CƠ BẢN VỀ XỬ LÝ SỰ CỐ ROUTER

1.1. Xử lý sự cố VLAN.

1.1.2 Giới thiệu chung.

Hiện nay VLAN đ−ợc sử dụng phổ biến. Với VLAN, ng−ời kỹ s− mạng có thể linh hoạt hơn trong thiết kế và triển khai hệ thống mạng. VLAN giúp giới hạn miền quảng bá, gia tăng khả năng bảo mật và phân nhóm theo logic. Tuy nhiên, với cơ bản chuyển mạch LAN, sự cố có thể xay ra khi chúng ta triển khai VLAN. Trong bài này sẽ cho thấy một vài sự cố có thể xảy ra với VLAN và cung cấp cho các bạn một số công cụ và kỹ thuật sử lý sự cố.

Sau khi hoàn tất bài này các bạn có thể thực hiện các việc sau:

• Phân tích hệ thống để tiếp xúc với sự cố của VLAN.

• Giải thích các b−ớc xử lý sự cố nói chung trong mạng chuyển mạch.

• Mô tả sự cố Spanning — Tree dẫn đến trận bão quảng bá nh− thế nào.

• Sử dụng lệnh show và debug để xử lý sự cố VLAN.

1.1.3. Tiến trình xử lý sự cố VLAN.

Điều quan trọng là bạn phải phát triển các b−ớc xử lý sự cố trên switch một cách có hệ thống. Sau đây là các b−ớc có thể giúp cho bạn xác định sự cố trong mạng chuyển mạch:

1. Kiểm tra các biểu hiện vật lý, nh− trạng thái LED.

2. Bắt đầu từ một cấu hình trên một switch và kiêm tra dần ra.

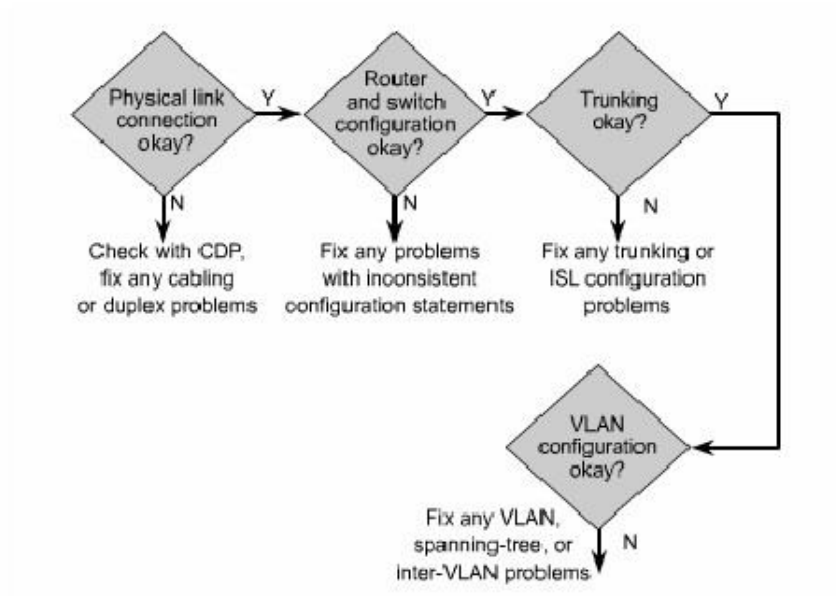
3. Kiểm tra kết nối lớp 1.

4. Kiểm tra kết nối lớp 2.

5. Xử lý sự cố VLAN xảy ra trên nhiều switch.

Khi xay ra sự cố, bạn nên kiểm tra xem đây là một sự cố lặp đi lặp lại hay là sự cố biệt lập. Một số sự cố lặp đi lặp lại có thể là do sự gia tăng của các dịch vụ phục vụ cho máy trạm, làm v−ợt qua khả năng cấu hình, khả năng đ−ờng trunking và khả năng truy cập tài nguyên trên server.

Ví dụ: Việc sử dụng các công nghệ web và các ứng dụng truyền thống nh− truyền tải file, email...sẽ làm gia tăng mật độ giao thông làm cho toàn bộ hệ thống bị trì trệ.



Hình 8.3.1

Hiện nay rất nhiều mạng LAN phải đối mặt với mô hình giao thông ch−a đ−ợc tính tr−ớc, là kết quả của sự gia tăng giao thông trong intranet, ít phân nhóm server hơn và tăng sử dụng multicast. Nguyên tắc 80/20 với chỉ có 20% giao thông đi lên các đ−ờng trục chính đã trở lên lạc hậu. Ngày nay, các trình duyệt web nội bộ có thể cho phép user xác định và truy cập thông tin ở bất kỳ đâu trong mạng nội bộ của tập đoàn.

Nếu mạng th−ờng xuyên bị nghẽn mạch, quá tải, rớt gói và truyền lại nhiều lần thì nghĩa là có quá nhiều port cho một đ−ơng trunk hoặc có quá nhiều yêu cầu truy suất vào các nguồn tài nguyên của toàn hệ thông và các server intranet.

Nghẽn mạch cũng có thể do phần lớn giao thông đều đ−ợc truyền lên đ−ờng trục chính, hoặc là do user mở ra nhiều tài nguyên và nhiêu ứng dụng đa ph−ơng tiện. Trong tr−ờng hợp này thị hệ thống mạng nên nâng cấp để đáp ứng nhu cầu phát triển.

1.1.4 Ngăn trặn cơn bão quảng bá.

Trận bão quảng bá xảy ra khi có quá nhiều gói quảng bá đ−ợc nhận vào trên một port. Việc sử lý chuyển mạch các gói này cho hệ thống mạng châm đi. Chúng ta có thể cấu hình cho switch kiểm soát bão trên từng port. Mặc định, chế độ kiểm soát bão trên switch bị tắt đi.

Để ngăn chặn bão quảng bá, chúng ta đặt một giá trị ng−ỡng cho port để huỷ gói dữ liệu và đóng port khi giá trị ng−ỡng này bị v−ớt qua.

STP (Spanning - Tree Protocol) có một số sự cố bao gồm trận bão quảng bá, lặp vòng, rớt gói BPDU va gói dữ liệu. Chức năng của STP là bảo đảm không có vòng lặp tồn tại trong mạng bằng cách chọn ra một bridge gốc. Bridge gốc này là điểm gốc của cấu trúc hình cây và nơi kiểm soát hoạt động của giao thức STP.

Nếu cần phải giảm l−ợng giao thông BPDU thì bạn sẽ cài đặt giá trị tối đa cho các khoảng thời gian hoạt động của bridge gốc. Đặc biệt là bạn nên đặt giá trị tối đa 30 giây cho khoảng thời gian chuyển trạng thái (Forward delay) và thời gian chờ tối đa (max - age) là 40 giây.

Một port vật lý trên router hoặc switch có thể là thành viên của một hoặc nhiều cấu trúc hình cây nếu port này kết nối vào đ−ờng trunk.

L−u ý: VTP chỉ chạy trên Catalyst switch chứ không chạy trên router.

Trên switch kết nối vào router, bạn nên cấu hình cho switch đó chạy ở chế độ VTP transparent cho đến khi nào Cisco hỗ trợ VTP trên router của họ.

Giao thức Spanning - Tree đ−ợc xem là một trong những giao thức lớp 2 quan trọng nhất trên Catalyst switch. bằng cách ngăn chặn các vòng luận lý trong mạng chuyển mạch, STP cho phép cấu trúc lớp 2 vẫn có các đ−ờng d− để dự phòng mà không gây ra trân bão quảng bá.

TẬP 4

PHÂN CHIA ĐỊA CHỈ IP

GIỚI THIỆU

Sự phát triển không ngừng của Internet đã làm cho những nhà nghiên cứu bất ngờ. Một trong những nguyên nhân làm cho Internet phát triển nhanh chóng như vậy là do sự linh hoạt, uyển chuyển của thiết kế ban đầu. Nếu chúng ta không có các biện pháp phân phối địa chỉ IP thì sự phát triển của Internet sẽ làm cạn kiệt nguồn địa chỉ IP. Để giải quyết vấn đề thiếu hụt địa chỉ IP, nhiều biện pháp đã được triển khai. Trong đó, một biện pháp đã được triển khai rộng rãi là chuyển đổi địa chỉ mạng (Network Address Translation – NAT).

NAT là một cơ chế để tiết kiệm địa chỉ IP đăng kí trong một mạng lớn và giúp đơn giản hóa việc quản lý địa chỉ IP. Khi một gói dữ liệu được định tuyến trong một thiết bị mạng, thường là firewall hoặc các router biên, địa chỉ IP nguồn sẽ được chuyển đổi từ địa chỉ mạng riêng thành địa chỉ IP công cộng định tuyến được. Điều này cho phép gói dữ liệu được truyền đi trong trong mạng công cộng, ví dụ như Internet. Sau đó, địa chỉ công cộng trong gói trả lời lại được chuyển đổi thành địa chỉ riêng để phát vào trong mạng nội bộ. Một dạng của NAT, được gọi là PAT (Port Address Translation), cho phép nhiều địa chỉ riêng được dịch sang một địa chỉ công cộng duy nhất.

Router, server và các thiết bị quan trọng khác trong mạng thường đòi hỏi phải được cấu hình bằng tay địa chỉ IP cố định. Trong khi đó, các máy tính client không cần thiết phải đặt cố định một địa chỉ mà chỉ cần xác định một dải địa chỉ cho nó. Dải địa chỉ này thường là một subnet IP. Một máy tính nằm trong subnet có thể được phân phối bất kì địa chỉ nào nằm trong subnet đó.

Giao thức DHCP (Dynamic Host Configuration Protocol) được thiết kế để phân phối địa chỉ IP và đồng thời cung cấp các thông tin cấu hình mạng quan trọng một cách tự động cho máy tính. Số lượng máy client chiếm phần lớn trong hệ thống mạng, do đó DHCP thực sự là công cụ tiết kiệm thời gian cho người quản trị mạng.

Sau khi hoàn tất chương này, các bạn có thể:

- Xác định địa chỉ IP riêng được mô tả trong RFC 1918.
- Nắm được các đặc điểm của NAT và PAT.
- Phân tích các lợi điểm của NAT.
- Phân tích cách cấu hình NAT và PAT, bao gồm cả chuyển đổi cố định, chuyển đổi động và chuyển đổi overloading.
- Xác định các lệnh dùng để kiệm tra cấu hình NAT và PAT.
- Liệt kê các bước xử lý sự cố NAT và PAT.
- Nắm được các ưu điểm và nhược điểm của NAT.
- Mô tả các đặc điểm của DHCP.
- Phân tích sự khác nhau giữa BOOTP và DHCP.
- Phân tích quá trình cấu hình DHCP client.
- Cấu hình DHCP server.
- Xử lý sự cố DHCP.
- Phân tích yêu cầu đặt lại DHCP.

1.1. Chia địa chỉ mạng với NAT và PAT

1.1.1. Địa *chỉ riêng*

RFC 1918 dành riêng 3 dải địa chỉ IP sau:

- 1 địa chỉ lớp A: 10.0.0.0/8.
- 16 địa chỉ lớp B: 172.16.0.0 – 172.31.255.255 (172.16.0.0/12).

