Mike Azure

Advanced Cisco CCNP Networking

AAA Configuration

Lab 7

Purpose

The purpose of this lab was to use a remote server to authenticate user access. We accomplished this by creating a Windows and Linux virtual machine running a RADIUS server that received and authenticated user access requests.

Background Information on Lab Concepts

AAA (Authentication, Authorization, Accounting) is a method used to securely authenticate and authorize users accessing Cisco routers. Imagine you are a network engineer employee at a large tech company. It is important that the network is secure. Therefore, whenever you access the routers at that company, you are required to login to an administrator account. It is worth noting that AAA allows permissions to be set for different user accounts, meaning entry level and senior employees can be granted different permissions. When the network employee logs into an account, the router uses AAA to verify the user. For this to function, the network engineer would have to set up a RADIUS (Remote Authentication Dial-In User Service) server, connected to the cisco router, that stores the users. The network engineer can also access the RADIUS server to view information such as what users accessed the routers and at what times. Overall, using a remote server to authenticate users significantly enhances security. RADIUS is commonly used on remote servers with AAA and can be configured on Windows or Linux operating systems. When a remote server is used, user tracking can also be utilized to log actions such as when a user logged on. Using AAA significantly enhances network security.

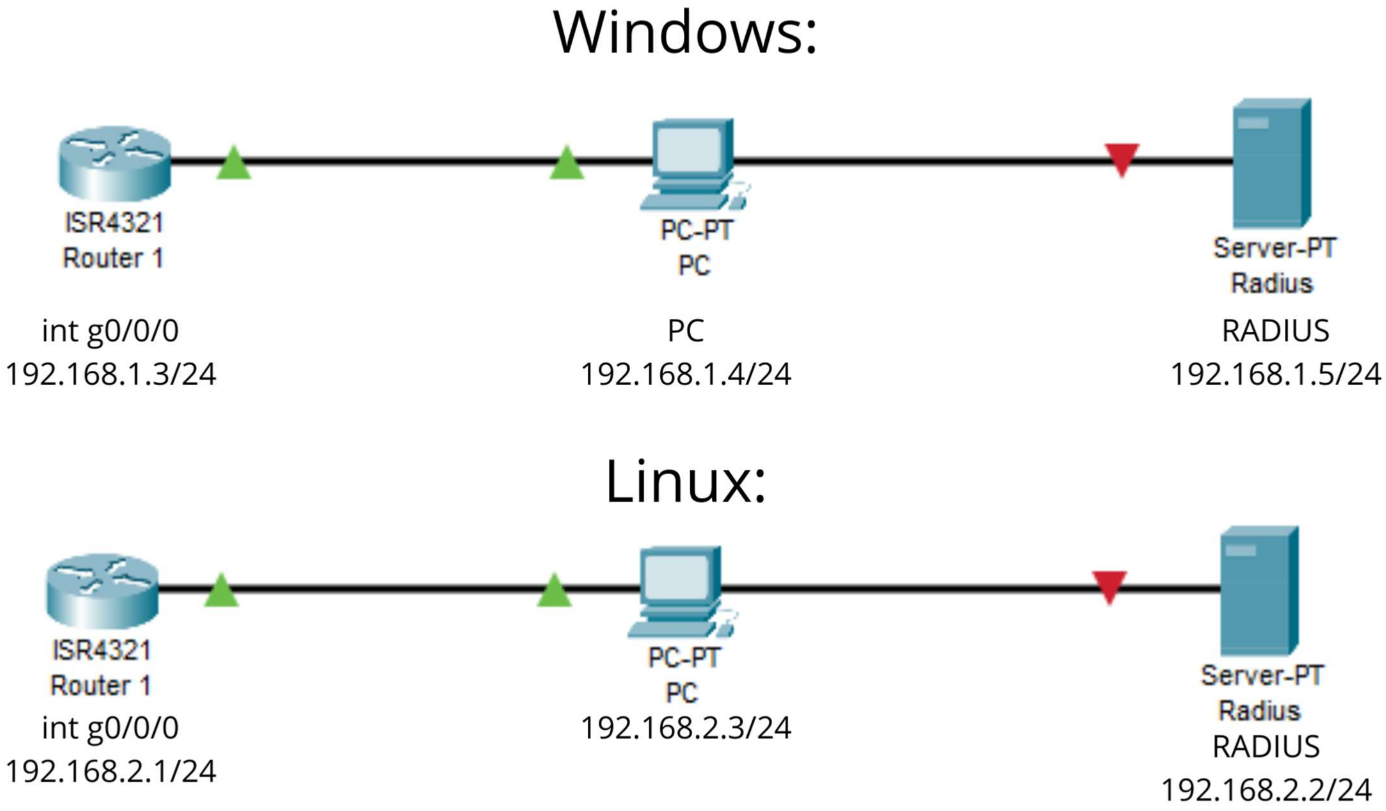
Lab Summary

