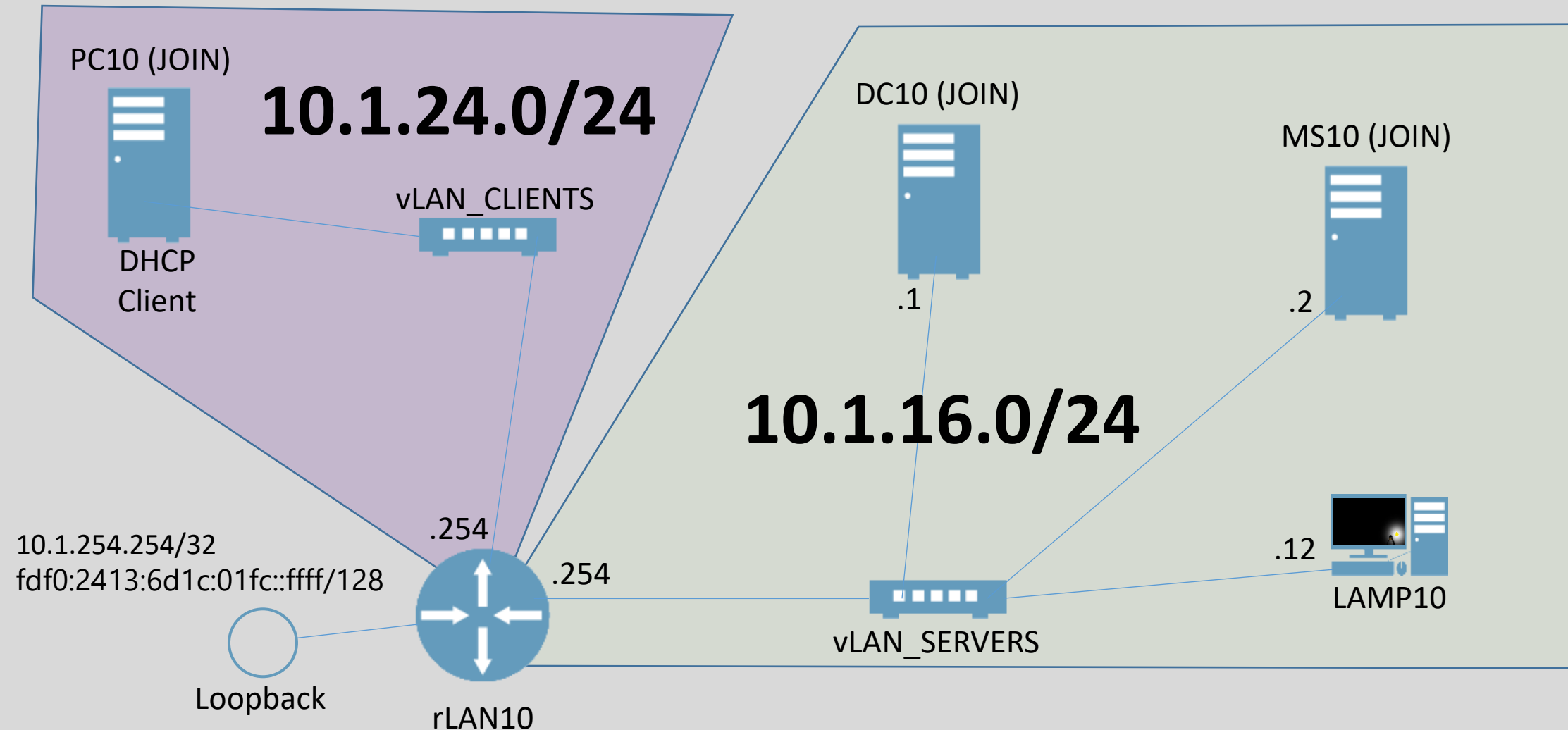
You will examine an existing DHCP implementation for two subnets, including reserved addresses. Next, you will create a new scope of available addresses. You will also configure DHCP replication for fault tolerance. Finally, you will configure a DHCP client to receive IP address settings from the DHCP server.



Lab 14: Assisted Lab: Analyze Application Security Configurations

15 minutes (+2x15ext)