• 256 địa chỉ lớp C: 192.168.0.0-192.168.255.255 (192.168.0.0/16).

Những địa chỉ trên chỉ dùng cho mạng riêng, mạng nội bộ. Các gói dữ liệu có địa chỉ như trên sẽ không định tuyến được trên Internet.

Địa chỉ Internet công cộng phải được đăng ký với một công ty có thẩm quyền Internet, ví dụ như American Registry for Internet Numbers (ARIN) hoặc Réseaux IP Européens (RIPE) và The Regional Internet Registry phụ trách khu vực Châu Âu và Bắc Phi. Địa chỉ IP công cộng còn có thể được thuê từ một nhà cung cấp dịch vụ Internet (ISP). Địa chỉ IP riêng được dành riêng và có thể được sử dụng bởi bất kỳ ai. Điều này có nghĩa là có thể có 2 mạng hoặc 2 triệu mạng sử dụng cùng một địa chỉ mạng riêng. Router trên Internet sẽ không định tuyến các địa chỉ RFC 1918.ISP cấu hình Router biên ngăn không cho các lưu lượng của địa chỉ riêng được phát ra ngoài.

NAT mang đến rất nhiều lợi ích cho các công ty và Internet. Trước đây, khi không có NAT, một máy tính không thể truy cập Internet với địa chỉ riêng. Bây giờ, sau khi có NAT, các công ty có thể cấu hình địa chỉ riêng cho một hoặc tất cả các máy tính và sử dụng NAT để truy cập Internet.

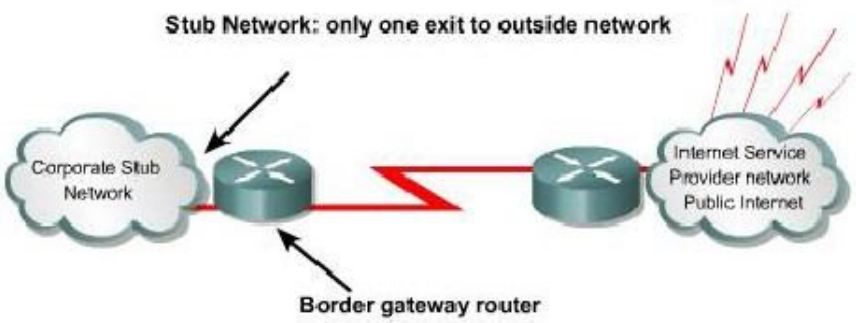
1.1.2. Giới thiệu NAT và PAT

NAT được thiết kế để tiết kiệm địa chỉ IP và cho phép mạng nội bộ sử dụng địa chỉ IP riêng. Các địa chỉ IP riêng sẽ được chuyển đổi sang địa chỉ công cộng định tuyến được bằng cách chạy phần mềm NAT đặc biệt trên thiết bị mạng. Điều này giúp cho mạng riêng càng được tách biệt và giấu được địa chỉ IP nội bộ.

NAT thường được sử dụng trên Router biên của mạng một cửa. Mạng một cửa là mạng chỉ có một kết nối duy nhất ra bên ngoài. Khi một host nằm trong mạng một cửa muốn truyền dữ liệu cho một host nằm bên ngoài nó sẽ truyền gói dữ liệu đến Router biên giới. Router biên giới sẽ thực hiện tiến trình NAT, chuyển đổi địa chỉ

riêng của host nguồn sang một địa chỉ công cộng định tuyến được. Trong thuật ngữ NAT, mạng nội bộ có nghĩa là tập hợp các địa chỉ mạng cần chuyển đổi địa chỉ. Mạng bên ngoài là tất cả các địa chỉ khác còn lai.

Mạng cục bộ chỉ có một cửa ra mạng bên ngoài.



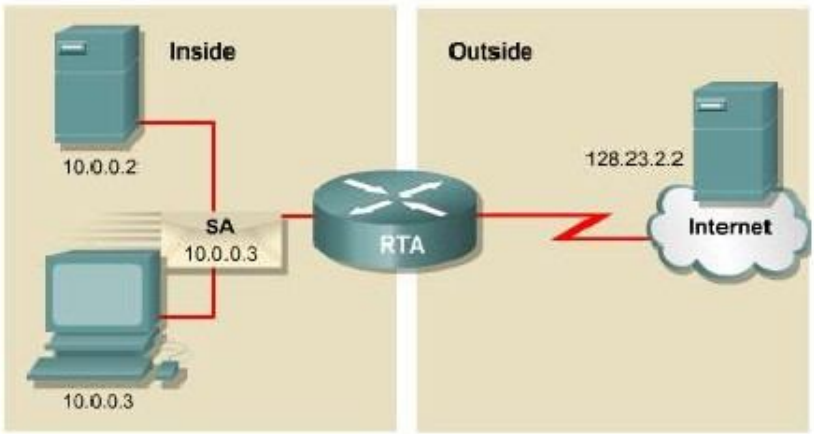
Hình 1.1.2.a. *Mạng một cửa*

Cisco định nghĩa các thuật ngữ NAT như sau:

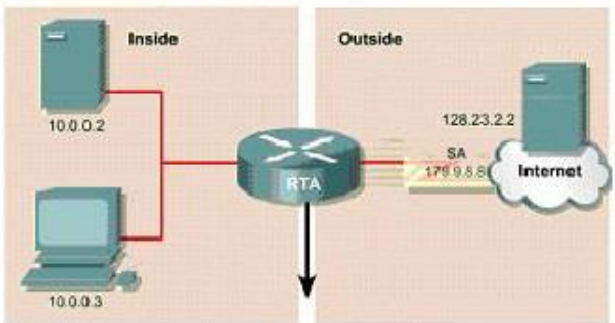
- Địa **chỉ cục bộ bên trong (Inside local address):** là địa chỉ được phân phối cho các host bên trong mạng nội bộ. Các địa chỉ này thường không phải là địa chỉ được cung cấp bởi InterNIC (Internet Network Information Center) hoặc bởi nhà cung cấp dịch vụ Internet. Địa chỉ này thường là địa chỉ riêng RFC 1918.

- Địa **chỉ toàn cục bên trong (Inside global address):** là địa chỉ IP hợp pháp được cung cấp bởi InterNIC hoặc bởi nhà cung cấp dịch vụ Internet. Địa chỉ này đại diện cho một hoặc nhiều địa chỉ nội bộ bên trong đối với thế giới bên ngoài.

- Địa **chỉ cục bộ bên ngoài (Outside local address):** là địa chỉ riêng của host nằm bên ngoài mạng nội bộ.
- Địa **chỉ toàn cục bên ngoài (Outside global address):** là địa chỉ công cộng hợp pháp của host nằm bên ngoài mạng nội bộ.

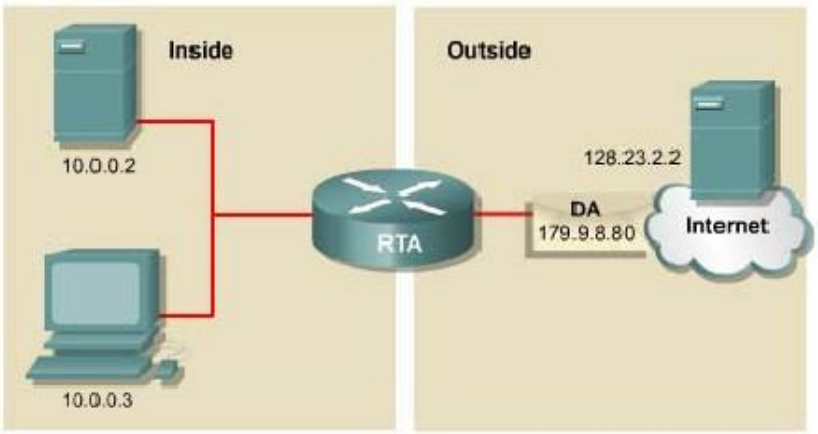


Hình 1.1.2.b. *Host nội bộ 10.0.0.3 muốn gửi gói dữ liệu cho một host nằm ngoài 128.23.2.2. Gói dữ liệu* được *gửi tới router biên giới RTA.*

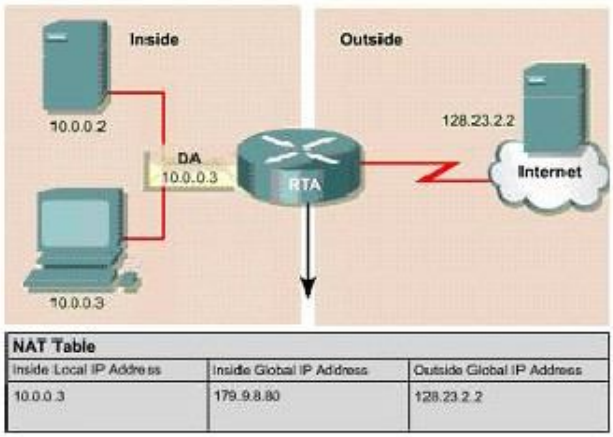


NAT Table		
Inside Local IP Address	Inside Global IP Address	Outside Global IP Address
10.0.0.3	179.9.8.80	128.23.2.2

Hình 1.1.2.c. *RTA nhận thấy gói dữ liệu này* được *gửi ra ngoài internet nên nó thực hiên tiến trình NAT, chuyển* đổi địa *chỉ nguồn 10.0.0.3 thành* địa *chỉ công cộng là 179.9.8.80. Sauk hi thực hiện NAT xong, gói dữ liệu từ RTA* đi *ra sẽ có* địa *chỉ nguồn là một* địa *chỉ công cộng hợp pháp 179.9.8.80.*



Hình 1.1.2.d. *Sau* đó *server 128..23.2.2 có thể gửi lại một gói trả lời. Khi* đó *gói trả lời sẽ có* địa *chỉ* đích *là 179.9.8.80.*



Hình 1.1.2.e. *RTA nhận thấy gói dữ liệu này* được *gửi từ bên ngoài vào trong mạng nội bộ. RTA sẽ tìm trong bảng NAT* để *ánh xạ từ* địa *chỉ* đích *công cộng sang* địa *chỉ riêng tương* ứng. *Sau khi thực hiên NAT xong, gói dữ liệu từ RTA phát vào trong mạng nội bộ sẽ có* địa *chỉ* đích *là* địa *chỉ riêng của host* đích *10.0.0.3.*

Xét ví dụ hình 1.1.2.b, đối với RTA:

- Địa chỉ nội bộ bên trong là 10.0.0.3.
- Địa chỉ toàn cục bên trong là: 179.9.8.80.
- Địa chỉ toàn cục bên ngoài là: 128.23.2.2.

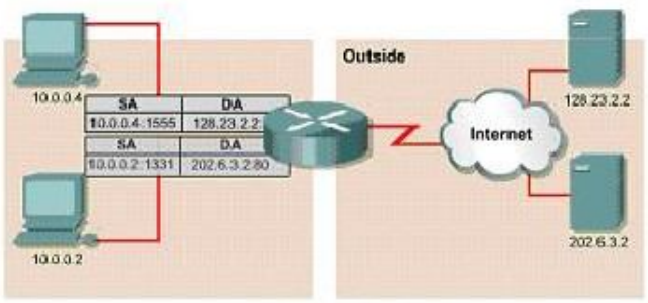
1.1.3. Các đặc điểm của NAT và PAT

Chuyển đổi NAT rất hữu ích cho nhiều mục đích khác nhau và có thể chuyển đổi động hoặc cố định. NAT cố định được thiết kế để ánh xạ **một-một,** từ **một** địa chỉ nội bộ sang **một** địa chỉ công cộng tương ứng duy nhất. Điều này rất tốt đối với những host cần phải có địa chỉ nhất định để truy cập từ Internet. Những host này có thể là các server toàn hệ thống hoặc các thiết bị mạng.

