CCNP ROUTING AND SWITCHING

LINUX RADIUS AAA

Brennen Tse
10/11/2022

Table of Contents:

Purpose:

In this lab, students are to recognize the uses of AAA and configure the two of the main AAA protocols, open-source RADIUS and Cisco proprietary TACACS+. Students are to set up a VM server with either Windows or Linux Ubuntu OS's. With either RADIUS or TACACS+ installed on the server, a Router should be able to establish remote authentication on the router to confirm user credentials with the server. In this report, I will be configuring RADIUS on the Linux VM.

Background Information:

Authentication, Authorization, Accounting

Triple A, or Authentication, Authorization, and Accounting is a standard used to control access to network devices (authentication), how much permission they have (authorization) and allows for the creation of activity logs (accounting). The main benefit of AAA services is security. If you don't use AAA, then authentication would have to be done locally on every individual device using shared usernames and passwords, creating exponential more chances for incidents, breaches and leaks of sensitive information. Also, local management is a large strain on the individual networks and using AAA is both more secure and efficient. The most popular services are RADIUS, TACACS+ and Diameter.

- *Authentication* provides a way to identify a user through both valid usernames and passwords before access and authentication is granted. When a user wants to remotely access a device, the device will compare the user's credentials with those stored on the remote AAA server. If the credentials match on the AAA server, the user is granted access to the device. Otherwise, the device is denied.

- *Authorization* is the process of determining the level of permission a user has, namely, what they are permitted to access. After a user is authenticated, they may be authorized to view or edit certain sensitive files.

- *Accounting* logs the activity of a user during access, which may include the length of time spent, what they accessed, or changes they made. These statistics can be used by higher officials to determine billing, trend analysis, time management, and such.

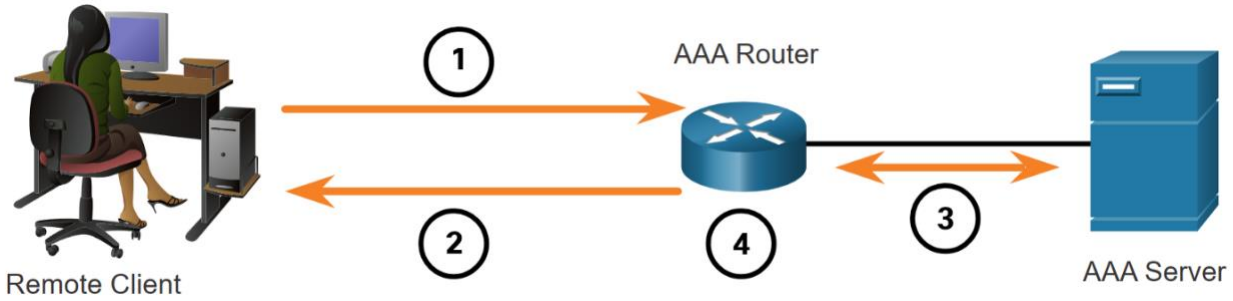
Linux:

Like other operating systems including Windows and MacOS, Linux can run applications, but excels at server-based services, such as hosting RADIUS servers, since it is much more lightweight than other software. In computing, something "lightweight" refers to software designed to have a small memory footprint (RAM), low CPU, and low overall usage of system resources. Perfect for something like a server, but less user friendly (unfortunately). Users will typically navigate Linux through the command-line with less focus on graphical applications. There isn't really a GUI for Linux so it's more complicated than more user-friendly systems like Windows.

Since Linux is an open-source OS, where anyone can take the base code and manufacture it to their liking, there are many *distributions* designed for specific purposes. I used Ubuntu for my virtual machine although this project could be replicated with any distribution of Linux like Debian or others. Just make sure that the open-source code is safe to use and doesn't contain any malicious code.

Virtual Box:

AAA Communication Process:



1. Remote client tries to login to router using PPP. In our case we use Putty.
2. AAA Router requests username and password.
3. Once username and password are given, AAA router sends these to AAA authentication server through either RADIUS or TACACS to check validity and authorization of user.
4. Once receiving this information, router either grants user access or denies access.

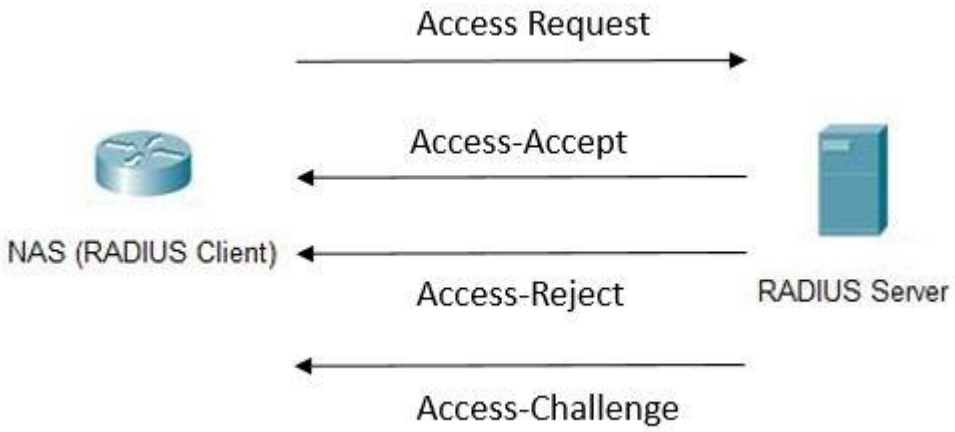
RADIUS vs TACACS:

Terminal Access Controller Access Control System (TACACS+) is used to communicate between the client and NAS server and is Cisco proprietary. Remote Access Dial-In User Service (RADIUS) is a protocol that is open standard used for the same purpose as TACACS+ but uses port 1812 and 1813. Both were designed for slightly different purposes can be used for the same roles, as RADIUS would ideally be used to authenticate and log remote users while TACACS+ is used for admin access to network devices like the router in this lab. TACACS+ is more reliable using TCP port 49 instead of RADIUS's UPD ports 1812 and 1813, and provides more control of authorization of commands. TACACS+ is more secure as all packets in are encrypted while only passwords are in RADIUS. However, RADIUS is open standard meaning it can be used on devices other than Cisco ones. The authentication processes are the same between both protocols.

