TACACS+ and Radius

Cisco CCNP Lab 5

Mason and Hoffman – Period 6-8

Jeffrey Zhang

Purpose

The purpose of this lab is to configure remote authentication protocols such as TACACS+ and Windows Radius to log into cisco network management devices.

Background

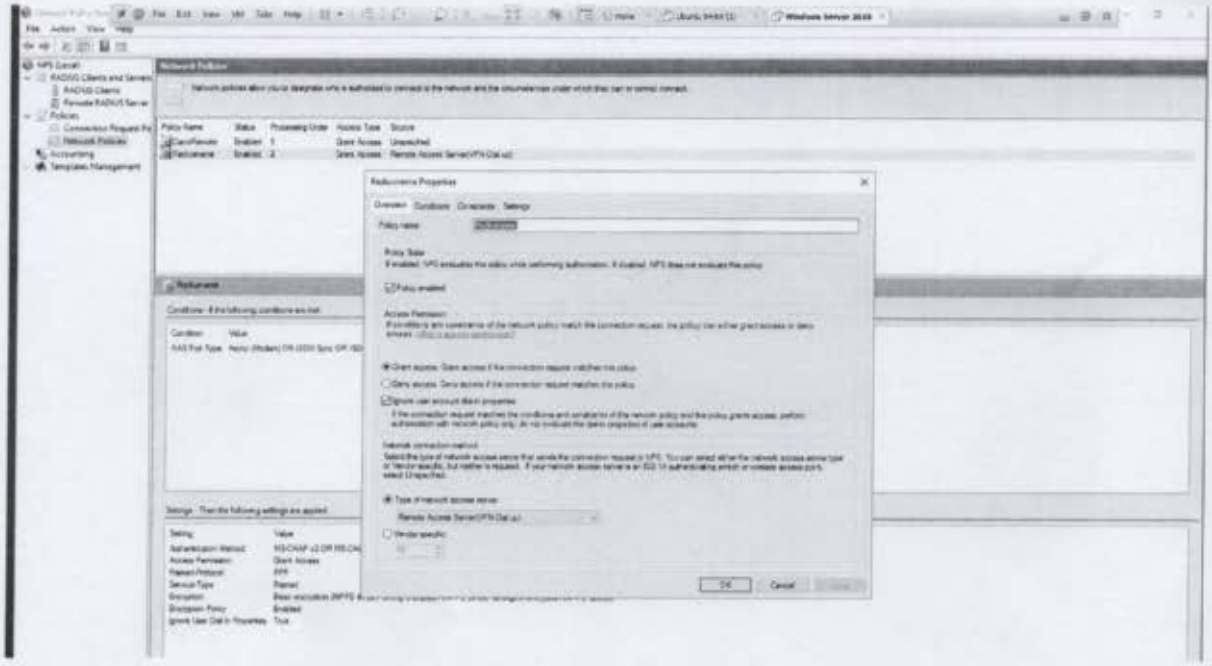
Local authentication that is performed on routers and switches tend to have security that isn't optimal, as such, could be bypassed easily by exploiting maintenance modes during boot. Remote authentication methods such as TACACS+ and Windows Radius will prevent the user from bypassing the authentication during boot.

