**Lab 03. Authentication**

**Submission:**

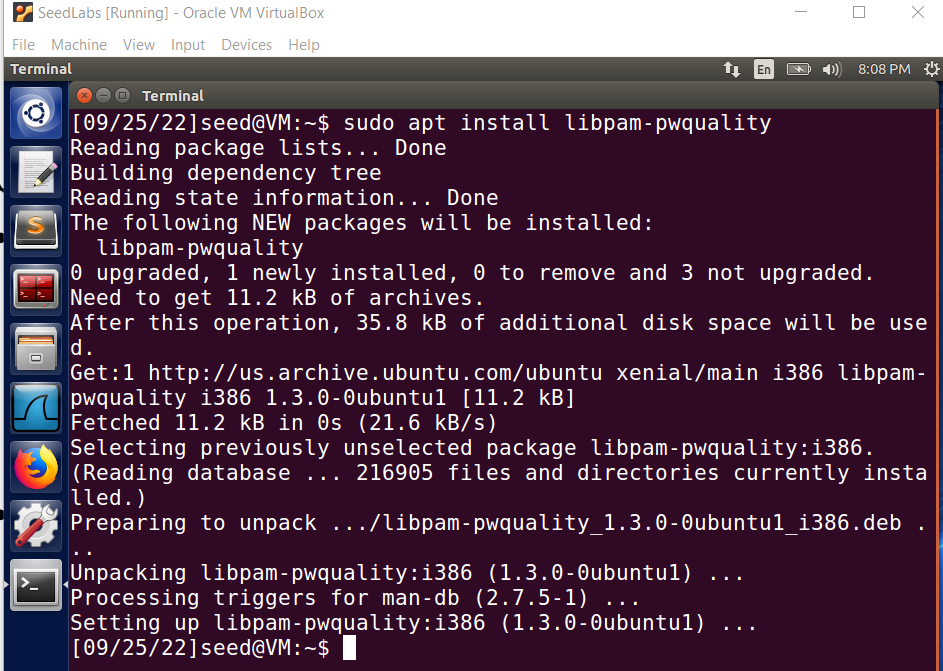
You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

**Time duration:** 1 week

1. **Password policies**
2. **Linux:Ubuntu**

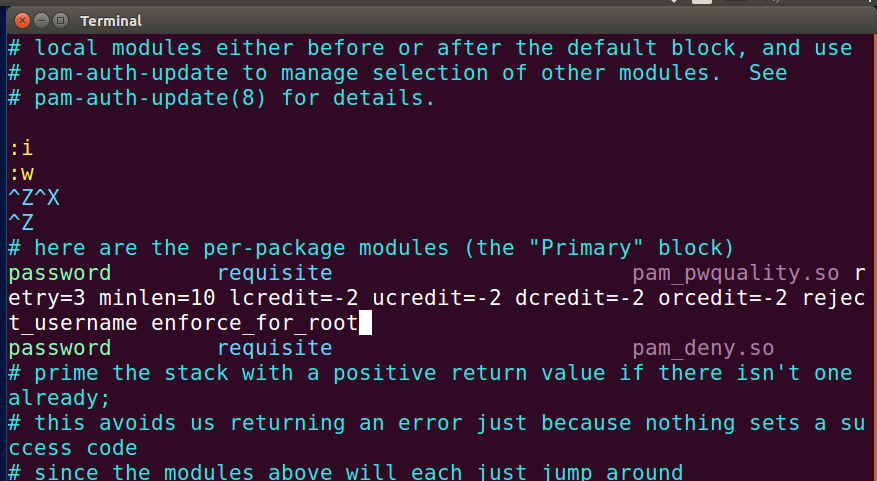
**Step 1. Install package: PAM (lib-pamquality)**

$ sudo apt install libpam-pwquality



**Step 2. Edit the configuration:**

$sudo vi /etc/pam.d/common-password



Options:

