

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Libvirt 64-bit

kali Linux 2023.4-vmware-amd64

root@kali: /home/kali/Desktop

```
13 80:18:8A:34:51:5E Test Unknown
14 18:D0:71:C8:C5:83 BaoNhan Unknown
15 1C:E6:C7:DC:58:60 Unknown
16 1C:E6:C7:DC:58:6F Unknown
17 1C:E6:C7:DC:5D:70 Unknown
18 1C:E6:C7:DC:63:00 FPTU_University Unknown
19 1C:E6:C7:DC:63:01 FPTU_Camera Unknown
20 1C:E6:C7:DC:63:02 FU_Service Unknown
21 1C:E6:C7:DC:63:03 FUG_Staffs Unknown
22 1C:E6:C7:DC:63:04 FPTU_Guest Unknown
23 1C:E6:C7:DC:63:05 FPTU_Laboratory Unknown
24 26:D8:56:12:87:2E Unknown
25 4B:50:73:1C:AF:52 TheSinhTourist-518-143.2v Unknown
26 50:17:FF:F5:63:E0 Unknown
27 50:17:FF:F5:68:24 FPTU_Guest Unknown
28 50:17:FF:F5:43:54 FPTU_Guest Unknown
29 58:60:8F:97:75:22 WPA (0 handshake)
30 68:8C:8C:C8:16:A0 FPTU_University Unknown
31 68:8C:8C:C8:16:A1 FPTU_Camera Unknown
32 68:8C:8C:C8:16:A2 FU_Service Unknown
33 68:8C:8C:C8:16:A3 FUG_Staffs Unknown
34 68:8C:8C:C8:16:A4 FPTU_Guest Unknown
35 68:8C:8C:C8:16:A5 FPTU_Laboratory Unknown
36 82:00:00:00:25:25 Connectify-me Unknown
37 86:D5:8C:C8:00:00 Unknown
38 90:06:28:BA:33:7B Ares Unknown
39 AA:66:A5:29:A7:34 oylly's 1p <3 Unknown
40 CA:E9:84:36:C2:68 LeNa WPA (1 handshake)
41 C8:3A:15:51:6C:2D08 KETOAN WPA (0 handshake)
42 CA:3A:15:51:6C:18:49 Unknown
43 DC:72:98:87:BA:D4 HUAWET P20 Pro Unknown
44 E8:ED:F3:EA:44:F0 FPTU_University Unknown
45 E8:ED:F3:EA:44:F1 FPTU_Camera Unknown
46 E8:ED:F3:EA:44:F2 FU_Service Unknown
47 E8:ED:F3:EA:44:F3 FUG_Staffs Unknown
48 E8:ED:F3:EA:44:F4 FPTU_Guest Unknown
49 E8:ED:F3:EA:44:F5 FPTU_Laboratory Unknown
50 E8:ED:F3:EA:44:FF Unknown
```

Index number of target network 7 0:

direct input to this VM, move the mouse pointer inside or press Ctrl+G.

21°C
Cố máy

11:16 pm
07/03/2024

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Libvirt 64-bit

kali Linux 2023.4-vmware-amd64

root@kali: /home/kali/Desktop

Aircrack-ng 1.7

[00:00:02] Tested 58350 keys (got 16391 IVs)

```
KB depth bytes{vets}
0 0/ 6 12(23286) 93(21766) 88(21504) 83(20992) 83(20736) 28(20736) 73(20224) 8F(20224) 9F(20224) AC(20224) 0E(19968) 85(19968) 0C(19968) 2F(19968) 0D(19968) 0B(19712) A9(19712) C3(19712) E3(19712)
1 0/ 3 34(24576) 34(22784) 99(22016) A2(21584) 81(21248) 23(21248) 7C(20992) 4D(20736) 88(20736) 3E(20480) A7(19968) 32(19712) 47(19712) 10(19456) 49(19456) 52(19456) C8(19456) E1(19456) A4(19200)
2 1/ 15 56(28992) F2(28692) 26(28692) 8C(28736) A1(28736) 6E(28736) 5B(28480) 6B(28480) 09(28480) E0(28224) E0(28224) 3A(28224) C1(19968) 26(19712) 67(19712) A9(19712) FA(19712) 05(19456)
3 1/ 13 19(20224) 14(19968) 10(19968) 76(19968) 0F(19968) 64(19712) 1A(19456) D6(19456) 2E(19200) F3(19200) 13(18944) 45(18944) 54(18944) A8(18944) BC(18944) 0B(18944) 16(18688) 34(18688) 3F(18688)
4 10/ 18 90(20224) CB(20224) 86(19968) A8(19968) 1C(19712) 65(19712) 79(19712) 9A(19712) 69(19456) AA(19456) BD(19456) 00(19200) 4D(19200) 5B(19200) FE(19200) 0A(18944) 2A(18944) 36(18944) 3E(18944)
```

KEY FOUND! [12:34:56:78:90]