In this lab, we configured a Cisco 4321 router to utilize AAA in order to authenticate users using a RADIUS server. We installed the RADIUS server on both a Windows and Linux virtual machine. We verified AAA functioned correctly by creating users on the RADIUS server and logging into them on the Cisco router.

Lab Commands

Command:	**Description:**
aaa new-model	Activates AAA
aaa authentication login default group radius local	Ensures usernames and passwords are verified by RADIUS. If RADIUS fails, the username and password are verified by the routers local user database.
radius server [server name] - address ipv4 [server address] - key [shared secret]	Sets RADIUS server name, IP address, and shared secret for secure connection between the router and RADIUS server.
test aaa group radius [username] [password] new-code	Sends RADIUS account validity verification request. Used for testing RADIUS without exiting privileged exec mode.

Network Diagram with IP’s



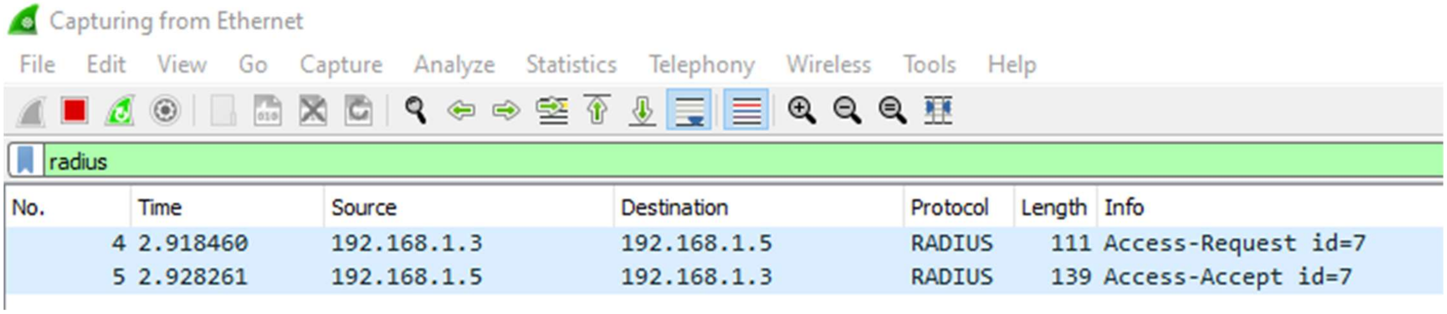
Configuration

Windows:

```
Router#show run
Building configuration...
Current configuration : 1406 bytes
Last configuration change at 17:40:55 UTC Mon Jun 6 2022
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
hostname Router
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 login default group radius local
aaa session-id common
subscriber templating
```

```
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO21441WDF
spanning-tree extend system-id
redundancy
 mode none
vlan internal allocation policy ascending
interface GigabitEthernet0/0/0
 ip address 192.168.1.3 255.255.255.0
 negotiation auto
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
interface Vlan1
 no ip address
 shutdown
ip forward-protocol nd
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
radius server freeradius
 address ipv4 192.168.1.5 auth-port 1645 acct-port 1646
 key cisco
control-plane
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
end
```