Lab Summary

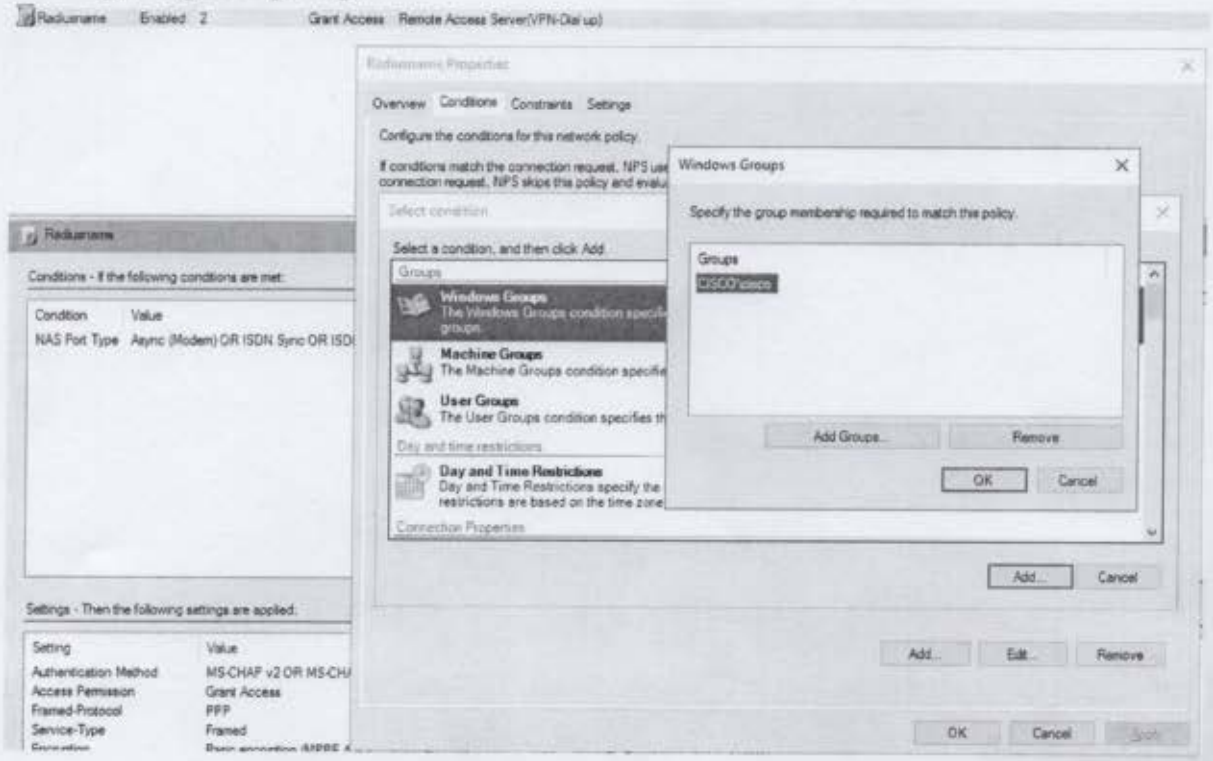
In this lab, my lab partner (Jimmy) and I configured TACACS+ and Windows Radius. We made 2 virtual machines that connected to real life Cisco 2901 routers; one for configuring TACACS+ and one for configuring Windows Radius.

I configured the virtual machine with Windows Radius using Windows Server 2016.

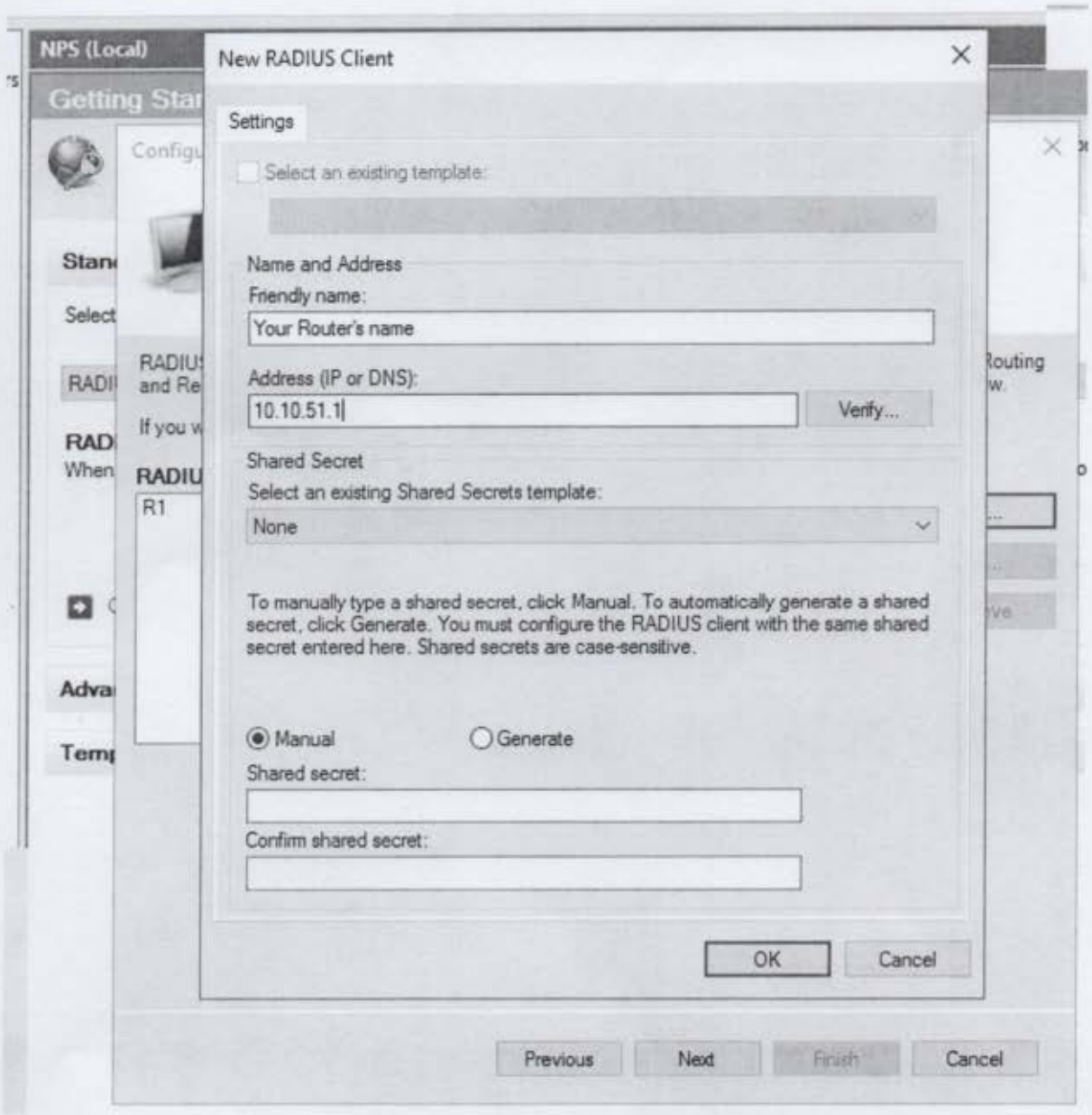
The process begins with initiating the various network policies required for configuring the routers.



