

Access Control M/618/5210

AC 2.1: Implement authentication to increase effectiveness and usability.

AC 2.2: Define a series of passwords policies and configure password authentication for multiple user IDs

| | | | |
|--------------|-------------------|------------|-------------|
| Learner Name | Oluwaseun Folarin | Tutor Name | Shamim Khan |
|--------------|-------------------|------------|-------------|

Scenario

"Pentest Ground" are a security services company based in New York and have employed you as their Access Control Administrator. They have requested that, as you develop their network, you use different methods of authentication according to security responsibilities and expectations, therefore, they have asked you to configure AAA authentication on their routers on their network.

Your objectives using Pentest Ground's existing network, are:

- Configure a local user account on Server2 and configure authenticate on the console using local AAA
- Verify local AAA authentication from the console and the PC-1 client
- Configure Local AAA Authentication for Console Access on R1

Follow the steps below using Cisco Packet Tracer and the file named "Pentest Ground Existing Network 2.1 and 2.2.pkt" to undertake the objectives, ensuring you capture evidence as you go.

Task

Step 1: Test connectivity

- Ping from PC-1 to PC-2
- Ping from PC-2 to PC-3
- Ping from PC-3 to PC-4

Step 2: Configure a local username on server2

- Configure a username of Admin1 with a secret password of admin1pa55

Step 3: Configure local AAA authentication for console access on server2

- Enable AAA on R1 and configure AAA authentication for the console login to use the local database

Step 4: Verify the AAA authentication method

- Verify the user EXEC login using the local database
- User Access Verification
- Username: Admin1
- Password: admin1pa55 R1>

Step 1: Test connectivity

- Ping from PC-1 to PC-2
- Ping from PC-2 to PC-3
- Ping from PC-3 to PC-4

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.5:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\> ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=7ms TTL=128
Reply from 192.168.1.4: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.1.4:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\> ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Annotation: Ping from PC-1 to PC-2

At first PC-1 did not ping to PC-2 as shown in the screenshot, then I tried pinging to PC-1 from PC-1 to verify if it actually pings and works which it did successfully as shown on the screenshot. After which I went back on the packet tracer, reconfigured PC-2 by updating its IPv4 Address to (192.168.1.5) and Subnet Mask to (255.255.255.0), I then went back to PC-1, open the 'Command Prompt' and pinged to PC-2 again as shown on the third ping in the screenshot, PC-1 successfully pinged to PC-2.

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Annotation: Ping from PC-2 to PC-3

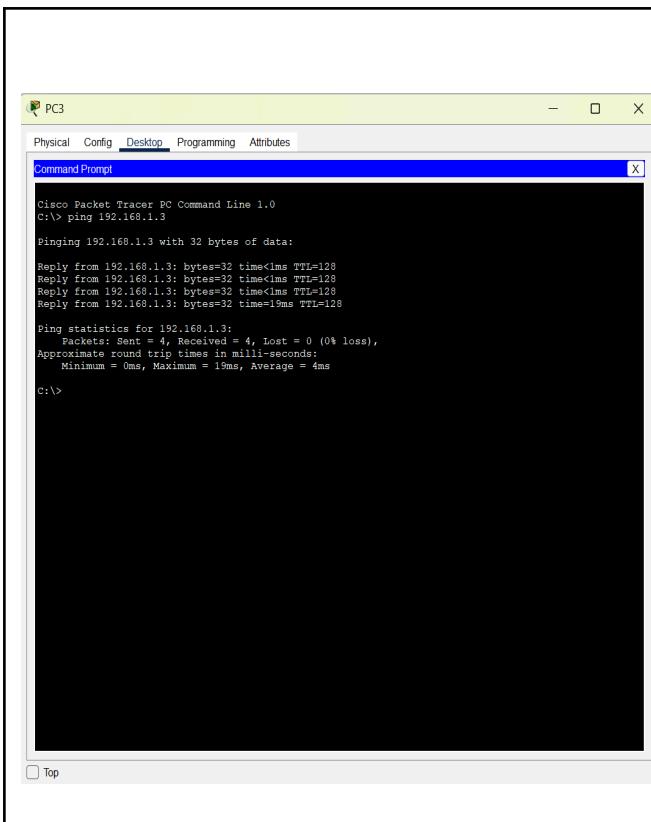
Clicked on PC-2 and PC-3

Checked both IP Configured to ensure the IP address is there and correct.

