The Future of Engineering Education
2024 Annual Conference & Exposition
Oregon Convention Center
Portland, OR . June 23 - 26, 2024
ASEE
Paper ID #43918

From Classroom to Career with Practical Network Training

Mr. Erwin Karincic, Virginia Commonwealth University

Erwin Karincic received B.S. and M.S. degrees in Computer Engineering from Virginia Commonwealth University (VCU) in 2020 and 2021, respectively. He is currently pursuing a Ph.D. degree from Virginia Commonwealth University. He is an experienced security researcher with focus on reverse engineering and exploit development. An avid learner in many different fields, his research interests are cyber security, reverse engineering, exploit development, Internet of Things, software defined radio, antenna analysis, and design. He currently holds 28 cyber security certifications.

Lauren Linkous, Virginia Commonwealth University

Lauren is with the College of Engineering at Virginia Commonwealth University in Richmond, Virginia. Her current research is in additive manufacturing, machine learning, computational electromagnetics, and optimization.

Dr. Erdem Topsakal, Virginia Commonwealth University

From Classroom to Career with Practical Network Training using Cisco Modeling Labs

The increasing demand for resilient and secure networks has become a critical concern in today's digital world. Due to a shortage of hands-on experience opportunities, a significant challenge is training students to acquire practical networking skills. While the foundational theory of networking is essential, ensuring that students are ready for the workforce necessitates proficiency in the actual design and implementation of networks. To bridge this gap, it is imperative to provide students with opportunities to practice in a real-world context. Educational institutions often possess physical networking equipment, however it is generally expensive to operate, requires maintenance to reset it for different labs, and often requires outside support in cases where Virtual Private Network (VPN) is allowed for remote access. This paper introduces a solution to these challenges by incorporating a flexible platform that emulates real networking software and allows students to practice at any time from any location. Cisco Modeling Labs (CML) for Education was selected as the platform to support the proposed curricula environment. CML is the only commercial platform that offers official Cisco software and seamless integration with various operating systems hosted in virtual machines (VMs). CML server deployment options are versatile, allowing installations on school servers, Amazon Web Services (AWS) cloud, and even hosted individually on student computers. Students can then access these training tools with any browser, further reducing the barrier to entry.

In this paper, we detail the development and delivery of practical lab exercises that cover the entire network lifecycle, including network design, configuration, and troubleshooting using CML. We provide preconfigured labs that are meant for easy integration into any networking class. These labs involve designing parts of the network to satisfy a set of requirements and troubleshooting network issues. Educators can further expand on these labs by modifying them to meet requirements based on their coursework. We also provide labs that teach cybersecurity concepts where students learn to build, demonstrate, and mitigate cyberattacks, gaining comprehensive knowledge of network security. Integrating the physical Internet of Things (IoT) devices is also explored, furthering the knowledge needed to interface with IoT devices. The purpose of this paper is to provide educators with an effective alternative to physical networking equipment and provide a comprehensive set of custom labs that can be integrated in their curriculum. The practical labs presented in this paper provide students at high school, college, or professional level with skills and knowledge required for the modern digital workforce.

Introduction

It is widely accepted that there exists a growing need for practical networking skills amidst a shortage of hands-on experience opportunities for students, and that this issue is exacerbated by resource shortages, staff shortages, domain knowledge constraints, and limited options for safe, practical ways for students to practice infrastructure skills [1, 2, 3]. To support current educational needs, Simulation Based Experiential Learning, or Simulation Based Learning (SBL) has been implemented in classrooms globally. SBL is an educational approach where learners engage with simulated environments or scenarios to acquire knowledge, practice skills, and gain experience in a safe and controlled setting. These simulations mimic real-world situations, allowing learners to explore, experiment, and make decisions without real-life consequences. Practicing in safe, interactive learning resources that provide immediate feedback to students also reduces the barrier to entry by allowing students access to repeatable, reproducible practice and a flexible learning environment. Courses implementing SBL can either implement it as units into an existing curriculum to reinforce more traditional instruction, or integrate it into existing material. Studies such as [1, 4] note that there is an increase in meeting lab-based learning outcomes when SBL is implemented, which suggests improvement in acquiring practical skills and knowledge. However, actual implementation of SBL in the classroom has been broad as courses are adapted to keep up with a rapidly evolving technology. In [2], multiple simulation tools, including Graphical Network Simulator 3 (GNS3), Optimized Network Engineering Tool (OPNET), NETSIM, and Network Simulator (NS-2/NS-3), but primarily Cisco Packet Tracer, are discussed. [2] found in review that almost 39% percent of papers with methods for teaching computer networks used Cisco Packet Tracer in some capacity. The usefulness of these tools in active learning cannot be understated, but they were found to primarily focus on simulations of tasks rather than recreating an environment. To address this, we propose the use of Cisco Modeling Labs (CML) for Education, a flexible platform that emulates real networking software, enabling students to practice from any location at any time.

Cisco Packet Tracer is a network simulation and visualization tool that allows users to design, configure, and simulate network topologies, and is often used in conjunction with the Cisco Networking Academy program for teaching basic network concepts. CML is intended to be realistic and it is used for designing, testing, and validating complex network designs in real-world scenarios. Packet Tracer simulates some of the most commonly used features of network devices, but CML uses actual network images used by network devices, providing the same feature set as representative devices. It allows users to create highly customizable and scalable network simulations to model real-world network environments. While Packet Tracer has been traditionally marketed towards students, educators, and entry level network professionals who are learning or teaching networking fundamentals, the community around CML and the available teaching resources have expanded such that a shift to CML is almost unavoidable in order to keep pace with today’s technological needs. Packet Tracer is also optimized for small to medium-sized network simulations and may not be suitable for modeling large-scale or enterprise-grade network deployments. CML is more accessible than ever to students and educators and it is designed to handle professional-grade education needs, including simulating enterprise-sized networks with complex interconnections.

CML is used both professionally and to support research with several of the aforementioned networking tools [5-8]. Originally, CML existed alongside Virtual Internet Routing Lab (VIRL) where CML was used for Enterprise simulations and VIRL was used for personal use. In April 2020, the release of CML 2.0 was a major update which included an updated platform [9]. At the same time, VIRL was deprecated and CML 2.0 Personal replaced VIRL which included the updated platform with concurrent 20 node resource limitation. Enterprise and educational versions do not have associated resource limitations. Prior research highlighting VIRL as a tool for network simulations remains relevant [7, 8], now enhanced by the substitution of CML for VIRL. Educational references may refer to either CML or VIRL, or both. In a classroom implementation, both VIRL and CML have been used with success. Preferences for CML, VIRL, or packet tracer largely rely on existing infrastructure, service familiarity, and legacy software or implementation [1-8, 10]. Criticisms of using CML in the classroom are largely limited to general critique of simulation-based learning; when hands-on education is possible, educators and students would prefer that method, but in many cases major barriers to acquisition and management of physical infrastructure make it so that the choice is between using simulations or nothing at all [10, 11]. However, CML additionally lowers the barrier to access because it can be used to model enterprise and complicated networks, which is increasingly important for students as real-world networking needs become more complicated.

To demonstrate the use of CML, this paper presents the development and delivery of 13 practical lab exercises compatible with explicit objectives covering network design, configuration, troubleshooting, cybersecurity concepts, and IoT device integration. These preconfigured labs aim to provide educators with an effective alternative to physical networking equipment, empowering students with the skills needed for the modern digital workforce. The presented labs cover several common networking concepts that can be explored in class as part of a series of hands-on lectures or assigned for designated lab assignments outside of lecture. To do this, each lab is presented with a description of the activity including the tasks that students will perform to complete the lab, and several learning outcomes. The labs, and their learning outcomes, are designed with the 5 elements described by the SMART mnemonic [12] - Specific, Measurable, Attainable, Relevant, and Time-bound - in mind. The labs are designed to cover specific topics, with measurable and attainable success markers. Students, and educators, know what to expect for each lab, and there is a clear end point to the exercise. Additionally, each lab can be completed in one sitting to improve retention and the ability to revisit materials. As the preconfigured labs are ‘live’ in a virtual machine, students are able to review concepts at their own pace, including pursuing additional experimentation, without the requirement of expensive networking equipment. While the labs are presented in a sequence with increases in network design complexity, the concepts in the labs are designed to reinforce each other and there is no set sequence in which to introduce the labs to students.

To address the evolving landscape of network technology and the continued need for adaptable educational approaches in regards to network training, this paper proposes a solution through the use of CML. Traditional training using physical networking hardware has been foundational, but faces challenges with the rapid pace of technological advancements, necessitating costly physical hardware updates. As previously described, CML offers a virtual platform that is adaptable for new technologies. Furthermore, the flexibility of CML's deployment options enhances its accessibility. It can be installed on local servers and deployed in the cloud on Amazon Web Services (AWS) ensuring that practical network training is available anywhere at any time. Important to course curricula, CML allows for the creation of complex labs and the flexibility of incorporating minor adjustments to existing labs to provide a variety of learning experiences. For educators, its modular nature means educational content can be developed for any network topology. Importantly, older material and network topologies can be adopted into CML to cover legacy networks or previous course material. The customizable, preconfigured labs in this paper cover a large set of network technologies, all of which can be customized to meet different course requirements, and updated to stay recent with technological advances.

The selection of CML is justified by its exclusive endorsement from Cisco for using their proprietary images within a virtual environment. This distinction not only secures legal compliance but also ensures users have access to the latest and most authentic networking software. CML offers several licensing models including a Personal license available for $200 and an Educational license that benefits from significant discounts for educational organizations [13]. The primary reasons for the selection of CML over alternative network simulators such as EVE-NG, GNS3, Packet Tracer, and NetSim are the rights to proprietary network images which simulate actual network devices running representative operating systems.

As part of the discussion on usage and features, the paper will guide readers through the processes of installing CML on both local servers and the AWS cloud. It will then provide in-depth information regarding the preconfigured labs highlighting their structure and objective. These labs showcase the platform’s capabilities and its suitability for enhancing network education.

Installation

Cisco Modeling Labs (CML) has several options for deployment within the educational environment [14], allowing for flexibility in course material based on the available resources. The deployment methods are as follows:

- Virtual Machine (VM) Deployment
    - This is the recommended deployment for local servers running a virtualization platform such as VMWare ESXi and VMWare Workstation.
- Cloud Amazon Web Services (AWS) Deployment
    - This is the recommended deployment for educational organizations using AWS which allow worldwide access without the need for local hardware.

- Bare Metal Deployment
    - Although available, this deployment method is not recommended as it is only supported on very specific servers – Cisco UCS C220 and C240 models.

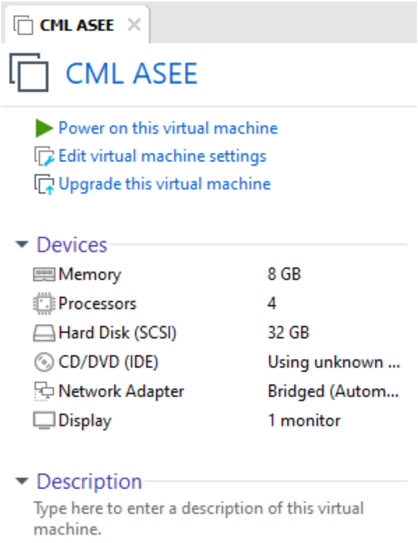
Both VM Deployment and AWS Deployment are recommended due to their adaptability and versatility to various educational environments. VM Deployment provides ease of integration within existing IT infrastructure and allows rapid provisioning and scaling of resources, including clustering of servers, to meet varying demands of class sizes and complexity of network simulations while keeping the cost down. AWS provides the highest scalability and flexibility with worldwide access, but it does have higher cost when compared to VM deployments.

In this paper, we will showcase VM deployment on VMWare Workstation and AWS Deployment, illustrating their practical usage within an educational setting.

VM Deployment

The VM Deployment requires the *CML controller* OVA file and the *rfplat* ISO file that contains all of the reference platforms. These reference platforms include a variety of Cisco system images and open-source system images that are licensed for use within the CML platform outlined in Appendix A. These files are available for download on the page provided by the vendor.

Deploying CML on VMWare Workstation begins by opening the OVA file [15], which has specific default settings as shown in Fig. 1. Prior to starting the VM, certain settings need to be adjusted: Intel Virtualization needs to be enabled, the disk size needs to be expanded to at least 50 GB, and the CD needs to be configured to reference the rfplat ISO file as shown in Fig. 2. These settings are the minimum required settings to run CML and they should be adjusted depending on the size and complexity of topologies used by the labs. Initial startup of the VM will initiate the installation process, which includes creation of system and user interface accounts, followed by copying of the reference platforms from the CD to the local VM as illustrated in Fig. 3. Once the reference platforms are copied, the installation process is complete and the IP address will be shown on the screen, which can be accessed as in Fig. 4, and once users log in, they will see the page in Fig. 5. The final step of deployment is to appropriately license the CML instance.



