TACACS and RADIUS+ Lab

# CCNP Lab 4

## Axel Li

## 5 November 2018

# Purpose

The purpose of this lab was to practice implementing server and client configurations of TACACS+ and RADIUS. For both TACACS+ and RADIUS, we were to configure a server on a virtual machine (running Ubuntu and Windows, respectively) and configure a router as the corresponding client. We then had to confirm that authentication was functioning correctly with only authenticated users able to access the routers.

# Background

TACACS+, standing for Terminal Access Controller Access-Control System Plus, is a protocol handling remote AAA through a centralized server developed by CISCO. The protocol can implement all aspects of authentication, authorization, and accounting either together or separately through facilitating communication between a client and a TACACS+ server via TCP port 49. When users attempt to access a device or input a command, the client will communicate with the server to confirm that that user is authenticated or authorized. The commands that are configured by users will likewise be communicated and recorded in the server for accounting. Unlike RADIUS, TACACS+ encrypts the full contents of each packet and provides command by command authorization, and thus is more secure. In corporate settings, TACACS+ is typically utilized for remote management of network devices.

RADIUS, Remote Access Dial-In User Service, is a similar client/server AAA protocol. RADIUS differs with TACACS+ in that it couples authentication and authorization together, utilizes UDP by default, and only encrypts passwords in the access-request packet. Functionally RADIUS provides similar services to TACACS+, using a server to check a user’s credentials, but as RADIUS is considered insecure, it is used more often for allowing access to regular network users rather than to network administrators. For example, it is commonly used by ISPs to manage access to the Internet, internal, or wireless networks.

# Summary

Before physically configuring the devices, my partner and I planned out the addressing and ports. In a saved file containing the configuration of the routers, we set up the necessary TACACS+, RADIUS, and AAA commands, then pasted the configuration into the routers. For the TACACS+ server, we installed the TACACS+ daemon and edited the configuration files manually to add the required users and user groups, then started the service to run on the virtual machine. The RADIUS server was more complex, requiring us to promote the active directory domain service to a new forest, configure a connection request policy, configure a RADIUS client and shared key, create a new user group and add a configured user, and configure a network policy.

To test the devices, we then input various show and ping commands to confirm that the network was set up and working as intended, then we attempted to log in via console and telnet to the routers to test that the authentication was correct.

In addition to the authentication required in the lab, my partner and I were able to set up basic command authorization and accounting for TACACS+. We created two users for this purpose, one of which was blocked from entering the show running-config and configure commands to confirm that authorization was correctly working.

# Commands

The key commands used in this lab for the routers were:

aaa new-model - enables new access control commands and functions

aaa authentication login default group tacacs+ local line none – configures AAA authentication via TACACS+ at login (defaults to the local database, then line password if unavailable)

aaa authentication enable default group tacacs+ enable none – configures AAA authentication via TACACS+ for when users attempt to access the privileged command level (defaults to the enable password if unavailable)

tacacs server [tacacs server configuration name] – enters TACACS+ server configuration mode

address ipv4 172.16.1.2 – specifies the IP address of the TACACS+ server

key [shared key] – specifies the shared key between the TACACS+ server and client

aaa group server tacacs+ [server-group name] – defines an AAA TACACS+ server group with the specified group name

server name [tacacs server name] – adds the TACACS+ server with the specified name to the server group

ip tacacs source-int g0/0 - specifies the interface for TACACS+

login authentication default - enables AAA authentication for logins

test aaa group tacacs+ [username] [password] new-code - attempts to log in via TACACS+ with the specified username and password

aaa authentication login default group radius local – configures AAA authentication via RADIUS at login (defaults to the local database if unavailable)

aaa authorization exec default group radius if-authenticated - configures AAA authentication via RADIUS for when users attempt to access the privileged command level (does not request if already authenticated)

username [username] privilege 15 secret [password] - create a local username and password for access to router with privilege 15 (for debugging and as a backup)  
radius-server host [server IP address] key [shared-key] - specifies the RADIUS host by IP address and the authentication/encryption key shared between the client and the RADIUS server

The key commands used in this lab for the TACACS+ server running on Ubuntu were:

service tacacs\_plus start – starts the TACACS+ daemon

tac\_pwd – produces a DES encryption of a specified password

systemctl status tacacs\_plus.service – checks the status of the TACACS+ daemon

nano – edits the contents of a specified file

# Tables and Diagrams

TACACS+ configurations:

|  |  |  |
| --- | --- | --- |
| user | “tacuser” | “netuser” |
| login | “taclogin” | “netlogin” |
| enable | “tacenable” | “netenable” |
| authorization | permit all | deny show running-config  deny configure  permit all |

TACACS+ IP Addresses:

|  |  |
| --- | --- |
| TACACS+ Client | 172.16.1.1 |
| TACACS+ Server | 172.16.1.2 |