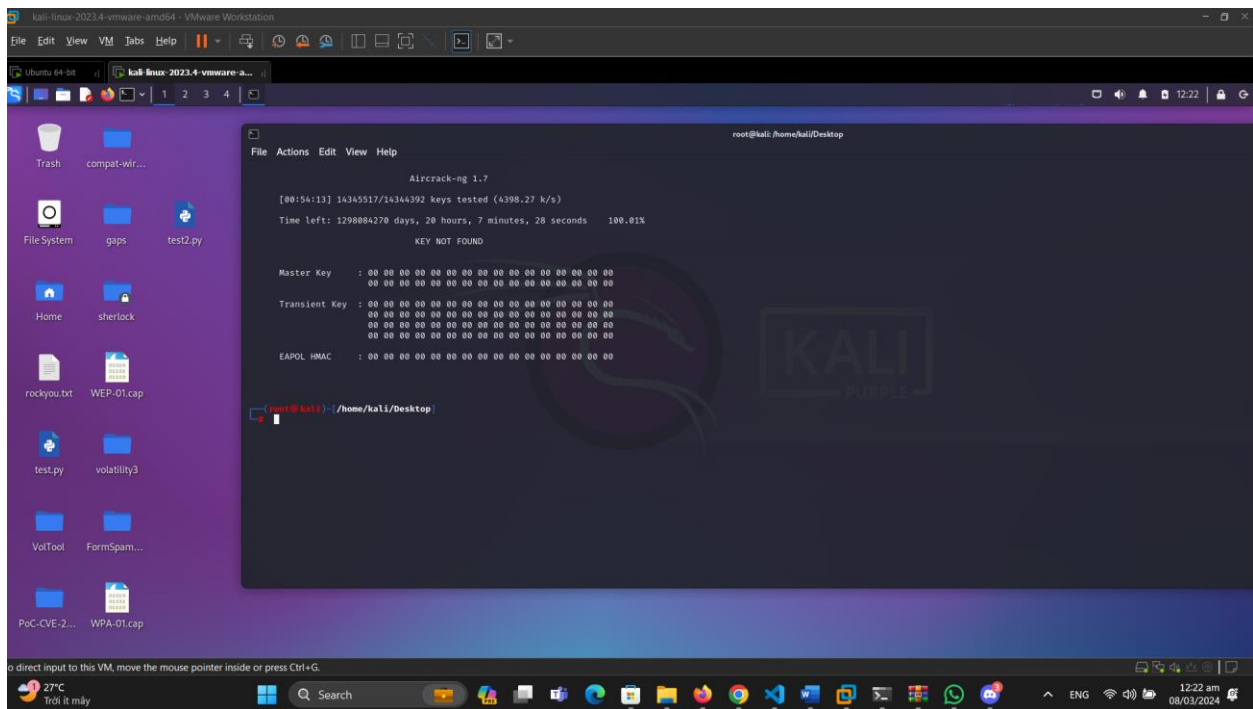
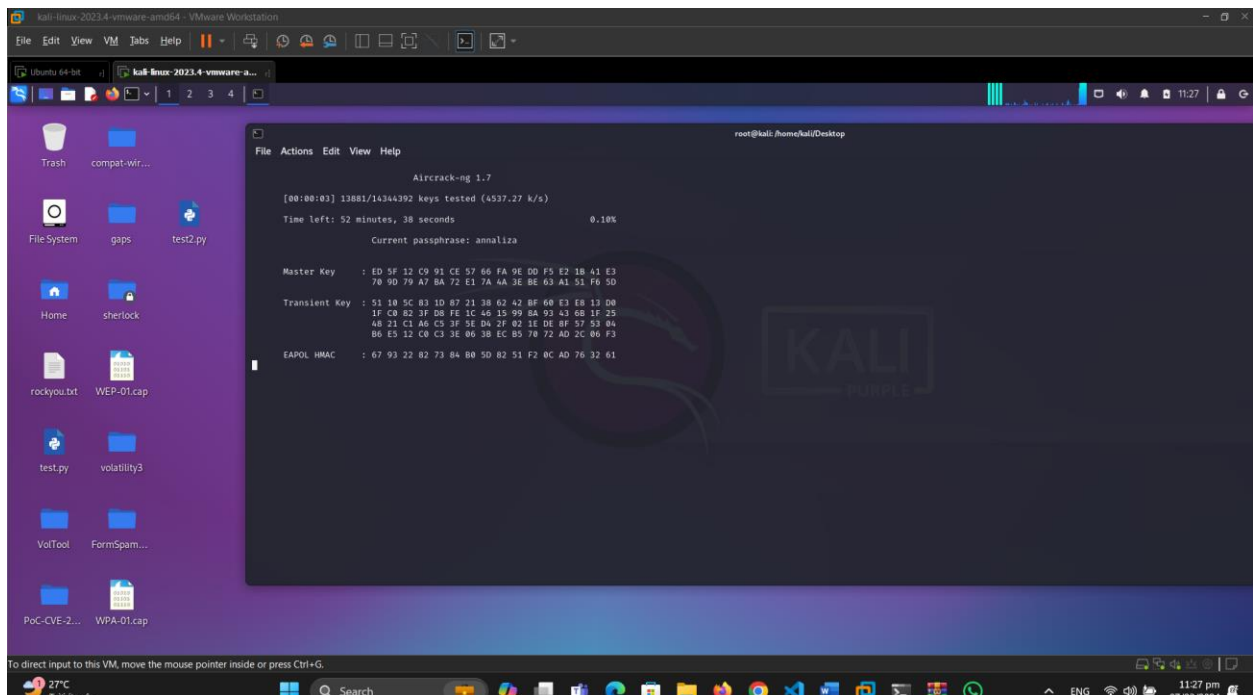
Decrypted correctly: 100%

root@kali: /home/kali/Desktop

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

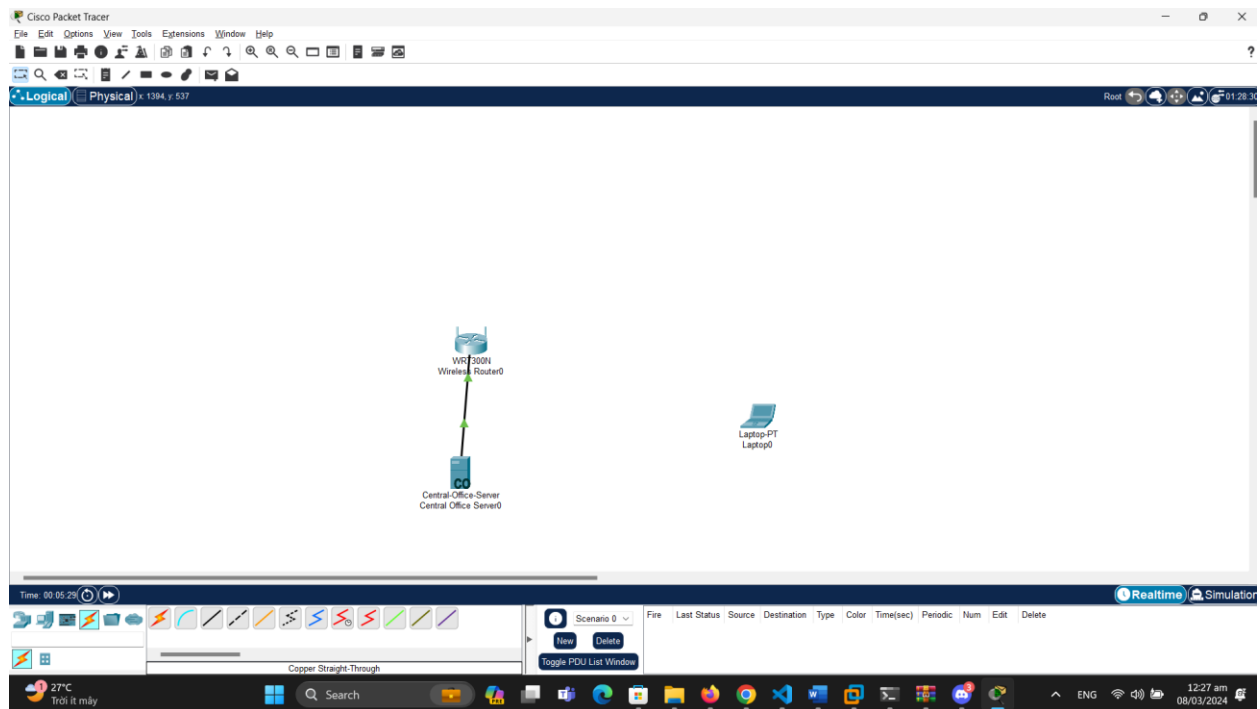
21°C
Cố máy

11:16 pm
07/03/2024



I, Chuẩn bị

- Để demo bài lab này thì ta dùng phần mềm Packet tracer, các bạn nhớ dùng phiên bản mới nhất (5.3.3).
- Các bạn kéo ra 1 con Linksys Router, 1 con Laptop, 1 con Server và kết nối như hình dưới