**Retry = 3: Cho phép nhập 3 lần**

**Minlen = 10:***độ dài ít nhất 10 ký tự*

**Difok = 0:**

**Lcredit = -2:***có ít nhất 2 chữ thường*

**Ucredit = -2: có ít nhất 2 chữ hoa**

**Dcredit = -2:***có ít nhất 2 số*

**Ocredit = -2:***có ít nhất 2 ký tự*

**reject\_username:***không trùng username*

**enforce\_for\_root:***Also enforce the policy for the root user*

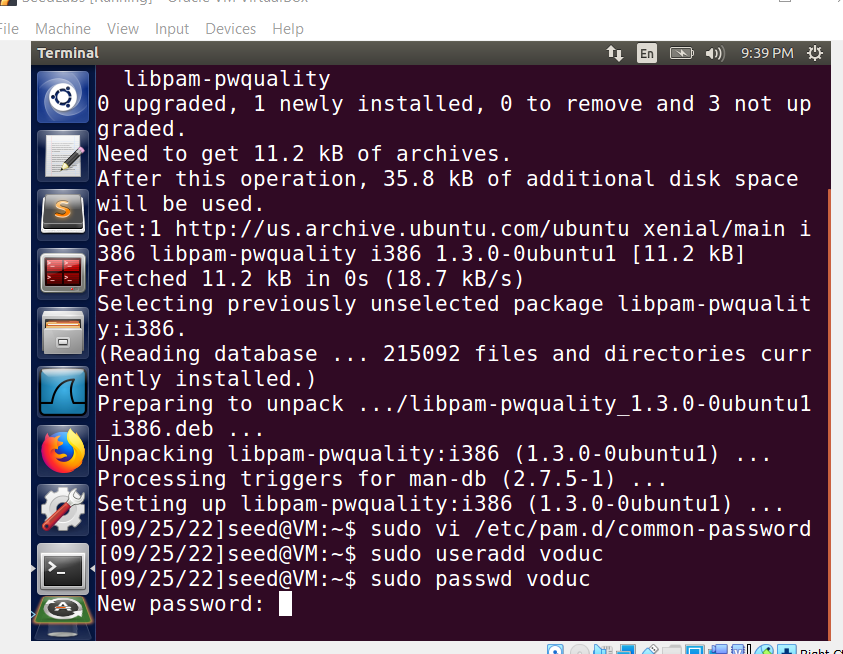
**Example:**

password        requisite pam\_pwquality.so retry=4 minlen=9 difok=4 lcredit=-2 ucredit=-2 dcredit=-1 ocredit=-1 reject\_username enforce\_for\_root

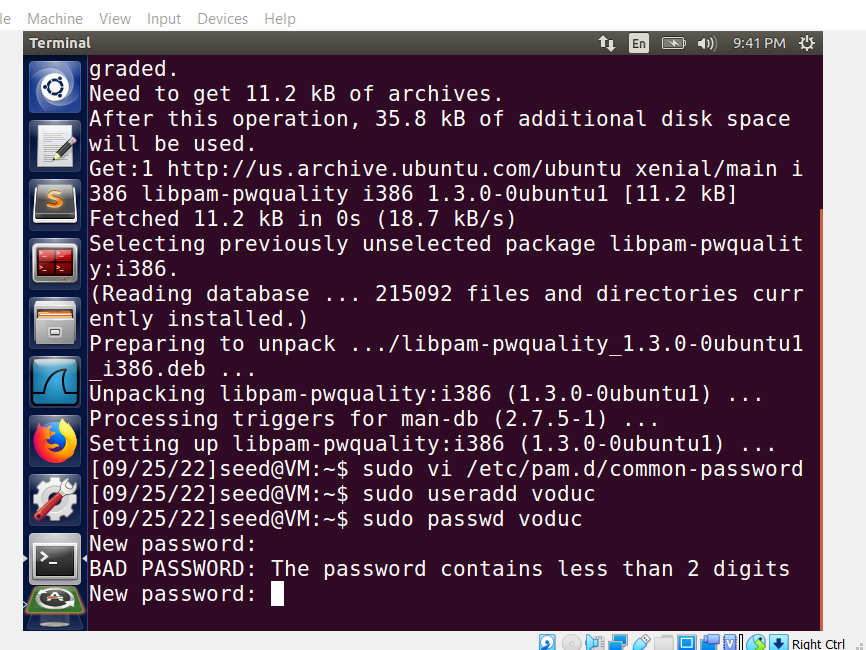
***Verify the configuration:***

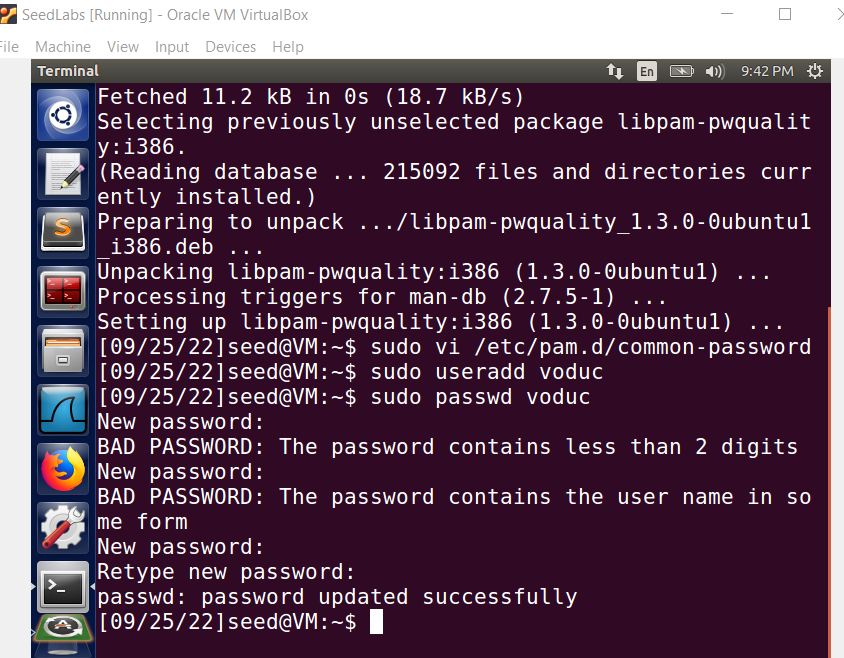
Create an account: $sudo useradd testuser