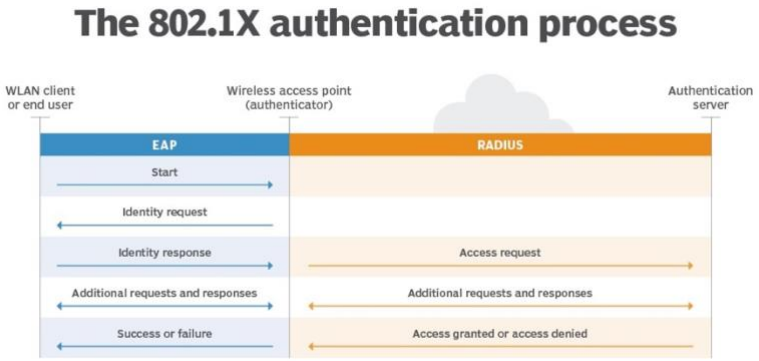
Differences:

TACACS+ separates each component of AAA, Authentication, Authorization and Accounting while RADIUS combines Authentication and Authorization, using port 1812 for them and 1813 for accounting. TACACS+ offers multiprotocol support and is used for device administration, while RADIUS is used for network access.

RADIUS PROTOCOLS:



1.After the user request with credentials is received, the NAS sends an Access Request to the RADIUS server with the credentials.
2. The RADIUS server checks the validity of the credentials using PAP, CHAP or EAP. It either responds with Access-Accept, which means its valid, Access-Reject, which means its not, and Access-Challenge, which is request for more information like another password. Unfortunately, most of this information is sent unencrypted in cleartext, and the protocol of DIAMETER is planned to replace RADIUS as a more secure form of AAA.



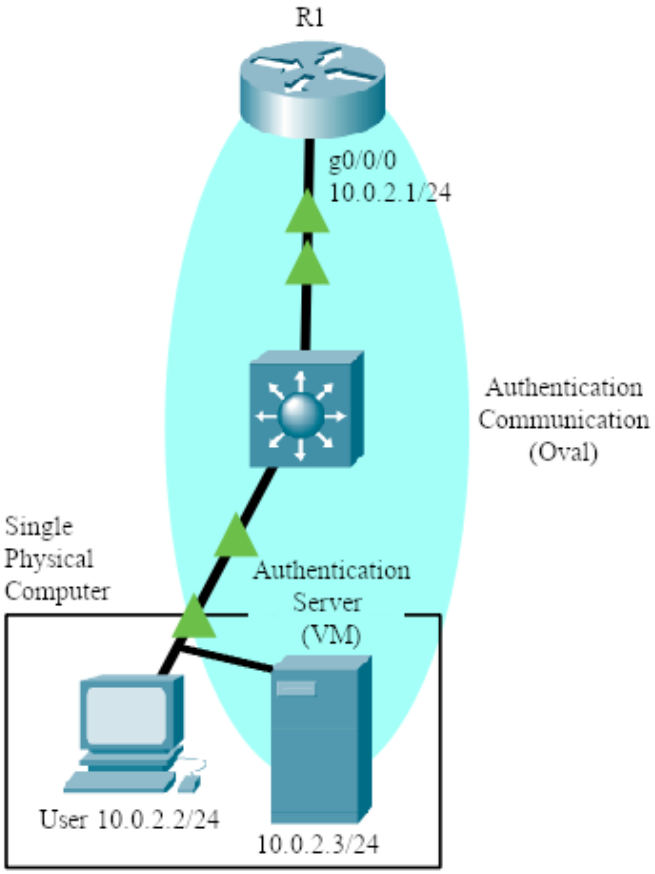
Lab Summary:

A router which serves as the authentication client and NAS is connected to a PC hosting the VM with the either the TACACS+ or RADIUS server. Although these devices are physically connected through a single link, they logically represent separate devices. To confirm that the authentication protocols are working, a new user profile should be added to the authentication database and confirmed that it works. Incorrect logins should also be checked to make sure that the authentication isn't set to allow all. For the RADIUS VM server we used

Linux's Ubuntu distribution 20.04 as the underlying OS and FreeRadius for the RADIUS software. When FreeRadius 3.0 is installed, you can configure the user and clients database in the "Users" and "Clients.conf" files using the NANO editor. You configure the username, password and shared secret (key). This key on the client file must be the same as the key on the NAS. The IP addresses should be in the same subnet and the VM should use the Bridged network adapter.

Upon successful client and server configuration, RADIUS should be fully functional. Attempting to access the router via either console or SSH (remote access), it prompts a login username and password. Any correct username and password pair is visible in the users file of the Linux server. The password to reach privileged EXEC mode is also configured there, under the username "$enab15$." New users were added afterwards to prove that verification was from the server rather than a local configuration. Changes of configuration afterwards are documented as evidence of functionality. After all elements of configuration, the protocols are operational and AAA is in use.

Network Diagram



LAB COMMANDS:

Router Commands:

Router(config)# **aaa new-model**

- Specifies AAA as the authentication method for VTY lines on the router

To configure any AAA services, you must first define aaa new-model.

// RADIUS Authentication

Router(config)# **aaa authentication attempts login [#]**

- Specifics the number of login attempts a user gets before the connection terminates

Router(config)# **aaa authentication banner** `*message*`

- Set a message for a user when they connect to the device

Router(config)# **aaa authentication fail-message** `*message*`

- Set a message if the user fails their credentials

Router(config)# **aaa authentication *login default group radius***

- Make the router verify login credentials with a radius server

Router(config)# **aaa authentication *enable default group radius***

- Make the router verify privilege exec mode credentials with a radius server

// Defining a RADIUS Server

Router(config)# **radius server [*name*]**

- Define a radius server

The router will use the ip address of the radius server subsequently provided to verify credentials. This command can only be typed after aaa new-model *has been declared.*

Router(config-radius-server)# **address ipv4 [*ip*] auth-port *1812* acct-port *1813***

- Define the *ip* of the radius server

Router(config-radius-server)# **key [*key*]**

- Define the *key* of the radius server

The key on the router should match the key in the radius server's configuration files.

Linux command side:

ls – Lists folders and files in current directory.

CD [*Folder name*] – Enter new directory of new folder.

