



21110432 Nguyen Le Gia Han lab3

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)



Scan to open on Studocu

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT TP.HCM
KHOA: CÔNG NGHỆ THÔNG TIN

-----□□□□-----



HCMUTE

BÁO CÁO
MÔN HỌC: AN TÒAN THÔNG TIN
LAB 3
AUTHENTICATION

GVHD: TS.Huỳnh Nguyên Chính

Sinh viên thực hiện: Nguyễn Lê Gia Hân

MSSV: 21110432

Mã LHP: INSE330380_23_1_09

TP.Hồ Chí Minh, tháng 09 năm 2023

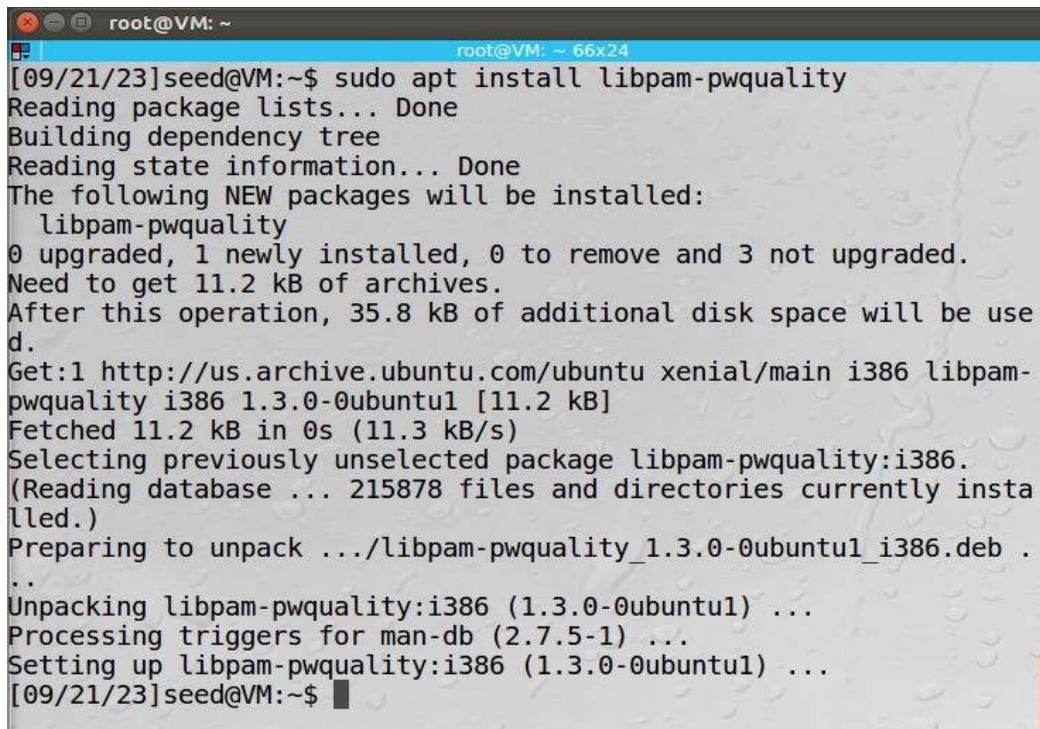
Lab 03. Authentication

I. Password policies

A, Linux:Ubuntu

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

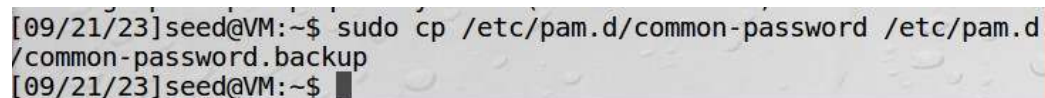
\$ sudo apt install libpam-pwquality

A terminal window titled 'root@VM: ~' showing the command 'sudo apt install libpam-pwquality' being executed. The output shows the package being installed successfully, including details about disk space and file downloads.

```
root@VM: ~  
[09/21/23]seed@VM:~$ sudo apt install libpam-pwquality  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following NEW packages will be installed:  
  libpam-pwquality  
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.  
Need to get 11.2 kB of archives.  
After this operation, 35.8 kB of additional disk space will be used.  
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main i386 libpam-pwquality i386 1.3.0-0ubuntu1 [11.2 kB]  
Fetched 11.2 kB in 0s (11.3 kB/s)  
Selecting previously unselected package libpam-pwquality:i386.  
(Reading database ... 215878 files and directories currently installed.)  
Preparing to unpack .../libpam-pwquality_1.3.0-0ubuntu1_i386.deb ...  
Unpacking libpam-pwquality:i386 (1.3.0-0ubuntu1) ...  
Processing triggers for man-db (2.7.5-1) ...  
Setting up libpam-pwquality:i386 (1.3.0-0ubuntu1) ...  
[09/21/23]seed@VM:~$
```

Backup lại mật khẩu:

- Mục đích phòng ngừa trường hợp cấu hình sai

A terminal window showing the command 'sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.backup' being executed to create a backup of the password configuration file.

```
[09/21/23]seed@VM:~$ sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.backup  
[09/21/23]seed@VM:~$
```

Step 2: Edit the configuration:

\$sudo vi /etc/pam.d/common-password

```

# To take advantage of this, it is recommended that you configure
any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      requisite      pam_pwquality.so r
etry=4 minlen=9 difok=4 lcredit=-2 dcredit=-1 ocredit=-1 reject_u
ername enforce_for_root
password      [success=1 default=ignore]      pam_unix.so obscur
e use authtok try_first_pass sha512
# here's the fallback if no module succeeds
password      requisite      pam_deny.so
# prime the stack with a positive return value if there isn't one
already;
# this avoids us returning an error just because nothing sets a su
ccess code
# since the modules above will each just jump around
password      required      pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional      pam_gnome_keyring.so
■ end of pam-auth-update config
35,1 Bot

```

Retry = 4 Số lần liên tiếp người dùng có thể nhập sai mật khẩu.

Minlen= 9 độ dài ngắn nhất của mật khẩu

Difok = 4 Số ký tự có thể giống với mật khẩu cũ

lcredit: = -2 Số chữ thường tối thiểu là 2

ucredit: Số chữ hoa tối thiểu là 2

dcredit: Số chữ số tối thiểu là 1

ocredit: Ký hiệu đặc biệt tối thiểu là 1

reject_username: Từ chối mật khẩu chứa tên người dùng

enforce_for_root: Cũng thực thi chính sách cho người dùng root

Verify the configuration:

Create an account: \$sudo useradd testuser

\$sudo passwd testuser

```
[09/21/23]seed@VM:~$ sudo useradd testuser
[09/21/23]seed@VM:~$ sudo passwd testuser
New password:
BAD PASSWORD: The password contains less than 2 lowercase letters
New password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
New password:
Retype new password:
passwd: password updated successfully
[09/21/23]seed@VM:~$ █
```

Đăng nhập vào user: testuser (Chuyển màn hình: ctrl+Alt+F1, quay về: ctrl+Alt+F7)

```
/dev/sda1: Clearing orphaned inode 678683 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: Clearing orphaned inode 678682 (uid=125, gid=132, mode=0100600, size=0)
/dev/sda1: clean, 302547/1245184 files, 1873803/4980480 blocks
[ 11.262677] piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!

Ubuntu 16.04.2 LTS VM tty1

VM login: testuser
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reboot[:59: integer expression expected:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

No directory, logging in with HOME=/
$ _
```



```
#
# Password aging controls:
#
#     PASS_MAX_DAYS    Maximum number of days a password may be u
sed.
#     PASS_MIN_DAYS    Minimum number of days allowed between pas
sword changes.
#     PASS_WARN_AGE    Number of days warning given before a pass
word expires.
#
PASS_MAX_DAYS    99999
PASS_MIN_DAYS    0
PASS_WARN_AGE    7
#
# Min/max values for automatic uid selection in useradd
#
UID_MIN          1000
UID_MAX          60000
# System accounts
#SYS_UID_MIN     100
#SYS_UID_MAX     999
```

Trích đoạn trong file cấu hình /etc/login.defs là để điều chỉnh các quy tắc liên quan đến tuổi thọ mật khẩu (password aging controls) và cấu hình các giới hạn cho việc tự động chọn UID (User ID) khi tạo mới tài khoản bằng lệnh useradd. Dưới đây là giải thích cho từng phần:

1. Password Aging Controls:

- **PASS_MAX_DAYS:** Đây là số ngày tối đa một mật khẩu có thể được sử dụng trước khi phải thay đổi. Giá trị 99999 trong trường này thường được sử dụng để cho phép mật khẩu không bao giờ hết hạn và không cần phải thay đổi.
- **PASS_MIN_DAYS:** Đây là số ngày tối thiểu phải trôi qua giữa hai lần thay đổi mật khẩu. Giá trị 0 cho phép bạn thay đổi mật khẩu bất cứ khi nào bạn muốn.
- **PASS_WARN_AGE:** Đây là số ngày trước khi mật khẩu hết hạn mà hệ thống sẽ cảnh báo cho người dùng. Trong trường hợp này, cảnh báo sẽ được hiển thị 7 ngày trước khi mật khẩu hết hạn.

2. Min/Max Values for Automatic UID Selection:

- **UID_MIN** và **UID_MAX** là giới hạn tối thiểu và tối đa cho việc tự động chọn User ID (UID) khi bạn tạo một tài khoản mới bằng lệnh useradd.
- Trong trường hợp này, tài khoản mới sẽ được gán một UID trong khoảng từ 1000 đến 60000. Điều này có nghĩa là nếu bạn tạo một tài khoản mới mà

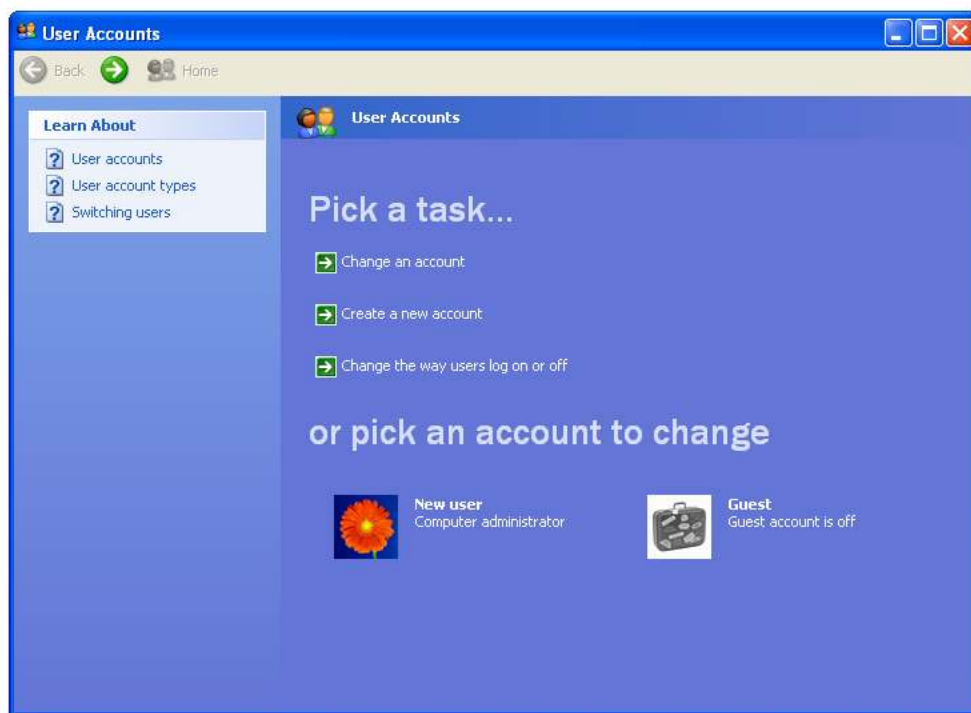
không cung cấp UID cụ thể, hệ thống sẽ tự động chọn một UID trong khoảng này để gán cho tài khoản.

- Việc giới hạn giữa UID_MIN và UID_MAX giúp quản lý UID tránh xung đột và hỗ trợ quản lý tài khoản người dùng trên hệ thống.