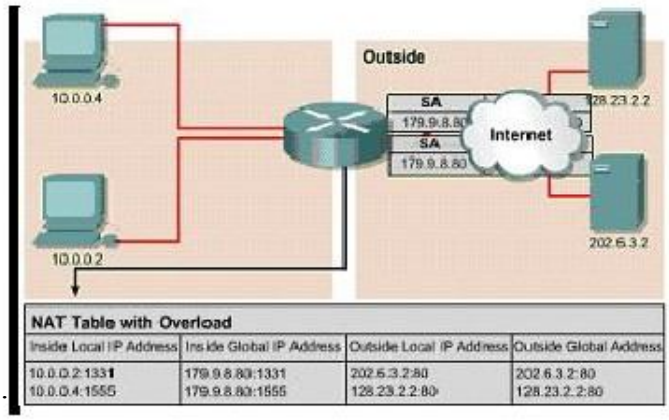
NAT động được thiết kế để ánh xạ **một** địa chỉ IP riêng sang **một** địa chỉ công cộng một cách tự động. Bất kỳ địa chỉ IP nào nằm trong dải địa chỉ IP công cộng đã được định trước đều có thể được gán cho một host bên trong mạng. Overloading hoặc PAT có thể ánh xạ **nhiều** địa chỉ IP riêng sang **một** địa chỉ IP công cộng vì mỗi địa chỉ riêng được phân biệt bằng số port.

PAT sử dụng số port nguồn cùng với địa chỉ IP riêng bên trong để phân biệt khi chuyển đổi. Số port được mã hóa 16 bit. Do đó có tới 65.536 địa chỉ nội bộ có thể được chuyển đổi sang một địa chỉ công cộng. Thực tế thì số lượng port có thể gán cho một địa chỉ IP là khoảng 4000 port. PAT sẽ cố gắng giữ nguyên số port nguồn ban đầu. Nhưng nếu số port này đã bị sử dụng thi PAT sẽ lấy số port còn trống đầu tiên trong các nhóm port 0-511, 512-1023, 1024-65535.

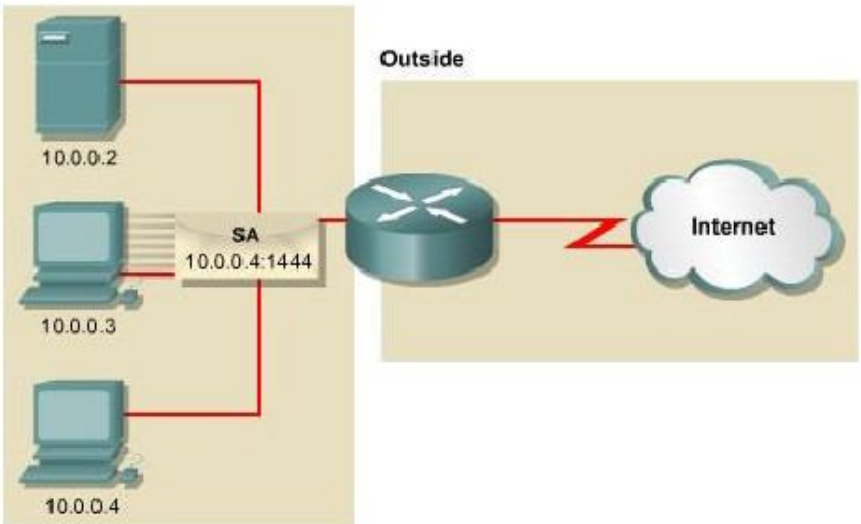
Khi không còn số port nào còn trống và vẫn còn địa chỉ IP công cộng khác đã được cấu hình thì PAT sẽ chuyển sang địa chỉ IP công cộng kế tiếp và bắt đàu xác định số port nguồn như trên. Quá trình này sẽ được thực hiện cho đến khi nào hết số port và địa chỉ IP công cộng còn trống.



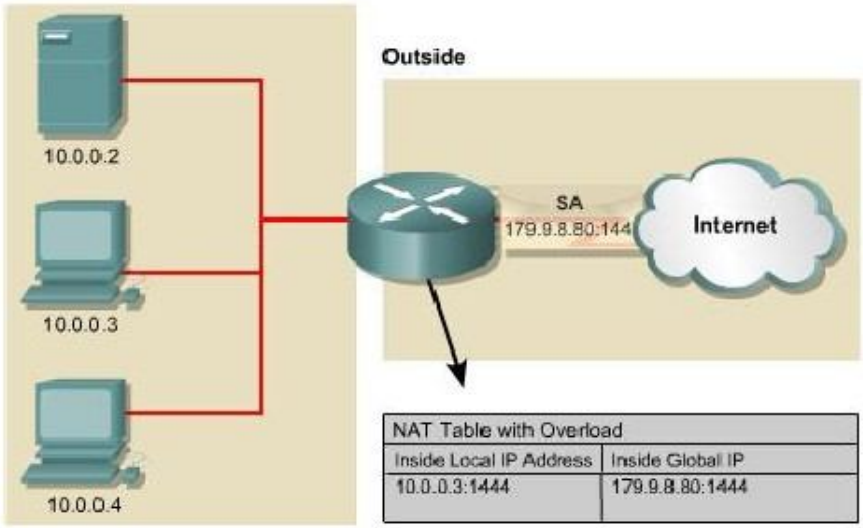
Hình 1.1.3.a.



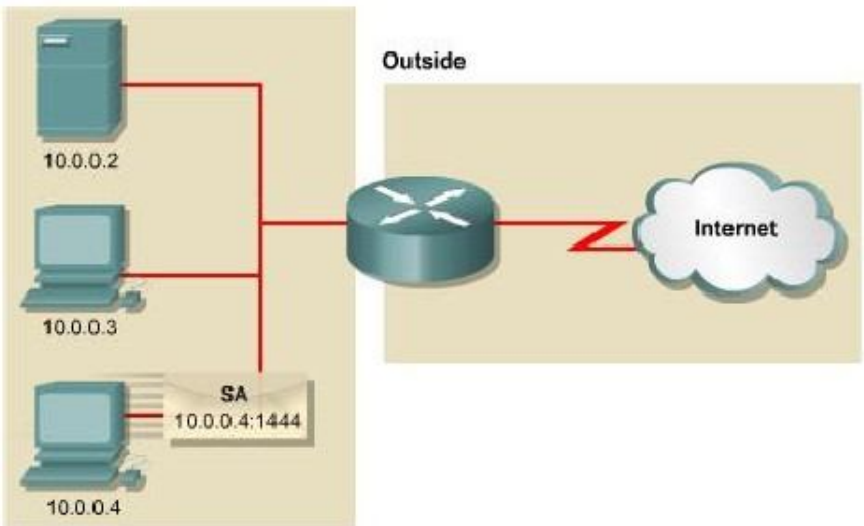
Hình 1.1.3.b.



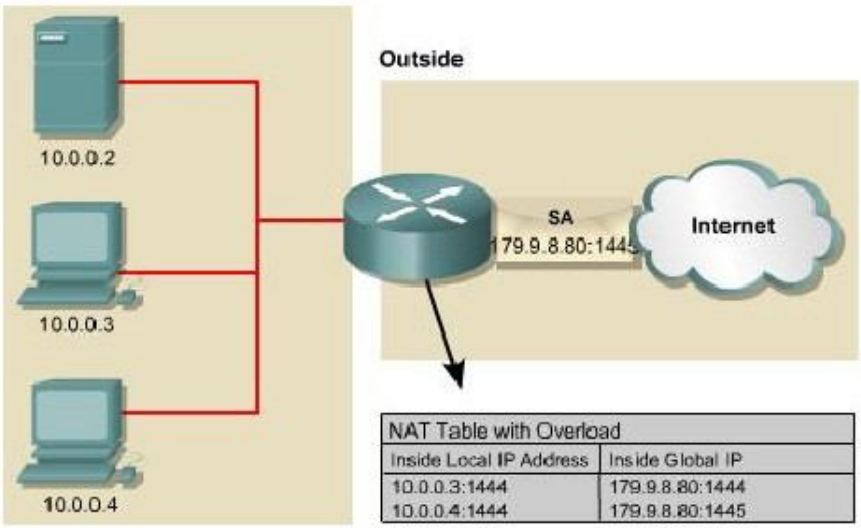
Hình 1.1.3.c. *Host 10.0.0.3 gửi gói dữ liệu ra internet. Trong gói dữ liệu này,* địa *chỉ IP nguồn là 10.0.0.3, port là* ***1444***



Hình 1.1.3.d. *Router thực hiện chuyển* đổi địa *chỉ IP nguồn từ 10.0.0.3 sang* địa *chỉ 179.9.8.80, port nguồn vẫn giữ nguyên là 1444.*



Hình 1.1.3.e. *Bây giờ Host 10.0.0.4 cũng gửi gói dữ liệu ra internet với* địa *chỉ nguồn là 10.0.0.4, port nguồn là 1444*



Hình 1.1.3.f. *Router thực hiện chuyển đổi địa chỉ IP nguồn từ 10.0.0.4 sang 179.9.8.80. Port nguồn là 1444 lúc này phải đổi sang 1445. Như vậy theo như bảng NAT trong hình ta thấy địa chỉ công cộng 179.9.8.80: 1444 là tương ứng với 10.0.0.3:1444, 179.9.8.80:1445 tương ứng với 10.0.0.4:1444. Bằng cách sử dụng kết hợp với số port như vậy, PAT có thể ánh xạ một địa chỉ IP công cộng cho nhiều địa chỉ riêng bên trong.*

NAT cung cấp những lợi điểm sau:

- Không cần phải gán địa chỉ IP mới cho từng host khi thay đổi sang một ISP mới. Nhờ đó có thể tiết kiệm được thời gian và tiền bạc.
- Tiết kiệm địa chỉ thông qua ứng dụng ghép kênh cấp độ port. Với PAT, các host bên trong có thể chia sẻ một địa chỉ IP công cộng để giao tiếp với bên ngoài. Với cách cấu hình này, chúng ta cần rất ít địa chỉ công cộng, nhờ đó có thể tiết kiệm địa chỉ IP.
- Bảo vệ mạng an toàn vì mạng nội bộ không để lộ địa chỉ và cấu trúc bên trong ra ngoài.