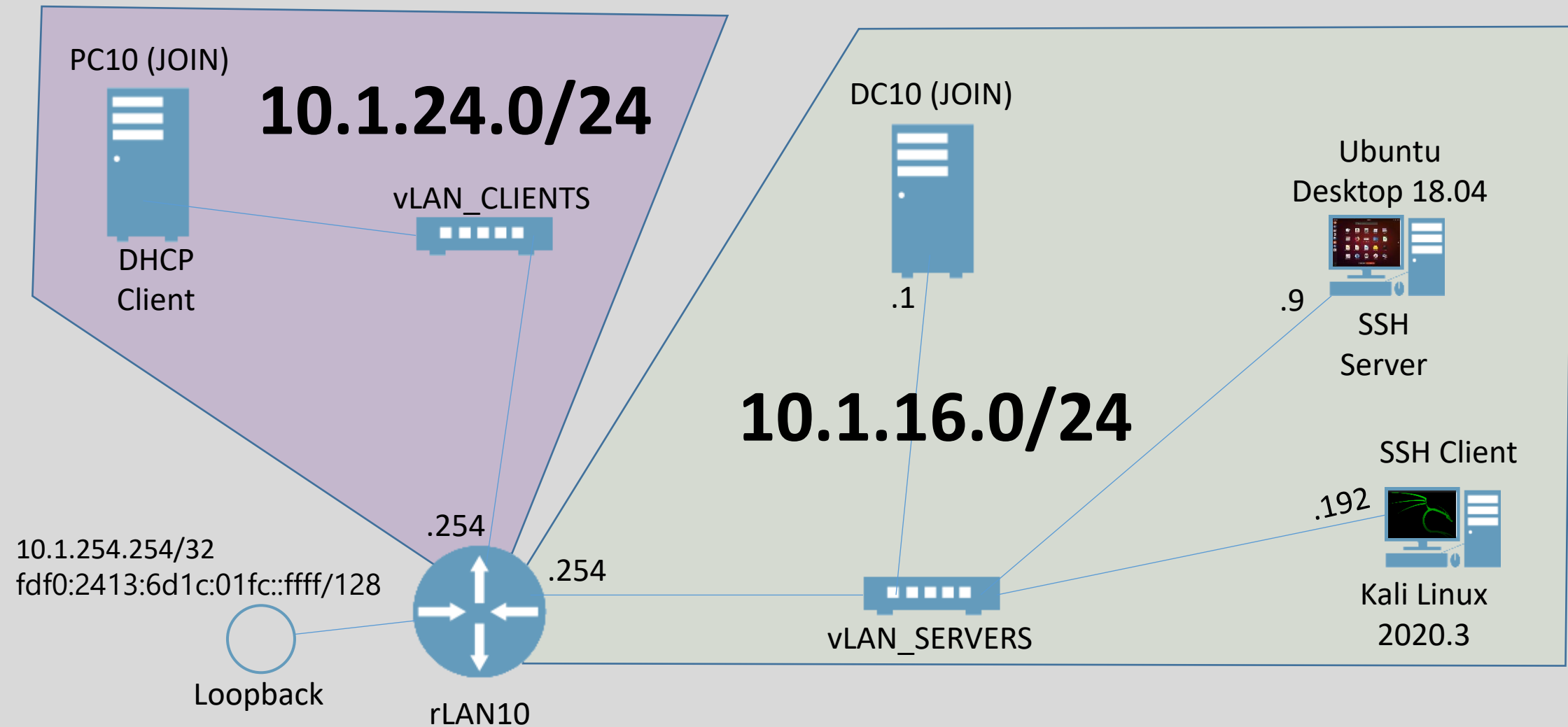
In this activity, you will use an email client to examine the effect of using unsecured protocols by intercepting messages with Wireshark.



Lab 15: Assisted Lab: Configure Secure Access Channels

25 minutes (+3x15ext)

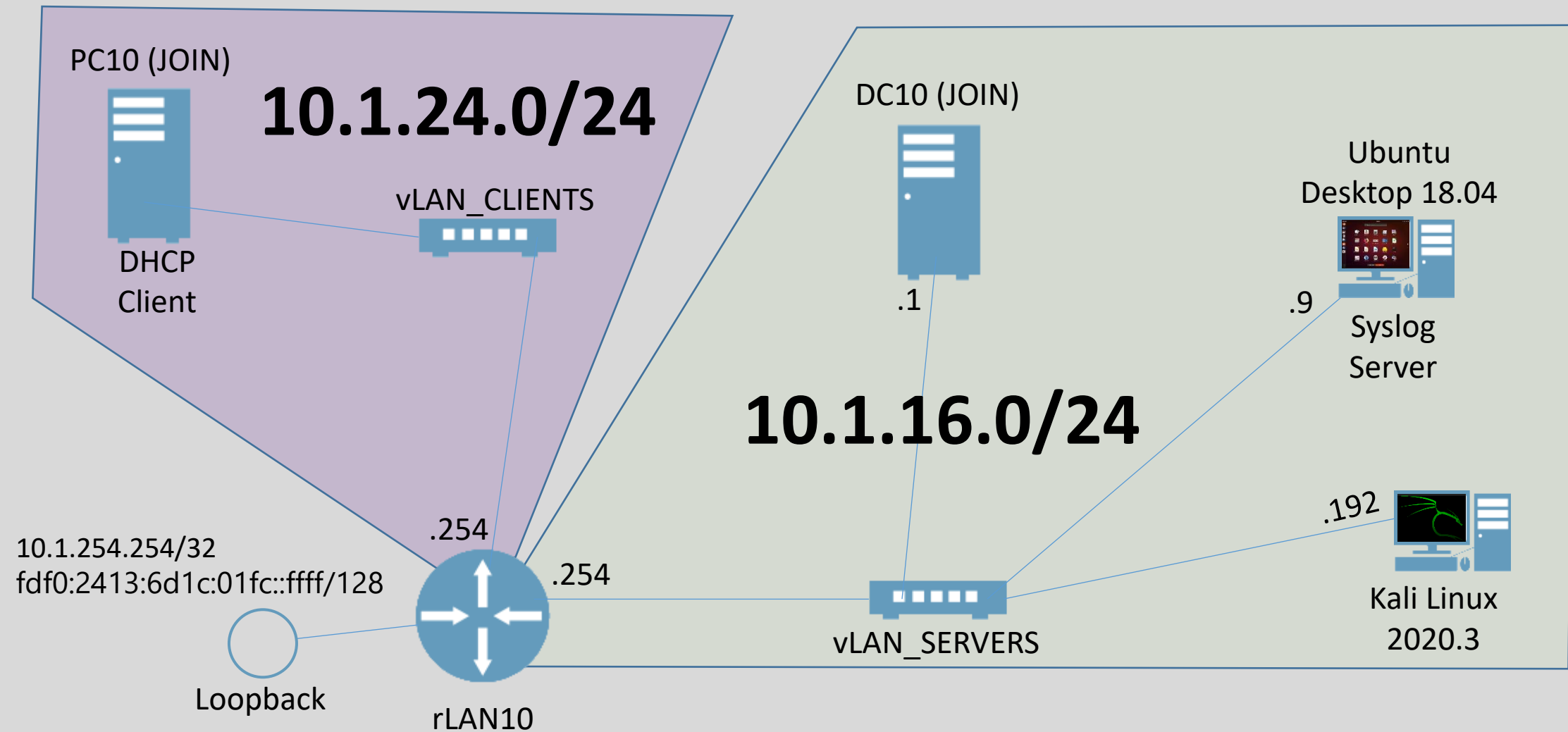
The Secure Shell (SSH) protocol is a common protocol for establishing remote connections to Linux, Unix, and other Unix-like systems. SSH functionality can be added to Windows, too. In this activity, you will configure several security settings on a remote destination SSH server. You'll be testing connectivity from an SSH client virtual machine.