Sudo su – Enters super admin mode. "Sudo…" syntax for admin permissions is not necessary on future commands after first used.

Sudo apt-get install FreeRadius {FreeRadius-utils} – Installs FreeRadius. {As well as other FreeRadius utilities, optional.}

Sudo apt policy FreeRadius – Checks FreeRadius version. v3.0 was used for this lab.

Service FreeRadius restart – Restarts the FreeRadius service. Updates changes.

FreeRadius -CX – Checks FreeRadius operation and seeks errors in file configuration.

Nano [*File name*]– Using the default file editor called "nano," opens and edits file contents.

```
Client [Client IP] {
     secret = [Secret name]
     nastype = [NAS type]
     shortname = [Device-type]
}
```

Under "nano clients.conf," the following creates the FreeRadius client. This set of commands determines its IP, shared secret key, NAS type, and a local nickname for the device. The key has to be exactly the SAME to the router-side configuration. NAS type of "cisco" and a shortname of "router" was used.

```
[username] Cleartext-Password := "[password]"
     Service-Type = NAS-prompt-user,
     Cisco-AVpair = shell:priv-lvl=[privilege number 1-15]
```

Under "nano users," the following creates the FreeRadius user credentials. This set of commands can be repeated and is used to create a user on this server. These usernames and passwords are the ones the router will check with upon each login request.

```
$enab15$ Cleartext-Password := "[enable password]"
     Service-Type = NAS-prompt-user,
     Cisco-AVpair = shell:priv-lvl=[privilege number 1-15]
```

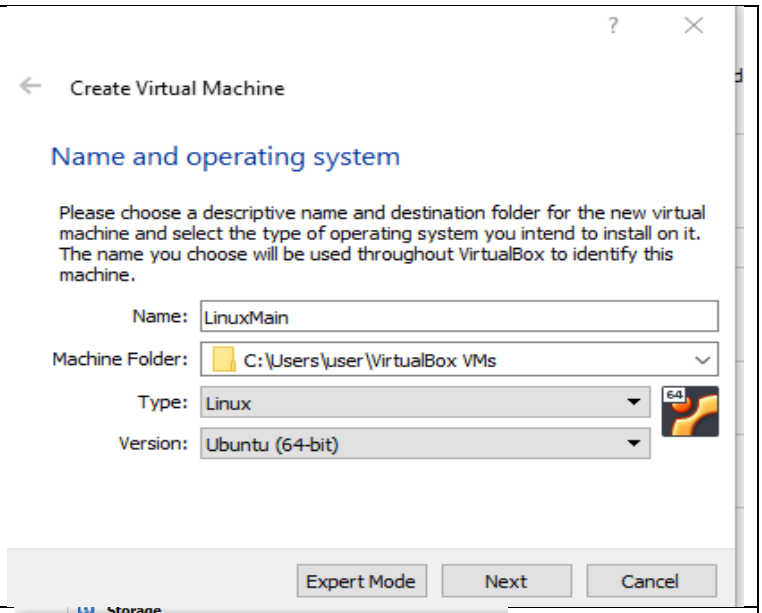
Creates password upon users' requests for entering privileged mode.

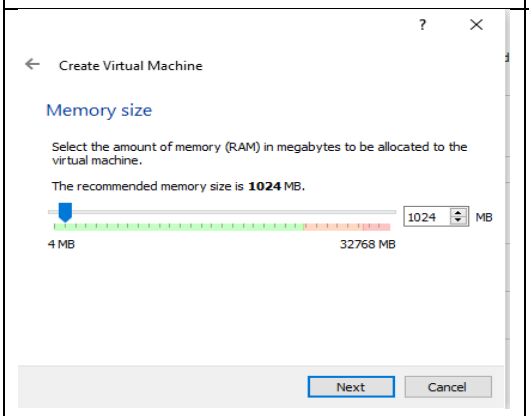
Important Commands:
Cd /etc/freeradius/3.0/
Nano users
Service freeradius restart
Freeradius -CX

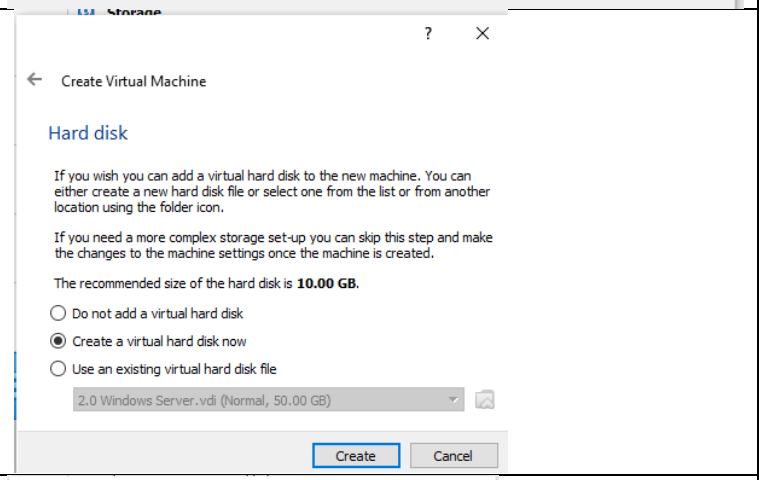
Linux Radius AAA
Download Oracle VM VirtualBox Manager