CML ASEE

CML ASEE

- Power on this virtual machine
- Edit virtual machine settings
- Upgrade this virtual machine

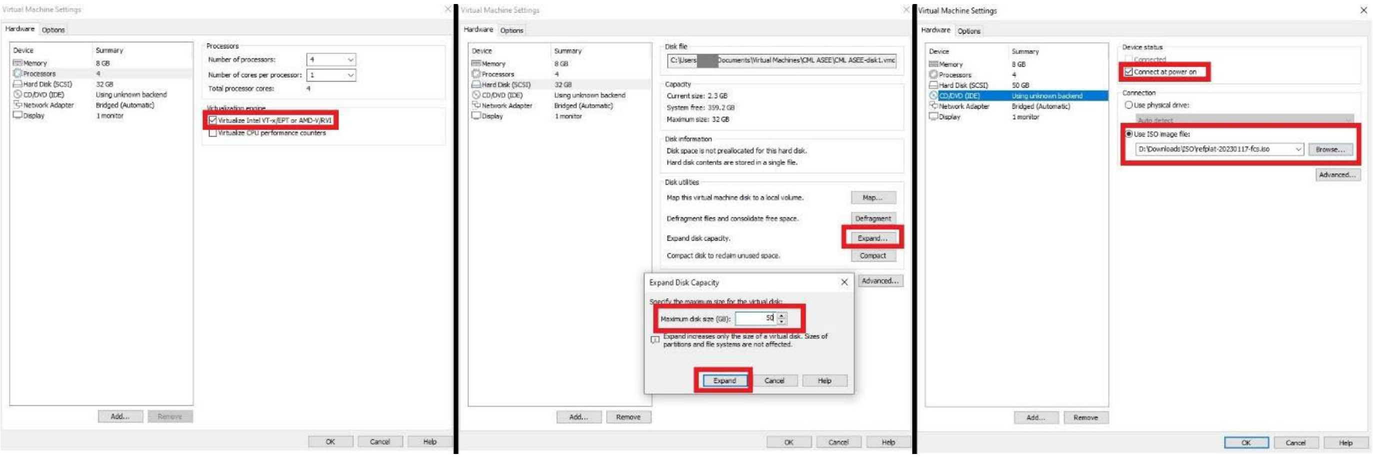
Devices

Memory	8 GB
Processors	4
Hard Disk (SCSI)	32 GB
CD/DVD (IDE)	Using unknown ...
Network Adapter	Bridged (Autom...
Display	1 monitor

Description

Type here to enter a description of this virtual machine.

Figure 1. VMWare Workstation initial settings after import of the CML instance.



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (SCSI)	32 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	Bridged (Automatic)
Display	1 monitor

Processors

Number of processors: 4

Number of cores per processor: 1

Total processor cores: 4

Virtualization engine

☑ Virtualize Intel VT-x/EPT or AMD-V/RVI

□ Virtualize CPU performance counters

Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (SCSI)	32 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	Bridged (Automatic)
Display	1 monitor

Disk file

C:\Users[redacted]Documents\Virtual Machines\CML ASEE\CML ASEE-disk1.vmc

Capacity

Current size: 2.3 GB

System free: 359.2 GB

Maximum size: 32 GB

Disk information

Disk space is not preallocated for this hard disk.

Hard disk contents are stored in a single file.

Disk utilities

Map this virtual machine disk to a local volume.

Defragment files and consolidate free space.

Expand disk capacity.

Compact disk to reclaim unused space.

Expand Disk Capacity

Specify the maximum size for the virtual disk:

Maximum disk size (GB): 50

Expand increases only the size of a virtual disk. Sizes of partitions and file systems are not affected.

Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	8 GB
Processors	4
Hard Disk (SCSI)	50 GB
CD/DVD (IDE)	Using unknown backend
Network Adapter	Bridged (Automatic)
Display	1 monitor

Device status

□ Connected

☑ Connect at power on

Connection

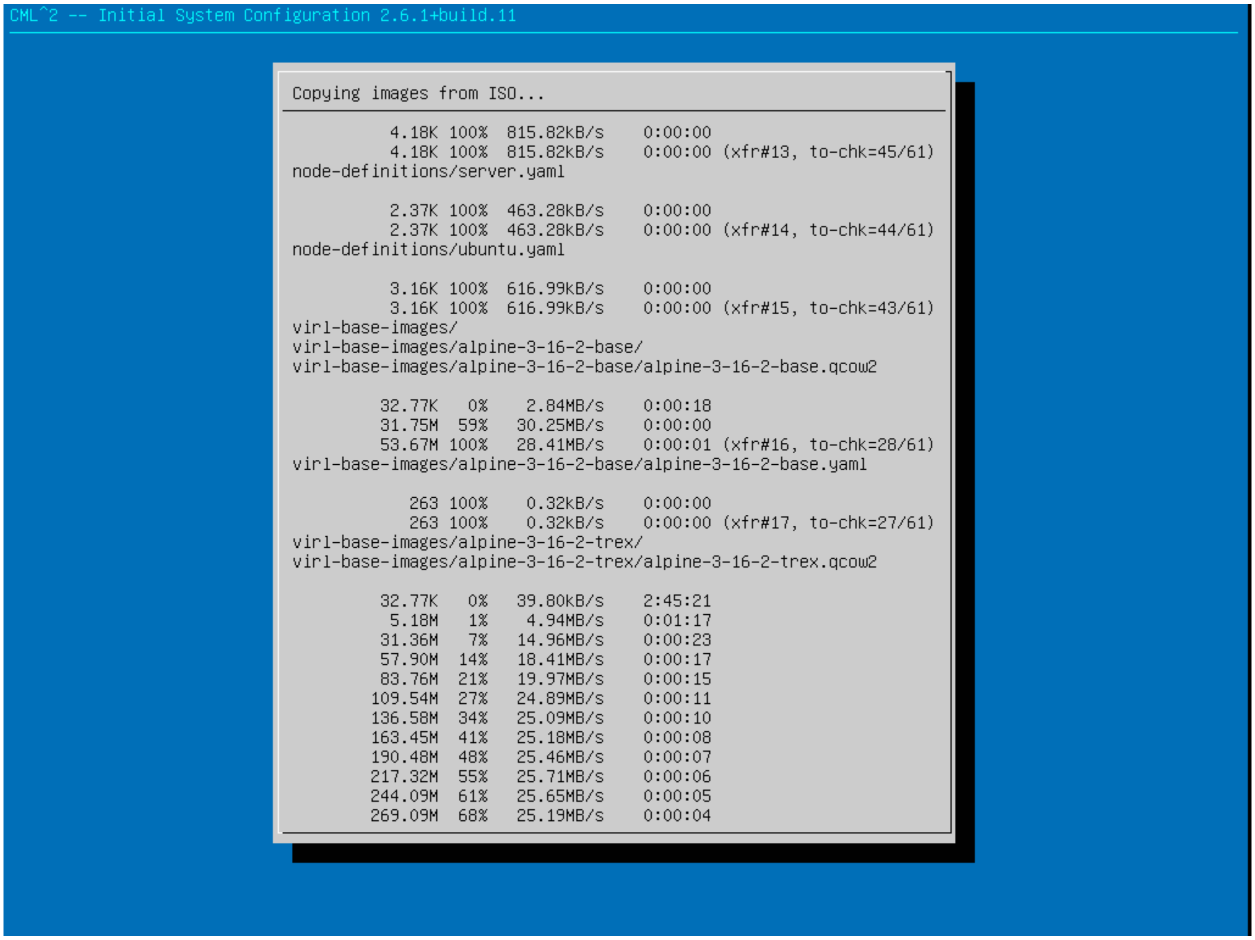
○ Use physical drive:

Auto detect

● Use ISO image file:

D:\Downloads\ISO\refplat-20230117-fcs.iso

Figure 2. VMWare Workstation modifications of Intel Virtualization, disk expansion, and CD drive configuration with rfplat ISO file.



```
CML^2 -- Initial System Configuration 2.6.1+build.11

Copying images from ISO...

          4.18K 100%  815.82kB/s    0:00:00
          4.18K 100%  815.82kB/s    0:00:00 (xfr#13, to-chk=45/61)
node-definitions/server.yaml

          2.37K 100%  463.28kB/s    0:00:00
          2.37K 100%  463.28kB/s    0:00:00 (xfr#14, to-chk=44/61)
node-definitions/ubuntu.yaml

          3.16K 100%  616.99kB/s    0:00:00
          3.16K 100%  616.99kB/s    0:00:00 (xfr#15, to-chk=43/61)
virl-base-images/
virl-base-images/alpine-3-16-2-base/
virl-base-images/alpine-3-16-2-base/alpine-3-16-2-base.qcow2

         32.77K   0%    2.84MB/s    0:00:18
         31.75M  59%   30.25MB/s    0:00:00
         53.67M 100%   28.41MB/s    0:00:01 (xfr#16, to-chk=28/61)
virl-base-images/alpine-3-16-2-base/alpine-3-16-2-base.yaml

            263 100%    0.32kB/s    0:00:00
            263 100%    0.32kB/s    0:00:00 (xfr#17, to-chk=27/61)
virl-base-images/alpine-3-16-2-trex/
virl-base-images/alpine-3-16-2-trex/alpine-3-16-2-trex.qcow2

         32.77K   0%   39.80kB/s    2:45:21
          5.18M   1%    4.94MB/s    0:01:17
         31.36M   7%   14.96MB/s    0:00:23
         57.90M  14%   18.41MB/s    0:00:17
         83.76M  21%   19.97MB/s    0:00:15
        109.54M  27%   24.89MB/s    0:00:11
        136.58M  34%   25.09MB/s    0:00:10
        163.45M  41%   25.18MB/s    0:00:08
        190.48M  48%   25.46MB/s    0:00:07
        217.32M  55%   25.71MB/s    0:00:06
        244.09M  61%   25.65MB/s    0:00:05
        269.09M  68%   25.19MB/s    0:00:04
```

Figure 3. CML status page during copying of reference images to the local VM.

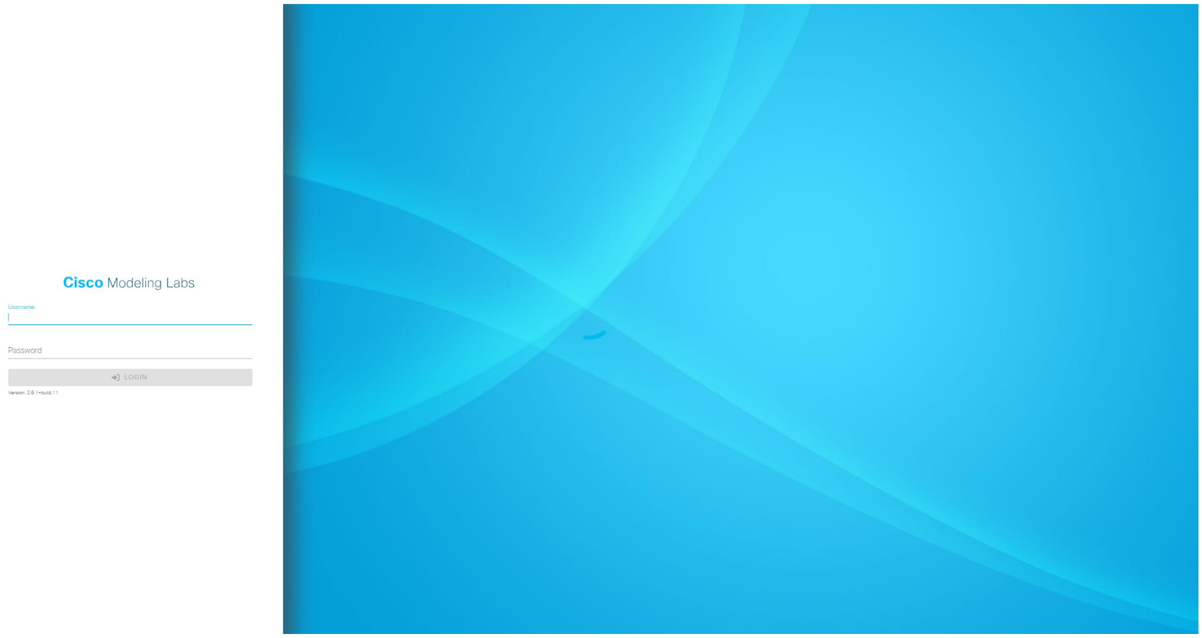


Figure 4. CML User Interface page.

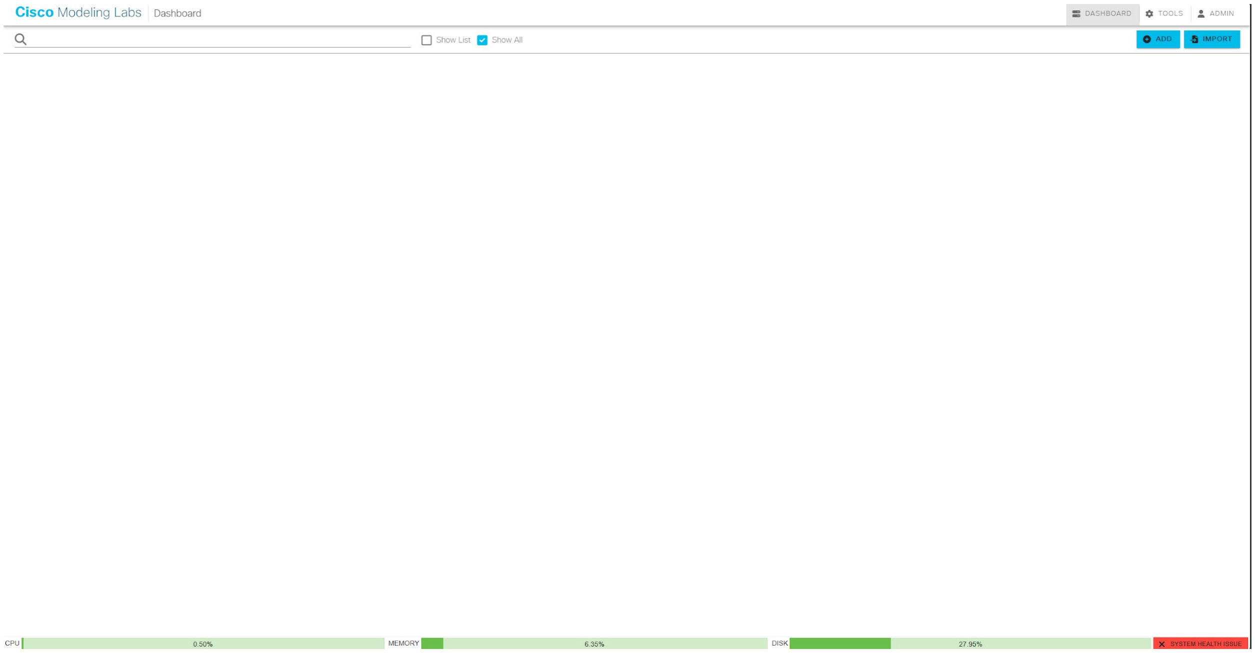


Figure 5. CML User Interface page after login.