Lab 16: Assisted Lab: Configure Syslog

20 minutes (+2x15ext)

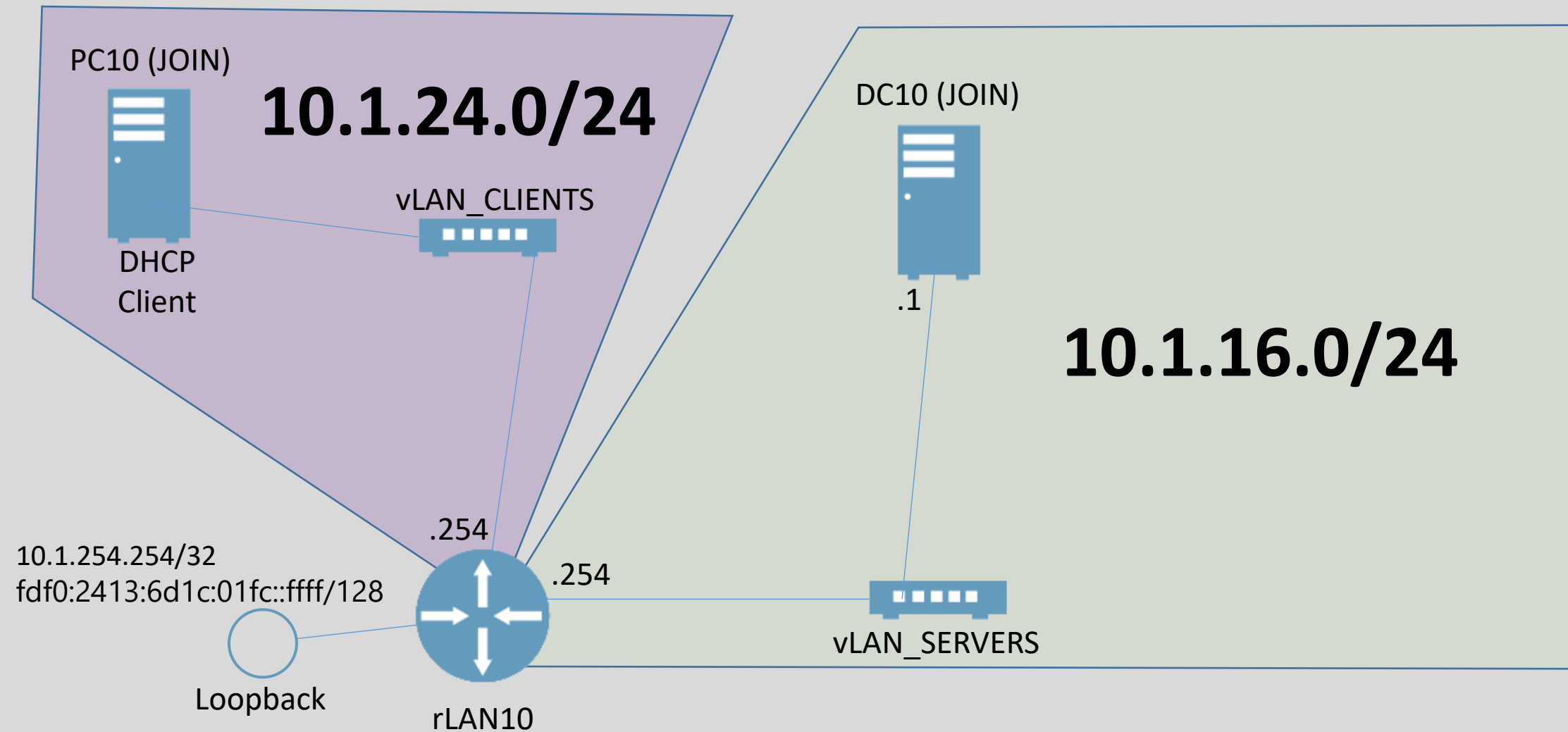
In this activity, you will configure a Linux virtual machine as a centralized log file storage server. You will then configure two Linux devices—a server and a router—to forward their log files to the central server. You will confirm the log file forwarding.



Lab 17: Assisted Lab: Analyze Network Performance

20 minutes (+1x15ext)