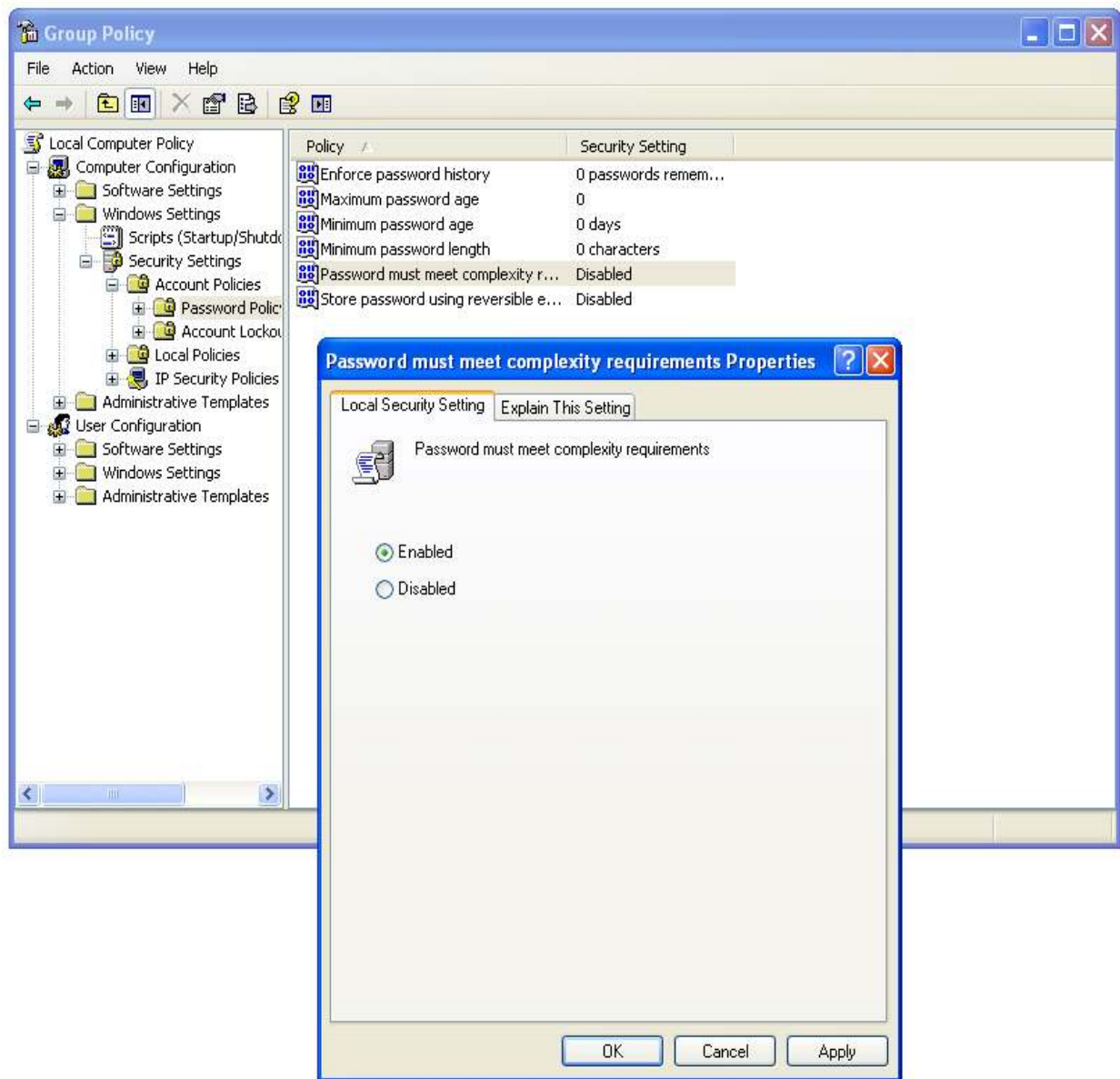
a) MS Windows:

Create an account and test some functionalities:

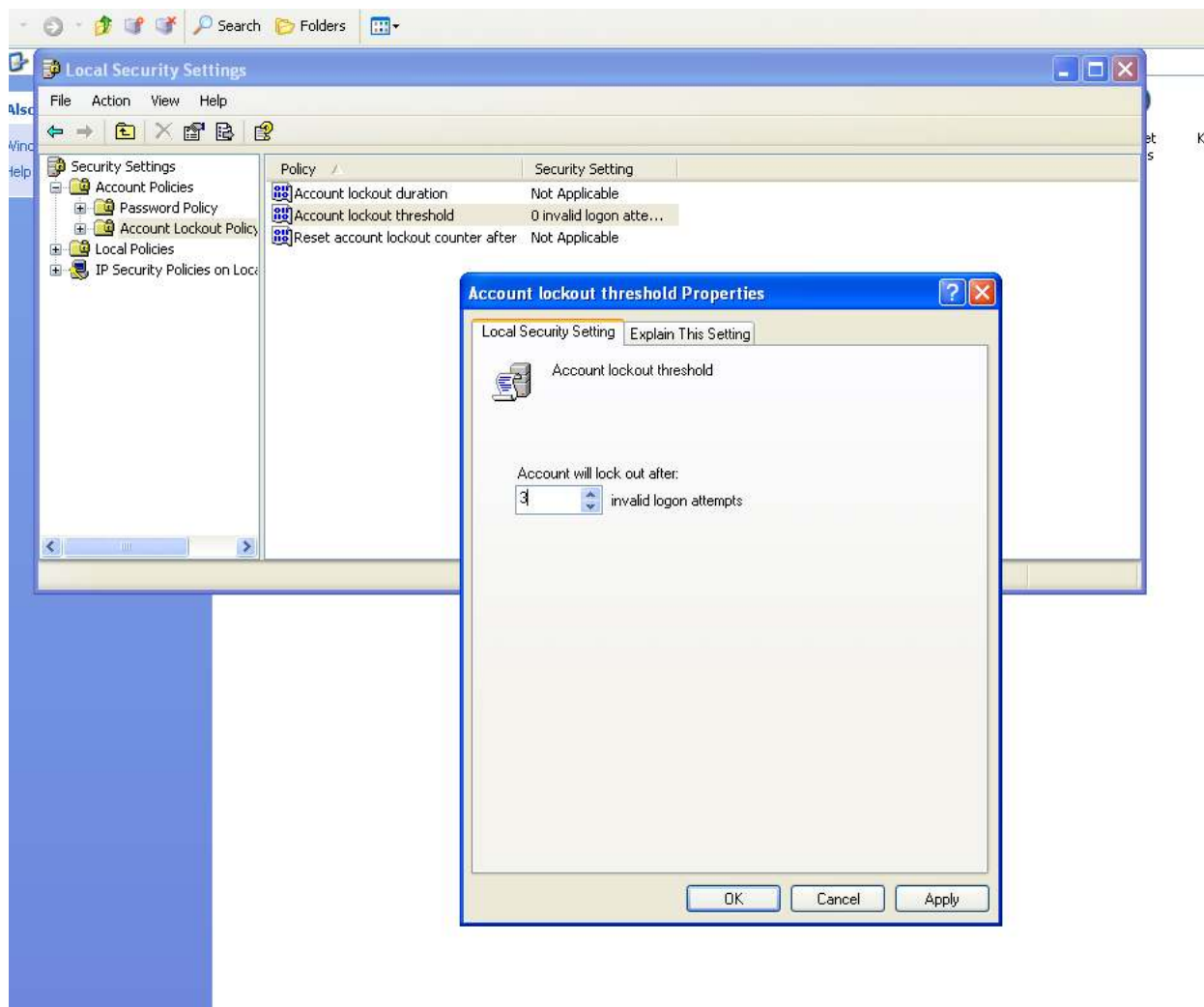
- Minimum the password length
- Strong password
- Account lockout threshold