Went back to PC-2 desktop and Selected 'Command Prompt'

Then I pinged to PC3 from PC-2 as shown in the screenshot

Successfully pinged from PC-2 to PC-3



```

Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=19ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms

C:\>

```

Annotation: Ping from PC-3 to PC-4

Clicked on PC-3 and PC-4

Checked both IP Configured to ensure the IP address is there and correct.

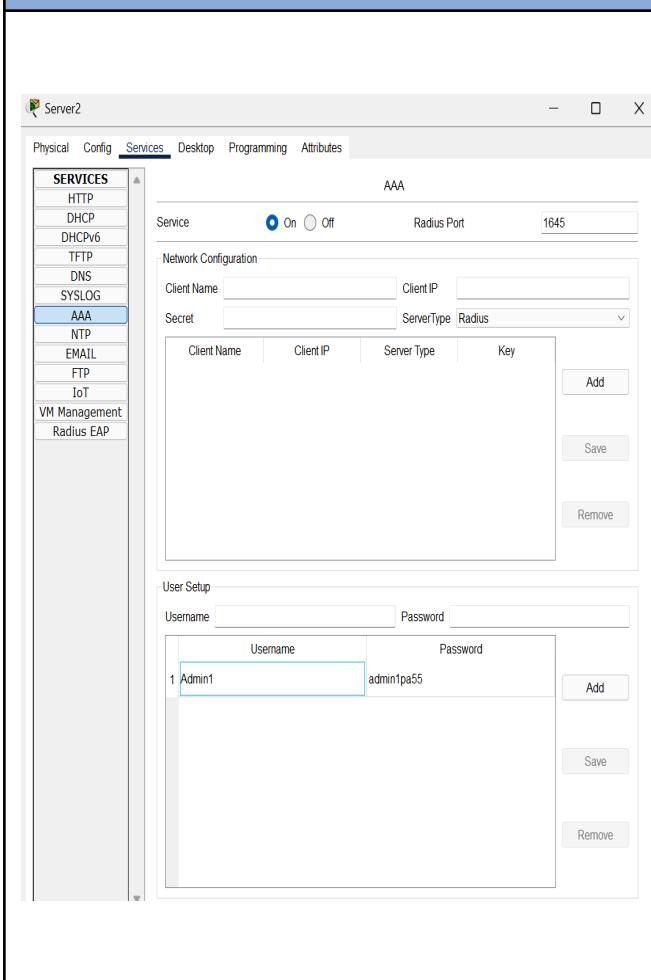
Went back to PC-3 desktop and Selected 'Command Prompt'

Then i pinged to PC-4 from PC-3 as shown in the screenshot

Successfully pinged from PC-2 to PC-3

Step 2: Configure a local username on server2

- Configure a username of Admin1 with a secret password of admin1pa55



| Client Name | Client IP | Server Type | Key |
|-------------|-----------|-------------|-----|
| | | | |

| Username | Password |
|----------|------------|
| 1 Admin1 | admin1pa55 |

Annotation:

Evidence of Username and password configuration for Server2

Clicked on Server2

Selected 'Service'

Under service, selected "AAA"

Switched on "AAA" service

Go down to "User Setup"

Fill in username and password as provided

Clicked "Add" to complete setting up the username and password

Closed the box

Step 3: Configure local AAA authentication for console access on server2

- Enable AAA on R1 and configure AAA authentication for the console login to use the local database

```

IOS Command Line Interface
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

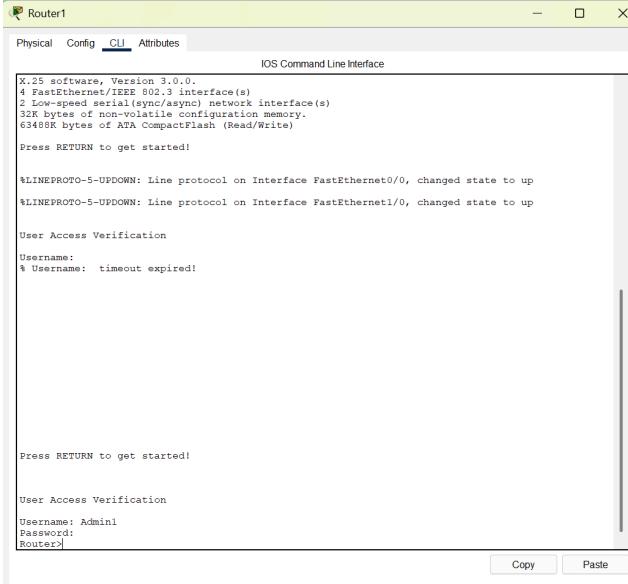
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#username Admin1 secret admin1pa55
Router(config)#aaa new-model
Router(config)#aaa authentication login default local
Router(config)#line console 0
Router(config-line)#login authentication default
Router(config-line)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
configure terminal^Z
Router#
Router#

```

Top



The screenshot shows the Router1 CLI interface. The title bar says "Router1". Below it, there are tabs for "Physical", "Config", and "CLI", with "CLI" being the active tab. The main window displays the following text:

```

IOS Command Line Interface

X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

User Access Verification
Username:
% Username: timeout expired!

Press RETURN to get started!

User Access Verification
Username: Admin1
Password:
Router>

```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons.