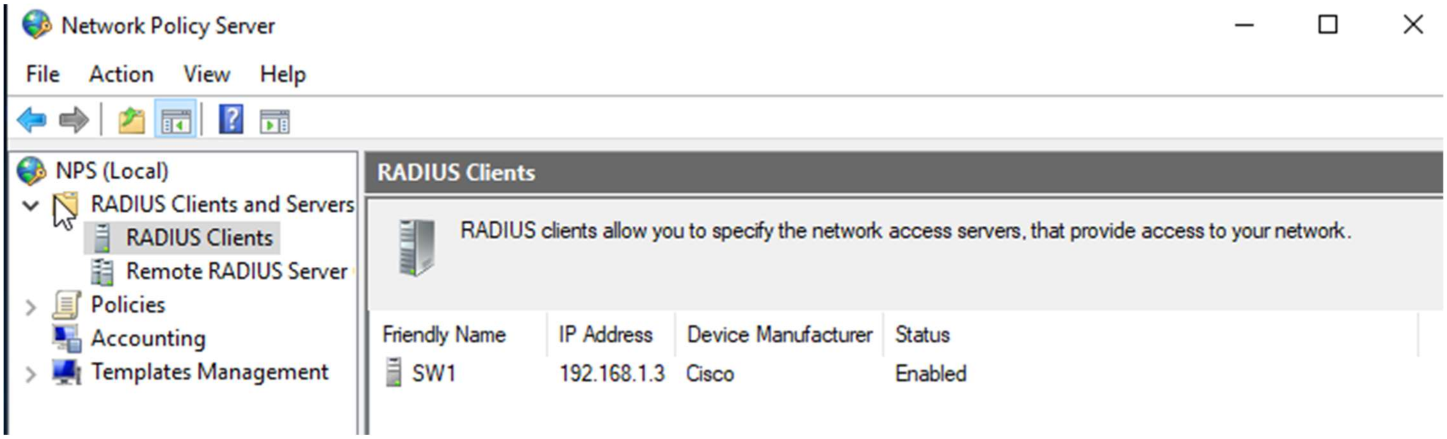
Proof of Connection:



radius

No.	Time	Source	Destination	Protocol	Length	Info
4	2.918460	192.168.1.3	192.168.1.5	RADIUS	111	Access-Request id=7
5	2.928261	192.168.1.5	192.168.1.3	RADIUS	139	Access-Accept id=7

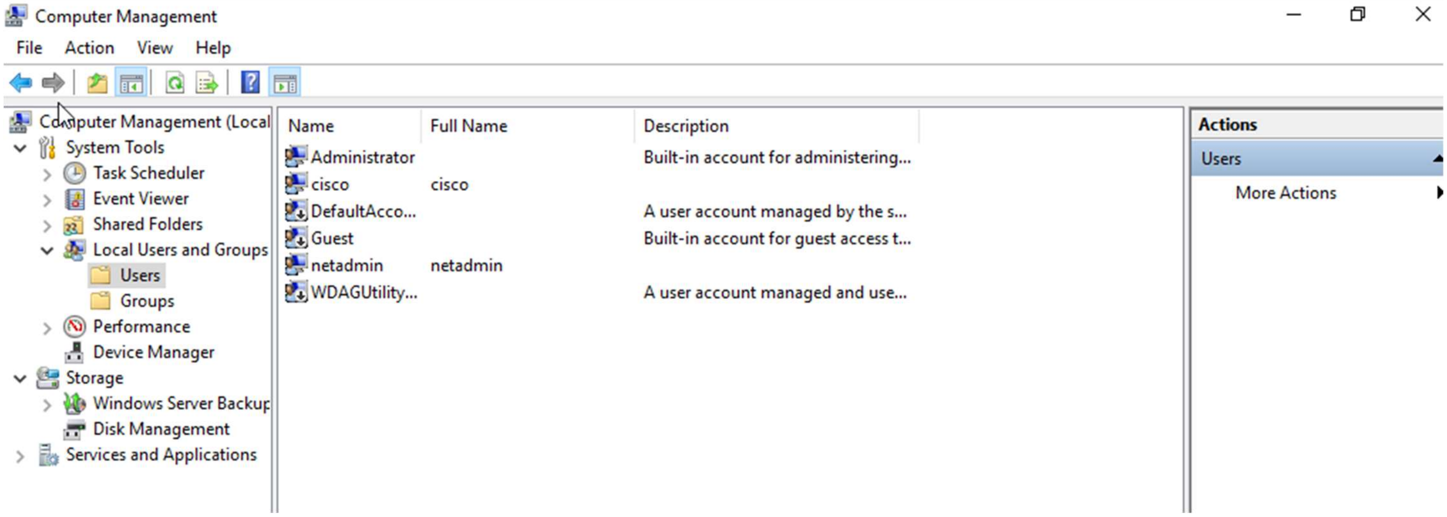
Radius Server:



RADIUS clients allow you to specify the network access servers, that provide access to your network.