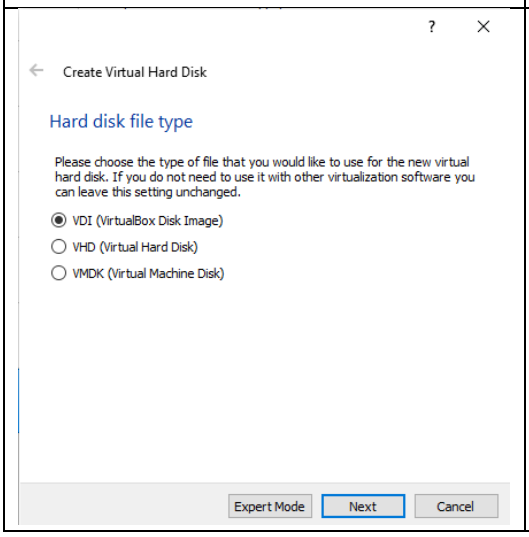
CREATING THE LINUX RADIUS VM

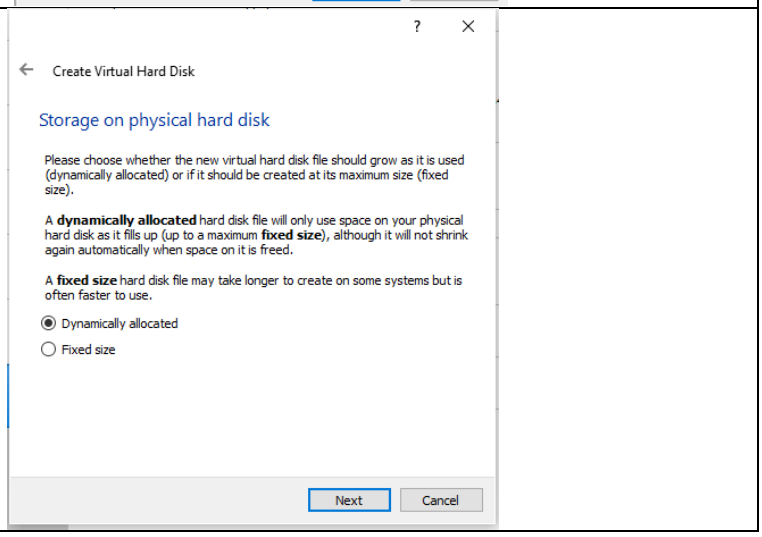
Click on the *new* icon to create a new Virtual Machine, select Linux and Ubuntu as the version, you should have a Linux machine image already downloaded to your computer.

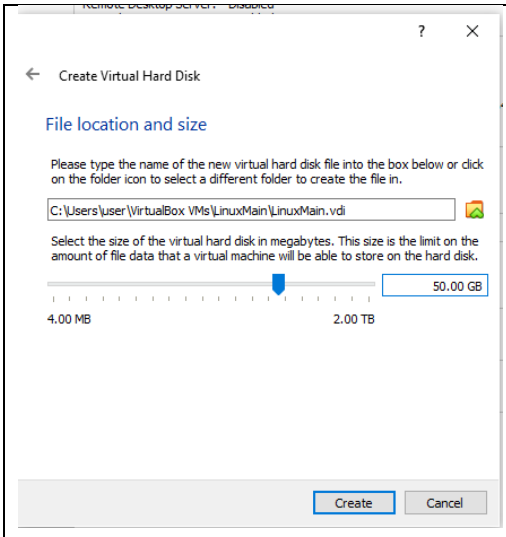


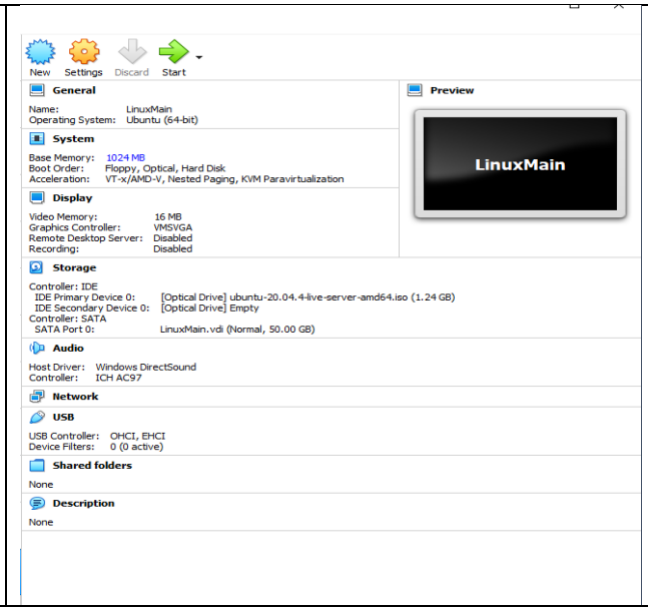


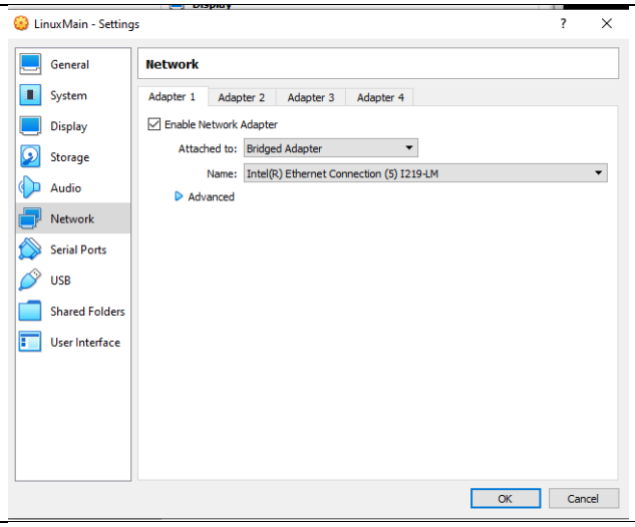
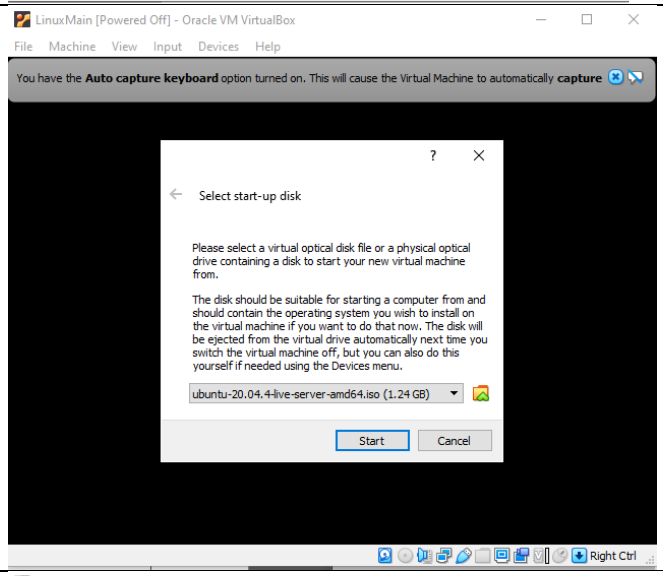
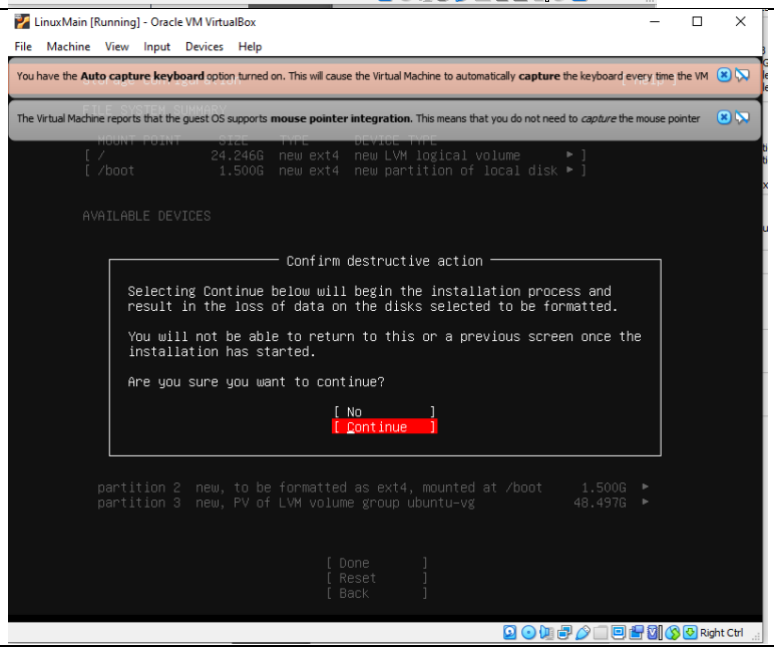


