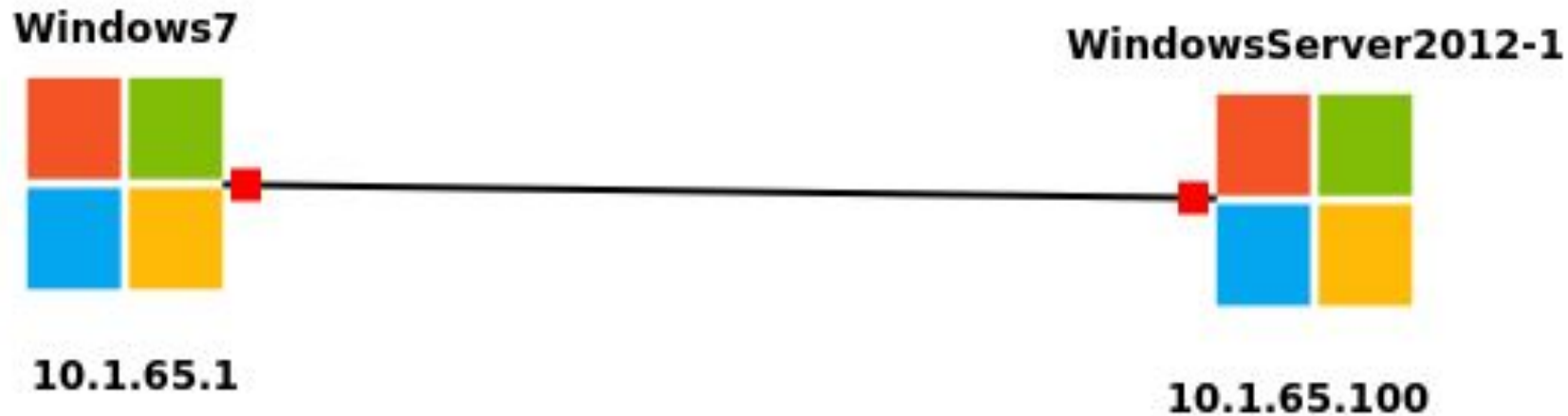


Triển khai giao thức telnet

- Ho tên: Nguyễn Văn Mạnh
- Lớp: AT12c
- Mã sinh viên: AT120336
- Email: nguyenmanh0397@gmail.com

I. Cài đặt

1. Sơ đồ mạng



2. Thêm một network vmnet2

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet IP Address
vmnet0	bridged	auto-bridging	—	—	—
vmnet1	host-only	none	vmnet1	yes	192.168.160.0
vmnet2	host-only	none	vmnet2	yes	10.1.65.0
vmnet3	host-only	none	vmnet3	no	172.16.1.0
vmnet4	host-only	none	vmnet4	yes	10.10.10.0
vmnet5	host-only	none	vmnet5	yes	172.16.10.0
vmnet8	NAT	NAT	vmnet8	yes	192.168.244.0

Add Network...

Remove Network

vmnet2

Bridged (connect VMs directly to the external network)

Bridged to: AutomaticAutomatic Settings...

NAT (share host's IP address with VMs)

NAT Settings...

Host-only (connect VMs internally in a private network)

Use local DHCP service to distribute IP addresses to VMs

Connect a host virtual adapter (vmnet2) to this network

Subnet IP: 10 . 1 . 65 . 0Subnet mask: 255.255.255. 0

Leave blank to automatically select an unused subnet IP.

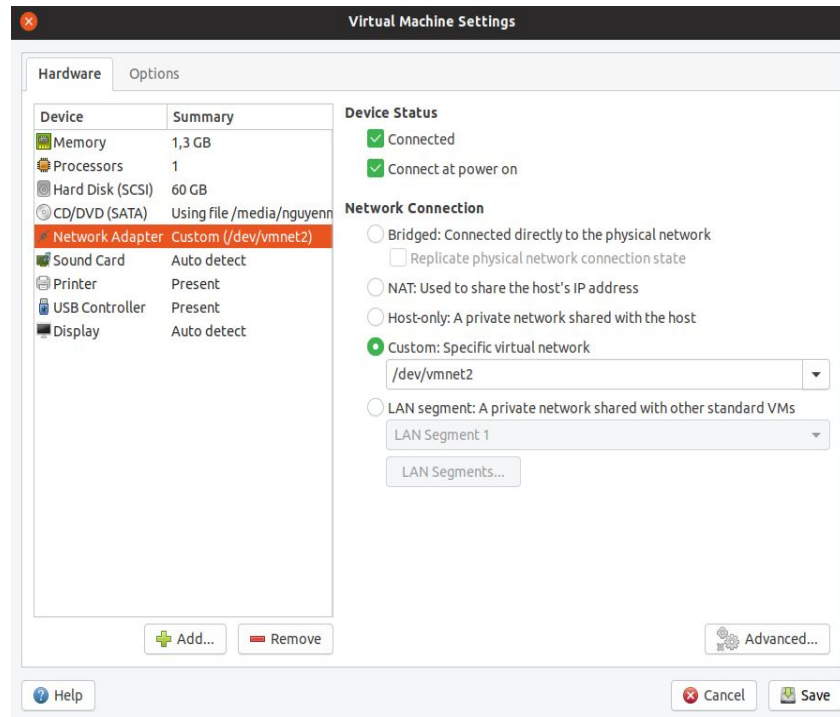
Help

Cancel

Save

3. Cài đặt network adapter

- Window 7 với cắm vào vmnet2
- Window server 12 cắm vào vmnet 2



4. Đặt địa chỉ ip tĩnh cho client và server

Client

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 1 . 65 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 1 . 65 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Server

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 10 . 1 . 65 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

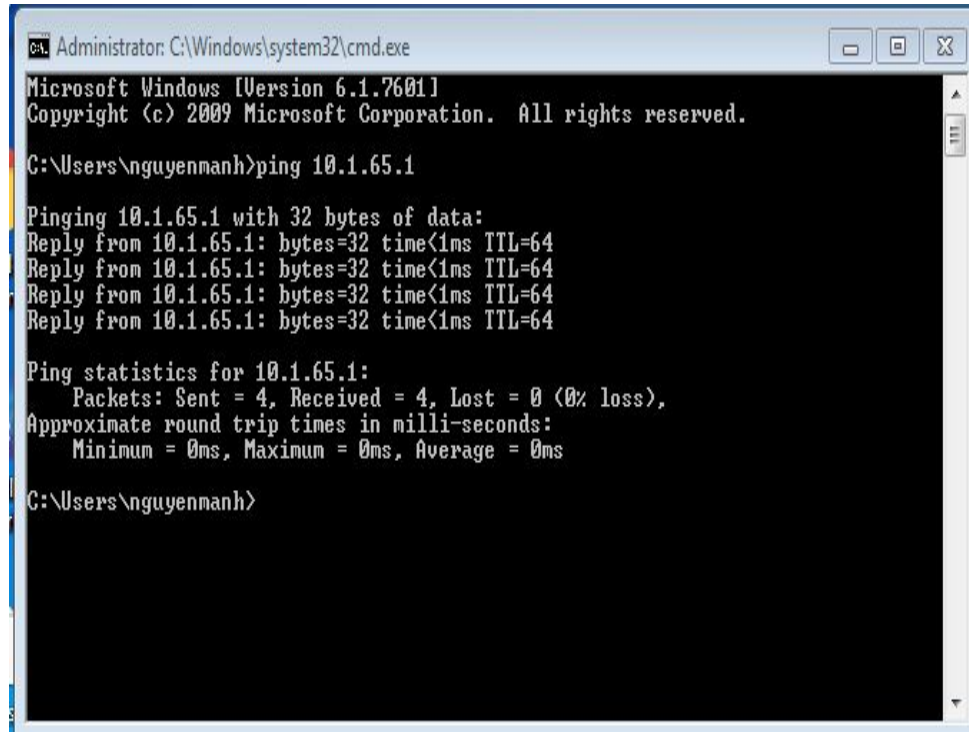
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