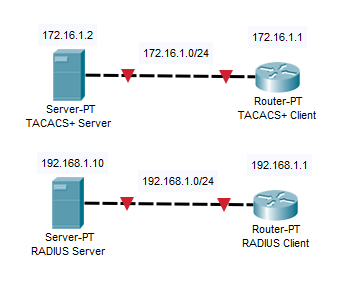
RADIUS configurations:

|  |  |
| --- | --- |
| user | “username” |
| login | “rad\_password1” |

RADIUS IP Addresses:

|  |  |
| --- | --- |
| RADIUS Client | 192.168.1.1 |
| RADIUS Server | 192.168.1.10 |

Topology Diagram:



# Configurations

\*extraneous information may be omitted\*

**TACACS+ Router:**

**R1#show tacacs**

Tacacs+ Server -  public :

              Server name: tacauth

           Server address: 172.16.1.2

              Server port: 49

             Socket opens:       103

            Socket closes:        103

            Socket aborts:          0

            Socket errors:          0

          Socket Timeouts:          0

  Failed Connect Attempts:          3

       Total Packets Sent:        129

       Total Packets Recv:        129

\*taken when “tacuser” logged in via console, “netuser” logged in via telnet\*

**R1#show aaa sessions**

Total sessions since last reload: 19

Session Id: 40

  Unique Id: 30

  User Name: tacuser

  IP Address: 0.0.0.0

  Idle Time: 0

  CT Call Handle: 0

Session Id: 47

  Unique Id: 32

  User Name: netuser

  IP Address: 172.16.1.10

  Idle Time: 0

  CT Call Handle: 0

\*taken with netuser\*

**R1#configure terminal**

Command authorization failed.

\*taken with “netuser”\*

**R1#show running-config**

Command authorization failed.

\*taken with “tacuser”\*

**R1#show running-config**

Building configuration...

Current configuration : 2548 bytes

Last configuration change at 20:43:52 UTC Fri Nov 2 2018

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname R1

enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

aaa new-model

aaa group server tacacs+ tacser

server name tacauth

aaa authentication login default group tacacs+ local line none

aaa authentication enable default group tacacs+ enable none

aaa authorization config-commands

aaa authorization exec default group tacacs+ if-authenticated

aaa authorization commands 0 default group tacacs+ if-authenticated

aaa authorization commands 15 default group tacacs+ if-authenticated

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 0 default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

interface GigabitEthernet0/0

ip address 172.16.1.1 255.255.255.0

duplex auto

speed auto

ip tacacs source-interface GigabitEthernet0/0

tacacs server tacauth

address ipv4 172.16.1.2

key 7 03105A080D0A38

line con 0

password 7 0205085A1815

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

transport input all

line vty 5 15

transport input all

scheduler allocate 20000 1000

end

**Ubuntu TACACS+ Server:**

**/etc/tacacs+/tac\_plus.conf**

accounting file = /var/log/tac\_plus.acct

key = tackey

group = network {

default service = permit

cmd = configure {

deny .\*

}

cmd = show {

deny running-config

}

}

user = netuser {

member = network

login = des 0DkzB4EbGjgBw

enable = des oNfJnxCB/lqS.

}

group = admin {

default service = permit

}

user = tacuser {

member = admin

login = des BIOVLNkpdP7PI

enable = des QMxu0r.4.3cDU

}

**/etc/default/tacacs+**

DAEMON\_OPTS="-C /etc/tacacs+/tac\_plus.conf"

/var/log/tac\_plus.acct

Nov  2 13:26:35 172.16.1.1 backup tty0 async stop task\_id=9 timezone=UTC service=shell priv-lvl=0 cmd=exit <cr>

Nov  2 13:26:35 172.16.1.1 backup tty0 async stop task\_id=6 timezone=UTC service=shell disc-cause=1 disc-cause-ext=9 pre-session-time=13 elapsed\_time=82 stop\_time=1541191589

Nov  2 13:26:39 172.16.1.1 netuser tty0 async start task\_id=11 timezone=UTC service=shell

Nov  2 13:26:43 172.16.1.1 netuser tty0 async stop task\_id=11 timezone=UTC service=shell priv-lvl=0 cmd=enable <cr>

Nov  2 13:26:46 172.16.1.1 netuser tty0 async stop task\_id=12 timezone=UTC service=shell priv-lvl=15 cmd=show running-config <cr>

Nov  2 13:26:54 172.16.1.1 netuser tty388 172.16.1.10 start task\_id=14 timezone=UTC service=shell

Nov  2 13:26:55 172.16.1.1 netuser tty388 172.16.1.10 stop task\_id=14 timezone=UTC service=shell priv-lvl=0 cmd=enable <cr>