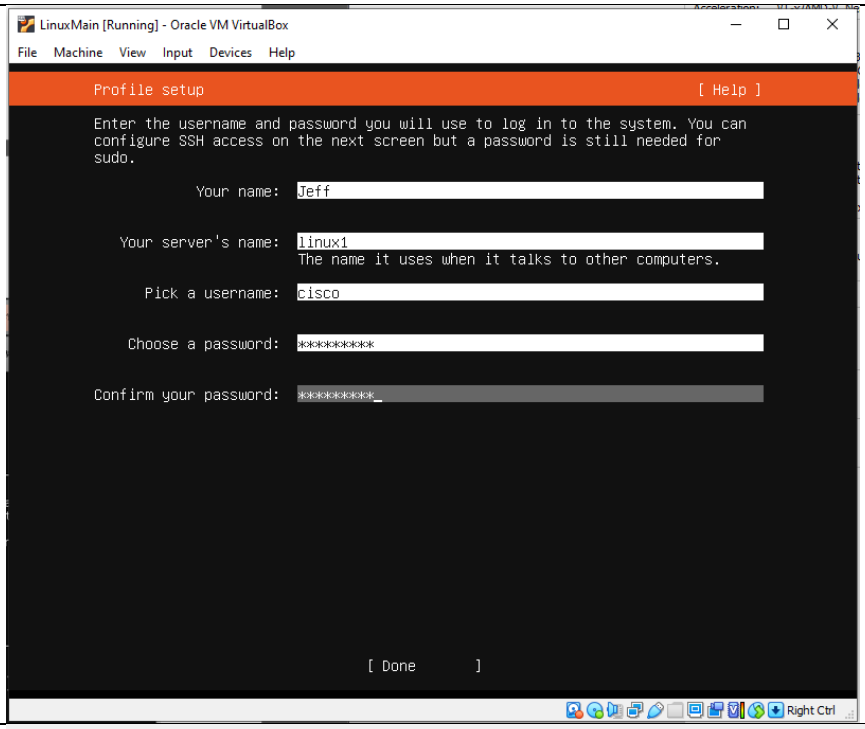
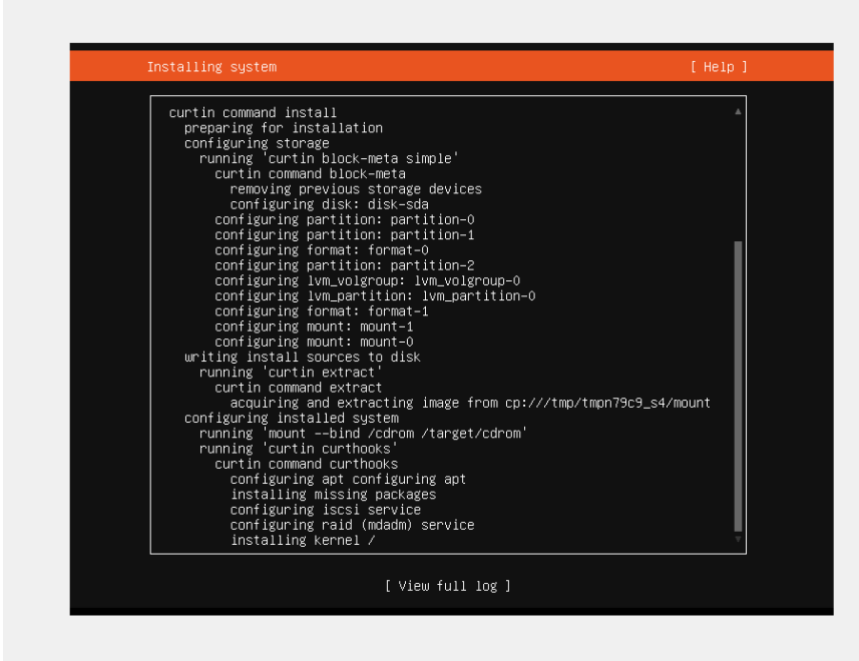