5. Kiểm tra ping 2 máy



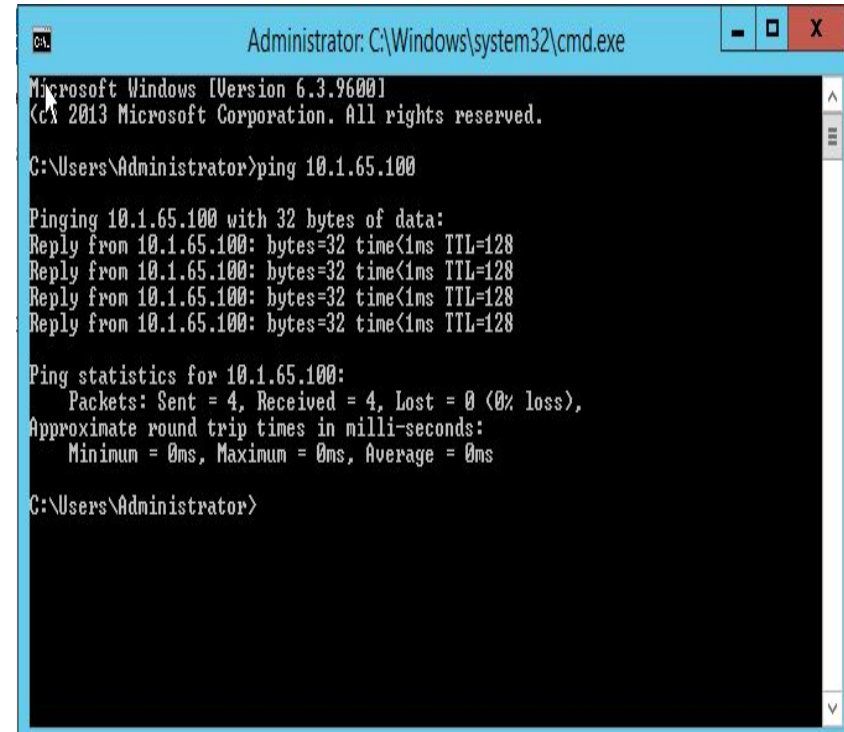
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\nguyenmanh>ping 10.1.65.1