$sudo passwd testuser



Nếu không thoã được các yêu cầu, mật khẩu sẽ unchange. Ngược lại sẽ được update

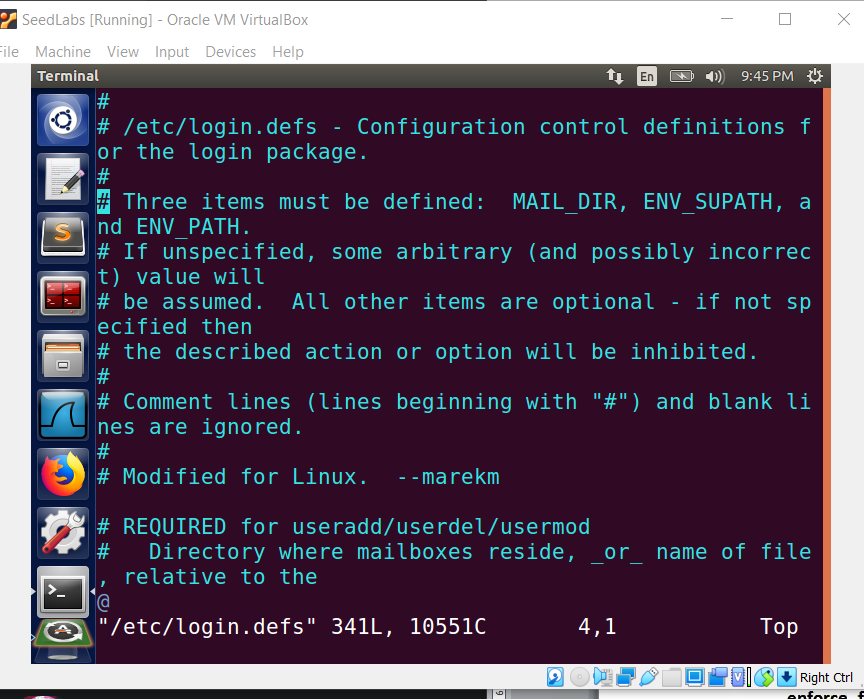




Mật khẩu: VANduc2112002@@

**Step 3. Edit the configuration:**

$sudo vi /etc/login.defs



**Verify the configuration**

1. **MS Windows:**

Create an account and test some functionalities:

* Minimum the password length
* Strong password
* Account lockout threshold



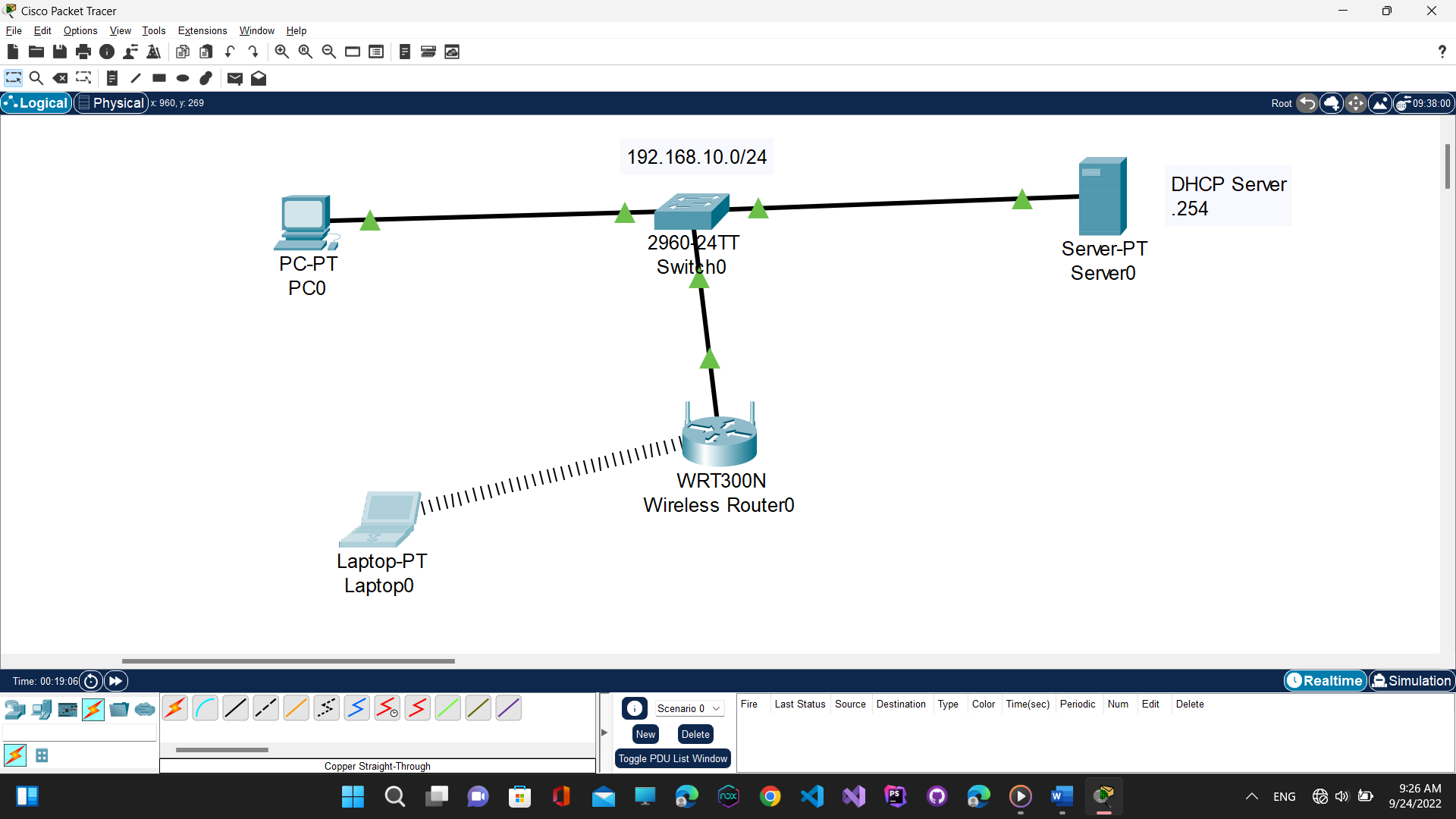
Step 1. Set up the network topology

Step 2. Upgrade Server to domain controller (HCMUTE.VN) & create an account (testuser)

Step 3. Join PC to Domain Controller (account: testuser)