Nov  2 13:36:49 172.16.1.1 netuser tty0 async stop task\_id=11 timezone=UTC service=shell disc-cause=4 disc-cause-ext=47 pre-session-time=4 elapsed\_time=610 stop\_time=1541192205

Nov  2 13:37:00 172.16.1.1 netuser tty388 172.16.1.10 stop task\_id=14 timezone=UTC service=shell disc-cause=4 disc-cause-ext=47 pre-session-time=4 elapsed\_time=606 stop\_time=1541192216

Nov  2 13:54:21 172.16.1.1 tacuser tty0 async start task\_id=19 timezone=UTC service=shell

Nov  2 13:54:23 172.16.1.1 tacuser tty0 async stop task\_id=19 timezone=UTC service=shell priv-lvl=0 cmd=enable <cr>

Nov  2 13:55:57 172.16.1.1 tacuser tty0 async stop task\_id=20 timezone=UTC service=shell priv-lvl=0 cmd=exit <cr>

Nov  2 13:55:57 172.16.1.1 tacuser tty0 async stop task\_id=19 timezone=UTC service=shell disc-cause=1 disc-cause-ext=9 pre-session-time=18 elapsed\_time=96 stop\_time=1541193353

Nov  2 13:56:04 172.16.1.1 stuff tty388 172.16.1.10 start task\_id=22 timezone=UTC service=shell

Nov  2 13:56:05 172.16.1.1 stuff tty388 172.16.1.10 stop task\_id=22 timezone=UTC service=shell priv-lvl=0 cmd=enable <cr>

Nov  2 13:56:09 172.16.1.1 stuff tty388 172.16.1.10 stop task\_id=23 timezone=UTC service=shell priv-lvl=0 cmd=enable <cr>

**RADIUS Client:**

**R2# show run**

service password-encryption

hostname R2

aaa new-model  
  
aaa authentication login default group radius local  
aaa authorization exec default group radius if-authenticated  
  
aaa session-id common  
  
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

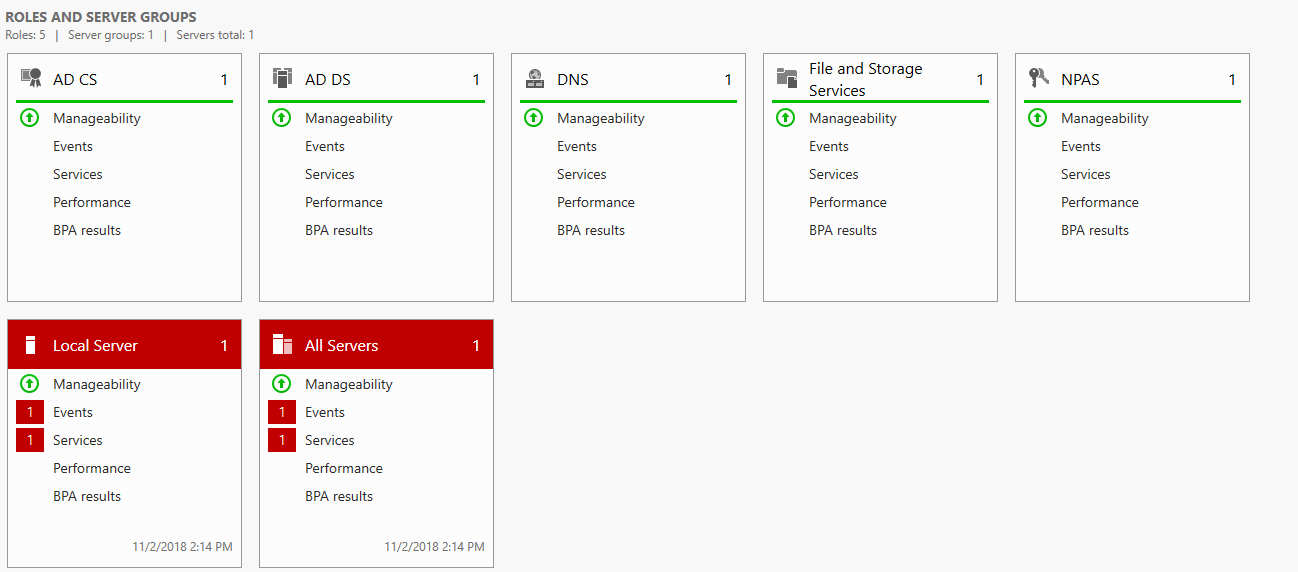
interface GigabitEthernet0/0  
 ip address 192.168.1.1 255.255.255.0  
 no shutdown  
 duplex auto  
 speed auto  
interface GigabitEthernet0/1  
 no ip address  
 shutdown  
 duplex auto  
 speed auto  
radius-server host 192.168.1.10 key 7 1303021C5A5E57