Pinging 10.1.65.1 with 32 bytes of data:
Reply from 10.1.65.1: bytes=32 time<1ms TTL=64
Reply from 10.1.65.1: bytes=32 time<1ms TTL=64
Reply from 10.1.65.1: bytes=32 time<1ms TTL=64
Reply from 10.1.65.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.65.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\nguyenmanh>
```



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
Copyright (c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 10.1.65.100

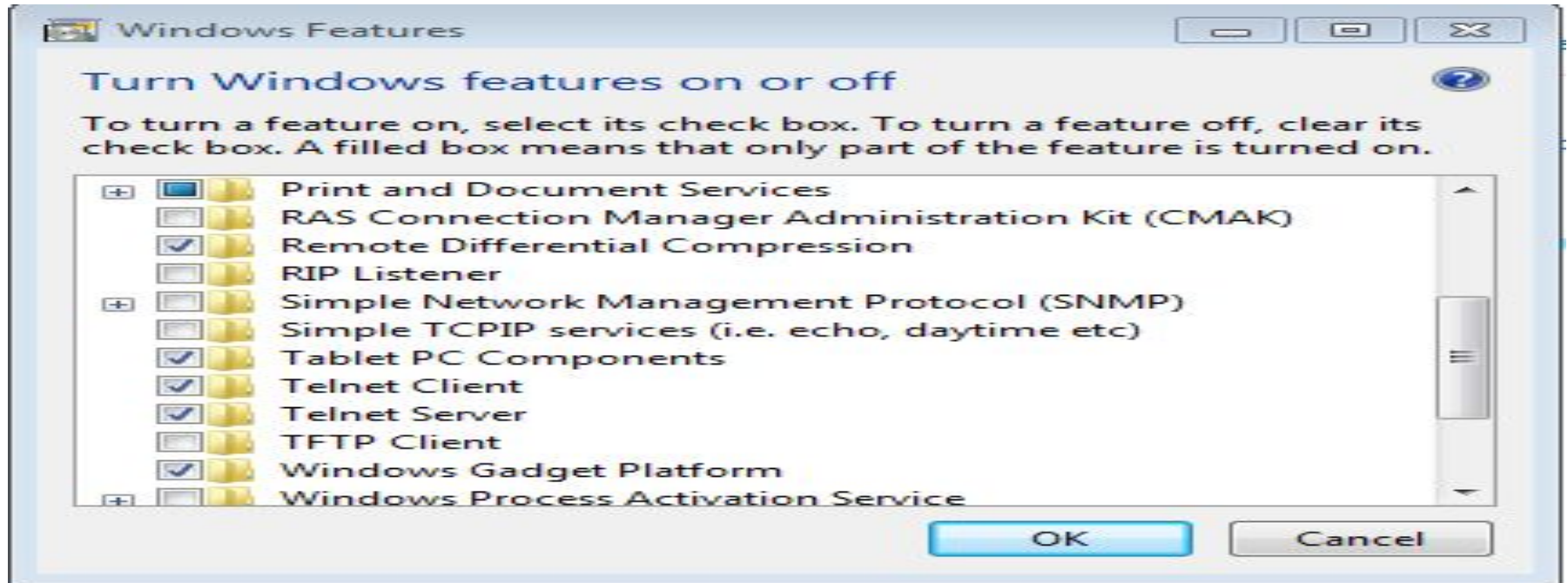
Pinging 10.1.65.100 with 32 bytes of data:
Reply from 10.1.65.100: bytes=32 time<1ms TTL=128
Reply from 10.1.65.100: bytes=32 time<1ms TTL=128
Reply from 10.1.65.100: bytes=32 time<1ms TTL=128