Step 4. Configure the password policy in Domain Controller

Step 5. Verify the configuration on the PC client



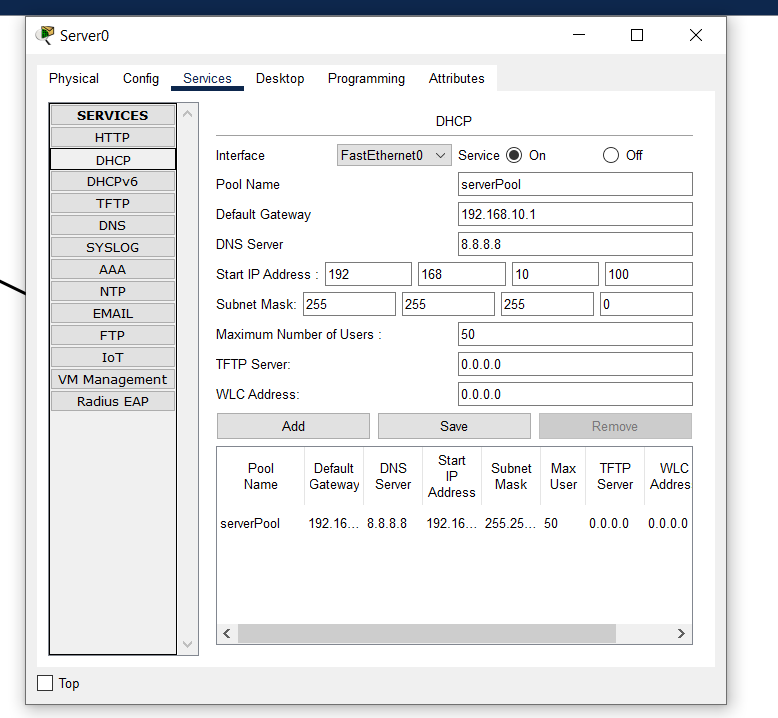
1. **WiFi authentication (WPA2)**

Network topology



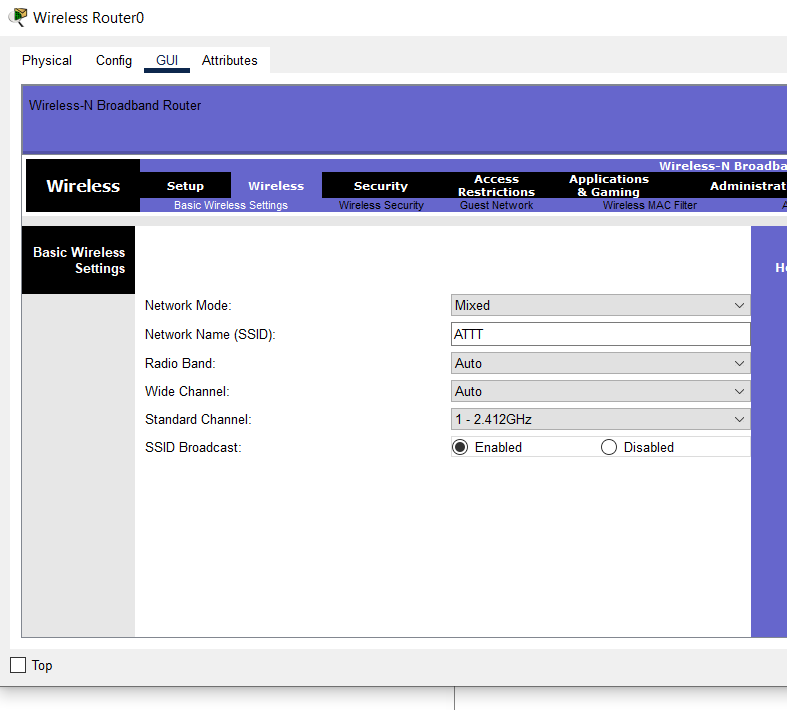
Step 1. Configure DHCP server

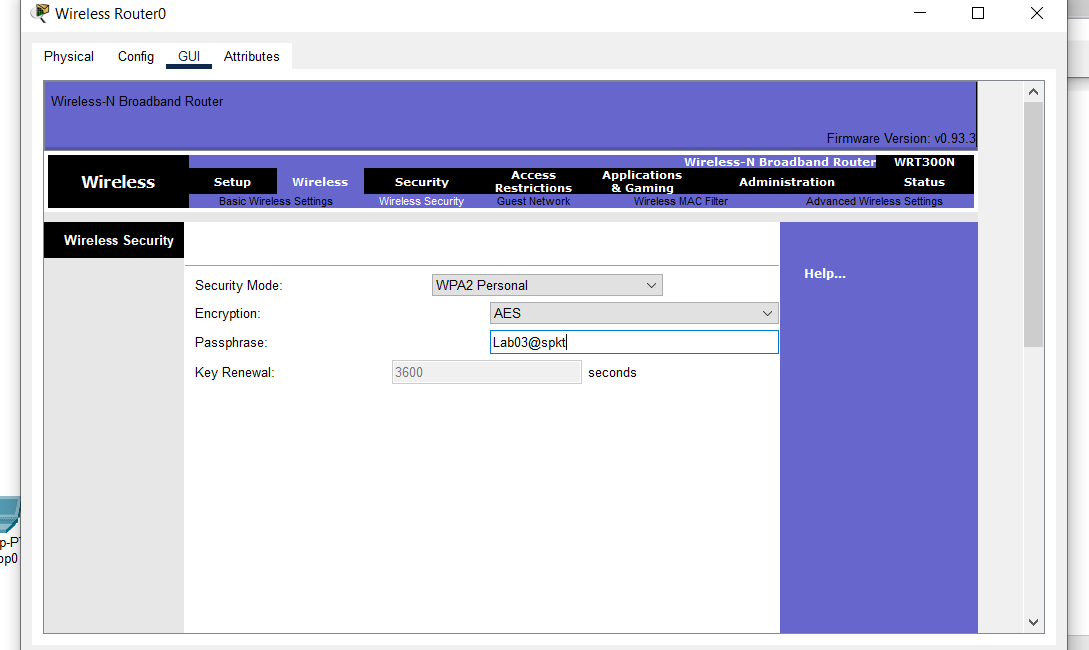
* IP address: 192.168.10.254
* DHCP server:
  + Network: 192.168.10.0/24
  + IP range: 192.168.10.100 – 192.168.10.200
  + Default gateway: 192.168.10.1
  + DNS: 8.8.8.8



Step 2. Configure AP

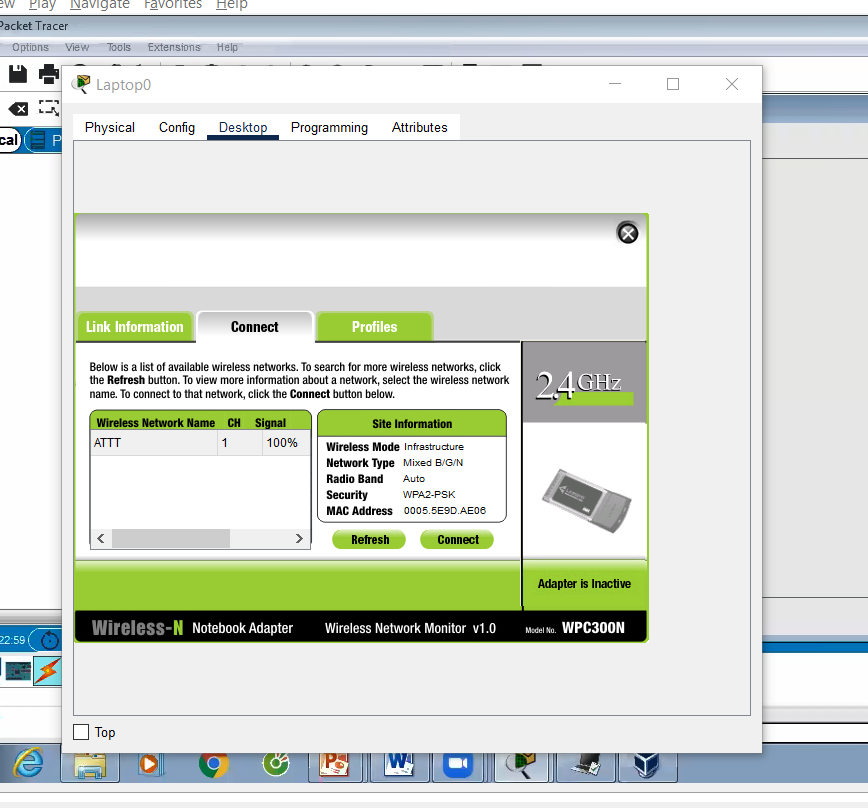
* SSID: ATTT
* Authentication: WPA2 – Personal
* Password: Lab03@spkt

