ỦY BAN NHÂN DÂN THÀNH PHỐ THỦ ĐỨC

**TRƯỜNG TRUNG CẤP ĐÔNG SÀI GÒN**

-----🙞🙜 🕮 🙞🙜-----



:

**TÀI LIỆU GIẢNG DẠY**

**HỆ ĐIỀU HÀNH CLIENT/SERVER**

**NGHỀ: QUẢN TRỊ MẠNG MÁY TÍNH**

**TRÌNH ĐỘ: TRUNG CẤP**

*(Ban hành theo Quyết định số: /QĐ-ĐSG ngày tháng năm 2023 của HIệu trưởng trường trung cấp ĐÔng Sài Gòn)*

[j0195384](http://images.google.com.vn/imgres?imgurl=http://img143.imageshack.us/img143/7847/ie7we1.jpg&imgrefurl=http://my.opera.com/forevermyweb/blog/show.dml/1993273&usg=__03V2klnQOGWgJljlmxJj_WVl9nA=&h=227&w=224&sz=19&hl=vi&start=141&tbnid=G3guPn1pxKqNhM:&tbnh=108&tbnw=107&prev=/images%3Fq%3Ddownload%2Bhinh%2Banh%2BIE%26gbv%3D2%26ndsp%3D18%26hl%3Dvi%26sa%3DN%26start%3D126)

**NĂM 2023**

**MỤC LỤC**

[1 Triển khai địa chỉ Ipv4 12](#_Toc97039929)

[2 Sử dụng phần mềm VMWare và Cài đặt Windows Server 2016 18](#_Toc97039930)

[3 Dịch vụ DNS 24](#_Toc97039931)

[4 Routing and Remote Access 33](#_Toc97039932)

[5 Dịch vụ DHCP 38](#_Toc97039933)

[6 Dịch vụ Web 52](#_Toc97039934)

[7 Dịch vụ FTP 61](#_Toc97039935)

[8 Dịch vụ NAT 66](#_Toc97039936)

[9 Windows Deployment service (WDS) 71](#_Toc97039937)

[10 Lưu trữ cục bộ tránh trùng lắp dữ liệu 86](#_Toc97039938)

[11 Dịch vụ VPN 88](#_Toc97039939)

[12 Triển khai hệ thống Domain 108](#_Toc97039940)

DANH MỤC CÁC HÌNH

Hình Trang

[Hình 2-1: Các card Vmnet trong máy ảo 18](#_bookmark2)

[Hình 2-2: Địa chỉ IP của máy thật 19](#_bookmark3)

[Hình 2-3: Địa chỉ IP của máy ảo 19](#_bookmark4)

[Hình 2-4: Địa chỉ IP máy thật 20](#_bookmark5)

[Hình 2-5: Địa chỉ IP máy ảo 20](#_bookmark6)

[Hình 2-6: Network của máy ảo 21](#_bookmark7)

[Hình 2-7: Card Vmnet 1 trong máy thật 21](#_bookmark8)

[Hình 2-8: Tạo Snapshot cho máy ảo 22](#_bookmark9)

[Hình 2-9: Giao diện cài windows Server 2016 22](#_bookmark10)

[Hình 2-10: Cấu hình ổ đĩa 23](#_bookmark11)

[Hình 2-11: Quá trình cài đặt 23](#_bookmark12)

[Hình 2-12: Yêu cầu đặt Password 23](#_bookmark13)

[Hình 3-1: Cài Role DNS Server 25](#_bookmark15)

[Hình 3-2: Tạo Zone mới 25](#_bookmark16)

[Hình 3-3: Đặt tên cho zone là newstar.vn 26](#_bookmark17)

[Hình 3-4: Tạo Reverse lookup zone 26](#_bookmark18)

[Hình 3-5: Lựa chọn phương thức Update 27](#_bookmark19)

[Hình 3-6: Tạo new host 27](#_bookmark20)

[Hình 3-7: Tạo Alias 28](#_bookmark21)

[Hình 3-8: kết quả phân giải tên miền thành công 28](#_bookmark22)

[Hình 3-9: Cấu hình DNS Secondary 30](#_bookmark23)

[Hình 3-10: Chọn Master DNS 30](#_bookmark24)

[Hình 3-11: Chọn Server để đồng bộ DNS 31](#_bookmark25)

[Hình 3-12: Chọn phương thức để đồng bộ 31](#_bookmark26)

[Hình 3-13: Quá trình đồng bộ đã xong 32](#_bookmark27)

[Hình 4-1: Cài dịch vụ Routing 33](#_bookmark29)

[Hình 4-2: Cấu hình Routing and Remote Access 34](#_bookmark30)

[Hình 4-3: Tạo New Route 34](#_bookmark31)

[Hình 4-4: Cấu hình định tuyến tĩnh 35](#_bookmark32)

[Hình 4-5: Kiểm tra kết nối 35](#_bookmark33)

[Hình 4-6: Cấu hình định tuyến động 36](#_bookmark34)

[Hình 4-7: Thêm Interface vào định tuyến 36](#_bookmark35)

[Hình 4-8: Kiểm tra kết quả 37](#_bookmark36)

[Hình 5-1: Cài dịch vụ DHCP 39](#_bookmark38)

[Hình 5-2: Cấu hình Scope 39](#_bookmark39)

[Hình 5-3: Đặt tên cho Scope 40](#_bookmark40)

[Hình 5-4: Cấu hình lớp mạng cho Scope 40](#_bookmark41)

[Hình 5-5: Trỏ Default Gateway 41](#_bookmark42)

[Hình 5-6: Cấu hình Prefer DNS 41](#_bookmark43)

[Hình 5-7: Máy Client nhận IP được cấp 42](#_bookmark44)

[Hình 5-8: Máy Client thứ 2 nhận IP 42](#_bookmark45)

[Hình 5-9: Dịch vụ DHCP quản lý các máy con 43](#_bookmark46)

[Hình 5-10: Cấu hình Exclusion 43](#_bookmark47)

[Hình 5-11: Cấu hình ip và chặn 44](#_bookmark48)

[Hình 5-12: Dãy IP bị bặn không được cấp phát 44](#_bookmark49)

[Hình 5-13: Gán IP cố định cho một máy dựa vào MAC 45](#_bookmark50)

[Hình 5-14: Cấu hình IP cố định cho một PC 45](#_bookmark51)

[Hình 5-15: Cấu hình Failover 46](#_bookmark52)

[Hình 5-16: cho biết Server Phụ 46](#_bookmark53)

[Hình 5-17: Chọn chế độ cho 2 DHCP 47](#_bookmark54)

[Hình 5-18: Server phụ đã nhận được thông tin từ Server chính 47](#_bookmark55)

[Hình 5-19: Quá trình cấp phát IP đã thành công 48](#_bookmark56)

[Hình 5-20: Máy Client nhận được IP do DHCP chính cấp 48](#_bookmark57)

[Hình 5-21: IP được cấp từ DHCP Phụ cấp 49](#_bookmark58)

[Hình 5-22: Cấu hình Relay Agent 49](#_bookmark59)

[Hình 5-23: Chọn cổng để nhận IP từ DHCP 50](#_bookmark60)

[Hình 5-24: Cấu hình Default Gateway 50](#_bookmark61)

[Hình 5-25: Nhập địa chỉ IP của DHCP 51](#_bookmark62)

[Hình 5-26: Đã nhận IP từ DHCP thông qua Relay Agent 51](#_bookmark63)

[Hình 6-1: Cài IIS 53](#_bookmark65)

[Hình 6-2: Giao diện IIS 53](#_bookmark66)

[Hình 6-3: Tạo Website 54](#_bookmark67)

[Hình 6-4: Chọn đường dẫn Website 54](#_bookmark68)

[Hình 6-5: Cấu hình Default Document 55](#_bookmark69)

[Hình 6-6: Cấu hình tên của Website khi boot 55](#_bookmark70)

[Hình 6-7: Máy Client truy cập vào IP của Web 55](#_bookmark71)

[Hình 6-8: Máy win 8 đăng nhập vào Web bằng IP 56](#_bookmark72)

[Hình 6-9: Cấu hình chạy web chạy bằng tên 56](#_bookmark73)

[Hình 6-10: Cấu hình DNS cho Website 56](#_bookmark74)

[Hình 6-11: Cấu hình Primary 57](#_bookmark75)

[Hình 6-12: Cấu hình tên cho website 57](#_bookmark76)

[Hình 6-13: Cấu hình host 58](#_bookmark77)

[Hình 6-14: Cấu hình tên miền Newstar 58](#_bookmark78)

[Hình 6-15: Cấu hình Zone dantri.com.vn 59](#_bookmark79)

[Hình 6-16: Các Zone DNS đã được tạo 59](#_bookmark80)

[Hình 6-17: Tạo Reverse Lookup Zone 60](#_bookmark81)

[Hình 6-18: Truy cập vào các trang web đã tạo 60](#_bookmark82)

[Hình 7-1: Cấu hình dịch vụ Web 62](#_bookmark84)

[Hình 7-2: Cấu hình FTP 62](#_bookmark85)

[Hình 7-3: Add FTP 63](#_bookmark86)

[Hình 7-4: Cấp quyền cho người truy cập 63](#_bookmark87)

[Hình 7-5: Truy cập FTP thành công 64](#_bookmark88)

[Hình 7-6: Cấu hình truy cập có tài khoản 64](#_bookmark89)

[Hình 7-7: Đăng nhập tài khoản trên web 65](#_bookmark90)

[Hình 7-8: Đăng nhập tài khoản trên windows Exploror 65](#_bookmark91)

[Hình 8-1: Cấu hình NAT 67](#_bookmark93)

[Hình 8-2: Thêm cổng 67](#_bookmark94)

[Hình 8-3: Cấu hình Public và Private 68](#_bookmark95)

[Hình 8-4: Kiểm tra kết nối 68](#_bookmark96)

[Hình 8-5: Cấu hình NAT website 69](#_bookmark97)

[Hình 8-6: Điền IP Server Private 69](#_bookmark98)

[Hình 8-7: Truy cập IP Public trên trình duyệt web 70](#_bookmark99)

[Hình 9-1: Cài đặt dịch vụ DHCP 72](#_bookmark101)

[Hình 9-2: Tùy chỉnh DHCP trên domain 72](#_bookmark102)

[Hình 9-3: Dãy Range cấp phát 73](#_bookmark103)

[Hình 9-4: Cài đặt dịch vụ WDS 73](#_bookmark104)

[Hình 9-5: Chọn cả 2 tùy chọn 74](#_bookmark105)

[Hình 9-6: Cấu hình WDS 74](#_bookmark106)

[Hình 9-7: Chọn chế độ domain 75](#_bookmark107)

[Hình 9-8: Chỉ đường dẫn lưu file cài 75](#_bookmark108)

[Hình 9-9: Thiết lập DHCP 76](#_bookmark109)

[Hình 9-10: Phản hồi cho tất cả các máy Client 76](#_bookmark110)

[Hình 9-11: Thêm file ảnh HDH 77](#_bookmark111)

[Hình 9-12: Đặt tên cho Group HDH 77](#_bookmark112)

[Hình 9-13: Chọn File Intall 78](#_bookmark113)

[Hình 9-14: Chọn HDH cần cài 78](#_bookmark114)

[Hình 9-15: Những HDH cài 79](#_bookmark115)

[Hình 9-16: Thêm file boot 79](#_bookmark116)

[Hình 9-17: Chọn file boot 80](#_bookmark117)

[Hình 9-18: Chọn HDH 32 bit 81](#_bookmark118)

[Hình 9-19: Những phiên bản được chọn cài 81](#_bookmark119)

[Hình 9-20: Thông tin file cài 82](#_bookmark120)

[Hình 9-21: Cấu hình File đăng nhập 82](#_bookmark121)

[Hình 9-22: Chọn file Unattend 83](#_bookmark122)

[Hình 9-23: Chỉnh sửa WDS 83](#_bookmark123)

[Hình 9-24: Cấu hình cho máy Client tác dụng 84](#_bookmark124)

[Hình 9-25: Điều chỉnh file boot 84](#_bookmark125)

[Hình 9-26: Điều chỉnh thông số Scope 85](#_bookmark126)

[Hình 9-27: Máy client đang load HDH 85](#_bookmark127)

[Hình 9-28: Lựa chọn HDH cài 85](#_bookmark128)

[Hình 10-1: Cài đặt dịch vụ Data Deduplication 86](#_bookmark130)

[Hình 10-2: Lựa chọn ổ đĩa để cấu hình 87](#_bookmark131)

[Hình 10-3: Tìm kiếm dữ liệu bị trùng lắp và khắc phục 87](#_bookmark132)

[Hình 11-1: Tạo user U1 89](#_bookmark134)

[Hình 11-2: Tùy chỉnh tài khoản U1 89](#_bookmark135)

[Hình 11-3: Tùy chỉnh Allow access 90](#_bookmark136)

[Hình 11-4: Tiến hành kết nối VPN ở máy Client 90](#_bookmark137)

[Hình 11-5: Lựa chọn kết nối 91](#_bookmark138)

[Hình 11-6: Nhập địa chỉ IP của máy Windows server 2016 91](#_bookmark139)

[Hình 11-7: VPN đã kết nối được 92](#_bookmark140)

[Hình 11-8: IP VPN đã cấp 92](#_bookmark141)

[Hình 11-9: Kiểm tra kết nối tới các IP trong nội bộ 93](#_bookmark142)

[Hình 11-10: Cài Remote Access 94](#_bookmark143)

[Hình 11-11: Cài RAS 95](#_bookmark144)

[Hình 11-12: Chọn RAS và Routing 95](#_bookmark145)

[Hình 11-13: Cấu hình RRAS 96](#_bookmark146)

[Hình 11-14: Tùy chọn Custom 96](#_bookmark147)

[Hình 11-15: Chọn các lựa chọn phù hợp 97](#_bookmark148)

[Hình 11-16: Cấu hình dịch vụ NAT 97](#_bookmark149)

[Hình 11-17: Cấu hình NAT cho cổng trong 98](#_bookmark150)

[Hình 11-18: Cấu hình NAT cho cổng ngoài 98](#_bookmark151)

[Hình 11-19: Cấu hình dịch VPN ở R1 99](#_bookmark152)

[Hình 11-20: Đặt tên cho cổng ở R1 99](#_bookmark153)

[Hình 11-21: Lựa chọn kết nối VPN ở R1 100](#_bookmark154)

[Hình 11-22:Chọn giao thức kết nối 100](#_bookmark155)

[Hình 11-23: Nhập địa chỉ IP Public Hà nội 101](#_bookmark156)

[Hình 11-24: Tùy chọn cổng và tạo tài khoản 101](#_bookmark157)

[Hình 11-25: Nhập mạng nội bộ bên Hà Nội 102](#_bookmark158)

[Hình 11-26: Nhập Password cho tài khoản hcm 102](#_bookmark159)

[Hình 11-27: Nhập tài khoản Hà nội 103](#_bookmark160)

[Hình 11-28: Cấu hình cổng interface 103](#_bookmark161)

[Hình 11-29: Ip Public cổng nhánh hcm 104](#_bookmark162)

[Hình 11-30: Nhập tài khoản ở Hà Nội 105](#_bookmark163)

[Hình 11-31: Nhập tài khoản hcm 105](#_bookmark164)

[Hình 11-32: VPN đã được kết nối 106](#_bookmark165)

[Hình 11-33: Đứng trong nội bộ hcm ping thấy nội bộ hn 106](#_bookmark166)

[Hình 11-34: Đứng trong nội bộ hn thấy nội bộ hcm 107](#_bookmark167)

[Hình 11-35: HN truy cập được file của HCM 107](#_bookmark168)

[Hình 12-1: Đặt IP cho Server Domain 109](#_bookmark170)

[Hình 12-2: Cài dịch vụ ADDS 109](#_bookmark171)

[Hình 12-3: Cài Domain 110](#_bookmark172)

[Hình 12-4: Nhập tên domain 110](#_bookmark173)

[Hình 12-5: Tạo tài khoản trên domain 111](#_bookmark174)

[Hình 12-6: Đặt IP trên máy Client 111](#_bookmark175)

[Hình 12-7: Nhập tài khoản trên domain 112](#_bookmark176)

[Hình 12-8: Đăng nhập tài khoản hiepdh 112](#_bookmark177)

[Hình 12-9: Đặt IP trên máy Client 113](#_bookmark178)

[Hình 12-10: Đăng nhập tài khoản hiepdh trên domain 113](#_bookmark179)

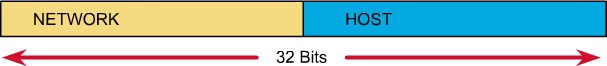
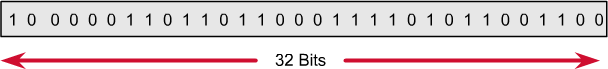
[Hình 12-11: Đăng nhập tài khoản Administrator domain trên máy client 114](#_bookmark180)

[Hình 12-12: Các máy Join domain 114](#_bookmark181)

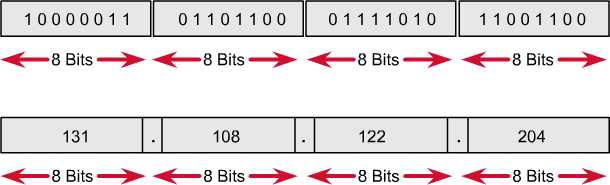
# Triển khai địa chỉ Ipv4

*Sau khi học bài này học viên sẽ triển khai được địa chỉ IP vào hệ thống mạng, chia IP cho hệ thống mạng lớn. Tư duy được khả năng quản trị hệ thống với số lượng IP lớn*

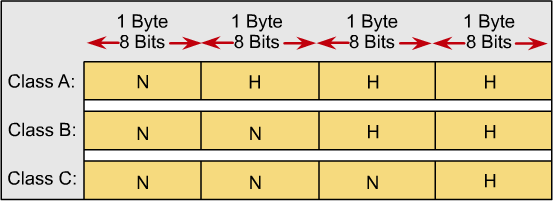
* + Địa chỉ IP 32 bits (*32 bit IP address* – IPv4). Địa chỉ IP gồm 2 phần: địa chỉ mạng (*Netid*) và địa chỉ máy trạm (*Hostid*).



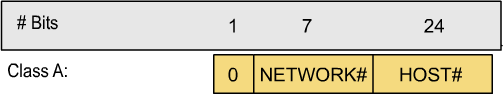
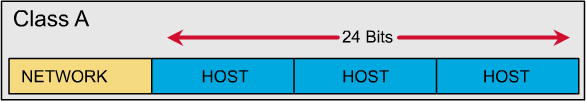
* + Network ID:
    - Xác định địa chỉ mạng.
    - Xác định lớp của địa chỉ IP
    - Tất cả các bits đồng thời không được bằng 0
  + Host ID:
    - Xác định địa chỉ máy
    - Tất cả các bits bằng 0: gọi là địa chỉ mạng
    - Tất cả các bits bằng 1: gọi là đại chỉ broadcast
  + Mỗi địa chỉ IP có độ dài 32 bits được tách thành 4 vùng có thể biểu thị dưới dạng thập phân, thập lục phân hay nhị phân. Cách viết phổ biến nhất là dùng ký pháp thập phân có dấu chấm (*dotted decimal notation*) để tách các vùng. Mục đích của địa chỉ IP là để định danh duy nhất cho một máy tính bất kỳ trên liên mạng.



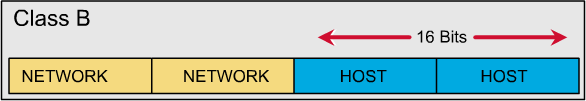
* + Phân loại IP
    - Địa chỉ IP được chia làm 5 lớp: A, B, C, D, E
    - Địa chỉ lớp D là lớp địa chỉ Multicast
    - Địa chỉ lớp E là lớp địa chỉ được để nghiên cứu
    - Sử dụng 3 lớp A, B, C

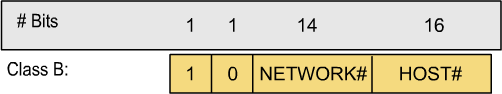


* + Địa chỉ lớp A
    - Nhận 1 octet đầu tiên của địa chỉ IP làm địa chỉ mạng
    - 3 Octet còn lại được sử dụng cho đánh địa chỉ máy
    - Bit đầu tiên của lớp A luôn luôn là bit **0**

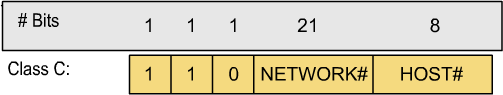
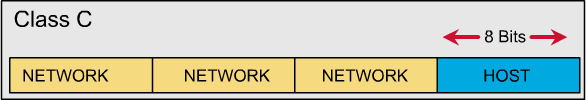


* + - Địa chỉ IP lớp A từ 1.0.0.0 đến 126.0.0.0
    - 127.0.0.0 là địa chỉ loopback
    - Mỗi địa chỉ lớp A có số host là 16,777,214
  + Địa chỉ lớp B
    - Nhận 2 octet đầu tiên của địa chỉ IP làm địa chỉ mạng
    - 2 Octet còn lại được sử dụng cho đánh địa chỉ máy
    - 2 Bit đầu tiên của lớp B luôn luôn là bit **10**





* + - Địa chỉ IP lớp B từ 128.0.0.0 đến 191.255.0.0
    - Mỗi địa chỉ lớp A có số host là 65,534
  + Địa chỉ lớp C
    - Nhận 3 octet đầu tiên của địa chỉ IP làm địa chỉ mạng
    - 1 Octet còn lại được sử dụng cho đánh địa chỉ máy
    - 3 Bit đầu tiên của lớp C luôn luôn là bit **110**



* + - Địa chỉ IP lớp B từ 192.0.0.0 đến 223.255.255.0
    - Mỗi địa chỉ lớp A có số host là 254
  + Tổng kết
    - 1.0.0.0 - 126.0.0.0 : Class A.
    - 127.0.0.0 : Loopback network.
    - 128.0.0.0 - 191.255.0.0 : Class B.
    - 192.0.0.0 - 223.255.255.0 : Class C.
    - 224.0.0.0 < 240.0.0.0 : Class D, multicast.
    - >= 240.0.0.0 : Class E, reserved.
  + Địa chỉ Private
    - Là địa chỉ dùng để gán cho các hệ thống mạng nội bộ
    - Không được kết nối ra internet
    - Class A: 10.X.X.X
    - Class B: 172.16-31.X.X
    - Class C: 192.168.X.X
  + Cách viết subnetmask
    - Dạng thập phân: VD: 255.255.255.0
    - Dạng biểu diễn số bit xác định đ/c mạng trong chuỗi bit subnet mask (bit1), viết: /<số bit đ/c mạng>. VD: 192.168.10.1/24
    - Bảng subnet mask mặc định của lớp A, B, C

|  |  |  |  |
| --- | --- | --- | --- |
| Lớp | Chuỗi bit subnet mask | Subnet mask | # |
| A | 11111111 00000000 00000000 00000000 | 255.0.0.0 | /8 |
| B | 11111111 11111111 00000000 00000000 | 255.255.0.0 | /16 |
| C | 11111111 11111111 11111111 00000000 | 255.255.255.0 | /24 |

 Ví dụ: 10.10.5.12/255.0.0.0 hoặc 10.10.5.12/8 172.31.23.2/255.255.0.0 hoặc 172.31.23.2/16

213.112.12.4/255.255.255.0 hoặc 213.112.12.4/24

* + Với IP lớp A, B, C có subnet mask mặc định

 Ví dụ: 10.10.5.12/8 => NetID là: 10.0.0.0 172.31.23.2/16 => NetID là: 172.31.0.0

213.112.12.4/24 => NetID là: 213.112.12.0

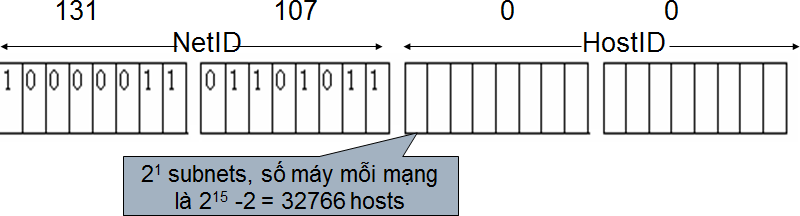
* + Ví dụ: Lớp C có thể đánh địa chỉ cho 254 máy nhưng nếu chỉ muốn đánh địa chỉ cho 14 máy. Khi đó:
* Địa chỉ IP sử dụng cho mạng có HostID là 4bit (14 ~ 24 = 16)
* Phần NetID là: 28 bit (32 – 4)
* Subnet mask là: 255.255.255.240 (240 ~ 11110000)
  + Biểu diễn:

|  |  |  |
| --- | --- | --- |
| Subnet mask mặc định | Thêm vào NetID | HostID |
| 11111111 11111111 11111111 | 1111 | 0000 |

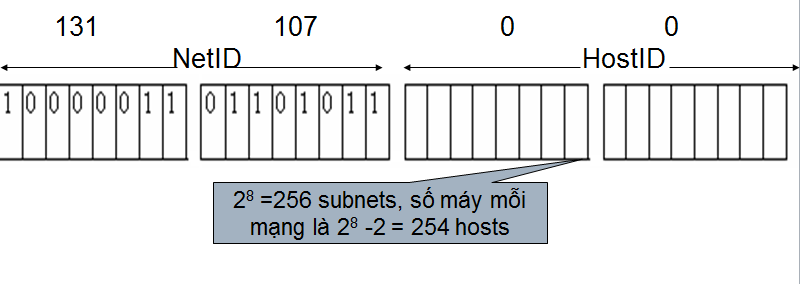
* + Tổng quát: Địa chỉ mạng trong địa chỉ IP của một máy được xác định bằng cách thực hiện phép AND các bit địa chỉ IP với các bit của subnet mask.
  + Ví dụ: máy có đ/cIP: 131.107.164.26/20, địa chỉ mạng được xác định:

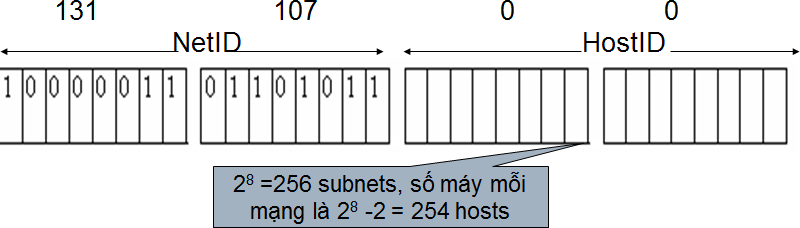
|  |  |  |  |
| --- | --- | --- | --- |
|  | NetID | HostID | Biểu diễn |
| Địa chỉ IP | 10000011 01101011 10100100 | 00011010 | 131.107.164.26 |
| Submask | 11111111 11111111 11110000 | 00000000 | 255.255.240.0 |
| Địa chỉ mạng | 10000011 01101011 10100000 | 00000000 | 131.107.160.0 |

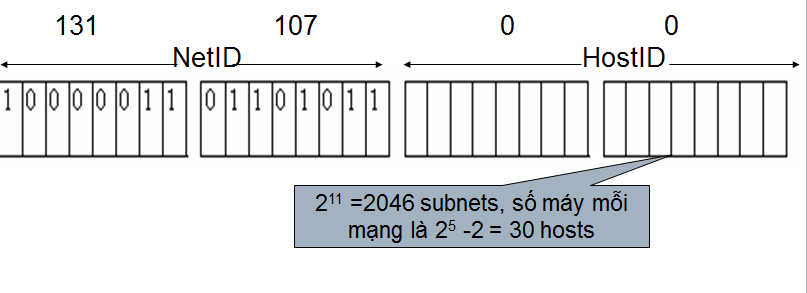
* + Khái niệm: Một k thuật cho phép người quản trị phân chia một mạng thành nhiều mạng nhỏ hơn bằng cách sử dụng các chỉ số mạng được gán.
    - Số mạng con phụ thuộc vào độ lớn của mạng thực tế
    - Việc phân chia mạng con phụ thuộc vào y/c thực tế cũng như sự phát triển tương lai của hệ thống.
  + Thuận lợi của việc sử dụng k thuật subnet
    - Nhằm giảm đụng độ trên mạng.
    - Đơn giản trong quản trị.
    - Cấu trúc lại mạng bên trong mà không ảnh hưởng đến mạng bên ngoài.
    - Cải thiện khả năng bảo mật.
    - Có thể cô lập lưu thông trên mạng.
  + Như vậy:Số mạng con được chia tỉ lệ nghịch với số máy có thể đánh địa chỉ trong mỗi mạng con
  + Khi số mạng con được phân chia ít, tức số bit NetID ít thì số máy có thể đánh đ/c nhiều, tức bit HostID nhiều
  + Khi chia nhiều mạng con, số bit NetID nhiều thì đánh ít địa chỉ hơn
  + Phân tích 1 số trường hợp phân chia subnet 131.107.0.0
  + TH1: thêm 1 bit cho phần NetID => NetID=16+1=17; HostID=15



TH2: Thêm 8bit cho phần NetID => NetID=16+8=24

Thêm 8bit cho phần NetID => NetID=16+8=24; HostID=8



Thêm 11bit cho phần NetID => NetID=16+11=27 HostID=5

 Ví dụ: 172.16.20.200

* + - Là địa chỉ IP lớp B
    - Phần network: 172.16
    - Phần host: 20.200
    - Địa chỉ network: 172.16.0.0
    - Địa chỉ Broadcast: 172.16.255.255

TH2:

TH3:

# Sử dụng phần mềm VMWare và Cài đặt Windows Server 2016

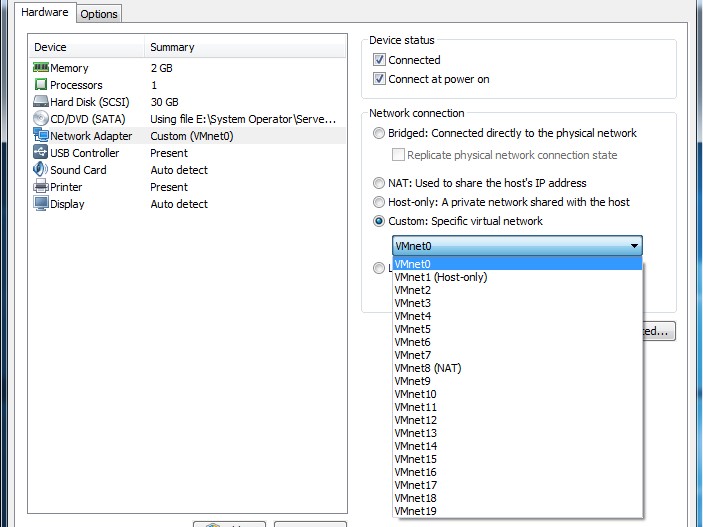
*Sau khi học bài này xong học viên có khả năng sử dụng máy ảo một cách thành thạo, tư duy về mô hình giả lập cho hệ thống mạng của công ty. Tạo các thuận lợi khi làm lab ảo*

* + Chuẩn bị:

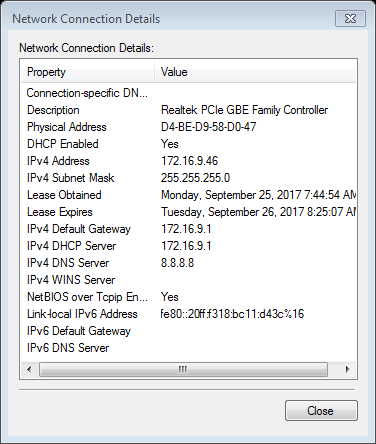
+ Một máy Windows Server 2016

* + Kết quả đạt được bài lab
* Sử dụng card Vmnet 0 nhận được địa chỉ IP cùng net với máy thật đồng thời kết nối internet
* Sử dụng card Vmet 8 nhận được địa chỉ IP khác mạng với máy thật đồng thời kết nối internet
* Sử dụng card Vmnet 1 kết nối với máy thật
* Sử dụng các card Vmnet còn lại sử dụng như một Switch
* Tạo Snapshot để lưu trữ lại các bài đã làm
  + Thực hiện