Cloud AWS Deployment

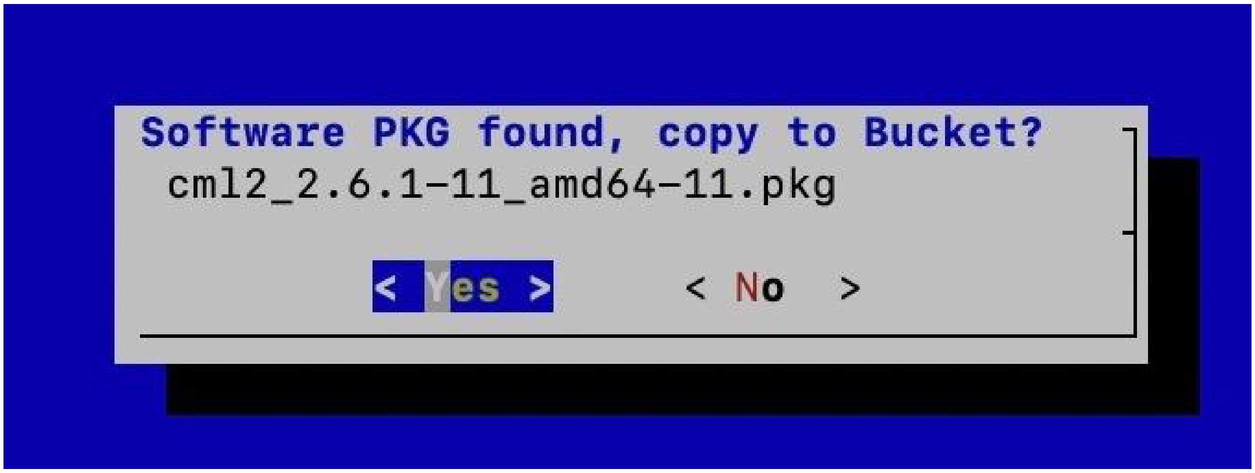
The AWS Deployment of CML leverages Terraform, an open-source ‘infrastructure as code’ software that enables provisioning of infrastructure [16]. This allows for the automated setup of various AWS cloud services needed for deploying CML. The prerequisite for this deployment is a set of comprehensive permissions within AWS Identity and Access Management (IAM) including the creation of new policies and groups. These groups and policies are assigned appropriate permissions needed to programmatically deploy CML in the most secure manner. While Cisco DevNet has developed Terraform scripts for creating the CML instance in AWS, these scripts do not automate the initial setup of required permissions [17]. This remains a manual process which can be a barrier to entry without comprehensive AWS knowledge. Addressing this gap, the paper introduces an additional Terraform script that automates the creation of these permissions, reducing the manual steps and potential errors.

Included within the repository [18] are the updated scripts, including the aforementioned Terraform script, and the entire detailed process of CML deployment. The setup of automated permissions within AWS starts by defining an SSH key used for securely connecting to the new CML instances and defining the name for an S3 bucket used for storing reference platforms. Users then provide their own AWS programmatic credentials and execute the Terraform script which executes following actions:

- Creates IAM user
- Creates IAM group
- Assigns IAM user to the group
- Creates an S3 bucket for node images
- Defines S3 policy that allows uploading, downloading, and listing files in the bucket
- Associates IAM policy with the S3 policy
- Creates IAM role that associates IAM policy with S3 access
- Associates EC2 full access policy to the IAM group
- Associates S3 access policy to the IAM group
- Creates a PassRole policy that allows passing of the IAM role to the EC2 instance
- Assigns the PassRole policy to the IAM group
- Associates generated SSH key with all provisioned EC2 instances
- Generates Access Key and Secret Key from the IAM user and stores it in a .csv file

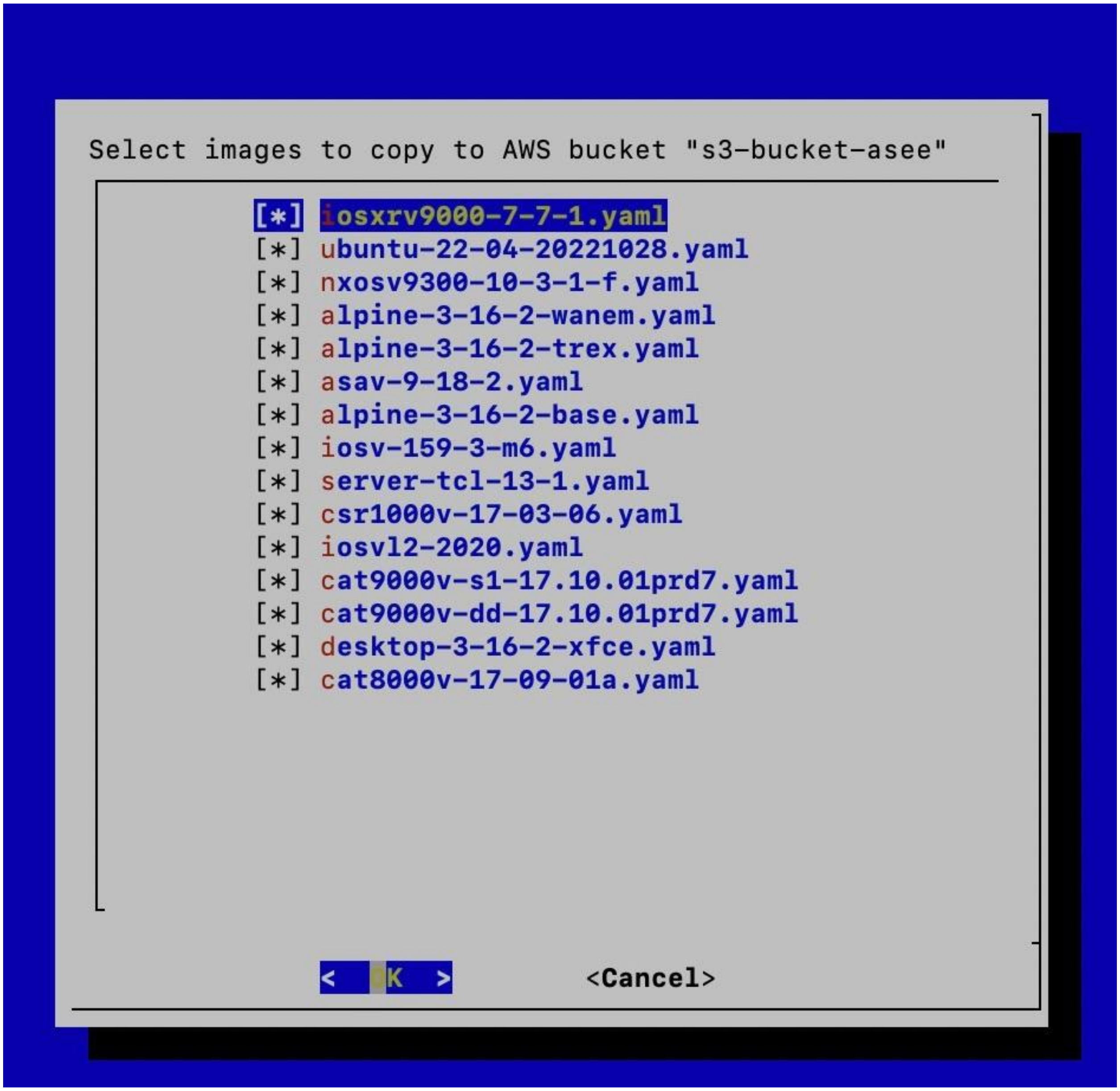
Following the permission setup, a script is used to upload reference platforms from the refplat ISO, which is compatible with both Linux and MacOS systems. The script starts a dialog confirming the upload of CML binary as shown in Fig. 6, followed by a selection screen for image uploads, Fig. 7, where all images are suggested to be uploaded. Progress is visually displayed during the upload process, shown in Fig. 8.

The final stage involves using Cisco DevNet provided Terraform script to finalize CML deployment. Once the process is complete, CML can be accessed by the given IP address with the output web page as shown in Fig. 4, and when using configured credentials, Fig. 5 is the screen that authenticated users see.



```
Software PKG found, copy to Bucket?
 cml2_2.6.1-11_amd64-11.pkg
```

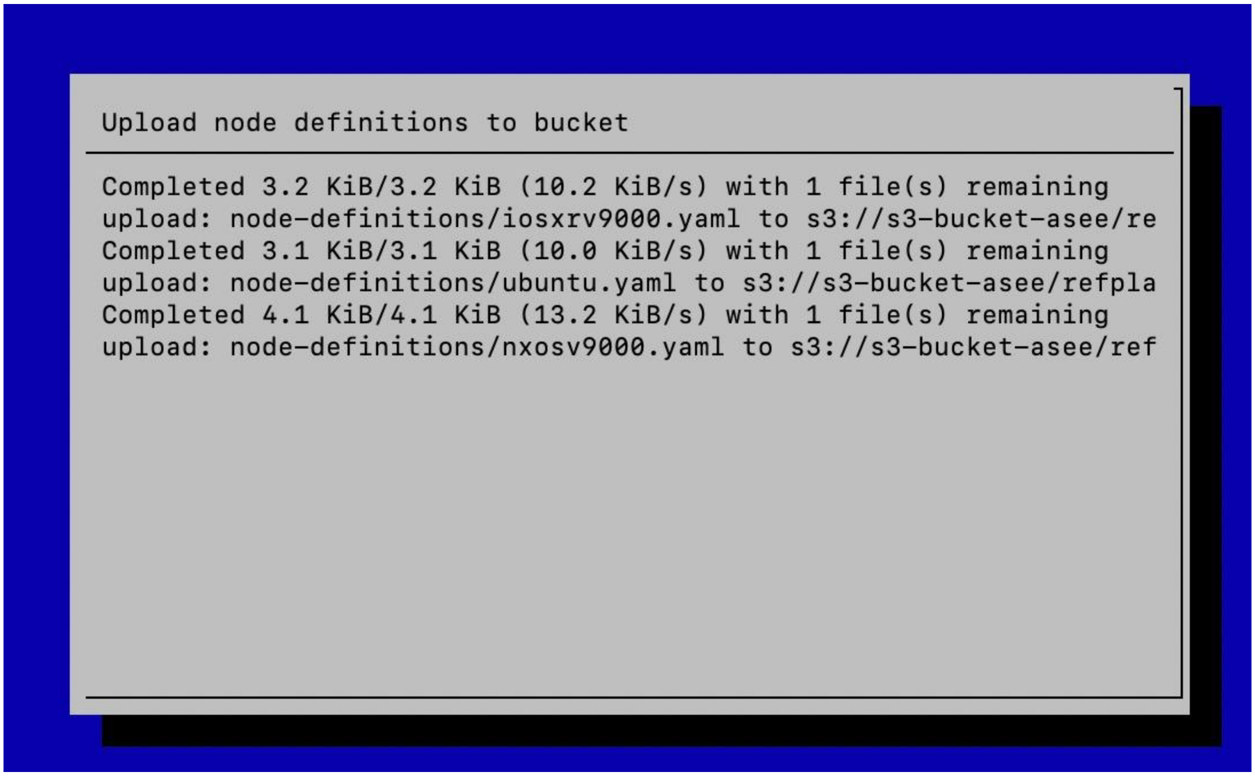
Figure 6. AWS S3 upload dialog regarding CML installation file.



```
Select images to copy to AWS bucket "s3-bucket-asee"

          [*] iosxrv9000-7-7-1.yaml
          [*] ubuntu-22-04-20221028.yaml
          [*] nxosv9300-10-3-1-f.yaml
          [*] alpine-3-16-2-wanem.yaml
          [*] alpine-3-16-2-trex.yaml
          [*] asav-9-18-2.yaml
          [*] alpine-3-16-2-base.yaml
          [*] iosv-159-3-m6.yaml
          [*] server-tcl-13-1.yaml
          [*] csr1000v-17-03-06.yaml
          [*] iosvl2-2020.yaml
          [*] cat9000v-s1-17.10.01prd7.yaml
          [*] cat9000v-dd-17.10.01prd7.yaml
          [*] desktop-3-16-2-xfce.yaml
          [*] cat8000v-17-09-01a.yaml
```

Figure 7. AWS S3 upload dialog regarding individual platforms.



```
Upload node definitions to bucket

Completed 3.2 KiB/3.2 KiB (10.2 KiB/s) with 1 file(s) remaining
upload: node-definitions/iosxrv9000.yaml to s3://s3-bucket-asee/re
Completed 3.1 KiB/3.1 KiB (10.0 KiB/s) with 1 file(s) remaining
upload: node-definitions/ubuntu.yaml to s3://s3-bucket-asee/refpla
Completed 4.1 KiB/4.1 KiB (13.2 KiB/s) with 1 file(s) remaining
upload: node-definitions/nxosv9000.yaml to s3://s3-bucket-asee/ref
```

Figure 8. AWS S3 upload progress.