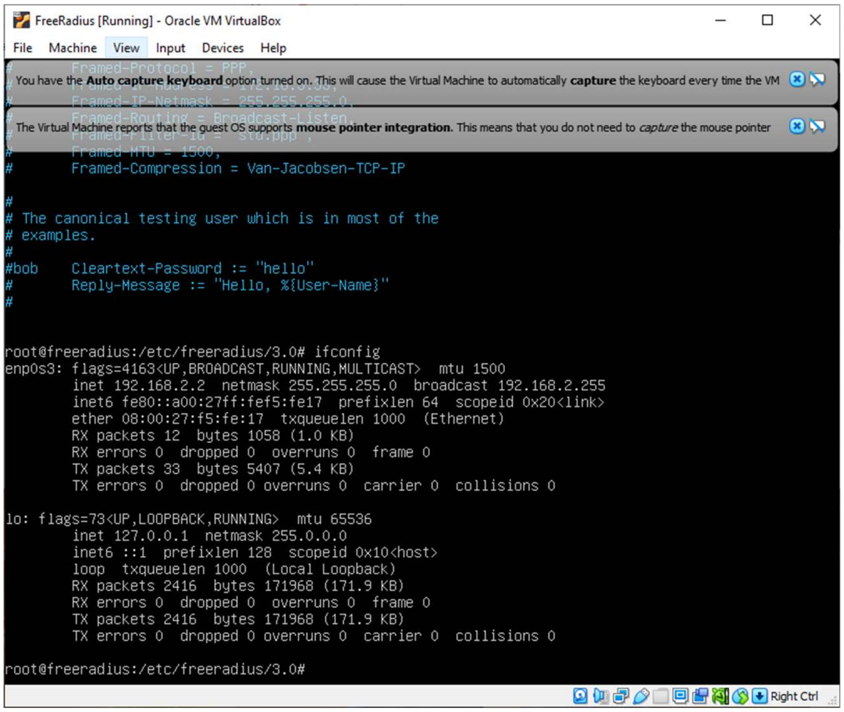
Friendly Name	IP Address	Device Manufacturer	Status
SW1	192.168.1.3	Cisco	Enabled

Accounts:



Name	Full Name	Description
Administrator		Built-in account for administering...
cisco	cisco	
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...
netadmin	netadmin	
WDAGUtility...		A user account managed and use...

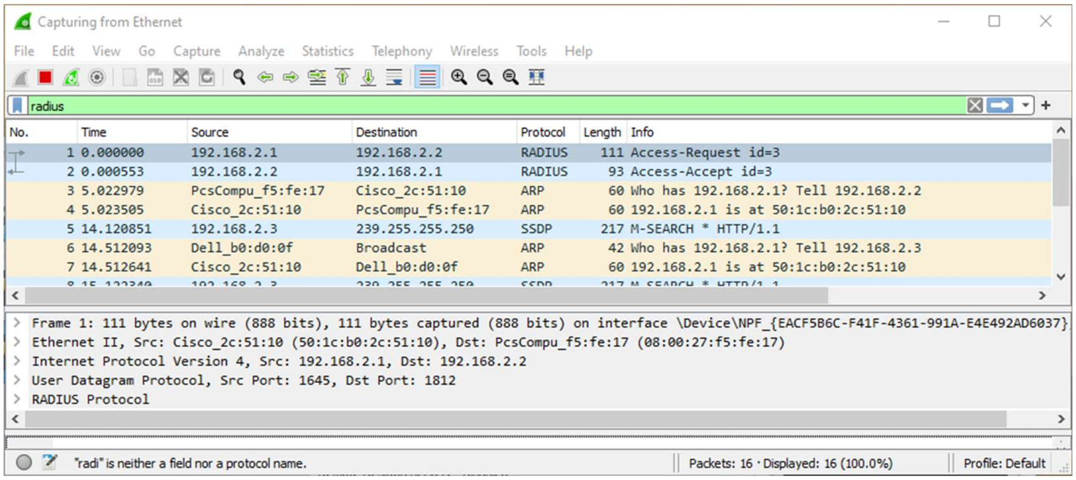
Linux:



You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer

```
#       Framed-Protocol = PPP,
#       Framed-IP-Address = 172.16.3.33,
#       Framed-IP-Netmask = 255.255.255.0,
#       Framed-Routing = Broadcast-Listen,
#       Framed-Filter-Id = "std.ppp",
#       Framed-MTU = 1500,
#       Framed-Compression = Van-Jacobsen-TCP-IP

#
# The canonical testing user which is in most of the
# examples.
#
#bob    Cleartext-Password := "hello"
#       Reply-Message := "Hello, %{User-Name}"
#


root@freeradius:/etc/freeradius/3.0# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.2  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::a00:27ff:fef5:fe17  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f5:fe:17  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 1058 (1.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 5407 (5.4 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 2416  bytes 171968 (171.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2416  bytes 171968 (171.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@freeradius:/etc/freeradius/3.0#
```

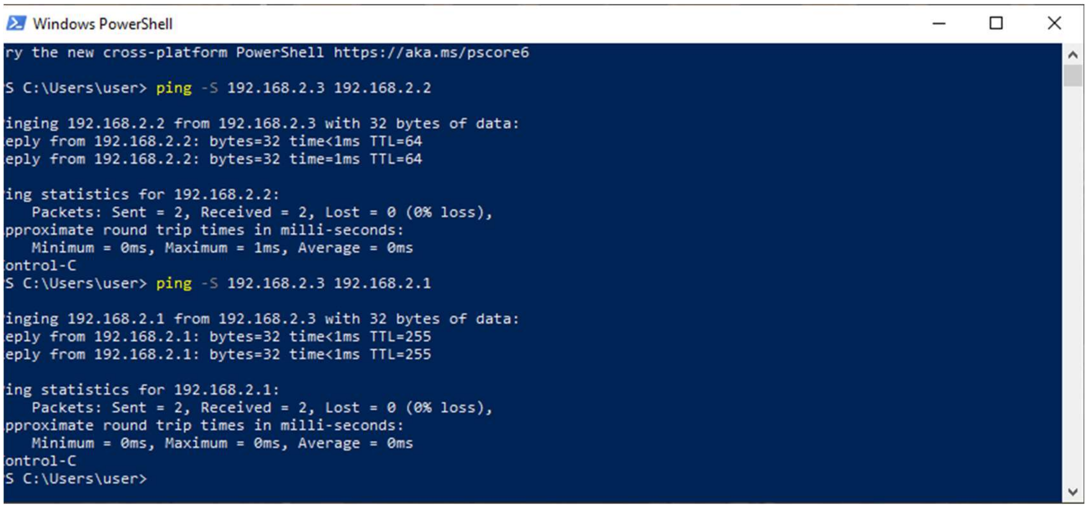


radius

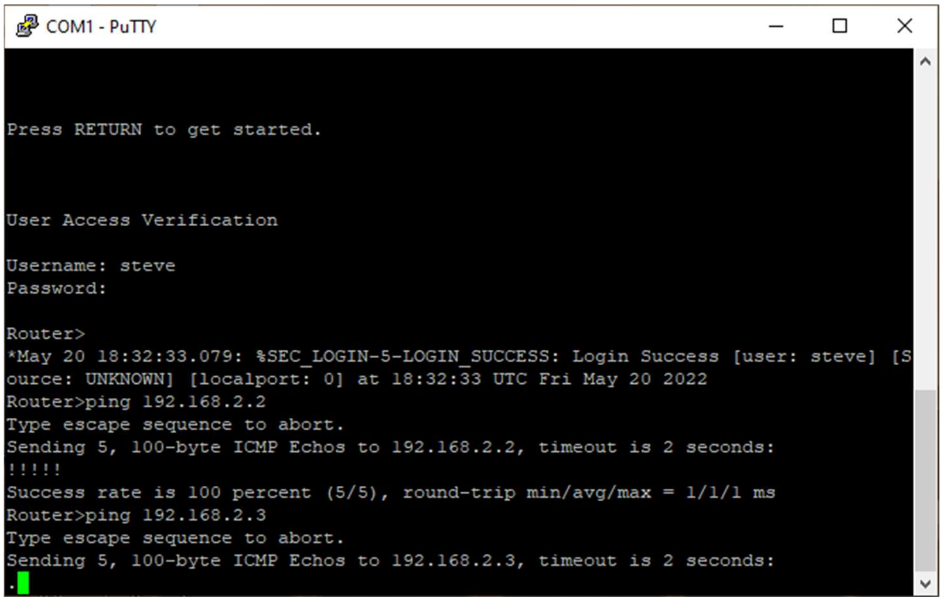
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.1	192.168.2.2	RADIUS	111	Access-Request id=3
2	0.000553	192.168.2.2	192.168.2.1	RADIUS	93	Access-Accept id=3
3	5.022979	PcsCompu_f5:fe:17	Cisco_2c:51:10	ARP	60	Who has 192.168.2.1? Tell 192.168.2.2
4	5.023505	Cisco_2c:51:10	PcsCompu_f5:fe:17	ARP	60	192.168.2.1 is at 50:1c:b0:2c:51:10
5	14.120851	192.168.2.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
6	14.512093	Dell_b0:d0:0f	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.3
7	14.512641	Cisco_2c:51:10	Dell_b0:d0:0f	ARP	60	192.168.2.1 is at 50:1c:b0:2c:51:10
8	15.122340	192.168.2.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

```
> Frame 1: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF_{EACF5B6C-F41F-4361-991A-E4E492AD6037}
> Ethernet II, Src: Cisco_2c:51:10 (50:1c:b0:2c:51:10), Dst: PcsCompu_f5:fe:17 (08:00:27:f5:fe:17)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.2
> User Datagram Protocol, Src Port: 1645, Dst Port: 1812
> RADIUS Protocol
```

"radi" is neither a field nor a protocol name. | Packets: 16 · Displayed: 16 (100.0%) | Profile: Default



```
ry the new cross-platform PowerShell https://aka.ms/pscore6

S C:\Users\user> ping -S 192.168.2.3 192.168.2.2