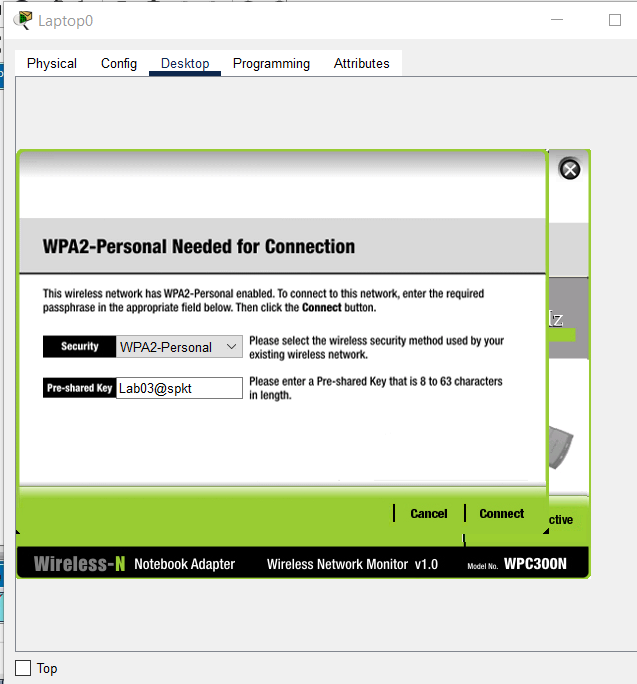




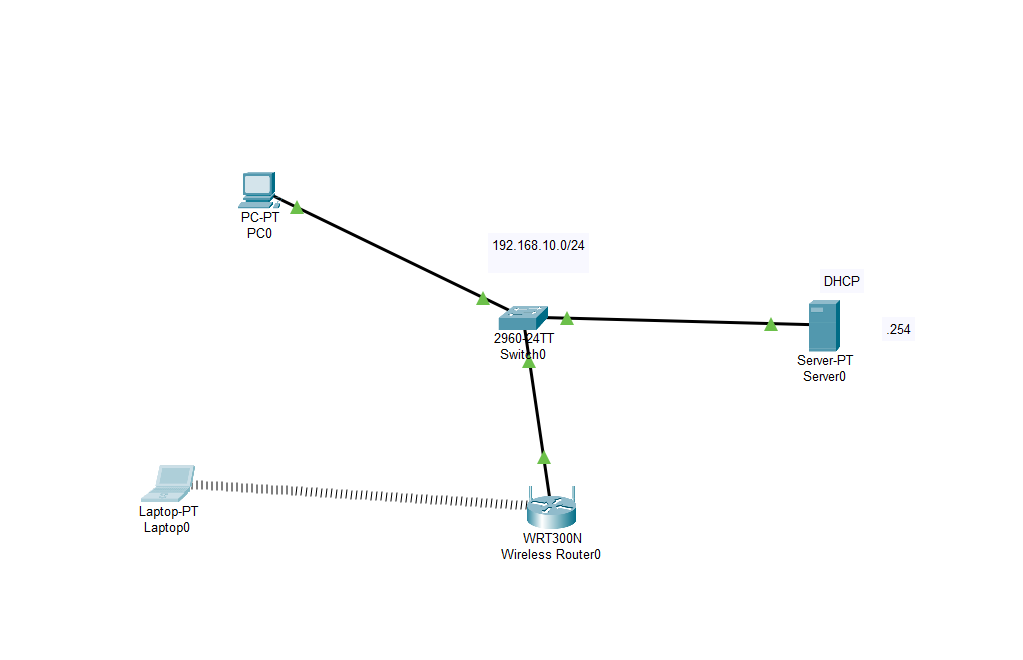
Step 3. Verify the configuration

Test on the Laptop: IP address, ping to other PCs.