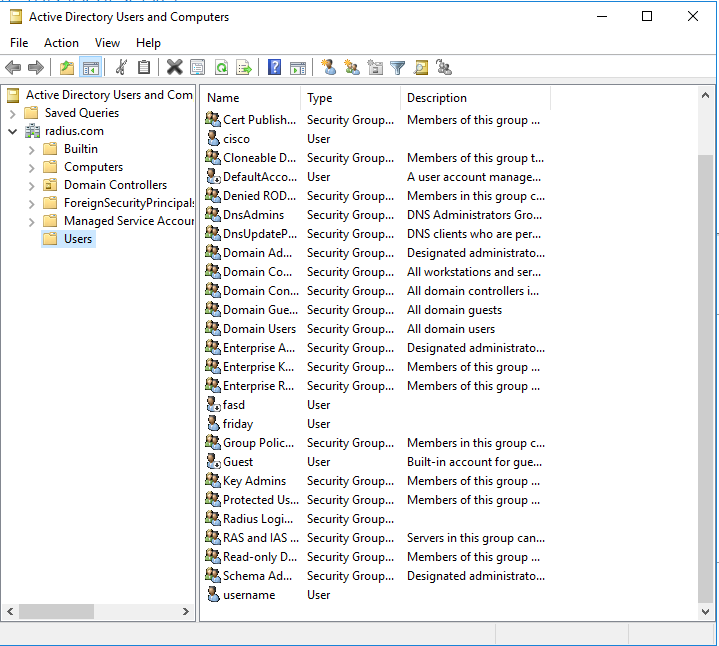
**R2# show radius server-group all**

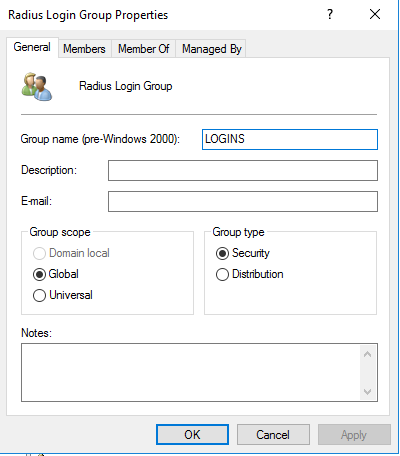
Server group radius  
    Sharecount = 1  sg\_unconfigured = FALSE  
    Type = standard  Memlocks = 1  
    Server(192.168.1.10:1645,1646) Transactions:  
    Authen: 26  Author: 0    Acct: 0  
    Server\_auto\_test\_enabled: FALSE  
     Keywrap enabled: FALSE

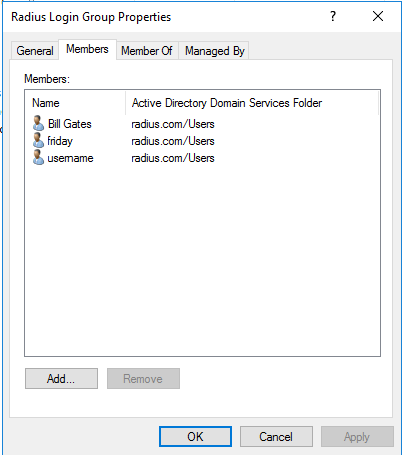
**R2# show radius statistics**  
                                  Auth. Acct. Both  
         Maximum inQ length:         NA NA 1  
       Maximum waitQ length:         NA NA 1  
       Maximum doneQ length:         NA NA 1  
       Total responses seen:         14 0 14  
     Packets with responses:         14 0 14  
  Packets without responses:          3 0 3  
  Access Rejects           : 6  
 Average response delay(ms):          5 0 5  
 Maximum response delay(ms):         32 0 32  
  Number of Radius timeouts:         12 0 12  
       Duplicate ID detects:          0 0 0  
 Buffer Allocation Failures:          0 0 0  
Maximum Buffer Size (bytes):        104 0 104  
Malformed Responses        : 0 0      0  
Bad Authenticators         : 0 0      0  
Unknown Responses          : 0 0      0  
 Source Port Range: (2 ports only)  
 1645 - 1646  
 Last used Source Port/Identifier:  
 1645/17  
 1646/0  
  
  Elapsed time since counters last cleared: 1h37m  
Radius Latency Distribution:  
<= 2ms :          5 0  
3-5ms  :    6 0  
5-10ms :          1 0  
10-20ms:          1 0  
20-50ms:          1 0  
50-100m:          0 0  
>100ms :          0 0  
  