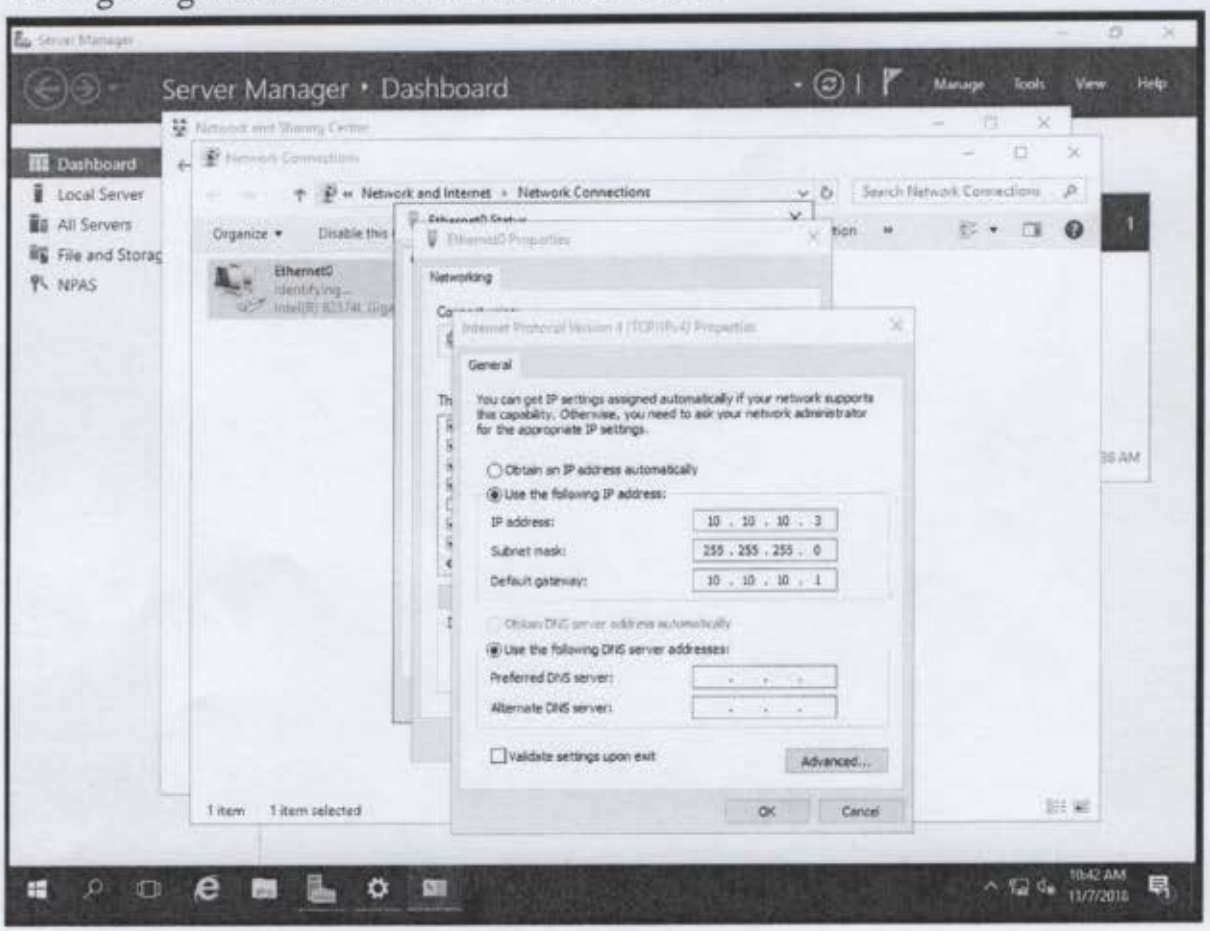
Configuring the groups



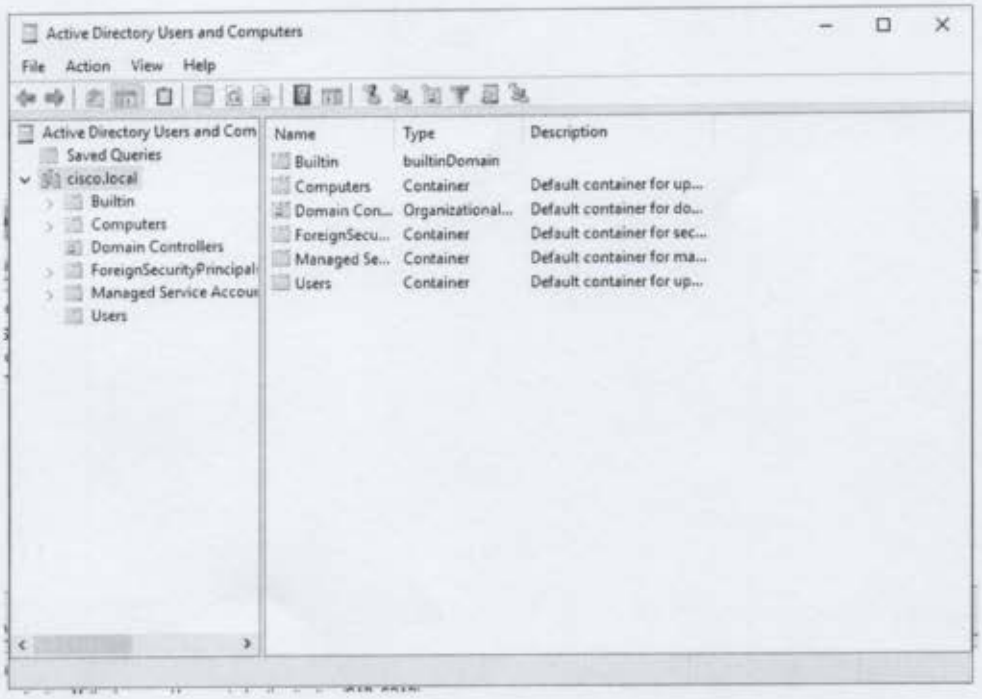
Adding the Windows Radius router