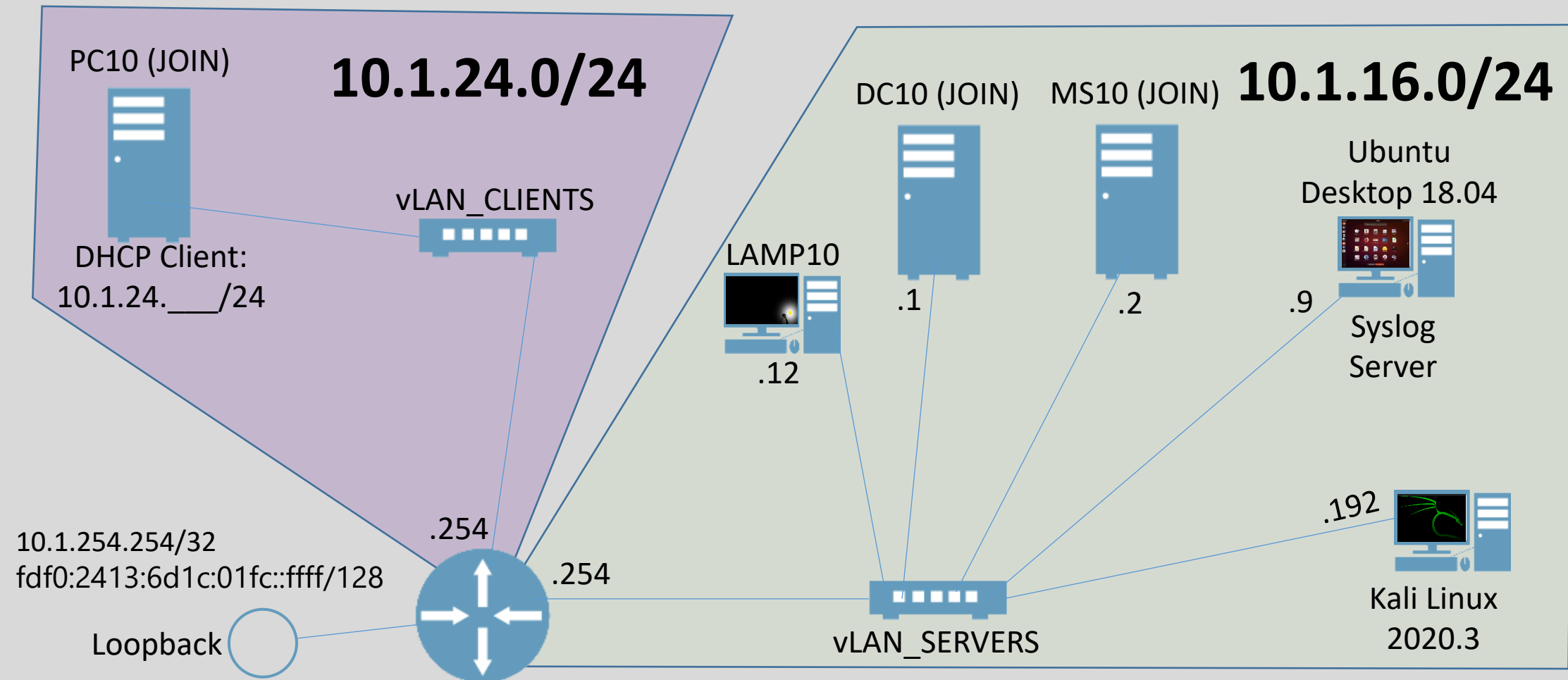
You have been asked to evaluate several network monitoring tools, including Windows Performance Monitor, Wireshark, and the Linux tool iftop. You will share out a folder from DC10 and then transfer a very large file into that folder across the network from PC10. You will review the information collected by the monitoring tools.



Lab 18: Applied Lab: Verify Service and Application Configuration

30 minutes (+3x15ext)

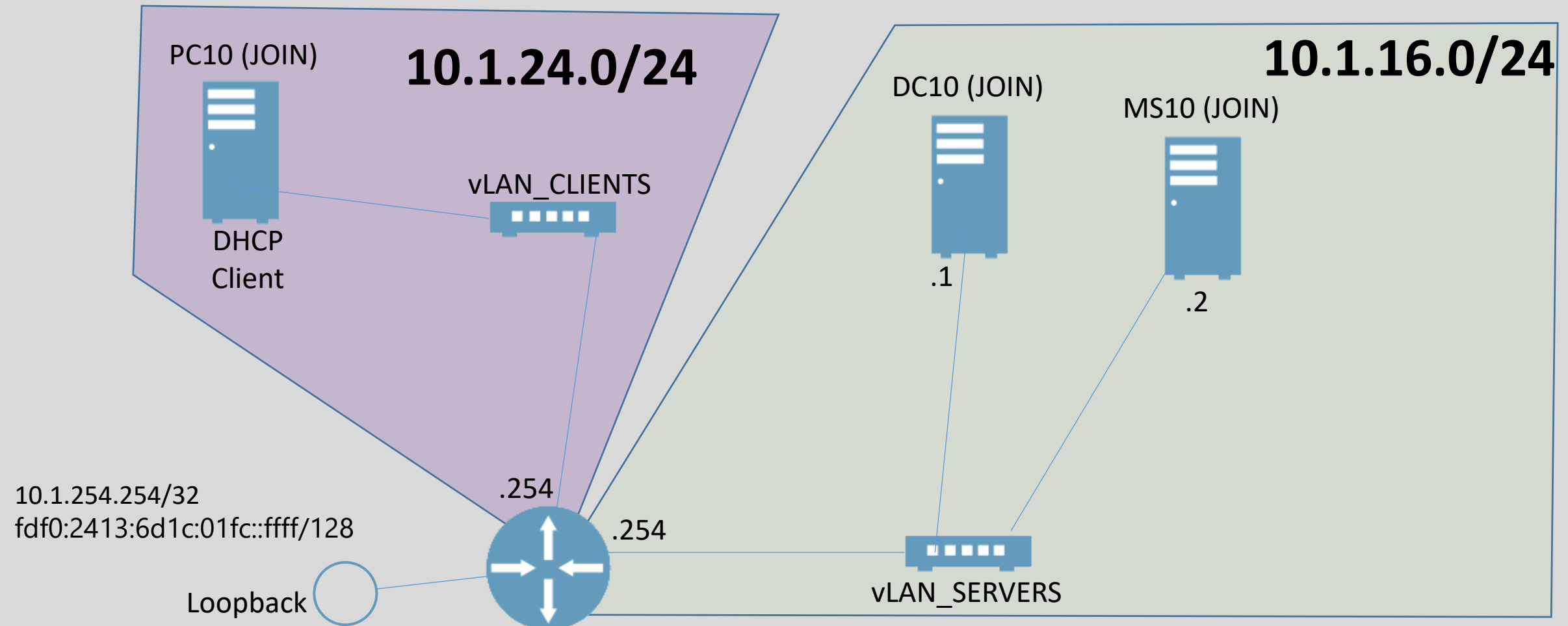
This is an applied lab where you will need to work more independently to complete the required tasks. Note that you may not retry grading attempts in this lab. Once you select the **Score** button for each task, the task will be evaluated as complete or incomplete and this result cannot be changed.