- Ta dùng RADIUS Server để chứng thực người dùng, mỗi người dùng sẽ có 1 username/password riêng, thay vì dùng "shared key" như các chuẩn WPA/WPA2 Personal

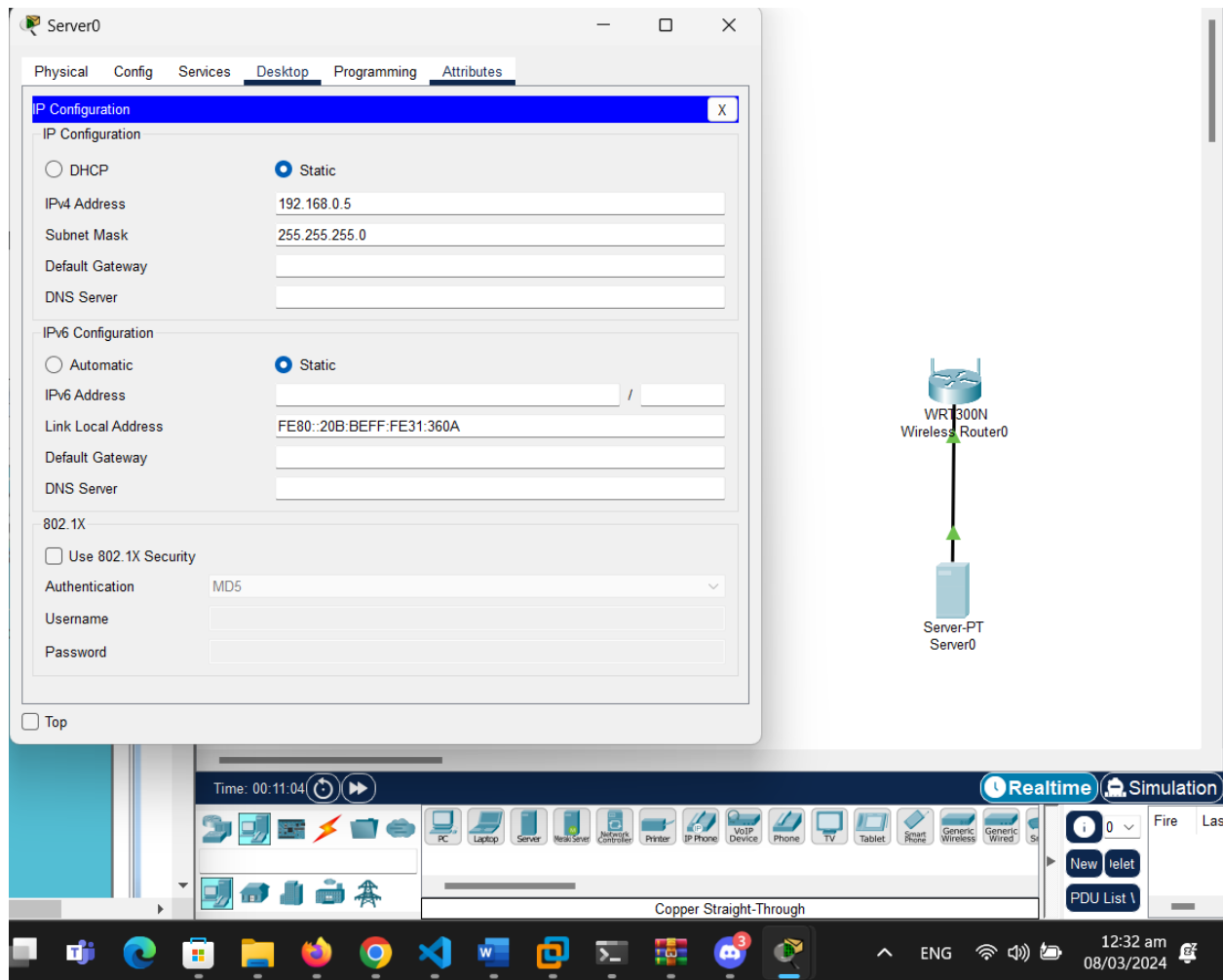
-Chia bài lab ra 3 bước cho dễ nhìn :

+ Bước 1 : đặt IP tĩnh cho Linksys và RADIUS Server

+ Bước 2 : Cấu hình xác thực giữa Linksys và RADIUS Server thông qua key "chungthucradius" , tạo user : radius với pass : chungthucradius để cấp cho Laptop

+ Bước 3 : Cài đặt để Laptop có thể bắt được Wifi II,

Bước 1 Đặt IP cho RADIUS Server



Đặt IP cổng LAN cho Linksys thông qua giao diện GUI. Với con Linksys thực nó dùng IP mặc định là 192.168.1.1, còn trong lab thì IP mặc định là 192.168.0.1. Ta điền DNS 8.8.8.8 để Linksys cấp phát DHCP cho Client.

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 305, y: 698 Root 04:25:30

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name LabRadius Client IP 192.168.0.1

Secret chungthucradius ServerType Radius

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

Add Save Remove

User Setup

Username Password

| Username | Password |
|----------|----------|
|----------|----------|

Add Save Remove

WR300N Wireless Router0

Server-PT Server0

Time: 00:11:50

Realtime Simulation

PC Laptop Server Wireless Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired

Copper Straight-Through

12:32 am 08/03/2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 437, y: 0 Root 04:37:30

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name Client IP Secret ServerType Radius

| | Client Name | Client IP | Server Type | Key | |
|---|-------------|-------------|-------------|--------------|----------------|
| 1 | LabRadius | 192.168.0.1 | Radius | chungthuc... | <div>Add</div> |

Save

Remove

User Setup

Username Password

| Username | Password | |
|----------|----------|--|
|----------|----------|--|

Add

Save

Remove

Wireless Router0

Server-PT Server0

Time: 00:12:14

Realtime Simulation

PC Laptop Server Work Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired

Copper Straight-Through

0 New Delete PDU List

12:33 am 08/03/2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x 437, y: 0 Root 04:47:00

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

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

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name Client IP Secret ServerType Radius

| Client Name | Client IP | Server Type | Key |
|-------------|-------------|-------------|--------------|
| 1 LabRadius | 192.168.0.1 | Radius | chungthuc... |