1.1.4. Cấu hình NAT và PAT

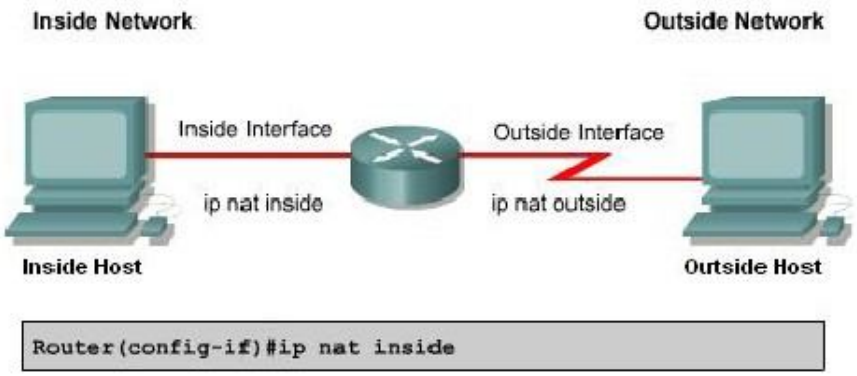
1.1.4.1. Chuyển đổi cố định

Để cấu hình chuyển đổi cố định địa chỉ nguồn bên trong, chúng ta cấu hình các bước như sau:

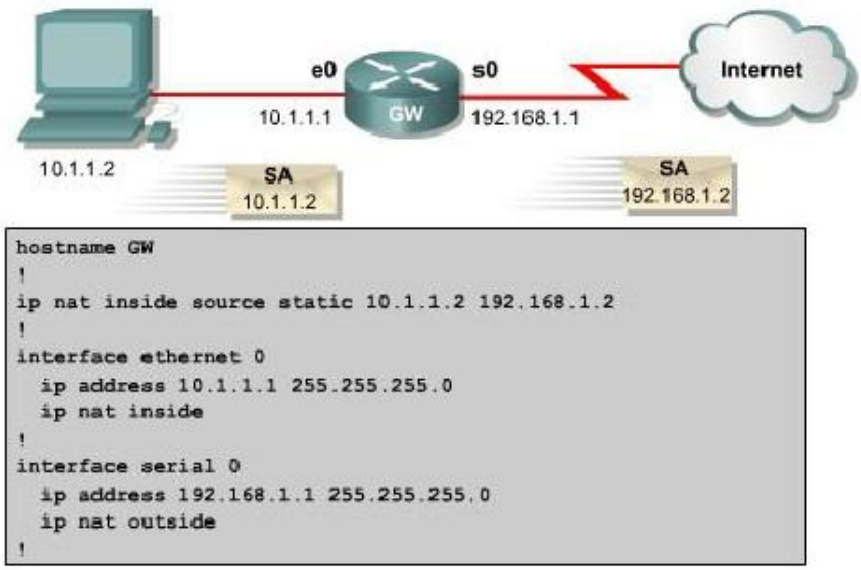
Bước	Thực hiện	Ghi chú
1	Thiết lập mối quan hệ chuyển đổi giữa địa chỉ nội bộ bên trong và địa chỉ đại diện cục, bạn bên ngoài *Router (config)* # **ip nat inside** **source static** *local-ip global-ip*	Trong chế độ cấu hình toàn dùng câu lệnh **no ip nat inside source static** để xóa sụ chuyển đổi địa chỉ cố định.
2	Xác định công kết nối vòa mạng bên trong. *Router (config)* # **interface** *type number*	Sau khi gõ lệnh **interface,** dấu nhắc của dòng lệnh sẽ chuyển từ (config) # sang (config-if) #
3	Đánh dấu công này là công kết nối vào mạng nội bộ bên trong. *Router (config-if)* # **ip nat inside**	
4	Thóat khỏi chế độ cấu hình công hiện tại. *Router (config-if)* # **exit**	
5	Xác định công kết nối ra mạng công cộng bên ngoài. *Router (config)* # **interface** *type number*	

6	Đánh dấu cổng này là cổng kết nối ra mạng công cộng bên ngoài. *Router (config-if) #* **ip nat outside**	

Hình vẽ - 2 hình



Hình 1.1.4.a *Sự chuyển* đổi địa *chỉ sẽ* được *thực hiện giữa hai cổng inside và outside*



Hình 1.1.4.b. *Cấu hình NAT chuyển đổi cố định từ địa chỉ 10.1.1.2 sang 192.168.1.2. Khi có một gói dữ liệu từ host 10.1.1.2 được gửi ra ngoài internet, router GW sẽ chuyển đổi địa chỉ nguồn 10.1.1.2 của gói dữ liệu sang địa chỉ 192.168.1.2 trước khi phát gói ra cổng s0.*

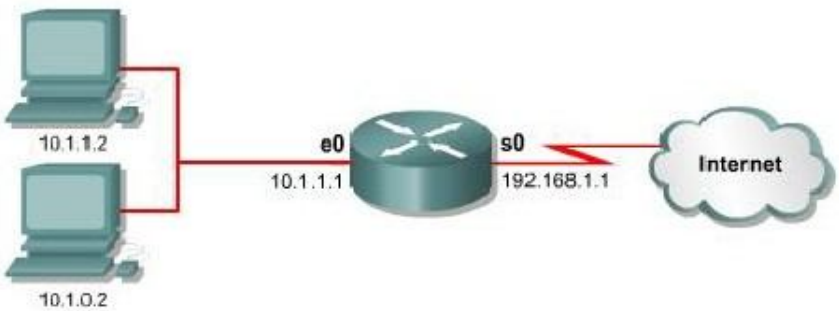
1.1.4.2. Chuyển đổi động

Để Chuyển đổi động địa chỉ nguồn bên trong, chúng ta cấu hình theo các bước như sau:

Bước	Thực hiện	Ghi chú
1	Xác định dải địa chỉ đại diện bên ngoài *Rourter (config) #* **ip nat pool** *name start-ip end-ip* [netmask *netmask /prefix-length prefix-length]*	Trong chế độ cấu hình toàn cục, gõ lệnh **no ip nat pool** *name* để xóa dải địa chỉ đại diên bên ngoài.
2	Thiết lập ACL cơ bản cho phép những địa Trong chế độ cấu hình chỉ nội bộ bên trong nào được chuyển đổi. *Router (config) #* **access-list** *access-list-number* **permit** *source [source-wildcard]*	toàn cục, gõ lệnh **no access-list** *access-list-number* để xóa ACL đó.
3	Thiết lập môi liên quan giữa địa chỉ nguồn Trong chế độ cấu hình đã được xác định trong ACL ở bước trên với toàn cục, gõ lênh **no ip** dải địa chỉ đại diện bên ngoài: *Router (config) #* **ip nat inside source list** *access-list-number* **pool** *name*	**nat inside source** để xóa sự chuyển đổi động này
4	Xác định công kết nối vào mạng nội bộ	Sau khi gõ xong lệnh

	Router (config) # **interface** *type number*	**interface,** dấu nhắc của dòng lệnh sẽ chuyển đổi từ config sang (config-if)#
5	Đánh dấu cổng này là cổng kết nối vào mạng nội bộ. *Router (config-if) #* ***ip nat inside***	
6	Thóat khỏi chế độ cổng hiện tại. *Router (config) #* **exit**	
7	Xác định cổng kết nối ra bên ngoài. *Router (config) #* **interface** *type number*	
8	Đánh dấu cổng này là cổng kết nối ra bên ngoài. *Router (config) #* **ip nat outside**	

Danh sách điều khiển truy cập (ACL – Access Control List) cho phép khai báo những địa chỉ nào được chuyển đổi. Bạn nên nhớ là kết thúc một ACL luôn có câu lệnh ẩn cấm tuyệt đối để tránh những kết quả không dự tính được khi một ACL có quá nhiều điều kiện cho phép. Cisco khuyến cáo là không nên dùng điều kiện cho phép tất cả **permit any** trong ACL sử dụng cho NAT vì câu lệnh này làm hao tốn quá nhiều tài nguyên của Router và do đó có thể gây ra sự cố mạng.




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

Hình 1.1.4.c

Xét ví dụ hình 1.1.4.c: Dải địa chỉ công cộng đại diện ben ngoài có tên là nat-pool1, bao gồm các địa chỉ từ 179.9.8.80 đến 179.9.95. Địa chỉ nội bộ bên trong được phép chuyển đổi được định nghĩa trong access-list 1 là 10.1.0.0 – 10.1.0.255. Như vậy, gói dữ liệu nào trong mạng nội bộ đi ra ngoài Internet có địa chỉ nguồn nằm trong dải địa chỉ 10.1.0.0 – 10.1.0.255 sẽ được chuyển đổi địa chỉ nguồn sang một trong bất kỳ địa chỉ nào còn trống trong dải địa chỉ công cộng 179.9.8.80 – 179.9.8.95. Host 10.1.1.2 sẽ không được chuyển đổi địa chỉ vì địa chỉ của nó không được cho phép trong acces-list 1, do đó nó không truy cập được Internet.

Overloading hay PAT

Overloading được cấu hình theo hai cách tùy theo địa chỉ IP công cộng được cấp phát như thể nào. Một ISP có thể cho một hệ thống mạng của khách hàng sử dụng chung một địa chỉ IP công cộng duy nhất, đia jchỉ IP công cộng này chính là địa chỉ của cổng giao tiếp trên Router nối về ISP. Sau đây là ví dụ cấu hình cho tình huống này:

Router (config) # access-list 1 permit 10.0.0.0 0.0.255.255

Router (config) ip nat inside source list 1 interface serial0/0 overload

Bước	Thực hiện	Ghi chú
1	Tạo ACL để cho phép những địa chỉ nội bộ Trong chế độ cấu hình nào được chuyển đổi. *Router(config) #* **access-list** *acl-number* **permit** *source [source-wildcard]*	toàn cục, gõ lệnh **no access-list** *access-list-number* để xóa access-list tương ứng.
2A	Thiết lập mối liên quan giữa địa chỉ nguồn đã được xác định trong access-list ở bước trên với địa chỉ đại diện là địa chỉ của cổng kết nối với bên ngoài. *Router (config) #* **ip nat inside source list** *acl-number* **interface** *interface* **overload**	Trong chế độ cấu hình toàn cục, gõ lệnh **no ip nat inside source** để xóa sự chuyển đổi động này. Từ khóa **overload** để cho phép chạy PAT
Hoặc 2B	Khai báo dải địa chỉ đại diện bên ngoài dùng overload. *Router (config)* **ip nat pool** *name start-ip end-ip* *[netmask netmask /* **prefix-length** *prefix-length]* Thiết lập chuyển đổi overload giữa địa chỉ nội bộ đã được xác định trong ACL ở bước 1 với dải địa chỉ đại diện bên ngoài mới khai báo ở	

	trên. Router (config) # **ip nat inside source list** *acl-number* **pool** *name* **overload**	
3	Xác định công kết nối với mạng nội bộ. Router (config) # **interface** *type number* Router (config-if) # **ip nat inside**	Sau khi gõ lệnh **interface,** dấu nhắc của dòng lệnh sẽ được đổi từ (config)# sang (config-if)#
4	Xác định công kết nối với bên ngoài. Router (config) # **interface** *type number* Router (config-if) # **ip nat outside.**	

Một cách khác để cấu hình Overload là khi ISP cung cấp một hoặc nhiều địa chỉ IP công cộng để cho hệ thống mạng khách hàng sử dụng làm dải địa chỉ chuyển đổi PAT. Cấu hình ví dụ cho tình huống này như sau:

- Xác định địa chỉ nội bộ được phép chuyển đổi là 10.0.0.0/16:

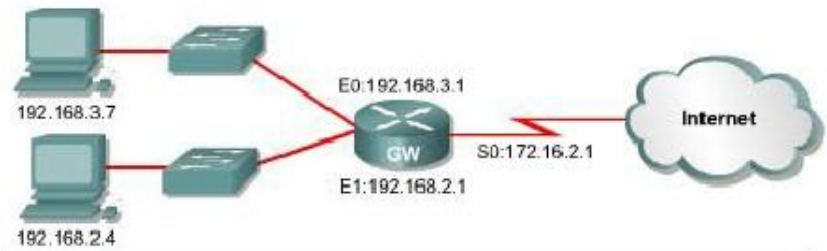
Router (config) # access-list 1 permit 10.0.0.0.0.0.255.255

- Khai báo dải địa chỉ đại diện bên ngoài với tên là nat-pool2, bao gồm các địa chỉ trong subnet 179.9.8.20/28:

  Router (config) # ip nat pool nat-pool2 179.9.8.20 netmask 255.255.255.240

- Thiết lập sự chuyển đổi Overload địa chỉ nội bộ được xác định trong access-list 1 với dải địa chỉ đại diện nat pool2:

  Router (config) # ip nat inside source list 1 pool nat-pool2 overload




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Hình 1.1.4.d.