Reply from 10.1.65.100: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.65.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

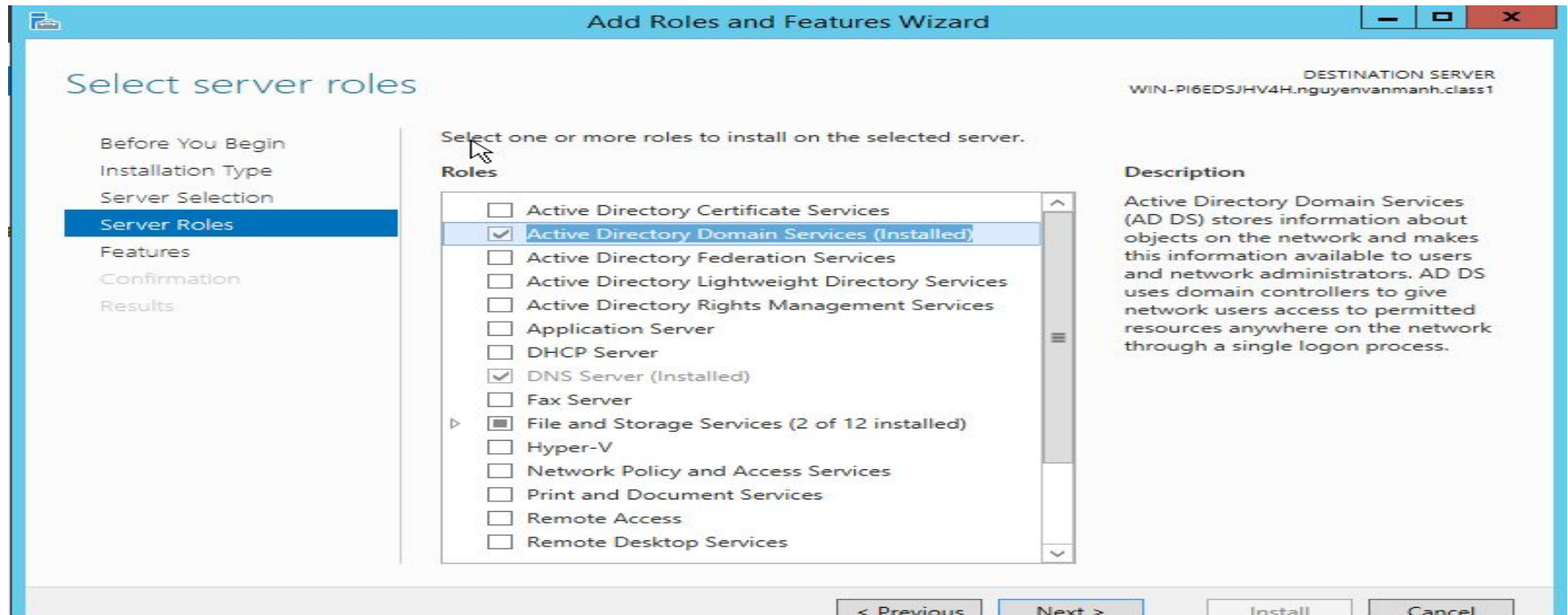
6. Khởi động dịch vụ telnet trên client

Control Panel -> Programs -> Turn Windows features on or off



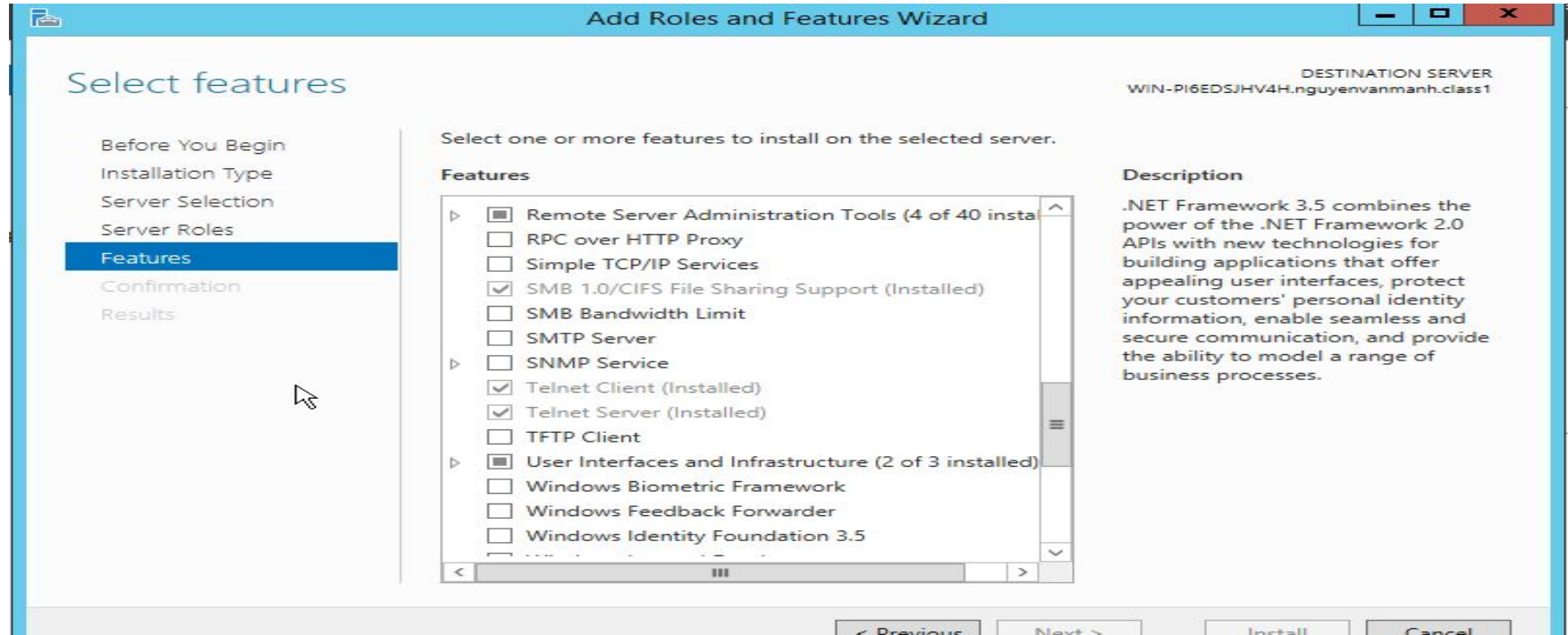
7. Khởi động dịch vụ telnet trên server

Cài đặt Active directory domain services



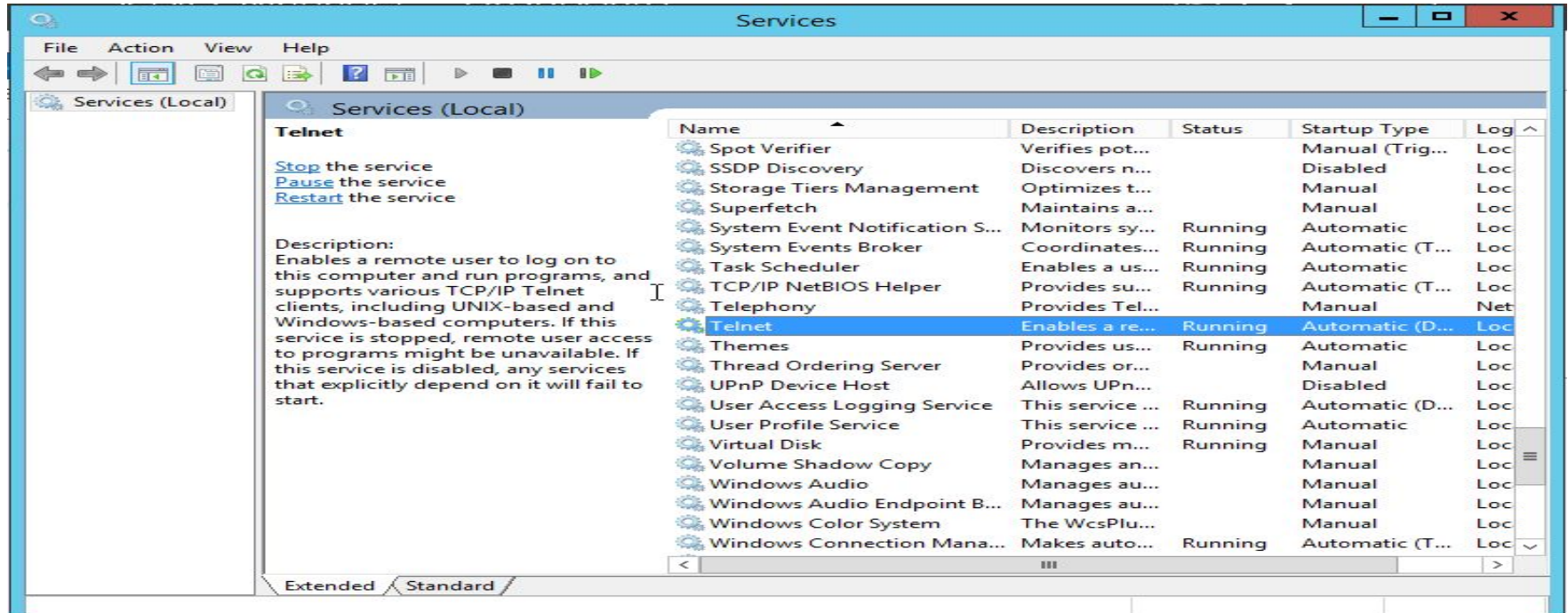
9. Khởi động dịch vụ telnet trên server

Cài đặt Telnet Client và Server sau đó Install



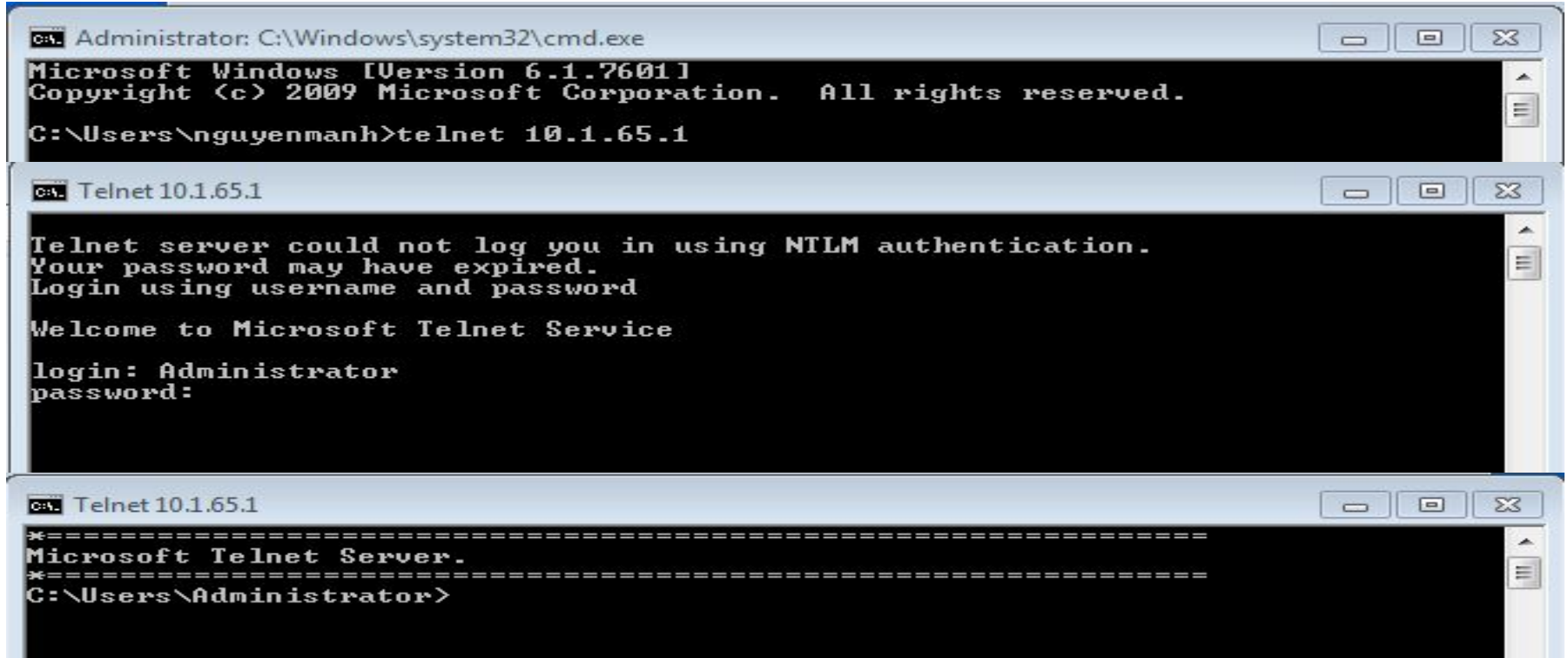
10. Khởi động dịch vụ telnet trên server

Khởi động telnet tại services



II. Tiến hành telnet

1. Thực hiện telnet từ client vào server