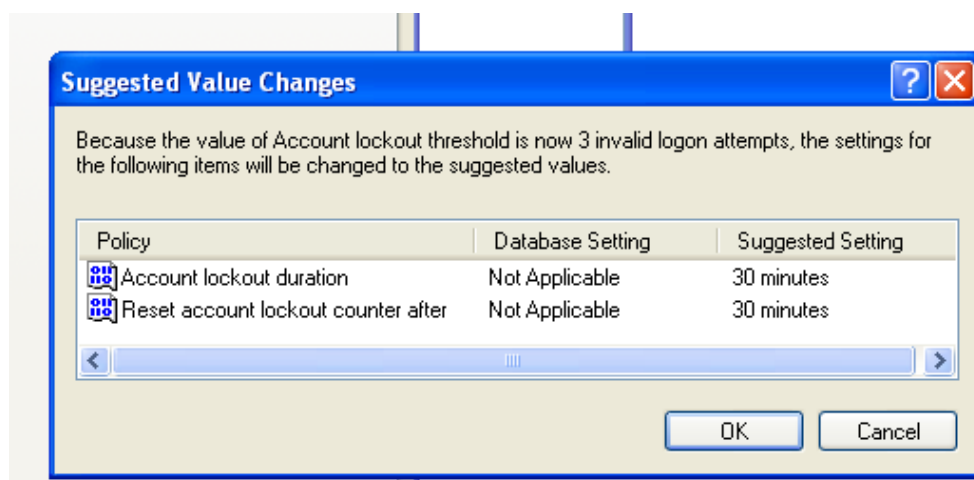
Thay đổi cấu hình yêu cầu mật khẩu mạnh



- Ngưỡng khóa tài khoản: Tài khoản sẽ bị tạm khóa khi nhập sai 3 lần



Tài khoản sẽ được khởi tạo lại sau 30 phút

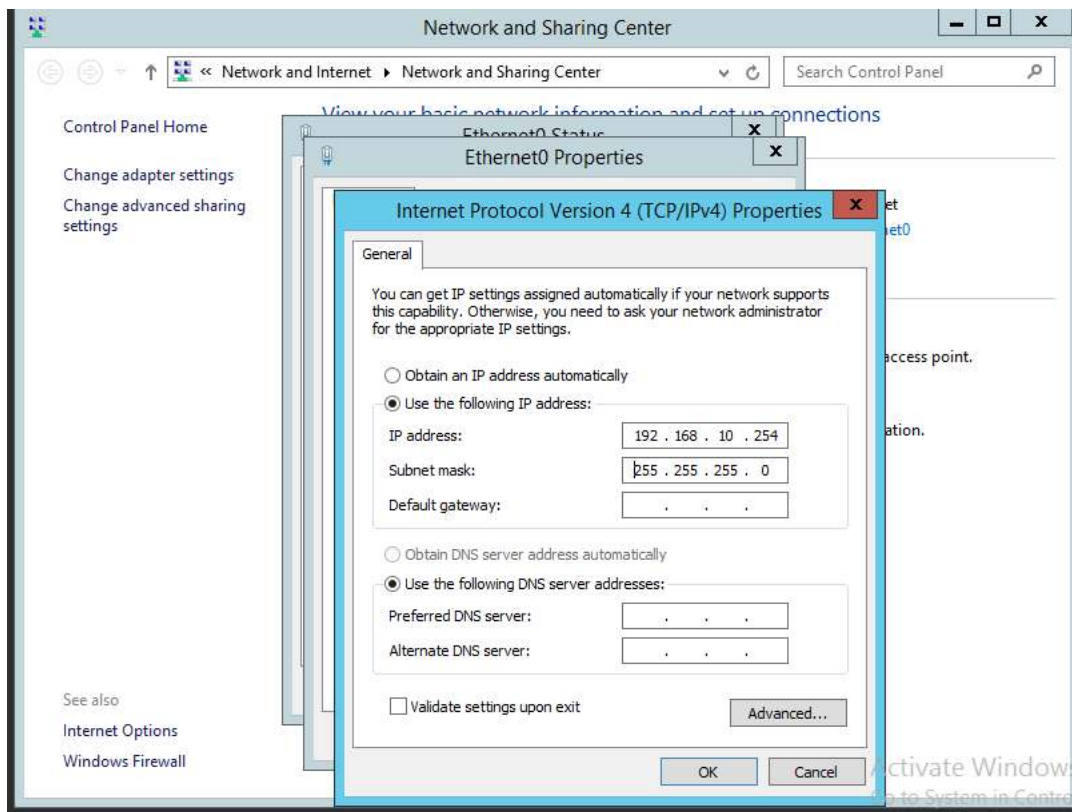


Thử khởi tạo một mật khẩu yếu chỉ toàn số và đây là cảnh báo của hệ thống

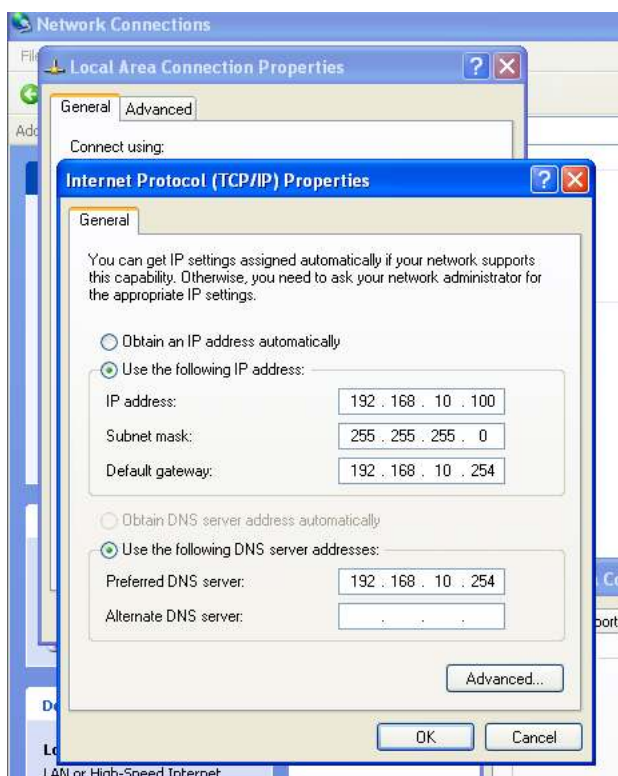


b. MS Window

Step 1: Set up the network topology



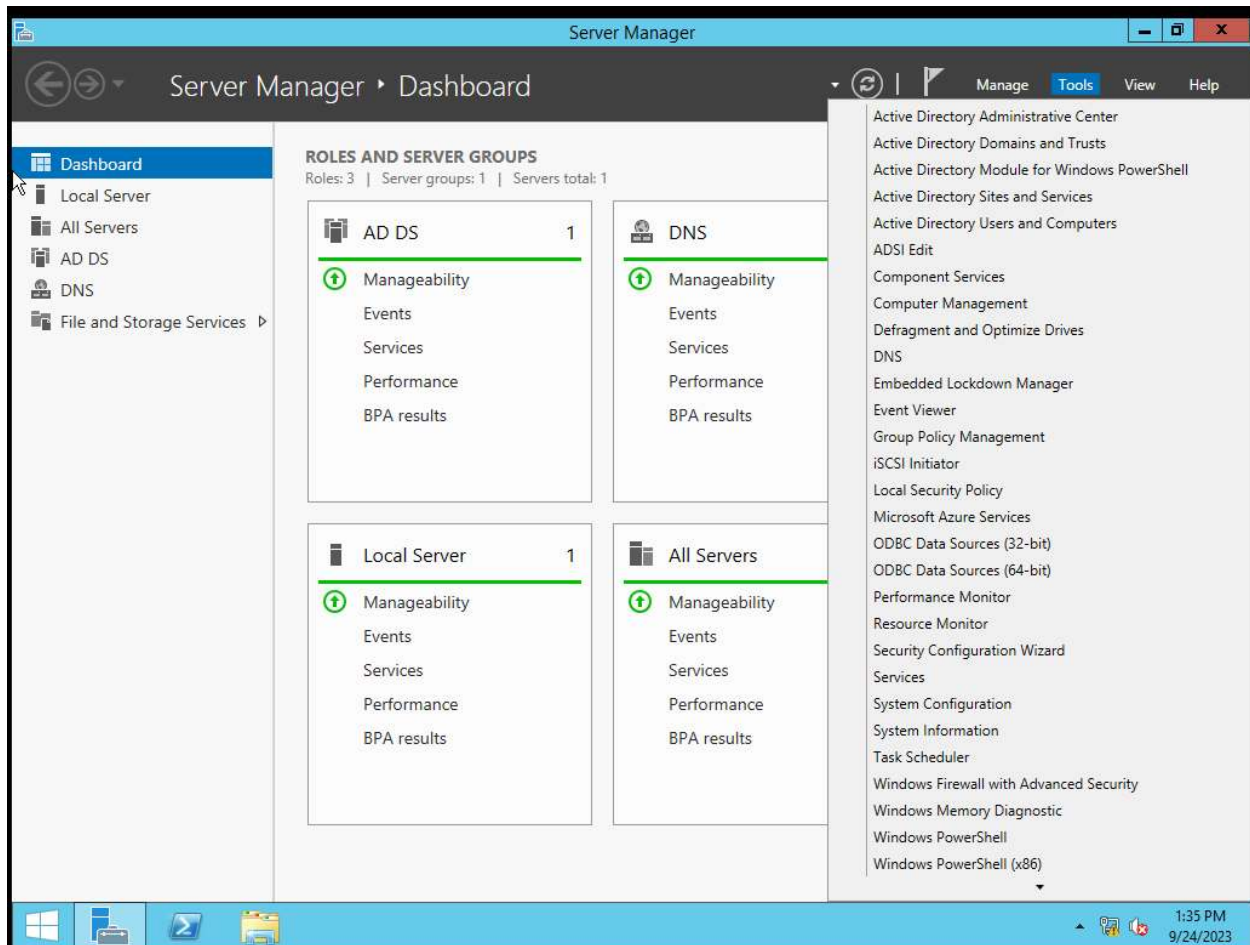
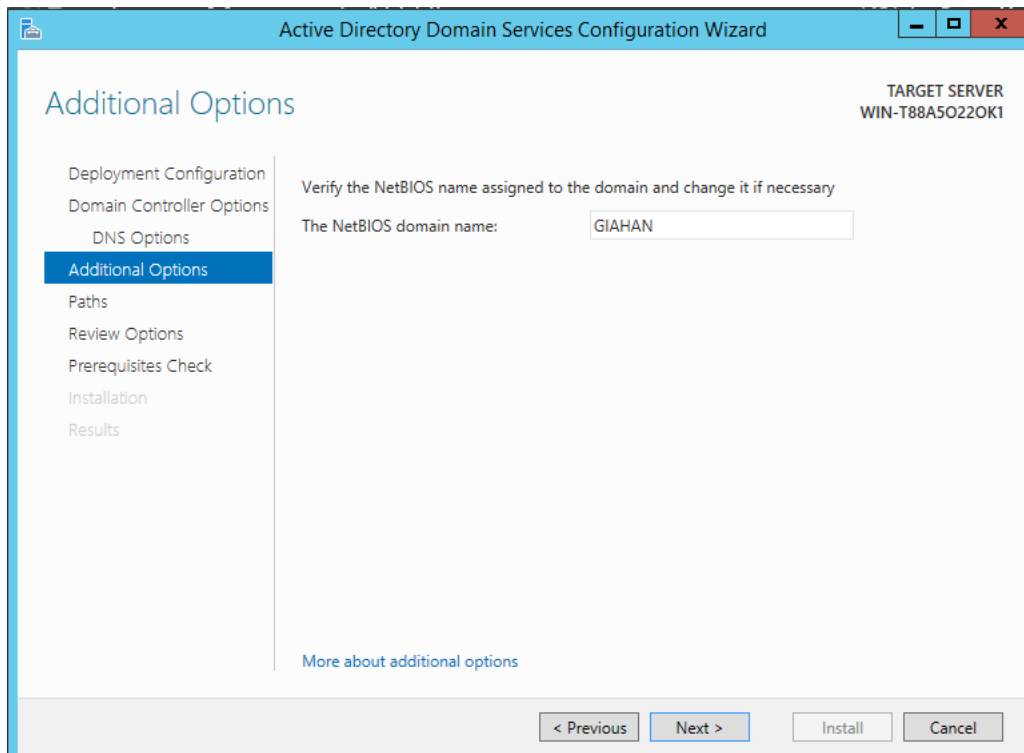
- Cấu hình cho máy server:
 - Địa chỉ ipv4: 192.168.10.254

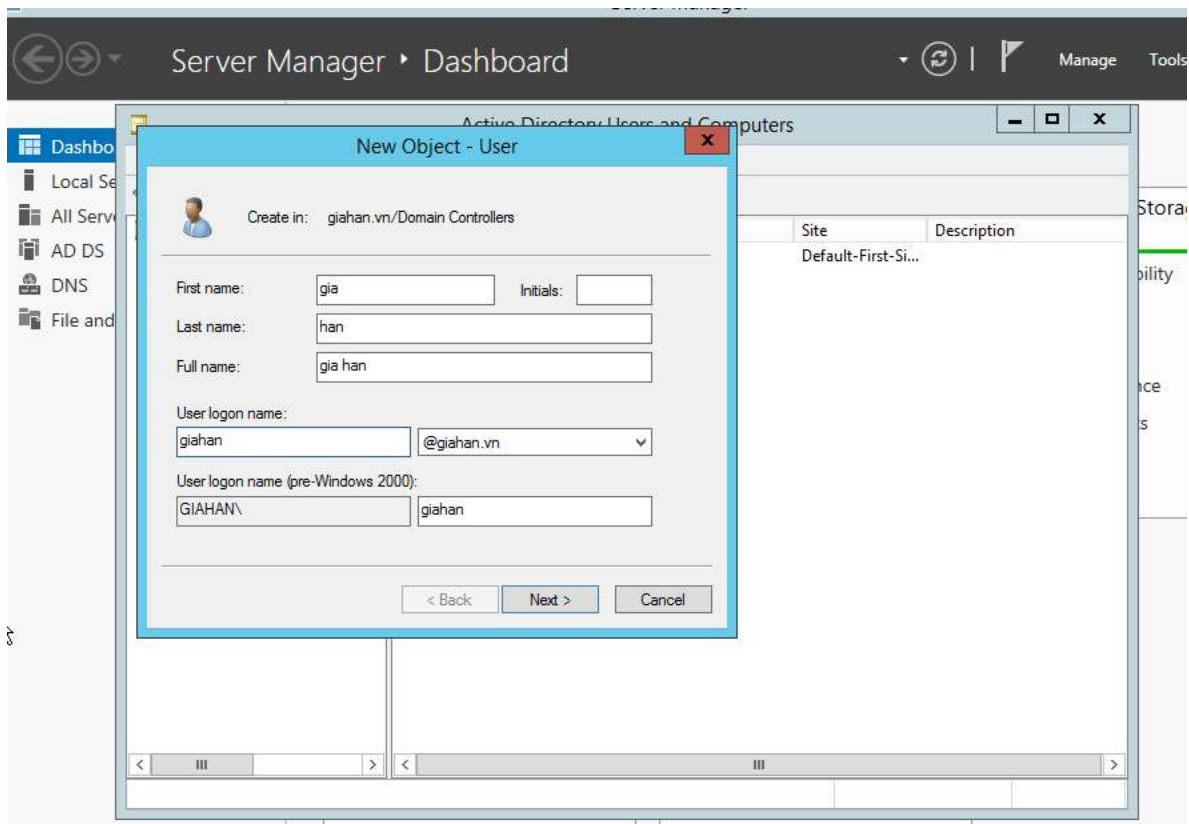
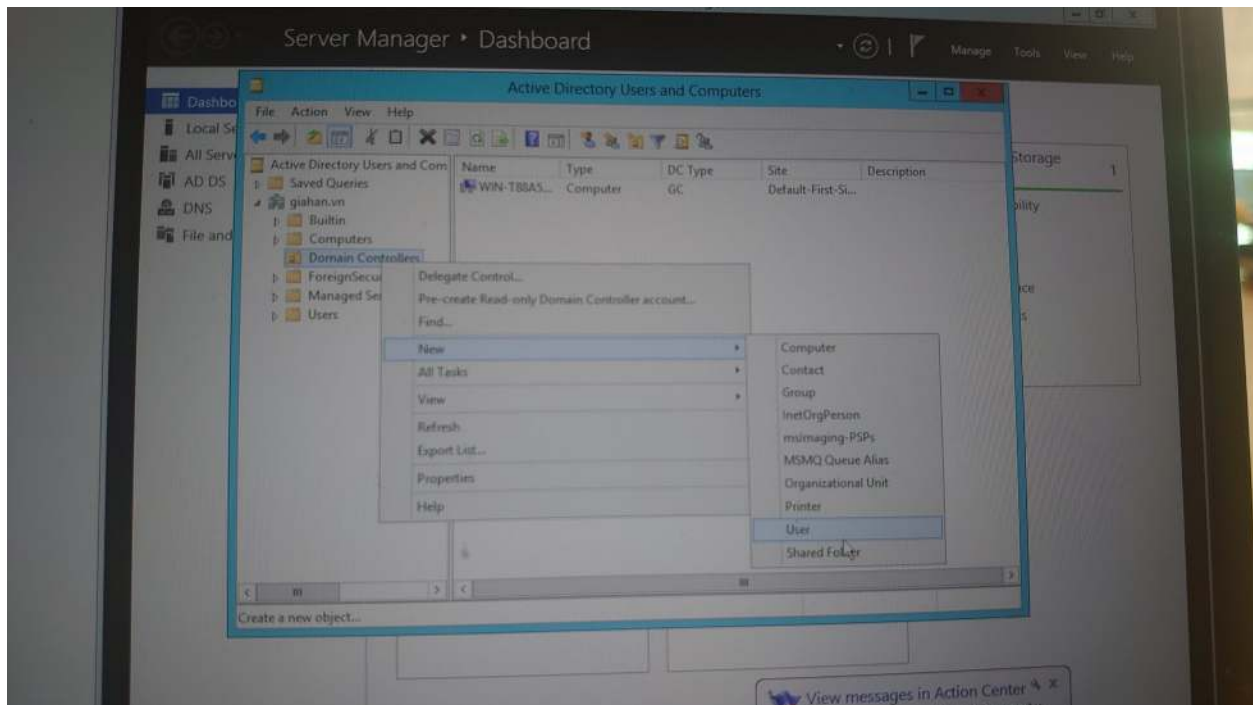


- Cấu hình máy client:
 - o Ip 192.168.10.100
 - o Preferred DNS server: 192.168.10.254

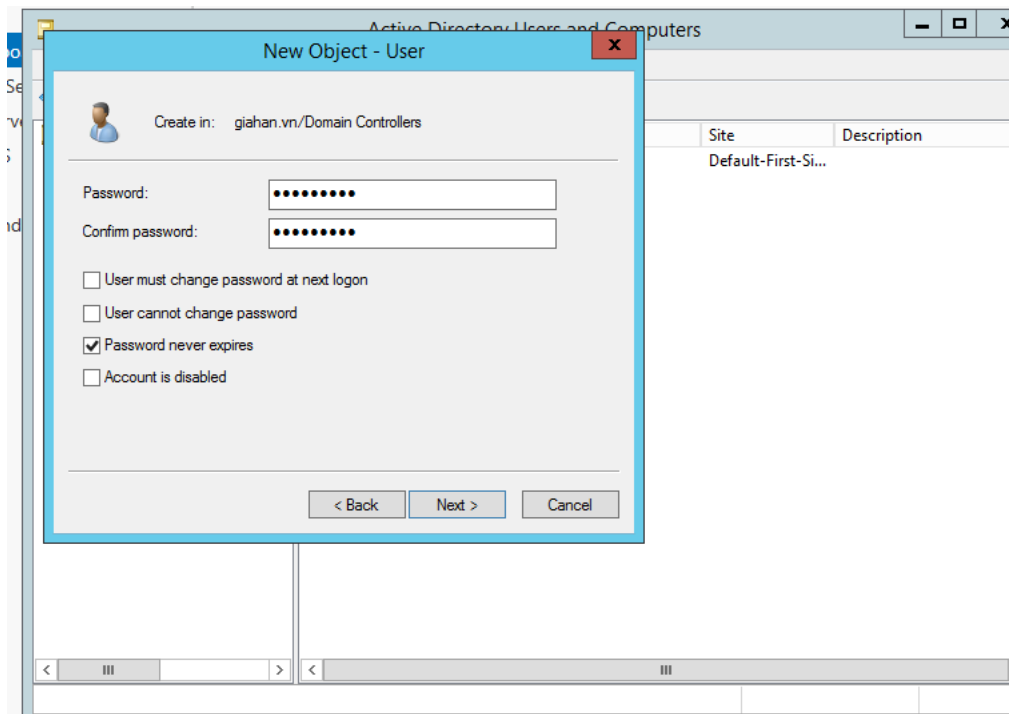
The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Deployment Configuration' step. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Deployment Configuration'. On the right, it says 'TARGET SERVER WIN-T88A5O22OK1'. On the left, there is a navigation pane with the following items: 'Deployment Configuration' (selected), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area contains the following text: 'Select the deployment operation' followed by three radio buttons: 'Add a domain controller to an existing domain', 'Add a new domain to an existing forest', and 'Add a new forest' (which is selected). Below this is the text 'Specify the domain information for this operation' followed by a label 'Root domain name:' and a text box containing 'giahan.vn'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about deployment configurations' is also present.

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window, specifically the 'Domain Controller Options' step. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main heading is 'Domain Controller Options'. On the right, it says 'TARGET SERVER WIN-T88A5O22OK1'. On the left, there is a navigation pane with the following items: 'Deployment Configuration', 'Domain Controller Options' (selected), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area contains the following text: 'Select functional level of the new forest and root domain' followed by two dropdown menus: 'Forest functional level:' (set to 'Windows Server 2012 R2') and 'Domain functional level:' (set to 'Windows Server 2012 R2'). Below this is the text 'Specify domain controller capabilities' followed by three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Below this is the text 'Type the Directory Services Restore Mode (DSRM) password' followed by two password fields: 'Password:' and 'Confirm password:'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about domain controller options' is also present.