Xét ví dụ hình 1.1.4.d: địa chỉ nội bộ bên trong được phép chuyển đổi được xác định trong access-list 1 là 192.168.2.0/24 và 192.168.3.0/24. Địa chỉ đại diện bên ngoài là địa chỉ của cổng serial 0, cổng kết nối ra Internet. Như vậy phải toàn bộ địa chỉ bên trong được chuyển đổi PAT với một địa chỉ IP đại diện duy nhất là địa chỉ của cổng kết nối ra Internet, cổng serial 0.

1.1.5. Kiểm tra cấu hình PAT

Sau khi NAT đã được cấu hình, chúng ta có thể dùng lệnh clear và show để kiểm tra hoạt động của NAT.

Mặc định, trong bảng chuyển đổi NAT động, mỗi một cặp chuyển đổi địa chỉ sẽ bị xóa đi sau một khoảng thời gian không sử dụng. Với chuyển đổi không sử dụng chỉ số Port thì khoảng thời gian mặc định là 24 giờ. Chúng ta có thể thay đổi khoảng thời gian này bằng lệnh **ip nat translation timeout** *timeout_seconds* trong chế độ cấu hình toàn cục.

Các thông tin về sự chuyển đổi có thể được hiển thị bằng các lệnh sau:

Lệnh	**Giải Thích**
Clear ip nat translation *	Xóa mọi cặp chuyển đổi địa chỉ động trong bảng NAT.
Clear ip nat translation inside *global-ip local-ip* [outside *local-ip global-ip]*	Xóa một cặp chuyển đổi địa chỉ động bên trong hoặc cả bên trong và bên ngoài tương ứng với địa chỉ cụ thể được khai báo trong câu lệnh.
Clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [outside *local-ip local-port global-ip global-port]*	Xóa một cặp chuyển đổi địa chỉ động mở rộng.
Show ip nat translations	Hiển thị bảng NAT đang hoạt động.
Show ip nat statistics	Hiển thị trạng thái hoạt động của NAT.

```
Router#show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
172.16.131.1          10.10.10.1         ---                ---
```