```
C:\> Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\nguyenmanh>telnet 10.1.65.1

C:\> Telnet 10.1.65.1

Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

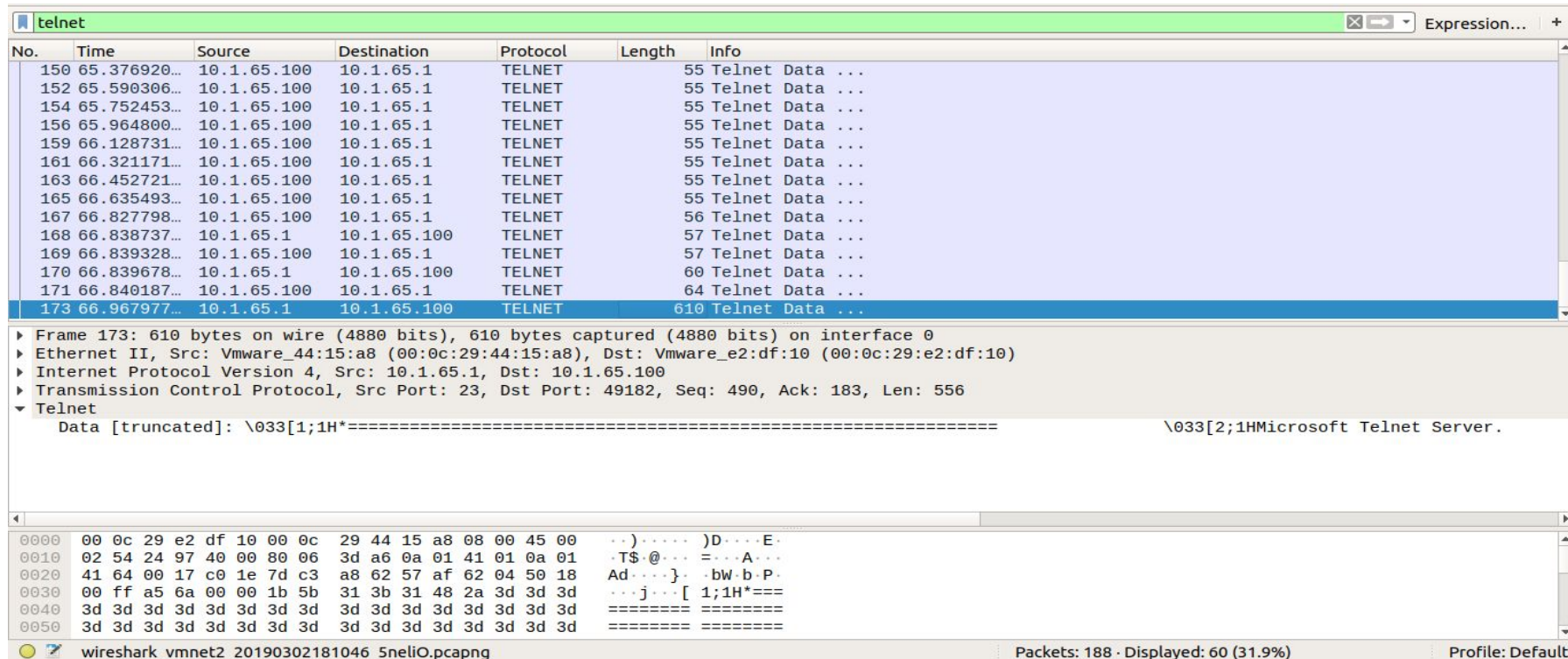
Welcome to Microsoft Telnet Service

login: Administrator
password:

C:\> Telnet 10.1.65.1

=====
Microsoft Telnet Server.
=====
C:\Users\Administrator>
```

2. Trên wireshark bắt gói tin telnet



Wireshark packet capture showing Telnet traffic. The packet list displays several Telnet packets from source 10.1.65.100 to destination 10.1.65.1. Packet 173 is selected, showing details of the Telnet connection establishment.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
150	65.376920...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
152	65.590306...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
154	65.752453...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
156	65.964800...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
159	66.128731...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
161	66.321171...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
163	66.452721...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
165	66.635493...	10.1.65.100	10.1.65.1	TELNET	55	Telnet Data ...
167	66.827798...	10.1.65.100	10.1.65.1	TELNET	56	Telnet Data ...
168	66.838737...	10.1.65.1	10.1.65.100	TELNET	57	Telnet Data ...
169	66.839328...	10.1.65.100	10.1.65.1	TELNET	57	Telnet Data ...
170	66.839678...	10.1.65.1	10.1.65.100	TELNET	60	Telnet Data ...
171	66.840187...	10.1.65.100	10.1.65.1	TELNET	64	Telnet Data ...
173	66.967977...	10.1.65.1	10.1.65.100	TELNET	610	Telnet Data ...

Packet Details (Frame 173):

- Frame 173: 610 bytes on wire (4880 bits), 610 bytes captured (4880 bits) on interface 0
- Ethernet II, Src: Vmware_44:15:a8 (00:0c:29:44:15:a8), Dst: Vmware_e2:df:10 (00:0c:29:e2:df:10)
- Internet Protocol Version 4, Src: 10.1.65.1, Dst: 10.1.65.100
- Transmission Control Protocol, Src Port: 23, Dst Port: 49182, Seq: 490, Ack: 183, Len: 556
- Telnet
 - Data [truncated]: \033[1;1H*===== \033[2;1HMicrosoft Telnet Server.

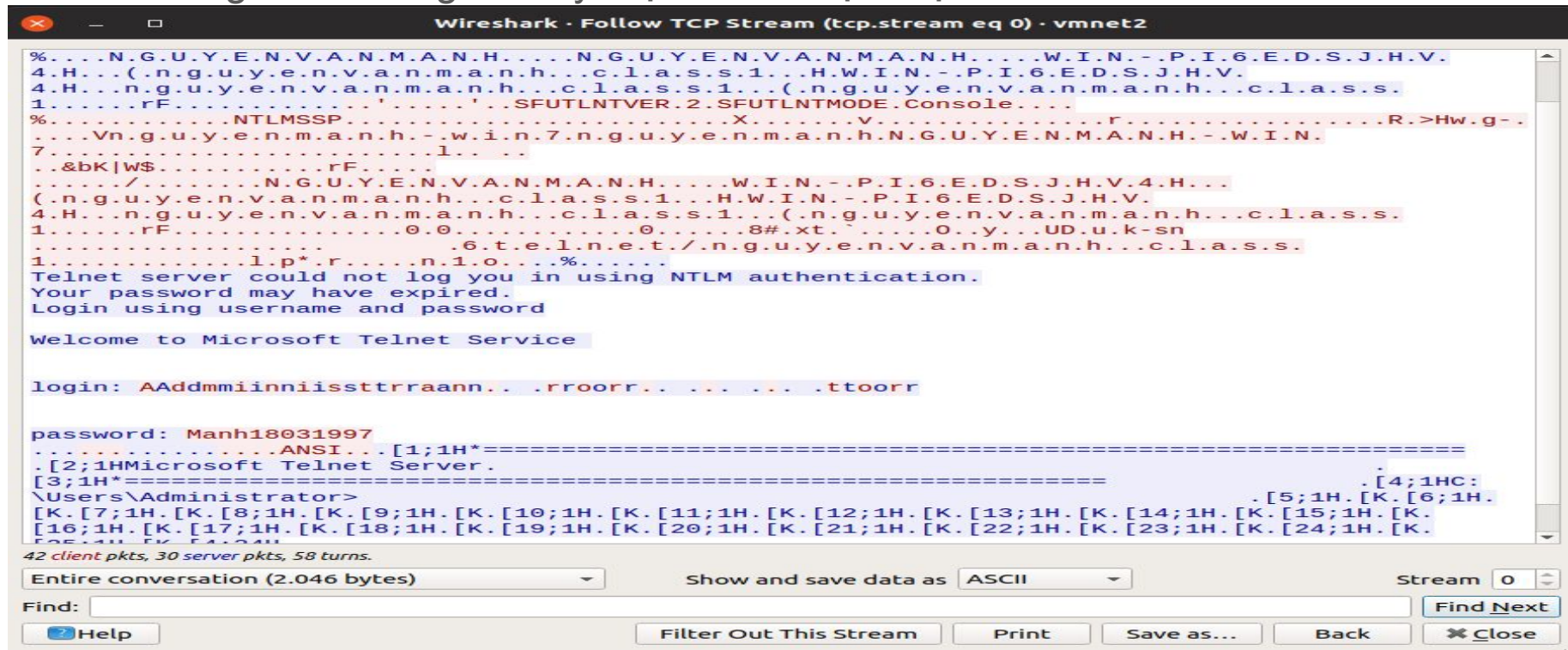
Packet Bytes:

Offset	Hex	ASCII
0000	00 0c 29 e2 df 10 00 0c 29 44 15 a8 08 00 45 00	..).D...E..
0010	02 54 24 97 40 00 80 06 3d a6 0a 01 41 01 0a 01	.T\$.@...=...A..
0020	41 64 00 17 c0 1e 7d c3 a8 62 57 af 62 04 50 18	Ad...}.bW.b.P.
0030	00 ff a5 6a 00 00 1b 5b 31 3b 31 48 2a 3d 3d 3d	...j...[1;1H*===
0040	3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d	=====