Add Save Remove

User Setup

Username Password

| Username | Password |
|----------|-----------------|
| 1 radius | chungthucradius |

Add Save Remove

Wireless Router0

Server-PT Server0

Time: 00:12:33

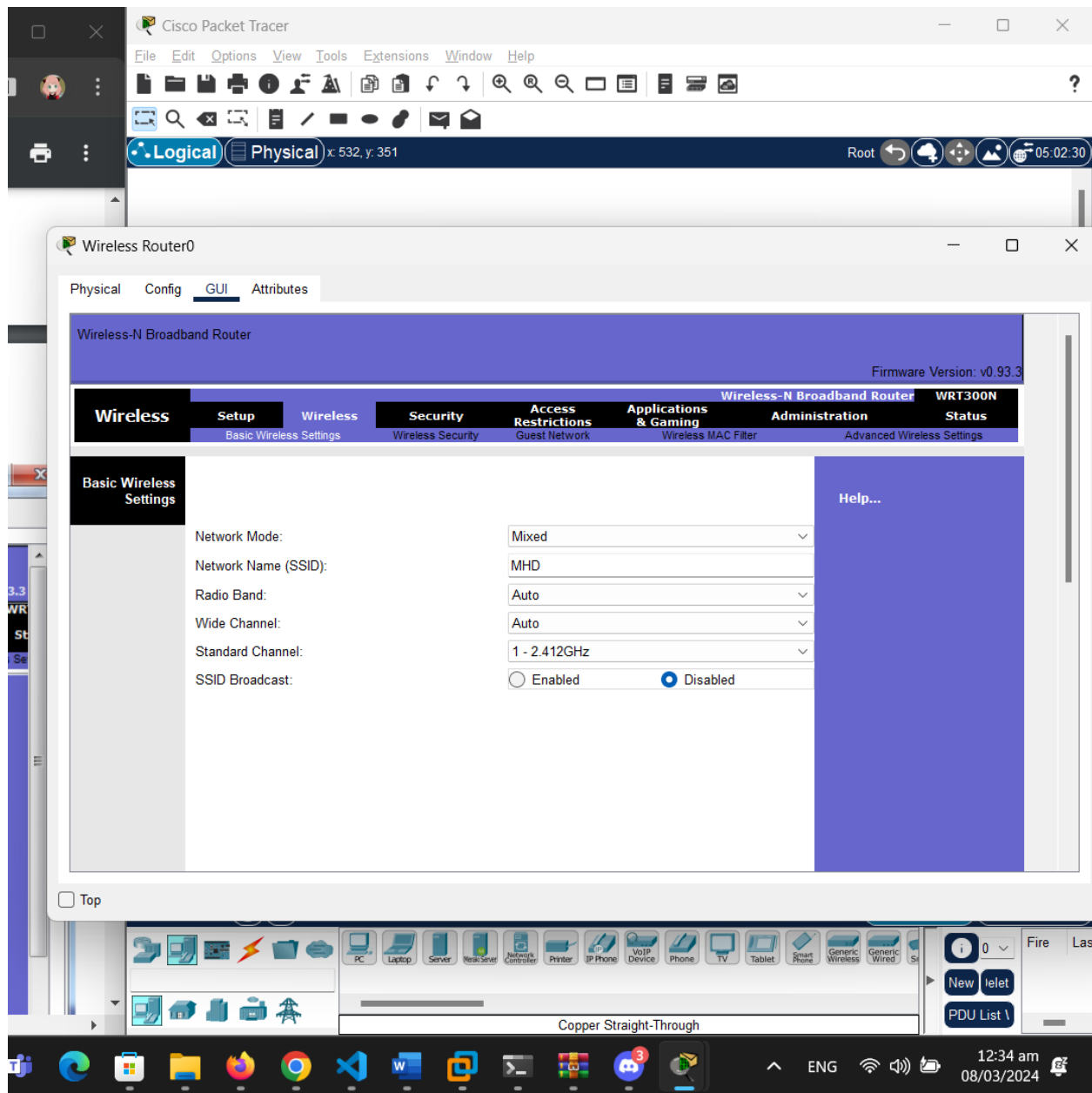
Realtime Simulation

PC Laptop Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired

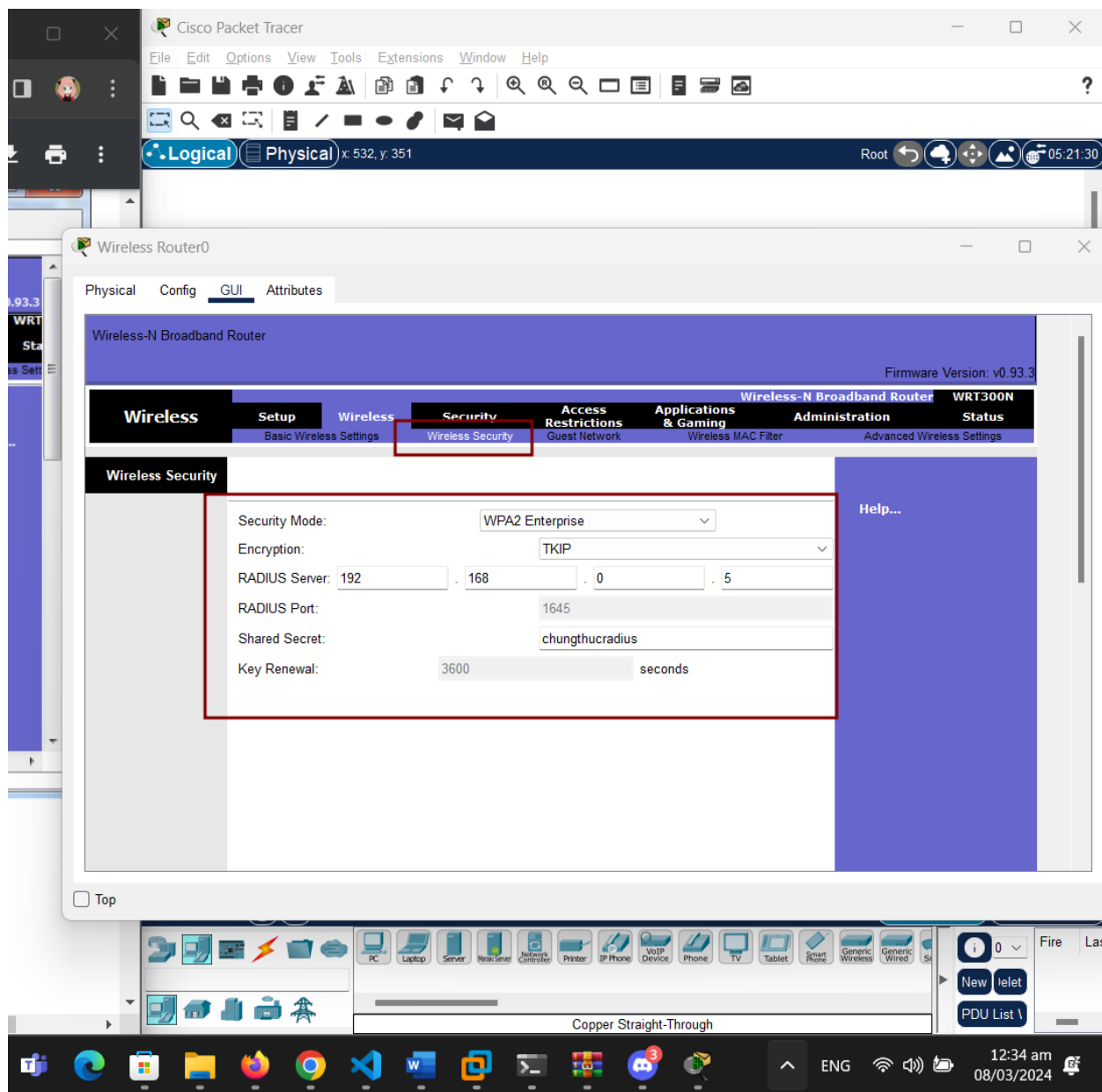
Copper Straight-Through

12:33 am 08/03/2024

Cấu hình Wireless cơ bản, tên mạng (SSID) là MHD, tắt tính năng quảng bá SSID (tắt rồi thì người dùng không còn thấy tên mạng nữa)