Current inQ length  : 0  
Current doneQ length: 0

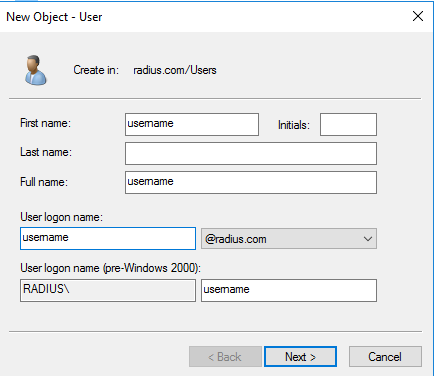
**Windows RADIUS Server:**

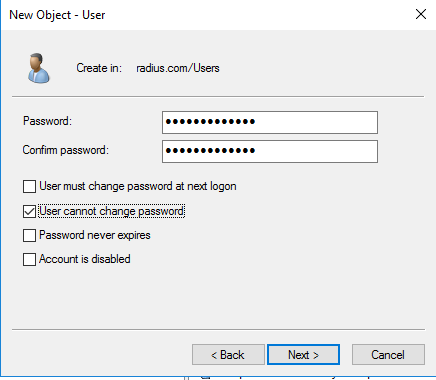


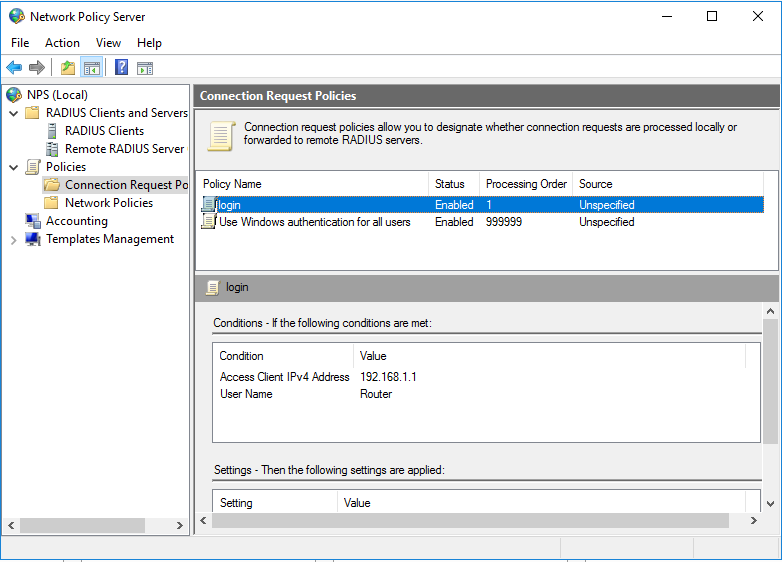