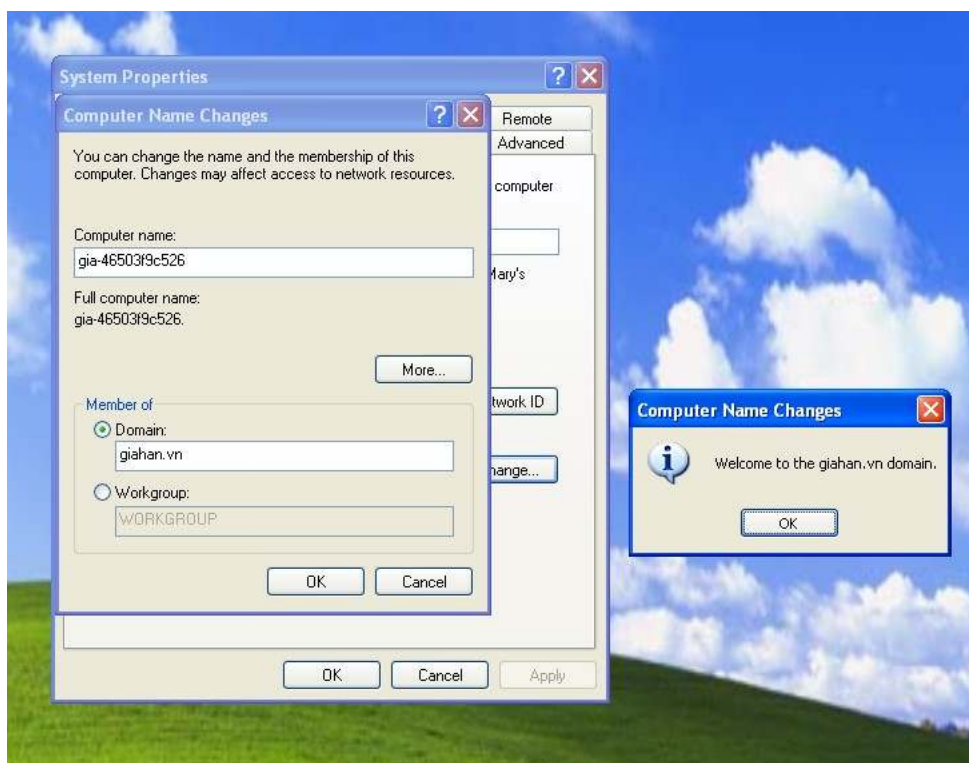




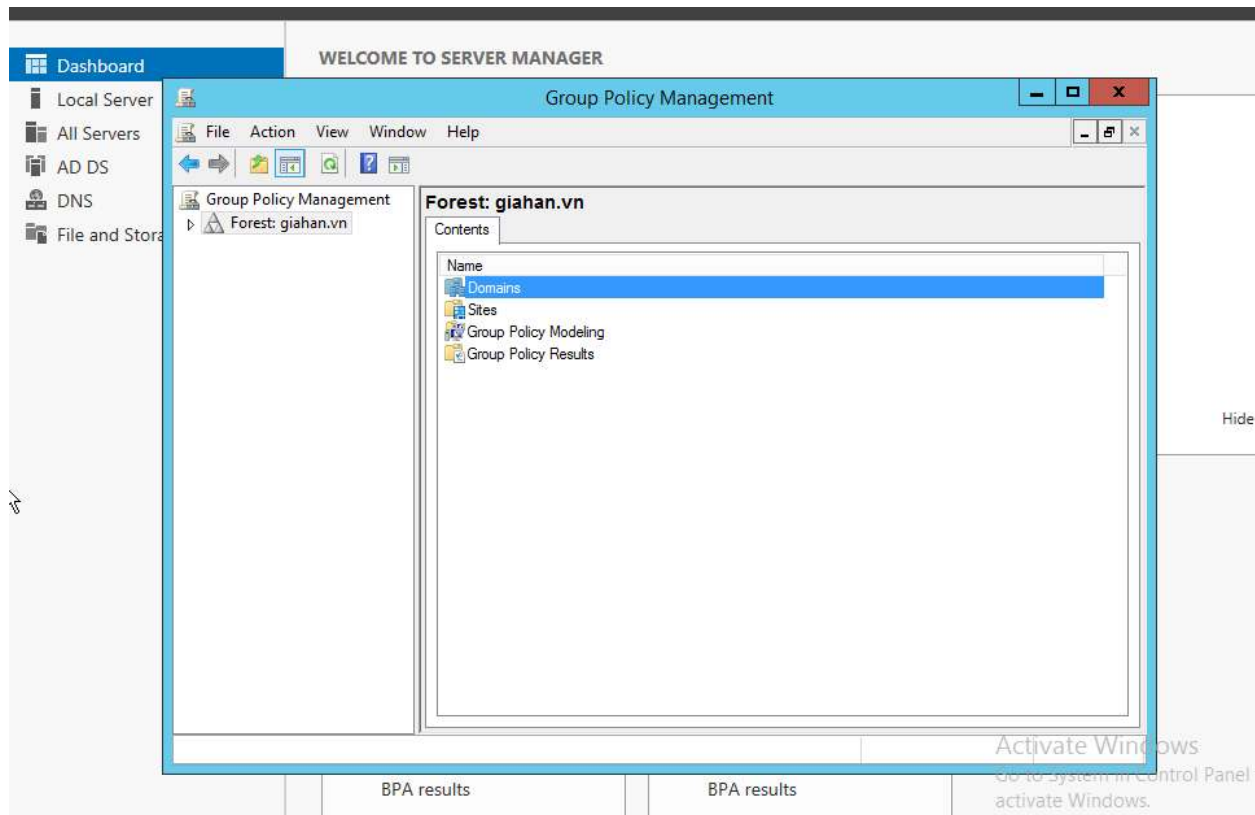
- Tạo tài khoản để đăng nhập vào domain:
 - o User: giahan
 - o Password: ANtoan@123



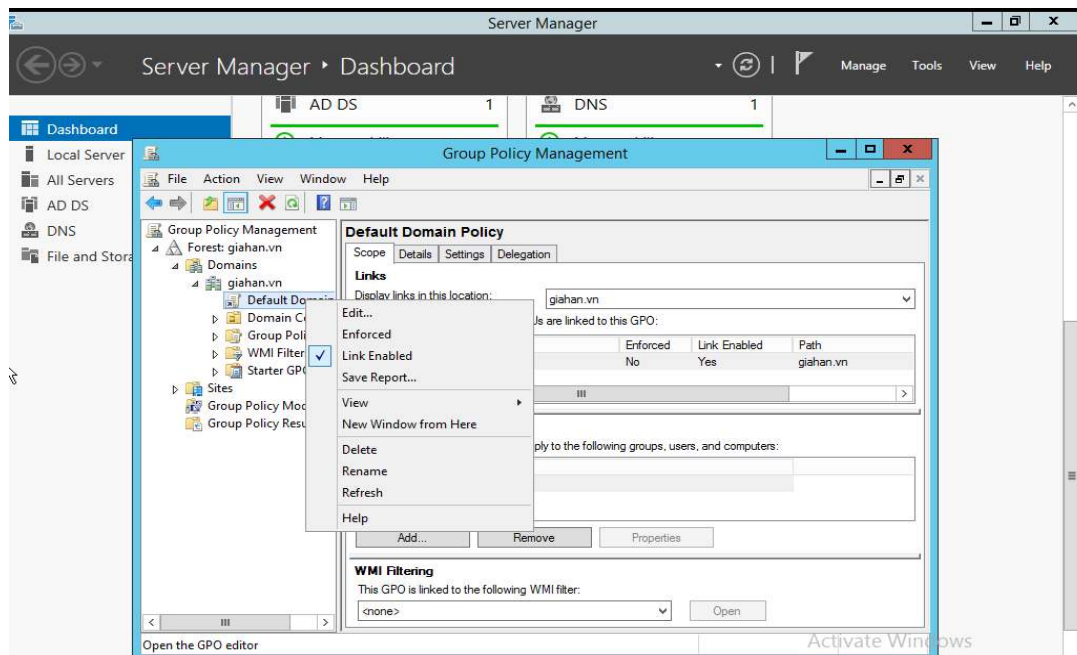
- Chuyển sang domain giahan.vn -> Đăng nhập tài khoản giahan tạo ở trên



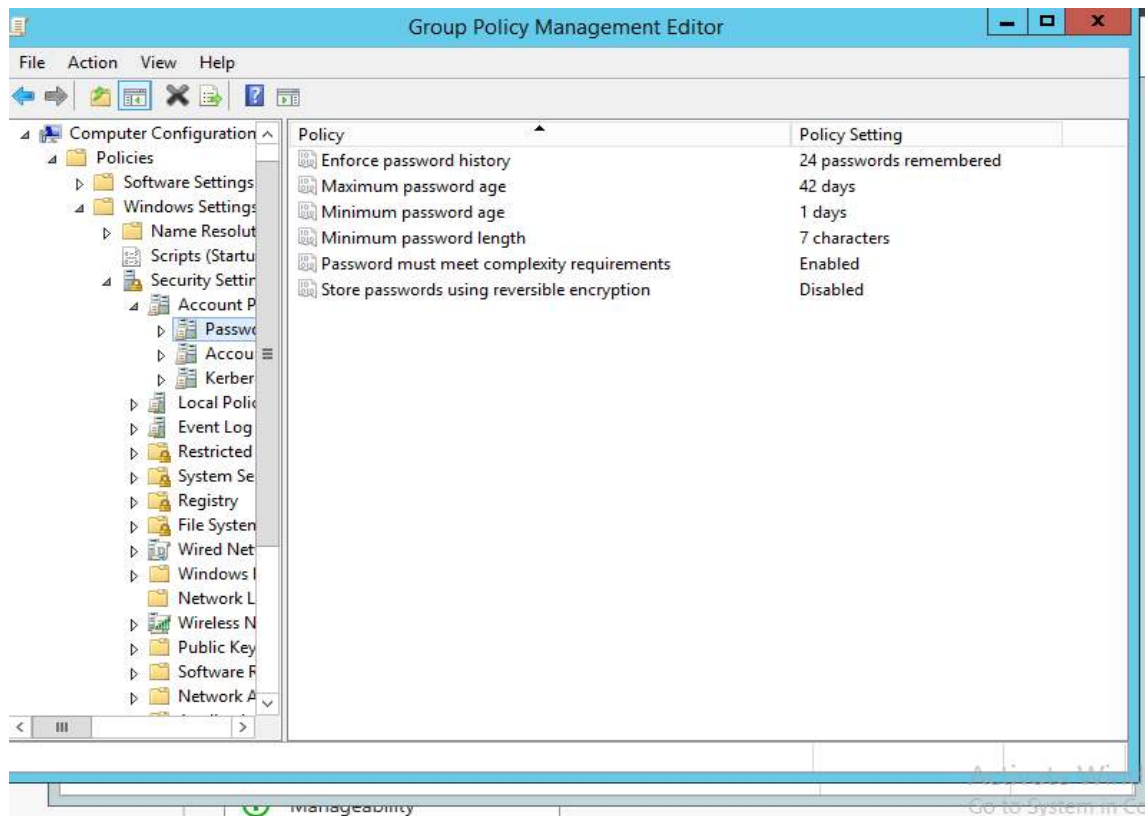
- Thực hiện tạo password policy



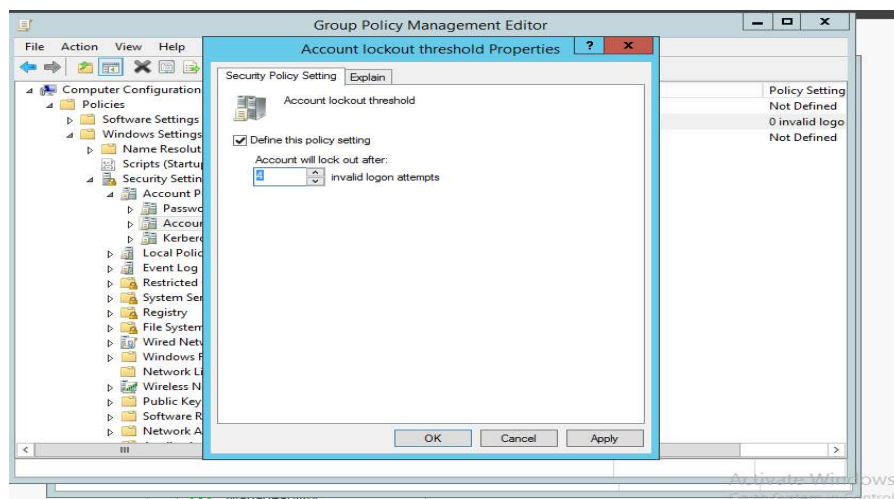
- Vào Domains -> giahan.vn (tên Domain cần cấu hình password policy) -> Default Domain policy-> chuột phải -> nhấn edit