Hình 1.1.5.a

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5  Misses:0
```

Hình 1.1.5.b

Chúng ta có thể dùng lệnh **show run** để kiểm tra lại các giá trị cần khai báo trong các câu lệnh cấu hình NAT, access-list, interface.

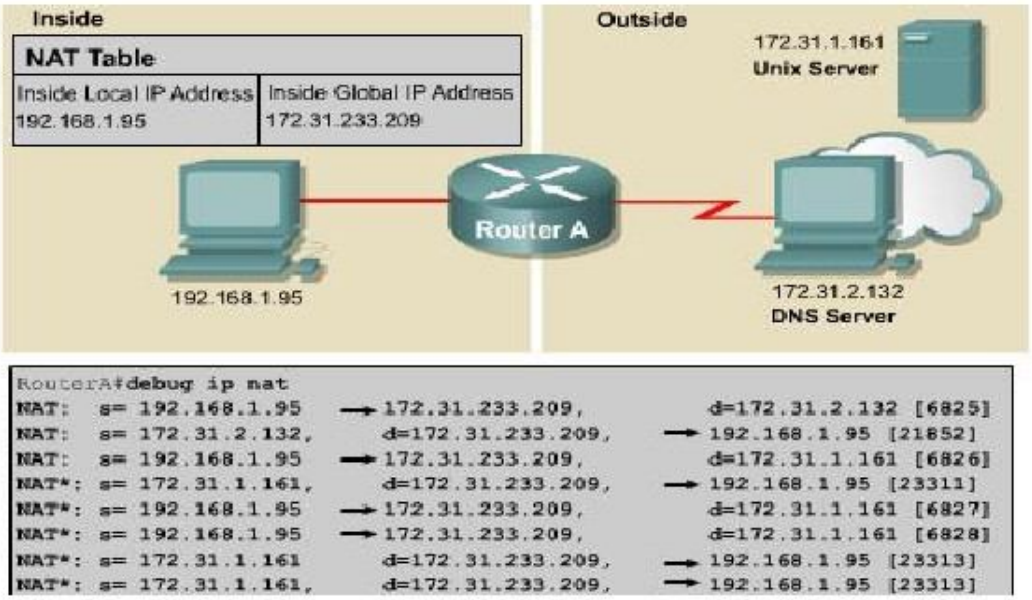
1.1.6. Xử lý sự cố cấu hình NAT và PAT

Thường rất khó xác định nguyên nhân của sự cố khi kết nối IP bị sự cố trong môi trường NAT. Nhiều khi chúng ta nhầm lẫn là do NAT gây ra nhưng thực sự nguyên nhân lại nằm ở chỗ khác.

Khi cố gắng xác định nguyên nhân sự cố của một kết nối IP, chung ta nên cố gắng xác định loại trừ khả năng từ NAT trước. Sau đay là các bước để kiểm tra hoạt động của NAT:

1. Dựa vào tập tin cấu hình, xác định rõ ràng NAT thực hiện những gì.
2. Kiểm tra bảng NAT xem các chuyển đổi địa chỉ có đúng không.
3. Kiểm tra hoạt động NAT xảy ra như thế nào bằng các lệnh **show** và **debug.**
4. Xem chi tiết những gì xảy ra cho một gói dữ liệu và kiểm tra xem router có định tuyến đúng cho gói dữ liệu hay không.

Sử dụng lệnh **debug ip nat** để kiểm tra hoạt động của NAT, hiển thị các thông tin về mỗi gói được chuyển đổi NAT bởi router. Lệnh **debug ip nat** *detal* còn cung cấp thêm một số thông tin liên quan đến sự chuyển của mỗi gói giúp chúng ta xác định lỗi, ví dụ như lỗi không xác định được địa chỉ đại diện bên ngoài.



Hình 1.1.6

Xét ví dụ hình 1.1.6. Hai dòng đầu tiên cho thấy các gói yêu cầu và trả lời DNS được phát đi. Những dòng còn lại cho biết về một kết nối Telnet từ một host bên trong tới một host bên ngoài mạng.

Để giải mã những thông tin hiển thị của lệnh **debug,** chúng ta dựa vào những điểm mấu chốt sau:

- Dấu * kế bên từ NAT cho biết sự chuyển đổi đang được thực hiện trên đường chuyển mạch nhanh. Gói dữ liệu đầu tiên của một phiên đối thoại luôn được xử lý chuyển mạch nên chuyển mạch chậm. Các gói dữ liệu tiếp theo được truyền chuyển mạch nhanh với bộ đệm, không cần xử lý nhiều như gói đầu tiên.

- S= a.b.c.d là địa chỉ nguồn.
- Địa chỉ nguồn a.b.c.d được dịch sang w.x.y.z.
- D=e.f.g.h là địa chỉ đích.
- Giá trị trong giấu ngoặc vuông là chỉ số danh đinh IP. Thông tin này có thể sẽ hữu dụng vì dựa vào đó chúng ta sẽ tìm được những gói dữ liệu tương ứng được phân tích từ những phần mền phân tích giao thức khác.

1.1.7. Những vấn đề của NAT

NAT có những ưu điểm sau:

- Tiết kiệm địa chỉ đăng ký hợp pháp bằng cách cho phép sử dụng địa chỉ riêng.
- Tăng tính linh hoạt của các kết nối ra mạng công cộng. Chúng ta có thể triển khai nhiều dải địa chỉ chia tải để đảm bảo độ tin cậy của kết nối mạng công cộng.
- Nhất quán hồ sơ địa chỉ mạng nội bộ. Nếu mạng không sử dụng địa chỉ IP riêng và NAT mà sử dụng địa chỉ công cộng thì khi thay đổi địa chỉ công cộng, toàn bộ hệ thống mạng phải đặt lại địa chỉ. Chi phí cho việc đặt lại địa chỉ toàn bộ các thiết bịi mạng nội bộ được giữ nguyên khi thay đổi địa chỉ công cộng.

NAT cũng không phải là không có nhược điểm. Khi chuyển đổi địa chỉ như vậy sẽ làm mất đi một số chức năng đặc biệt của giao thức và ứng dụng có cần đến các thông tin địa chỉ IP trong gói IP. Do đó cần phải có thêm các hỗ trợ khác cho thiết bị NAT.

NAT làm tăng thời gian trễ. Thời gian trễ chuyển mạch sẽ lớn hươn do đó phải chuyển đổi từng địa chỉ IP trong mỗi dữ liệu. Gói dữ liệu đầu tiên luôn phải sử lý chuyển mạch nên thời gian chuyển mạch nhanh hơnnếu có bộ đệm.

Hiệu suất hoạt động cũng là một vấn đề cần được quan tâm vì NAT được thực hiện trong tiến trình chuyển mạch. CPU phải được kiểm tra từng gói dữ liệu để quyết định gói dữ liệu đó có cần chuyển đổiđịa chỉ hay không. CPU phải thay đổi phần gói IP của gói dữ liệu và cũng có htể phải thay cả phần đóng gói TCP hoặc UDP.

Một nhược điểm đáng kể khi sử dụng NAT là sự mất đi khả nặng truy tìm địa chỉ IP đầu cuối-đến-đầu cuối. Việc truy theo gói dữ liệu sẽ trở nên khó hơn do gói dữ liệu thay đổi địa chỉ nhiều lần qua nhiều trạm NAT. Hacker sẽ rất khó khăn khi muốn xác định địa chỉ nguồn hoặc đích của gói dữ liệu.

NAT cũng làm cho một số ứng dụng sử dụng địa chỉ IP không hoạt động được vì nó giấu địa chỉ IP đầu cuối-đến-đầu cuối. Những ứng dụng sử dụng địa chỉ vật lý thay vì sử dụng tên miền sẽ không đến được đích nằm sau router NAT. Đôi khi, sự cố này có thể tránh được bằng cách ánh xạ NAT cố định.

Cisco IOS NAT hỗ trợ các loại lưu lượng sau:

- ICMP
- File Transfer Protocol (FTP), bao gồm lệnh PPRRT và PÁV.
- Dịch vụ NetBIOS qua TCP/IP, gói dự liệu, tên và phiên giao tiếp.
- RealNetworks' RealAudio
- White Pines' CUSeeMe
- Xing Technologies' StreamWorks
- DNS "A" and "PTR" queries
- H.323/Microsoft NetMeeting, IOS versions 12.0(1)/ 12.0(1) T và sau đó.
- VDOnet's VDOLive, IOS version 11.3(4)11.3(4)T và sau đó.
- VXtreme's Web Theater, IOS versions 11.3(4)11.3(4)T và sau đó.
- IP Multicast, IOS version 12.0(1)T chỉ chuyển đổi địa chỉ nguồn.

Cisco IOS NAT không hỗ trợ các loại giao thức sau:

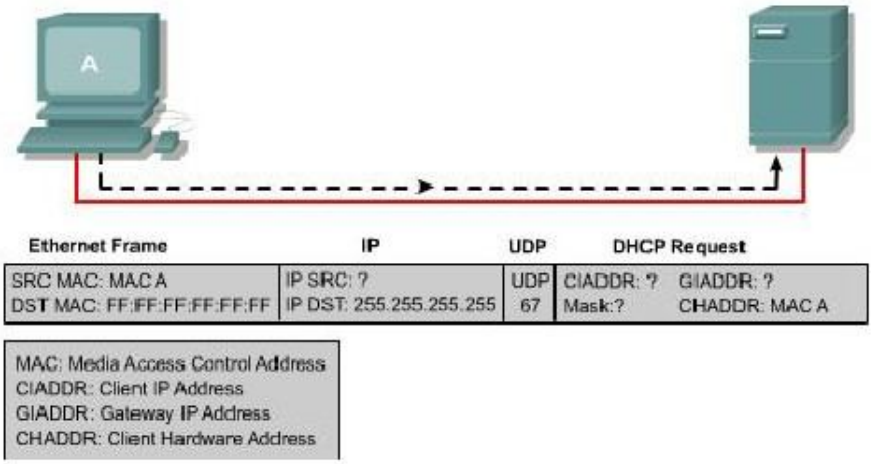
- Thông tin cập nhật bảng định tuyến.
- Chuyển đổi vùng DNS.
- BOOTP
- Giao thức talk and ntalk.
- Giao thức quản lý mạng đơn giản – Simple Network Management Protocol (SNMP)

1.2. DHCP

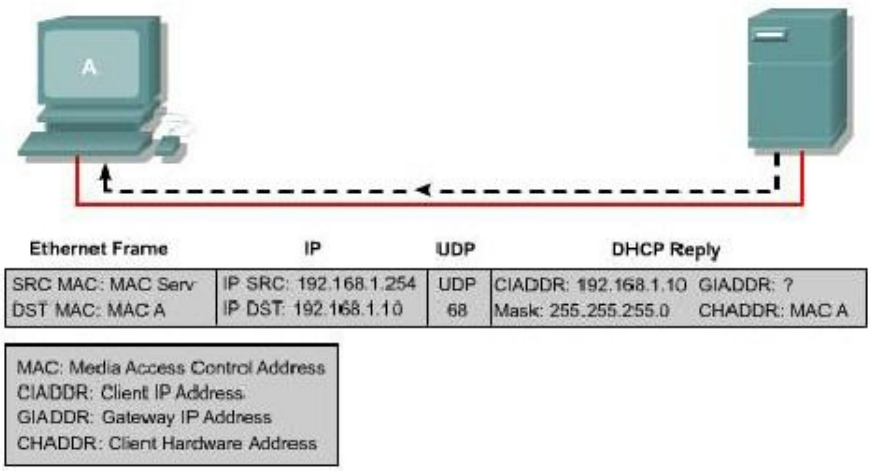
1.2.1. Giới thiệu DHCP

Giao thức cấu hình hoạt động (DHCP – Dynamic Host Configuration Protocol) làm việc theo chế độ client-server. DHCP cho phép các DHCP client trong một mạng IP nhận cấu hình IP của mình từ một DHCP server. Khi sử dụng DHCP thì công việc quản lý mạng IP sẽ ít hơn vì phần lớn cấu hình IP của client được lấy về từ server. Giao thức DHCP được mô tả trong RFC 2131.

Một DHCP client có thể chạy hầu hết các hệ điều hành Windows, Netvell Netửae, Sun Solaris, Linux và MAC OS. Client yêu cầu server DHCP cấp một địa chỉ cho nó. Server này quản lý việc cấp phát địa chỉ IP, sẽ gửi trả lời cấu hình IP cho client. Một DHCP có thể phục vụ cho nhiều subnet khác nhau nhưng không phục vụ cho cấu hình router, switch và các server khác vì những thiết bị này cần phải có địa chỉ IP cố định.



Hình 1.2.1.a. *Client gửi trực tiếp quảng bá một yêu cầu DHCP. Trường hợp đơn giản nhất là có DHCP server nằm trong cùng subnet với client, server DHCP này sẽ nhận được gói yêu cầu. Server thấy phần GIADDR bỏ trống thì biết client nằm trong cùng subnet với server. Đồng thời server sẽ đọc địa chỉ vật lý (địa chỉ MAC) của client.*



Hình 1.2.1.b. *Server sẽ lấy một địa chỉ IP trong dải địa chỉ tương ứng để cấp cho client. Sau đó server dùng địa chỉ của vật lý của client để gửi gói trả lời lại cho client.*

Hình 1.2.1.c. *Hệ điều hành trên DHCP client sẽ dùng những thông tin nhận được trong gói trả lời server để cấu hình IP cho client đó.*

Server chạy DHCP thực hiện tiến trình xác định địa chỉ IP cấp cho client. Client sử dụng địa chỉ được cấp từ server trong một khoảng thời gian nhất định do người quản trị mạng quy định. Khi thời này hết hạn thì client phải yêu cầu cấp lại địa chỉ mới mặc dù thông thường client sẽ vẫn được cấp lại địa chỉ cũ.

Các nhà quản trị mạng thường sử dụng dịch vụ DHCP vì giải pháp này giúp quản lý hệ thống mạng dễ và có khả năng mở rộng. Cisco router có thể sử dụng Cisco IOS có hỗ trợ Easy IP để làm DHCP server. Mặc định , Easy IP cấp cấu hình IP cho client sử dụng trong 24 tiếng. Cơ chế này rất tiện lợi cho các văn phòng nhỏ hoặc những văn phòng tại nhà, người sử dụgn tại nhà có thể tận dụng diạhc vụ DHCP và NAT của router mà không cần phải có thêm một server NT hoặc UNIX. Người quản trị mạng cài đặt dải địa chỉ cho DHCP server còn có thể cung cấp nhiều thông tin khác như địa chỉ DNS server, địa chỉ WINS server và tên miền. Hầu hết các DHCP server đều cho phép người quản trị mạng khai báo những địa chỉ MAC nào cần phục vụ và tự động cấp cho những địa chỉ MAC này địa chỉ IP không thay đổi mỗi lần chúng yêu cầu.

DHCP sử dụng giao thức UDP (User Datagram Protocol) làm giao thức vận chuyển của nó. Client gửi thông điệp cho server trên port 67. Server gửi thông điệp cho client trên port 68.

1.2.2. Những điểm khác nhau giữa BOOTP và DHCP

Đầu tiên cộng đồng Internet phát triển giao thức BOOTP để cấu hình cho máy trạm không có ổ đĩa. BOOTP được định nghĩa trong RFC 951 vào năm 1985. Là một phiên bản đi trước của DHCP nên BOOTP cũng có nhiều đặc điểm hoạt động tương tự như DHCP. Cả hai giao thức này đêgu dựa trên cơ sở client-server và sử dụng port UDP 67, 68. Hai port này hiện vẫn được biết đến như là port BOOTP.

Một cấu hình IP cơ bản bao gồm 4 thông tin sau:

- Địa chỉ IP.
- Địa chỉ Gateway.
- Subnet mask.
- Địa chỉ DNS server.

BOOTP không tự động cấp phát địa chỉ IP cho một host. Khi client yêu cầu một địa chỉ IP, BOOTP server tìm trong bảng đã được cấu hình trước xem có hàng nào tương ứng với địa chỉ MAC của client hay không.Nếu có thì địa chỉ IP tương ứng sẽ được cung cấp cho client. Điều này có nghĩa là địa chỉ MAC và địa chỉ IP tương ứng phải được cấu hình trước trên BOOTP server.

Sau đây là hai điểm khác nhau cơ bản giữa BOOTP và DHCP:

- DHCP cấp một địa chỉ IP cho một client trong một khoảng thời gian nhất định. Hết khoảng thời gian này địa chỉ IP có thể được cấp cho client khác. Client có thể lấy địa chỉ mới hoặc vẫn có thể tiếp tục giữ địa chỉ cũ.
- DHCP cung cấp cho client nhiều thông tin cấu hình IP khác như địa chỉ WINS server, tên miền.

BOOTP	DHCP
Ánh xạ cố định giữ địa chỉ MAC và Ánh xạ tự động giữa địa chỉ MAC và địa chỉ IP	dải địa chỉ IP tương ứng.
Cấp cố định	Cấp trong một khoảng thời gian nhất định
Chỉ cung cấp 4 thông tin cơ bản của Có thể cung cấp hơn 30 thông tin cấu cấu hình IP	hình IP

1.2.3. Những điểm chính của DHCP

Có 3 cơ chế dùng để cấp phaqst một địa chỉ IP cho client:

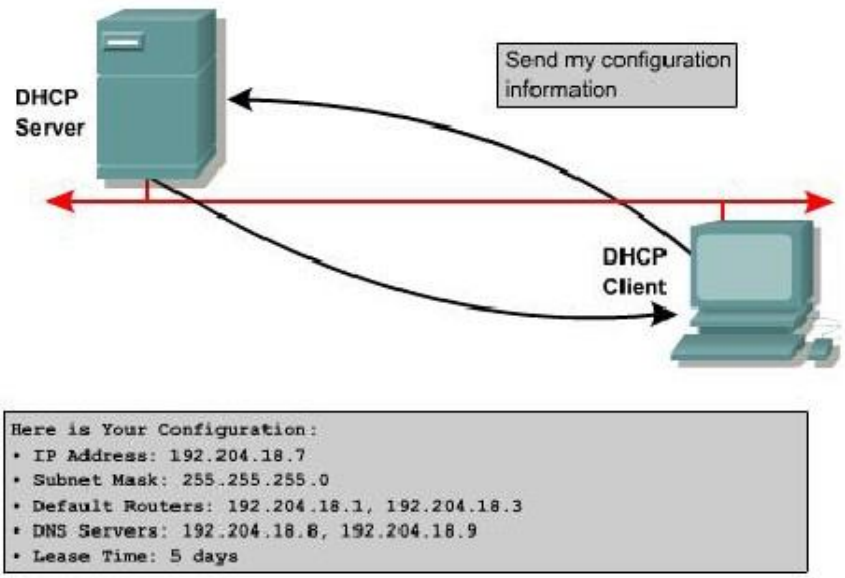
- Cấp phát tự động – DHCP tự động chọn một địa chỉ IP trong dải địachỉ được cấu hình và cấp địa chỉ IP đó cố định, không thay đổi cho một client.
- Cấp phát cố định – Địa chỉ IP của một client do người quản trị mạng quyết định. DHCP chỉ truyền địa chỉ này cho client đó.
- Cấp phát động – DHCP cấp và thu hồi lại một địa chỉ IP của client theo một khoảng thời gian giới hạn.

Trong phần này chúng ta tập trung vào cơ chế cấp phát động. Một số thông số cấu hình được liệt kê trong IÈT RFC 1533 là:

- Subnet mask
- Router
- Tên miền
- Server DNS
- WINS server

Chúng ta có thể tạo trên DHCP server nhiều dải địa chỉ IP và thông số như trên tương ứng. Mỗi một dải địa chỉ dành riêng cho một subnet IP. Điều này cho phép

có thể có nhiều DHCP cùng trả lời và IP client có thể di động. Nếu có nhiều server cùng trả lời thì client có thể chọn một trả lời duy nhất.



Hình 1.2.3

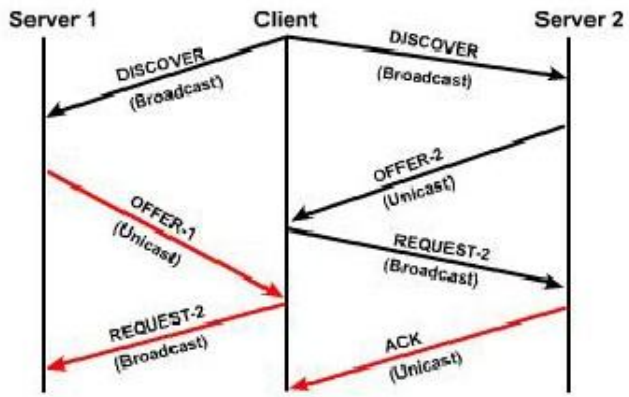
1.2.4. Hoạt động của DHCP

Quá trình DHCP client lấy cấu hình DHCP diễn ra theo các bước sau:

1. Client phải có cấu hình DHCP khi bắt đầu tiến trình tìm các thành viên trong mạng. Client gửi một yêu cầu cho server để yêu cầu cấu hình IP. Đôi khi client có thể đề nghị trước địa chỉ IP mà nó muốn, ví dụ như khi nó hết thời gian sử dụng địa chỉ IP hiện tại và muốn gia hạn thêm thời gian. Client sẽ xác định được DHCP server bằng cách gửi gói quảng bá gọi là DHCPDISCOVER.
2. Khi server nhận được gói quảng bá, nó sẽ tìm trong cơ sở dữ liệu của nó và quyết định là có trả lời được yêu cầu này không. Nếu server không trả lời yêu cầu thì nó sẽ gửi gói trả lời trực tiếp bằng DHCPOFFER về cho client, trong đó mời client sử dụng cấu hình IP của server. Trong DHCPOFER có

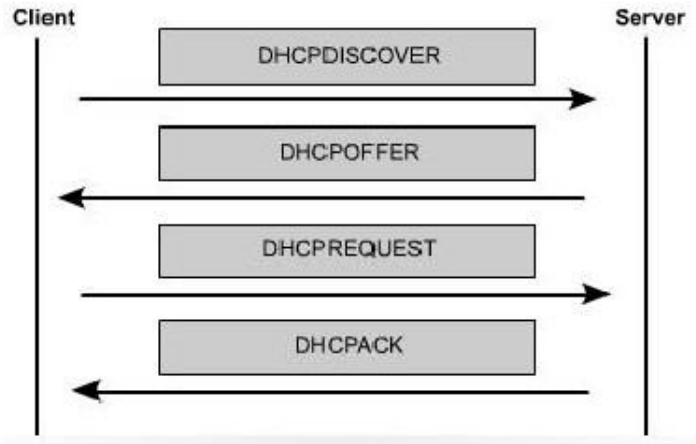
thể có các thôngtin cho client về địa chỉ IP, địa chỉ DNS server và thời gian sử dụng địa chỉ này.

3. Nếu client nhận thấy lời mời của server phù hợp thì nó sẽ gửi quảng bá một DHCPREQUEST để yêu cầu cung cấp những thông cố cụ thể của cấu hình IP. Tại sao lúc này client lại gửi quảng bá mà nó không gửi trực tiếp cho server? Do thông điệp đầu tiên là DHCPDISCOVER đã được gửi quảng bá nên thông điệp này có thể sẽ đến được nhiều server DHCP khác nhau. Khi đó, có thể sẽ có nhiều server cùng mời một client chấp nhận. Thông thường lời mời mà client nhận được đầu tiên sẽ được chấp nhận.
4. Server nào nhận được DHCPREQUEST cho biết client đã chấp nhận sử dụng cấu hình IP mà server đã mời thì server đó sẽ gửi trả lời trực tiếp cho client một gói DHCPACK. Rất hiếm khi nhưng cũng có thể server sẽ không gửi DHCPACK vì có thể cấu hình IP đó đã được cấp cho client khác rồi.
5. Sau khi client nhận được DHCPACK thì có thể bắt đầu sử dụng địa chỉ IP ngay.
6. Nếu client phát hiện rằng địa chỉ IP này đã được sử dụng trong cùng mạng nội bộ với nó thì client sẽ gửi thông điệp DHCPDECLINE và bắt đầu tiến trình DHCP lại từ đầu. Hoặc nếu client nhận được thông điệp DHCPNAK từ server trả lời cho thông điệp DHCPREQUEST thì sau đso client cũng bắt đầu tiến trình lại từ đầu.
7. Nếu client không cần sủ dụng địa chỉ IP này nữa thì client guiử thống điệp DHCPRELEASE cho server.



Hình 1.2.4.a. *Tiến trình hoạt động DHCP*

Tùy theo quy định của mỗi tổ chức, công ty, người quản trị mạng có thể cấp cố định cho một địa chỉ IP nằm trong dải địa chỉ của một DHCP server. Cisco IOS DHCP server luôn luôn phải kiểm tra một địa chỉ IP đã được sử dụng trong mạng hay chưa trước khi mời client sử dụng địa chỉ IP đó. Server sẽ phát một yêu cầu ICMP echo, hay còn gọi là ping, đến các địa chỉ IP nằm trong dải địa chỉ của mình trước khi gửi DHCPOFFER cho client. Số lượng ping mặc định được sủ dụng để kiểm tra một địa chỉ IP là 2 gói và chúng ta có thể cấu hình con số này được.



Hình 1.2.4.b. *Thứ tự các thông điệp DHCP được gửi đi trong tiến trình DHCP.*

1.2.5. Cấu hình DHCP

Tương tự như NAT, DHCP server cũng yêu cầu người quản trị mạng phải khai báo trước dải địa chỉ. Câu lệnh **ip dhcp pool** dùng để khai báo dải địa chỉ mà server có thể cấp pháp cho host.

Câu lệnh đầu tiên, **ip dhcp pool,** tạo dải địa chỉ với một tên cụ thể và đặt router vào chế độ cấu hình DHCP. Trong chế độ cấu hình DHCP, lệnh **network** được dùng để xác định dải địa chỉ được cấp phát. Nếu trong mạng đã có sử dụng cố định một số địa chỉ IP nằm trong dải đã khai báo thì chúng ra quay trở lại chế độ cấu hình toàn cục.

Chúng ra sử dụng lệnh **ip dhcp excluded-address** để cấu hình cho Router loại trừ một số hoặc một dải địa chỉ khi phân phối địa chỉ cho client. Những địa chỉ dành riêng này thường được cấu hình cố định cho những host quan trọng và cho các cổng của Router.