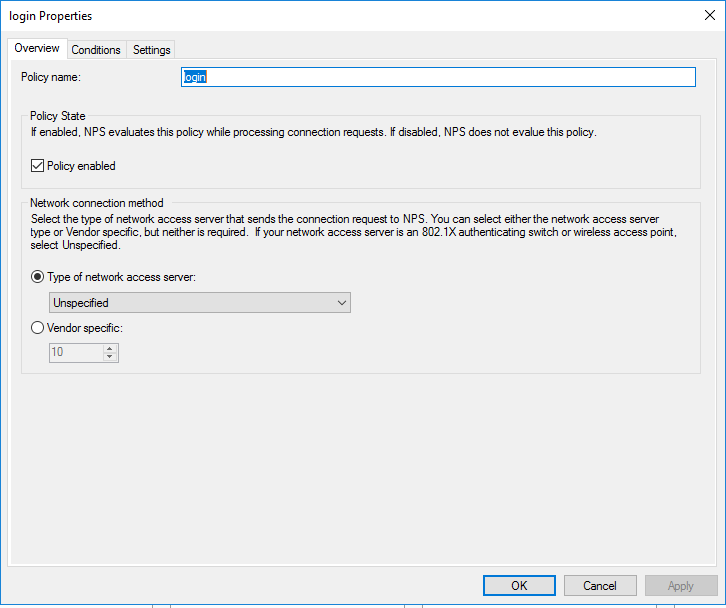


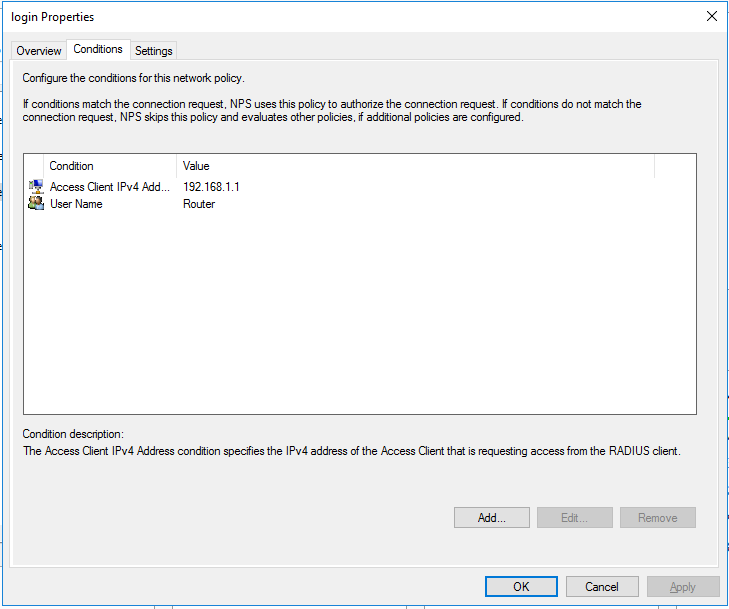


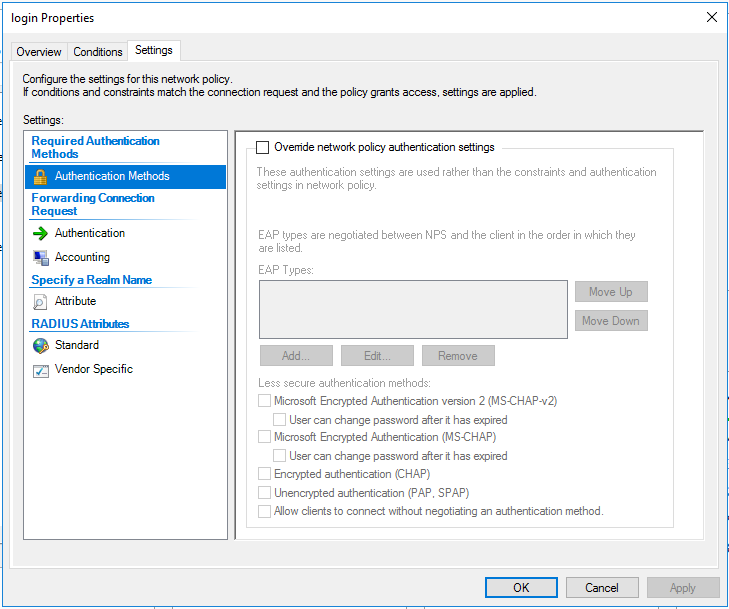


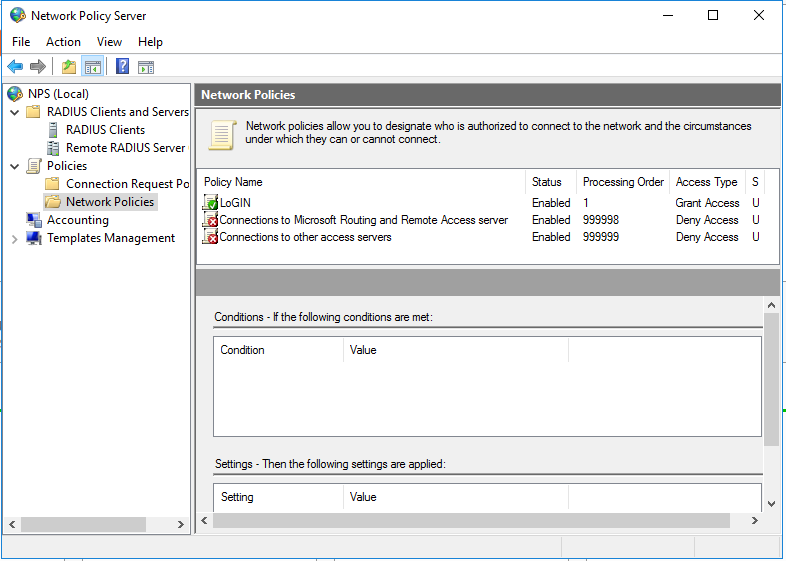