Labs

In this section, we will describe thirteen practical lab exercises that cover a variety of use cases supported by CML. These labs are fully functional and can be directly integrated into networking courses [19]. Each lab is independent and educators can easily change the order of the labs depending on their coursework goals. The configuration of each lab can easily be modified for additions and variations, if desired. CML with these labs can be installed on school servers running VMWare ESXi or WMWare Workstation as well as AWS cloud and then accessed by students using a web browser remotely. This reduces the barrier to entry as any web browser can access the labs. The following labs are presented in no particular order and can be re-ordered based on the requirements of networking classes.

1. DHCP Lab
2. VLAN Lab
3. RSTP Lab
4. Dual Stack IPv4 and IPv6 Lab
5. NAT Lab
6. VRRP Lab
7. OSPF Lab
8. Security ACL Lab
9. GRE + IPSec Lab

10. ASA IPSec Lab
11. Advanced OSPF Troubleshooting Lab
12. Security OSPF Takeover Lab
13. IoT Lab

DHCP Lab:

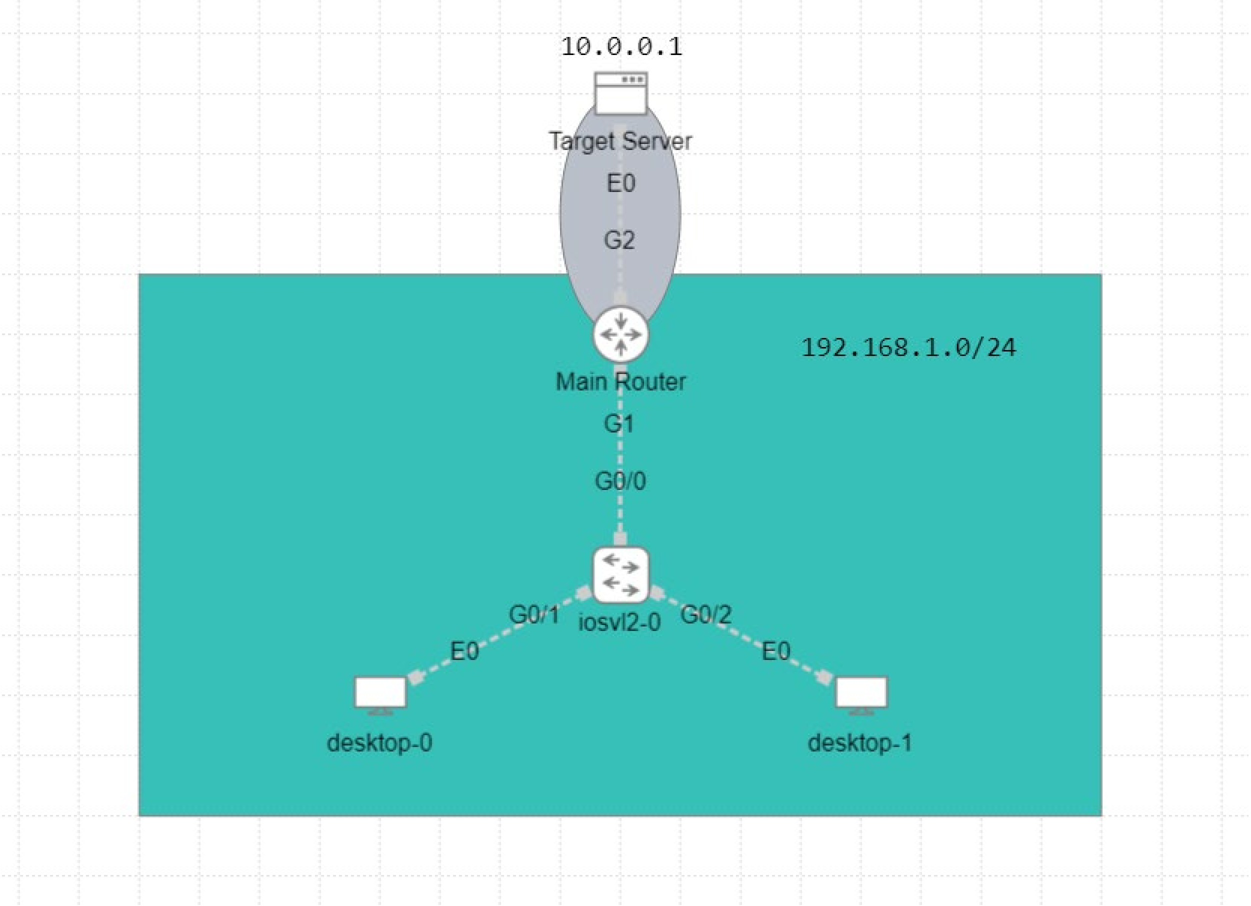


Figure 9. DHCP Lab with two desktops, a switch, Main Router, and a Target Server.

Description:

This lab is designed to teach the fundamentals of the Dynamic Host Configuration Protocol (DHCP). DHCP dynamically assigns IP addresses and other network configuration parameters to devices. This lab includes observing DHCP client and server interactions, including 4 DHCP messages: Discover, Offer, Request, and ACK messages.

Students will configure a DHCP server on the Main Router to offer dynamic network configuration for 192.168.1.0/24 network. The setup should enable Desktop 0 and Desktop 1 to obtain IP addresses from this DHCP server and maintain connectivity with the Target Server located at IP address 10.0.0.1.

CML offers a feature that supports packet capture on network links by clicking on a link and selecting ‘Packet Capture’ as shown in Fig. 10, which allows for observing network traffic in the CML web interface as shown in Fig. 11. In addition to using the web interface for analysis, captured packets can be downloaded in pcap form and analyzed in Wireshark as shown in Fig. 12.

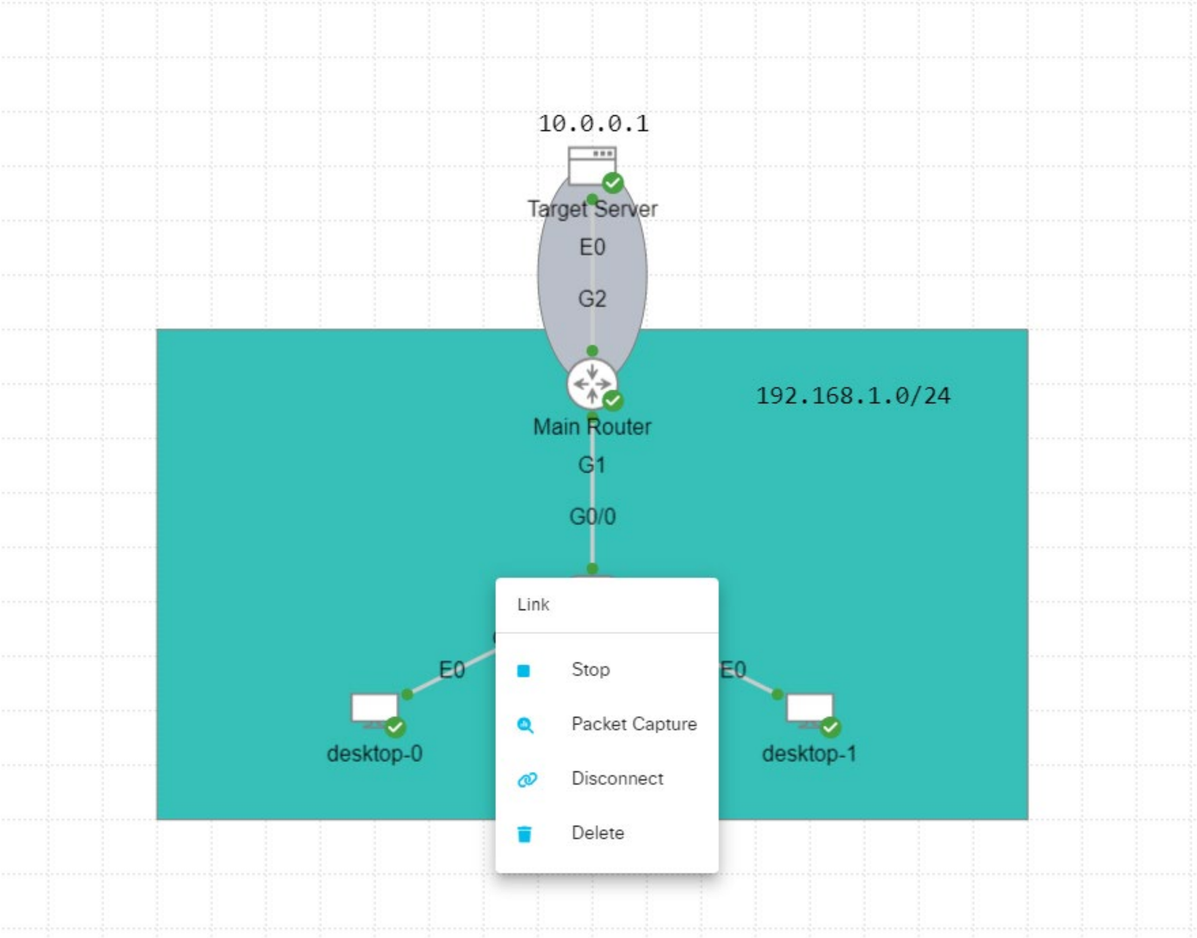
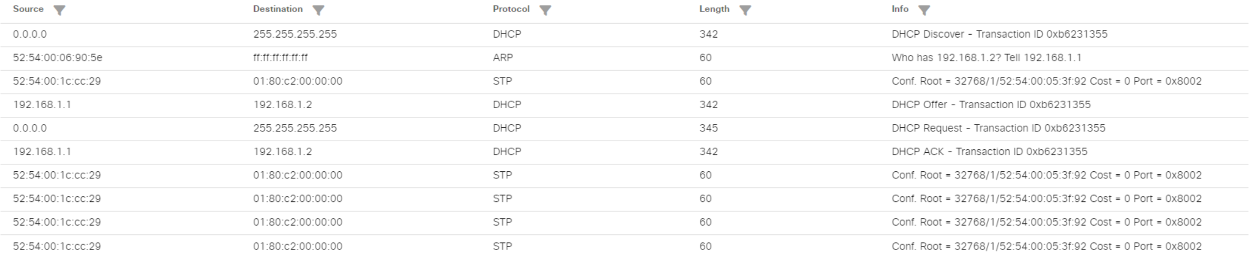
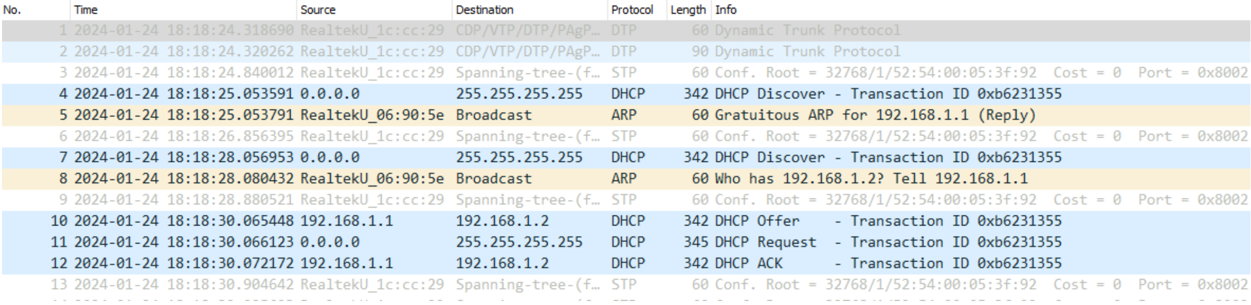


Figure 10. DHCP Lab Packet Capture dialog box.



Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb6231355
52:54:00:06:90:5e	ff:ff:ff:ff:ff:ff	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
52:54:00:1c:cc:29	01:80:c2:00:00:00	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
192.168.1.1	192.168.1.2	DHCP	342	DHCP Offer - Transaction ID 0xb6231355
0.0.0.0	255.255.255.255	DHCP	345	DHCP Request - Transaction ID 0xb6231355
192.168.1.1	192.168.1.2	DHCP	342	DHCP ACK - Transaction ID 0xb6231355
52:54:00:1c:cc:29	01:80:c2:00:00:00	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
52:54:00:1c:cc:29	01:80:c2:00:00:00	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
52:54:00:1c:cc:29	01:80:c2:00:00:00	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
52:54:00:1c:cc:29	01:80:c2:00:00:00	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002

Figure 11. DHCP Lab Packet Capture in CML.