```
Router(config)#ip dhcp excluded-address low-address [high-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

Hình 1.2.5. *Cấu hình ví dụ một DHCP server trên router*

Thông thường, chúng ta còn có thể cấu hình thêm nhiều thông tin khác ngoài thông tin về địa chỉ IP cho một DHCP server. Trong chế độ cấu hình DHCP, chúng ta dùng lệnh **default-router** để khai báo cổng mặc định gateway, lệnh **dns-server** để khai báo địa chỉ của DNS server, lệnh netbios-name-server dùng để khai báo cho WINS server.

Dịch vụ DHCP được chạy mặc định trên các phiên bản Cisco IOS có hỗ trợ dịch vụ này. Để tắt dịch vụ này, chúng ta dùng lệnh **no service dhcp** và dùng lệnh **ip service dhcp** để chạy lại dịch vụ này.

Lệnh	Giải thích
network network-number [mask / /prefix-length]	Khai báo địa chỉ mạng và subnet mask tương ứng cho dải địa chỉ DHCP. Chiều dài bit thuộc phần network có thể được khai báo bằng subnet mask hoặc bằng con số thể hiện số lượng bit, con số này luôn có dấu xổ phải (/) đứng trước.
Default-router Addresss [address2 … Address8]	Khai báo địa chỉ của cổng mặc định gateway cho DHCP client. Mặc dù chỉ cần một địa chỉ những trong cấu lệnh này bạn có thể khai báo tới 8 địa chỉ.
Dns-server Address [address2 … Address8]	Khai báo địa chỉ của DNS server cho DHCP client. Mặc dù chỉ cần một địa chỉ những trong câu lệnh này bạn có thể khai báo tối đa 8 địa chỉ.
Netbios-name- **Server** address [address2…	Khai báo địa chỉ NetBios WINS server cho các Microsoft DHCP client. Mặc dù chỉ cần một địa chỉ những trong câu lệnh này bạn có thể khai báo tới 8 địa chỉ.

Address8]	
Domain-name Name	Khai báo tên miền cho client.
Lease [days [hours} [minutes] / infinite]	Khai báo khoảng thời gian cho phép client được sử dụng một địa chỉ IP. Thời gian mặc định là một ngày.

1.2.6. Kiểm tra hoạt động DHCP

Để kiểm tra hoạt động DHCP, bạn dùng lệnh show ip dhcp binding. Lệnh này sẽ hiển thị danh sách các địa chỉ IP đã được dịch vụ DHCP cấp phát cho các host nào tương ứng.

Để xem các thông điệp DHCP mà router đã gửi đi và nhận vào, chúng ta dùng lệnh show ip dhcp server statistics. Lệnh này sẽ hiển thị các thông tin về số lượng các thông điệp DHCP mà Router đã gửi đi và nhận vào.

```
Router#show ip dhcp binding
```

```
Router#show ip dhcp binding
IP address      Hardware address    Lease expiration        Type
172.16.12.11    0100.10a4.97f4.6d   Mar 02 1993 12:38 AM    Automatic
Router#
```

Hình 1.2.6

1.2.7. Xử lý sự cố DHCP

Để xử lý sự cố của hoạt động DHCP server chúng ta có thể dùng lệnh **debug ig dhcp server events.** Lệnh này sẽ cho biết chu kỳ kiểm tra của server để xem địa chỉ IP nào đã hết thời hạn được sử dụng và tiến trình lấy lại hoặc cấp phát một địa chỉ IP.

```
Router#debug ip dhcp server events
```

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

Hình 1.2.7.

1.2.8. Chuyển tiếp DHCP

DHCP client sử dụng IP quảng bá để tìm DHCP server trong mạng nội bộ. Điều gì sẽ xảy ra khi server và client không nằm trong cùng một mạng và bị ngăn cách nhau bởi Router? Router không hề chuyển tiếp gói quảng bá.