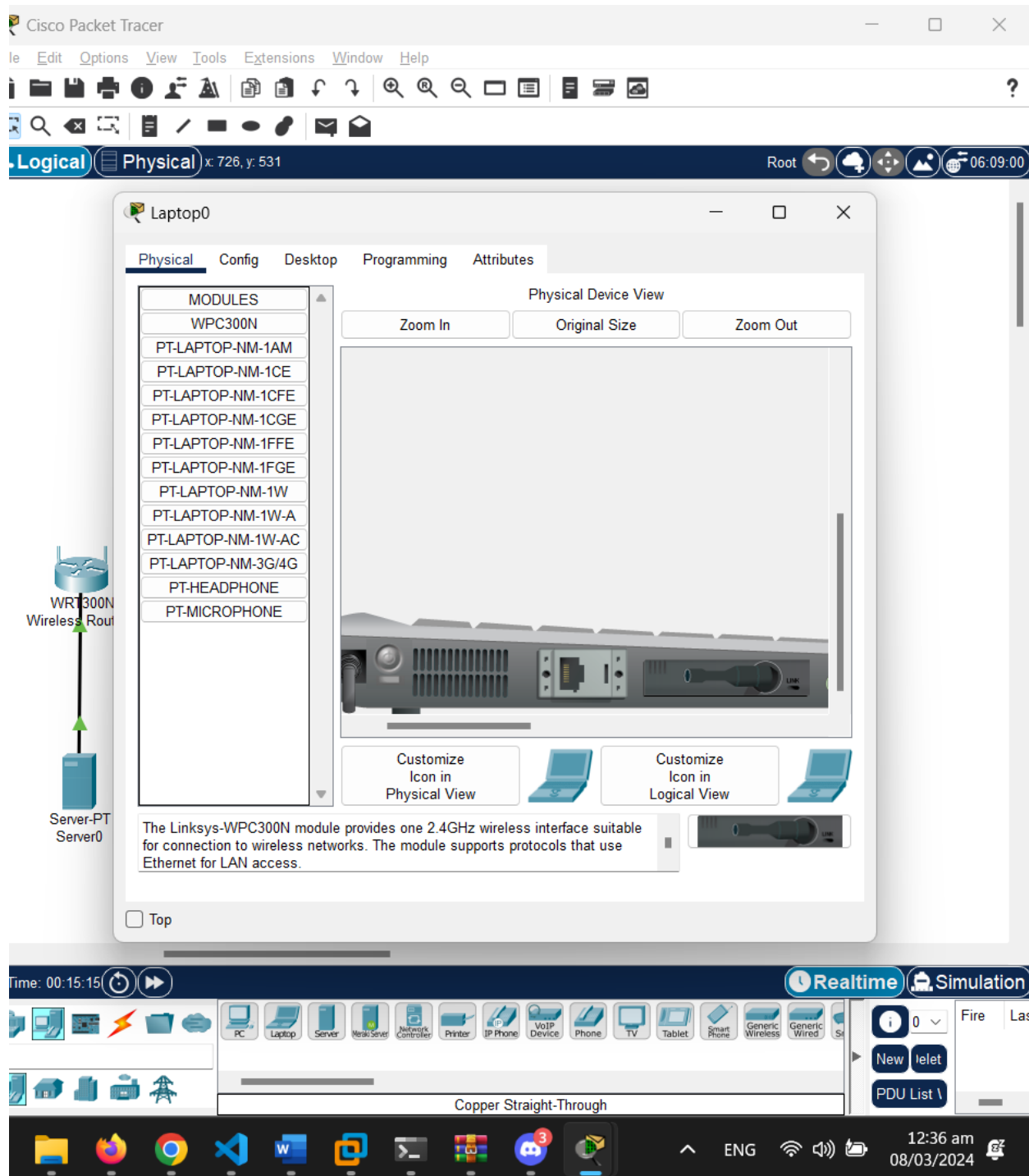
Cấu hình bảo mật cho Wireless, chọn Mode ở dạng Enterprise (doanh nghiệp lớn) sẽ thấy mục dành cho RADIUS. Nhập IP của RADIUS Server, chọn key để xác thực với RADIUS Server là chungthucradius. Encryption thì các bạn chọn TKIP cho dễ làm, ai thành công rồi thì hãy chọn AES (cái này là theo kinh nghiệm dùng Packet Tracer)



Mỗi lần chỉnh sửa gì ở Linksys, nhớ Save lại ngay trước khi sang bước mới.