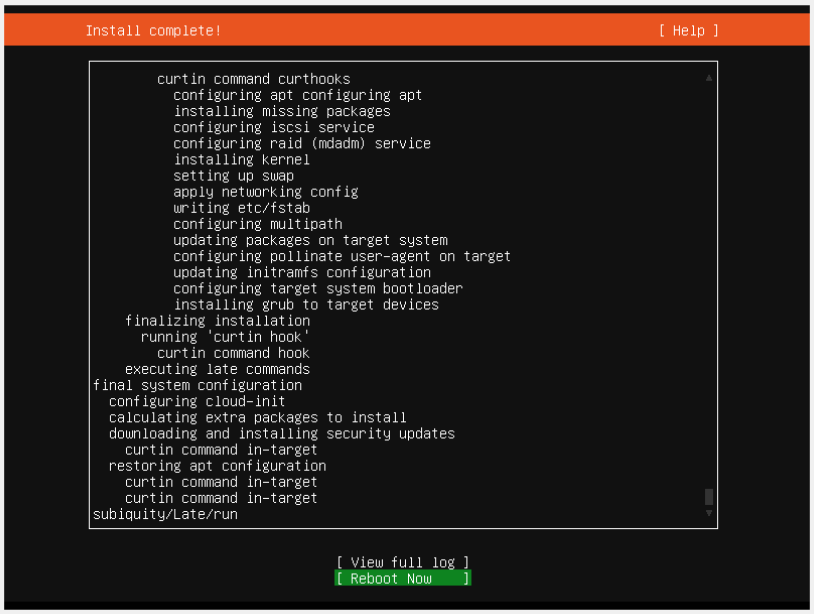



Create Virtual Hard Disk
File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
C:\Users\user\VirtualBox VMs\LinuxMain\LinuxMain.vdi
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
50.00 GB
4.00 MB
2.00 TB
Create
Cancel


New
Settings
Discard
Start
General
Name: LinuxMain
Operating System: Ubuntu (64-bit)
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Primary Device 0: [Optical Drive] ubuntu-20.04.4-live-server-amd64.iso (1.24 GB)
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: LinuxMain.vdi (Normal, 50.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None
Preview
LinuxMain

Navigate to settings and change the network adapter from NAT to Bridged Adapter Ethernet.	
Select the correct ubuntu start-up disk after clicking the start arrow.	
Select Continue	

Setup your profile. Remember the username and password as this will be important later.	
	

Reboot the VM	

INSTALLING FreeRADIUS

After rebooting, enter this command which gets and installs freeradius on the Linux Machine.	`cisco@linux1:~$ sudo apt-get install freeradius freeradius-utils_`

Check that freeradius is installed and has the correct version using the command *sudo apt policy freeradius*	`cisco@linux1:~$ sudo apt policy freeradius`
	`freeradius:`
	`  Installed: 3.0.20+dfsg-3ubuntu0.1`
	`  Candidate: 3.0.20+dfsg-3ubuntu0.1`
	`  Version table:`
	`  *** 3.0.20+dfsg-3ubuntu0.1 500`
	`  500 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages`
	`  100 /var/lib/dpkg/status`
	`  3.0.20+dfsg-3build1 500`
	`  500 http://us.archive.ubuntu.com/ubuntu focal/main amd64 Packages`

Use the sudo su to gain root access and check the files using the cd /etc/freeradius/3.0/ ls command.	`cisco@linux1:~$ sudo su`
	`root@linux1:/home/cisco# cd /etc/freeradius/3.0/`
	`root@linux1:/etc/freeradius/3.0# ls`
	`certs  experimental.conf  mods-available  panic.gdb  radiusd.conf  sites-enabled  users`
	`clients.conf  hints  mods-config  policy.d  README.rst  templates.conf`
	`dictionary  huntgroups  mods-enabled  proxy.conf  sites-available  trigger.conf`
	`root@linux1:/etc/freeradius/3.0# _`

Install the nano editor using the command sudo apt install nano. Then enter the clients.conf file using the command nano clients.conf	`root@linux1:/etc/freeradius/3.0# sudo apt update`
	`Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease`
	`Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]`
	`Get:3 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]`
	`Get:4 http://us.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]`
	`Fetched 336 kB in 1s (324 kB/s)`
	`Reading package lists... Done`
	`Building dependency tree`
	`Reading state information... Done`
	`38 packages can be upgraded. Run 'apt list --upgradable' to see them.`
	`root@linux1:/etc/freeradius/3.0# sudo apt install nano`
	`Reading package lists... Done`
	`Building dependency tree`
	`Reading state information... Done`
	`nano is already the newest version (4.8-1ubuntu1).`
	`0 upgraded, 0 newly installed, 0 to remove and 38 not upgraded.`
	`root@linux1:/etc/freeradius/3.0# nano clients.conf`

When you are greeted with this text file, scroll down.	`GNU nano 4.8  clients.conf`
	`# -*- text -*-`
	`##`
	`## clients.conf -- client configuration directives`
	`##`
	`##  $Id: 76b300d3c55f1c5c052209b76bf28ac3a370bbb2 $`
	`#######################################################################`
	`#`
	`#  Define RADIUS clients (usually a NAS, Access Point, etc.).`
	`#`
	`#  Defines a RADIUS client.`
	`#`
	`#  '127.0.0.1' is another name for 'localhost'.  It is enabled by default,`
	`#  to allow testing of the server after an initial installation.  If you`
	`#  are not going to be permitting RADIUS queries from localhost, we suggest`
	`#  that you delete, or comment out, this entry.`
	`#`
	`#`
	`#`
	`#  Each client has a "short name" that is used to distinguish it from`
	`#  other clients.`
	`#`
	`#  In version 1.x, the string after the word "client" was the IP`
	`#  address of the client.  In 2.0, the IP address is configured via`
	`#  the "ipaddr" or "ipv6addr" fields.  For compatibility, the 1.x`
	`#  format is still accepted.`
	`#`
	`client localhost {`
	`  #  Only *one* of ipaddr, ipv4addr, ipv6addr may be specified for`
	`  #  a client.`
	`  #`
	`[ Read 268 lines ]`
	`^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo`
	`^X Exit  ^R Read File  ^\ Replace  ^U Paste Text  ^T To Spell  ^_ Go To Line  M-E Redo`

When you reach the end of the blue text, input the related user and user information into the file.

```
  GNU nano 4.8                          clients.conf                          Modified

#client private-network-2 {
#       ipaddr          = 198.51.100.0/24
#       secret          = testing123-2
#}

################################################################################
#
#  Per-socket client lists.  The configuration entries are exactly
#  the same as above, but they are nested inside of a section.
#
#  You can have as many per-socket client lists as you have "listen"
#  sections, or you can re-use a list among multiple "listen" sections.
#
#  Un-comment this section, and edit a "listen" section to add:
#  "clients = per_socket_clients".  That IP address/port combination
#  will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#       client socket_client {
#               ipaddr = 192.0.2.4
#               secret = testing123
#       }
#}
client 10.0.2.1 {
        secret = secretkey
        nasype = cisco
        shrotname = router
}

Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

Enter the users file using nano user. Create the user profile with password and enable password.