inging 192.168.2.2 from 192.168.2.3 with 32 bytes of data:
eply from 192.168.2.2: bytes=32 time<1ms TTL=64
eply from 192.168.2.2: bytes=32 time=1ms TTL=64

ing statistics for 192.168.2.2:
   Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 1ms, Average = 0ms
ontrol-C
S C:\Users\user> ping -S 192.168.2.3 192.168.2.1

inging 192.168.2.1 from 192.168.2.3 with 32 bytes of data:
eply from 192.168.2.1: bytes=32 time<1ms TTL=255
eply from 192.168.2.1: bytes=32 time<1ms TTL=255

ing statistics for 192.168.2.1:
   Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
ontrol-C
S C:\Users\user>
```



```
Press RETURN to get started.



User Access Verification

Username: steve
Password:

Router>
*May 20 18:32:33.079: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: steve] [S
ource: UNKNOWN] [localport: 0] at 18:32:33 UTC Fri May 20 2022
Router>ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router>ping 192.168.2.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
.
```

Problems

When building the RADIUS configuration for Windows, we encountered issues on how to successfully create user accounts. One issue was the excessive password length and character requirements by Windows. However, a larger issue was what method to use when creating user accounts: the active directory or the local users and groups built into Windows computer management. We were unable to successfully login to user accounts when creating accounts using the active directory. However, once the active directory was uninstalled and accounts were created through the local users and groups built into Windows computer management, they functioned correctly.

Another problem we encountered was a lack of clarity on the documentation for setting up AAA. Our Cisco 4321 routers were running a different syntax than was outlined in the documentation for setting up AAA. We remedied this issue by using other online resources and “question marking” commands in the Cisco IOS.

Conclusions

In conclusion, we setup AAA on Windows and Linux using a RADIUS server. We setup RADIUS on a virtual machine and used AAA running on the router to verify the usernames and passwords of users attempting to login. Using RADIUS to store usernames and passwords significantly enhances network security. It allows for different user accounts with different permissions, and it logs user activity.

Instructor Signoff