IV, Bước 3 :

Trên Laptop, gỡ card LAN ra, lắp card Wifi vào, nhớ tắt nguồn trước khi gỡ, bật nguồn lại sau khi lắp



Vào tab Desktop, chọn PC Wireless, chọn Profiles sẽ thấy đang có sẵn 1 Profile tên là Default. Mọi người sửa thông tin trong Default cũng được, không thì tạo Profile mới. Chọn edit để sửa

Cisco Packet Tracer

FileEditOptionsViewToolsExtensionsWindowHelp

LogicalPhysical

x 724, y: 506

Root

07:03:00

Laptop0

PhysicalConfigDesktopProgrammingAttributes

Link InformationConnectProfiles

To connect to a network, select the profile name then click the **Connect** button. To create or edit a profile, use the menu bar at the bottom of the screen.

| Profile | Wireless Network Name |
|---------|-----------------------|
| Default | Default |

| Site Information | |
|------------------|----------------|
| Wireless Mode | Infrastructure |
| Wide Channel | Auto |
| Standard Channel | Auto |
| Security | Disable |
| Authentication | Auto |

Connect

2.4GHz

Adapter is Inactive

NewEditImportExportDelete

Wireless-N Notebook AdapterWireless Network Monitor v1.0Model No. WPC300N

Time: 00:17:03

RealtimeSimulation

0