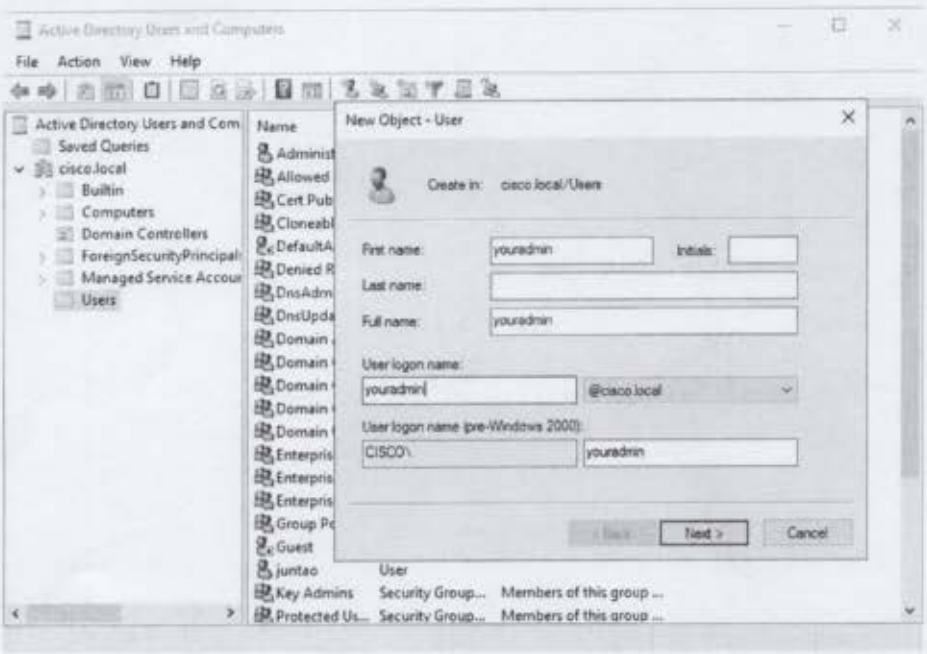


Configuring the IP address of the server itself.

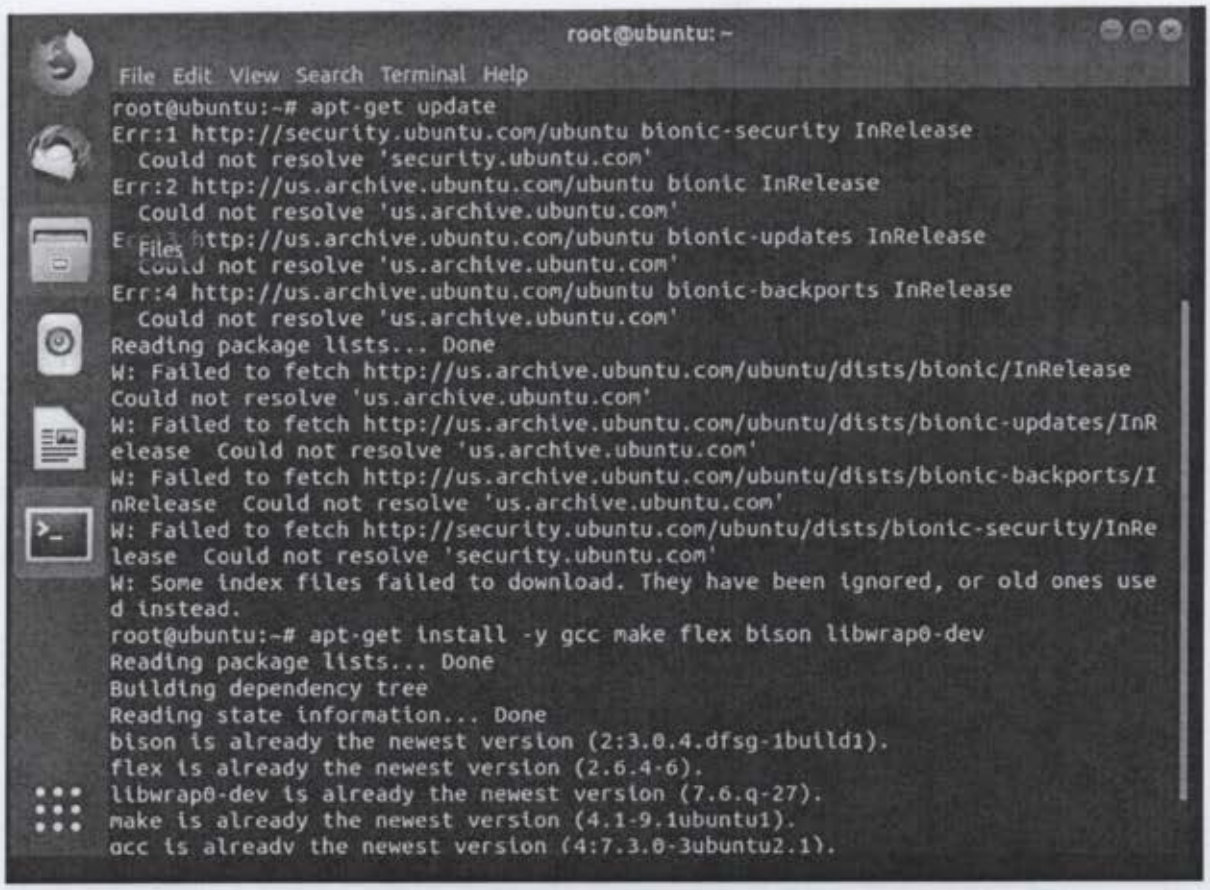


After setting up the Radius client on the server, we entered active directory services, in which we added our user group, domain, and user to log into our router.