No.	Time	Source	Destination	Protocol	Length	Info
1	2024-01-24 18:18:24.318690	RealtekU_1c:cc:29	CDP/VTP/DTP/PAgP…	DTP	60	Dynamic Trunk Protocol
2	2024-01-24 18:18:24.320262	RealtekU_1c:cc:29	CDP/VTP/DTP/PAgP…	DTP	90	Dynamic Trunk Protocol
3	2024-01-24 18:18:24.840012	RealtekU_1c:cc:29	Spanning-tree-(f…	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
4	2024-01-24 18:18:25.053591	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb6231355
5	2024-01-24 18:18:25.053791	RealtekU_06:90:5e	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.1 (Reply)
6	2024-01-24 18:18:26.856395	RealtekU_1c:cc:29	Spanning-tree-(f…	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
7	2024-01-24 18:18:28.056953	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb6231355
8	2024-01-24 18:18:28.080432	RealtekU_06:90:5e	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
9	2024-01-24 18:18:28.880521	RealtekU_1c:cc:29	Spanning-tree-(f…	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002
10	2024-01-24 18:18:30.065448	192.168.1.1	192.168.1.2	DHCP	342	DHCP Offer - Transaction ID 0xb6231355
11	2024-01-24 18:18:30.066123	0.0.0.0	255.255.255.255	DHCP	345	DHCP Request - Transaction ID 0xb6231355
12	2024-01-24 18:18:30.072172	192.168.1.1	192.168.1.2	DHCP	342	DHCP ACK - Transaction ID 0xb6231355
13	2024-01-24 18:18:30.904642	RealtekU_1c:cc:29	Spanning-tree-(f…	STP	60	Conf. Root = 32768/1/52:54:00:05:3f:92 Cost = 0 Port = 0x8002

Figure 12. DHCP Lab Packet Capture in Wireshark.

Learning Outcomes:

Upon completing this lab, students will gain an understanding of the Dynamic Host Configuration Protocol (DHCP) and its significance in dynamically assigning IP addresses and network configuration parameters. Through configuring, observing, and analyzing DHCP interaction, students will learn the necessary skills for ensuring devices within a network are appropriately configured with IP addresses and other essential network settings, preparing them for more complex network configuration and troubleshooting tasks.

VLAN Lab:

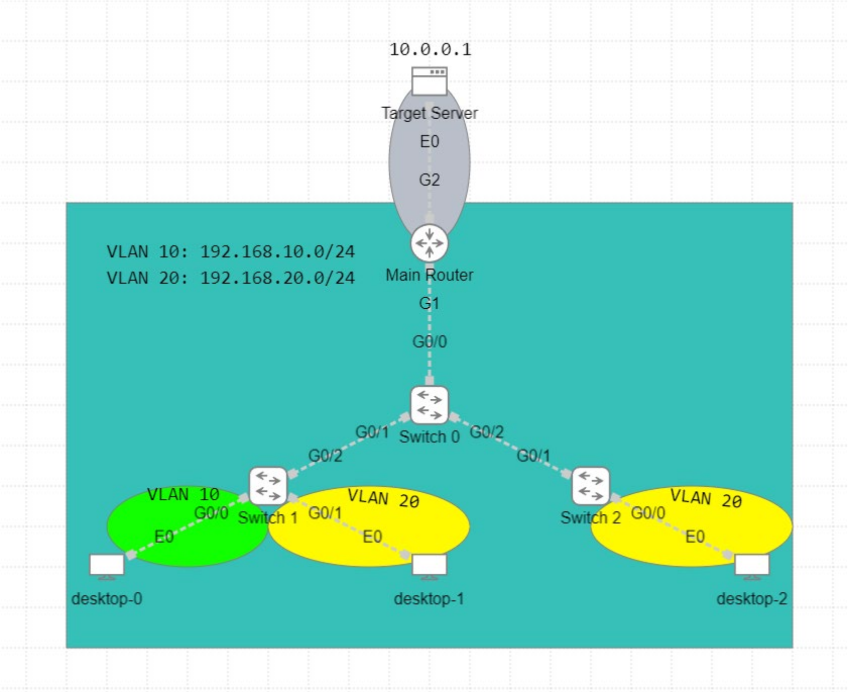


Figure 13. VLAN Lab with three desktops, three switches, Main Router, and a Target Server.

Description:

In this lab, we explore the concepts of Virtual Local Area Networks (VLANs) which logically separate physical networks as seen in Fig. 13.

Students will configure two VLANs, VLAN 10 and 20, across three switches. The configuration requires that Desktop 0 is assigned to VLAN 10 while Desktops 1 and 2 should be assigned in VLAN 20. Each switch interface connected to desktops must properly tag the traffic according to VLAN membership and preserve these tags across links between switches and the router. The Main Router should be configured with two subinterfaces correlating to each of the two VLANs. IP addresses need to be configured on all of the devices according to the network design with VLAN 10 configured for 192.168.10.0/24 network and VLAN 20 for 192.168.20.0/24 network. Successful configuration will enable every desktop to communicate with Target Server at 10.0.0.1, as well as every other desktop. For students seeking extra credit, configuring Access Control List (ACL) on the Main Router to block inter-VLAN communication will restrict desktops to reaching desktops in other VLANs while still being able to reach the Target Server.

Learning Outcomes:

Upon completing this lab, students will develop a foundational understanding of how Virtual Local Area Networks (VLANs) operate within network infrastructure, learning to configure and manage VLANs to enhance network segmentation and security. Students will acquire the skills necessary to effectively assign devices to VLANs, manage traffic tagging on switch interfaces and set up routing to facilitate communication across segmented networks. Students will demonstrate their competence in creating network configurations that support both restricted and unrestricted communication paths.

RSTP Lab:

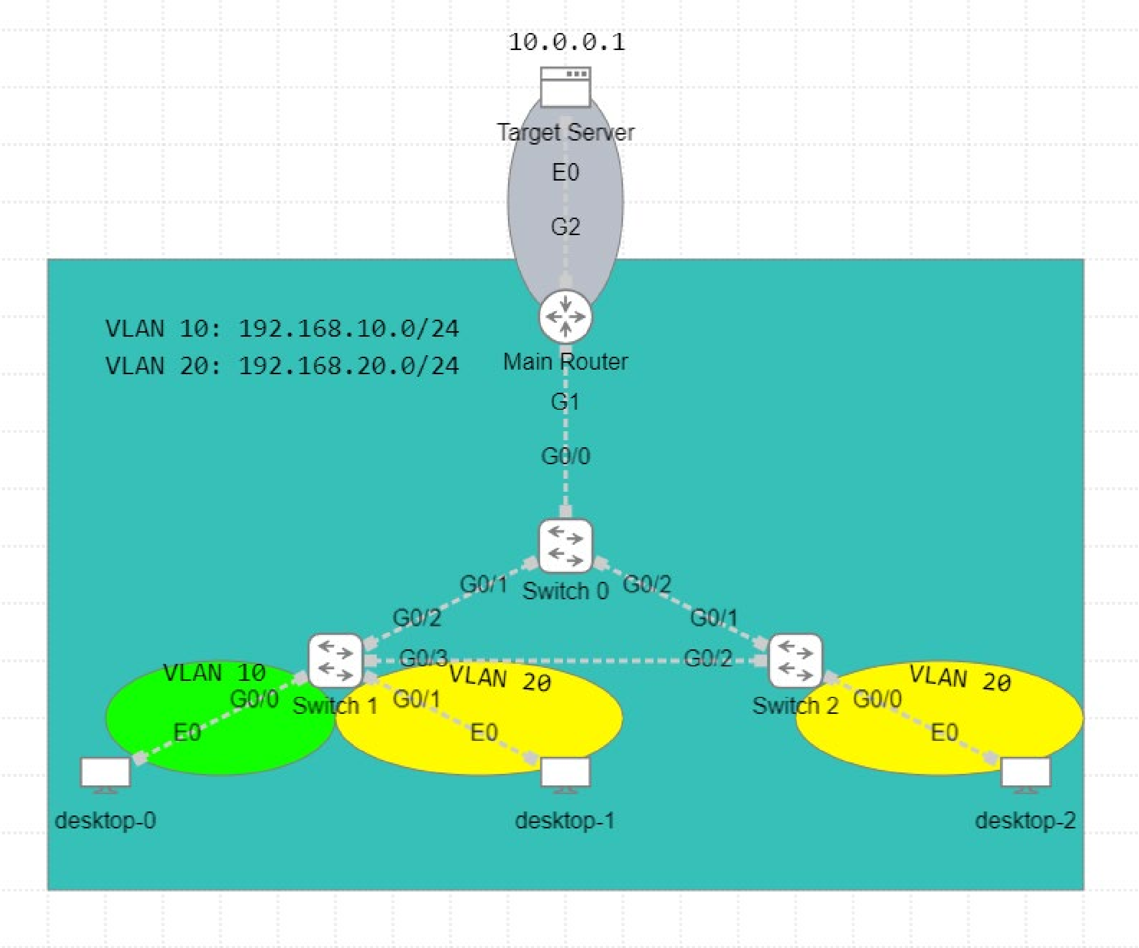


Figure 14. RSTP Lab with three desktops, three switches, Main Router, and a Target Server.

Description:

This lab intends to teach Rapid Spanning Tree Protocol (RSTP) concepts. RSTP enhances traditional Spanning Tree Protocol (STP). It is used to prevent loops in the switched network by blocking certain ports and removing the loop in software, but physical redundancy still exists, and if any link failure occurs, ports blocked by Spanning Tree will be unblocked. RSTP is significantly quicker than traditional STP, offering much quicker recovery while ensuring loop prevention.

Students will configure RSTP on all switches and ensure that Switch 0 has the highest priority and is always the root of the network for all of the VLANs. Additionally, ports going to desktops should transition quickly to a forwarding state and should block BPDUs in the case that they are discovered on those ports. This requires a separate configuration on those ports.

Learning Outcomes:
Upon completing this lab, students will gain an understanding of Rapid Spanning Tree Protocol (RSTP) and its advantages over traditional Spanning Tree Protocol (STP) in preventing network loops. They will learn to configure RSTP across multiple switches, ensuring efficient and quick network recovery while maintaining physical redundancy. By prioritizing Switch 0 as the root in the network configuration, students will demonstrate their ability to control network topology.

Dual Stack IPv4 and IPv6 Lab:

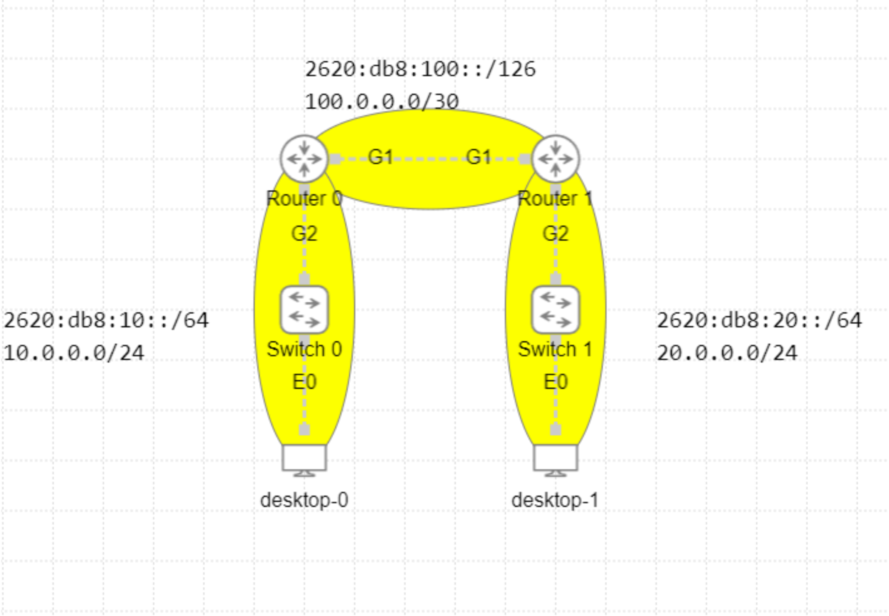


Figure 15. Dual Stack IPv4 and IPv6 Lab with two desktops, two switches, and two routers.

Description:

This lab introduces the concepts of dual stack IPv4 and IPv6 networking. The example in Fig. 15 is a very common setup since the industry is attempting to move to IPv6, and until IPv4 is completely phased out, dual stack networking needs to exist to continue to support both networks.

The task behind this lab is for students to configure IPv4 and IPv6 addresses on Routers 0 and 1 and appropriately configure static routing between the two routers to ensure connectivity between Desktop 0 and 1. The successful configuration will allow communication between the two desktops.

Learning Outcomes:
Upon completing this lab, students will develop an understanding of dual stack IPv4 and IPv6 networking, recognizing the necessity for simultaneous support of both protocols as the industry

transitions towards IPv6. By configuring both IPv4 and IPv6 addresses on Routers 0 and 1, students will learn the details of managing a network that operates with dual protocol stacks. By setting up static routing between the two routers over both IPv4 and IPv6, students will ensure connectivity between devices, demonstrating their ability to maintain network communication in a mixed protocol environment.