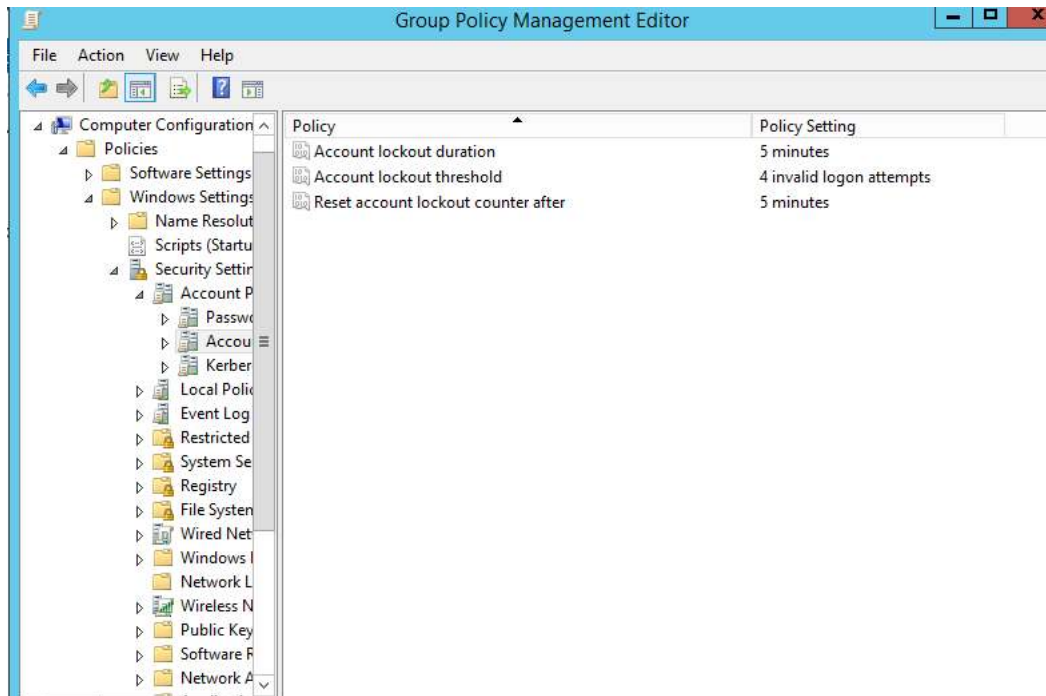
- Tiếp tục vào Policies -> Windows Settings -> Security Setting -> Account policies -> Chuột phải vào Password policies. Sau đó chỉnh những policy tương ứng mà mình muốn chỉnh



- VD: Chỉnh Password length từ 7 sang 5. Không thể tạo tài khoản với số ký tự ít hơn 4



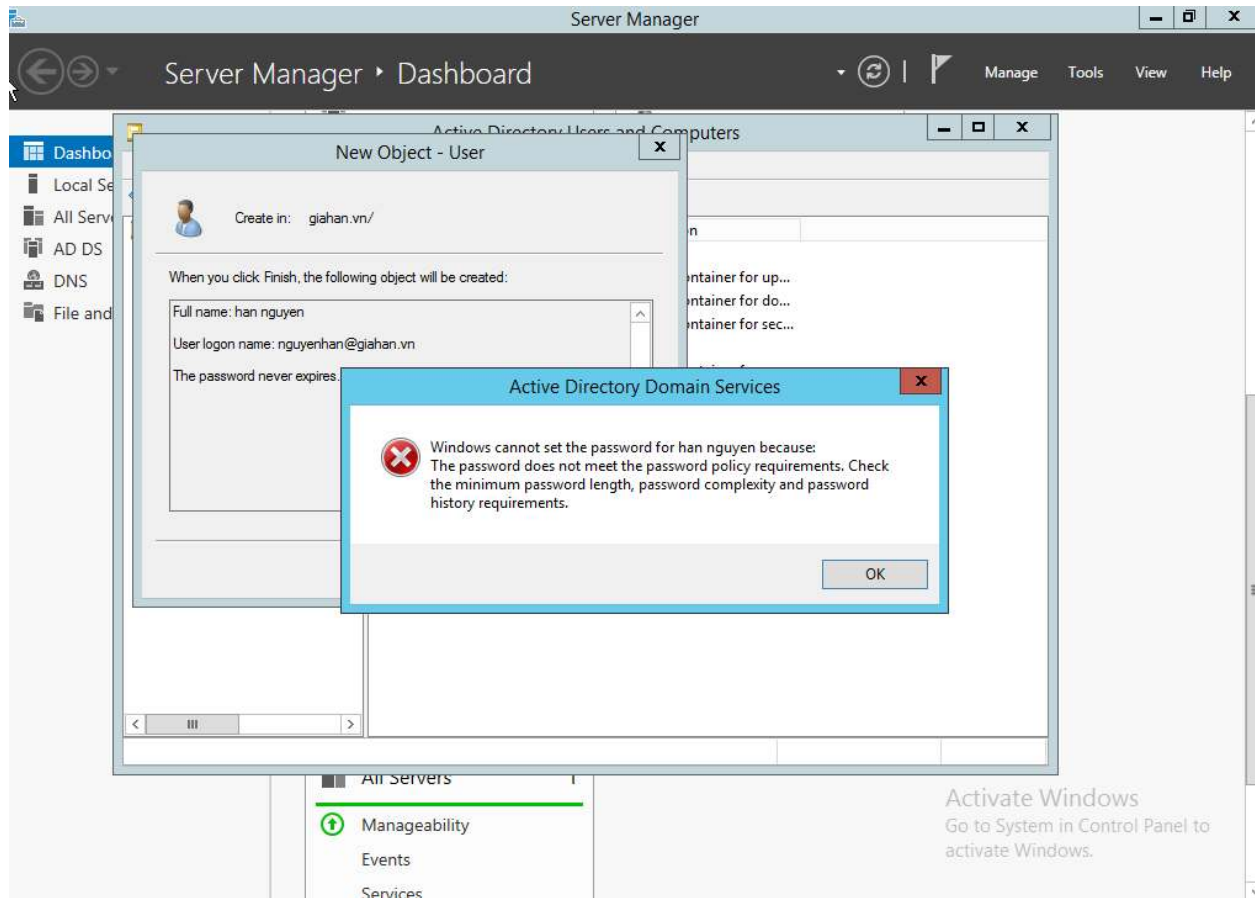
- Để chỉnh Account lockout threshold. Vào Group Policy Managment Editor
- Tiếp tục vào Policies -> Windows Settings -> Security Setting -> Account policies -> Chuột phải vào Account Policy
- Chỉnh Account lockout threshold lên 4 (Khi nhập sai mật khẩu 4 lần tài khoản sẽ bị khóa)
- Account lockout duration: thời gian khóa là 5 phút



Vd: Khi nhập sai mật khẩu quá 4 lần thì tài khoản bị khóa

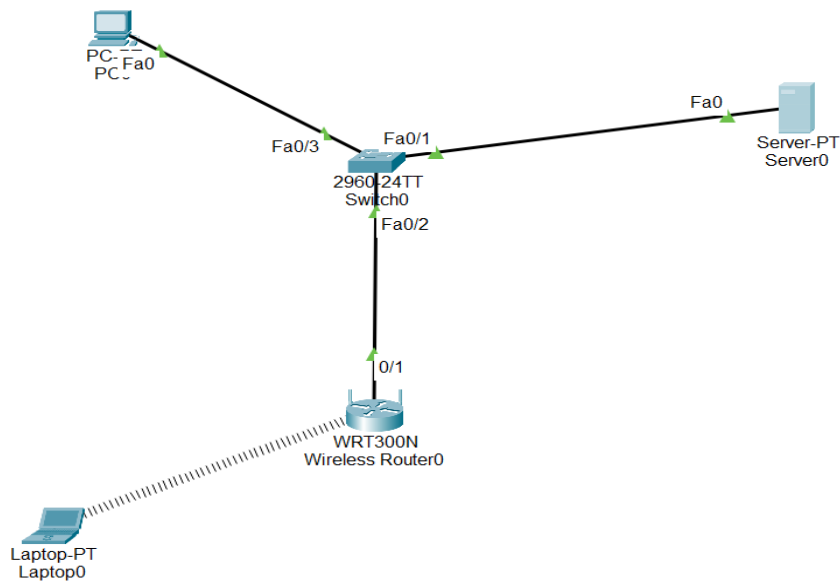


VD: Thử tạo mật khẩu ngắn vi phạm policy. MK: 012



->Không đủ số kí tự

II. WiFi authentication (WPA2) Sơ đồ mạng



Step 1. Configure DHCP server

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.10.1

DNS Server: 8.8.8.8

Start IP Addr: 192.168.10.100

Subnet Mask: 255.255.255.0

Maximum Number of Users: 50

TFTP Server: 0.0.0.0

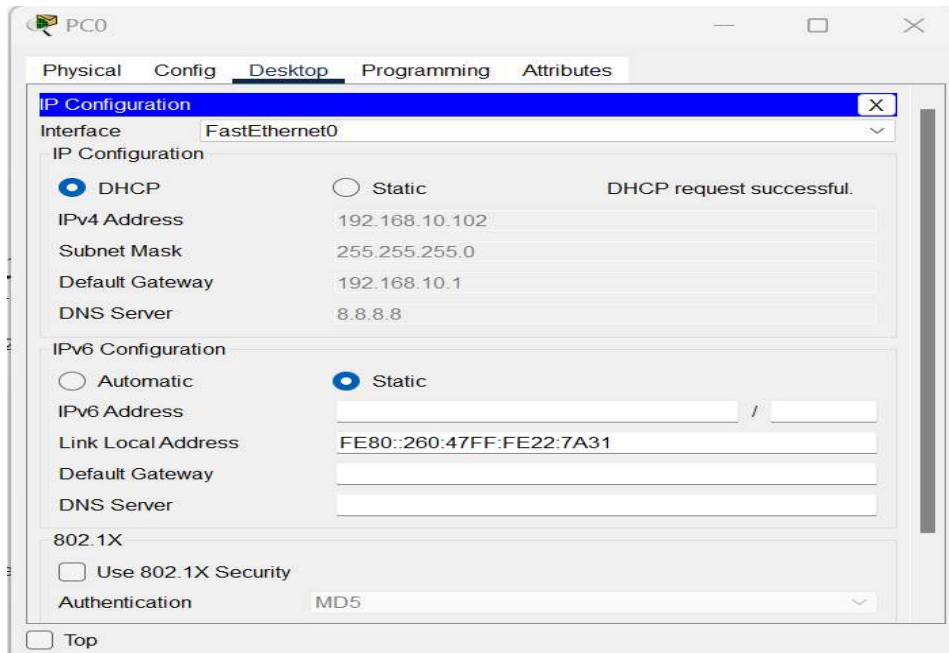
WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.10.1	8.8.8.8	192.168.10.100	255.255.255.0	50	0.0.0.0	0.0.0.0