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
cisco.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
Name Type Description
Builtin builtinDomain
Computers Container Default container for up...
Domain Con... Organizational... Default container for do...
ForeignSecu... Container Default container for sec...
Managed Se... Container Default container for ma...
Users Container Default container for up...


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
cisco.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accou
Users
New Object - User
Create in: cisco.local/Users
First name: youradmin
Initials:
Last name:
Full name: youradmin
User logon name:
youradmin
@cisco.local
User logon name (pre-Windows 2000):
CISCO\
youradmin
Next >
Cancel
juntao User
Key Admins Security Group... Members of this group ...
Protected Us... Security Group... Members of this group ...

My partner Jimmy used a Linux Ubuntu Virtual Machine to configure TACACS+. He entered the terminal executed the "sudo –i" and then "apt-get update" so that he could install other services through the terminal.



After downloading TACACS+ services, he edited the configuration file section with "nano …" to setup TACACS+ remote authentication protocol.

```
root@ubuntu:~# nano /etc/tacacs+/tac_plus.conf
root@ubuntu:~#
```

Inside the configuration file, I defined the key (domain) between my server and router, the group with privilege levels and users in such groups.

```
key = testing123

group = admin {
        default service = permit
        service = exec {
                priv-lvl= 15
        }
}

user= sourish {
        member = admin
        login = cleartext cisco
}
user= random {
        member =admin
        login = cleartext cisco
}
```

The last step was to check port 49 with the command "lsof -i :49" to see whether TACACS+ protocol is running. To finalize the setup of TACACS+ protocol, the command must be case sensitive in order for it to work.

Configurations

Below are the router configurations for the Windows Radius router.

```
hostname R1

boot-start-marker

boot-end-marker

enable password cisco
```

```
aaa new-model

aaa authentication login default group radius
local

aaa authorization exec default group radius
if-authenticated

Username backup password cisco

aaa session-id common

memory-size iomem 10

ip cef

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

voice-card 0

license udi pid CISCO2901/K9 sn FTX1704Y038

license accept end user agreement

license boot module c2900 technology-package
securityk9

license boot module c2900 technology-package
uck9

vtp domain cisco
```

```
vtp mode transparent
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
interface Serial0/0/1
```

```
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
no ip httbackp server
no ip http secure-server
radius-server host 10.10.10.3 key 123456
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 password 123456
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
```

```
 transport output pad telnet rlogin lapb-ta
mop udptn v120 ssh
 stopbits 1
line vty 0 4
 transport input all
scheduler allocate 20000 1000
end
```

TACACS+ Router configurations:

```
hostname R1

aaa new-model
aaa authentication login default group tacacs+
local
aaa authentication enable default group
tacacs+ enable
aaa authorization config-commands
aaa authorization commands 0 default group
tacacs+ none
```

```
aaa authorization commands 15 default group
tacacs+ none
aaa accounting send stop-record authentication
failure
aaa accounting update newinfo periodic 5
aaa accounting exec default start-stop group
tacacs+
aaa accounting network default start-stop
group tacacs+

aaa session-id common
ip domain name cisco.com
no ipv6 cef

vtp domain cisco
vtp mode transparent
username backup password 0 cisco

interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
```

```
 duplex auto
 speed auto
 no shutdown
ip tacacs source-interface GigabitEthernet0/0
tacacs-server host 10.10.10.3
tacacs-server directed-request
tacacs-server key testing123
end
```

Problems

Since we never dealt with Windows server 2016 before, we had to solely rely on the internet to go through the lab. The main issue was, most of the guides that we found were out of date, and didn't match our current version of Windows server. So we had to take reliable patches of certain credible articles to piece together the process of executing Windows Radius successfully on Windows Server 2016. The router configurations were mostly up to date however. While Jimmy configured TACACS+, he ran into the same issue where a lot of the guides setting up TACACS+ were out of date, or weren't relevant to our current situation.

Conclusion

This lab aims to teach us how to configure remote authentications over the less secure local authentications on cisco devices. This also serves as my first lab configuring Windows Radius on a virtual machine, connected to a physical cisco router.