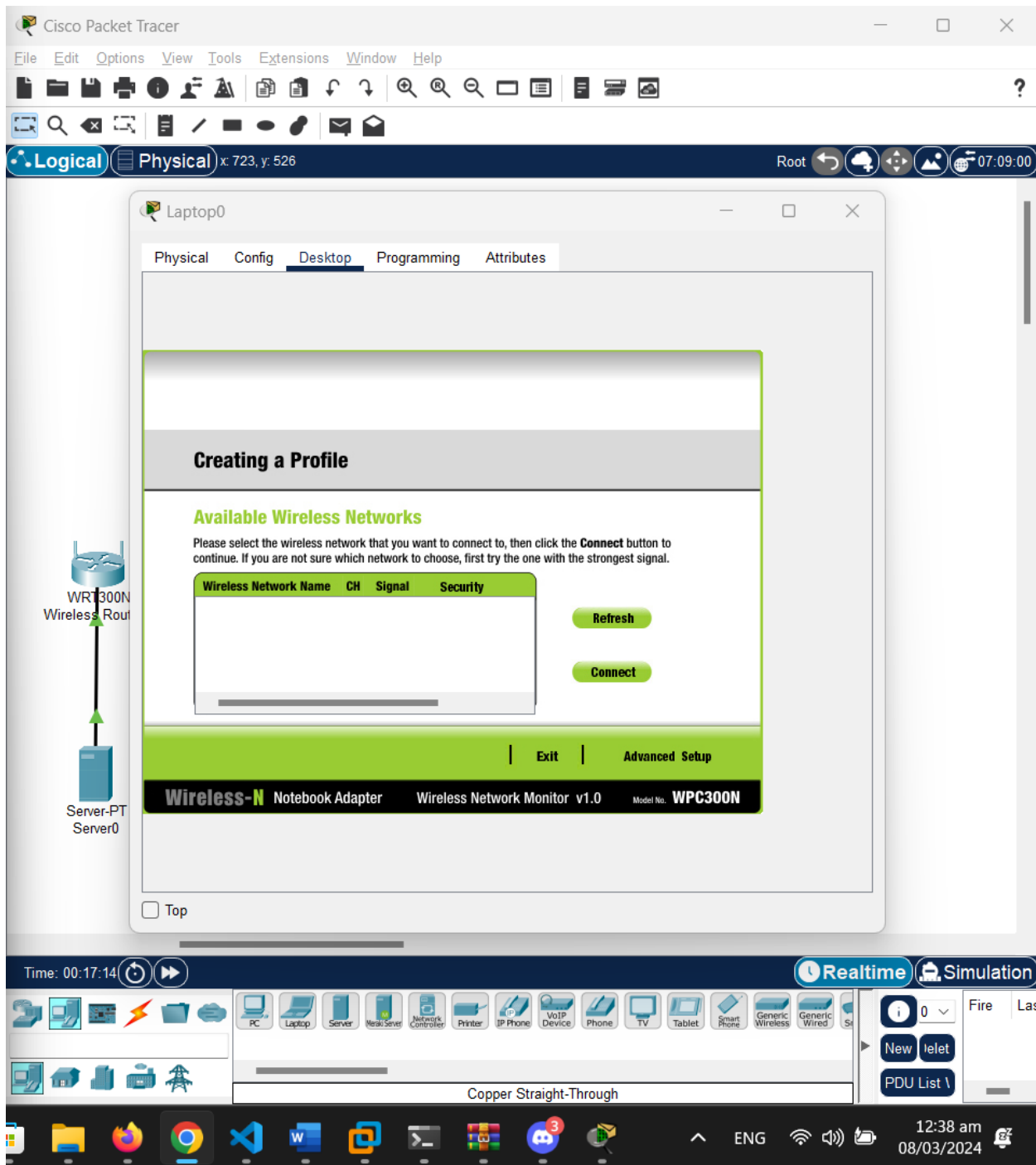
NewDelete

PDU List

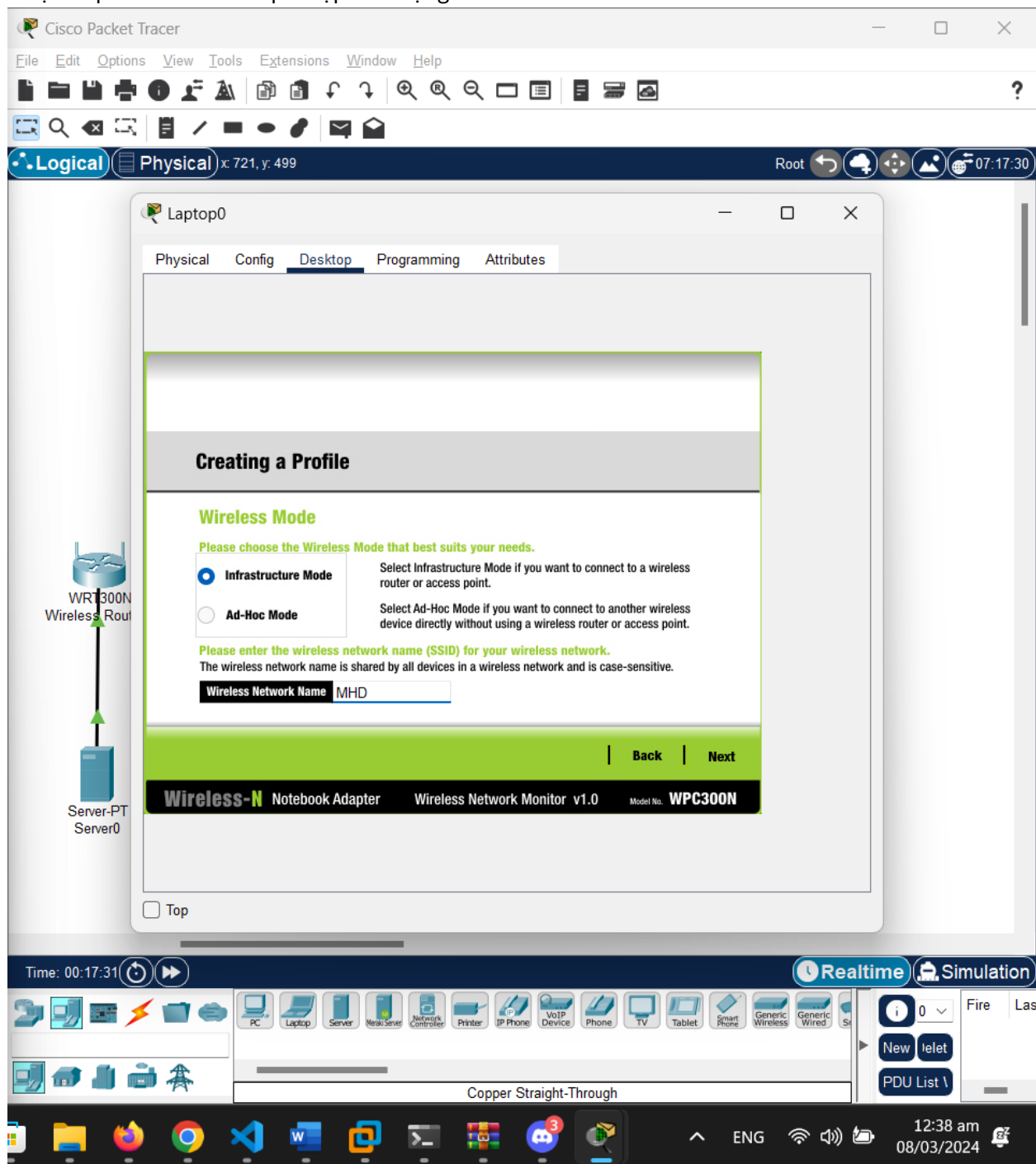
FireLas

Copper Straight-Through

12:38 am08/03/2024



Chọn tiếp Advanced Setup Nhập tên mạng là MHD



Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 628, y: 392 Root 07:28:00

Laptop0

Physical Config Desktop Programming Attributes

Creating a Profile

Network Settings

☒ Obtain network settings automatically (DHCP)
Select this option to have your network settings assigned automatically.

☐ Specify network settings
Select this option to specify the network settings for the adapter.

| | | | |
|-----------------|--|-------|--|
| IP Address | | DNS 1 | |
| Subnet Mask | | DNS 2 | |
| Default Gateway | | | |

Back Next

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

Top

WR300N Wireless Router

Server-PT Server0

Time: 00:17:52 Realtime Simulation

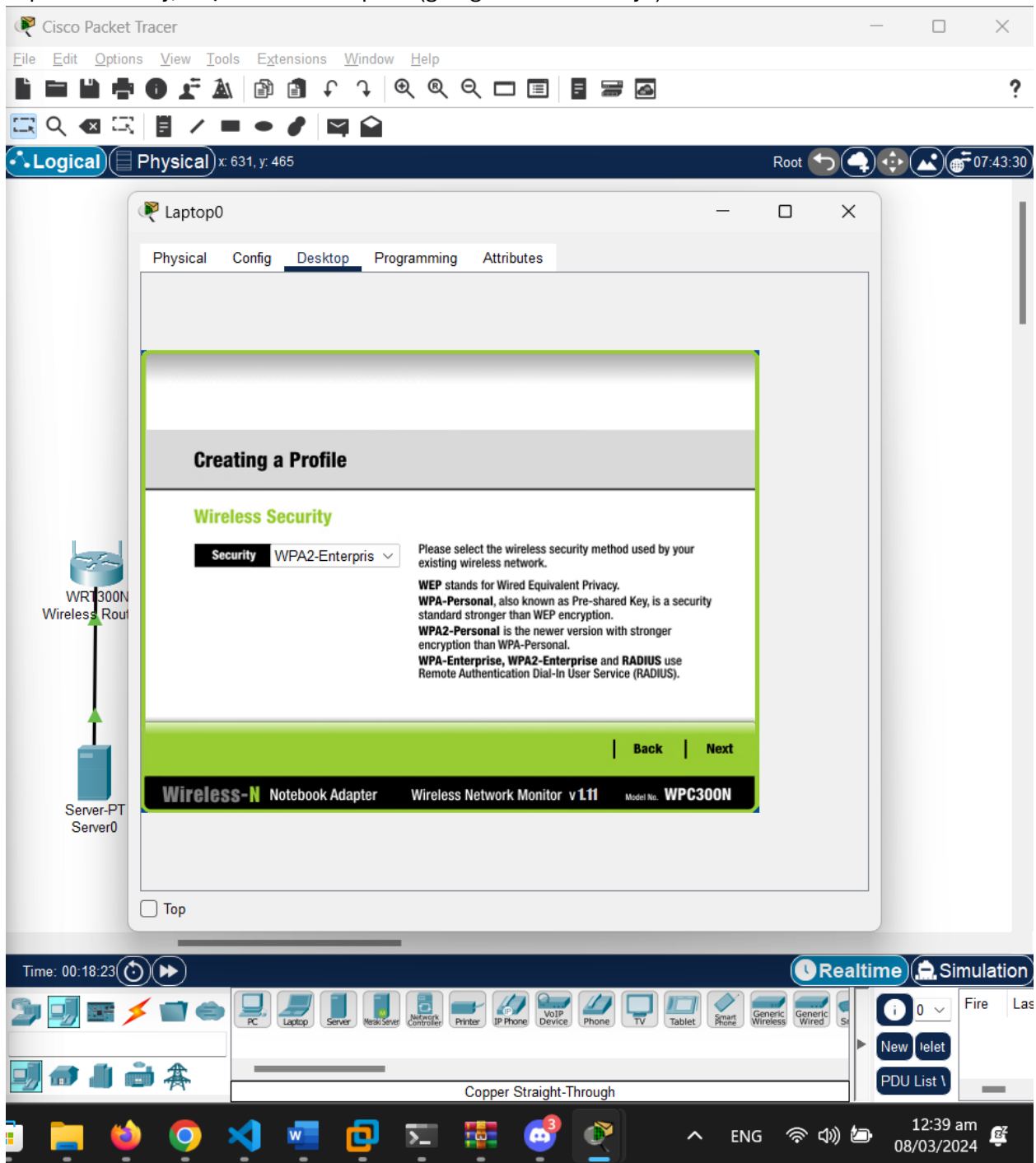
PC Laptop Server Wireless Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired Smart

Copper Straight-Through

New Delete PDU List

12:39 am 08/03/2024

Ở phần Security, chọn WPA2 Enterprise (giống như trên Linksys)