☐ Top

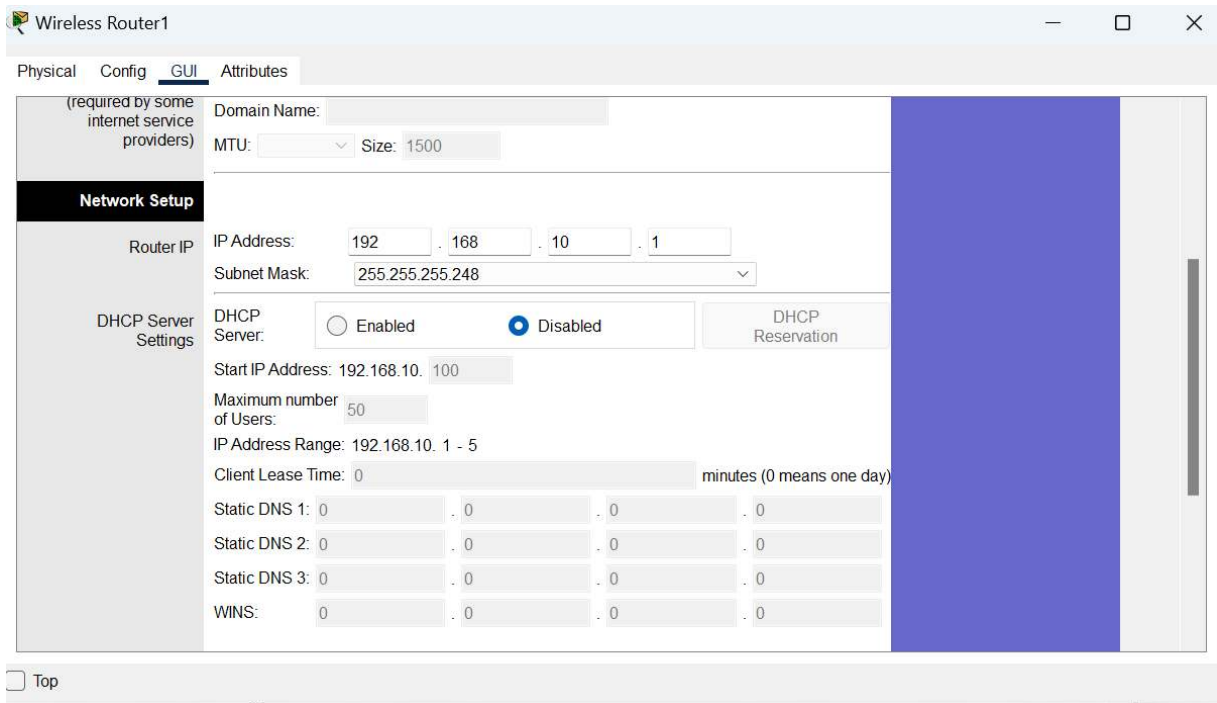
Cấp IP thành công



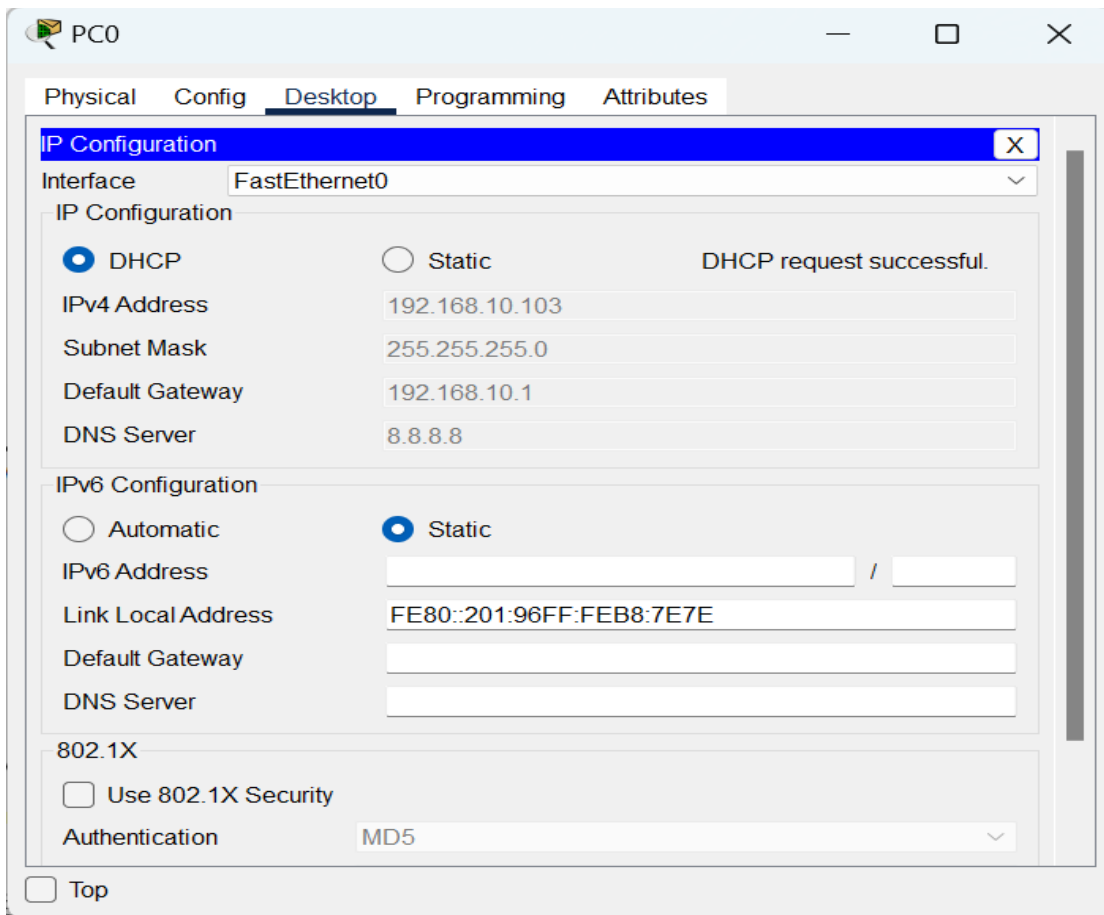
Step 2. Configure AP

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

Tắt DHCP của access point



Cấp IP thành công



Cài đặt trên access point

Network Setup

Router IP

IP Address: 192 . 168 . 10 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ☐ Enabled ☒ Disabled [DHCP Reservation](#)

Start IP Address: 192.168.10. 100

Maximum number of Users: 50

IP Address Range: 192.168.10. 100 - 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Cài đặt security cho access point

Physical Config **GUI** Attributes

Wireless-N Broadband Router Firmware Version: v0.93.3

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter Advanced Wireless Settings

Wireless Security

Security Mode: WPA2 Personal

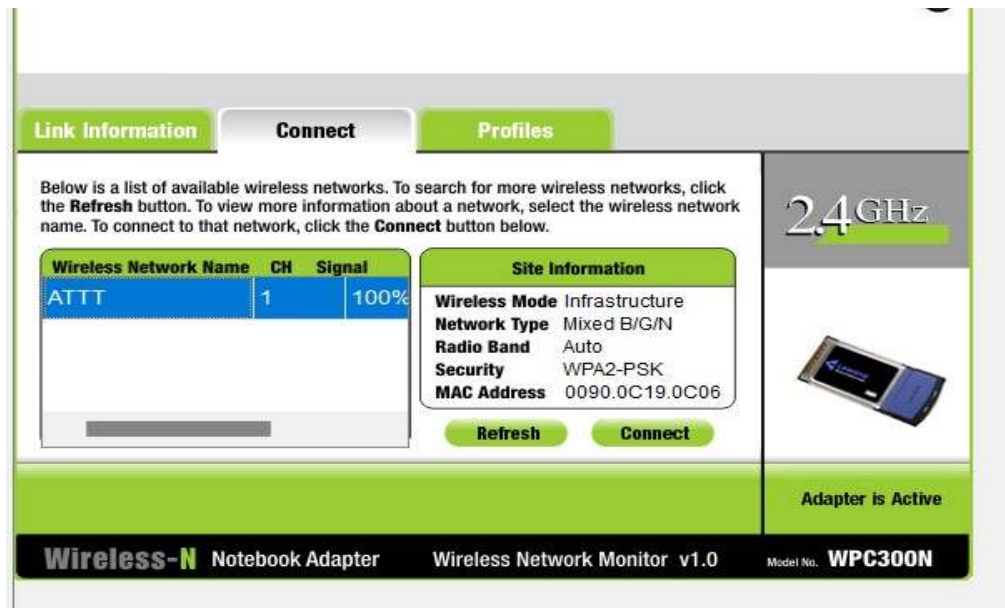
Encryption: AES

Passphrase: Lab03@spkt

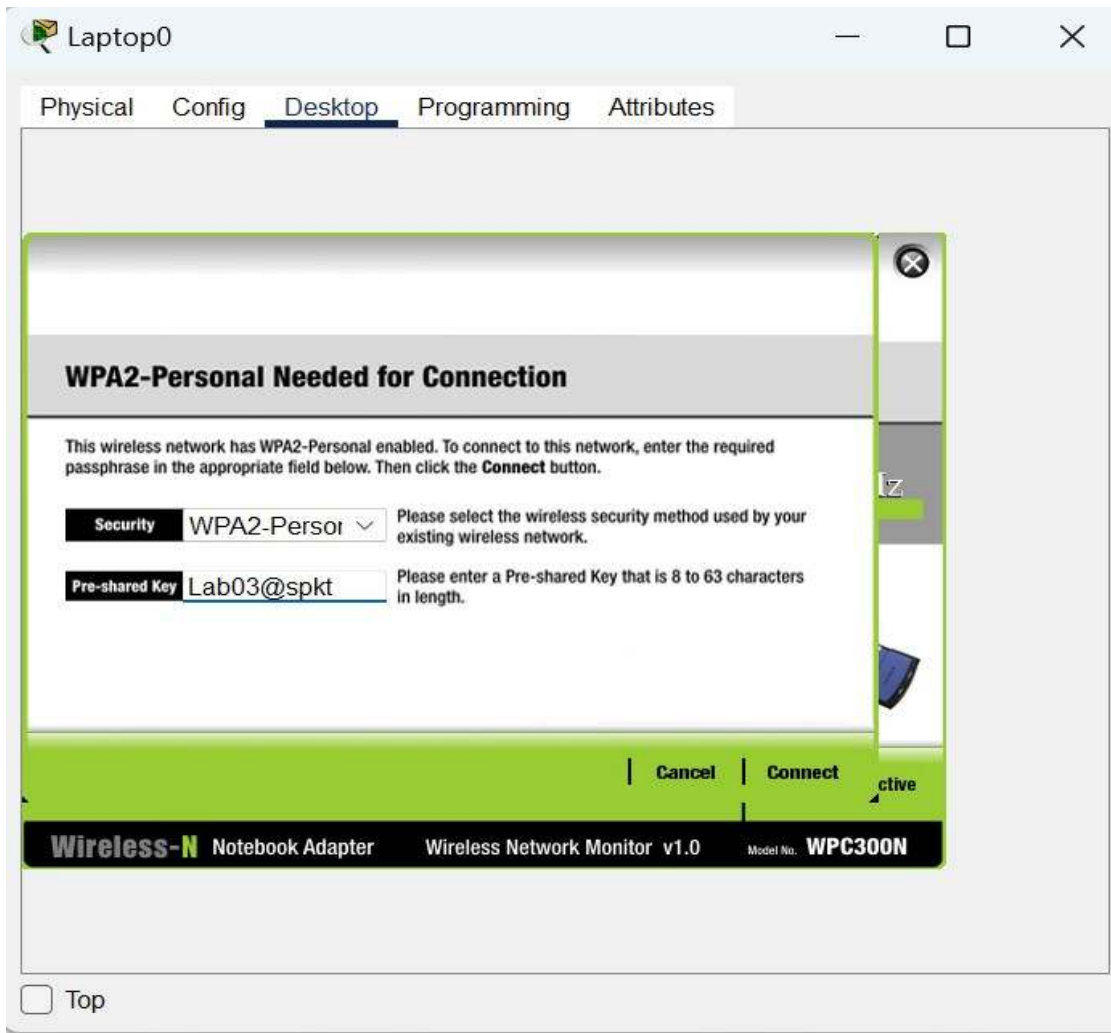
Key Renewal: 3600 seconds

[Help...](#)