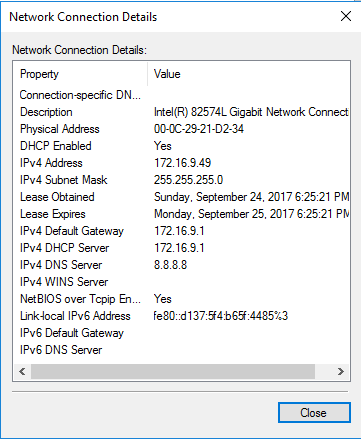
1. Sử dụng phần mềm máy ảo

* Trong VMWare có 20 card mạng ảo

*Hình 2-1: Các card Vmnet trong máy ảo*

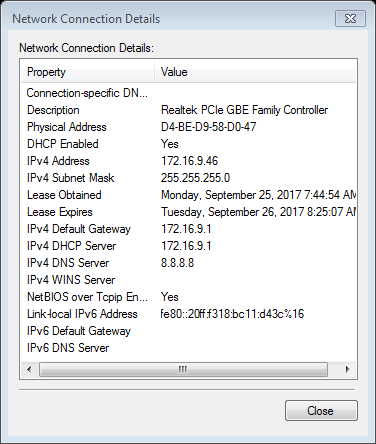
* Tính chất card Vmnet 0 (Bridge): Giúp máy ảo ra internet thông qua card mạng thật, Network của card mạng ảo Vmnet0 cùng network với Netwok mạng thật

*Hình 2-2: Địa chỉ IP của máy thật*

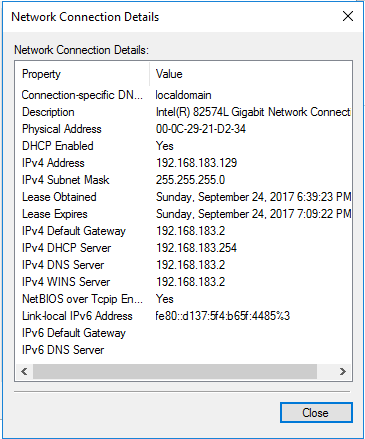


*Hình 2-3: Địa chỉ IP của máy ảo*

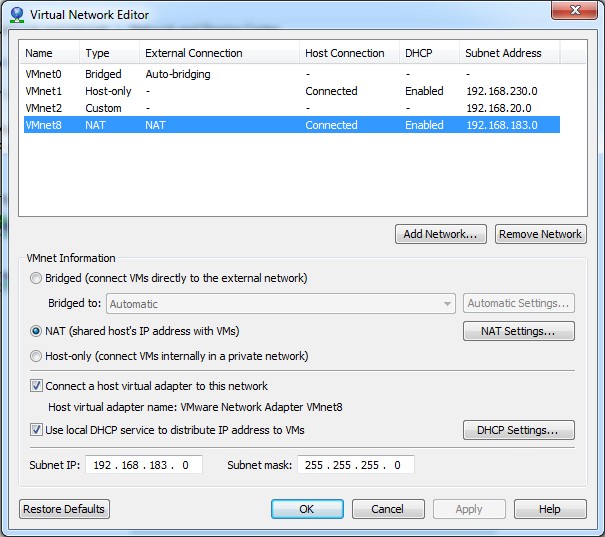
* Tính chất card Vmnet 8 (NAT): Giúp máy ảo ra internet thông qua card mạng thật, Network của card mạng ảo Vmnet0 **khác** network với Netwok mạng thật



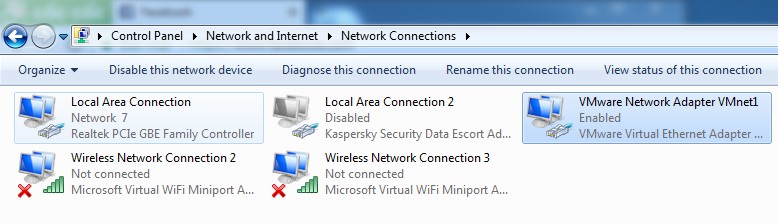
*Hình 2-4: Địa chỉ IP máy thật*



*Hình 2-5: Địa chỉ IP máy ảo*



*Hình 2-6: Network của máy ảo*

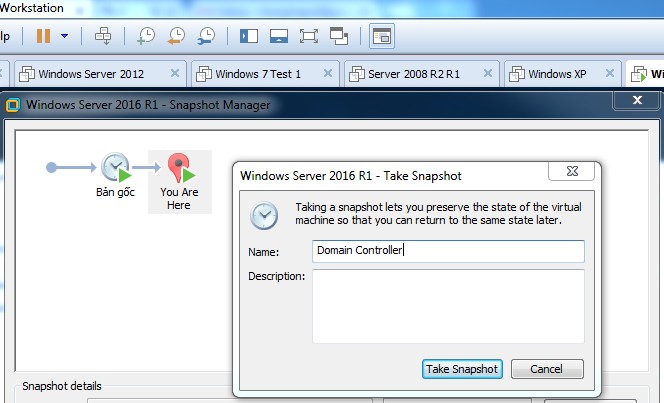
* Tính chất card Vmnet 1 (Localhost): Giúp máy ảo ra kết nối với máy thật

*Hình 2-7: Card Vmnet 1 trong máy thật*

 Tính chất card Vmnet 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,

19: Mỗi Card là một Switch

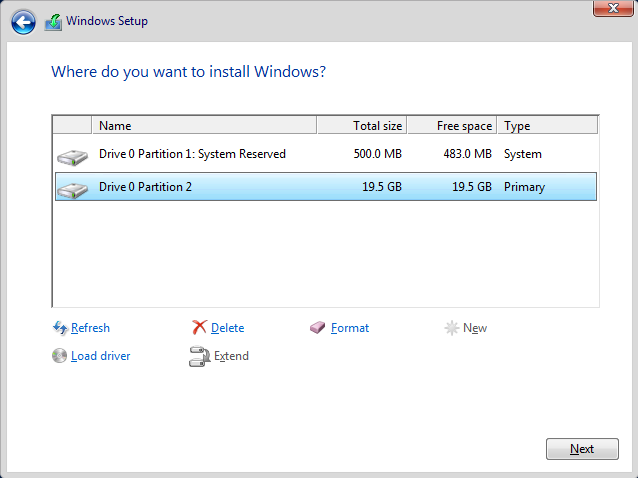
* Để thuận tiện cho việc làm lab, học viên nên tạo bảng Snapshot thuận lợi chỉnh sửa khi bị lỗi



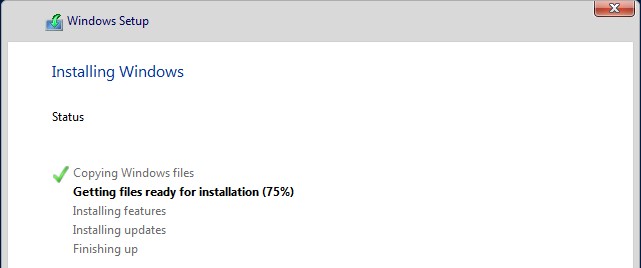
*Hình 2-8: Tạo Snapshot cho máy ảo*

1. Cài máy ảo Windows Server 2016

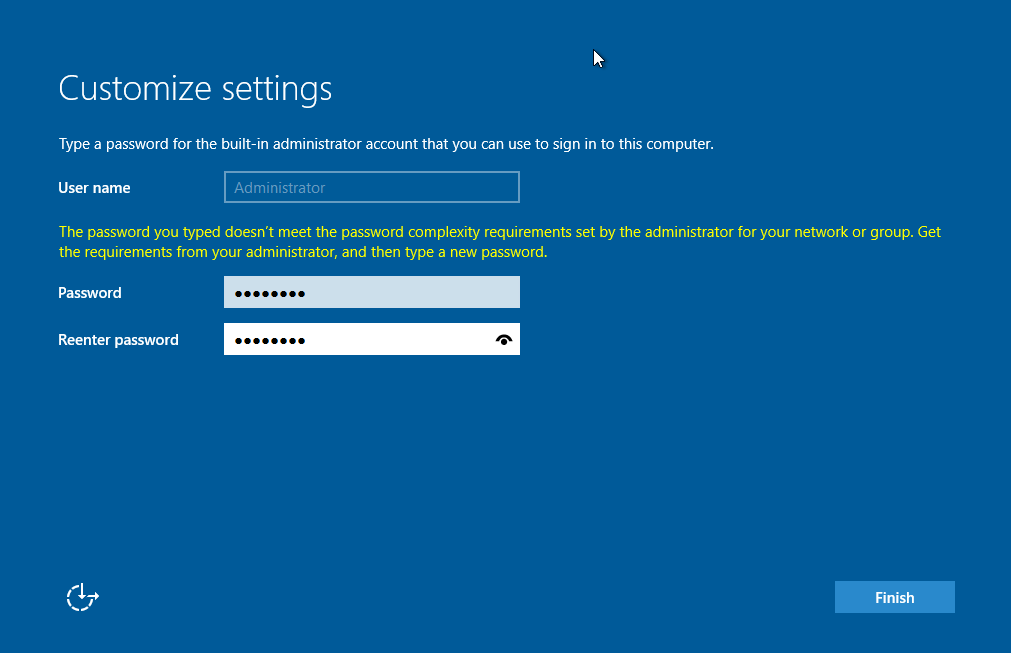
*Hình 2-9: Giao diện cài windows Server 2016*



*Hình 2-10: Cấu hình ổ đĩa*



*Hình 2-11: Quá trình cài đặt*



*Hình 2-12: Yêu cầu đặt Password*

# Dịch vụ DNS

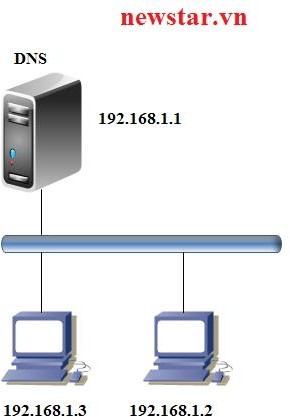
*Sau khi học bài này học viên có thể phân giải được tên miền của các dịch vụ trong hệ thống mạng. Thay vì chúng ta phải truy cập bằng tên thì ở đây chúng ta sẽ truy cập bằng địa chỉ IP*

1. DNS Primary
   * Chuẩn bị:

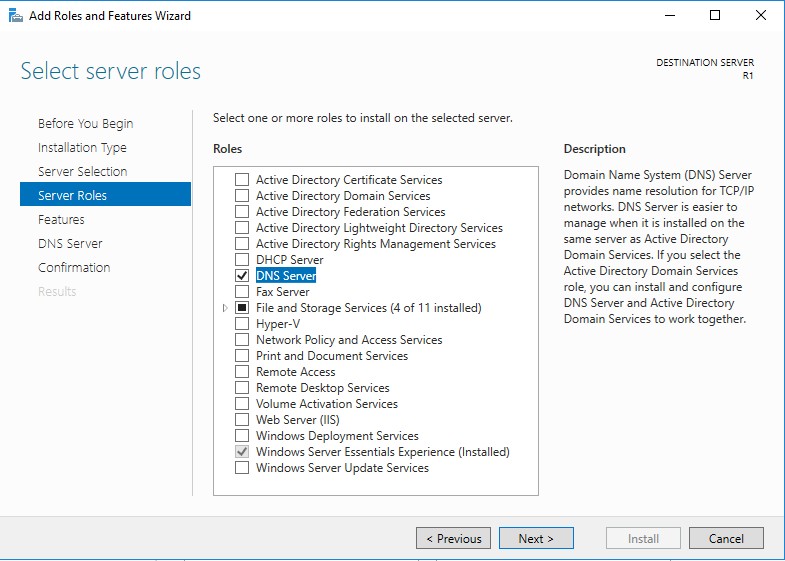
+ Một máy server cài Windows Server 2016

+ Hai máy Client Windows 7 và Windows XP

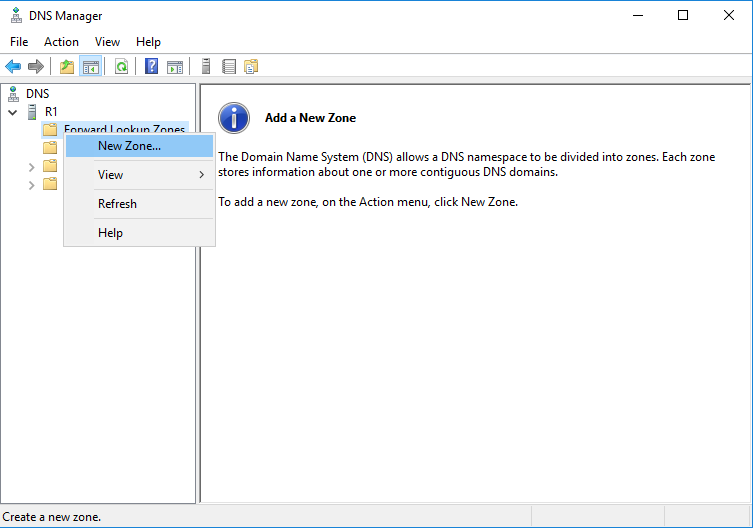
* + Mô hình



* + Kết quả đạt được
    - Phân giải được tên miền newstar.vn
  + Thực hiện
* Cài dịch vụ DNS trên Windows server 2016



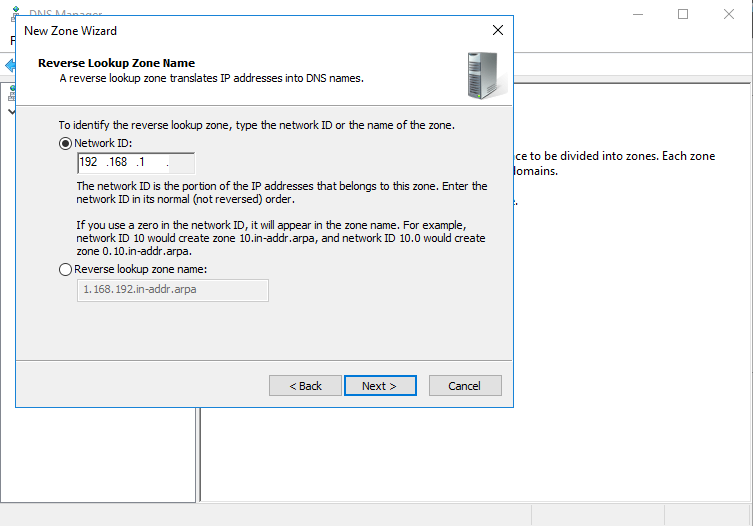
*Hình 3-1: Cài Role DNS Server*

* Tạo Zone mới để phân giải tên miền

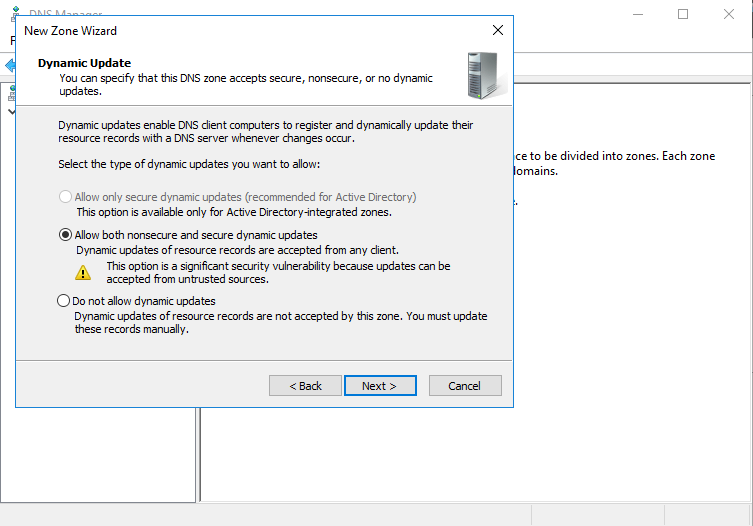
*Hình 3-2: Tạo Zone mới*



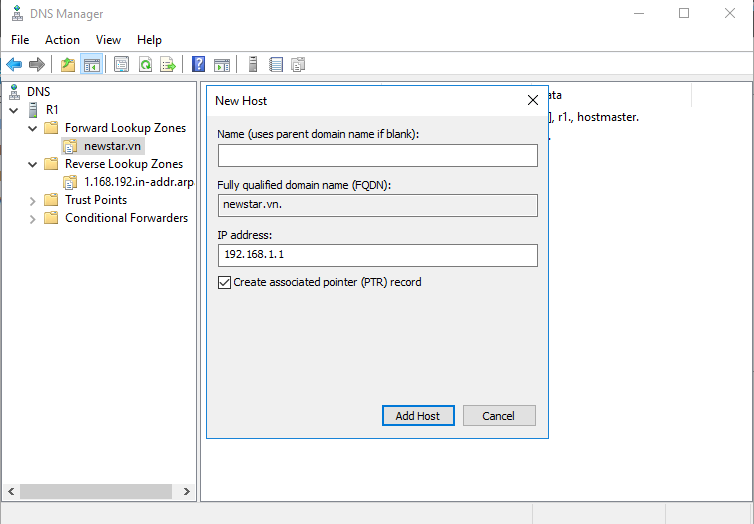
*Hình 3-3: Đặt tên cho zone là newstar.vn*

* Nhập địa chỉ IP để phân giải tên miền

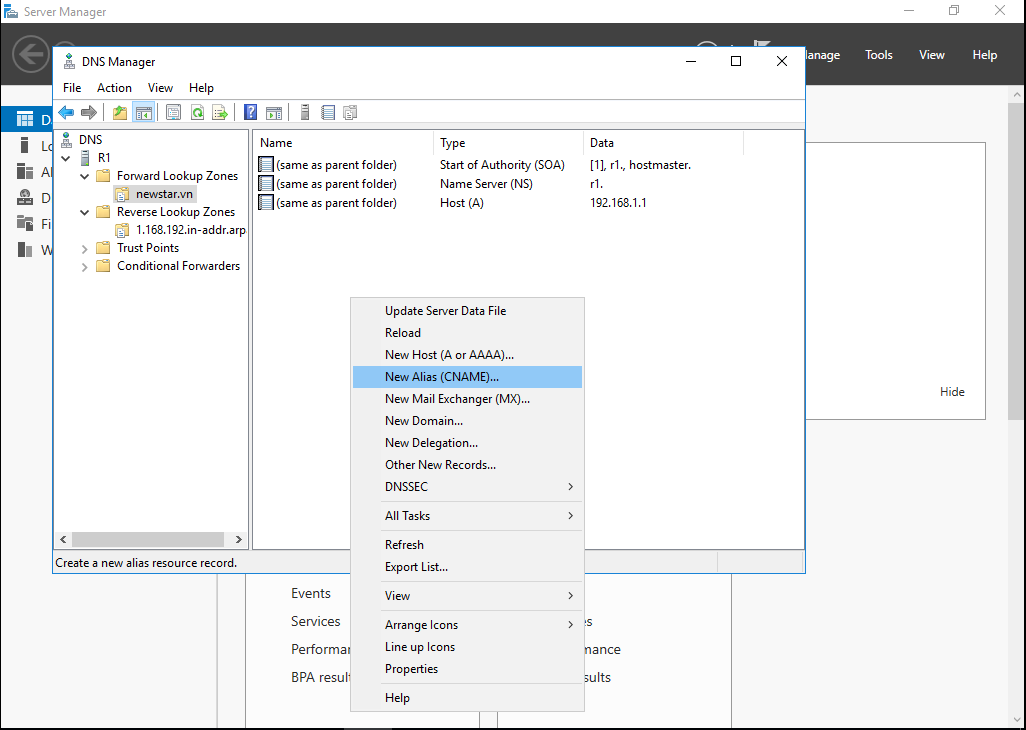
*Hình 3-4: Tạo Reverse lookup zone*



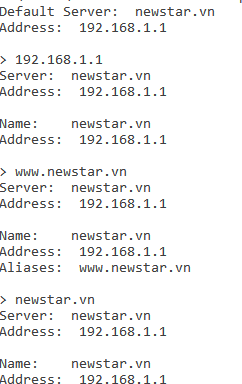
*Hình 3-5: Lựa chọn phương thức Update*

* Chọn check Create associated pointer (PTR) record để tự động add IP qua Reverse lookup Zones khi thêm host vào

*Hình 3-6: Tạo new host*

* Tạo mặc danh cho tên miền newstar.vn

*Hình 3-7: Tạo Alias*

* Sao khi cấu hình xong thì phân giải thành công

*Hình 3-8: kết quả phân giải tên miền thành công*

1. DNS Secondary

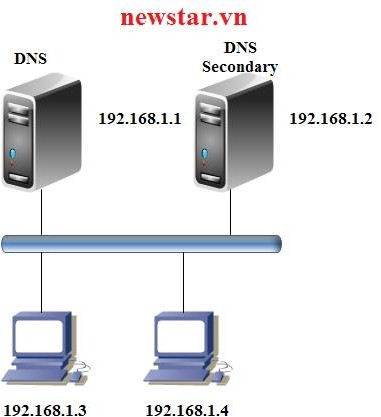
*Sau khi học bài này xong học viên có thể xây dựng một hệ thống DNS có một server chính và một server phụ cần nhau phân giải tên miền*

* + Chuẩn bị:

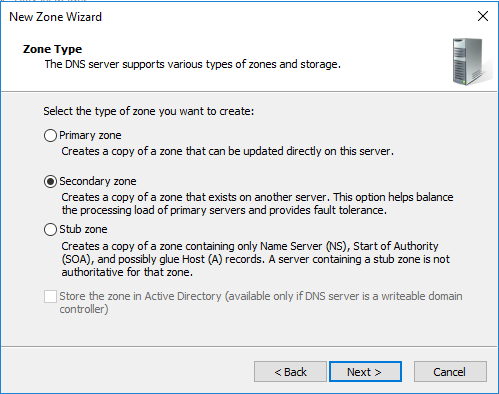
+ Một 2 máy server cài Windows Server 2016

+ Hai máy Client Windows 7 và Windows XP

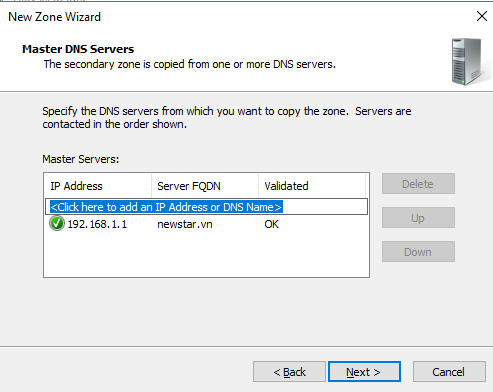
* + Mô hình



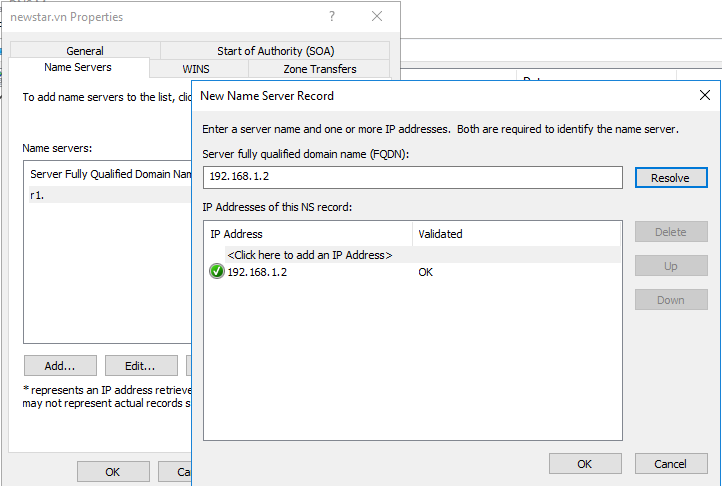
* + Kết quả đạt được
    - Đồng bộ DNS và DNS secondary
  + Thực hiện
* Thực hiện cấu hình DNS secondary dự phòng và cân bằng tải cho server Primary



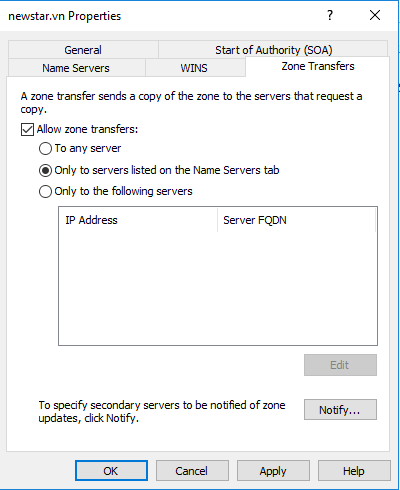
*Hình 3-9: Cấu hình DNS Secondary*



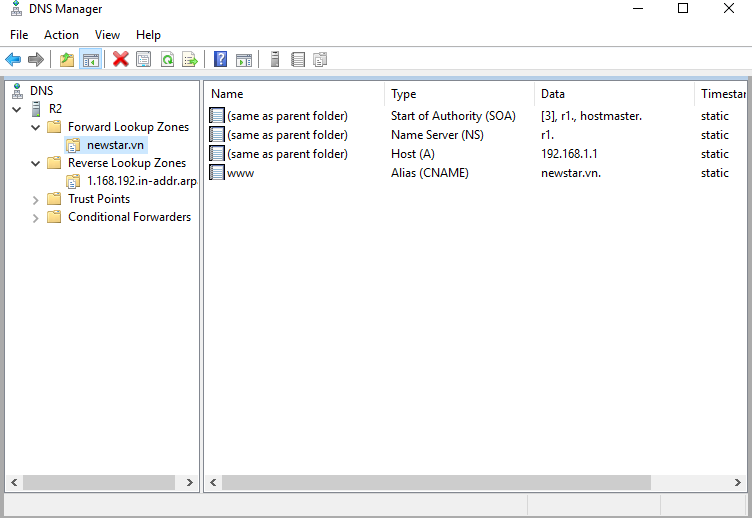
*Hình 3-10: Chọn Master DNS*



*Hình 3-11: Chọn Server để đồng bộ DNS*



*Hình 3-12: Chọn phương thức để đồng bộ*



*Hình 3-13: Quá trình đồng bộ đã xong*

# Routing and Remote Access

*Sau khi học bài này học viên có thể định tuyến giữa hai hệ thống mạng khác network với nhau. Trong này sử dụng giao thức Static route và Rip*

* + Chuẩn bị:

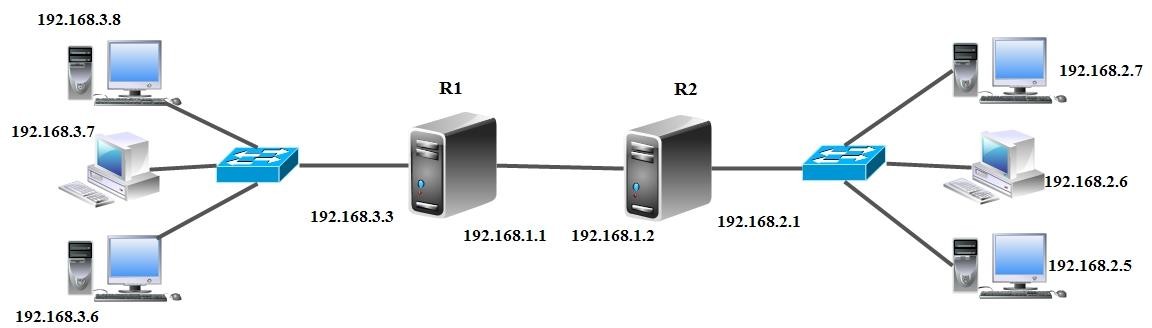
+ Một máy Windows server 2016 đặt tên R1

+ Một máy Windows server 2016 đặt tên R2

+ Một máy Windows 7 đặt tên test1

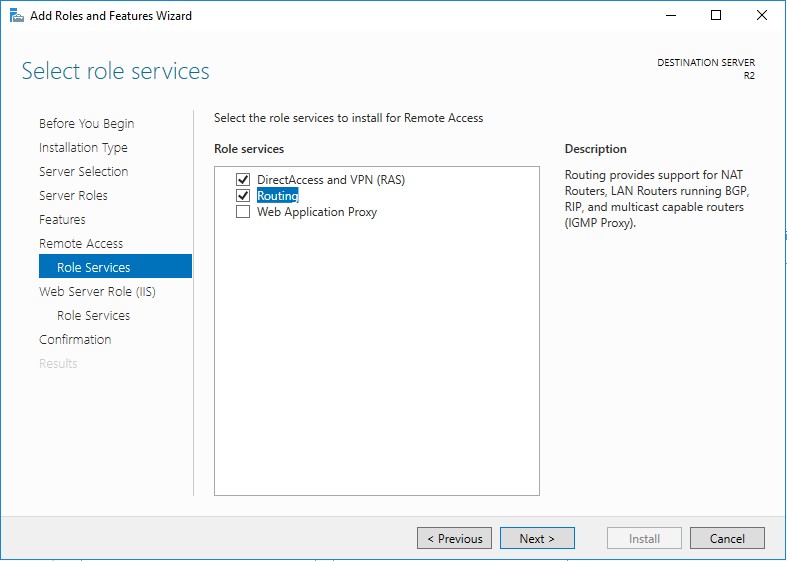
+ Một máy Windows 7 đặt tên test2

* + Mô hình

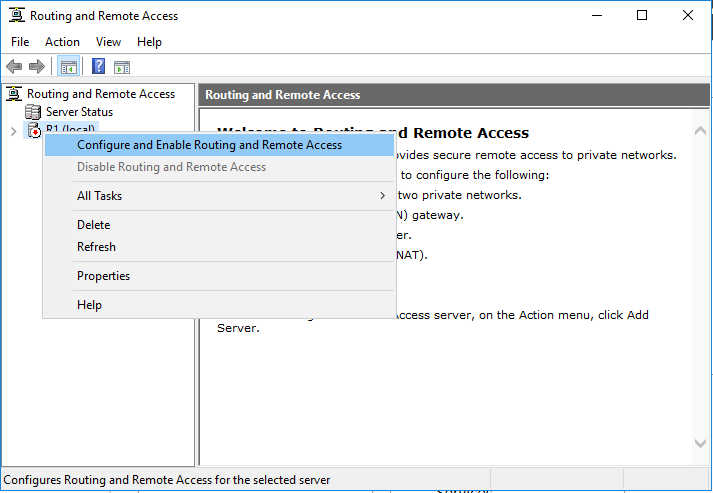


* + Kết quả đạt được

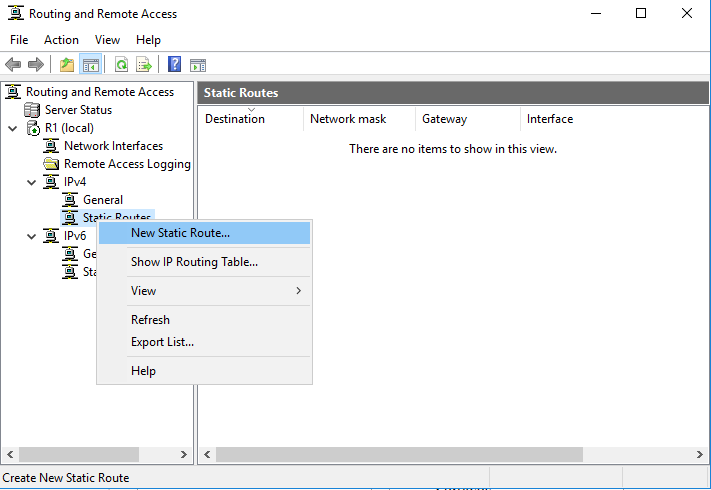
 PC 192.168.2.7 ping được PC 192.168.3.8