```
  GNU nano 4.8                              users                             Modified
DEFAULT Hint == "SLIP"
        Framed-Protocol = SLIP

#
# Last default: rlogin to our main server.
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User


# On no match, the user is denied access.


############################################################
# You should add test accounts to the TOP of this file! #
# See the example user "bob" above.                      #
############################################################

First Cleartext-Password := "user"
        Service-Type = NAS-Prompt-User,
        Cisco-AVpair = "shell:priv-lvl=15"
$enab15$ Cleartext-Password := "enable"
        Service-Type = NAS-Prompt-User,
        Cisco-AVpair = "shell:priv-lvl=15"

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

Install net-tools and use the ifconfig command to check the ethernet addresses.	
Enter the netplan file using NANO.	
Enter the addressing information.	
Enter these commands to save the static IP config and restart freeradius.	
Do a radtest to confirm that a login would work.	

```
root@linux1:/etc/freeradius/3.0# apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
net-tools is already the newest version (1.60+git20180626.aebd88e-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 38 not upgraded.
root@linux1:/etc/freeradius/3.0# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe82:8119  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:82:81:19  txqueuelen 1000  (Ethernet)
        RX packets 2741  bytes 3275865 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1160  bytes 90063 (90.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 128  bytes 10576 (10.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 128  bytes 10576 (10.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

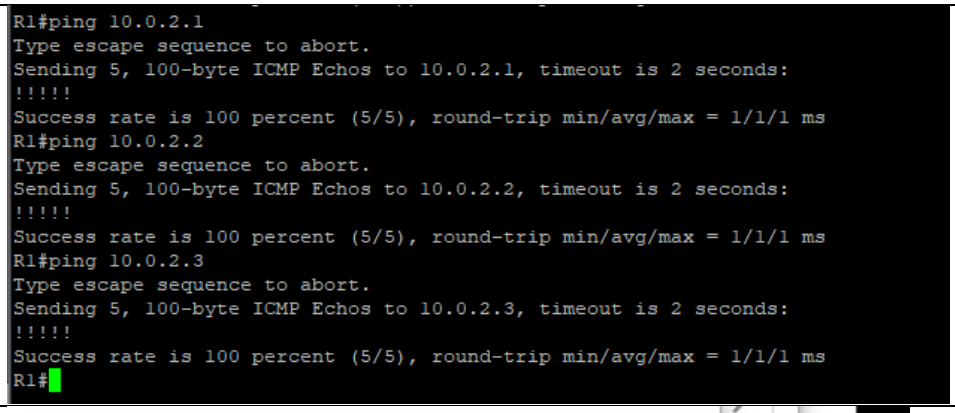
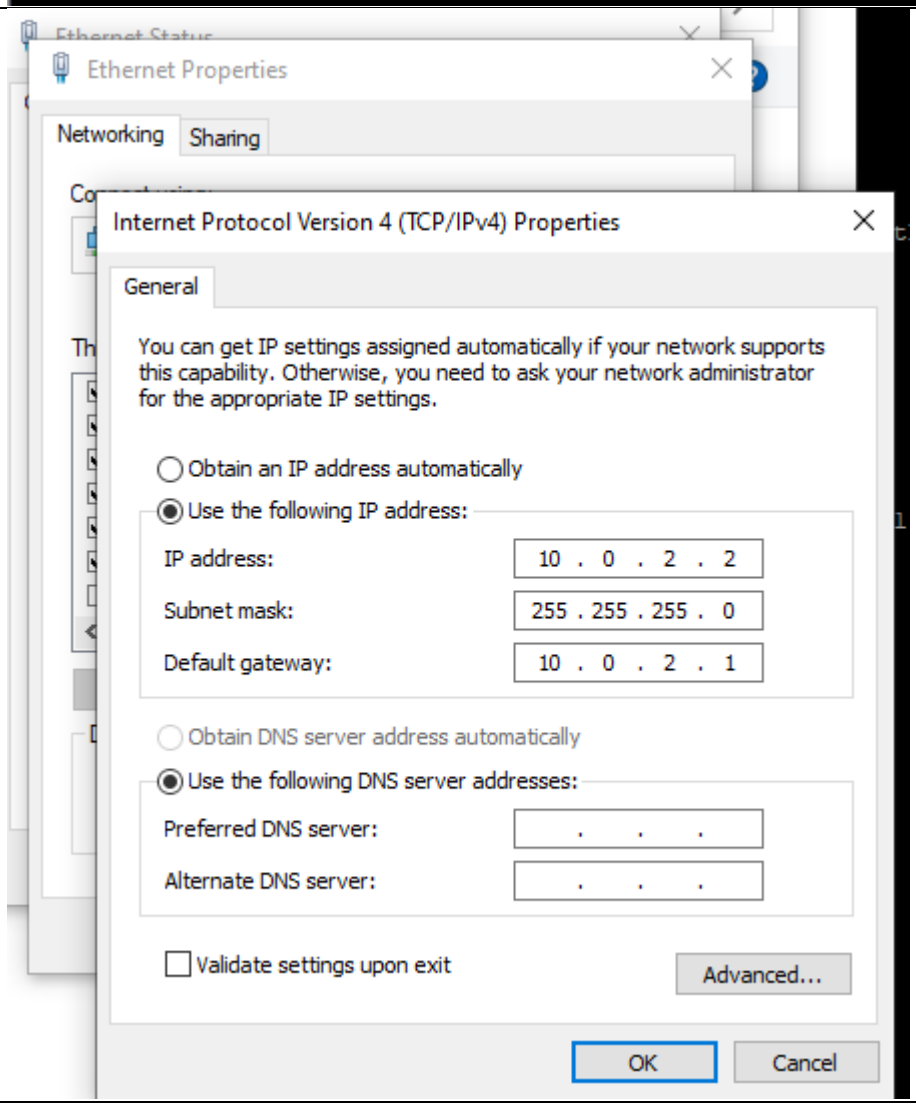
```
root@linux1:/etc/netplan# cd /etc/netplan/
root@linux1:/etc/netplan# ls
00-installer-config.yaml
root@linux1:/etc/netplan# nano /etc/netplan/00-installer-config.yaml
```