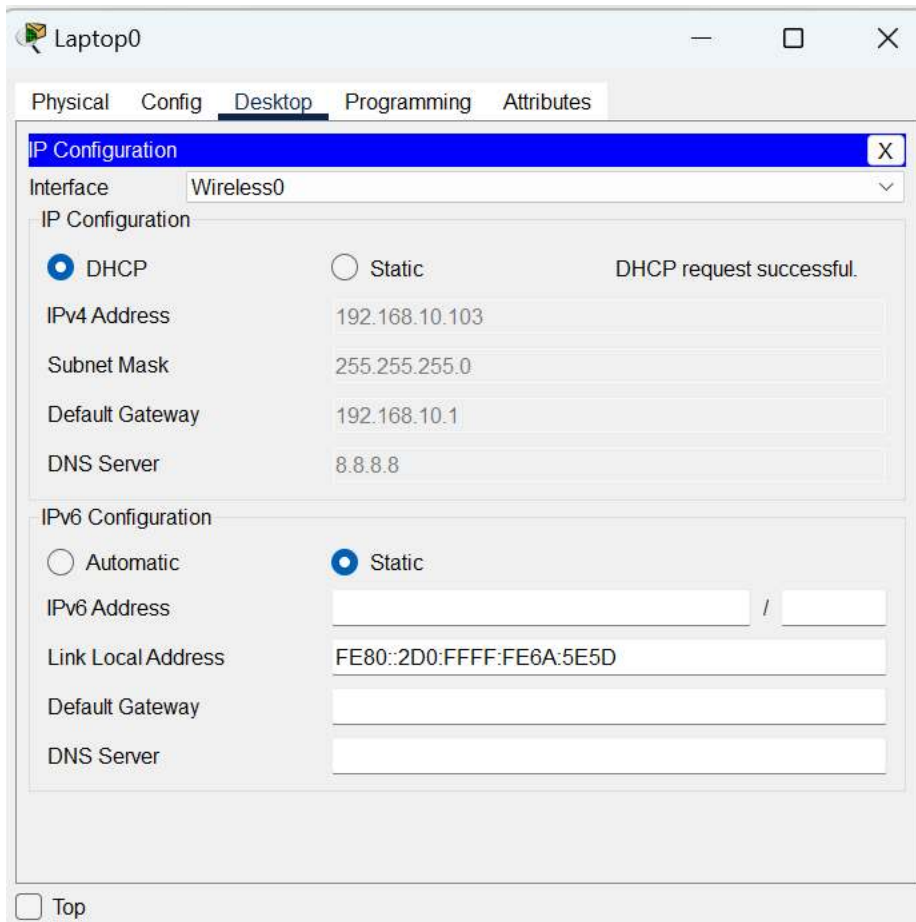
Đặt module cho laptop



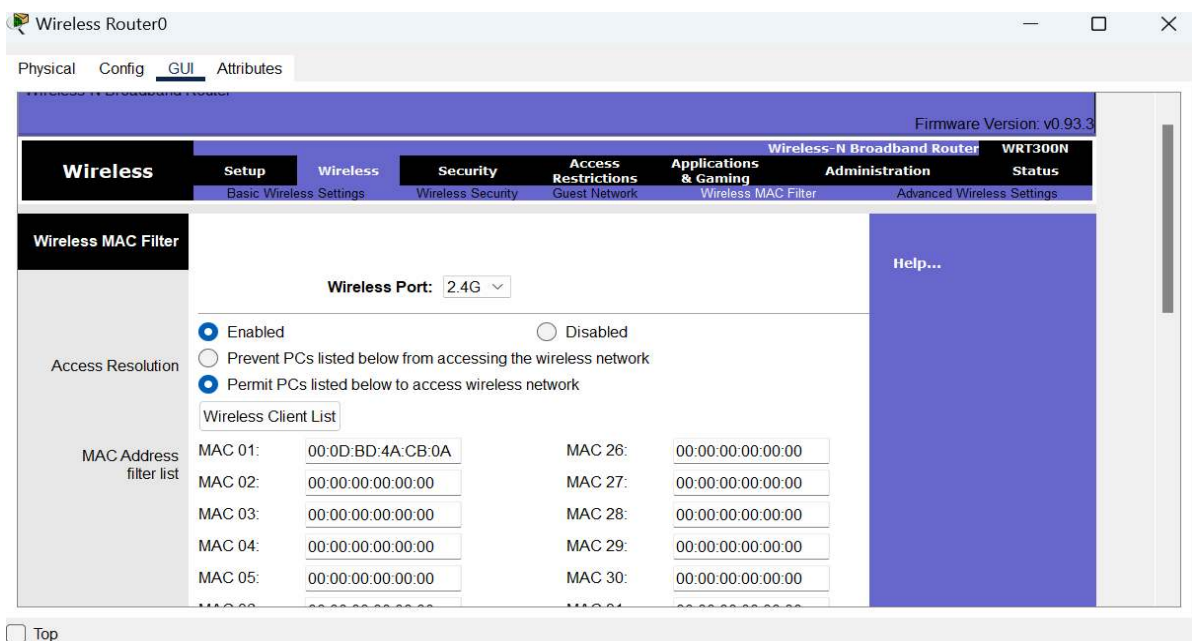
Truy cập từ wireless



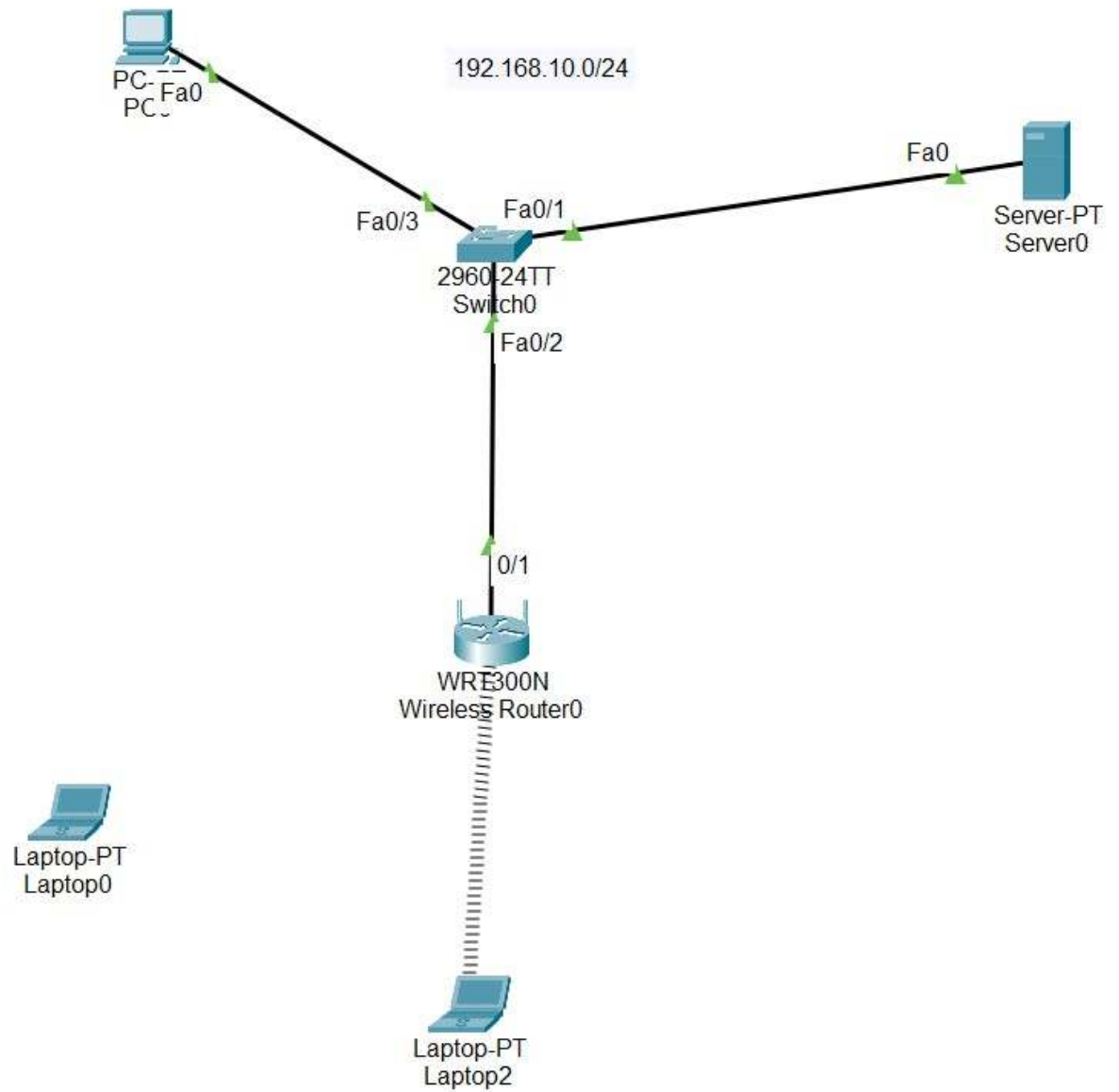
Truy cập thành công



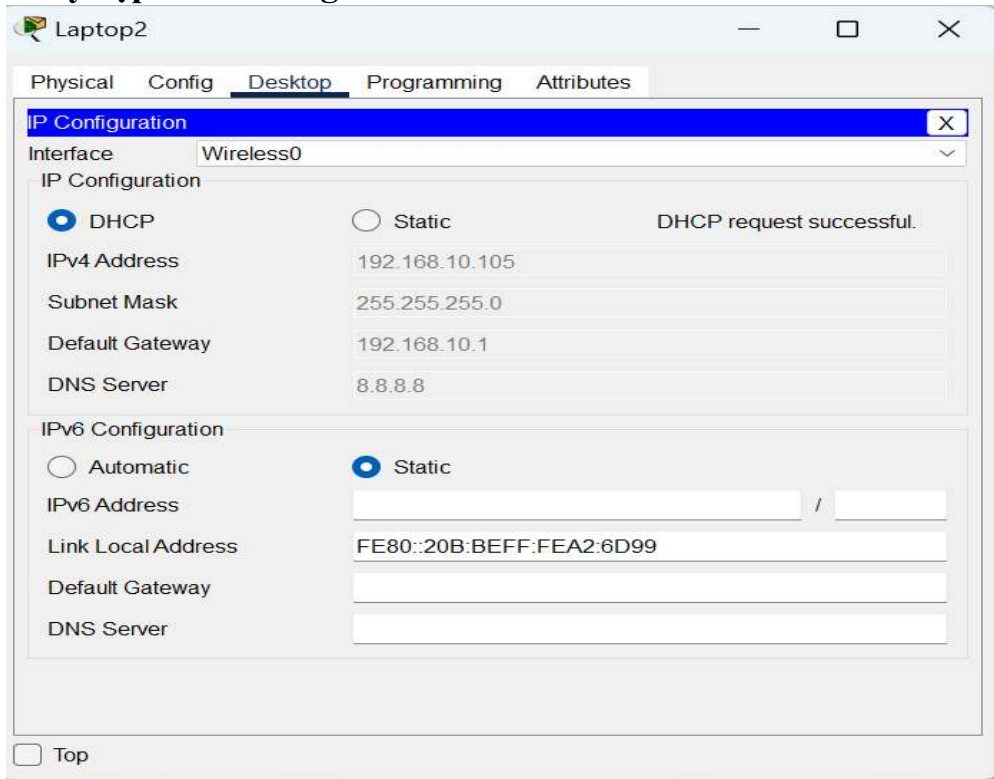
Thêm MAC



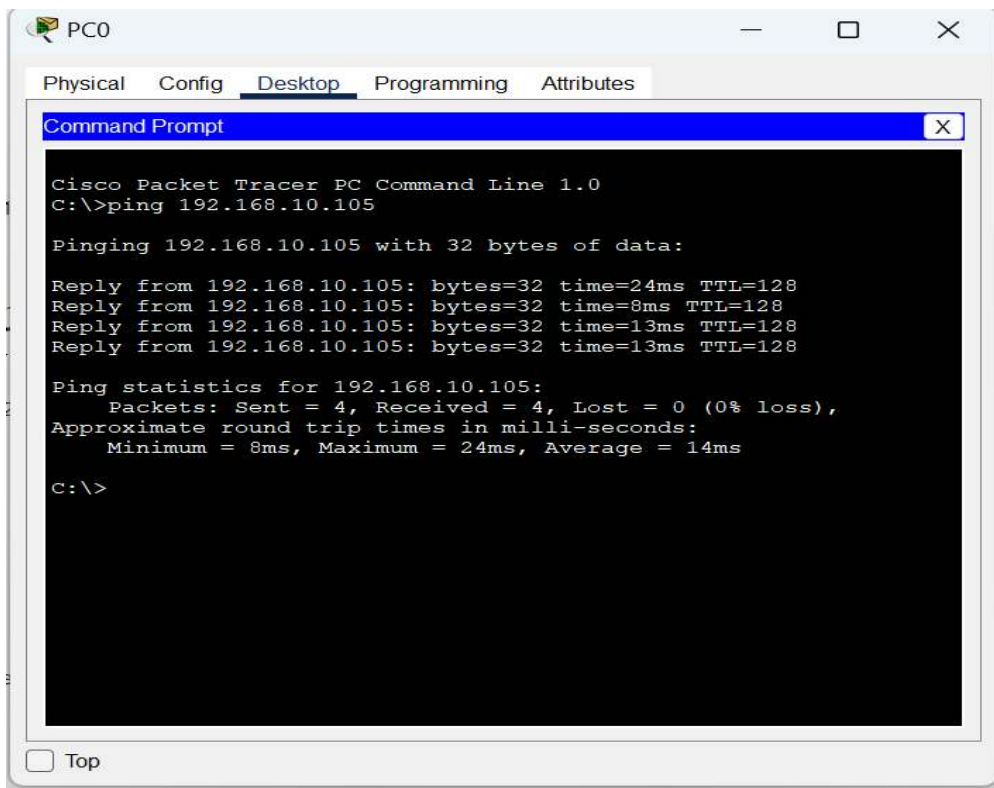
Thêm laptop để kiểm tra MAC



Truy cập thành công



Ping từ PC đến laptop



III. Authentication with Radius server (802.1X)

Step 1: Configure IP address & DHCP server

Configure IP address & DHCP server

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

The screenshot shows the 'Services' tab in the Server0 configuration window. The 'DHCP' service is selected in the left sidebar. The main configuration area for DHCP is displayed, showing the following settings:

- Interface: FastEthernet0
- Service: On (radio button selected)
- Pool Name: serverPool
- Default Gateway: 192.168.10.1
- DNS Server: 8.8.8.8
- Start IP Address: 192.168.10.100
- Subnet Mask: 255.255.255.0
- Maximum Number of Users: 100
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

Below the configuration fields are buttons for 'Add', 'Save', and 'Remove'. At the bottom, there is a table showing the configured DHCP pool:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.10.1	8.8.8.8	192.168.10.100	255.255.255.0	100	0.0.0.0	0.0.0.0

Step 2: Configure AP's IP address

- AP's IP address: 192.168.10.100/24

- SSID: ATTT
- Authentication (radius server): WPA2 - Enterprise

Network Setup

Router IP: IP Address: 192 . 168 . 10 . 100
Subnet Mask: 255.255.255.0

DHCP Server Settings: DHCP Server: ☐ Enabled ☒ Disabled

Start IP Address: 192.168.0. 100
Maximum number of Users: 50
IP Address Range: 192.168.0. 100 - 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0

Wireless-N Broadband Router Firmware Version: v0.93.3

Wireless **Setup** **Wireless** **Security** **Access Restrictions** **Applications & Gaming** **Administration** **Status**

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter Advanced Wireless Settings

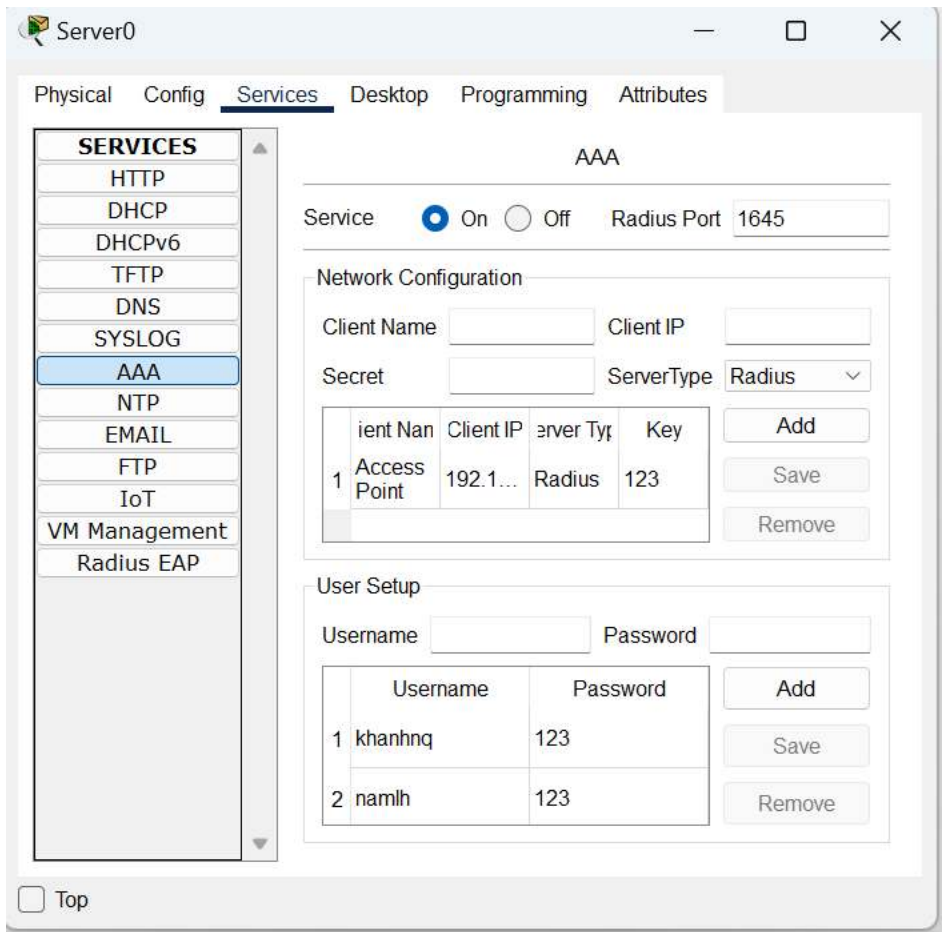
Wireless Security

Security Mode: WPA2 Enterprise
Encryption: AES
RADIUS Server: 192 . 168 . 10 . 254
RADIUS Port: 1645
Shared Secret: 123
Key Renewal: 3600 seconds

[Help...](#)

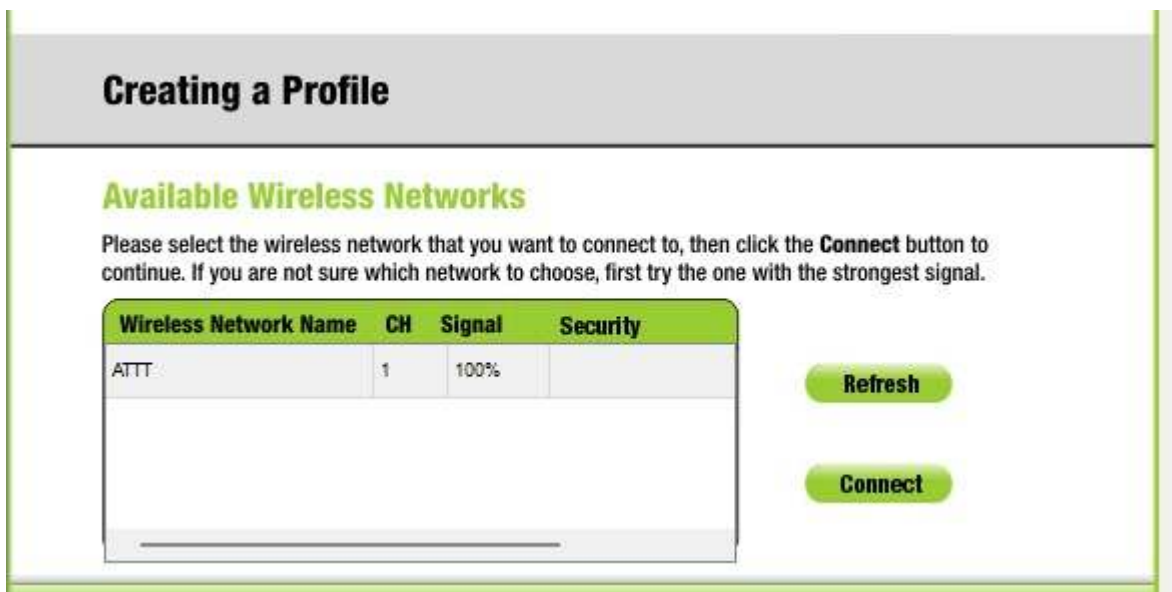
Step 3: Configure RADIUS server

- Set the IP address of the Radius client (the authenticator – AP's IP address) : 192.168.10.100
- Set the **key-ID** : 123
- Create accounts : namlh, khanhnq



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

- Creating a profile



Creating a Profile

Wireless Security

Security

WPA2-Enter

Please select the wireless security method used by your existing wireless network.