Top

Annotation:

Evidence of how I enabled AAA on Router1 and configured AAA authentication for the console login to use the local database.

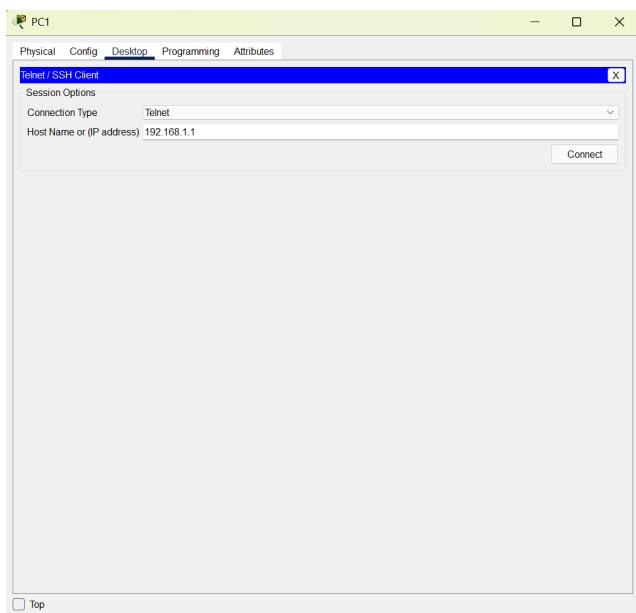
I clicked on Router1, selected CLI (Command Line Interface), at the end of the CLI, I pressed enter which brought up (Router>), I then proceeded to type in enable which opened the configuration terminal. I configured login details making the password (invisible) by adding "secret" before it as shown in the screenshot. I specified that the AAA authentication login was to use the local database and ensured to configure the AAA authentication login as a new model for the console, then end configuration.

In this shot, I tested the AAA authentication I configured in the (Command Line Interface) of the router. The configuration worked out fine. I was presented with a "User Access Verification" as expected. I was timed out at first because I did not provide a username on time.

Input the username and password as requested and as shown in the screenshot, it works fine.

Step 4: Verify the AAA authentication method

- Verify the user EXEC login using the local database
- User Access Verification
- Username: Admin1
- Password: admin1pa55 R1>

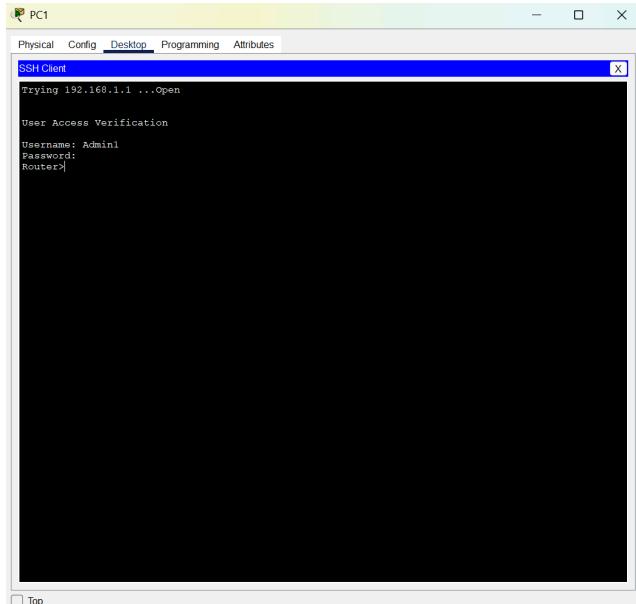


Annotation:

Evidence showing the AAA authentication method is verified.

I went on PC-1, clicked on Desktop then clicked on Telnet/SSH Client.

Under “connection type”, I selected Telnet and filled in the router IP address where it says (Host name), and clicked connect.



After I clicked connect, this SSH Client page came up where I was asked for “User Access Verification”. I filled in the username & password to verify and I can confirm it works as shown in the screen shot.