* + Thực hiện
* Cài đặt dịch vụ Routing cho mô hình

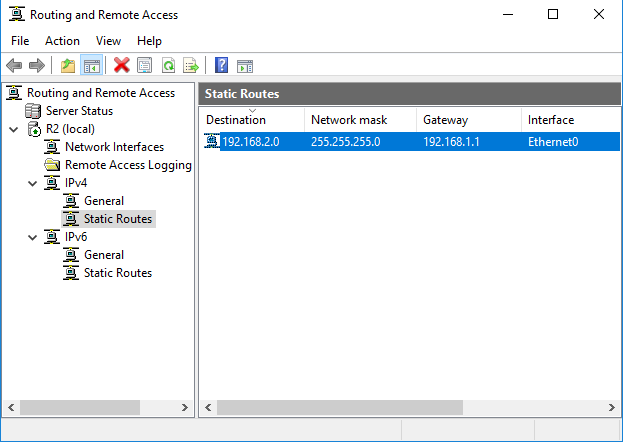
*Hình 4-1: Cài dịch vụ Routing*



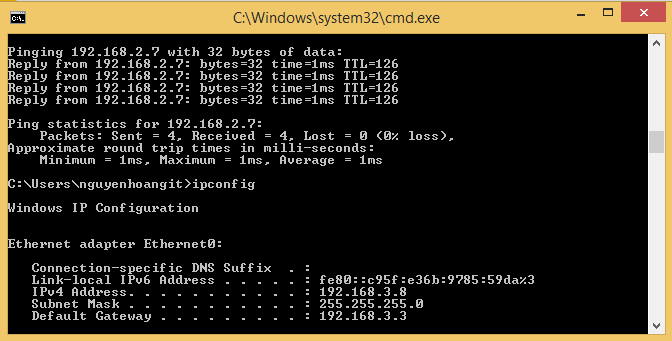
*Hình 4-2: Cấu hình Routing and Remote Access*

* Cấu hình định tuyến tĩnh (Static route)

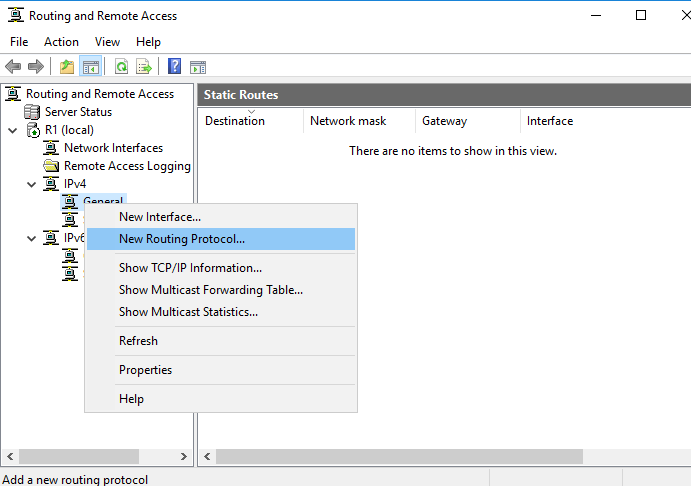
*Hình 4-3: Tạo New Route*



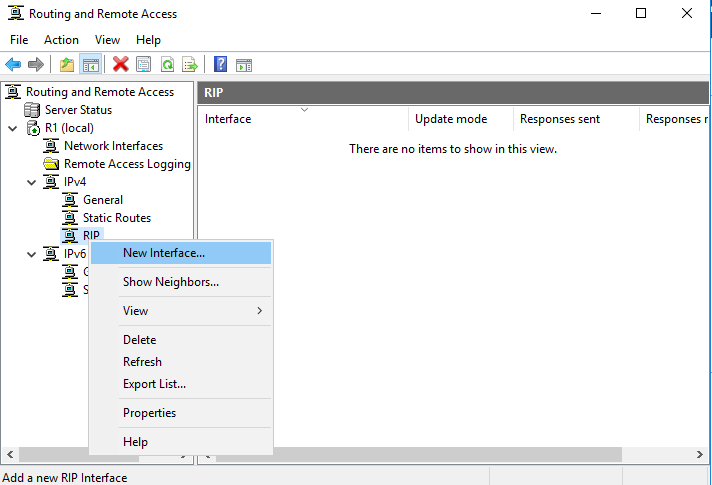
*Hình 4-4: Cấu hình định tuyến tĩnh*



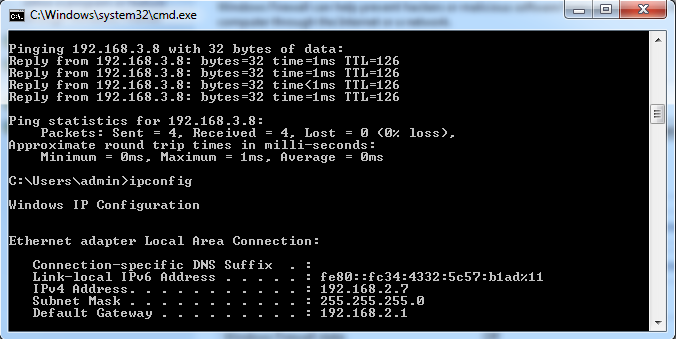
*Hình 4-5: Kiểm tra kết nối*

* Cấu hình định tuyến động (Rip)

*Hình 4-6: Cấu hình định tuyến động*



*Hình 4-7: Thêm Interface vào định tuyến*



*Hình 4-8: Kiểm tra kết quả*

# Dịch vụ DHCP

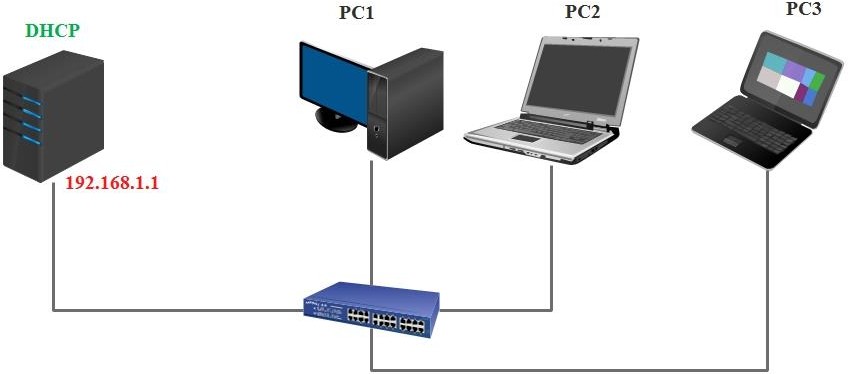
*Sau khi học xong bài này thì học viên có khả năng cấp phát địa chỉ ip động cho hệ thống mạng. Cấp cho hệ thống cùng network và cấp cho hệ thống khác Network (relay agent), Xây dựng hệ thống DHCP cân bằng tải và dự phòng*

* + Chuẩn bị:

+ Một máy Windows Server 2016

+ Ba máy client

* + Mô hình



* + Kết quả đạt được
* Cấp IP cho các máy client và luôn luôn cấp có máy PC2 là 192.168.1.79
  + Thực hiện

+ Chuẩn bị dãy địa chỉ IP cần cấp phát

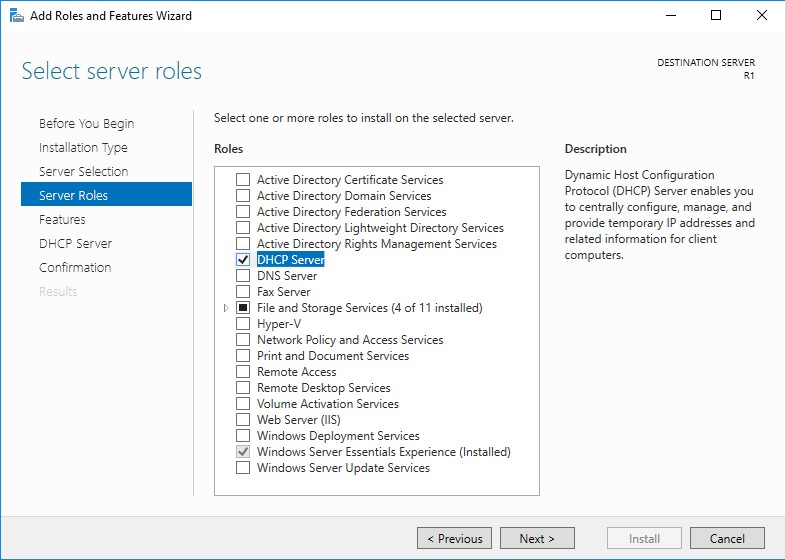
* Địa chỉ mạng: **192.168.1.0/24**
* Dãy cấp phát: **192.168.1.10-192.168.1.100**
* Gateway: **192.168.1.1**
* DNS: **8.8.8.8**

+ Cấu hình dãy địa chỉ IP bỏ qua trong dãy cấp phát

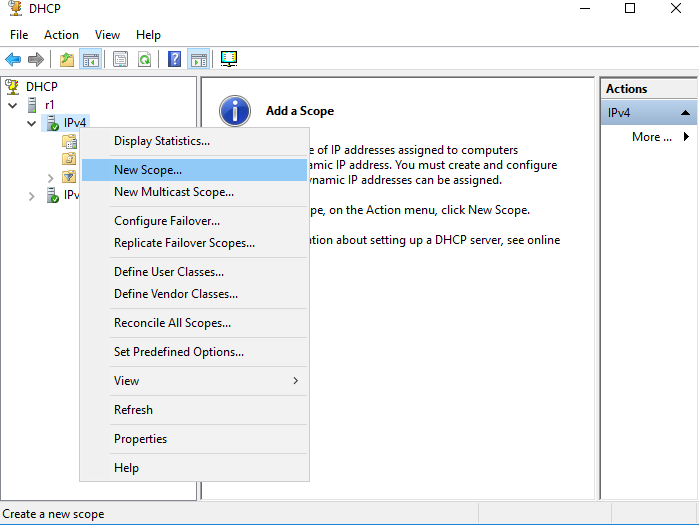
* Dãy ip chặn không được cấp: **192.168.1.11 – 192.168.1.20**

+ Cấu hình một mấy cố định cho một IP cố định

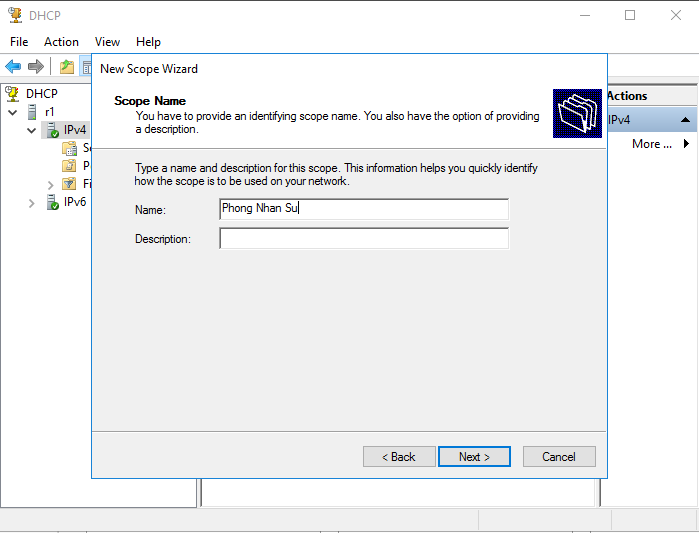
* Gán cho PC2 luôn luôn nhận IP: **192.168.1.79**



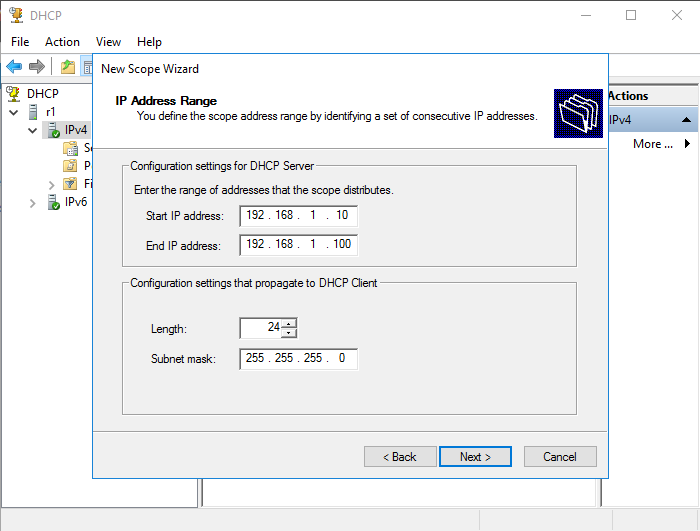
*Hình 5-1: Cài dịch vụ DHCP*

* Tiến hành cấu hình DHCP

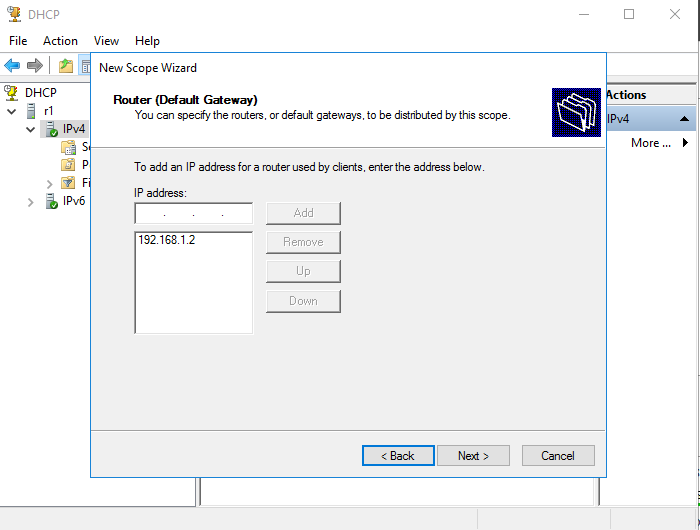
*Hình 5-2: Cấu hình Scope*



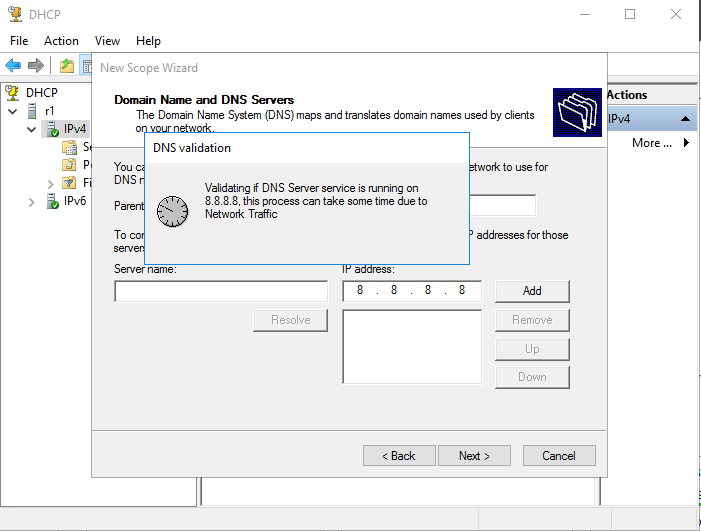
*Hình 5-3: Đặt tên cho Scope*



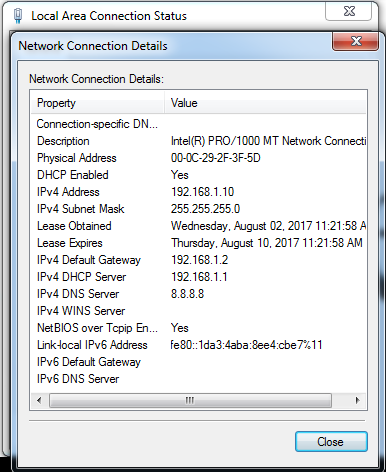
*Hình 5-4: Cấu hình lớp mạng cho Scope*



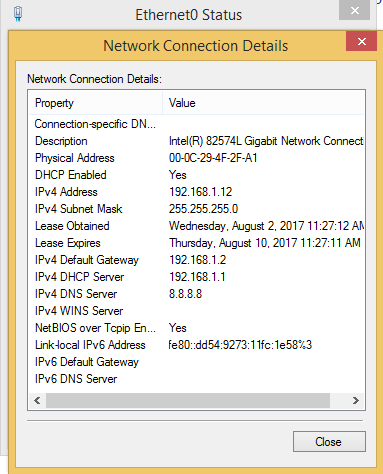
*Hình 5-5: Trỏ Default Gateway*



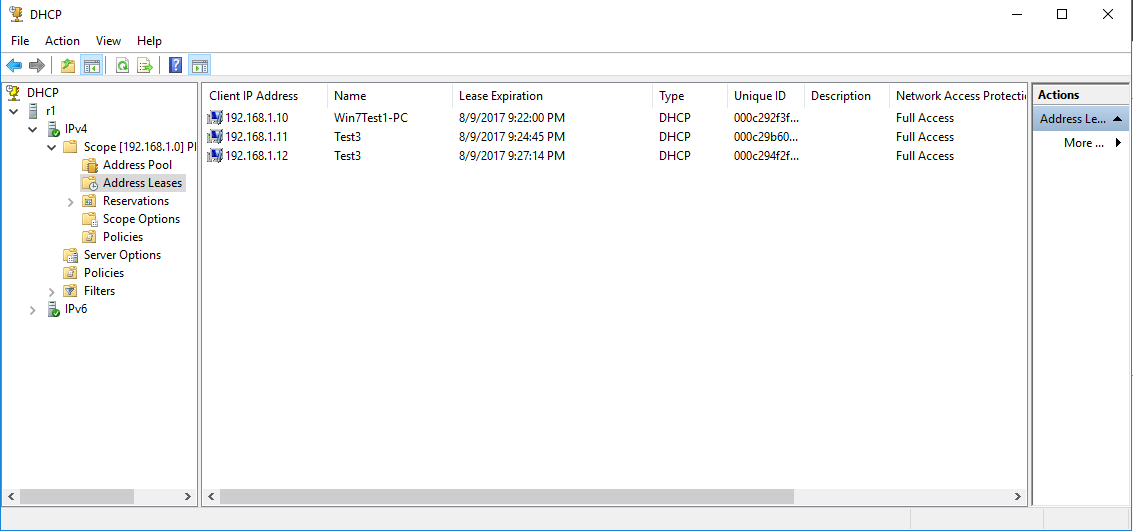
*Hình 5-6: Cấu hình Prefer DNS*



*Hình 5-7: Máy Client nhận IP được cấp*

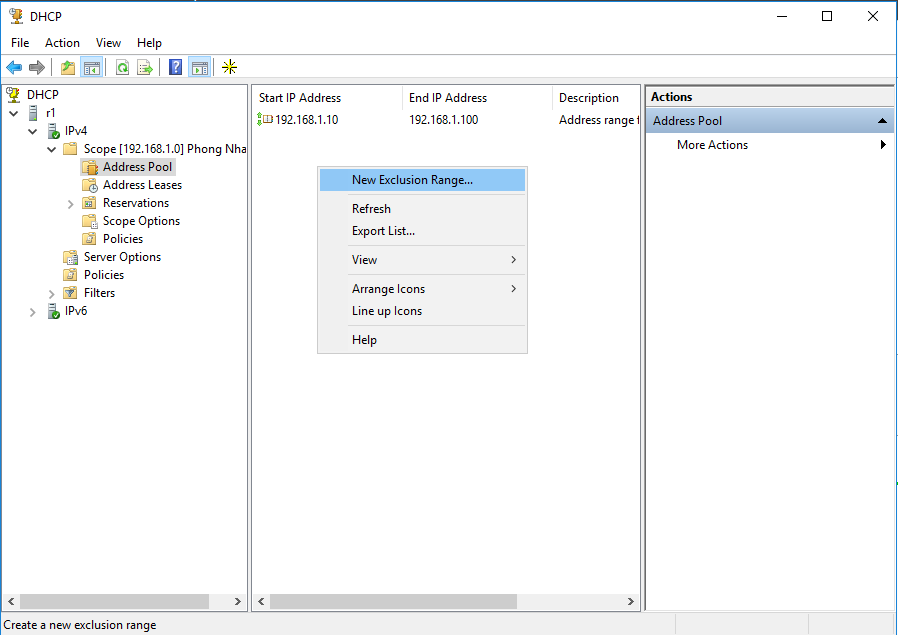


*Hình 5-8: Máy Client thứ 2 nhận IP*

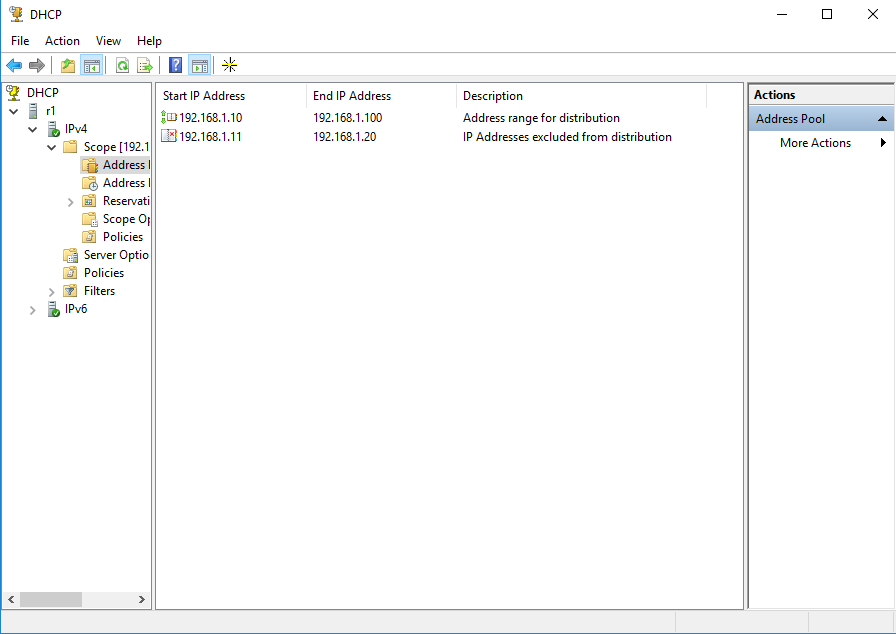


*Hình 5-9: Dịch vụ DHCP quản lý các máy con*

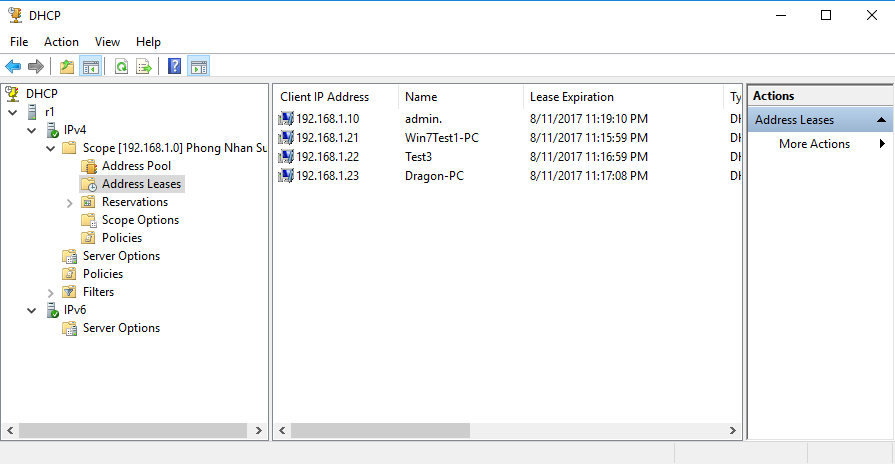
* Trong dãy địa chỉ IP cấp phát là 192.168.1.10 – 192.168.1.100 thì ta không cho cấp phát dãy từ 192.168.1.11 - 192.168.1.20



*Hình 5-10: Cấu hình Exclusion*

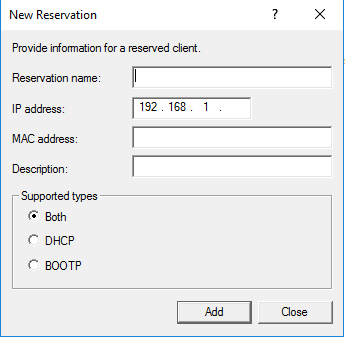


*Hình 5-11: Cấu hình ip và chặn*

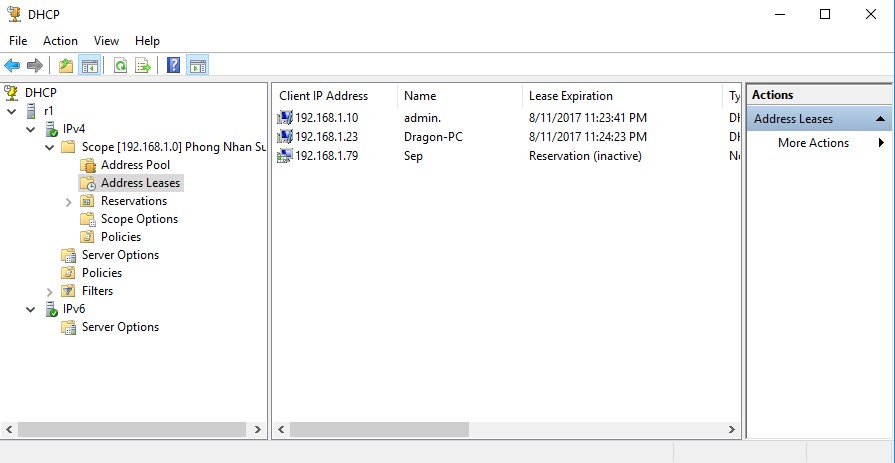


*Hình 5-12: Dãy IP bị bặn không được cấp phát*

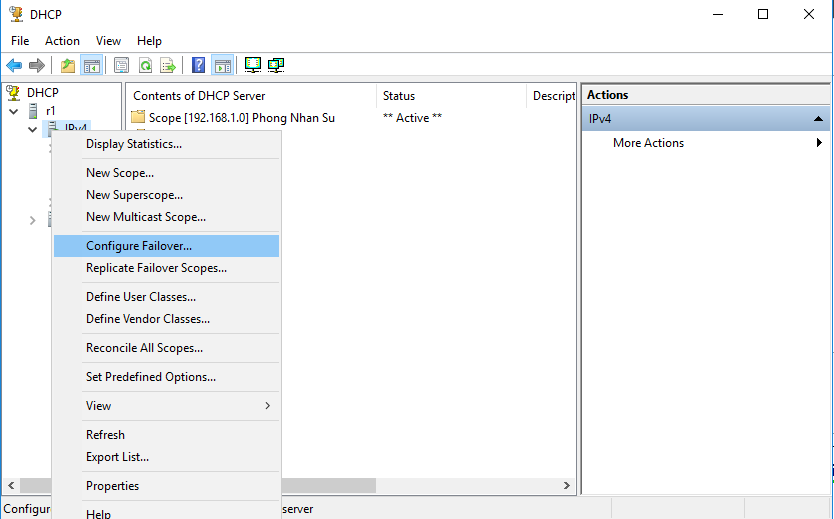
* Để cấp phát địa chỉ IP cho một máy cố định thì ta tiến hành chọn vào Revervation -> chọn new Reservation  Nhập tên vào Reservation, IP cần cấp cho máy đó ở ô IP, MAC address: nhập MAC của máy cần cấp IP cố định



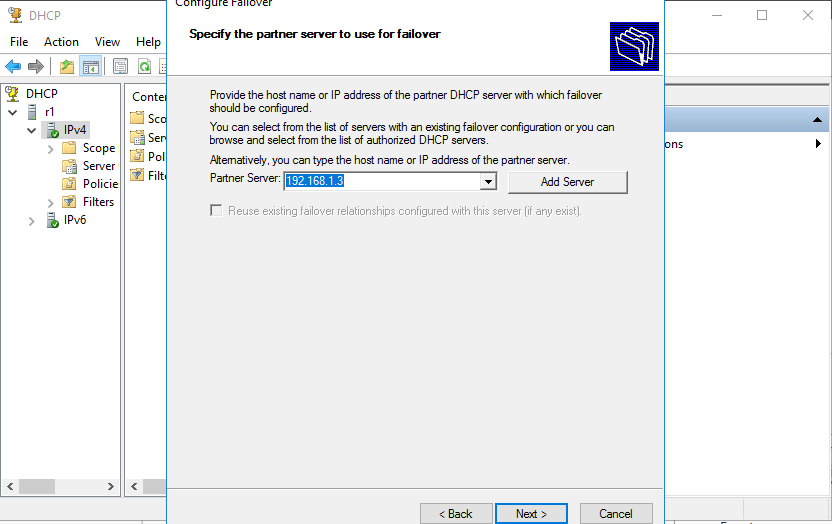
*Hình 5-13: Gán IP cố định cho một máy dựa vào MAC*



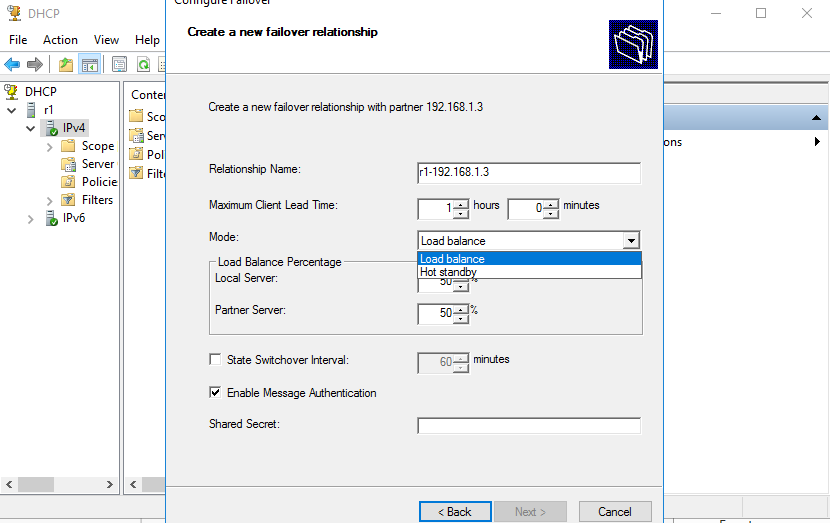
*Hình 5-14: Cấu hình IP cố định cho một PC*

* Thực hiện cấu hình cân bằng tải và dự phòng cho DHCP

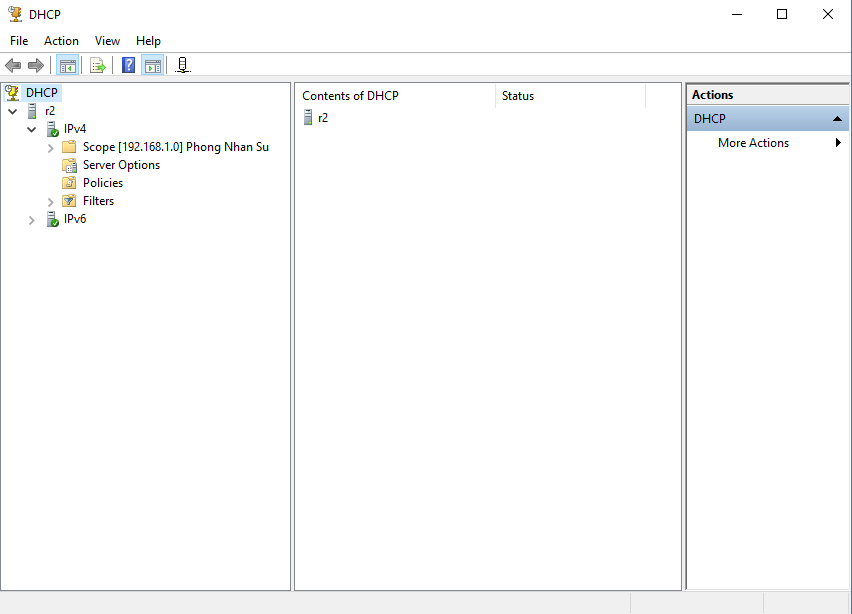
*Hình 5-15: Cấu hình Failover*



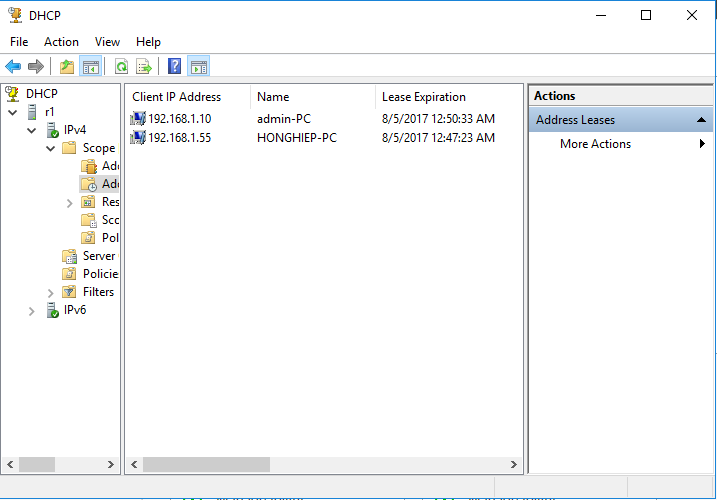
*Hình 5-16: cho biết Server Phụ*

* Chọn cơ chế 50% thì dãy địa chỉ IP sẽ chia làm hai. Nữa đầu do server chính cấp, nữa sau do server phụ cấp. Khi một DHCP nào mất kết nối thì Server còn lại sẽ đảm nhận cấp hết địa chỉ IP cho hệ thống mạng