Lab 19: Assisted Lab: Configure Remote Access

30 minutes (+3x15ext)

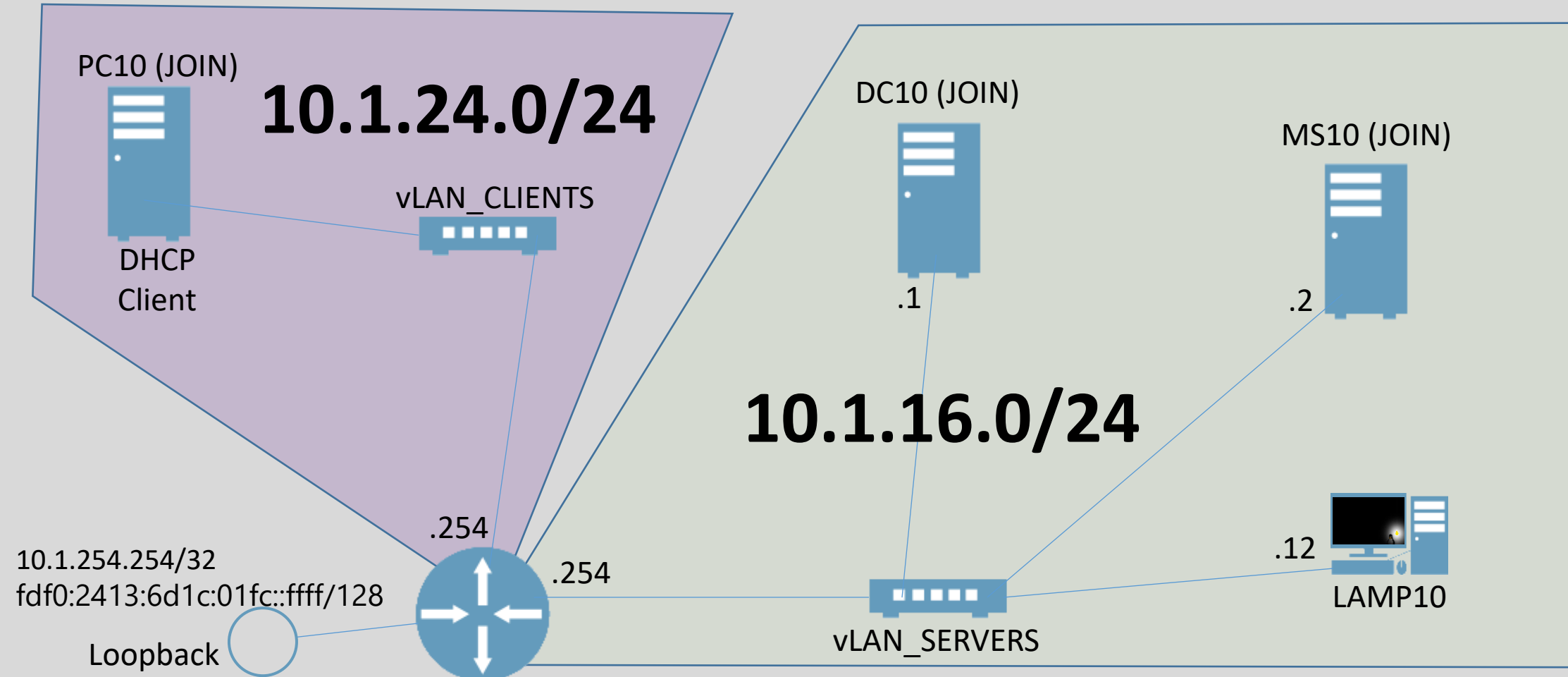
To complete this task, configure an IPsec policy that requires a client (PC10) to establish a secure connection with a server (MS10). IPsec policies can be enabled to encrypt connections between systems, whether on an internal LAN or a VPN connection. The principle is the same in both cases. A zero-trust model ensures that all communications between servers or between servers and clients is authenticated, authorized, and encrypted. This type of model depends heavily on the use of digital certificates to identify each host. Certificates can be deployed along with Internet Protocol Security (IPsec) to meet some of the goals of zero trust.



Lab 20: Assisted Lab: Develop Network Documentation

25 minutes (+2x15ext)