NAT Lab:

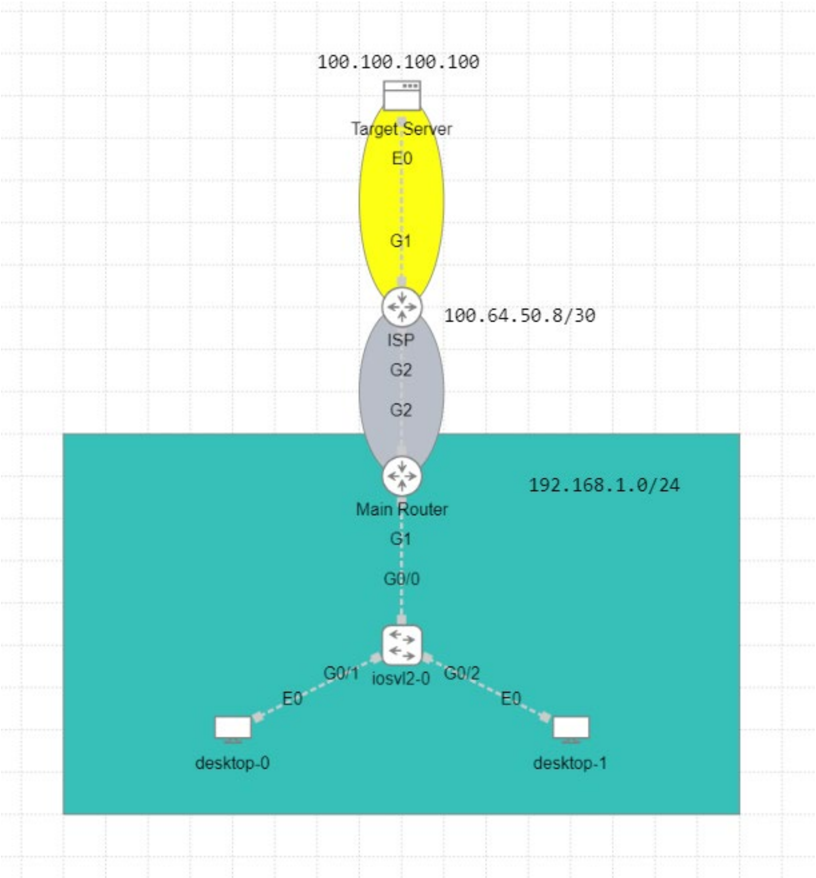


Figure 16. NAT Lab with two desktops, a switch, Main Router, ISP Router, and a Target Server.

Description:

This lab explores Network Address Translation (NAT), a protocol that performs network translation, which is vital for extending the IPv4 address space. NAT was developed in response to the impending exhaustion of IPv4 space as well as the definition of private address ranges as defined in RFC 1918 [20], namely 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/24 networks. These ranges are commonly used in residential and commercial settings where they are appropriately translated to one or more public IP addresses. At the edge of the network, a router connecting to the Internet Service Provider (ISP) performs NAT from a private IP address to a public IP address.

Students will configure DHCP on the Main Router interface to receive a dynamic IP address by the ISP and then configure NAT to translate internal network 192.168.1.0/24 to the address received by the ISP. This is also called Port Address Translation (PAT), as every private IP address will be translated to one public IP address and tracking of connections will be done based on port numbers, rather than by a direct translation between one private and one public IP address. At the end of the lab, Desktop 0 and 1 should be able to reach the Target Server at 100.100.100.100.

Learning Outcomes:

Upon completing this lab, students will understand the practical application of Network Address Translation (NAT), understanding its role in extending the IPv4 address space and facilitating private-to-public IP address translation as outlined in RFC 1918. This process involves translating multiple private IP addresses to a single public IP address, ensuring devices within a private network can access external resources.

VRRP Lab:

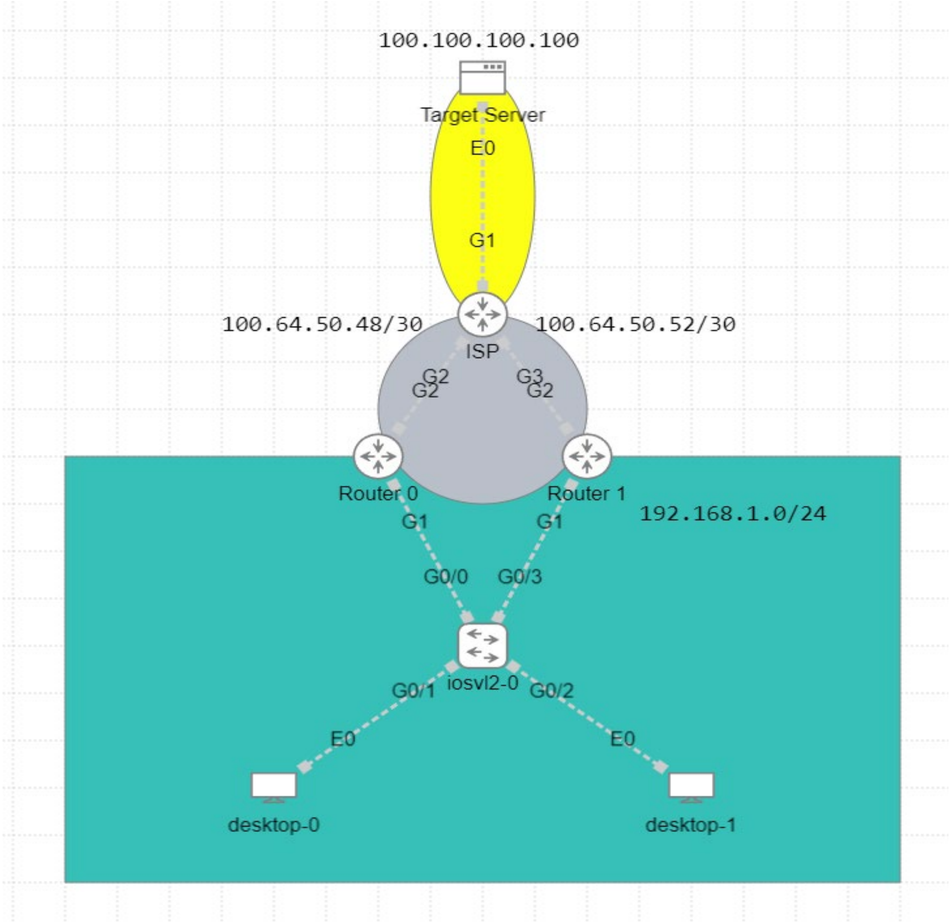


Figure 17. VRRP Lab with two desktops, a switch, two routers, ISP Router, and a Target Server.

Description:

This lab introduces concepts of Virtual Router Redundancy Protocol (VRRP). VRRP is a protocol that is used to create a virtual IP address shared between multiple routers, primarily for default gateway redundancy.

Students will configure Router 0 and Router 1 with VRRP. Both routers should monitor the external interface, and if one goes down, the other router should assume the default gateway role for the network. Additionally, both routers should use authentication and Router 0 should be configured with higher priority. The successful implementation will be demonstrated by seamless transition of the gateway between routers when the external interface goes down.

Learning Outcomes:
Upon completing this lab, students will understand the benefits of the Virtual Router Redundancy Protocol (VRRP), particularly its role in ensuring default gateway redundancy through the creation of a virtual IP address shared by multiple routers. Students will learn how to maintain network reliability and continuous access despite external network failures.

<u>OSPF Lab:</u>

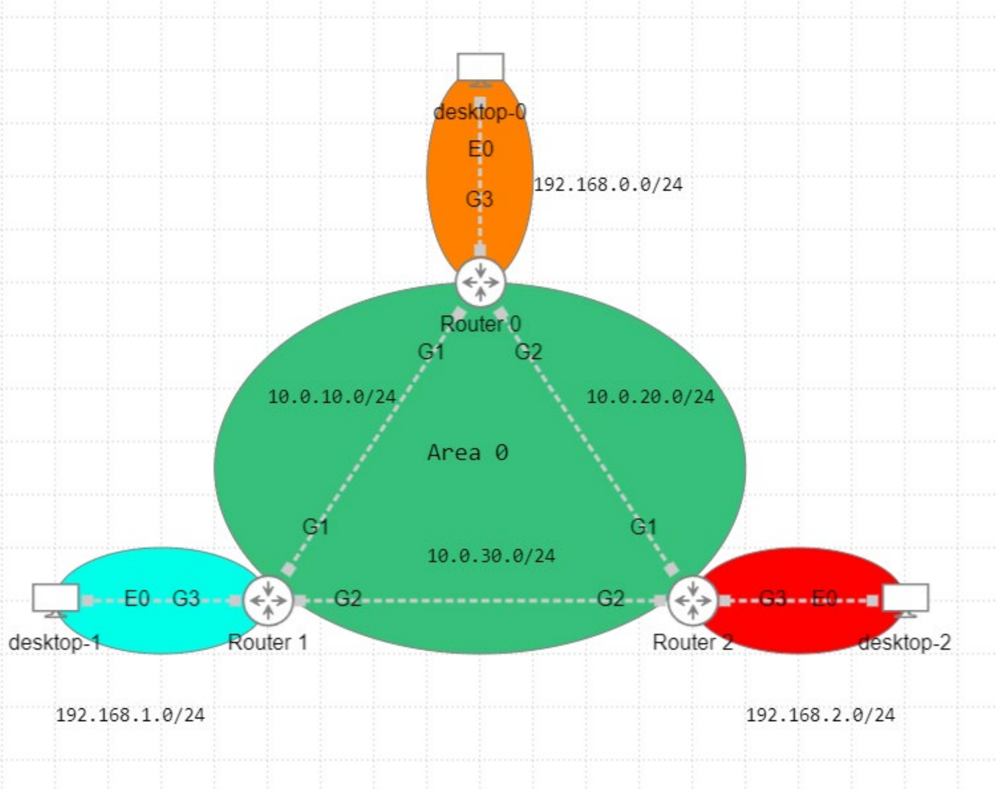


Figure 18. OSPF Lab with three desktops and three routers.

Description:

This lab focuses on Open Shortest Path First (OSPF), a dynamic routing protocol that uses Dijkstra's algorithm to determine the shortest path for each network route.

Students are tasked to configure Routers 0, 1, and 2 with OSPF where all networks are advertised with OSPF. Successful implementation will be indicated by the connectivity between each of the Desktop computers. Additionally, no OSPF advertisements should be sent on interfaces connected to desktops.

Learning Outcomes:

Upon completing this lab, students will gain an understanding of the Open Shortest Path First (OSPF) protocol, understanding its application in dynamically determining the most efficient network routes using Dijkstra's algorithm. The task of preventing OSPF advertisements on interfaces connected to desktops will introduce students to selective routing advertisements and the importance of minimizing unnecessary network traffic. Successful connectivity among the Desktop computers will demonstrate the effective application of OSPF in real-world networking scenarios.

Security ACL Lab:

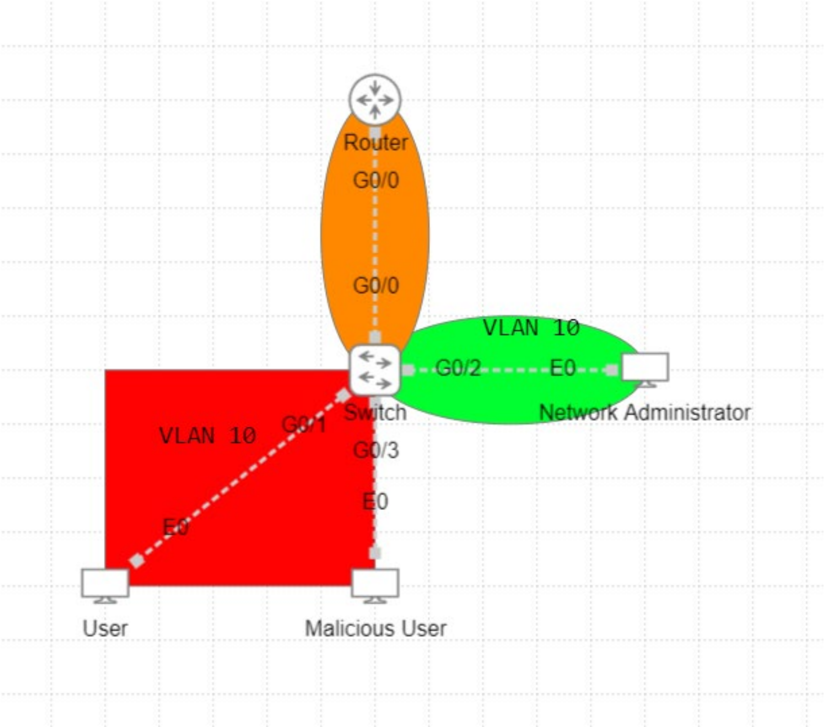


Figure 19. Security ACL Lab with three desktops, a switch, and Main Router.

Description:

This lab introduces the principles of Access Control Lists (ACLs), which are crucial for network security. ACLs enable network administrators to control the traffic flow and access within a network based on specified rules.

Students will simulate an attack with a defensive action taken by the network administrator. The entire network is one, flat network on VLAN 10. A Malicious User discovered that telnet to the Router is possible with username 'cisco' and password 'cisco'. These are the same credentials used by the Network Administrator, who also logs into the Router and then configures ACL to only allow the administrator's IP address. At this point the Malicious User should not be able to telnet to the Router anymore. For extra credit, two additional tasks can be given to students. The first is to configure SSH instead of telnet. The second task is to move Network Administrator to VLAN 20 and appropriately configure that entire network for the allow list, which would not allow Malicious User to just assume the Network Administrator's IP address in VLAN 10 for access to the Router.