WEP stands for Wired Equivalent Privacy.

WPA-Personal, also known as Pre-shared Key, is a security standard stronger than WEP encryption.

WPA2-Personal is the newer version with stronger encryption than WPA-Personal.

WPA-Enterprise, WPA2-Enterprise and **RADIUS** use Remote Authentication Dial-In User Service (RADIUS).

Back

Next

Wireless-N

Notebook Adapter

Wireless Network Monitor v 1.11

Model No. WPC300N

Fill username & password

Creating a Profile

Wireless Security - WPA2 Enterprise

Authentication

PEAP

Login Name

khanhng

Password

••••

Server Name

Certificate

Trust Any

Inner Authen.

TOKEN CARD

Please select the authentication method that you use to access your network.

Enter the Login Name used for authentication.

Enter the Password used for authentication.

Enter the Server Name used for authentication. **(Optional)**

Please select the certificate used for authentication.

Please select the inner authentication method used inside the PEAP tunnel.

Back

Next

Wireless-N

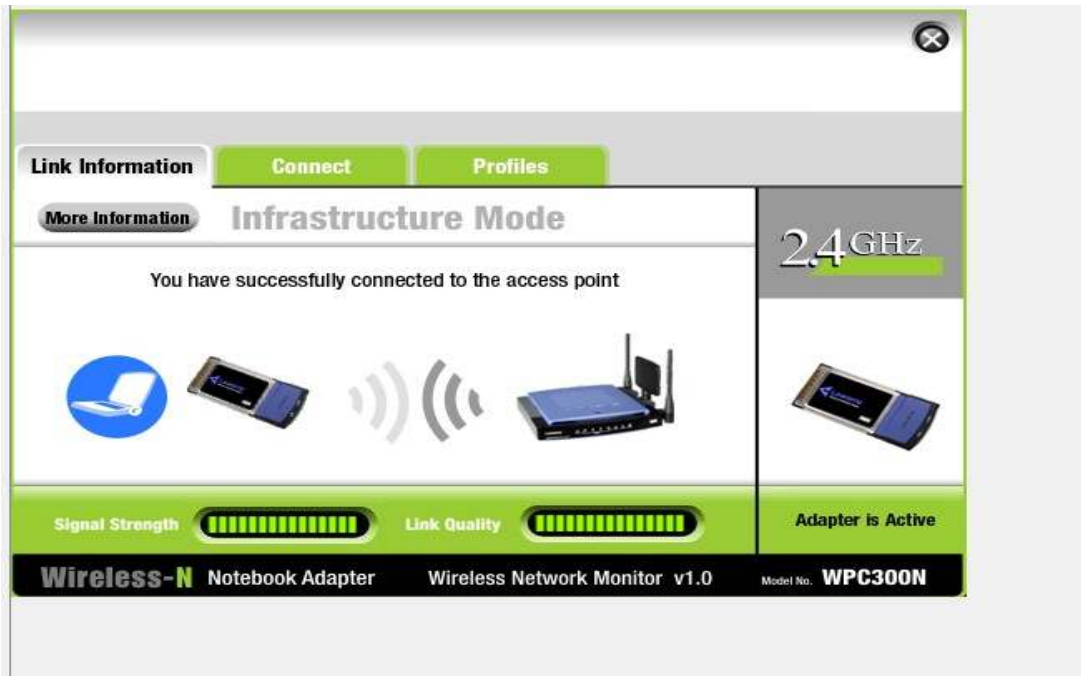
Notebook Adapter

Wireless Network Monitor v 1.11

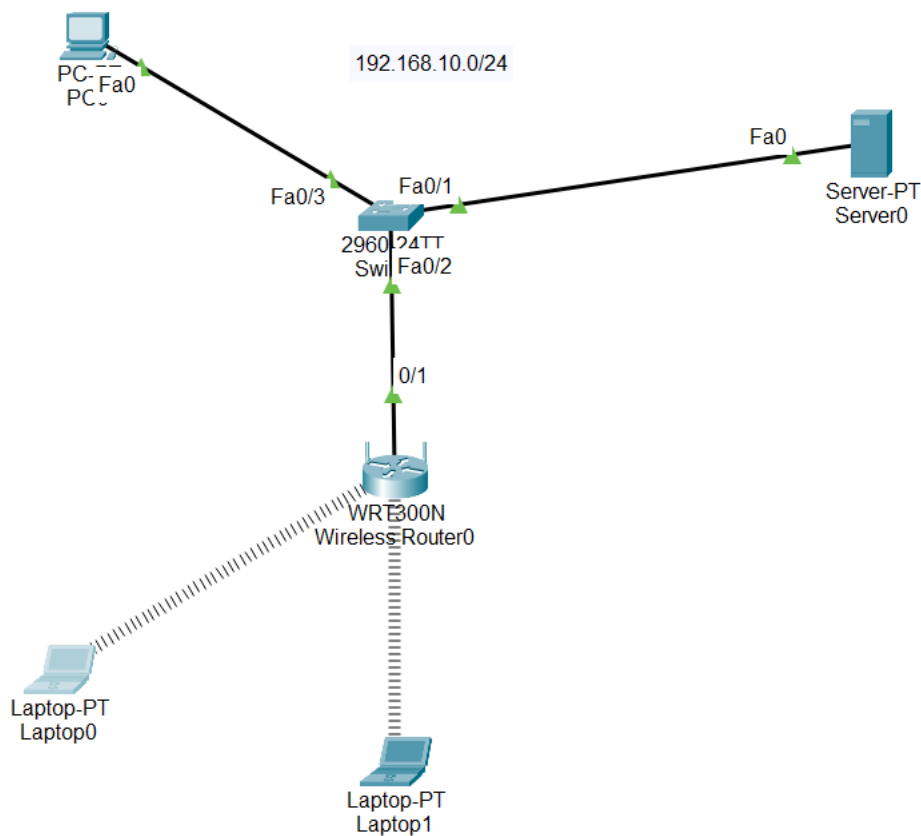
Model No. WPC300N

Top

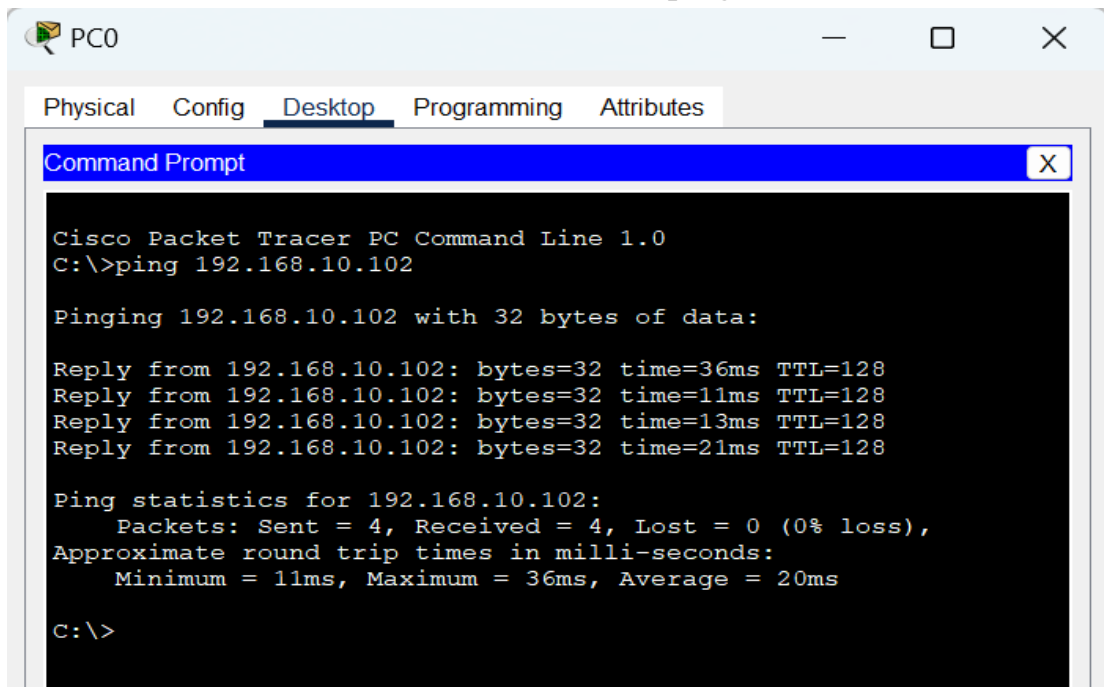
Kết nối thành công



Step 5: Verify the configuration - test on the supplicant



- Check IP address information and ping to other PCs



The screenshot shows a window titled "PC0" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a "Command Prompt" window. The command prompt shows the output of a ping command to 192.168.10.102. The output indicates that the ping was successful with 0% loss and an average round trip time of 20ms.

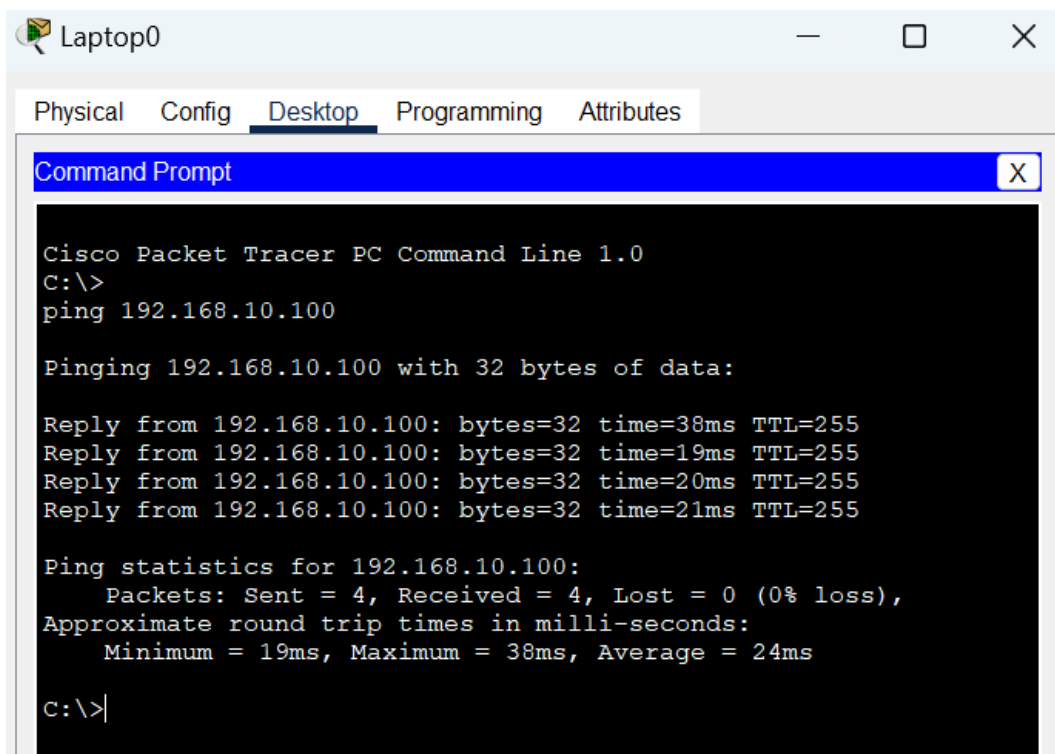
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.102

Pinging 192.168.10.102 with 32 bytes of data:

Reply from 192.168.10.102: bytes=32 time=36ms TTL=128
Reply from 192.168.10.102: bytes=32 time=11ms TTL=128
Reply from 192.168.10.102: bytes=32 time=13ms TTL=128
Reply from 192.168.10.102: bytes=32 time=21ms TTL=128

Ping statistics for 192.168.10.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 36ms, Average = 20ms

C:\>
```



The screenshot shows a window titled "Laptop0" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a "Command Prompt" window. The command prompt shows the output of a ping command to 192.168.10.100. The output indicates that the ping was successful with 0% loss and an average round trip time of 24ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time=38ms TTL=255
Reply from 192.168.10.100: bytes=32 time=19ms TTL=255
Reply from 192.168.10.100: bytes=32 time=20ms TTL=255
Reply from 192.168.10.100: bytes=32 time=21ms TTL=255

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 38ms, Average = 24ms

C:\>|
```