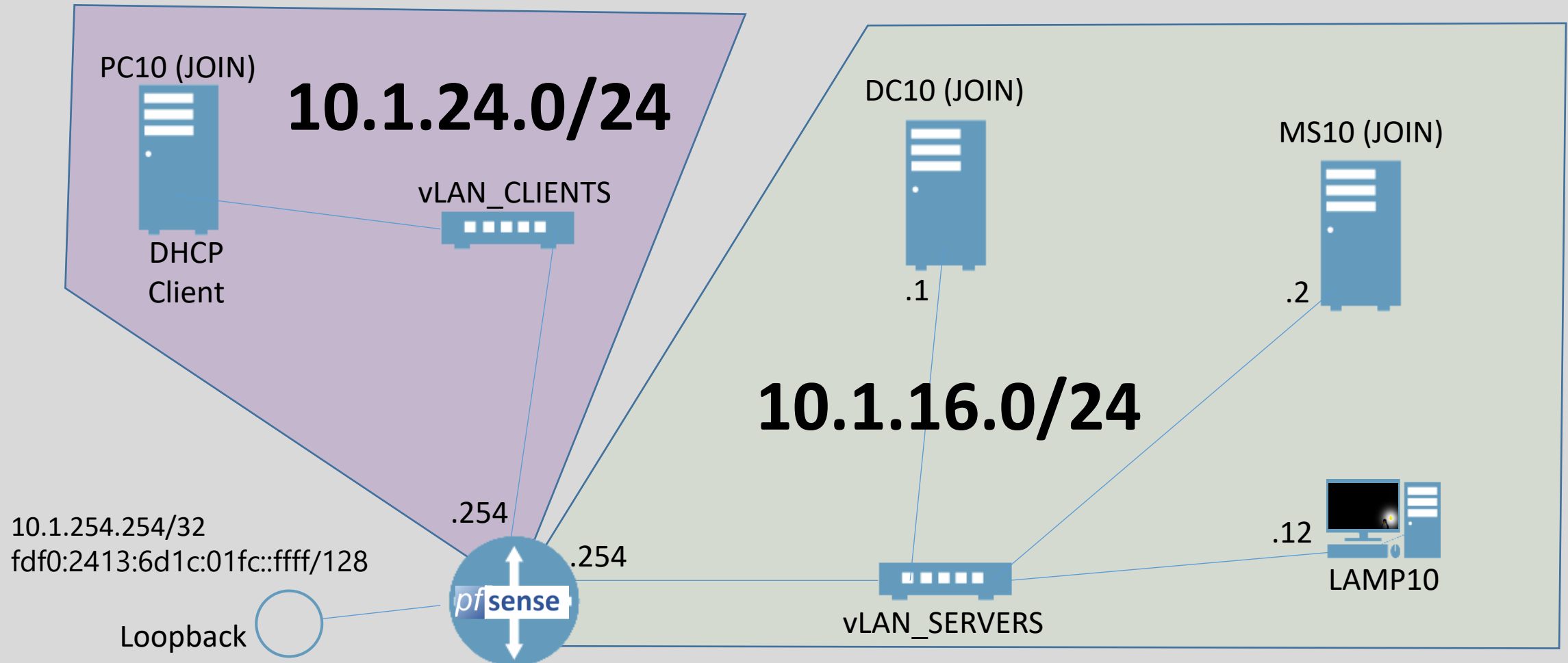
You will use various network and system tools to document hostnames, IP address configurations, DNS resource records, DHCP reservations, and other information for network hosts. You will also document configuration management information for Windows networks.



Lab 21: Assisted Lab: Backup and Restore Network Device Configuration

15 minutes (+2x15ext)

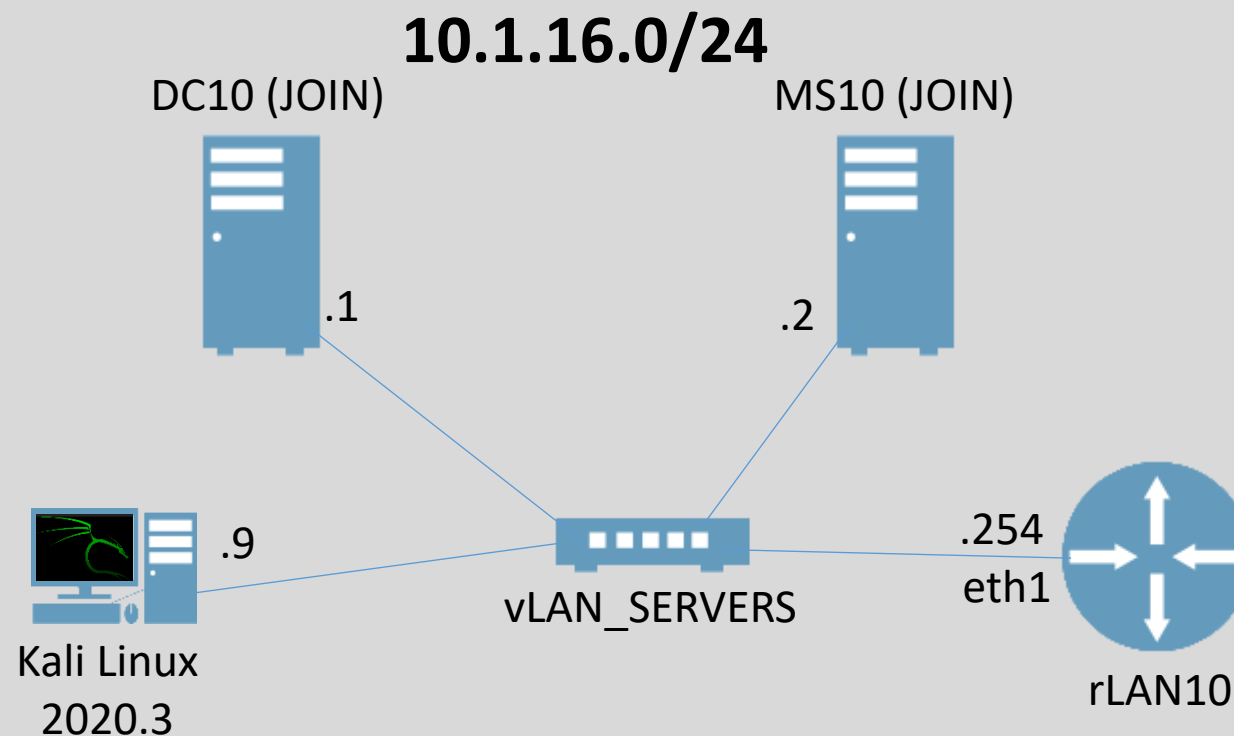
In this lab you will backup the configuration of the pfSense router. You will also backup the configuration of a Windows and a Linux web server. You will be asked to identify common disaster recovery terms.