Learning Outcomes:

Upon completing this lab, students will understand the role of Access Control Lists (ACLs) in enhancing network security. By simulating an attack and implementing defensive measures, students will gain practical experience in securing the network. Students will identify a security loophole that allows a Malicious User to gain unauthorized access and then configure an ACL to restrict access, thwarting further unauthorized access attempts. This lab emphasizes the importance of robust security configurations and network segmentation strategies in safeguarding network resources against unauthorized access.

GRE + IPSec Lab:

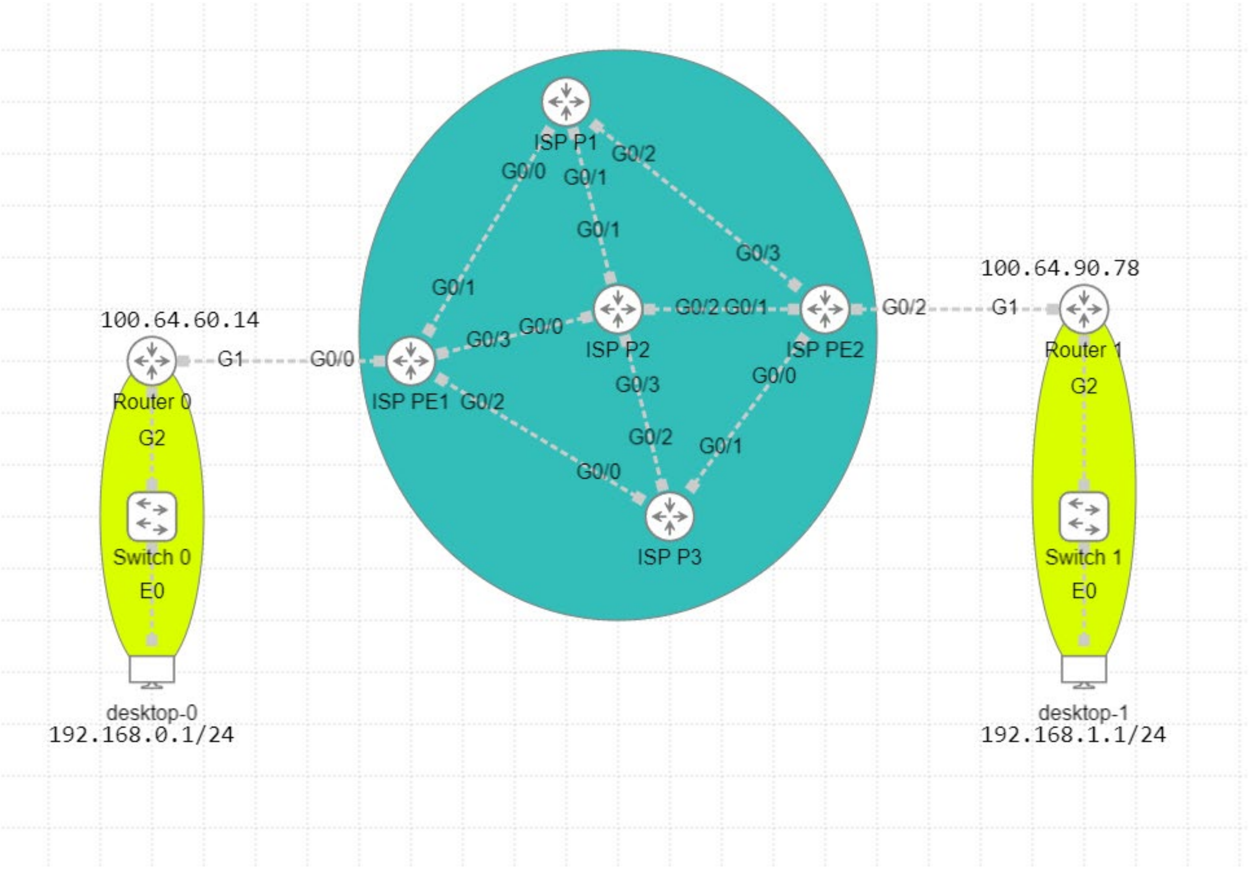


Figure 20. GRE + IPSec Lab with two desktops, two switches, and two routers as well as 5 ISP routers.

Description:

This lab is designed to teach encapsulation and encryption techniques in networking. Encapsulation and encryption are fundamental concepts for securing data transmission across networks. This lab will demonstrate these concepts using Generic Routing Encapsulation (GRE) and Internet Protocol Security (IPSec).

Students will begin by configuring a GRE tunnel between Router 0 and 1, establishing connectivity between two private subnets. This will enable Desktop 0 to communicate with Desktop 1. The first part of the task involves monitoring traffic over the router and ISP links using Wireshark to observe the data transmitted between two desktops.

The next step is to enhance security by configuring an IPSec tunnel over the existing GRE tunnel. This will encrypt the data being transferred. Students must then repeat the monitoring process to observe that the communication between Desktop 0 and Desktop 1 is now encapsulated within ESP (Encapsulating Security Payload) headers, indicating that the data is encrypted as it traverses the internet. This will highlight the effectiveness of encryption in securing data transmission.

Learning Outcomes:

Upon completing this lab, students will understand the concepts of encapsulation and encryption as methods for securing data transmission across networks. By establishing a Generic Routing Encapsulation (GRE) tunnel between two routers, students will first demonstrate the capability to link two private subnets and then using Wireshark students will monitor the traffic to observe that data is not encrypted. Students will then enhance network security by overlaying the GRE tunnel with an Internet Protocol Security (IPSec) tunnel. This step introduces students to the process of encrypting data in transit. By configuring IPSec, students will learn to apply encryption standards to protect data, observing the change through Wireshark as data packets are now encrypted. This direct comparison before and after encryption implementation will emphasize the effectiveness and necessity of encryption in protecting data across the internet.

ASA IPSec Lab:

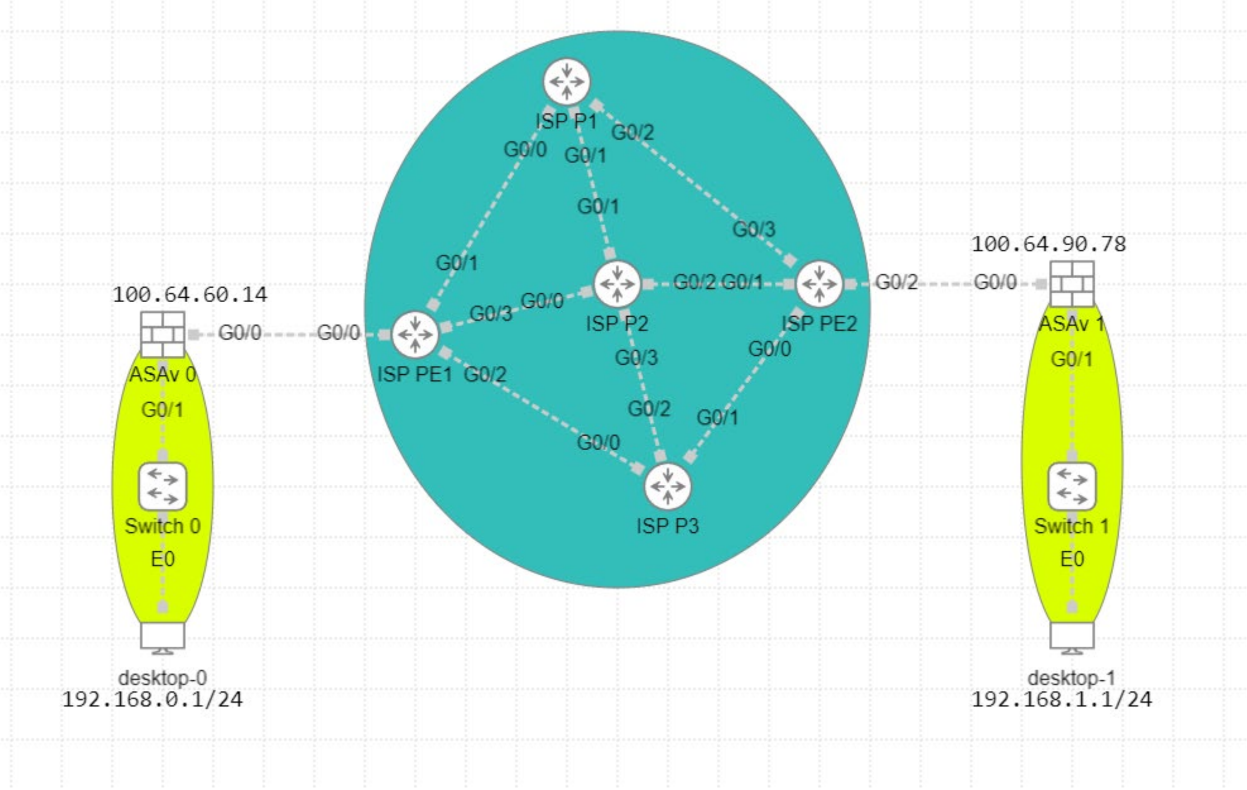


Figure 21. ASA IPSec Lab with two desktops, two switches, two firewalls as well as 5 ISP routers.

Description:

This lab is designed to teach encapsulation and encryption techniques in networking using Adaptive Security Appliance (ASA) firewalls. Students will learn ASA command line syntax and implement IPSec with ASA firewalls. This will help students understand the implementation using ASA when compared to traditional Cisco routers.

Students will configure an IPSec tunnel that encapsulates and encrypts data between two networks, establishing secure connectivity between two private subnets. The students should monitor traffic over the router and ISP links and observe that data transmitted is encrypted.

Learning Outcomes:

Upon completing this lab, students will understand the concepts of encapsulation and encryption as methods for securing data transmission across networks, focusing specifically on the use of Adaptive Security Appliance (ASA) firewalls. The lab is designed to familiarize students with ASA command line syntax, differentiating the implementation of IPSec on ASA firewalls from its configuration on traditional Cisco routers.

Advanced OSPF Troubleshooting Lab:

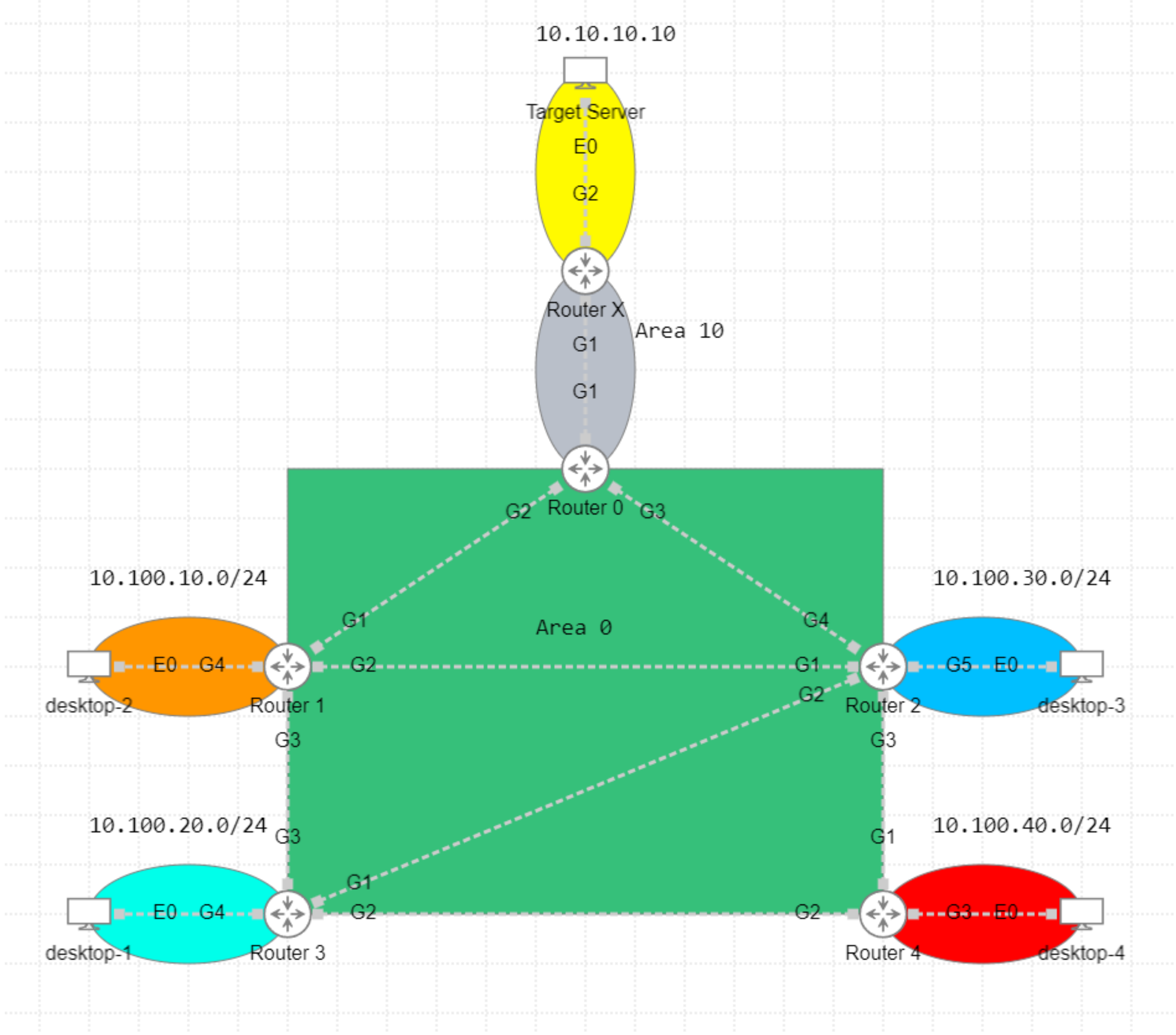


Figure 22. Advanced OSPF Troubleshooting Lab with 4 desktops, 6 routers, and a Target Server.