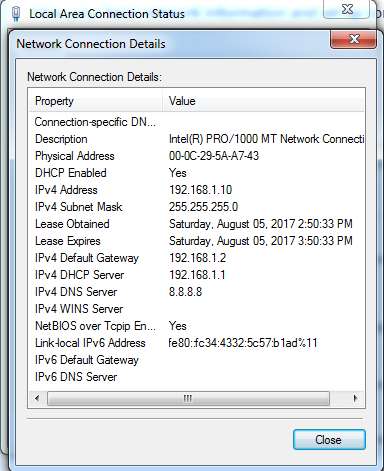
*Hình 5-17: Chọn chế độ cho 2 DHCP*



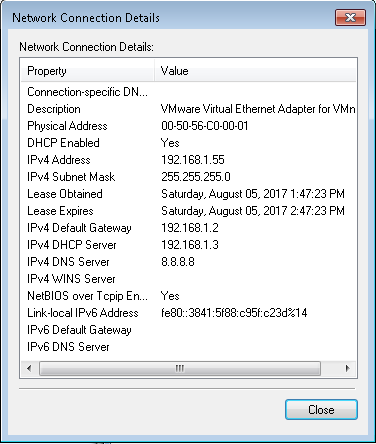
*Hình 5-18: Server phụ đã nhận được thông tin từ Server chính*



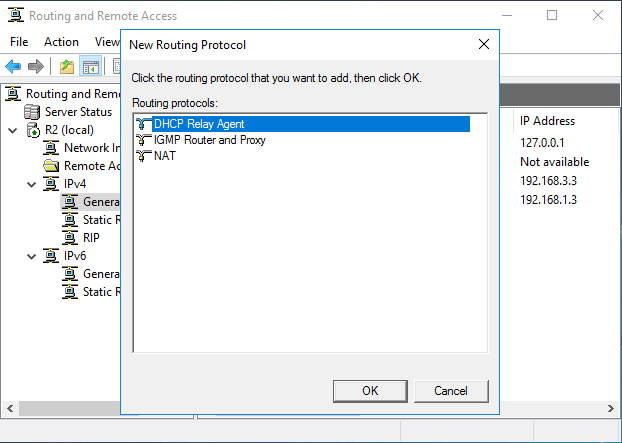
*Hình 5-19: Quá trình cấp phát IP đã thành công*



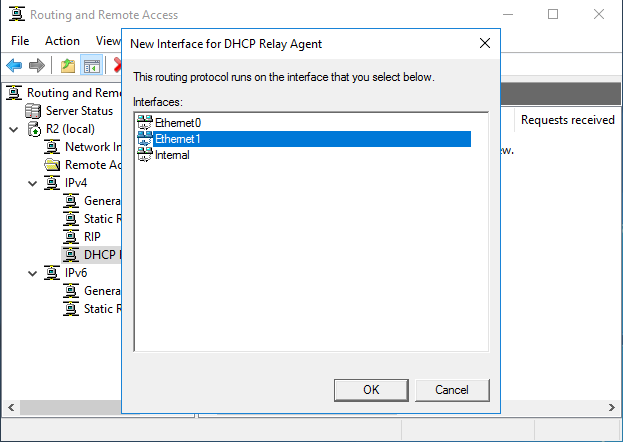
*Hình 5-20: Máy Client nhận được IP do DHCP chính cấp*



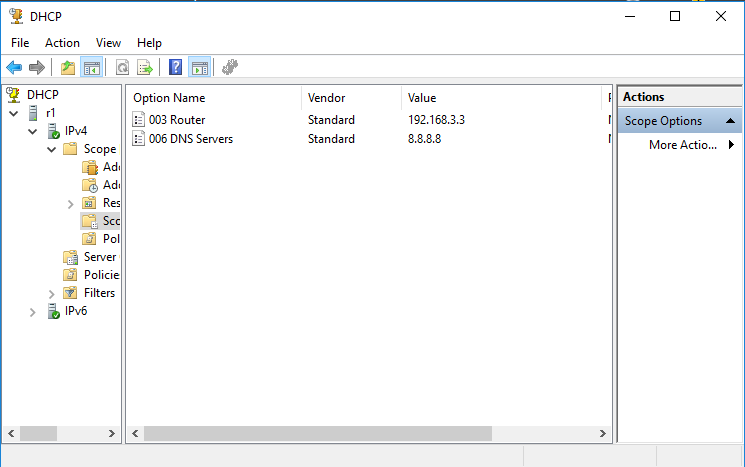
*Hình 5-21: IP được cấp từ DHCP Phụ cấp*

* Cấu hình DHCP Relay Agent. Trong bài này ta sẽ dùng DHCP ở một network này để cấp IP cho network khác thông qua Server DHCP relay Agent. Trước khi làm bài này thì ta phải thực hiện định tuyến cho hệ thống mạng

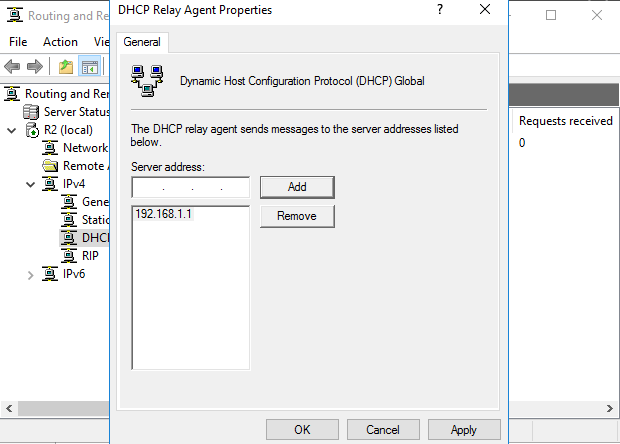
*Hình 5-22: Cấu hình Relay Agent*

* Chọn cổng mà cần cấp IP cho hệ thống mạng trên Relay Agent

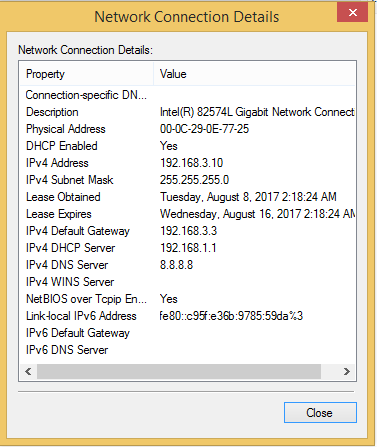
*Hình 5-23: Chọn cổng để nhận IP từ DHCP*

* Cấu hình DNS và Default gateway cho hệ thống của mạng cần cấp

*Hình 5-24: Cấu hình Default Gateway*

* DHCP Relay agent trỏ về DHCP chính

*Hình 5-25: Nhập địa chỉ IP của DHCP*



*Hình 5-26: Đã nhận IP từ DHCP thông qua Relay Agent*

# Dịch vụ Web

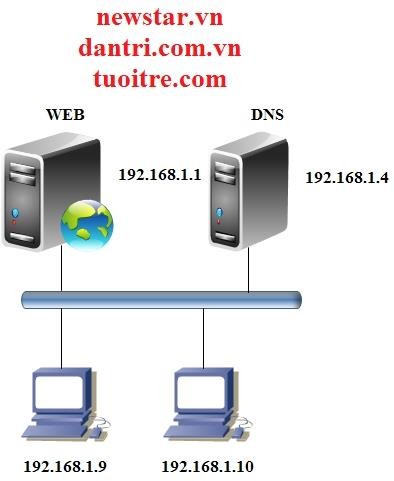
*Sau khi học xong bài này thì học viên có khả năng xây dựng website để cho người dùng truy cập vào. Trong bài này chúng ta thực hiện xây dựng nhiều website cùng lúc trên cùng một Server Web*

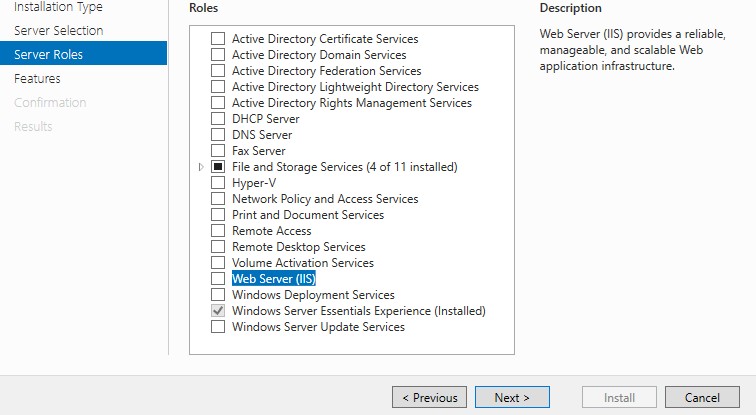
* + Chuẩn bị:

+ Hai máy windows server 2016

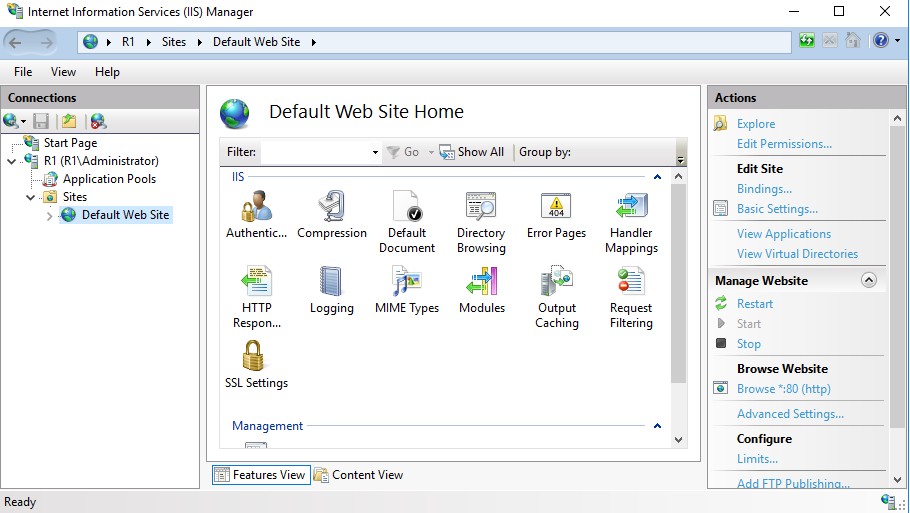
+ Hai máy Client Windows 7

* + Mô hình

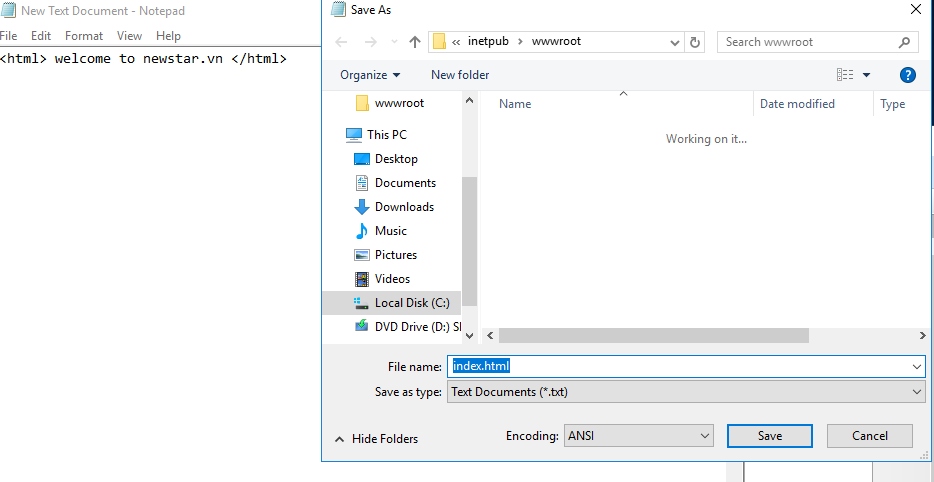


* + Kết quả đạt được
* Phân giải được cả 3 website newstar.vn, dantri.com.vn , tuoitre.com
  + Thực hiện
* Tiến hành cài đặt dịch vụ Web

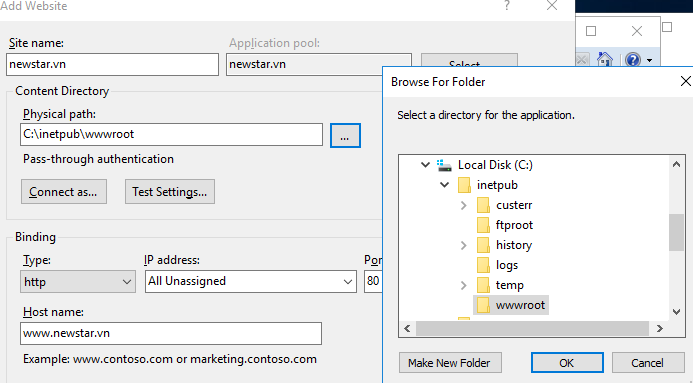
*Hình 6-1: Cài IIS*



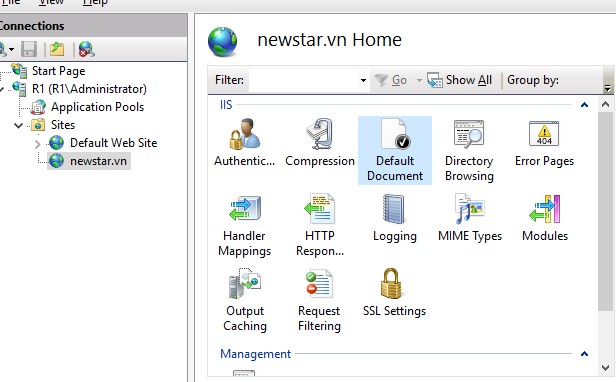
*Hình 6-2: Giao diện IIS*



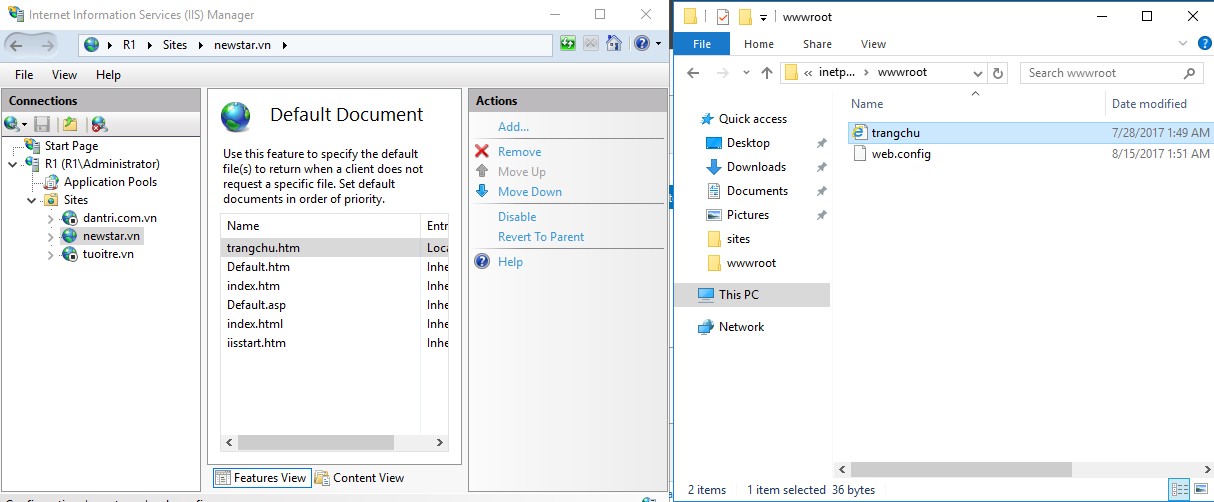
*Hình 6-3: Tạo Website*



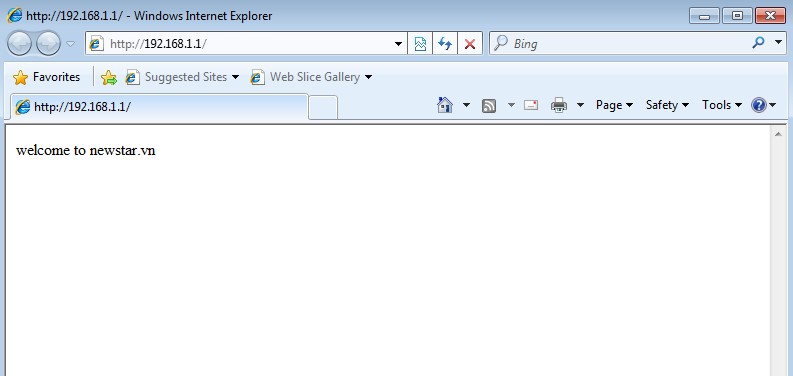
*Hình 6-4: Chọn đường dẫn Website*



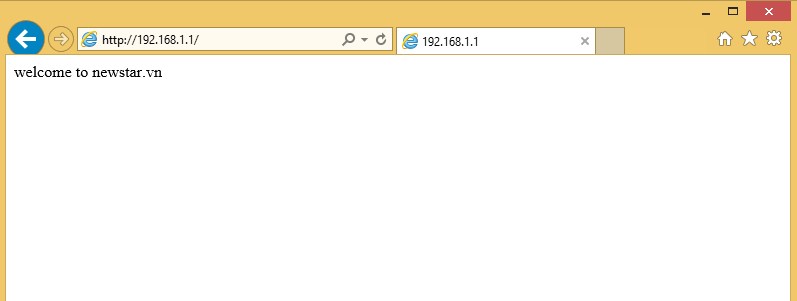
*Hình 6-5: Cấu hình Default Document*

* Mặc định trên Default Document của IIS có những tên bên dưới. Nếu ta muốn lấy tên Trangchu.html thì ta phải vào đó thêm name vào thì mới sử dụng được

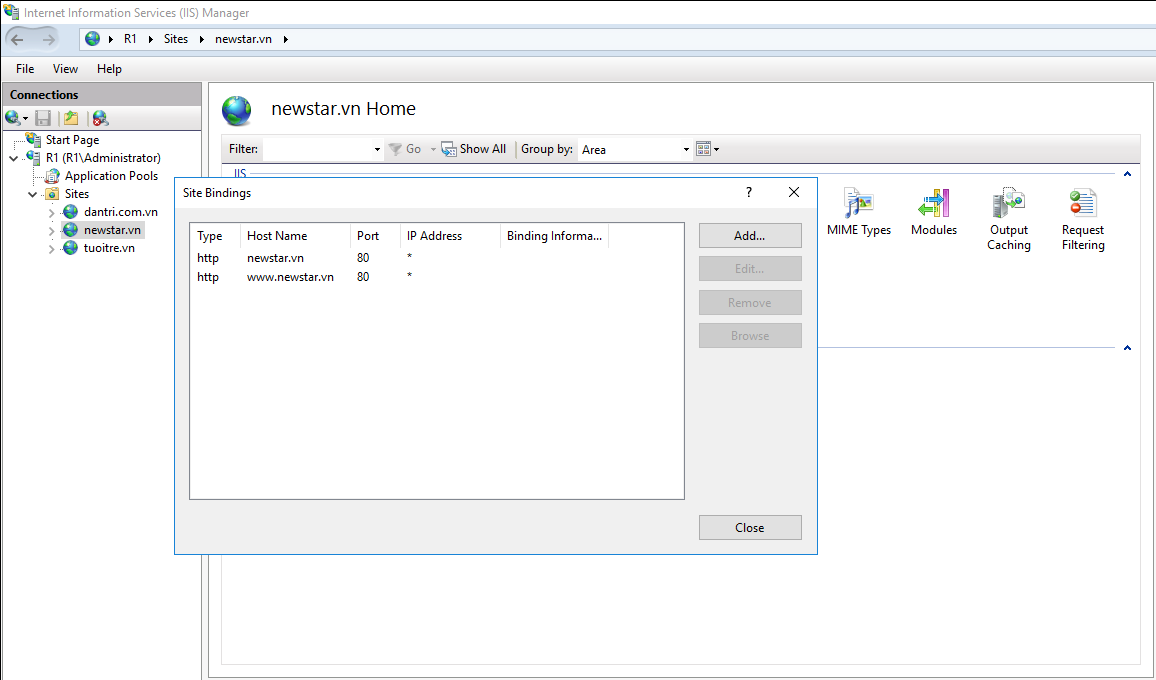
*Hình 6-6: Cấu hình tên của Website khi boot*



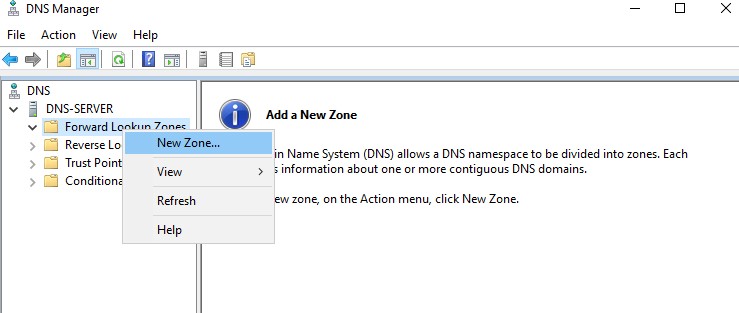
*Hình 6-7: Máy Client truy cập vào IP của Web*



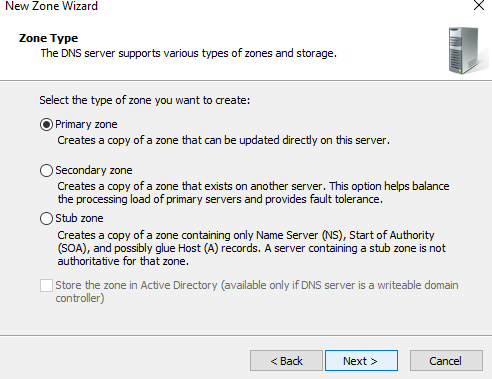
*Hình 6-8: Máy win 8 đăng nhập vào Web bằng IP*

* Tiến hành cho phép website truy cập bằng Tên hay thế địa chỉ IP

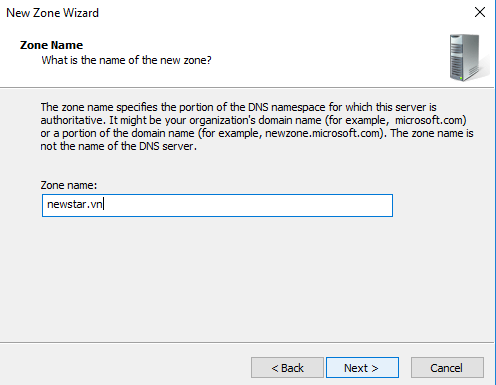
*Hình 6-9: Cấu hình chạy web chạy bằng tên*



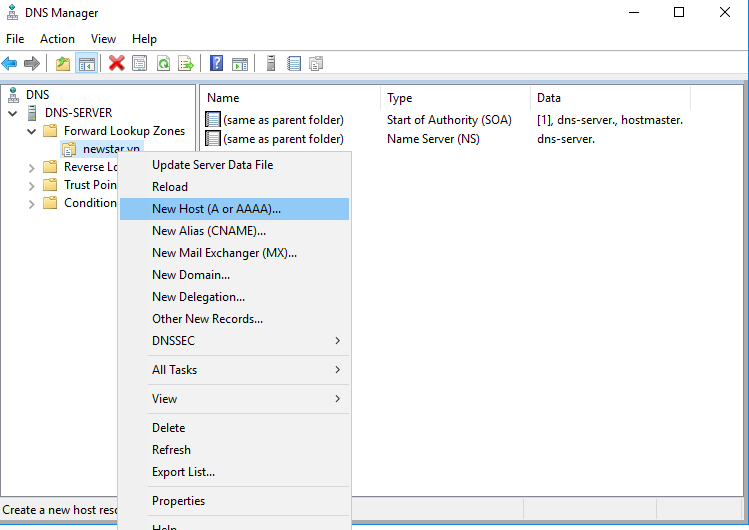
*Hình 6-10: Cấu hình DNS cho Website*



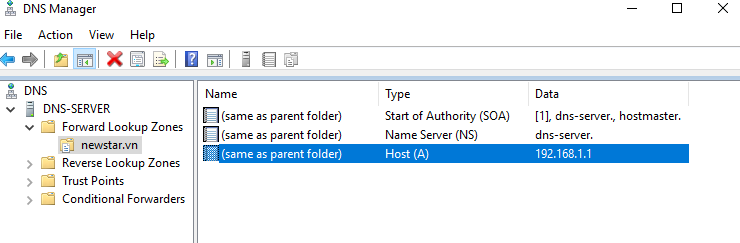
*Hình 6-11: Cấu hình Primary*



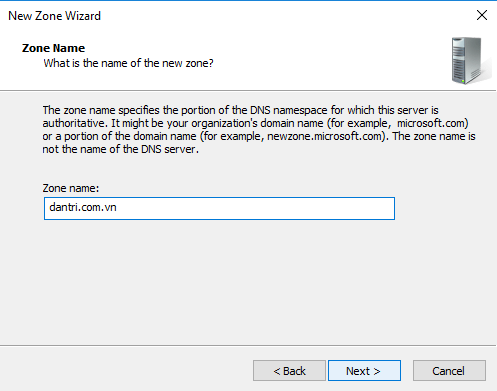
*Hình 6-12: Cấu hình tên cho website*



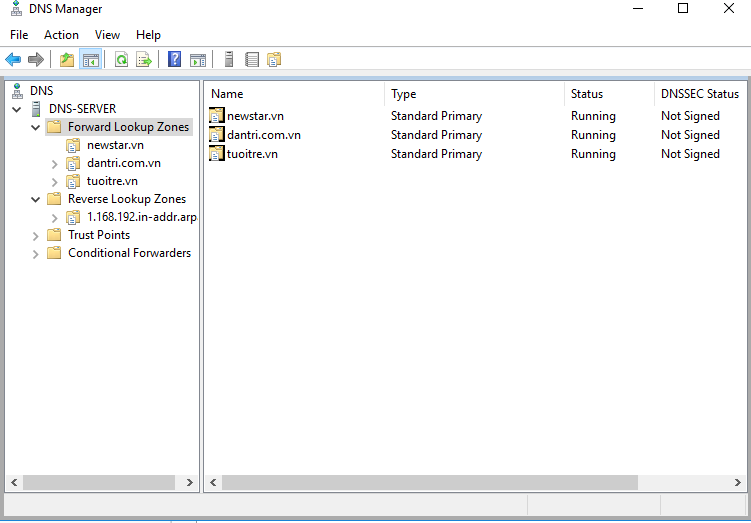
*Hình 6-13: Cấu hình host*



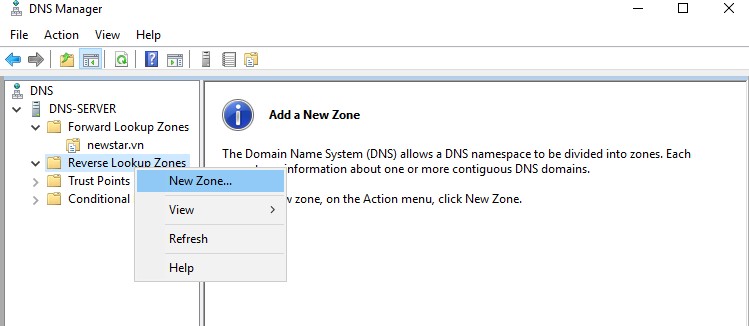
*Hình 6-14: Cấu hình tên miền Newstar*



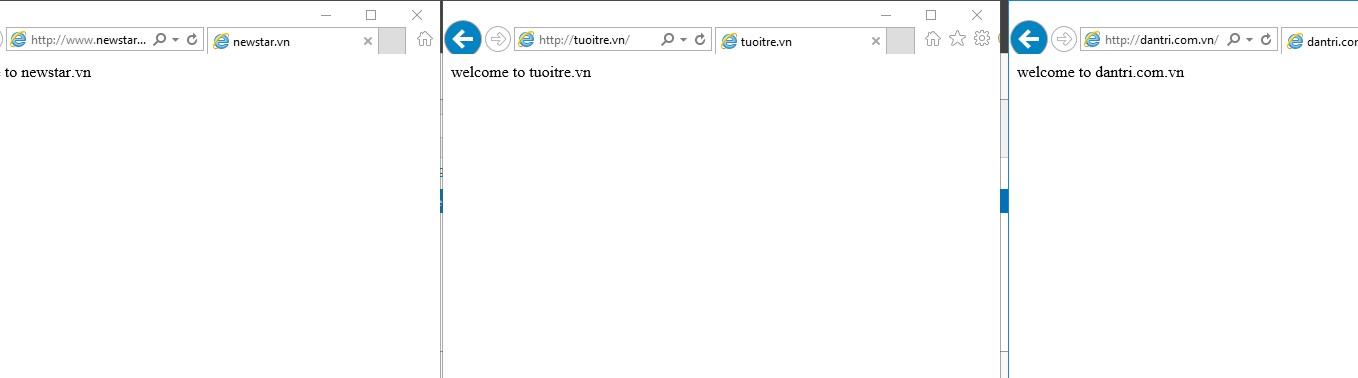
*Hình 6-15: Cấu hình Zone dantri.com.vn*