Nhập Username radius và pass chungthucradius đã tạo trên RADIUS Server

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 622, y: 366 Root 08:10:30

Laptop0

Physical Config Desktop Programming Attributes

Creating a Profile

Wireless Security - WPA2 Enterprise

| | | |
|----------------|------------|--|
| Authentication | PEAP | Please select the authentication method that you use to access your network. |
| Login Name | radius | Enter the Login Name used for authentication. |
| Password | •••••••••• | Enter the Password used for authentication. |
| Server Name | | Enter the Server Name used for authentication. (Optional) |
| Certificate | Trust Any | Please select the certificate used for authentication. |
| Inner Authen. | TOKEN CARD | Please select the inner authentication method used inside the PEAP tunnel. |

Back Next

Wireless-N Notebook Adapter Wireless Network Monitor v111 Model No. WPC300N

Top

Time: 00:19:17 Realtime Simulation

PC Laptop Server Wireless Router Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired

Copper Straight-Through

12:40 am 08/03/2024

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 622, y: 366 Root 08:18:30

Laptop0

Physical Config **Desktop** Programming Attributes

Confirm New Settings

| Profile Settings | | | |
|-----------------------|-----------------|-----------------|------|
| Wireless Network Name | MHD | IP Address | Auto |
| Wireless Mode | Infrastructure | Subnet Mask | Auto |
| Network Mode | Mixed Mode | Default Gateway | Auto |
| Radio Band | Auto | DNS1 | Auto |
| Wide Channel | Auto | DNS2 | |
| Standard Channel | Auto | | |
| Security | WPA2 Enterprise | | |
| Authentication | Auto | | |

Exit Back Save

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No. WPC300N

☐ Top

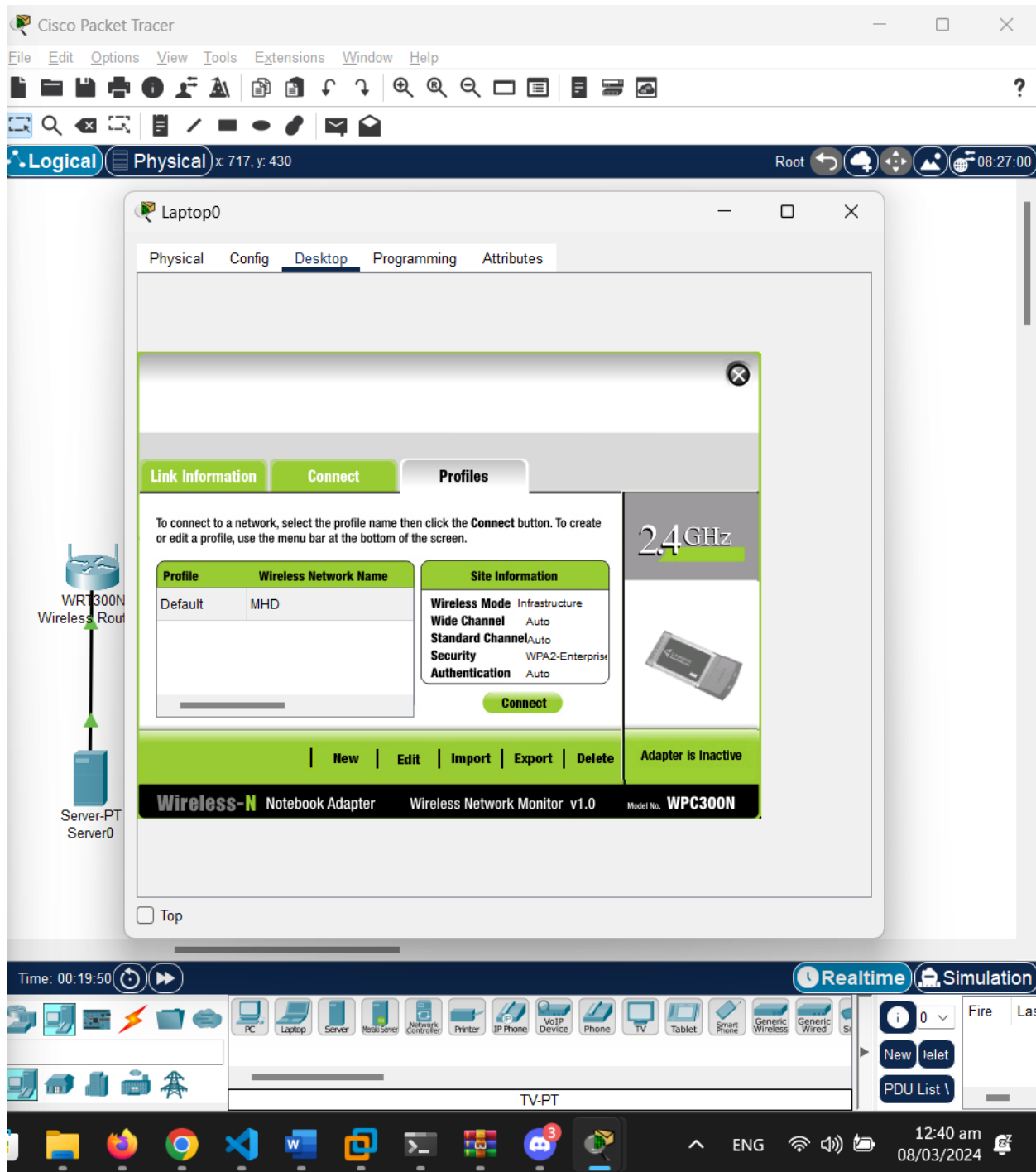
Time: 00:19:33 Realtime Simulation

PC Laptop Server Wireless Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired Smart Phone

Copper Straight-Through

0 New Delete PDU List

12:40 am 08/03/2024



Quay lại Profiles, xem lại các thông số đã đặt cho mạng MHD, và ấn Connect Để thành công, trên Laptop đang cấu hình vào tab Config, chọn mục Wireless. Tại mục Encryption chọn TKIP là xong.

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 629, y: 527 Root 09:15:00

Laptop0

Physical Config Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 11 Mbps

MAC Address 0005.5ED8.9594

SSID MHD

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☐ WPA2-PSK PSK Pass Phrase

☐ WPA ☒ WPA2 User ID radius

Password chungthucradius

☐ 802.1X Method: MD5

User Name

Password

Encryption Type TKIP

IP Configuration

☒ DHCP

☐ Static

IPv4 Address 169.254.149.148

Subnet Mask 255.255.0.0

IPv6 Configuration

☐ Automatic

Top

Time: 00:21:25 Realtime Simulation

PC Laptop Server Wireless Server Network Controller Printer IP Phone VoIP Device Phone TV Tablet Smart Phone Generic Wireless Generic Wired

Copper Straight-Through

12:42 am 08/03/2024