Description:

This advanced lab focuses on troubleshooting an already configured OSPF (Open Shortest Path First) network. The objective is to provide students with a practical understanding of common OSPF misconfigurations and their solutions.

The existing OSPF network is already configured, but it has 3 different misconfigurations that students will discover. All desktops should be able to reach Target Server, but only Desktop 2 can reach it with this configuration. Students will discover these issues and remedy them. Each issue remedied will allow connectivity between a desktop and the Target Server.

Learning Outcomes:

Upon completing this lab, students will enhance their skills in troubleshooting and resolving common misconfigurations within an OSPF network. This lab is designed to simulate a real-world scenario where students are presented with a network that, while already configured for OSPF, suffers from connectivity issues due to three distinct misconfigurations. This lab will not only improve their technical proficiency in troubleshooting OSPF networks but also cultivate critical thinking and problem-solving skills essential for network engineers.

Security OSPF Takeover Lab:

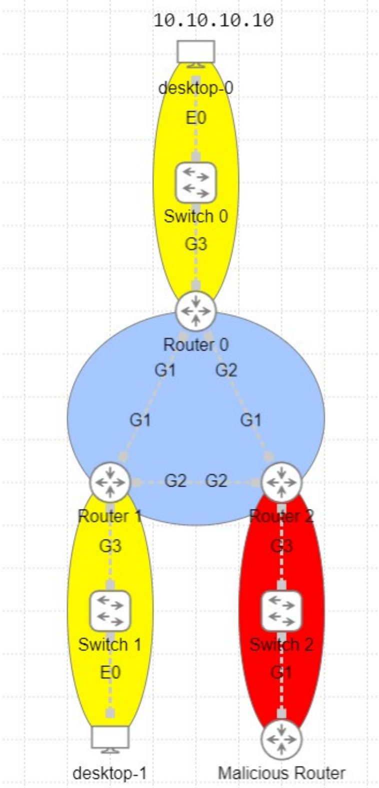


Figure 23. Security OSPF Takeover Lab with two desktops, three switches, three routers, and a Malicious Router.

Description:

This lab aims to teach the security issues associated with the Open Shortest Path First (OSPF). It focuses on the risks of a poorly secured OSPF network and how it can be exploited by a malicious entity.

The first part of the lab involves students observing the configuration of existing routers in the OSPF network which was set up with minimal security. Students are tasked with configuring a Malicious Router to join this OSPF network. Their objective is to create a disruptive OSPF advertisement that redirects traffic meant for the real server at 10.10.10.10. The successful execution of this task will be evidenced by Desktop 1 being unable to reach Desktop 0 due to the rogue advertisement.

The second part of the lab involves addressing the security issues of this OSPF network. Students will enhance the security by blocking unauthorized OSPF advertisements with the end goal of reestablishing secure network routing and preventing the Malicious Router from affecting network traffic.

Learning Outcomes:

Upon completing this lab, students will gain an understanding of the security vulnerabilities inherent in OSPF networks and the critical importance of implementing robust security measures to mitigate these risks. This two-part lab is designed to first expose students to the practical implications of minimal security configurations within OSPF networks, allowing them to witness how such vulnerabilities can be exploited by a malicious entity. This first part of the lab aims to illustrate the ease with which network routing can be compromised without adequate security, providing a realistic example of the potential consequences of such attacks. The second part of the lab shifts focus towards remediation and enhancement of network security. This experience will equip students with the knowledge and skills necessary to identify and address security weaknesses in OSPF configurations.

IoT Lab:

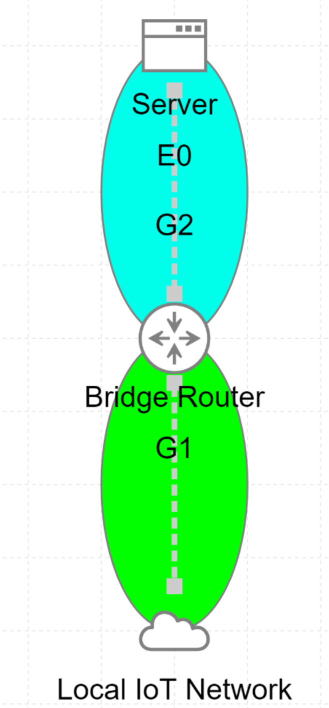


Figure 24. IoT Lab with one router, one server, and an external connectivity to the local network with an IoT device.

Description:

This lab demonstrates Internet of Things (IoT) concepts, particularly the integration of physical IoT devices with virtual networks used by CML.

Students will use an External Connector in a bridge mode to connect a physical IoT device, such as a Raspberry Pi, to a virtual network within CML. The Raspberry Pi will be configured with the address of the G1 interface on the Bridge Router in the CML network as its default gateway. G1 interface is the first gigabit Ethernet interface on the router. This will establish connectivity between the IoT device and the Server in the virtual network. Through this lab, students will learn how to bridge physical and virtual networking components, understand the practical applications of IoT connectivity, and gain experience in configuring IoT devices to interact with larger network infrastructures.

Learning Outcomes:

Upon completing this lab, students will gain an understanding of Internet of Things (IoT) integration within CML, highlighting the connectivity between physical IoT devices and virtual network environments. This lab serves as an experiential learning opportunity for students to grasp the importance of IoT in today's technology landscape and acquire hands-on experience in configuring network settings to facilitate the integration of IoT devices with virtual networks.

Solutions

Educators can request solutions to all of the labs by reaching out to the author and providing public information that they are teaching a networking course, including an educational email address.

Conclusion

In conclusion, this paper outlines the potential of Cisco Modeling Labs (CML) in addressing the critical gap in practical networking education. The platform offers an accessible solution that significantly lowers the barrier to entry for students seeking necessary hands-on experience needed for a career in networking. The preconfigured labs presented as part of this paper offer educators a robust starting point for teaching a wide range of technologies used in the real world. By using these labs, students not only gain theoretical understanding, but they get to practice with these technologies in a risk-free environment that is representative of real-world configurations. This approach aligns with the findings of studies highlighting the effectiveness of Simulation Based Learning (SBL) by improving the acquisition of practical skills and paving the way for the next generation of network professionals.

References

[1] E. Lampi, “The Effectiveness of using Virtual Laboratories to Teach Computer Networking Skills in Zambia,” Ph.D dissertation, Career and Technical Education, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, 2013. [Online]. Available: https://www.proquest.com/docview/1512636920

[2] J. Allison, “Simulation-based learning via Cisco Packet Tracer to enhance the teaching of computer networks,” *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1*, Jul. 2022. doi:10.1145/3502718.3524739

[3] S. Asadi, J. Allison, M. Khurana, and M. Nilashi, “Simulation-based learning for computer and networking teaching: A systematic literature review and Bibliometric analysis,” *Education and Information Technologies*, Feb. 2024. doi:10.1007/s10639-024-12476-7

[4] A. Abdrabou and W. Shakhatreh, “On assessment and evaluation of Teaching Computer Networks to electrical engineering students by the aid of a lab course,” *Journal of Technology and Science Education*, vol. 11, no. 2, p. 388, Jun. 2021. doi:10.3926/jotse.1186

[5] A. Botta, R. Canonico, A. Navarro, G. Stanco and G. Ventre, "Towards a Highly-Available SD-WAN: Rapid Failover based on BFD Protocol," *2023 IEEE Conference on Network*

Function Virtualization and Software Defined Networks (NFV-SDN), Dresden, Germany, 2023, pp. 153-158, doi: 10.1109/NFV-SDN59219.2023.10329617.

[6] J. Abhishek Singh, M. R. Sachin Kumar and K. S. Shushrutha, "Implementation of Segment Routing-Traffic Engineering over MPLS," *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2021, pp. 1-5, doi: 10.1109/ICCCNT51525.2021.9579691.

[7] S. V. Tagliacane, P. W. C. Prasad, G. Zajko, A. Elchouemi and A. K. Singh, "Network simulations and future technologies in teaching networking courses: Development of a laboratory model with Cisco Virtual Internet Routing Lab (Virl)," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016, pp. 644-649, doi: 10.1109/WiSPNET.2016.7566212.

[8] L. M. Moreira Zorello, S. Troia, S. Giannotti, R. Alvizu, S. Bregni and G. Maier, "On the Network Slicing for Enterprise Services with Hybrid SDN," *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, Santo Domingo, Dominican Republic, 2020, pp. 1-6, doi: 10.1109/LATINCOM50620.2020.9282318.

[9] "Cisco Modeling Labs 2.0 Release notes - cisco modeling labs 2.0 [Cisco Modeling Labs]," Cisco, https://www.cisco.com/c/en/us/td/docs/cloud_services/cisco_modeling_labs/v200/release/notes/b_cml_release_notes_2-0/m_overview.html (accessed Mar. 20, 2024).

[10] J. Gomez, E. F. Kfoury, J. Crichigno, and G. Srivastava, "A survey on network simulators, emulators, and testbeds used for research and Education," *Computer Networks*, vol. 237, p. 110054, Dec. 2023. doi:10.1016/j.comnet.2023.110054

[11] M. Shimba, M. P. Mahenge, and C. A. Sanga, "Virtual Labs versus hands-on labs for teaching and Learning Computer Networking: A comparison study," *International Journal of Research Studies in Educational Technology*, vol. 6, no. 1, Oct. 2016. doi:10.5861/ijrset.2017.1660

[12] D. 12 and J. Corral, "How to Write Well-Defined Learning Objectives," *The Journal of Education in Perioperative Medicine: JEPM*, vol. 19, no. 4, Art. no. E610, Oct. 2017. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5944406/

[13] Cisco Systems, Inc., "Cisco Modeling Labs," Cisco, [Online]. Available: https://www.cisco.com/c/en/us/products/cloud-systems-management/modeling-labs/index.html#~licensing. [Accessed: Jan. 25, 2024].

[14] Cisco DevNet, "CML Installation Guide," Cisco Developer, [Online]. Available: https://developer.cisco.com/docs/modeling-labs/#!cml-installation-guide. [Accessed: Jan. 25, 2024].

[15] Cisco DevNet, "Deploying the OVA File on VMware Workstation/Fusion," Cisco Developer, [Online]. Available: https://developer.cisco.com/docs/modeling-labs/#!deploying-the-ova-file-on-vmware-workstation-fusion. [Accessed: Jan. 25, 2024].

[16] "Introduction to Terraform," HashiCorp, Inc.,. [Online]. Available: https://www.terraform.io/. [Accessed: Jan. 25, 2024].

[17] CiscoDevNet, "Run Cisco Modeling Labs on cloud infrastructure," GitHub, Aug 10, 2023. [Online]. Available: https://github.com/CiscoDevNet/cloud-cml. [Accessed: Jan. 25, 2024].

[18] E. Karincic (Dollarhyde), "Terraform Cloud CML," GitHub, Jan 22, 2024. [Online]. Available: https://github.com/Dollarhyde/terraform-cloud-cml. [Accessed: Jan. 25, 2024].

[19] E. Karincic (Dollarhyde), "CML Labs," GitHub, Feb 7, 2024. [Online]. Available: https://github.com/Dollarhyde/cml-labs. [Accessed: Feb. 7, 2024].

[20] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, "Address Allocation for Private Internets," RFC 1918, February 1996. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc1918. [Accessed: Jan. 25, 2024].

[21] Cisco DevNet, "Adding Additional VM Images," in Cisco Modeling Labs v2.6 Documentation, [Online]. Available: https://developer.cisco.com/docs/modeling-labs/#!vm-images-for-cml-labs/adding-additional-vm-images. [Accessed: Jan. 25, 2024].

Appendix A: Reference Platforms in the lab

These following reference platforms are represented as nodes within the lab [21]:

1. IOSv: Legacy Cisco IOS router platform.

2. IOSvL2: Cisco IOS Layer 2 switch platform

3. ASAv: Cisco ASA virtual firewall platform.

4. CSR 1000v: Cisco Cloud Services Router, running IOS XE.

5. CAT 8000v: Catalyst 8000v router for SD-WAN, the successor to CSR 1000v, running IOS XE.

6. IOS XRv 9000: Virtual router for Service Provider networks, running IOS XR Software.

7. NX OS 9000: Virtual router for Datacenter networks, running Nexus NX-OS Software.

8. Server: Server representation in labs, running Tiny Core Linux.

9. Alpine: Server setup for lab hosts, running Alpine Linux.

10. Desktop: Host representation with a graphical desktop, running Alpine Linux.

11. Ubuntu: Server setup for lab hosts, running Ubuntu Linux.

12. Trex: Server setup for utilizing Trex traffic generator, running Alpine Linux.

13. WAN Emulator: Provides metrics on packet loss, latency, and throughput limitations, running Alpine Linux.