0050	3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d	=====

Wireshark vmnet2_20190302181046_5neliO.pcapng Packets: 188 - Displayed: 60 (31.9%) Profile: Default

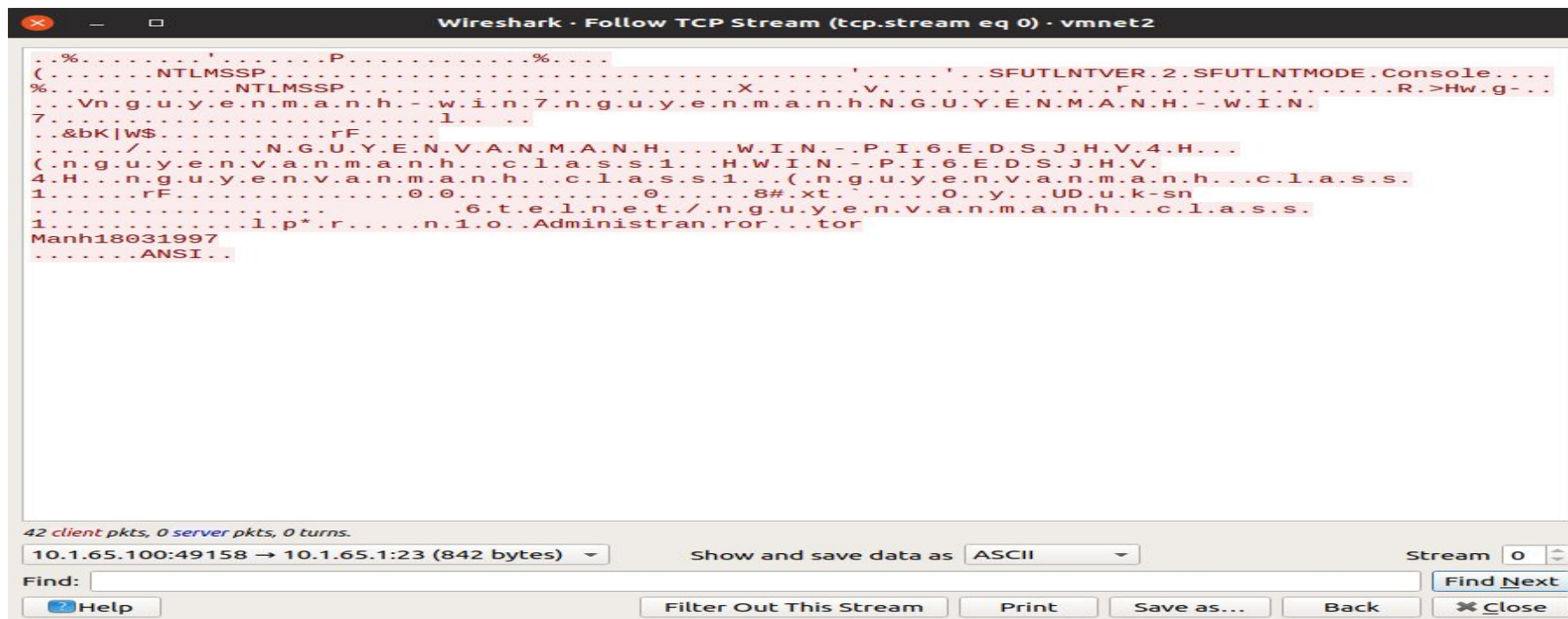
3. Phân tích luồng tcp

Phân tích gói tin chúng ta thấy mật khẩu được hiện ở bản rõ.



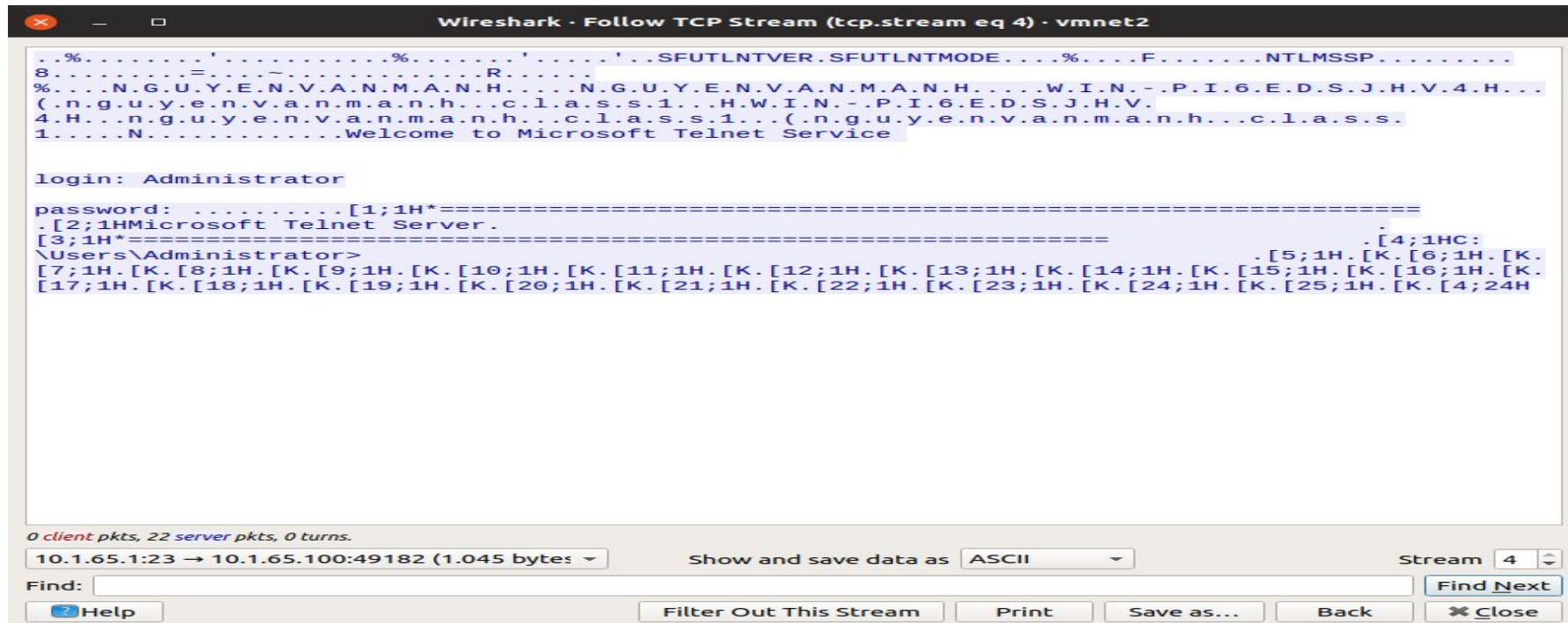
Phân tích luồng tcp

Luồng dữ liệu từ client (window 7) vào server (window server 2012)



Phân tích luồng tcp

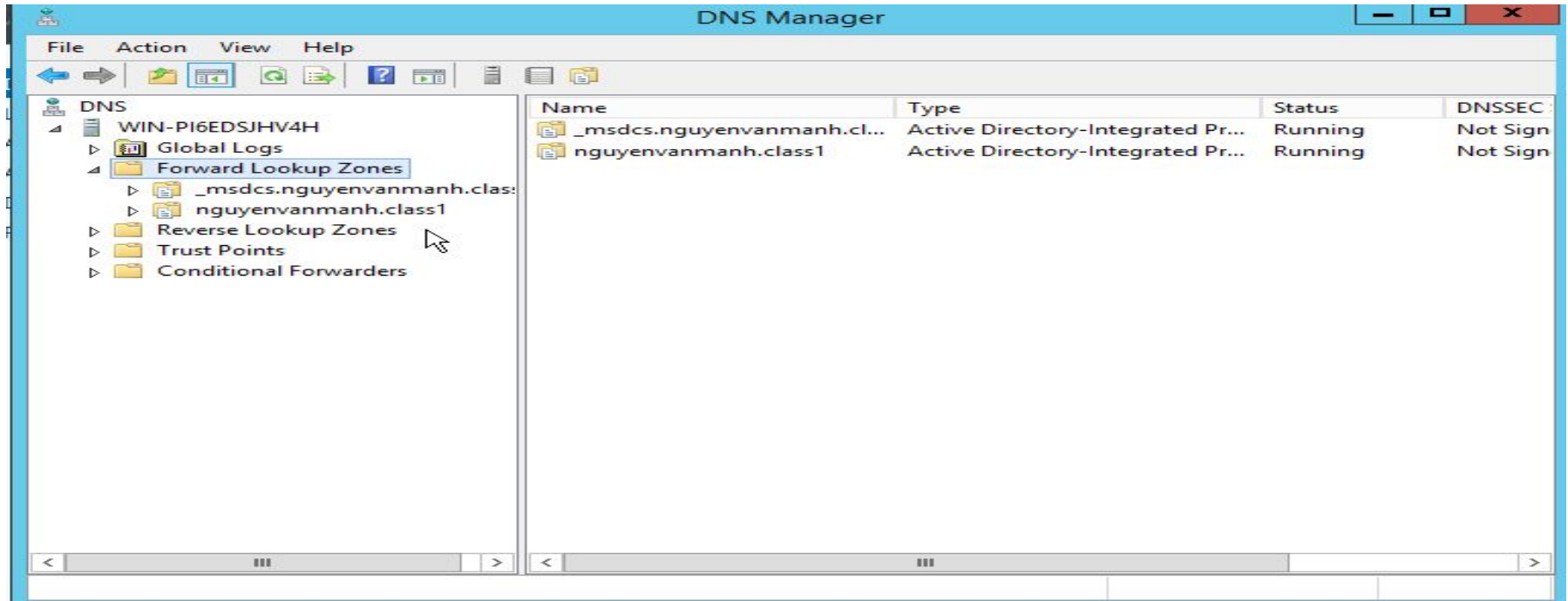
Luồng dữ liệu từ server (window server 2012) vào client (window 7)



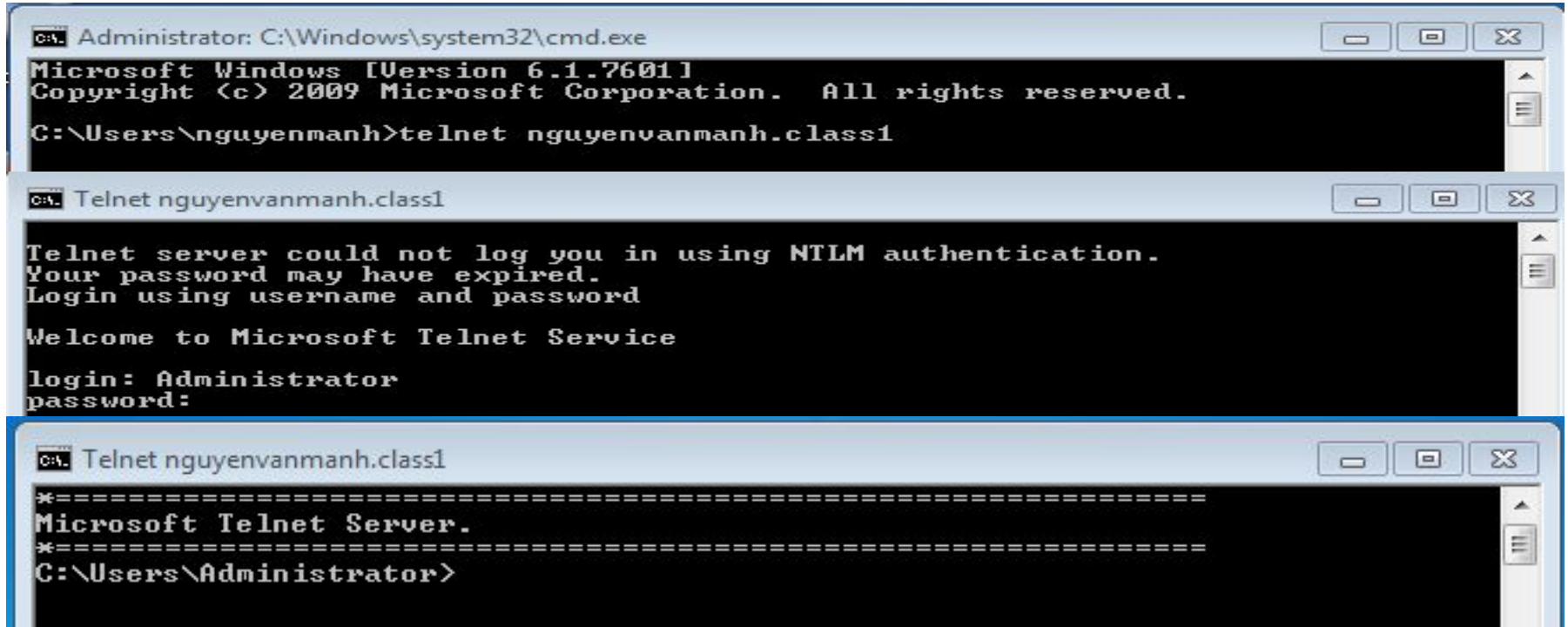
III. Thiết lập telnet với domain

1. Thiết lập domain cho máy chủ

Server Manager -> Tool -> DNS -> Forward Lookup Zone -> New Zone



2. Telnet từ client vào server bằng domain



The image displays three sequential screenshots of Windows command prompt windows, illustrating the steps to telnet from a client to a server using domain authentication.

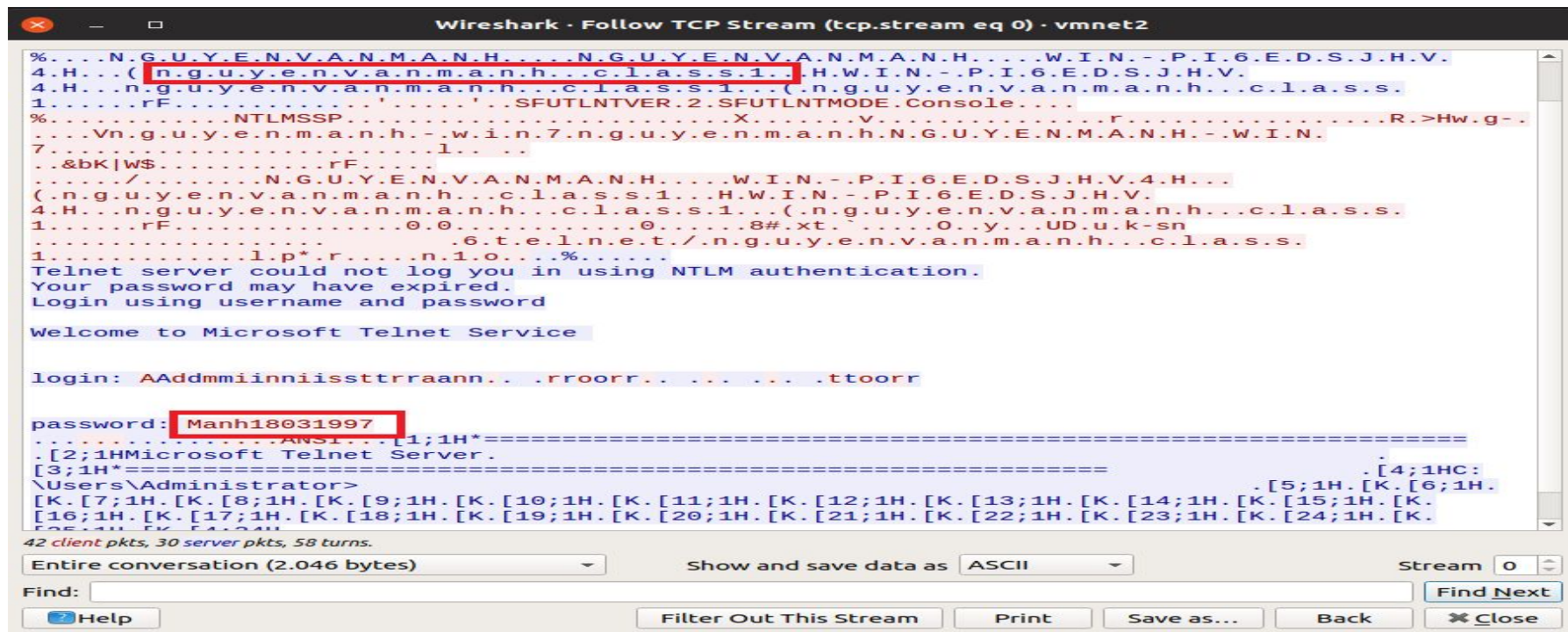
Window 1: Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\nguyenmanh>telnet nguyenvanmanh.class1

Window 2: Telnet nguyenvanmanh.class1
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password
Welcome to Microsoft Telnet Service
login: Administrator
password:

Window 3: Telnet nguyenvanmanh.class1
=====
Microsoft Telnet Server.
=====
C:\Users\Administrator>

3. Phân tích gói tin

Mật khẩu vẫn được hiển thị ở dạng bản rõ.



Phân tích gói tin

Gói tin gửi từ window 7 sang window server 2012



Phân tích gói tin

Gói tin gửi từ window server 2012 sang window 7

The image shows a Wireshark packet capture window titled "Wireshark - Follow TCP Stream (tcp.stream eq 4) - vmnet2". The packet list on the left shows a single packet (No. 1) of type "Telnet" from 10.1.65.1:23 to 10.1.65.100:49182. The packet details pane shows the "Raw" data of the packet, which is a Telnet session. The session starts with a "Welcome to Microsoft Telnet Service" message, followed by a login prompt "login: Administrator". The user enters the password "Administrator", and the server responds with a confirmation message. The session then ends with a "Disconnect" message.