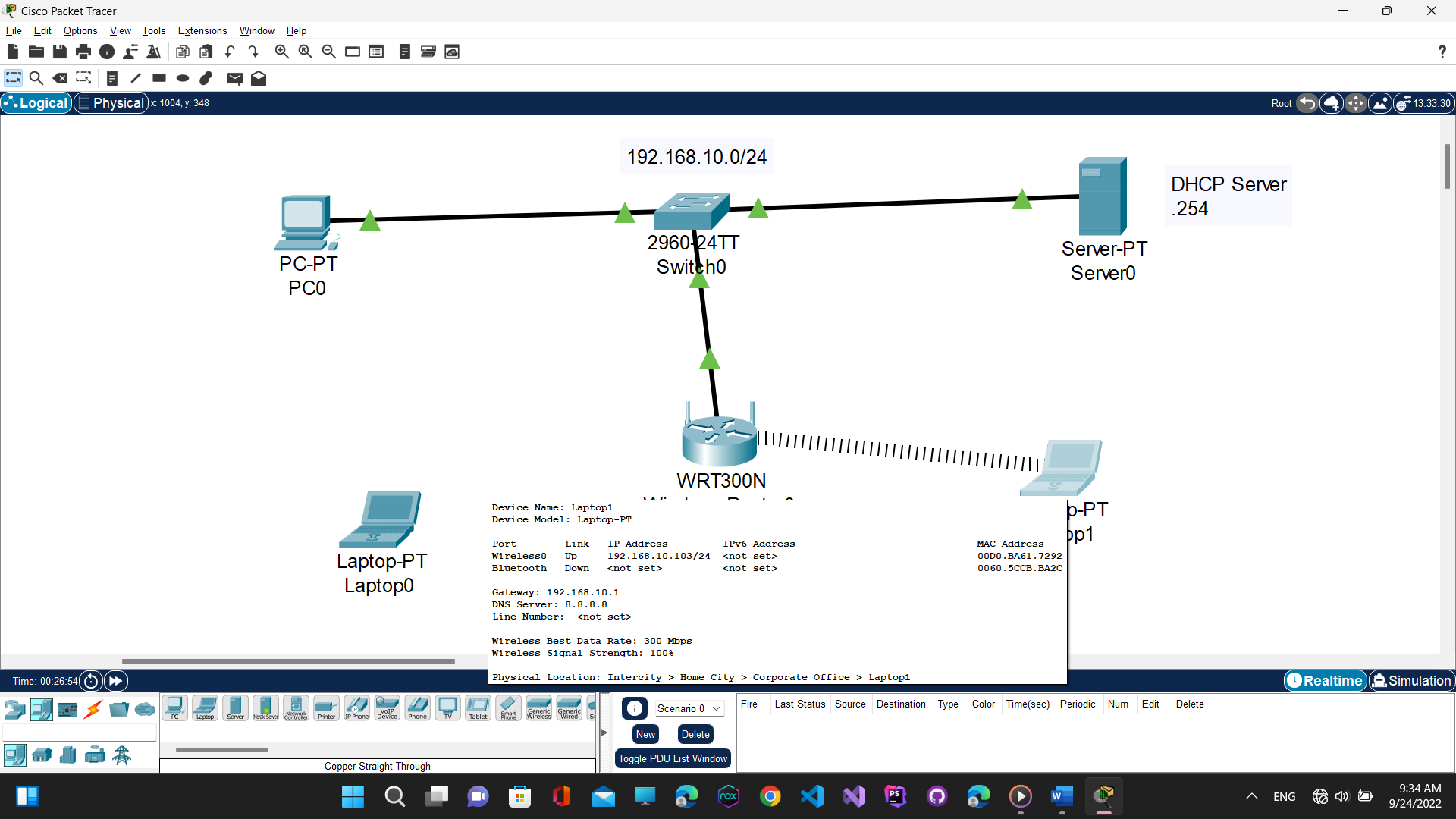








Chứng thực theo MAC Address, Laptop 1 có MAC Address thuộc danh sách nên được connect, còn Laptop 0 không connect được mặc dù biết password



1. **Authentication with Radius server (802.1X)**

Network topology:



Lab environment: **Cisco Packet Tracer**

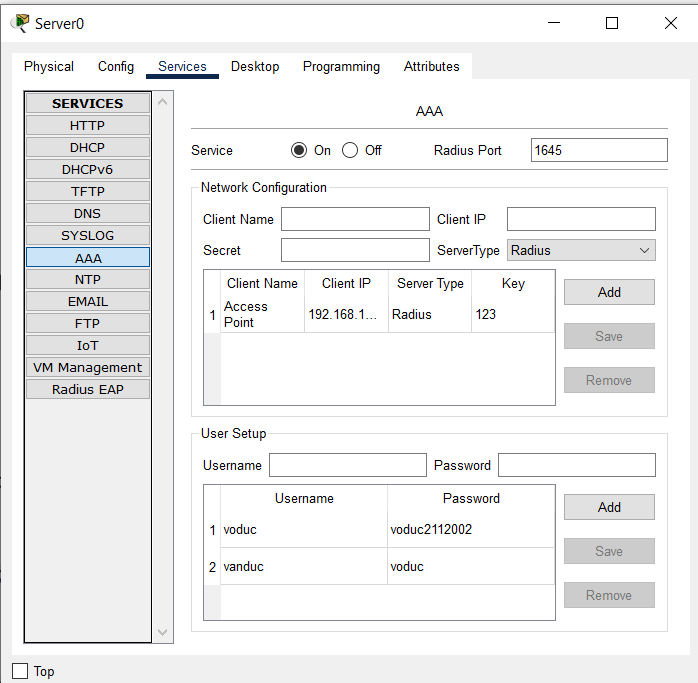
Step 1. Configure IP address & DHCP server

* DHCP server: 192.168.10.254/24
* Configure DHCP server
  + Network: 192.168.10.0/24
  + IP range: 192.168.10.100 – 192.168.10.200
  + Default gateway: 192.168.10.1
  + DNS: 8.8.8.8

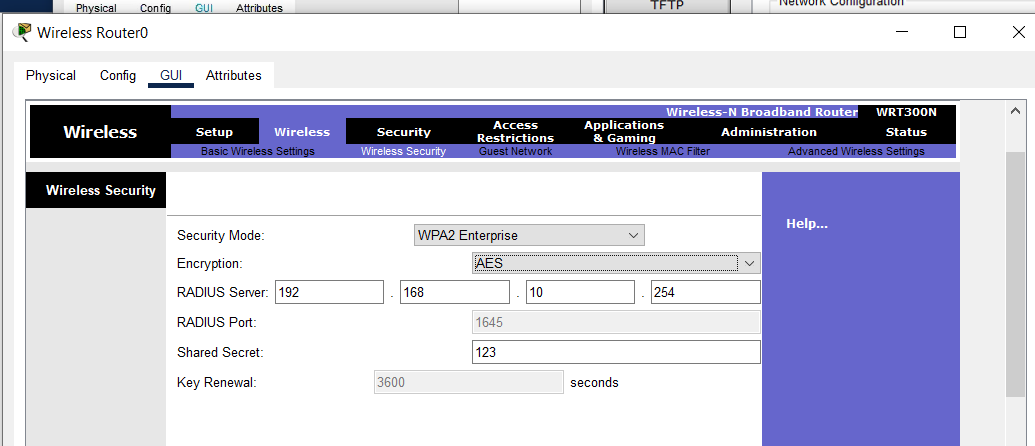
Step 2. Configure AP’s IP address

* AP’s IP address: 192.168.10.250/24
* SSID: ATTT
* Authentication (radius server): WPA2 - Enterprise

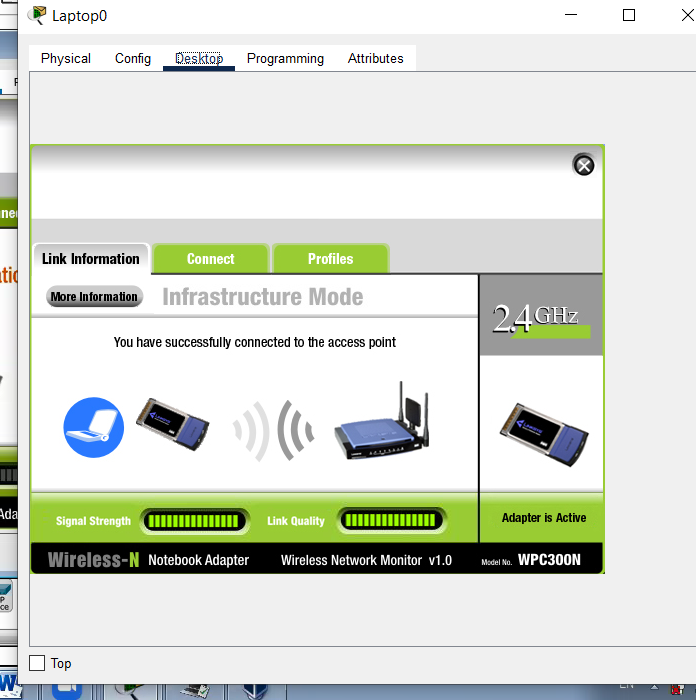
Step 3. Configure RADIUS server

* Set the IP address of the Radius client (the authenticator – AP’s IP address)
* Set the key-ID
* Create accounts
* 

Step 4. Configure RADIUS client ( authenticator) on the AP

* Set the IP address of the Radius server
* Set the key-ID (the same as Key-ID on the Radius server)
* 

Step 5. Verify the configuration - test on the supplicant

* Check IP address information and ping to other PCs
* 
* 