```
  GNU nano 4.8                    /etc/netplan/00-ins
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: true
      addresses: [10.0.2.3/24]
      gateway4: 10.0.2.1_
  version: 2
```

```
root@linux1:/etc/netplan# sudo netplan apply
root@linux1:/etc/netplan# service freeradius restart
root@linux1:/etc/netplan# _
```

```
root@linux1:/etc/netplan# service freeradius restart
root@linux1:/etc/netplan# freeradius -CX_
```

```
root@linux1:/etc/netplan# radtest First user localhost 0 testing123
Sent Access-Request Id 219 from 0.0.0.0:39123 to 127.0.0.1:1812 length 75
        User-Name = "First"
        User-Password = "user"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "user"
Received Access-Accept Id 219 from 127.0.0.1:1812 to 127.0.0.1:39123 length 51
        Service-Type = NAS-Prompt-User
        Cisco-AVPair = "shell:priv-lvl=15"
root@linux1:/etc/netplan#
```

If the router was configured correctly, you should have connectivity, see the configuration section for router configs.	
The PC the VM is hosted on should also have this as the ethernet addressing.	

Verification of Connection

```
AUTHORIZED ACCESS ONLY
Username: First
Password:

R1>enable
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
```

```
AUTHORIZED ACCESS ONLY
Username: hacker
Password:
UNAUTHORIZED ACCESS DETECTED
Username:
```

```
AUTHORIZED ACCESS ONLY
Username: Admin123
Password:

R1>enable
Password:
R1#
```

```
#######################################################
# You should add test accounts to the TOP of this file! #
# See the example user "bob" above.                     #
#######################################################

Admin123 Cleartext-Password := "user"
        Service-Type = NAS-Prompt-User,
        Cisco-AVpair = "shell:priv-lvl=15"
$enab15$ Cleartext-Password := "enable"
        Service-Type = NAS-Prompt-User,
        Cisco-AVpair = "shell:priv-lvl=15"
```

R1 RADIUS:

```
R1#show run | include RADIUS
aaa authentication login default group RADIUS enable
aaa authentication enable default group RADIUS enable
RADIUS server Linux1

R1#show run | include aaa
aaa new-model
aaa authentication banner ^CAUTHORIZED ACCESS ONLY^C
aaa authentication fail-message ^CUNAUTHORIZED ACCSS DETECTED^C
aaa authentication login default group RADIUS enable
aaa authentication enable default group RADIUS enable
aaa session-id common
```

RADIUS ROUTER CONFIG

```
version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname R1
!
boot-start-marker
boot-end-marker
```

```
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
aaa new-model
!
!
aaa authentication banner ^CAUTHORIZED ACCESS ONLY^C
aaa authentication fail-message ^CUNAUTHORIZED ACCESS DETECTED^C
aaa authentication login default group radius enable
aaa authentication enable default group radius enable
!
aaa session-id common
!
subscriber templating
vtp domain cisco
vtp mode transparent
!
multilink bundle-name authenticated
!
license udi pid ISR4321/K9 sn FDO220523GF
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
 mode none
!
interface GigabitEthernet0/0/0
 ip address 10.0.2.1 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto
!
```

```
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip tftp source-interface GigabitEthernet0
!
radius server Linux1
 address ipv4 10.0.2.3 auth-port 1812 acct-port 1813
 timeout 2
 retransmit 2
 key secretkey
!
control-plane
!
line con 0
 transport input none
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
End
```

Problems for RADIUS and TACACS+

There were, expectedly, many problems during configuration, testing, and troubleshooting, especially those stemming from the inexperience of the new interfaces and outdated software. The one that would end up causing the greatest confusion is the necessity to restart the protocol service after making major changes, such as changing the shared secret key or an IP address. This caused many understanding conflicts as configurations do not update and apply instantaneously, making certain changes and configurations not display properly from a user device perspective. This interfered with expectations of certain commands and confused the general understanding of whether a command functioned or not. Ultimately, the “service FreeRadius restart” command for RADIUS and the “sc start/stop TACACS.net” for TACACS+ became go-to commands after any edit.

For FreeRadius v3 and Oracle VirtualBox, there were relatively small issues in regard to downloading the proper bootstrap version for USB integration. This was done to download operating disk images and .exe files for the virtual machine. The problem mainly stemmed from the inability to access files from the USB with TACACS+ and transfer it to the VM. After some troubleshooting, I discovered that VirtualBox as a default supports USB 2.0, instead of USB 3.0, which was needed to file share with the latest USB’s. After an extension pack was found, the problem was resolved. All versions and options are

found on the Oracle VirtualBox website. Version 6.0 was used for this lab. An important configuration directed towards VirtualBox is the necessity to change the network adapter to a *bridged adapter*. This allows the virtual machine to share and connect their information via ethernet, where it would otherwise be isolated. This was the key solution to more than a couple pinging problems.

Other quicker issues relating to TACACS+ included the lack of permission to run TacTest commands, which could be fixed by using the *admin* command prompt, done by right-clicking the command prompt application. When TACACS+ needed to be restarted but the start command says that it is already running, stop the TACACS before trying to restart it. The wording for the commands must be very accurate, and even a slight mistype can lead to later bugs, as in some cases the interface will accept the incorrect command without notifying you. This led to a problem with my TACACS+ software in that the router was not connecting to the VM because the proper interface was still in its shutdown mode. With TACACS+ especially you needed to ensure that the right brackets were deleted to get the proper parts of the software working on the Windows Machine.

Conclusion

This revealing lab was indisputably valuable in the new interfaces to be familiar with. As my first useful application with Linux and VirtualBox, I learned and navigated a wide array of commands, specifically those of Ubuntu Linux, Oracle VirtualBox, and Notepad++. In the foreign environment, it was an achievement to be able to understand and execute the protocols fully and functionally. AAA and other security protocol and frameworks like CIA are essential parts of today's cybersecurity architecture, and continuing to improve and expand their use will lead to a more secure and safe world for all Internet users.