```
..%.....'.....%.....'.....'..SFUTLNTVER.SFUTLNTMODE....%....F.....NTLMSSP.....  
8.....=.....~.....R.....  
%.....N.G.U.Y.E.N.V.A.N.M.A.N.H.....N.G.U.Y.E.N.V.A.N.M.A.N.H.....W.I.N.-.P.I.6.E.D.S.J.H.V.4.H...  
(.n.g.u.y.e.n.v.a.n.m.a.n.h...c.l.a.s.s.1...H.W.I.N.-.P.I.6.E.D.S.J.H.V.  
4.H...n.g.u.y.e.n.v.a.n.m.a.n.h...c.l.a.s.s.1...(n.g.u.y.e.n.v.a.n.m.a.n.h...c.l.a.s.s.  
1.....N.....Welcome to Microsoft Telnet Service  
  
login: Administrator  
  
password: .....[1;1H*=====.  
.[2;1HMicrosoft Telnet Server.  
[3;1H*=====.[4;1HC:  
\Users\Administrator>.[5;1H.[K.[6;1H.[K.  
[7;1H.[K.[8;1H.[K.[9;1H.[K.[10;1H.[K.[11;1H.[K.[12;1H.[K.[13;1H.[K.[14;1H.[K.[15;1H.[K.[16;1H.[K.  
[17;1H.[K.[18;1H.[K.[19;1H.[K.[20;1H.[K.[21;1H.[K.[22;1H.[K.[23;1H.[K.[24;1H.[K.[25;1H.[K.[4;24H
```

0 client pkts, 22 server pkts, 0 turns.

10.1.65.1:23 → 10.1.65.100:49182 (1.045 bytes) Show and save data as ASCII Stream 4

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close