*Hình 6-16: Các Zone DNS đã được tạo*



*Hình 6-17: Tạo Reverse Lookup Zone*

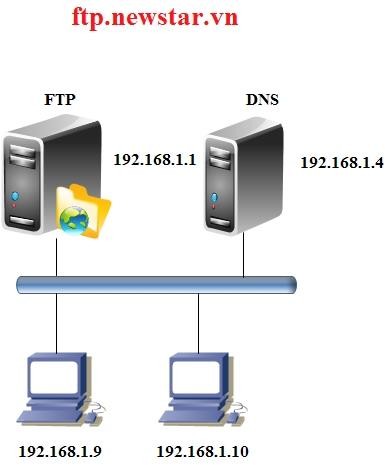


*Hình 6-18: Truy cập vào các trang web đã tạo*

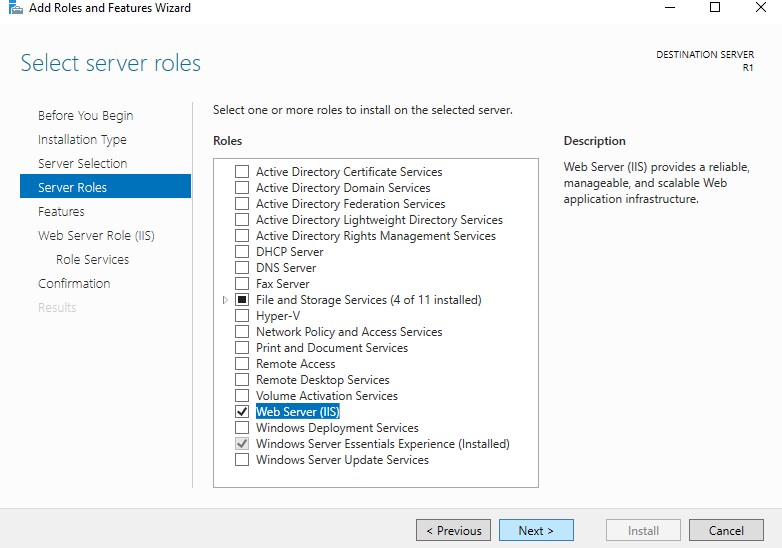
# Dịch vụ FTP

*Sau khi học xong bài này thì học viên có khả năng xây dựng một hệ thống FTP cung cấp tài liệu cho người dùng nội bộ và internet. Trong bài này ta sẽ dùng DNS để phân giải tên miền*

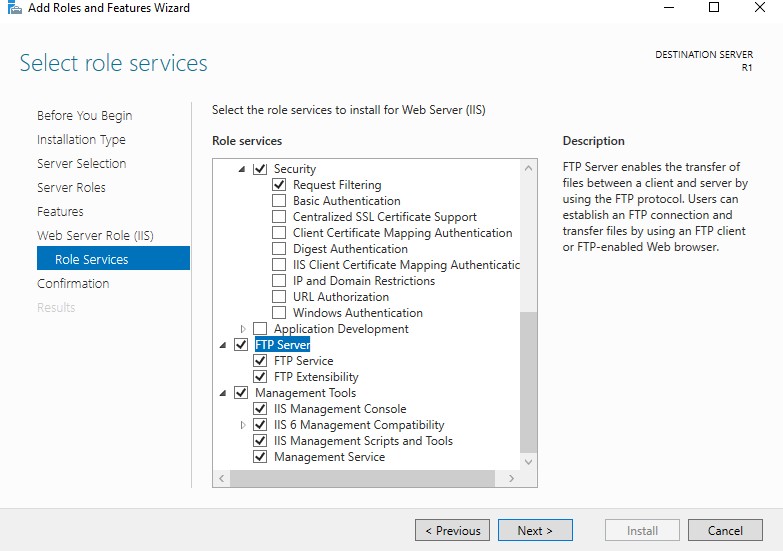
* + Chuẩn bị:
* Hai máy server 2016
* Hai máy Client Win 7
  + Mô hình



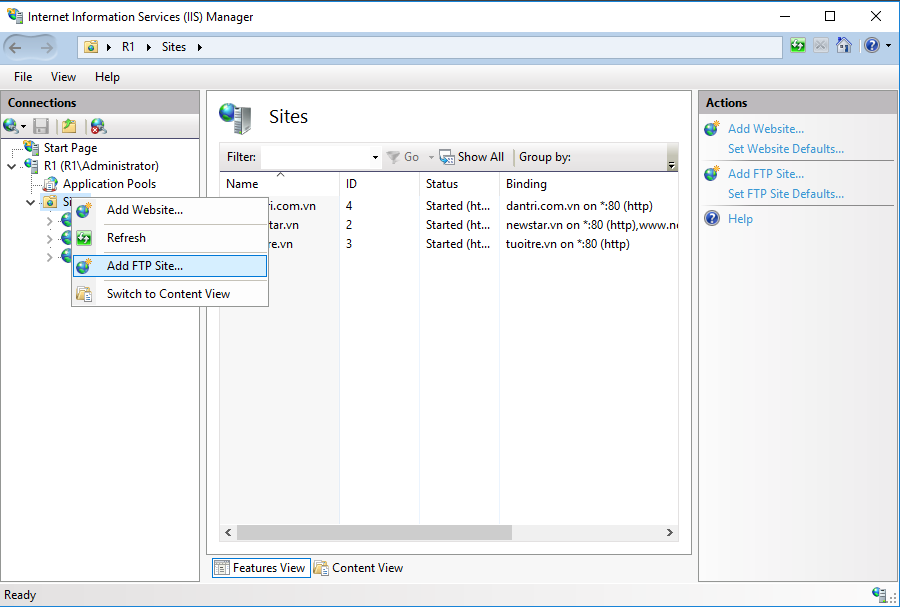
* + Kết quả đạt được
* Máy client truy cập được vào ftp://ftp.newstar.vn
  + Thực hiện
* Thực hiện cài dịch vụ FTP. Dịch vụ này nằm trong Webserver. Ta chọn vào Webserver  chọn next để Chọn FTP Server (Chọn cả 2 dấu check con trong đó)



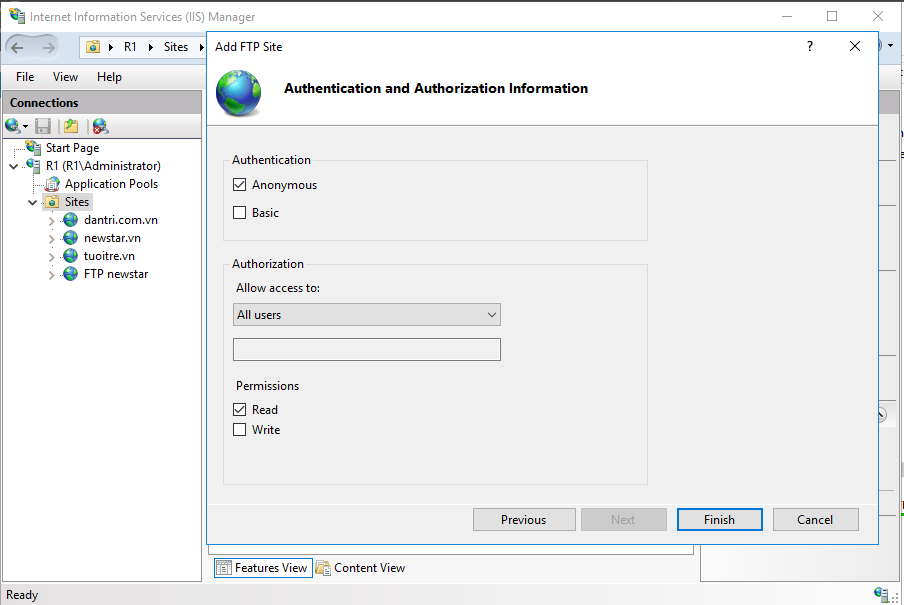
*Hình 7-1: Cấu hình dịch vụ Web*



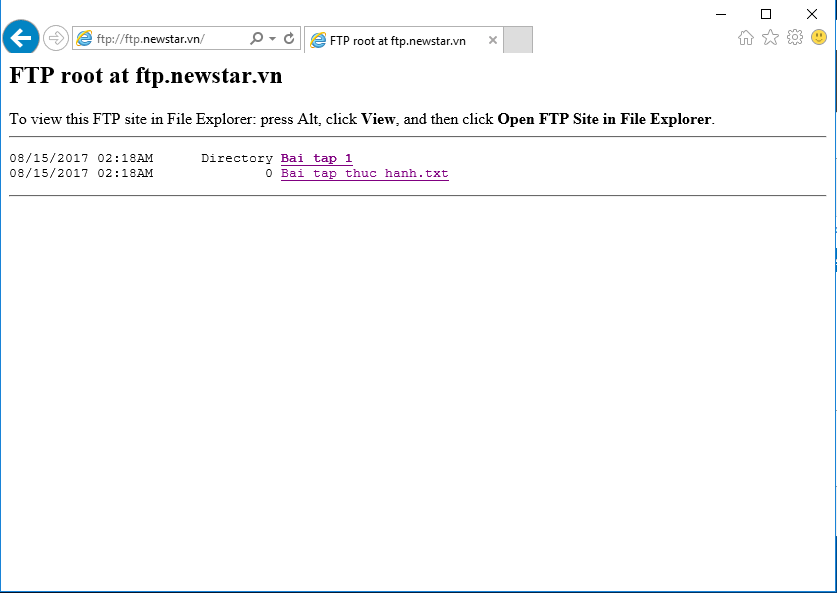
*Hình 7-2: Cấu hình FTP*

* Mở IIS tiến hành add dịch vụ FTP

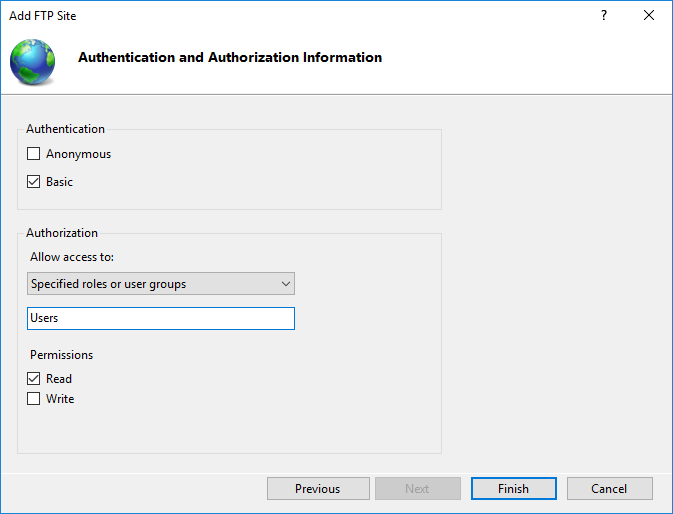
*Hình 7-3: Add FTP*

* Để cho các user có thể truy cập vào FTP thì ta phải cho một quyền mặc danh cho họ là Anonymous

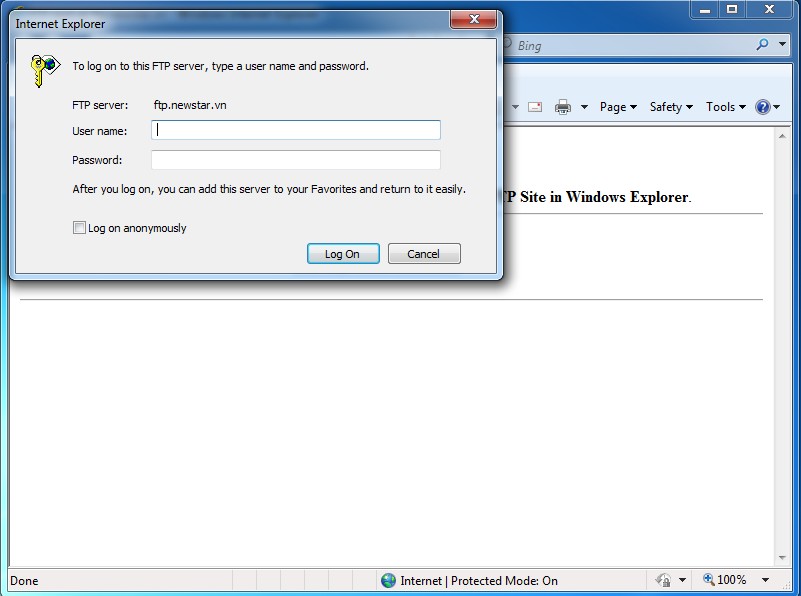
*Hình 7-4: Cấp quyền cho người truy cập*



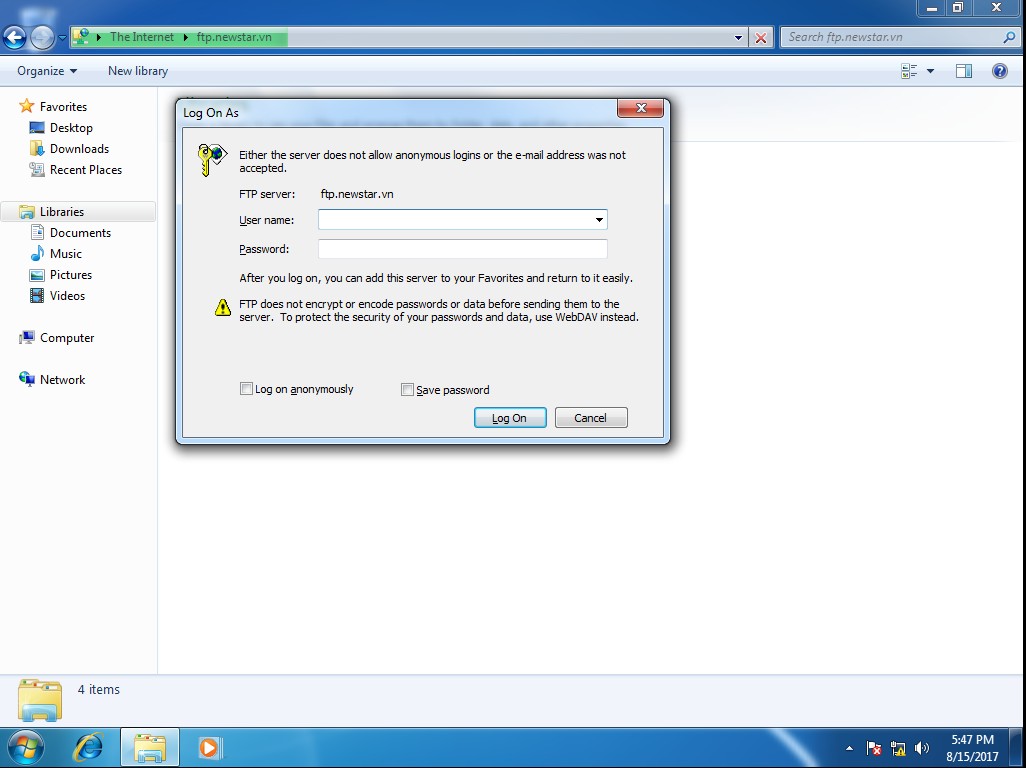
*Hình 7-5: Truy cập FTP thành công*

* Muốn xây dựng FTP mà có tài khoản mới truy cập được thì dùng chính sách Basic kèm theo tài khoản cho phép. Tài khoản này được tạo trên Server File Service.

*Hình 7-6: Cấu hình truy cập có tài khoản*

* Trong quá trình truy cập FTP ta có thể truy cập trên trình duyệt web hoặc trên Windows Exploror

*Hình 7-7: Đăng nhập tài khoản trên web*



*Hình 7-8: Đăng nhập tài khoản trên windows Exploror*

# Dịch vụ NAT

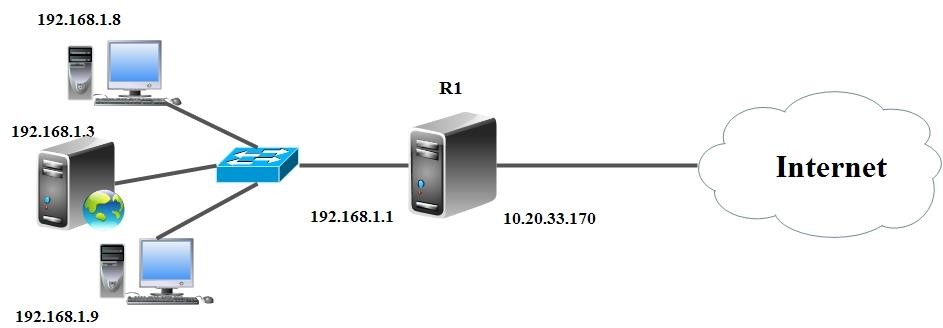
*Sau khi học bài này xong học viên có khả năng Nat các địa chỉ IP Private có thể kết nối Internet. Đồng thời NAT Server Web được truy cặp từ bên ngoài*

* + Chuẩn bị:

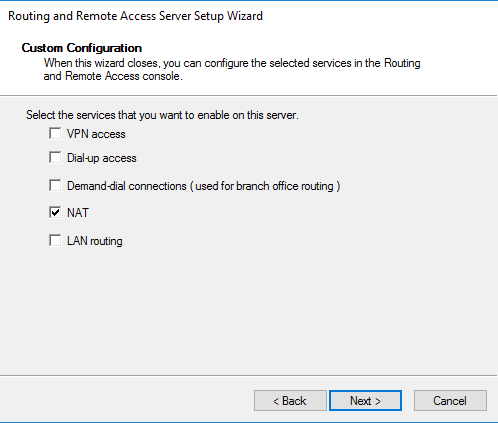
+ Hai máy server 2016

+ Hai máy Client windows 7

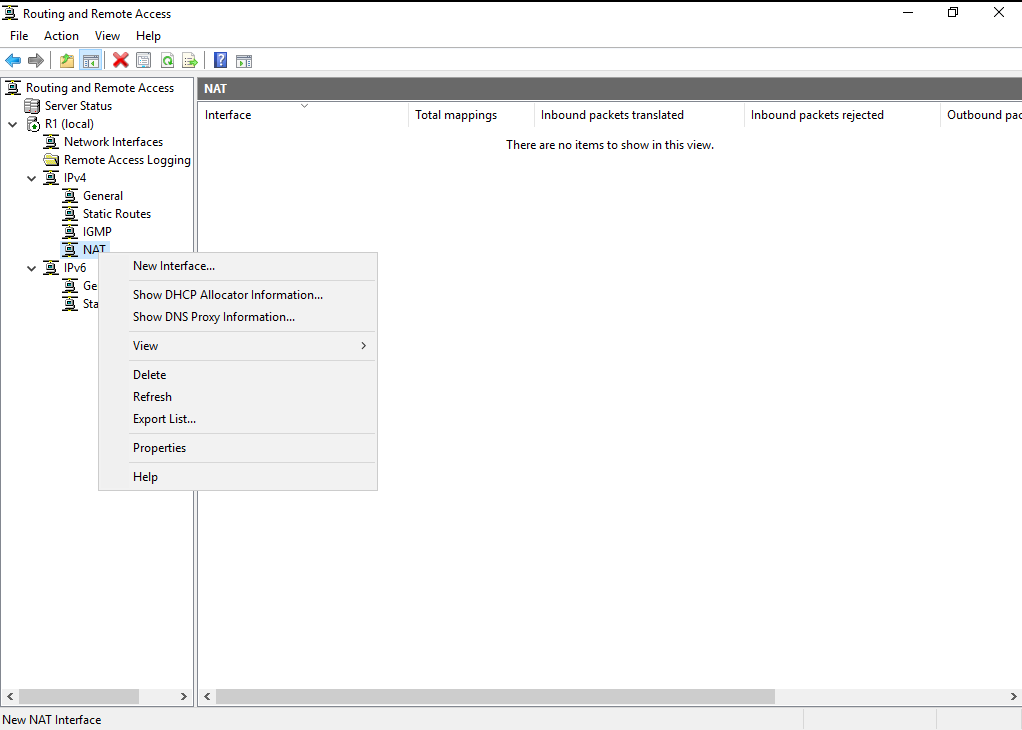
* + Mô hình



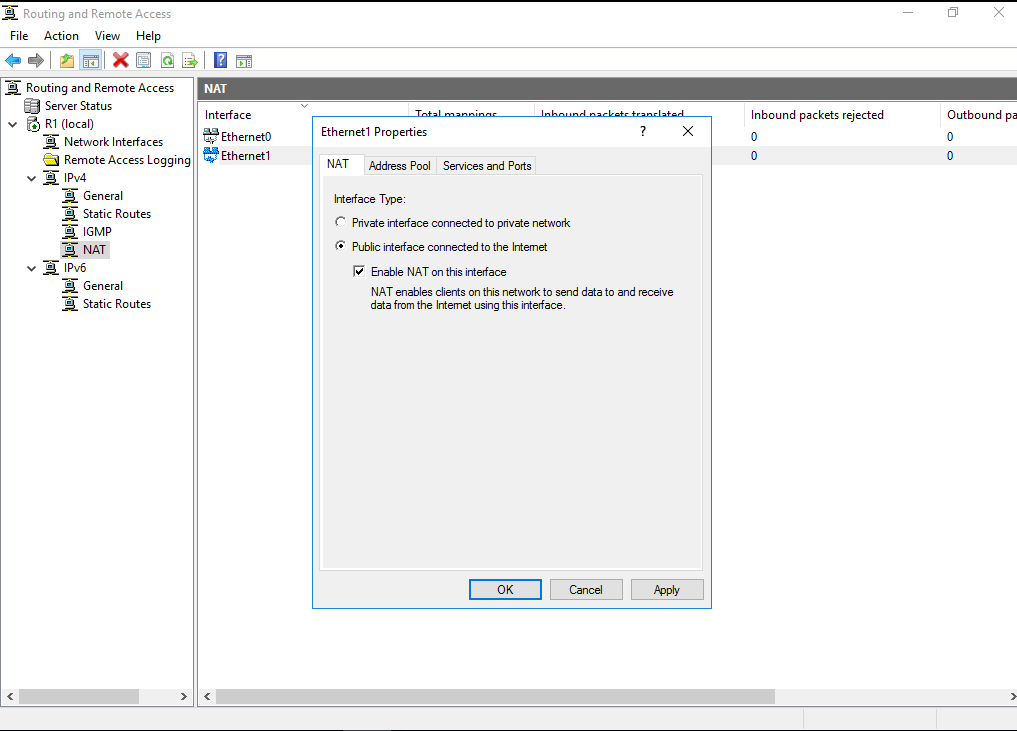
* + Kết quả đạt được
* Các máy client trong mạng nội bộ truy cập được internet và người dùng internet có thể truy cập vào website newstar.vn
  + Thực hiện
* Cài đặt dịch vụ NAT trong Routing and Remote Access



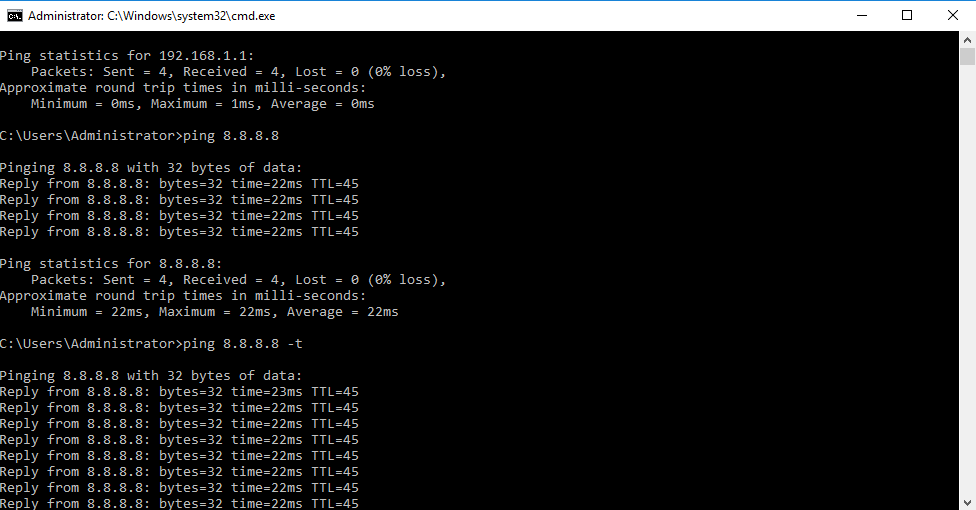
*Hình 8-1: Cấu hình NAT*

* Thêm cổng Private và Public cho Server NAT

*Hình 8-2: Thêm cổng*

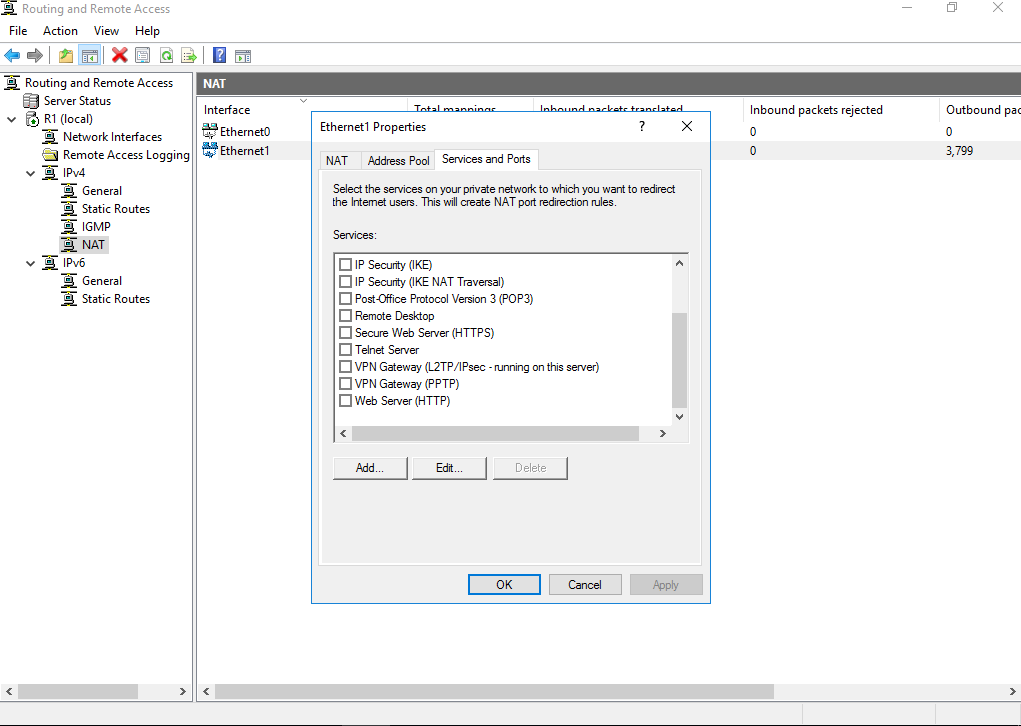


*Hình 8-3: Cấu hình Public và Private*

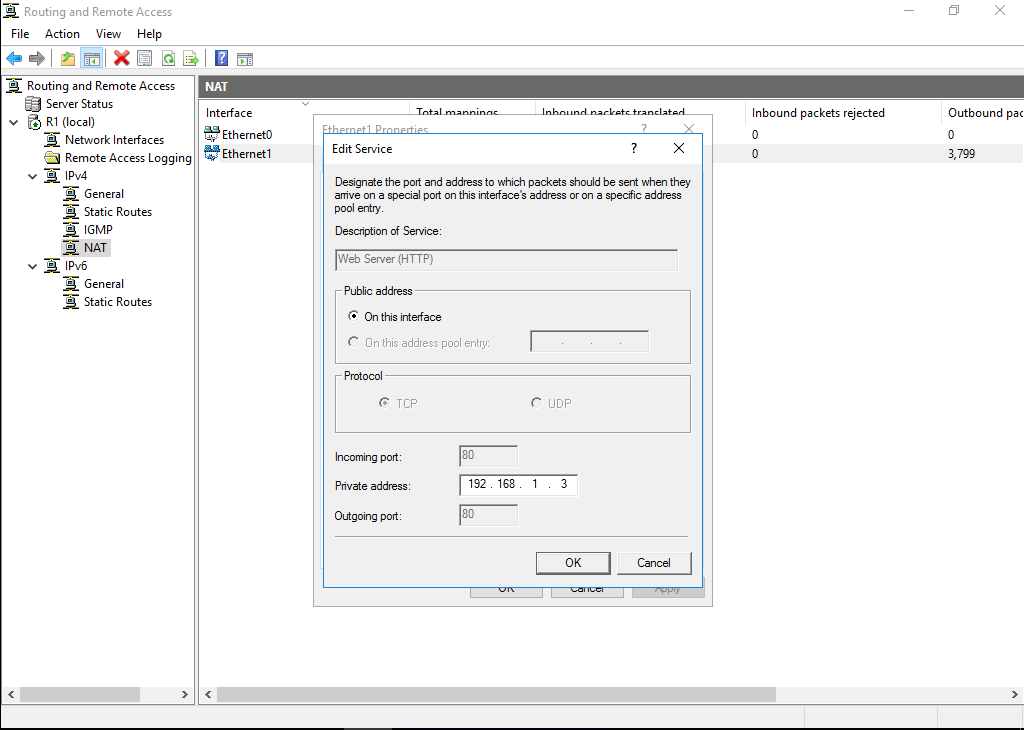


*Hình 8-4: Kiểm tra kết nối*

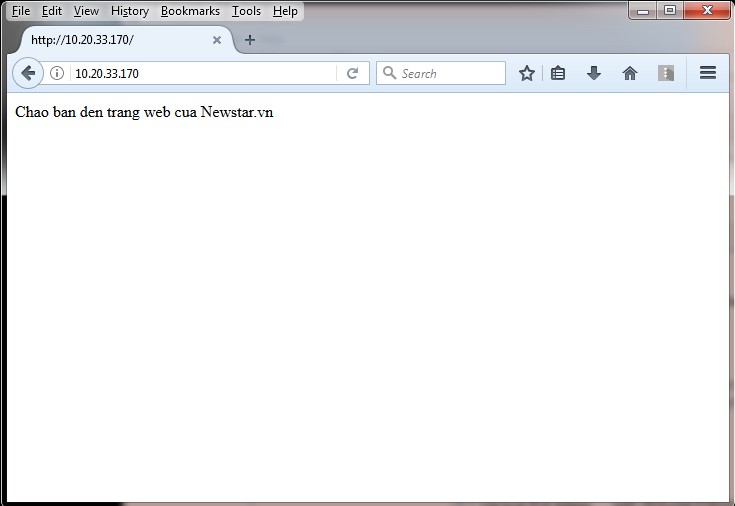
* Cần đưa website đưa ra cho người dùng ngoài Internet truy cập. Tiến hành NAT server web



*Hình 8-5: Cấu hình NAT website*



*Hình 8-6: Điền IP Server Private*



*Hình 8-7: Truy cập IP Public trên trình duyệt web*

# Windows Deployment service (WDS)

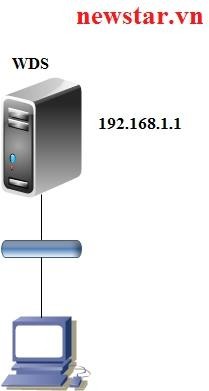
*Sau khi học bài này học viên có thể cài hệ điều hành cho các máy client thông qua Server đã có dịch vụ DHCP*

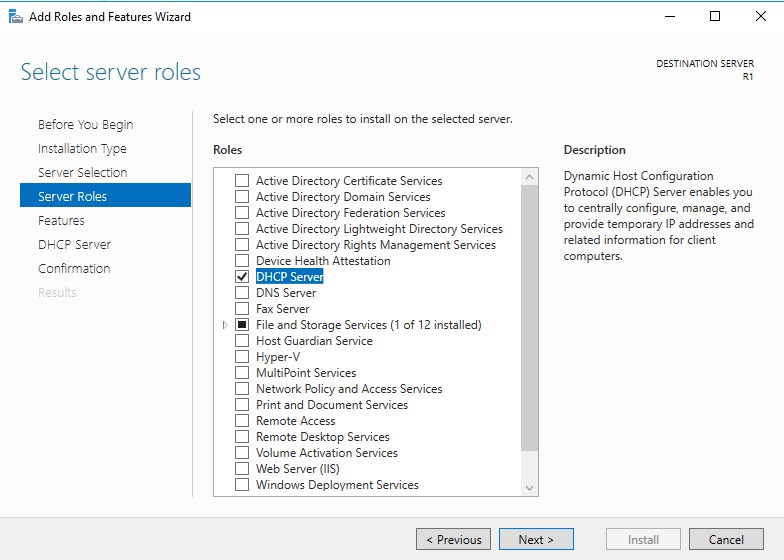
* + Chuẩn bị:

+ Một máy server 2016

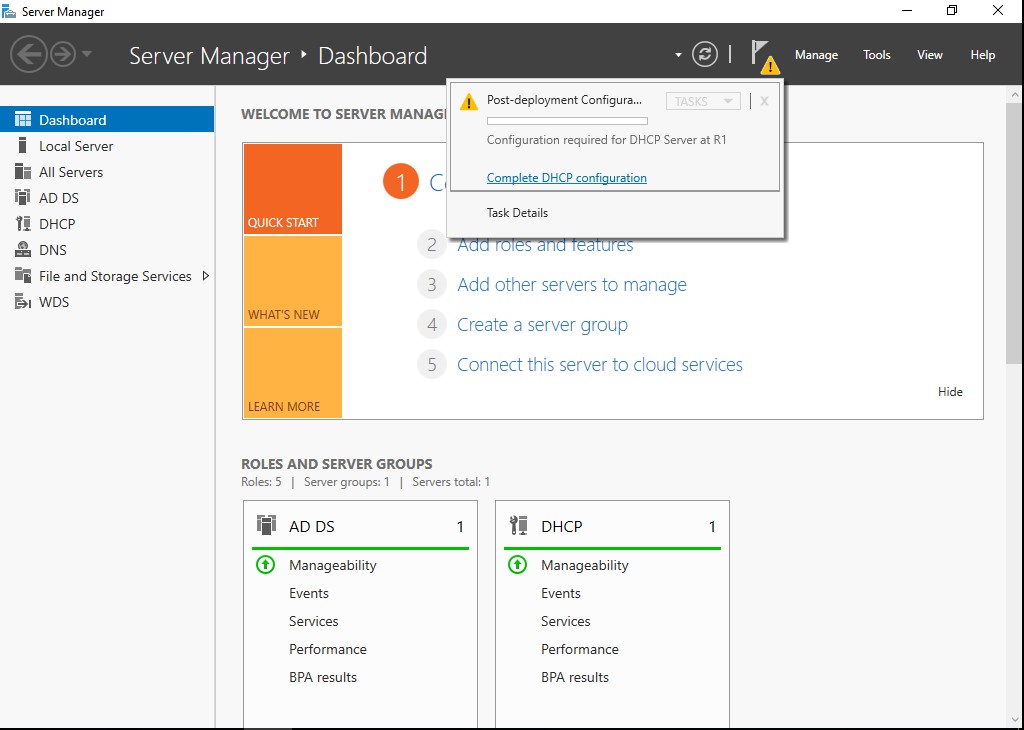
+ Một máy Client windows 7

* + Mô hình

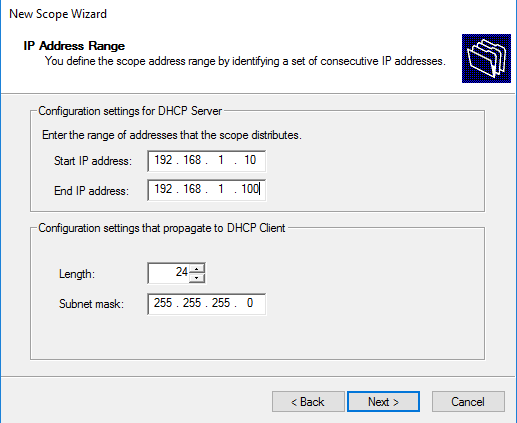


* + Kết quả đạt được
* Cài windows 7 tự động cho máy client thông qua WDS
  + Thực hiện
* Tiến hành cài đặt dịch vụ DHCP

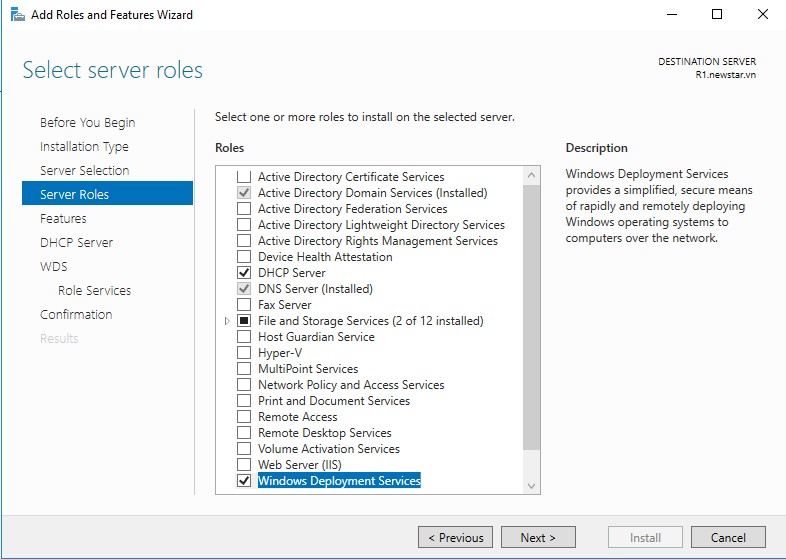
*Hình 9-1: Cài đặt dịch vụ DHCP*



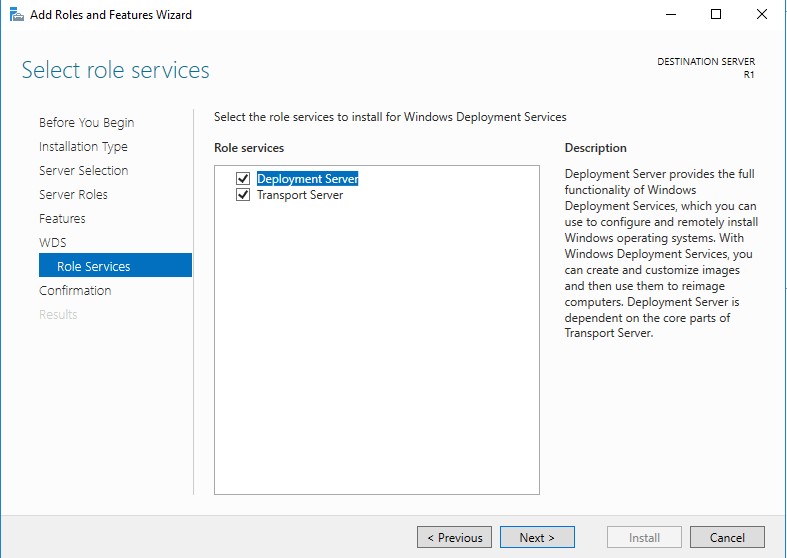
*Hình 9-2: Tùy chỉnh DHCP trên domain*



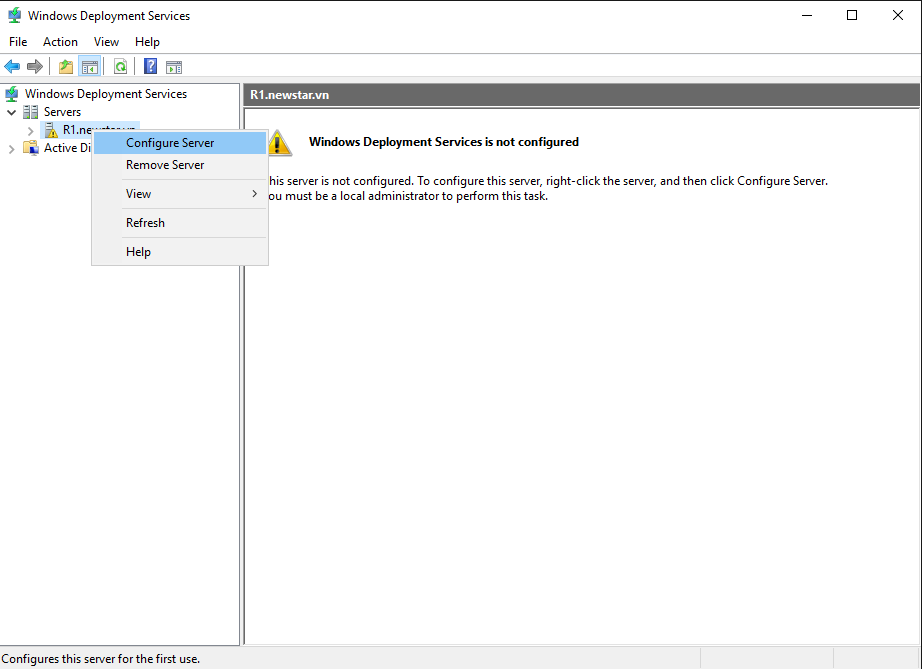
*Hình 9-3: Dãy Range cấp phát*

* Tiến hành cài đặt dịch vụ WDS

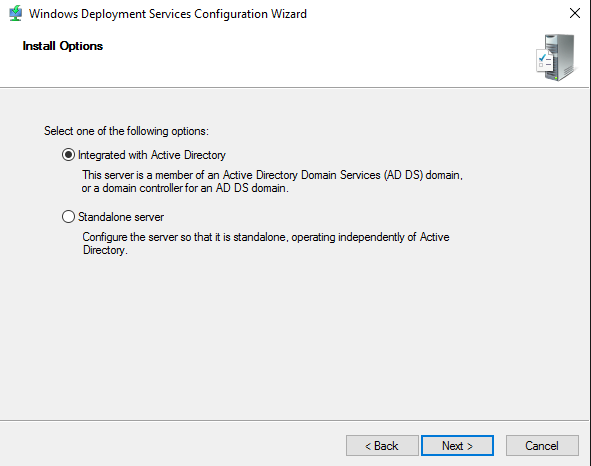
*Hình 9-4: Cài đặt dịch vụ WDS*



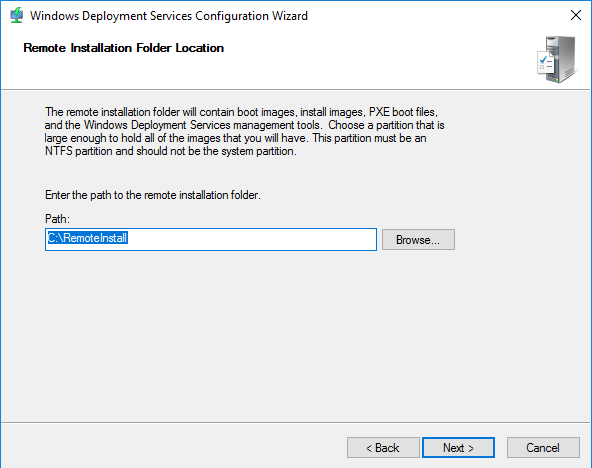
*Hình 9-5: Chọn cả 2 tùy chọn*



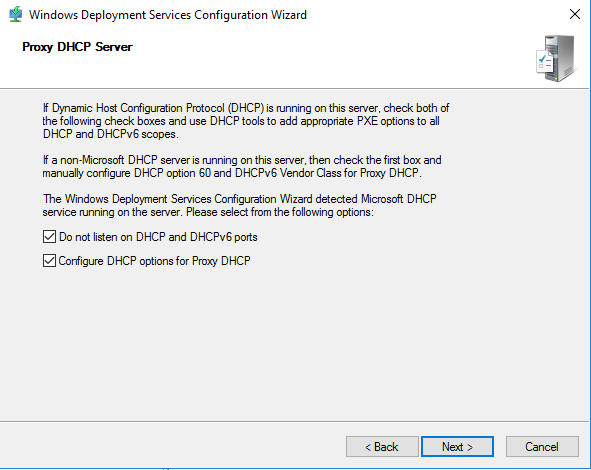
*Hình 9-6: Cấu hình WDS*



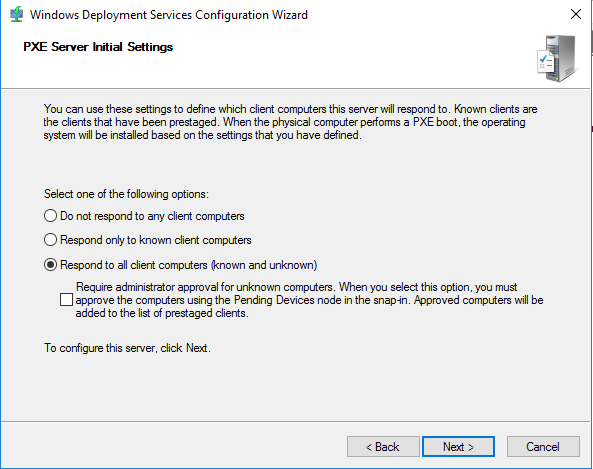
*Hình 9-7: Chọn chế độ domain*



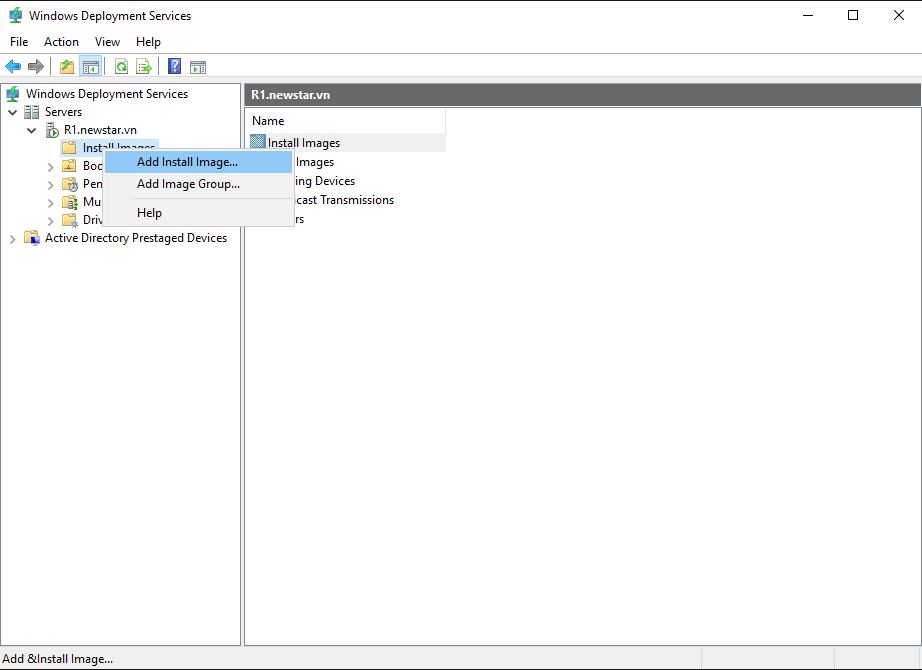
*Hình 9-8: Chỉ đường dẫn lưu file cài*



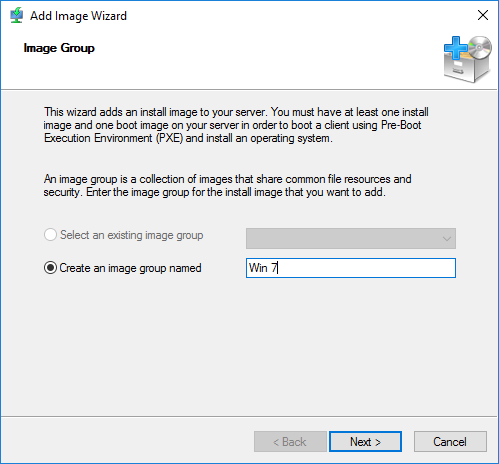
*Hình 9-9: Thiết lập DHCP*



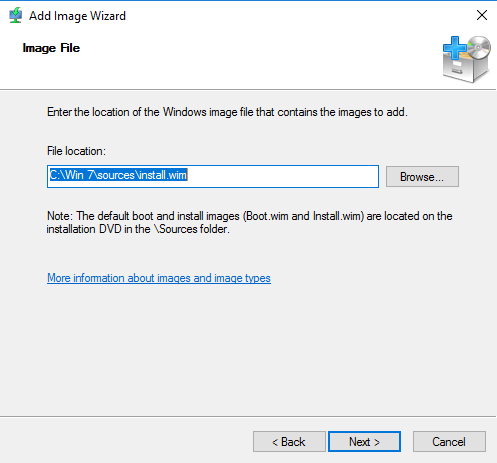
*Hình 9-10: Phản hồi cho tất cả các máy Client*



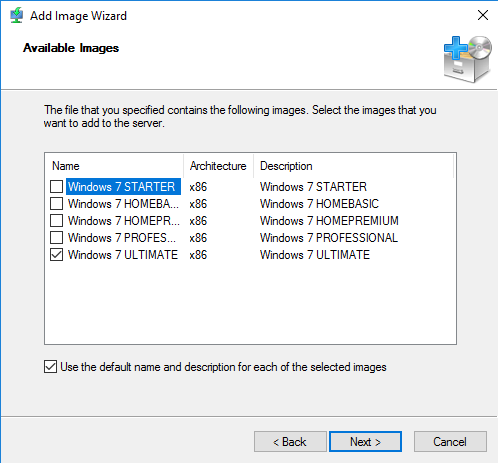
*Hình 9-11: Thêm file ảnh HDH*



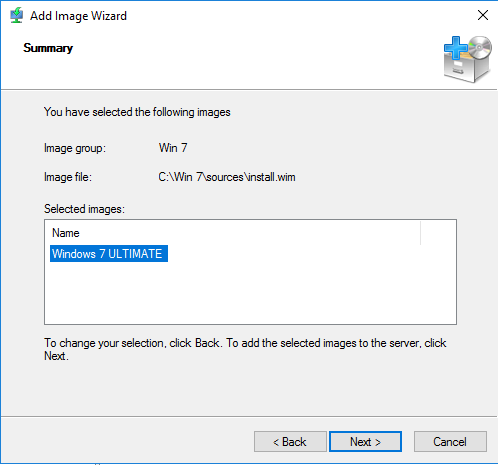
*Hình 9-12: Đặt tên cho Group HDH*



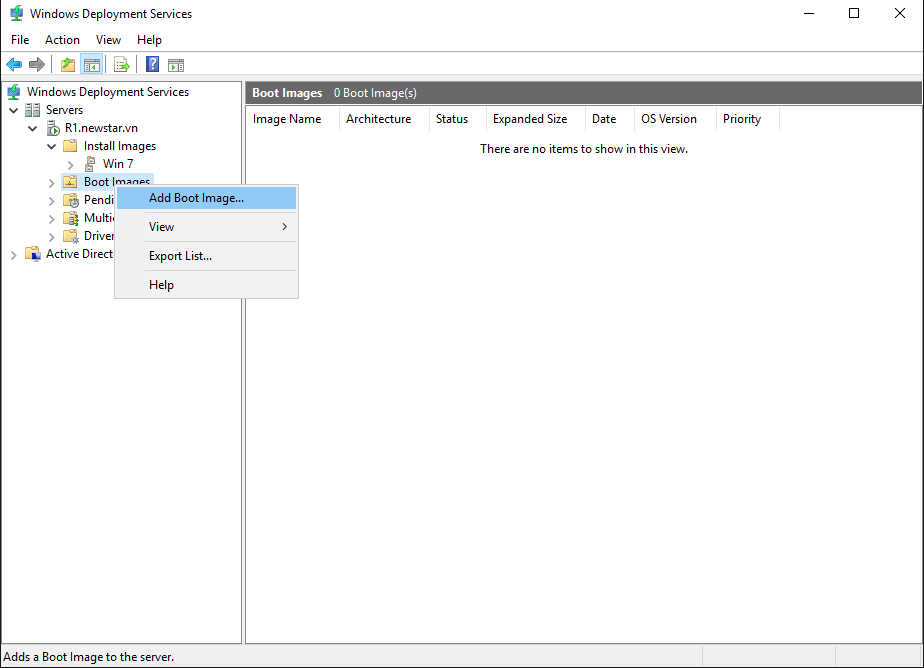
*Hình 9-13: Chọn File Intall*



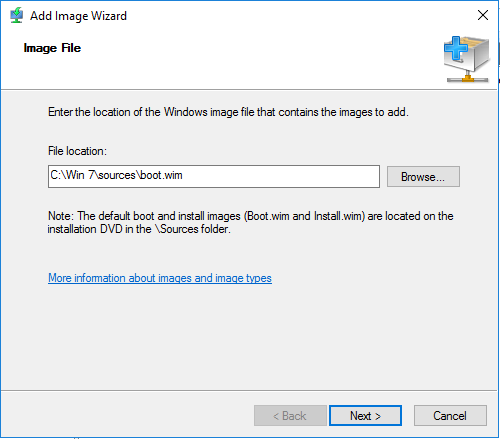
*Hình 9-14: Chọn HDH cần cài*



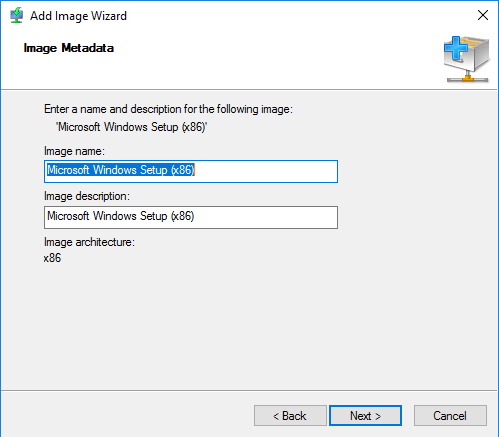
*Hình 9-15: Những HDH cài*



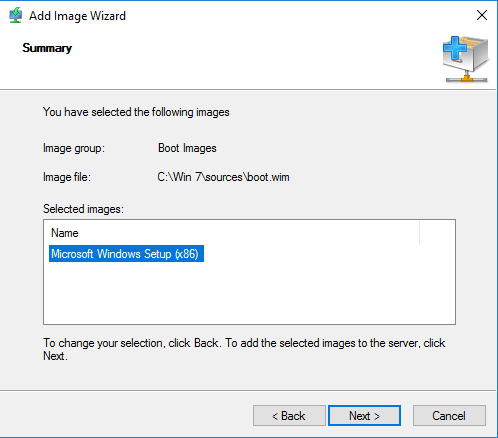
*Hình 9-16: Thêm file boot*



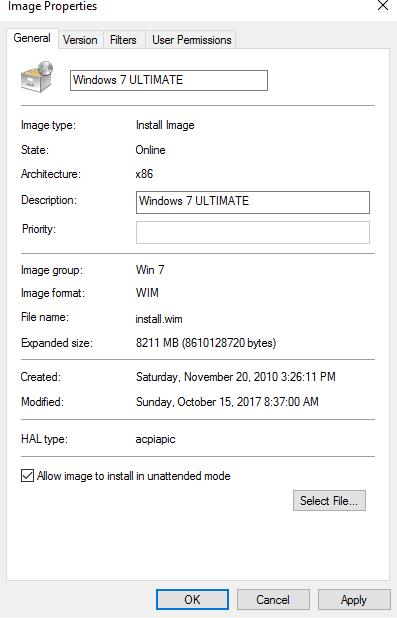
*Hình 9-17: Chọn file boot*



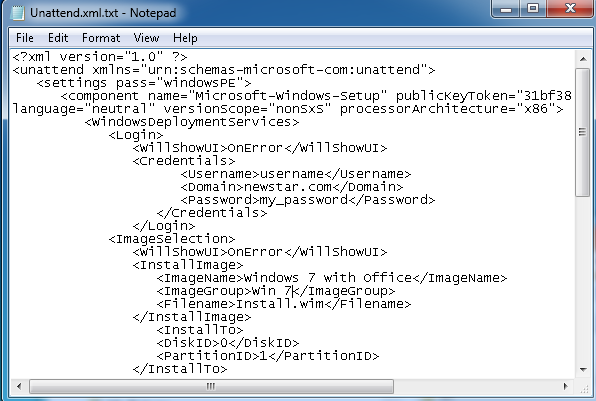
*Hình 9-18: Chọn HDH 32 bit*



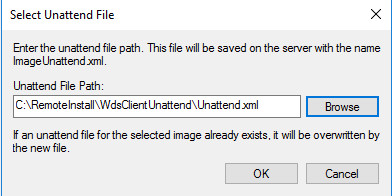
*Hình 9-19: Những phiên bản được chọn cài*



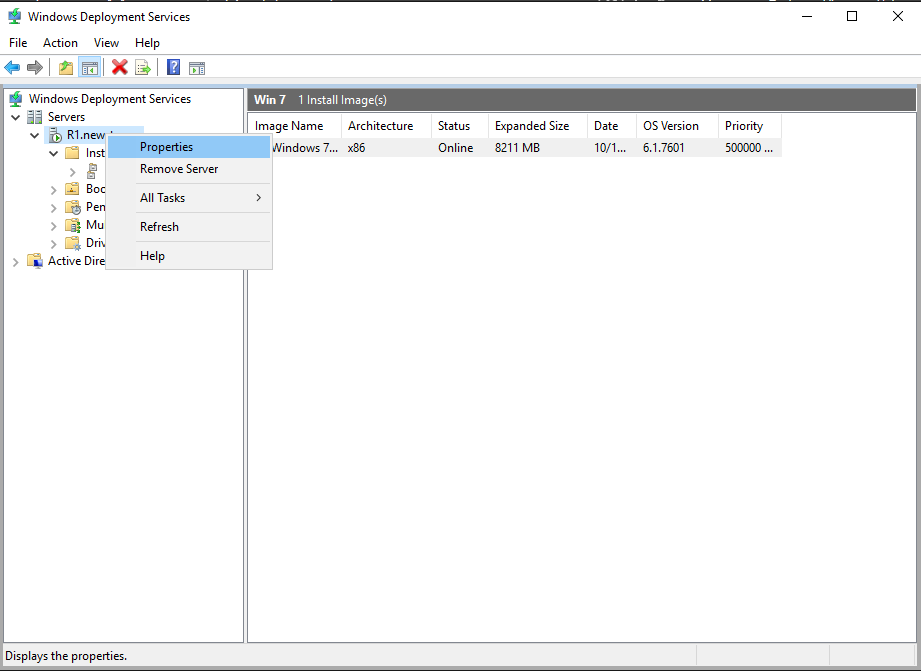
*Hình 9-20: Thông tin file cài*



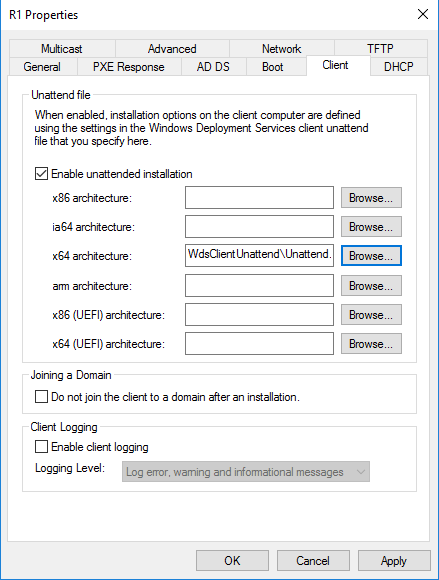
*Hình 9-21: Cấu hình File đăng nhập*



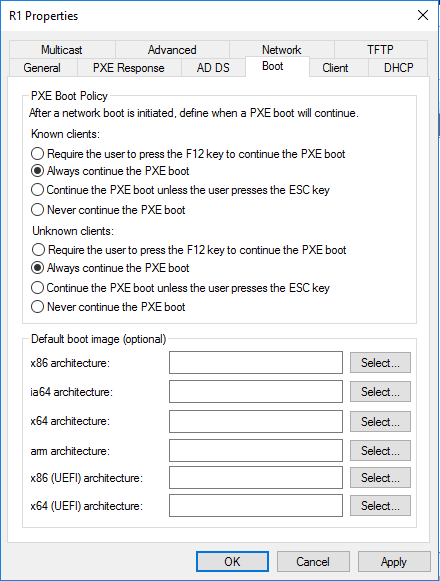
*Hình 9-22: Chọn file Unattend*



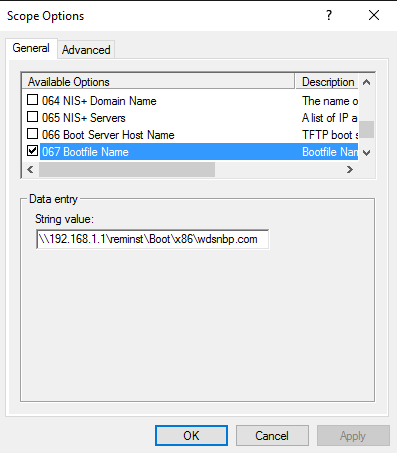
*Hình 9-23: Chỉnh sửa WDS*



*Hình 9-24: Cấu hình cho máy Client tác dụng*



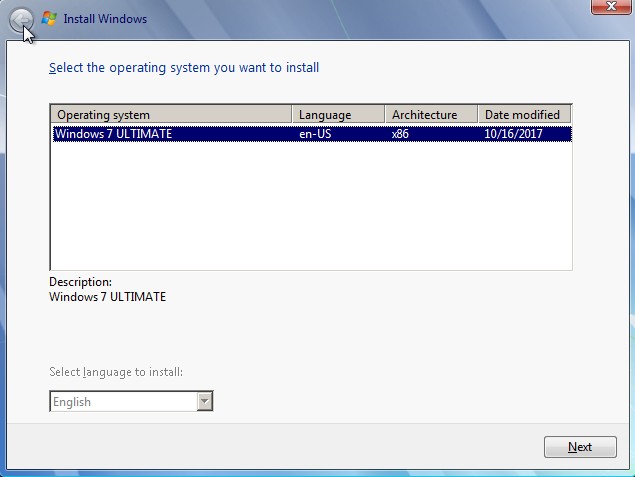
*Hình 9-25: Điều chỉnh file boot*



*Hình 9-26: Điều chỉnh thông số Scope*



*Hình 9-27: Máy client đang load HDH*



*Hình 9-28: Lựa chọn HDH cài*

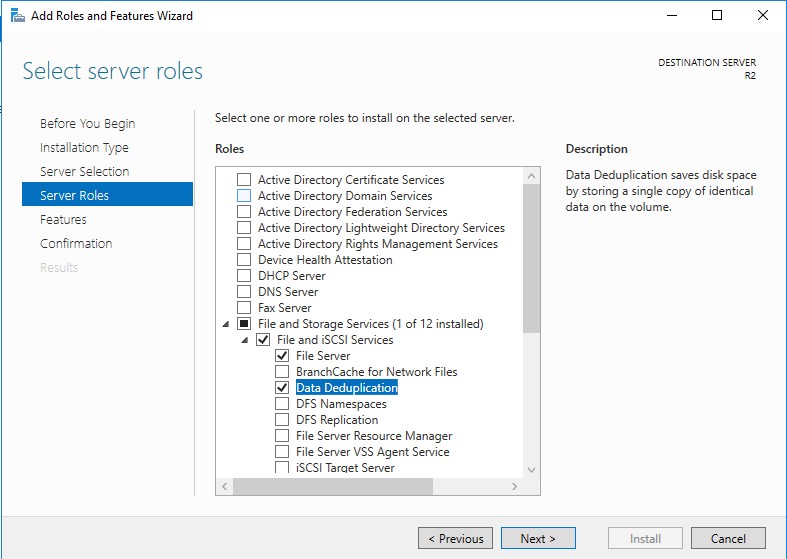
# Lưu trữ cục bộ tránh trùng lắp dữ liệu

*Sau khi học bài này học viên có khả năng khắc phục được việc trùng lắp dữ liệu trên windows Server 2016*

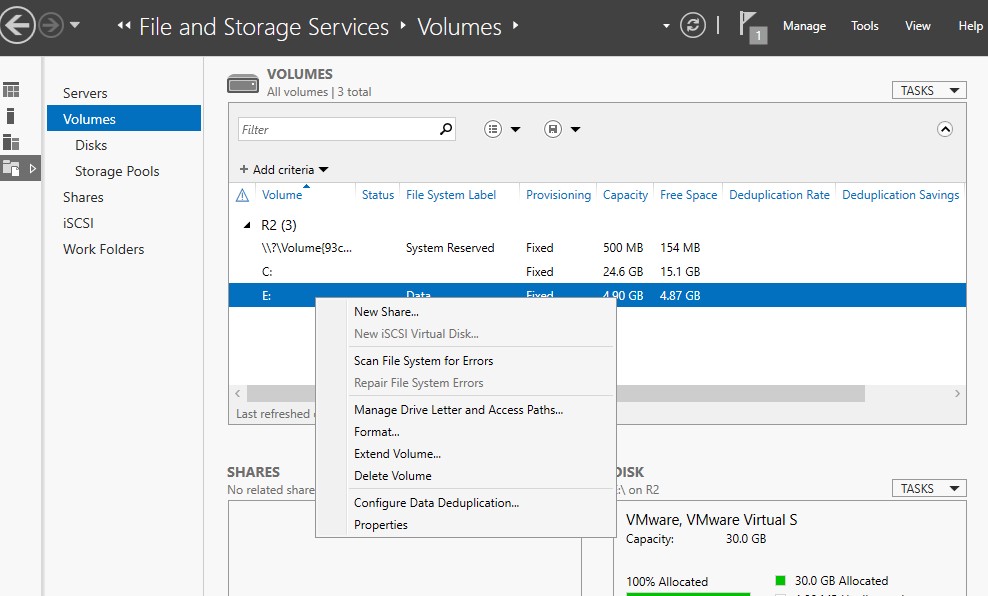
* + Chuẩn bị:

+ Một máy server 2016

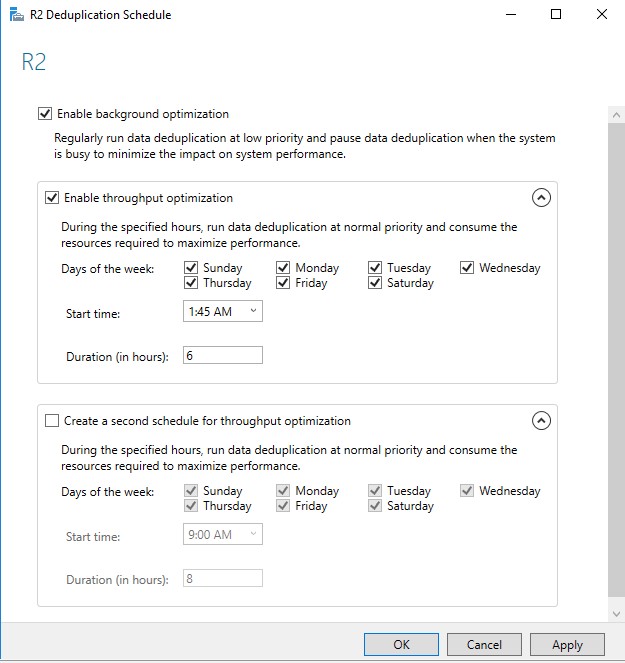
* + Kết quả đạt được
* Dữ liệu được tìm kiếm và giải quyết chuyện trùn lắp dữ liệu
  + Thực hiện



*Hình 10-1: Cài đặt dịch vụ Data Deduplication*



*Hình 10-2: Lựa chọn ổ đĩa để cấu hình*



*Hình 10-3: Tìm kiếm dữ liệu bị trùng lắp và khắc phục*

# Dịch vụ VPN

1. Client to Site

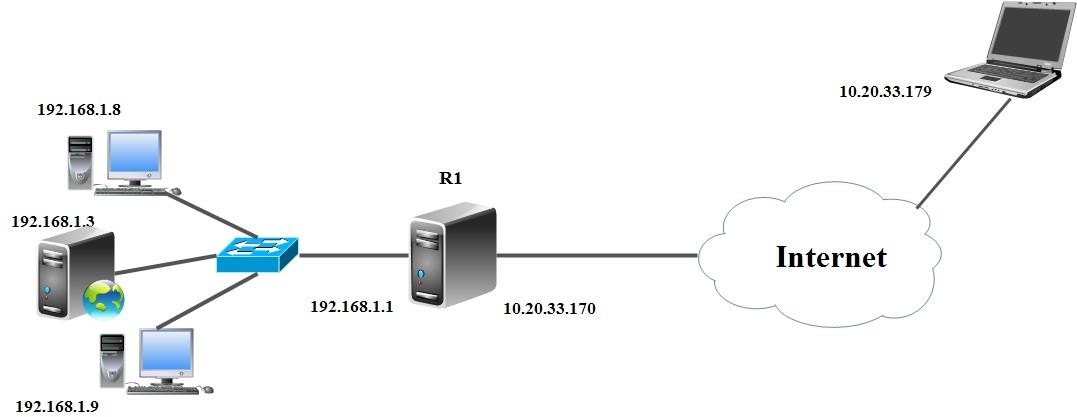
*Sau khi học bài này học viên có khả năng truy cập từ bên ngoài Internet vào bên trong hệ thống mạng nội bộ bên trong*

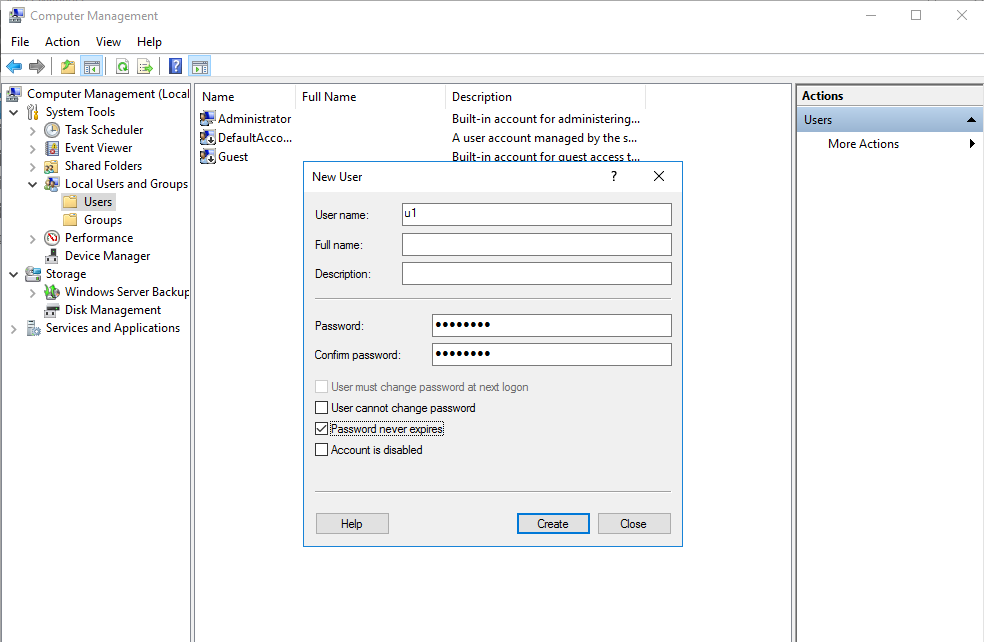
* + Chuẩn bị:

+ Một máy server 2016

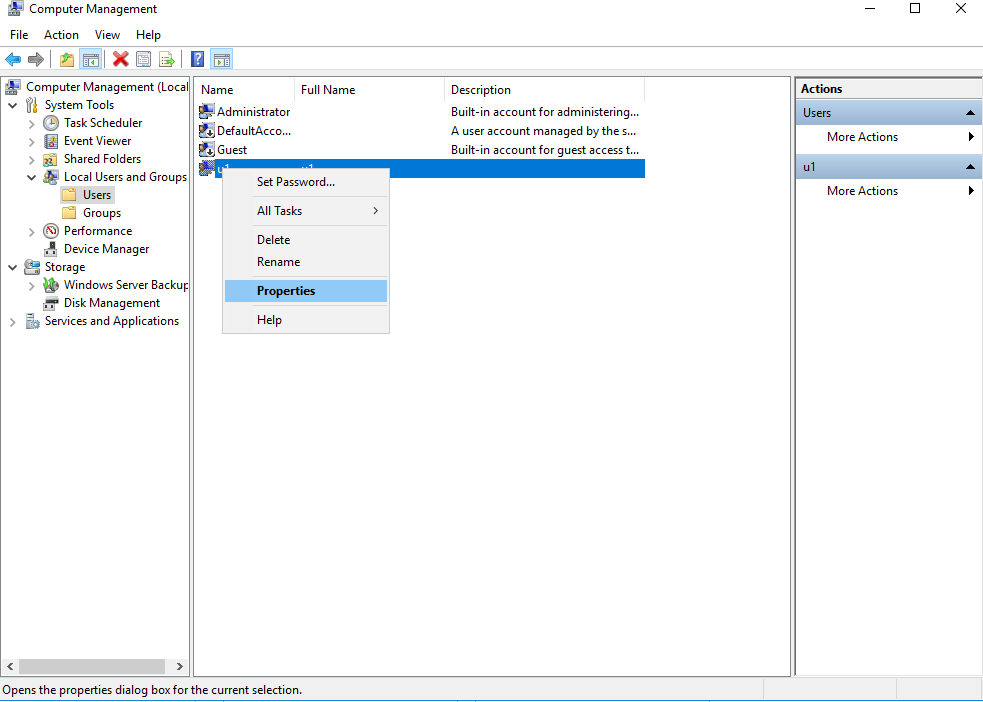
+ Hai máy Windows 7

* + Mô hình

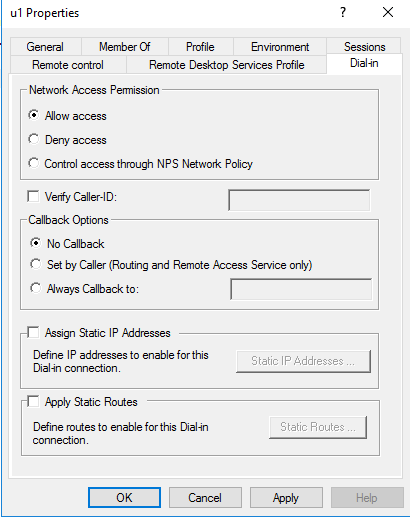


* + Kết quả đạt được
    - PC1 ngoài internet ping được nội bộ và truy cập nội bộ
  + Thực hiện
* Thực hiện ở máy Server 2016

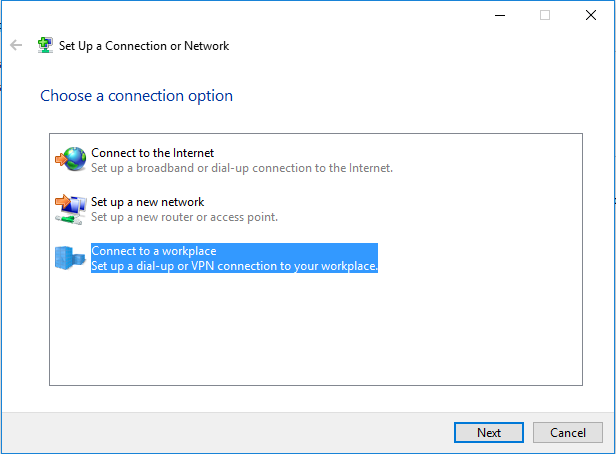
*Hình 11-1: Tạo user U1*



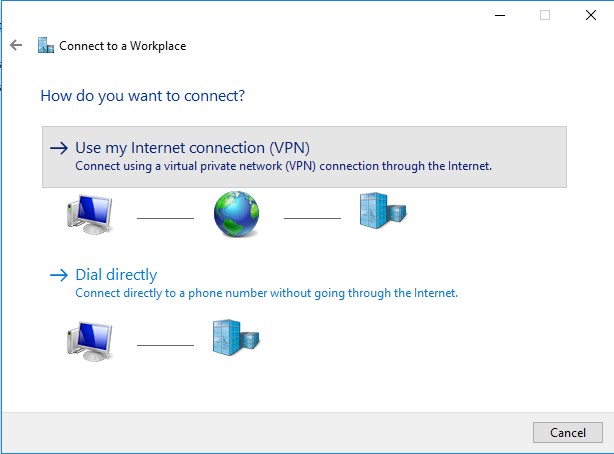
*Hình 11-2: Tùy chỉnh tài khoản U1*



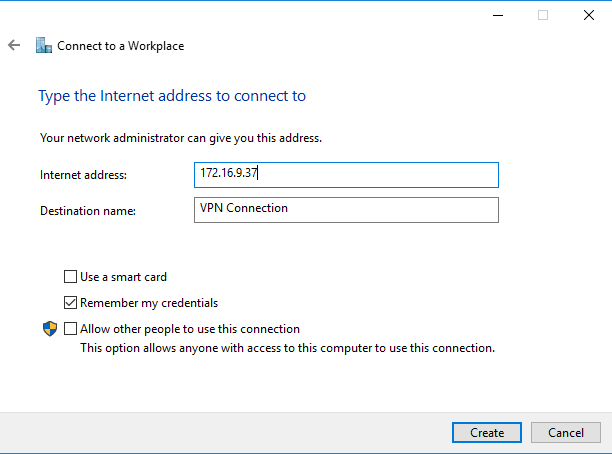
*Hình 11-3: Tùy chỉnh Allow access*

* Thực hiện ở máy Windows 7

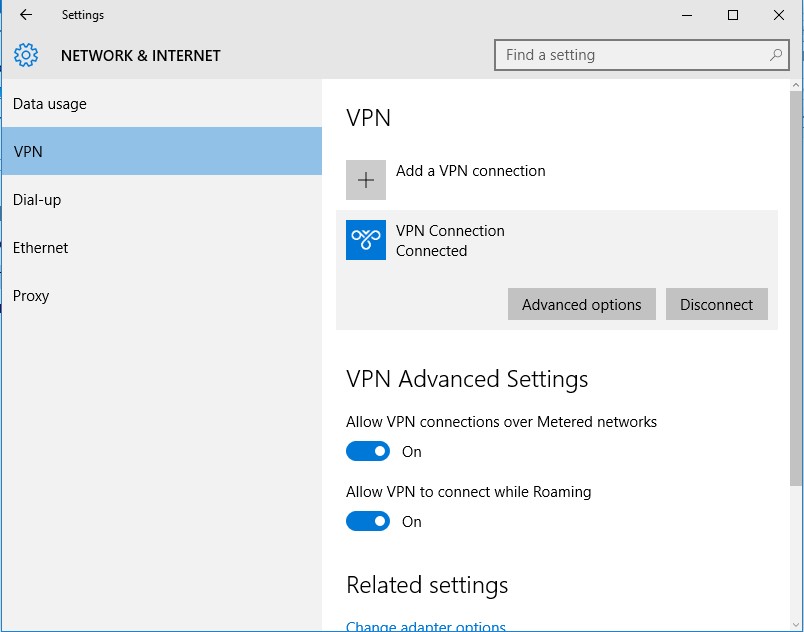
*Hình 11-4: Tiến hành kết nối VPN ở máy Client*



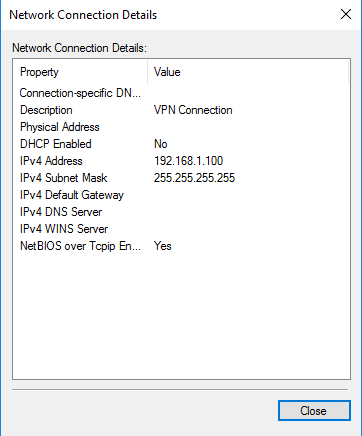
*Hình 11-5: Lựa chọn kết nối*



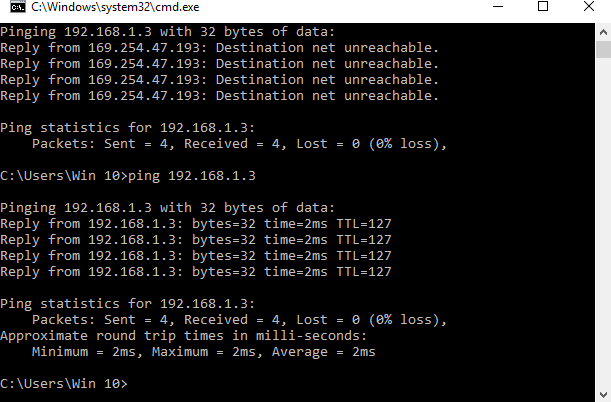
*Hình 11-6: Nhập địa chỉ IP của máy Windows server 2016*



*Hình 11-7: VPN đã kết nối được*



*Hình 11-8: IP VPN đã cấp*



*Hình 11-9: Kiểm tra kết nối tới các IP trong nội bộ*

1. VPN site to site

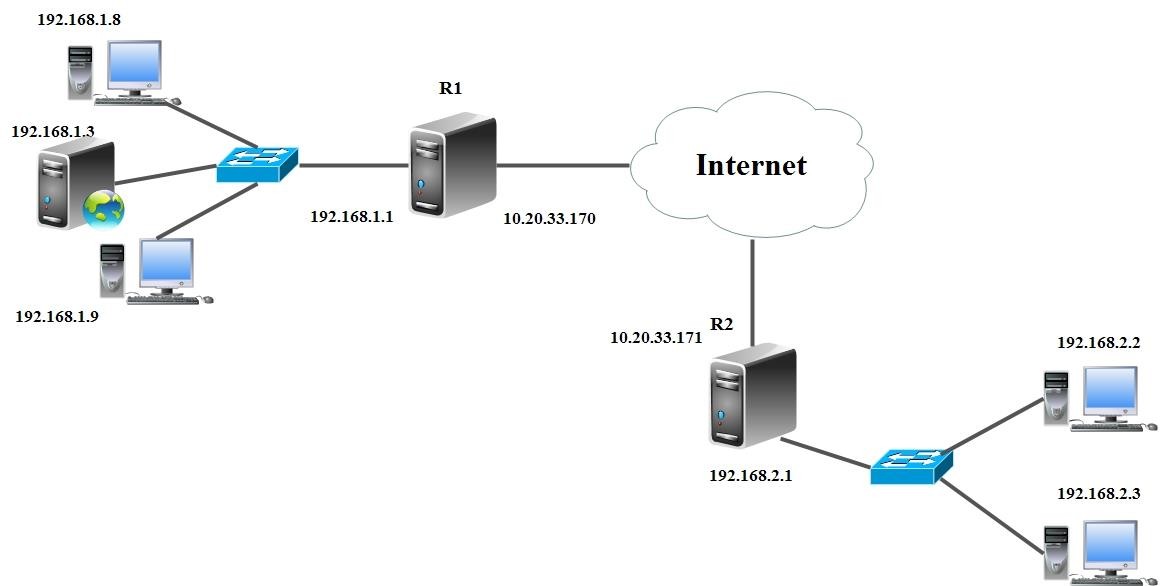
*Sau khi học bài xong học viên có khả năng cấu hình VPN từ một trụ sở tới một chi nhánh của công ty. Giúp kết nối mạng giữa hai chi nhánh xa về mặt vật lý*

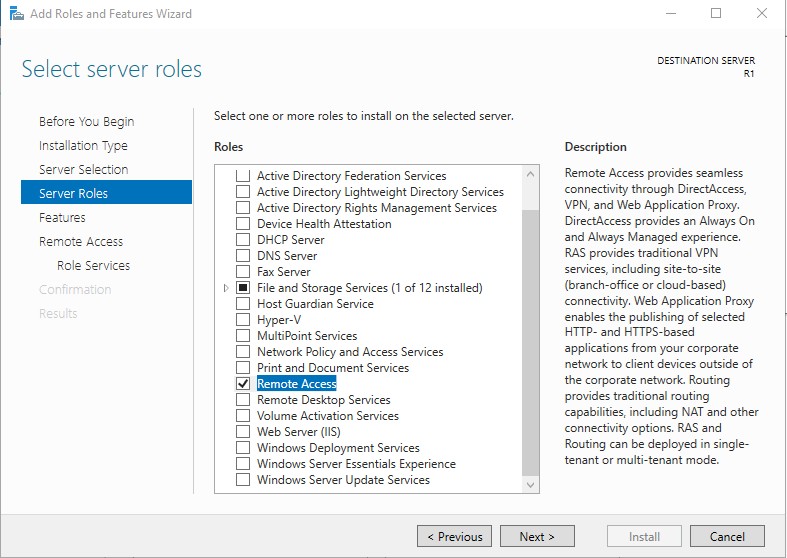
* + Chuẩn bị:

+ Hai máy server 2016

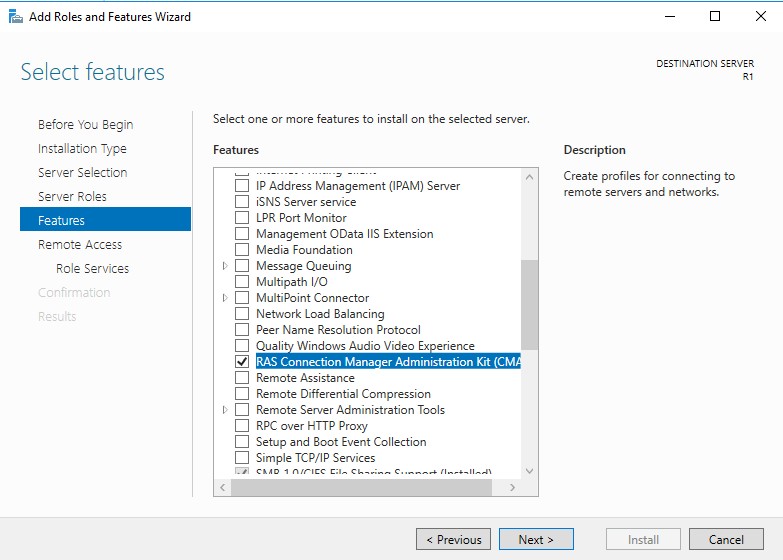
+ Hai máy windows 7

* + Mô hình

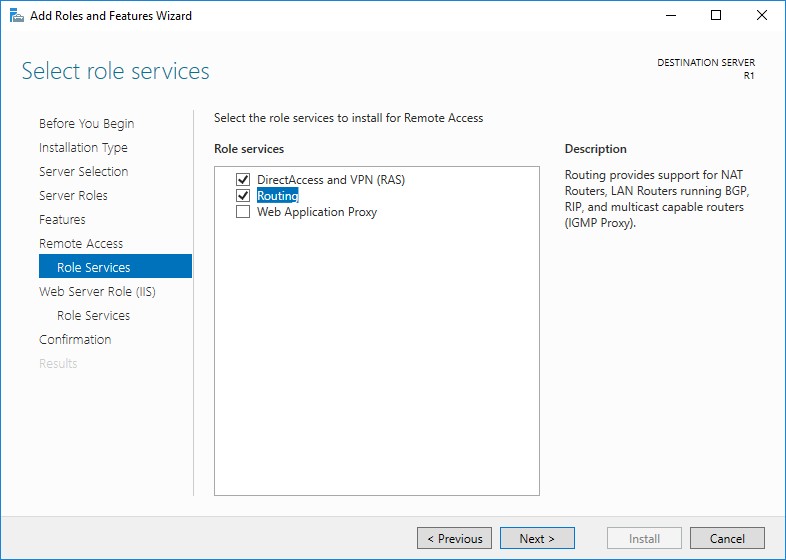


* + Kết quả đạt được
    - Mạng nội bộ hội PC 192.168.1.3 ping được 192.168.2.3
  + Thực hiện
* Trong bài này ta phải cấu hình NAT ở từng Server cho các máy client kết nối Internet, tuy nhiên các máy client của nhánh này không ping thấy nhánh kia
* Tiến hành cài dịch vụ NAT và VPN ở R1

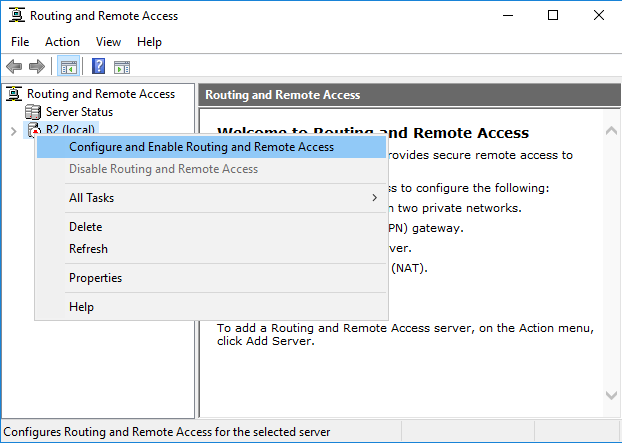
*Hình 11-10: Cài Remote Access*



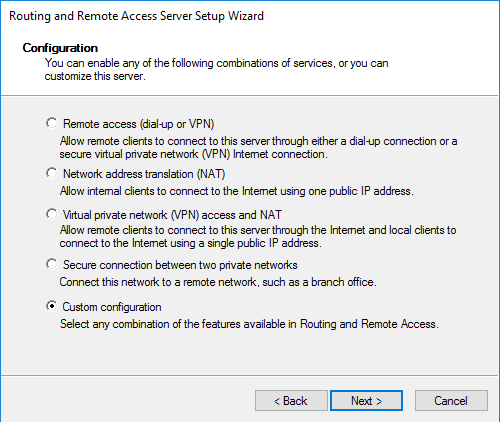
*Hình 11-11: Cài RAS*



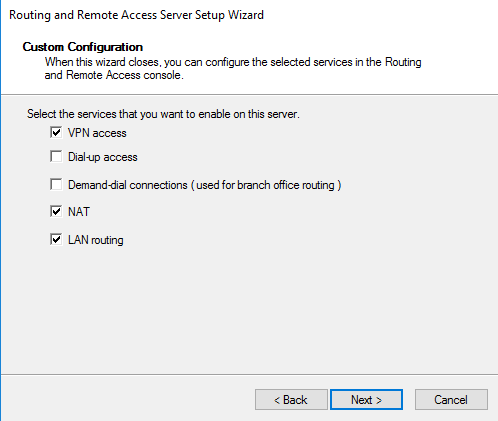
*Hình 11-12: Chọn RAS và Routing*



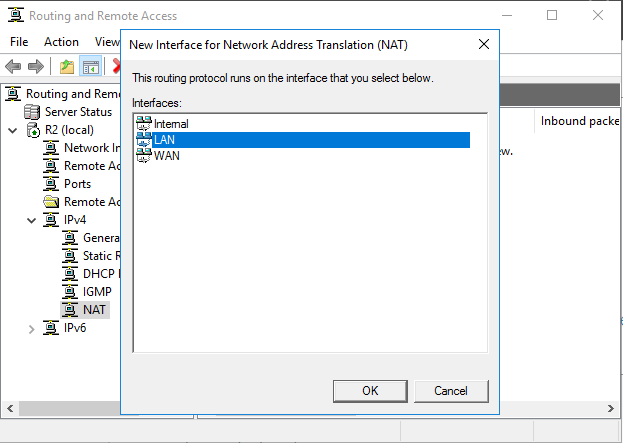
*Hình 11-13: Cấu hình RRAS*



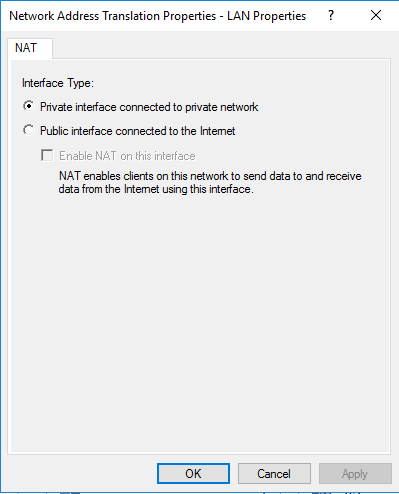
*Hình 11-14: Tùy chọn Custom*



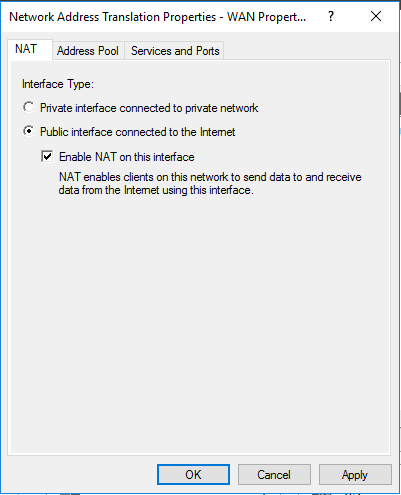
*Hình 11-15: Chọn các lựa chọn phù hợp*



*Hình 11-16: Cấu hình dịch vụ NAT*

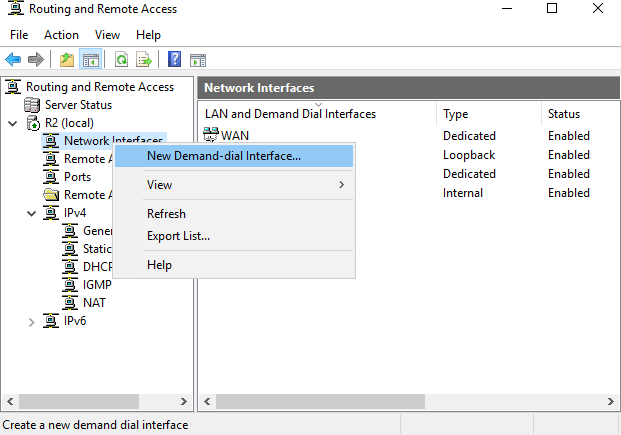


*Hình 11-17: Cấu hình NAT cho cổng trong*

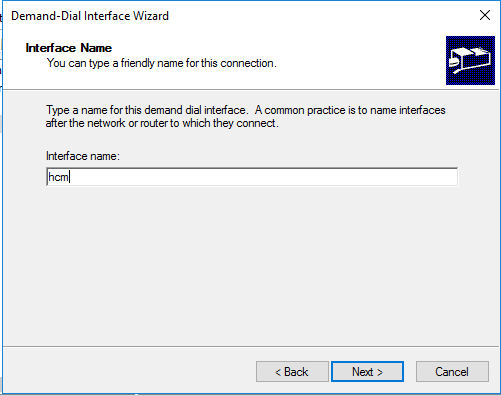


*Hình 11-18: Cấu hình NAT cho cổng ngoài*

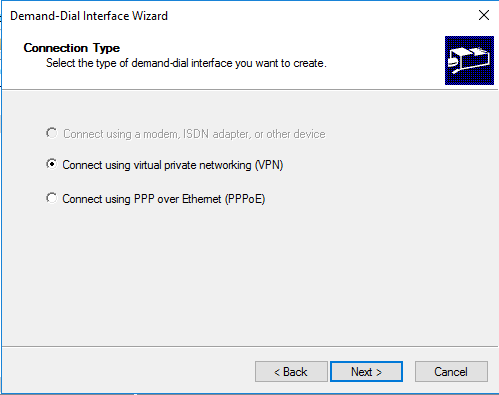
* Tương tự cho R2, ta cũng phải cài đặt dịch vụ NAT
* Tiến hành cấu hình VPN ở R1