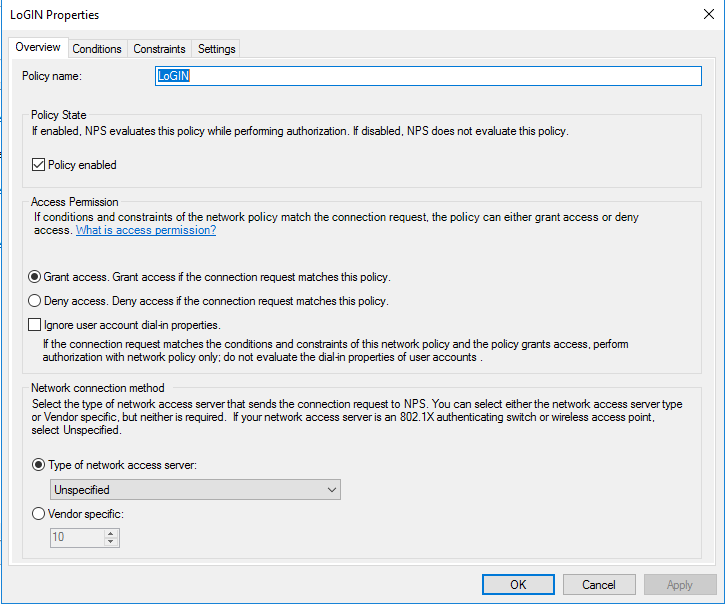


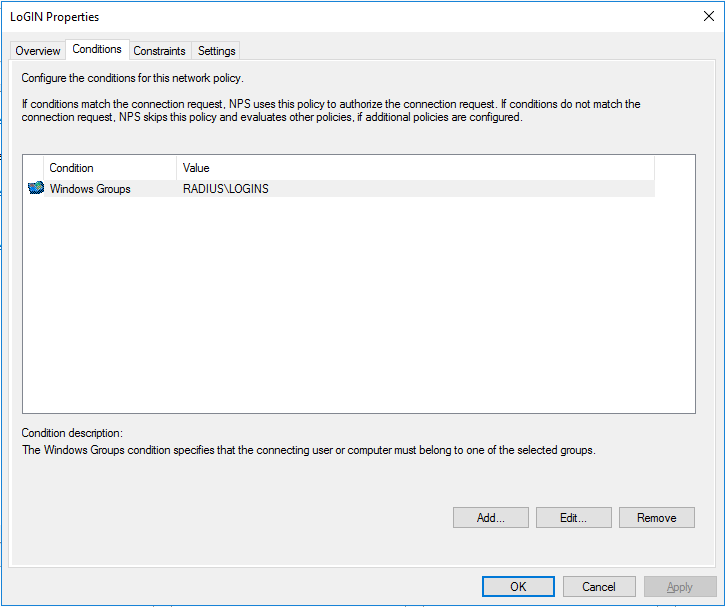


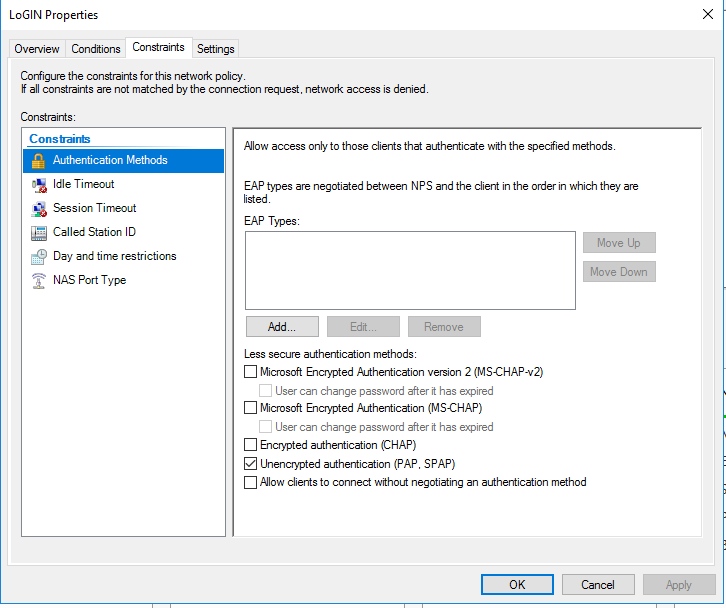


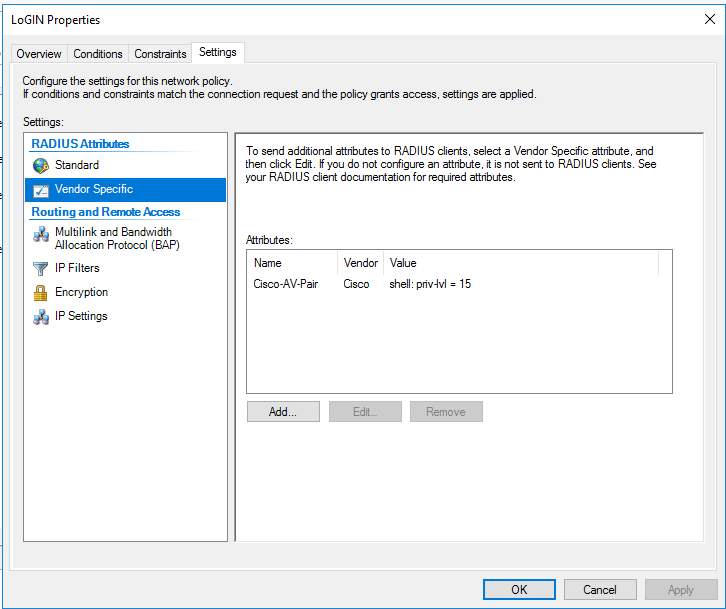
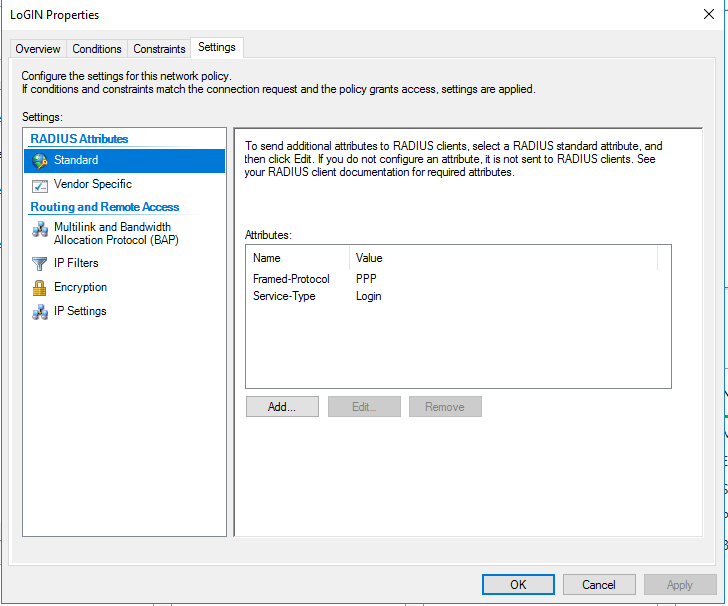