Lab 22: Assisted Lab: Analyze an On-path Attack

15 minutes (+2x15ext)

Security penetration testing software can generate various network attacks. In this scenario, you will use a tool named Ettercap to perform an ARP spoofing or poisoning attack on the MS10 virtual machine. The attack will redirect packets away from the legitimate router interface to the attacker's own network interface. First you will document the MS10 server's MAC address. Next, you will configure the Man-in-the-Middle (MitM) attack and packet capture. You will then examine the captured packets. Finally, you will confirm the attack is over by checking MAC address information on MS10.



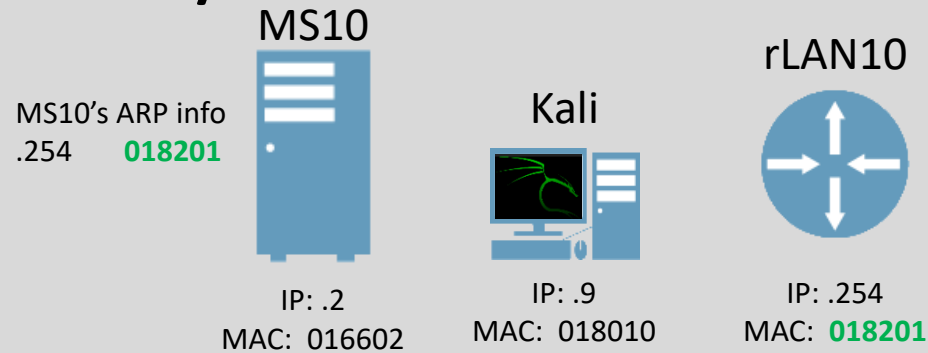
Next slide shows some context: ➡

Lab 22: A bit of context

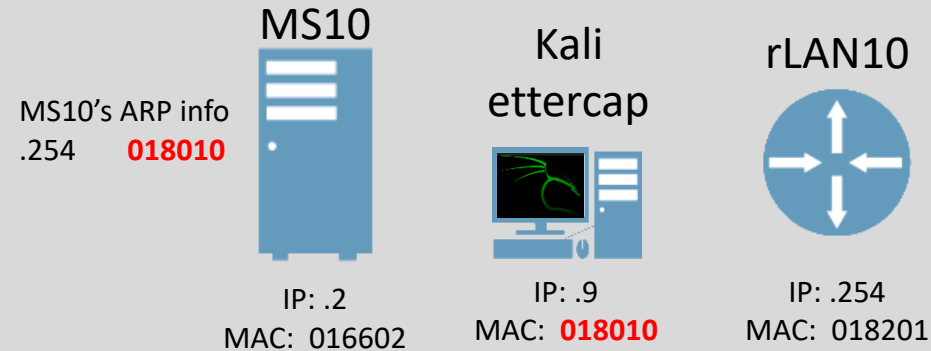
Network ID: 10.1.16.0/24

MAC OUI: 00155D

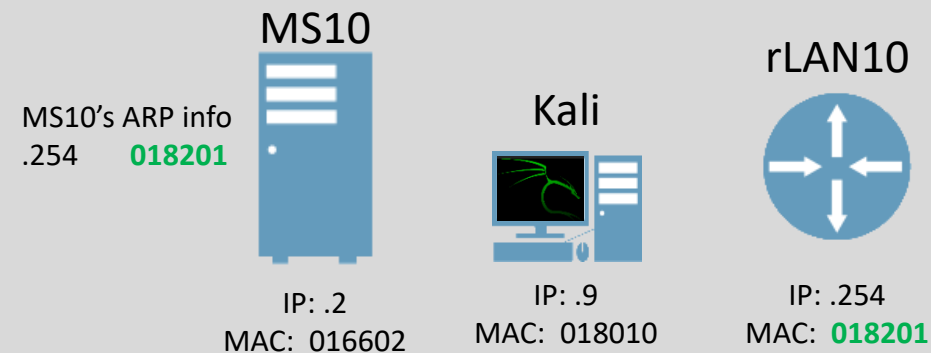
Network information
before the MitM attack



Network information
during the MitM attack



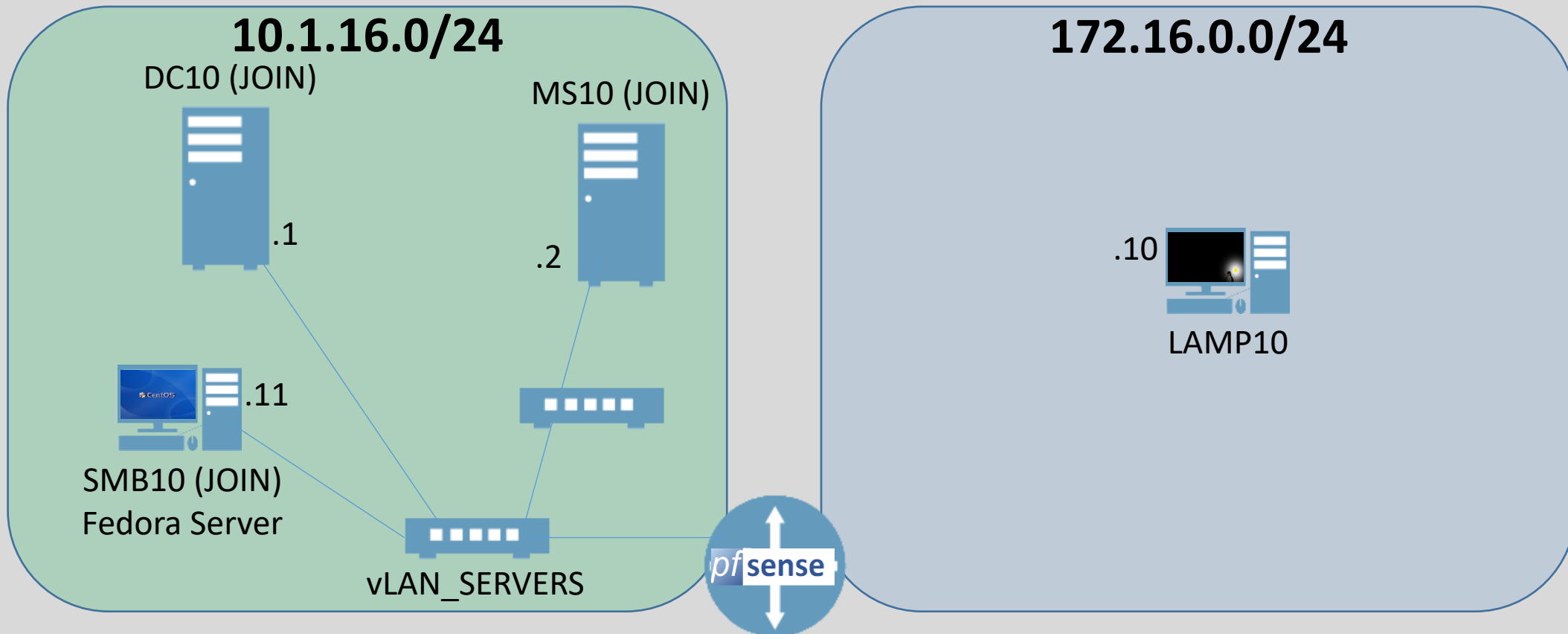
Network information
after the MitM attack
ends