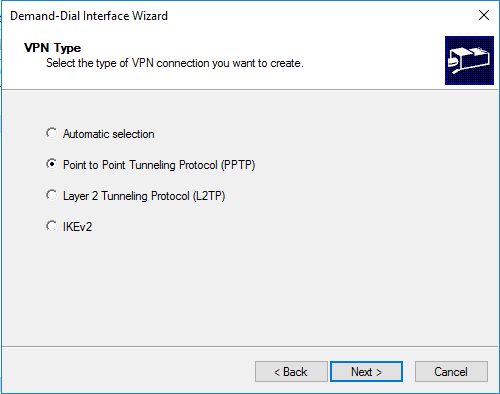
*Hình 11-19: Cấu hình dịch VPN ở R1*



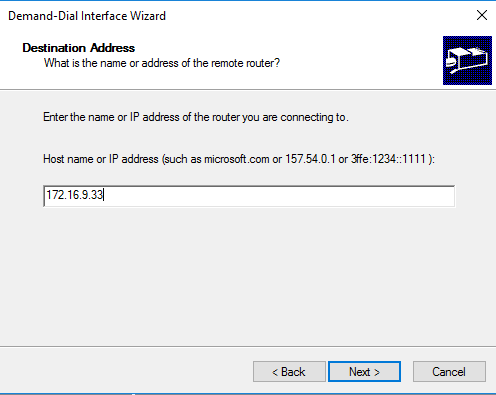
*Hình 11-20: Đặt tên cho cổng ở R1*



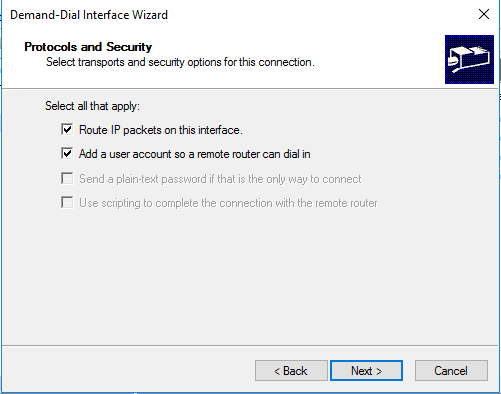
*Hình 11-21: Lựa chọn kết nối VPN ở R1*



*Hình 11-22:Chọn giao thức kết nối*

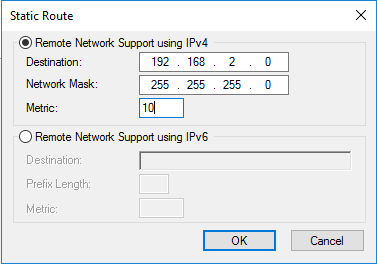


*Hình 11-23: Nhập địa chỉ IP Public Hà nội*

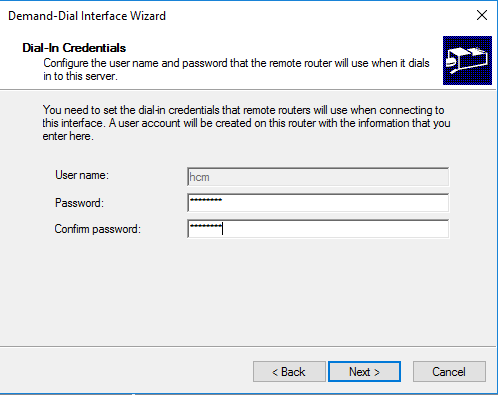


*Hình 11-24: Tùy chọn cổng và tạo tài khoản*

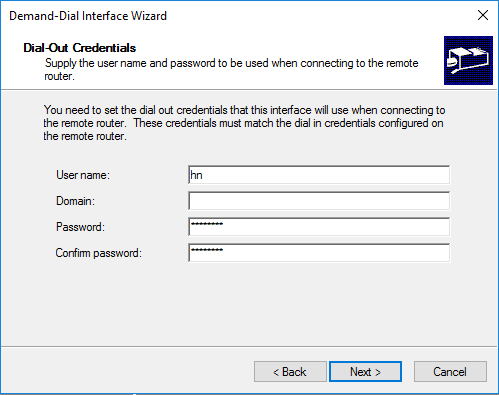
* Định tuyến tĩnh cho hai chi nhánh



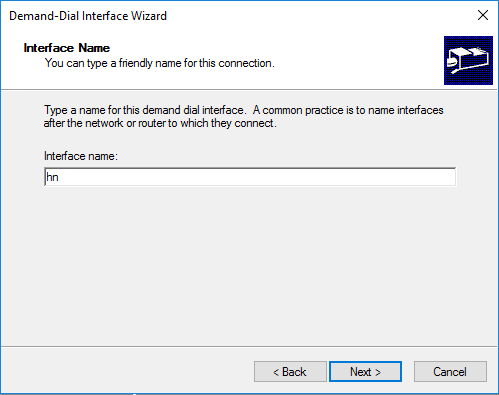
*Hình 11-25: Nhập mạng nội bộ bên Hà Nội*



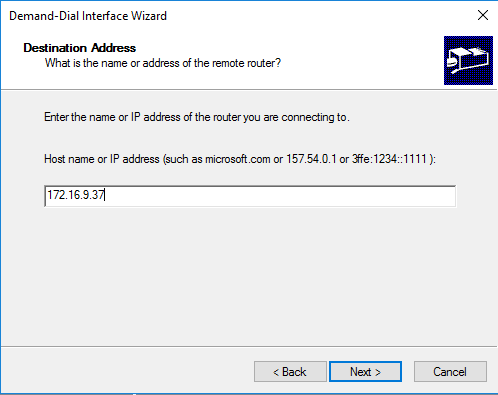
*Hình 11-26: Nhập Password cho tài khoản hcm*



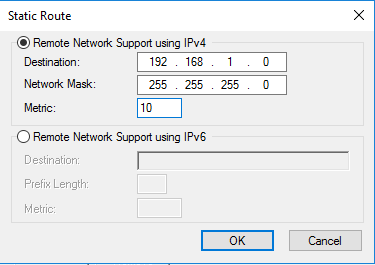
*Hình 11-27: Nhập tài khoản Hà nội*

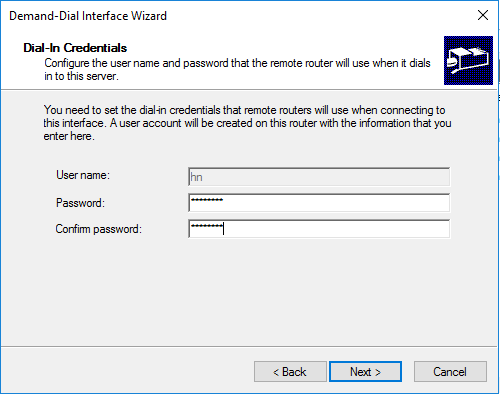
* Tiến hành cấu hình VPN trên R2

*Hình 11-28: Cấu hình cổng interface*

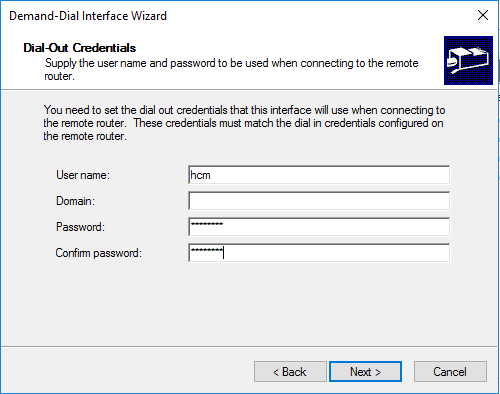


*Hình 11-29: Ip Public cổng nhánh hcm*

* Định tuyến tĩnh cho 2 chi nhánh

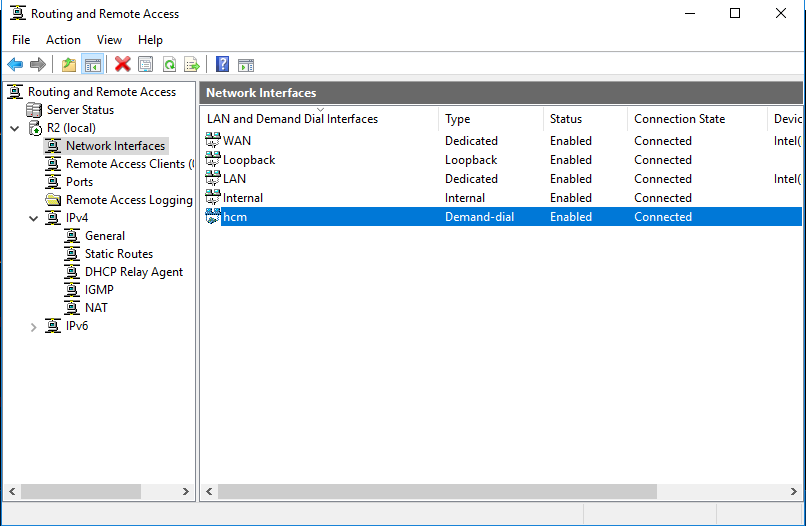


*Hình 11-30: Nhập tài khoản ở Hà Nội*

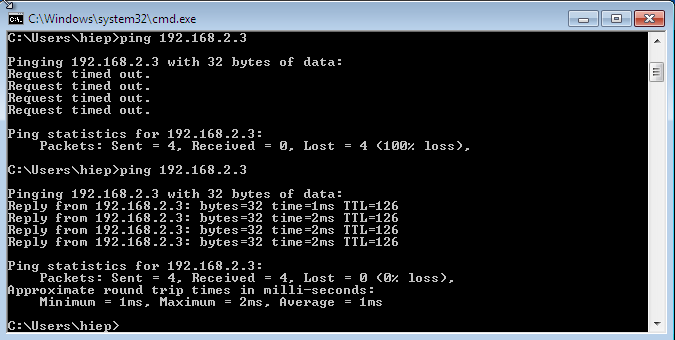


*Hình 11-31: Nhập tài khoản hcm*

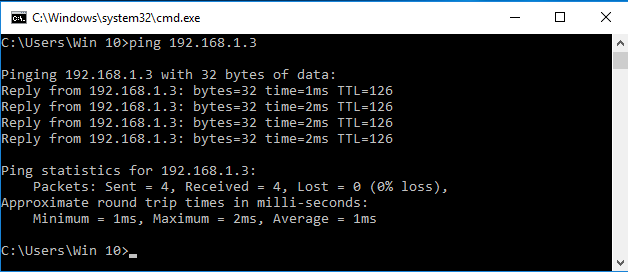
* Ở một trong hai nơi kết nối thì ta chỉ chọn vào card mạng một bên và sau đó chọn kết nối



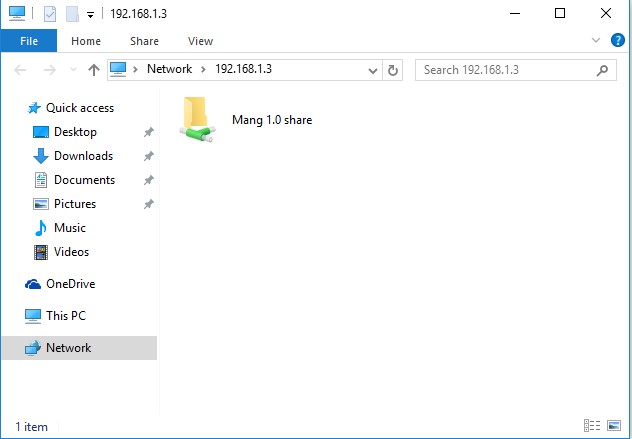
*Hình 11-32: VPN đã được kết nối*



*Hình 11-33: Đứng trong nội bộ hcm ping thấy nội bộ hn*



*Hình 11-34: Đứng trong nội bộ hn thấy nội bộ hcm*



*Hình 11-35: HN truy cập được file của HCM*

# Triển khai hệ thống Domain

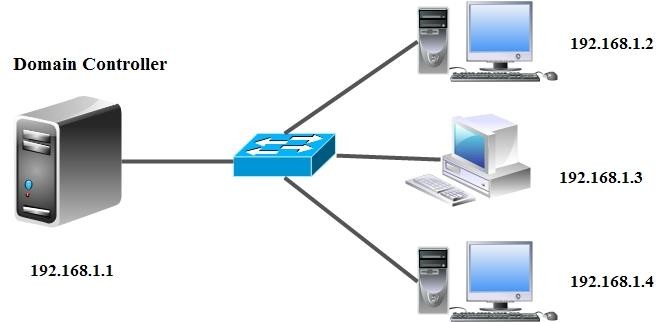
*Sau khi học bài này học viên có khả năng nâng cấp một máy Windows Server 2016 thành một máy Domain Controller, giúp các máy con gia nhập vào hệ thống domain mà ta đã nâng cấp*

* + Chuẩn bị:

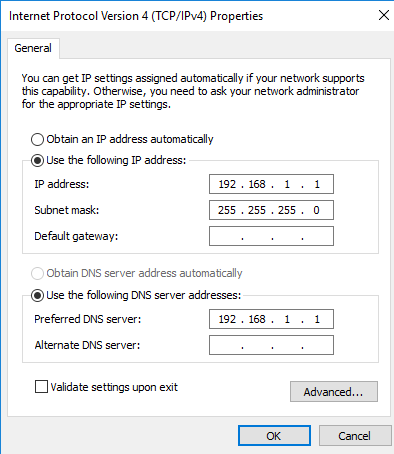
+ Một máy server 2016

+ Một máy Client windows 7

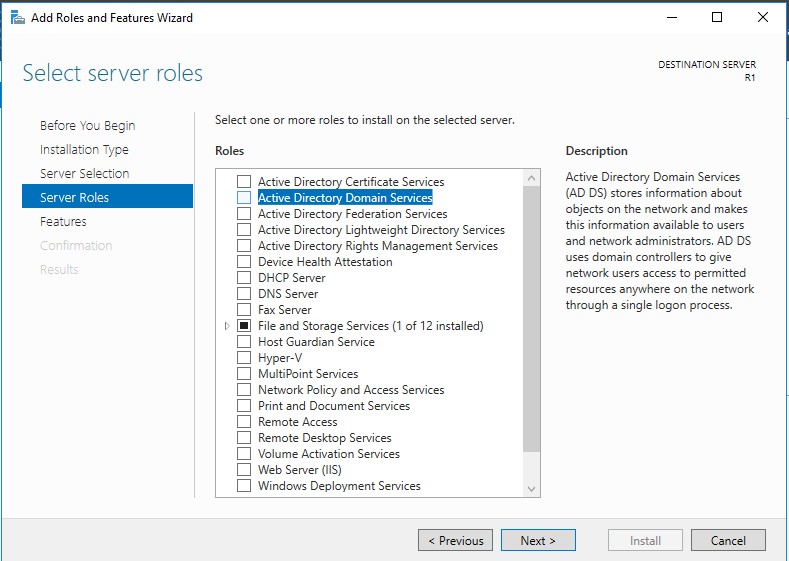
* + Mô hình



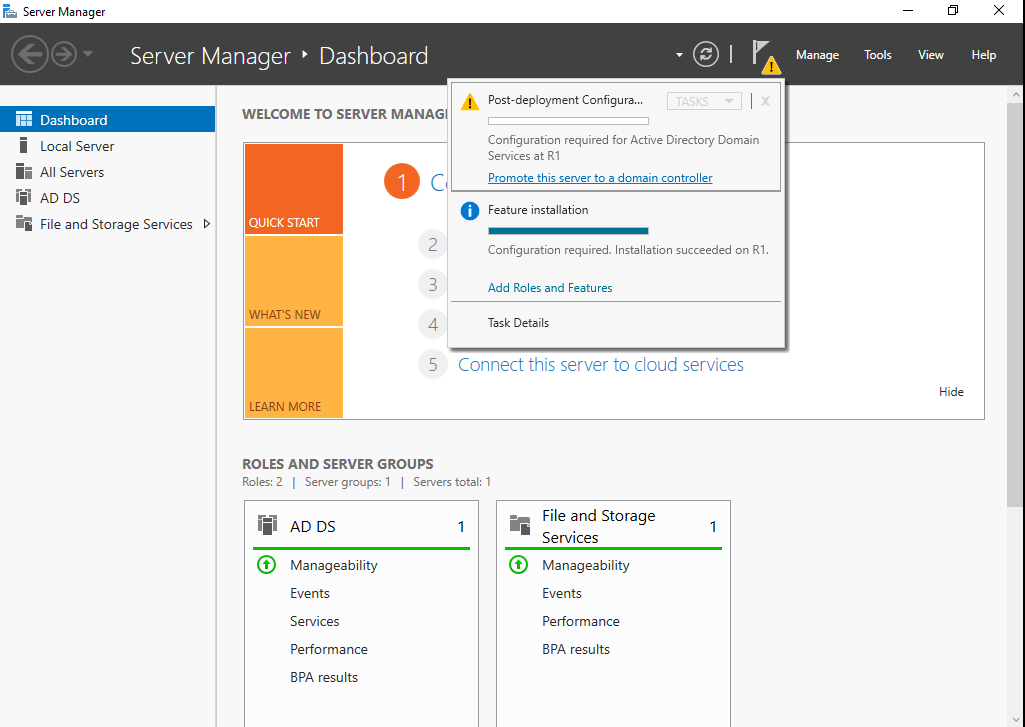
* + Kết quả đạt được
* Máy client join vào domain, đăng nhập tài khoản ở ADDS trên máy client
  + Thực hiện
* Khi đặt địa chỉ IP cho Server thì phải trỏ DNS về chính Server vì nó sẽ là nơi để phân giải tên miền mà ta sẽ sử dụng trong quá trình nâng cấp domain



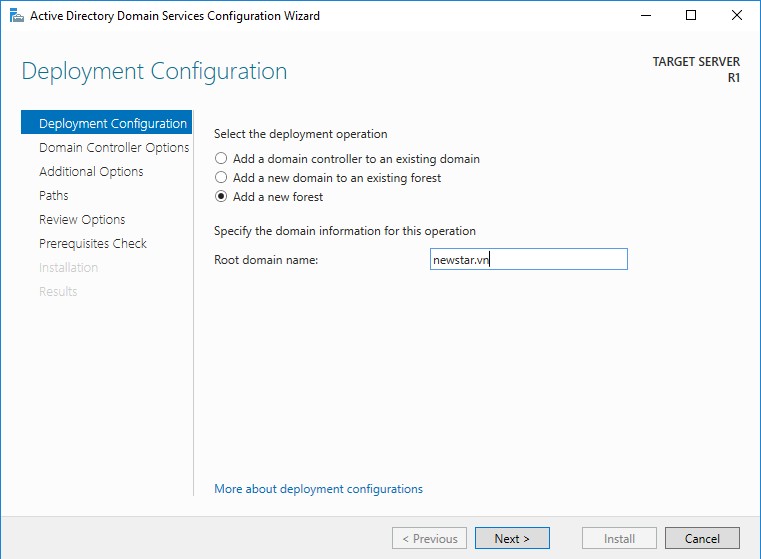
*Hình 12-1: Đặt IP cho Server Domain*



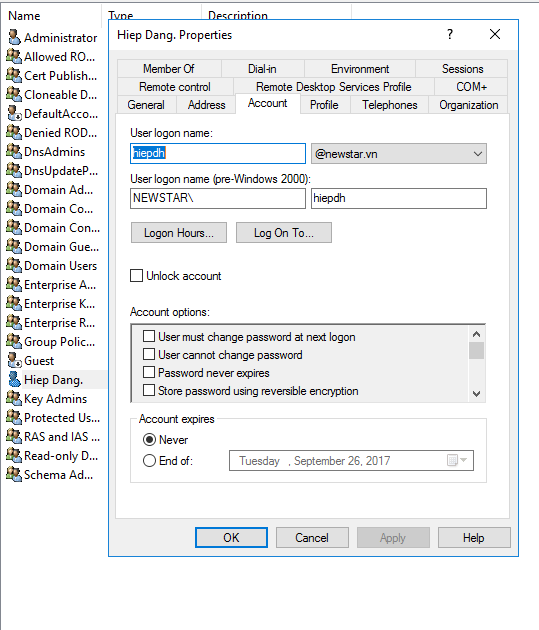
*Hình 12-2: Cài dịch vụ ADDS*



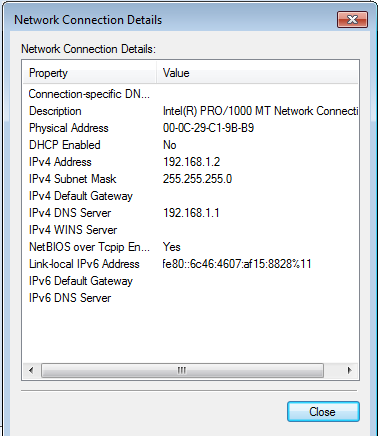
*Hình 12-3: Cài Domain*



*Hình 12-4: Nhập tên domain*

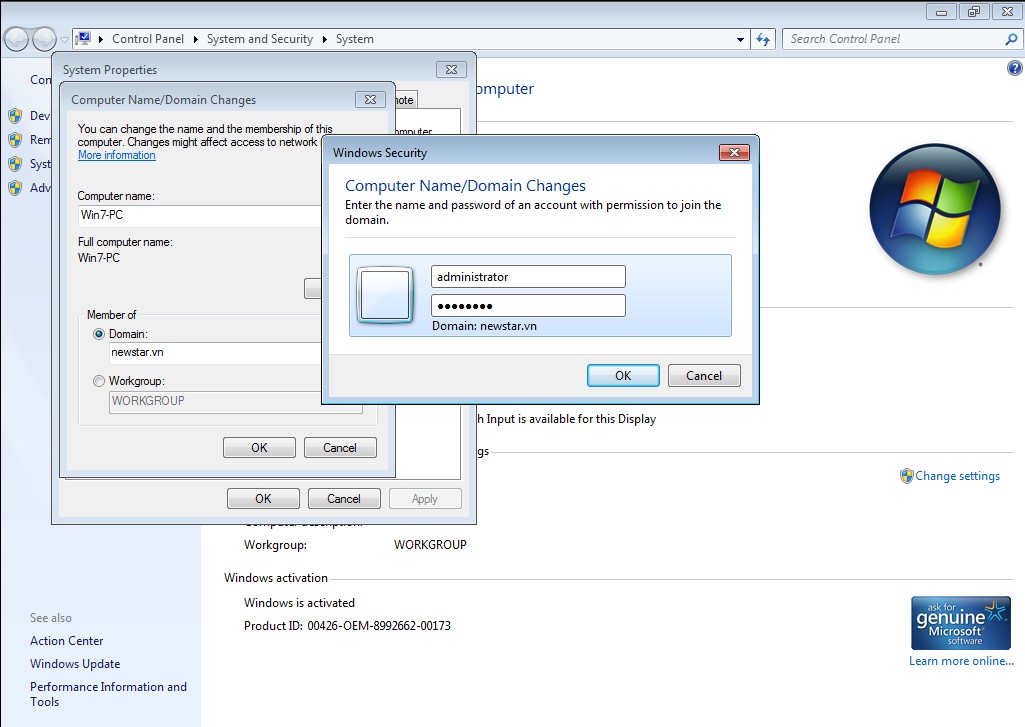
* Quá trình nâng cấp domain đã xong, ta tiến hành tạo tài khoản trên domain

*Hình 12-5: Tạo tài khoản trên domain*

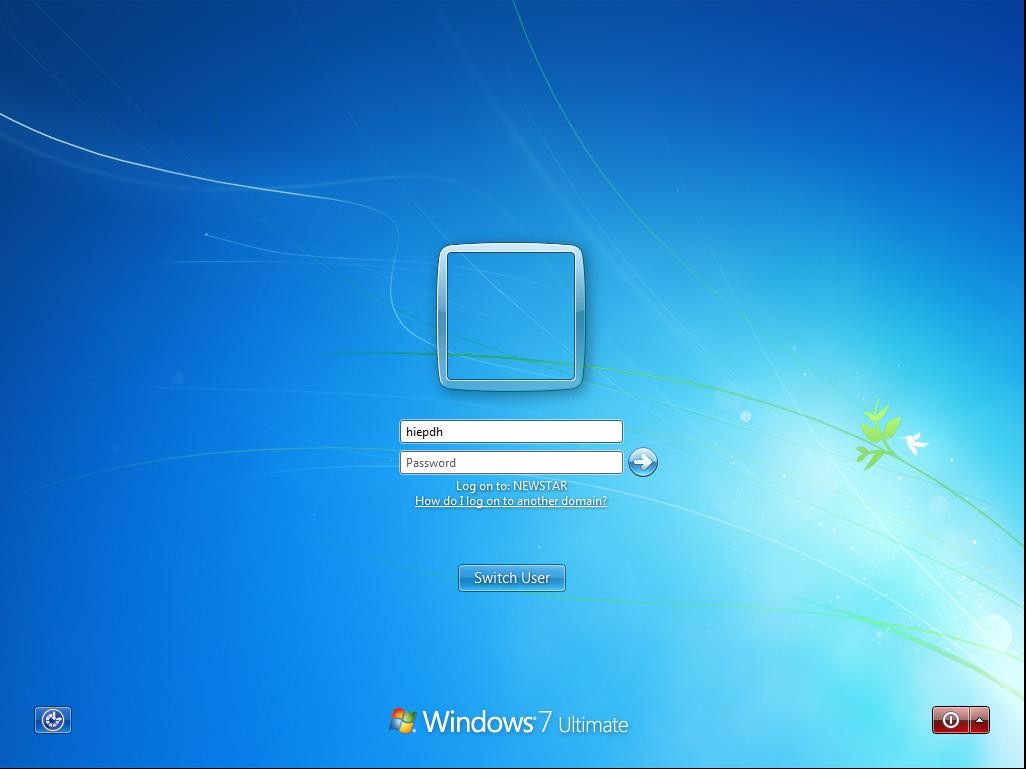
* Đặt Ip trên máy client, trỏ DNS về Domain Controller

*Hình 12-6: Đặt IP trên máy Client*

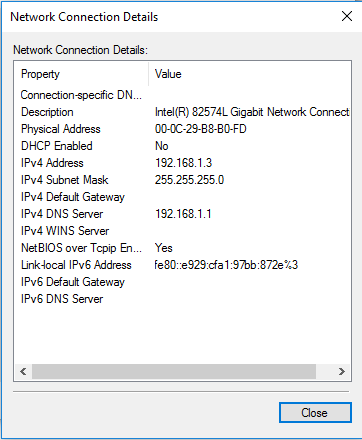
* Tiến hành gia nhập domain, nhập phải chuột vào My computer chọn vào Property  change setting  Change, check mục Domain nhập tên domain

vào. Sau đó có thông báo yêu cầu nhập tài khoản bên Domain, Nhập tài khoản administrator

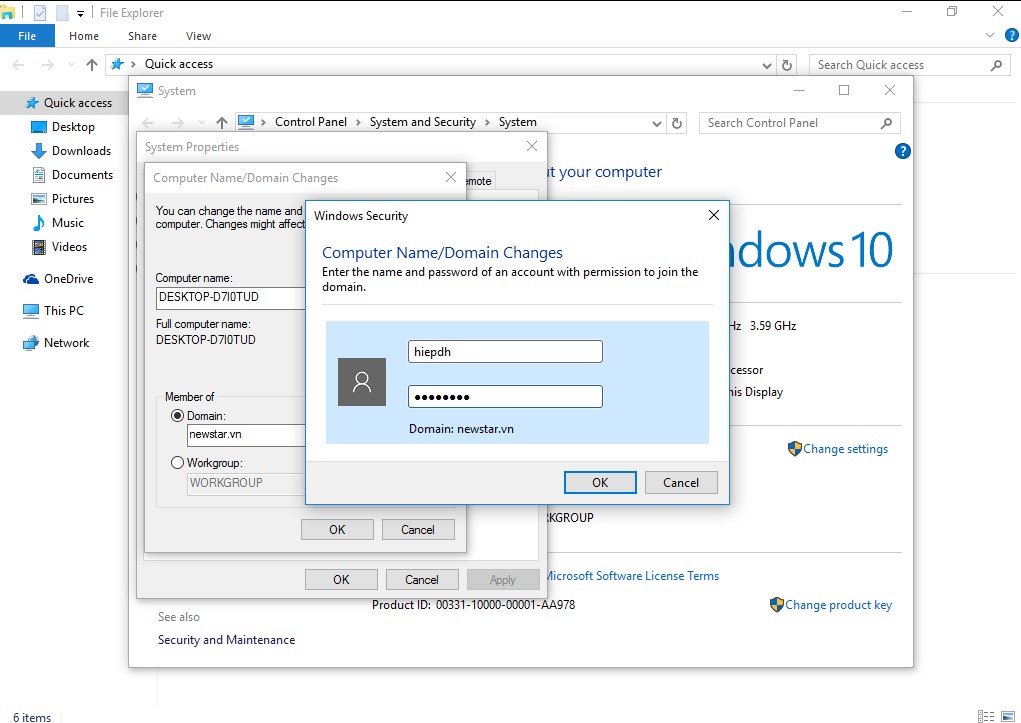
*Hình 12-7: Nhập tài khoản trên domain*



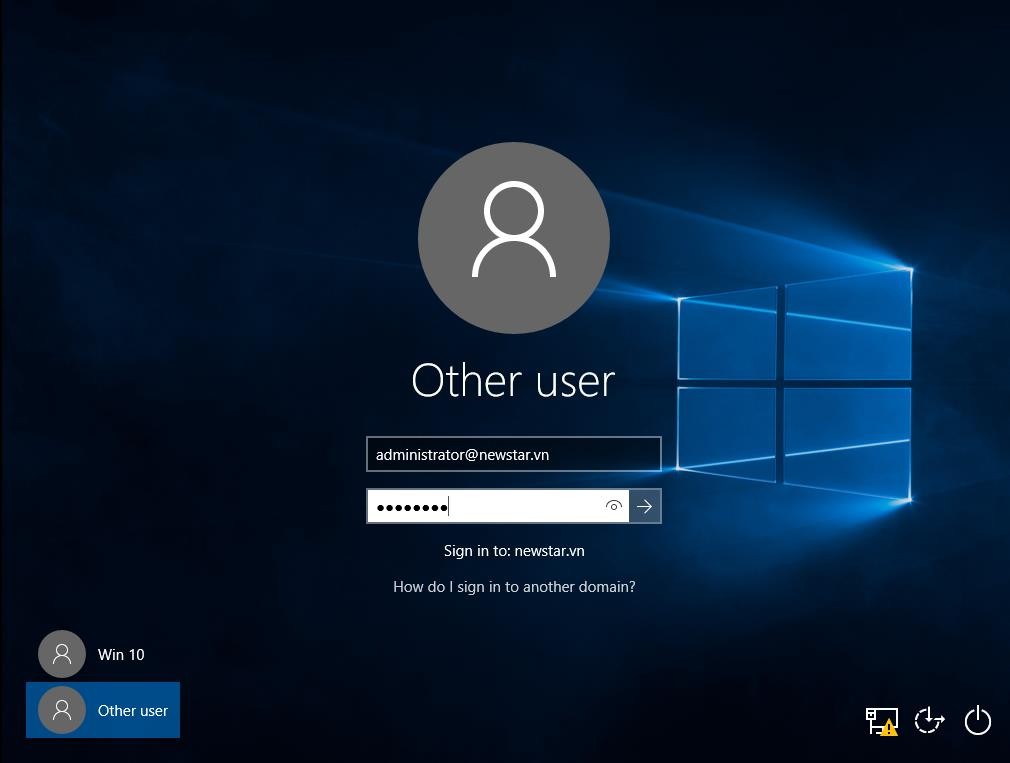
*Hình 12-8: Đăng nhập tài khoản hiepdh*

* Thực hiện gia nhập Domain trên máy windows 8

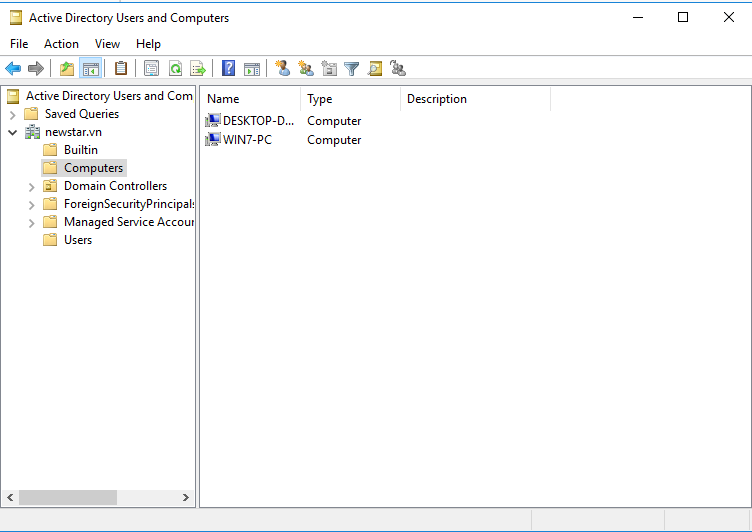
*Hình 12-9: Đặt IP trên máy Client*



*Hình 12-10: Đăng nhập tài khoản hiepdh trên domain*



*Hình 12-11: Đăng nhập tài khoản Administrator domain trên máy client*

* Sau khi gia nhập xong vào máy Domain ta sẽ thấy các máy client đã gia nhập

*Hình 12-12: Các máy Join domain*