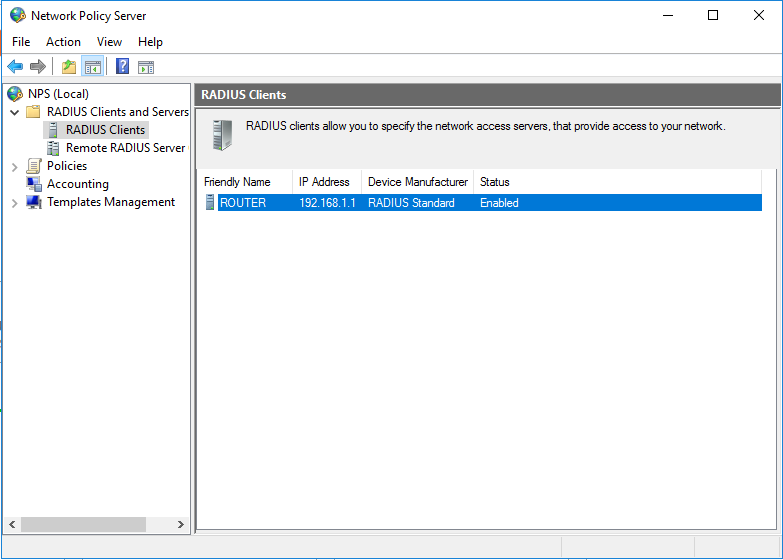


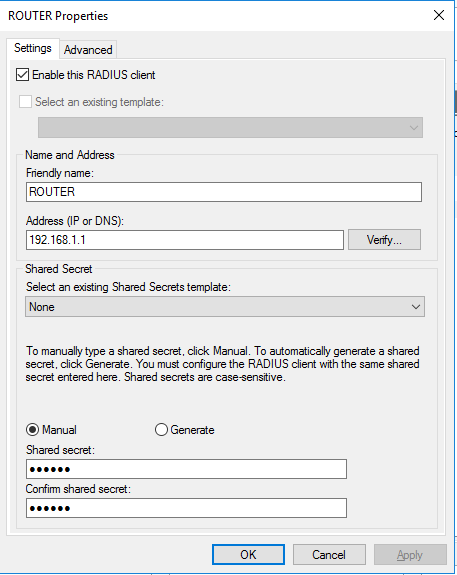












# Problems

Due to our inexperience with setting up servers in virtual machines, my partner and I ran into numerous difficulties in completing the lab. We were completely unfamiliar with setting up Linux and Windows servers, meaning that we essentially had to learn from scratch and even simple errors could take a long time to fix because we lacked the basic skills. For example, we did not realize that the TACACS+ configuration file utilized strict syntax and that a single space could result in a failure, which caused us some problems.

Configuring the RADIUS server was the most difficult and confusing out of the lab. Initially when configuring Active Directory in RADIUS, we had added Active Directory Domain and Certification services as new roles/features, but did not complete the configuration for Domain Services. It turned out that it was necessary to promote the Active Directory towards being a domain controller/promoting it into a forest. We also missed many other key pieces as we were configuring the server initially, such as adding the DNS as a new role, configuring the server through an administrator account, and configuring network and connection request policies

Regarding the routers, one major problem was that certain commands for TACACS+ were deprecated, which caused a lot of confusion regarding which specific commands to use. This was eventually solved by cross-referencing many online guides, though only after we had spent a large amount of time trying to figure out what was wrong.

# Conclusion

The lab overall was a basic task in implementing TACACS+ and RADIUS authentication via servers on Ubuntu and Windows virtual machines. Overall I was able to learn basics of AAA via TACACS+ and RADIUS, and was able to familiarize myself in setting up servers and working with virtual machines.