Lab 23: Assisted Lab: Configure Port Security

15 minutes (+2x15ext)

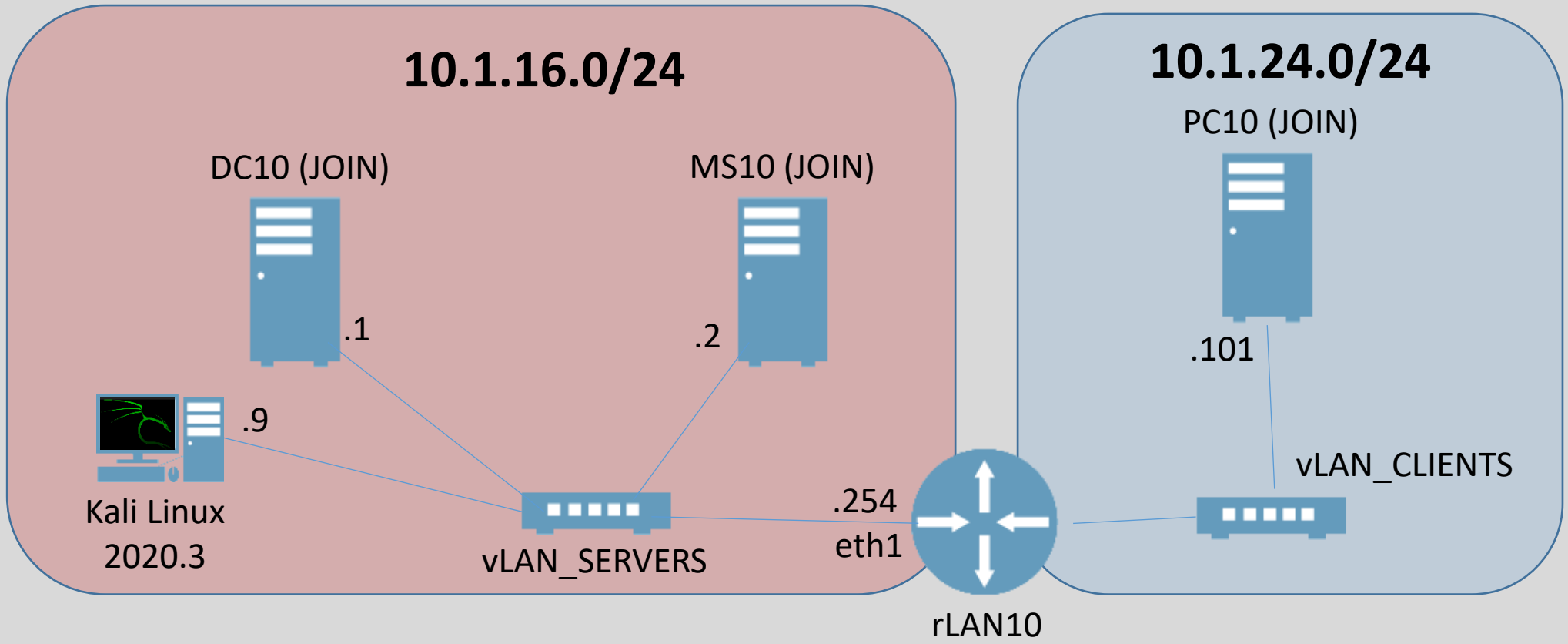
In this lab you will configure and test firewall settings for a router and a server.



Lab 24: Applied Lab: Troubleshoot Service and Security Issues

30 minutes (+3x15ext)

This is an applied lab where you will need to work more independently to complete the required tasks. Note that you may not retry grading attempts in this lab. Once you select the **Score** button for each task, the task will be evaluated as complete or incomplete and this result cannot be changed.



Go to: eval.interfacett.com

Choose this class from the drop-down list.

Select radio button of your choice and click next.

You are forwarded to the rest of the survey. Once there, choose this class (make sure it has MY name as the instructor) and do the remainder of the survey.

Click Next on each page then Submit on the last page to complete the survey.

You should receive a confirmation email from CompTIA early next week.

Audit policy: You can retake the class again up to a year for free. Replay is available for a year as well. You have access to the labs for 6 months. No exam vouchers unless you or (your company) purchased them at the time of class registration. ☹️

markj@interfacett.com blogs.interfacett.com

Thank you!!