DHCP không phải là một dịch vụ quan trọng duy nhất sử dụng quảng bá Cisco router và các thiết bị khác cũng sử dụng quảng bá để tìm TFTP server. Một số client cần sử dụng quảng bá để tìm TACACS server. TACACS server là một server bảo vệ. Thông thường, trong cấu trúc mạng phân cấp phức tạp, client này phát quảng bá để tim server thì mặc định là router sẽ không chuyển các gói quảng bá ra ngoài subnet của client.

Tuy nhiên có nhiều client sẽ không thể hoạt động được nếu không có những dịc vụ như DHCP chẳng hạn, khi đó phải chon lựa một trong hai giải pháp. Người quả trị mạng có thể đặt server cho mọi subnet trong mạng hoặc là sử dụng đặc tính giúp

đỡ địa chỉ của Cisco IOS. Việc chạy các dịch vụ như DHCP hay DNS trên nhiều máy tính sẽ tạo sự quá tải và khó quản trị nên giải pháp đầu không hiệu quả. Nếu có thể thì người quản trị mạng nên sử dụng giải pháp thứ hai là dùng lệnh **ip helper-address** để chuyển tiếp yêu cầu quảng bá cho những dịch vụ UDP quan trọng này.

Khi sử dụng đặc tính giúp đỡ địa chỉ, router sẽ có thể được cấu hình để tiếp nhận yêu cầu quảng bá của một dịch vụ UDP và sau đó chuyển tiếp yêu cầu đó một cách trực tiếp đến một địa chỉ IP cụ thể. Mặc định, **lệnh ip helper-address** có thể cho phép chuyển tiếp yêu cầu của 8 dịch vụ UDP sau:

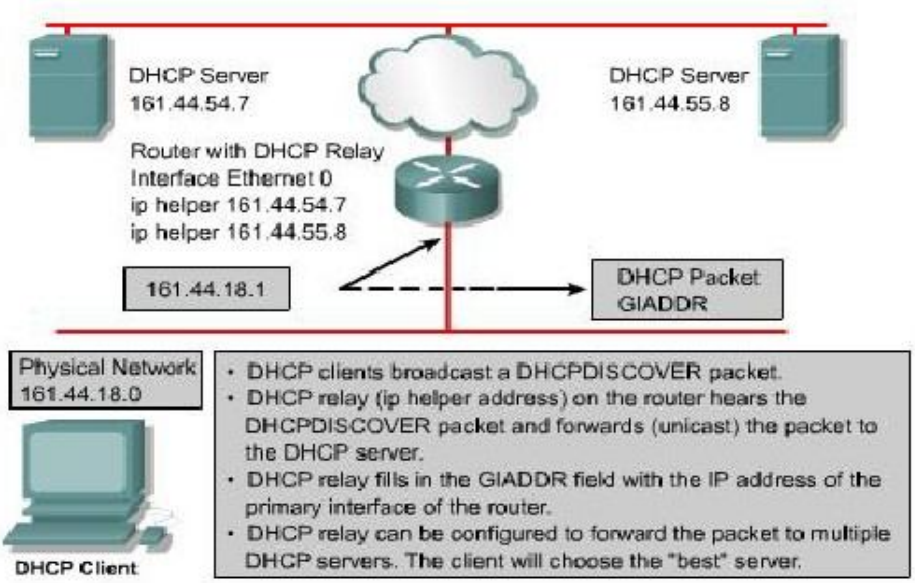
- Time
- TACES
- DNS
- BOOTP/DHCP server
- BOOTP/DHCP client
- TFTP
- Dịch vụ NetBIOS name
- Dịch vụ NetBIOS datagram

Chúng ta xét cụ thể dịch vụ DHCP, client phát quảng bá gói DHCPDISCOVER ra mạng nội bộ của nó. Gói quảng bá này sẽ đến được Gateway chính là router. Nếu trên router có cấu hình lệnh ip helper-address thì gói DHCP này sẽ dược chuyển tiếp cho một địa chỉ IP xác định. Trước khi chuyển tiếp gói yêu cầu này, Router sẽ điền địa chỉ của cổng Router kết nối với client vào phần GIADDR của gói DHCPDISCOVER. Địa chỉ này sẽ là địa chỉ Gateway cho DHCP client sau khi client lấy được địa chỉ IP.

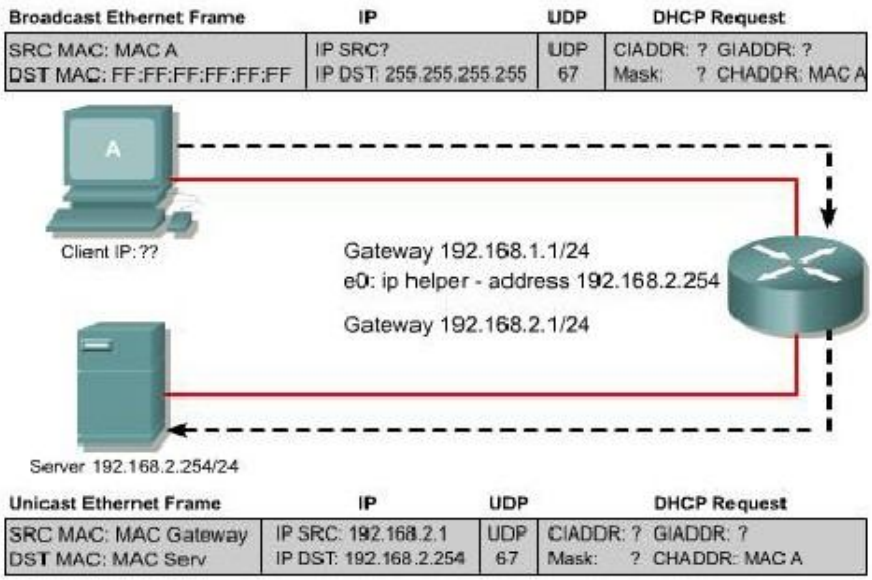
DHCP server nhận được gói DHCPDISCOVER. Đựa vào địa chỉ nằm trong phần GIADDR server sẽ xác định được Gateway này tương ứng với dải địa chỉ nào. Sau đó server sẽ lấy một địa chỉ IP còn trống trong dải để cấp cho client.

OP Code (1)	Hardware Type (1)	Hardware Length (1)	Hops (1)
Transaction ID (XID) - 4 bytes			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Filename - 128 bytes			
DHCP Options - 312 bytes			

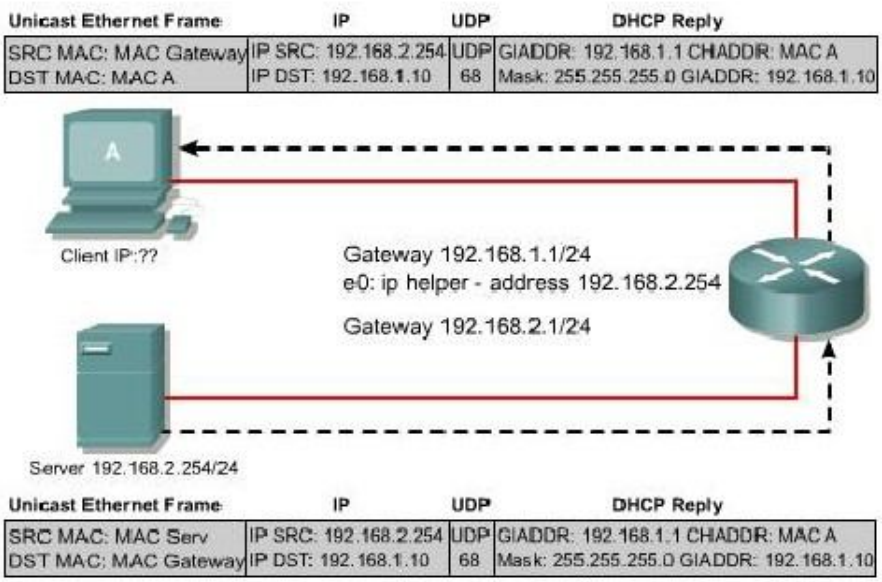
Hình 1.2.8.a. *Cấu trúc gói DHCP*



Hình 1.2.8.b. *Chuyển tiếp DHCP*



Hình 1.2.8.c. *Client A gửi quảng bá DHCPDISCOVER và router chuyển tiếp yêu cầu này cho server DHCP 192.168.2.254. Trước khi chuyển tiếp yêu cầu này router* điền địa *chỉ của cổng kết nối với client A là 192.168.1.1 vào phần GIADDP của gói DHCPDISCOVER.*



Hình 1.2.8.d. *DHCP server nhận* được *gói yêu cầu DHCP từ router. Dựa vào* địa *chỉ 192.168.1.1 trong phần GIADDR, server sẽ xác* định được *client A nằm trong subnet nào và chọn một* địa *chỉ IP còn trống trong giải* địa *chỉ tương* ứng để *cấp cho client A.. Trong gói trả lời của DHCP server chúng ta thấy client A* được *cấp* địa *chỉ 192.168.1.10.*

TỔNG KẾT

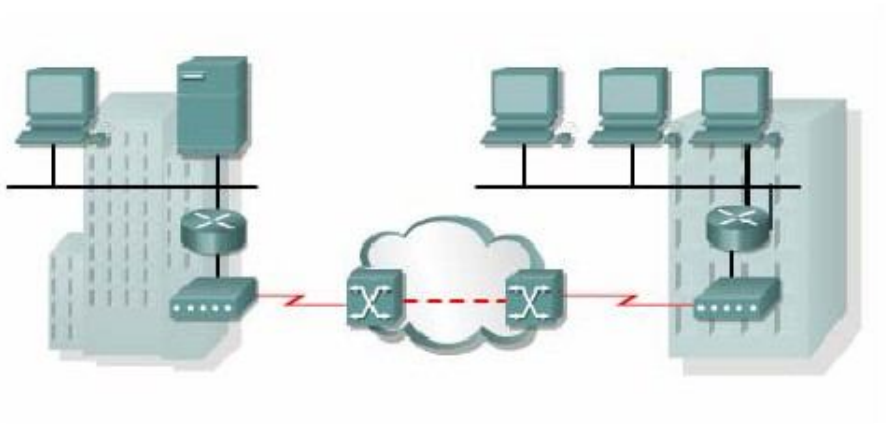
Sau đây là những điểm quan trọng cần nắm trong chương này:

- Địa chỉ riêng được sử dụng cho các mạng riêng, nội bộ và không bao giờ được định tuyến trên các Router Internet công cộng.
- NAT thay đổi phần IP header của gói dữ liệu để chuyển đổi địa chỉ nguồn hoặc đích hoặc cả hai.
- PAT sử dụng một địa chỉ IP công cộng duy nhất cùng với số port để ánh xạ cho nhiều địa chỉ nội bộ bên trong.
- Chuyển đổi NAT có thể được thực hiện cố định hoặc tự động tùy theo mục đích sử dụng.
- NAT và PAT có thể được cấu hình để chuyển đổi cố định, chuyển đổi động và chuyển đổi overloading.
- Lệnh clear và show được sử dụng để kiểm tra hoạt động của NAT và PAT.
- Lệnh debug ip nat được sử dụng để tìm sự cố của cấu hình NAT và PAT.
- Những ưu điểm và nhược điểm của NAT
- DHCP làm việc theo chế độ client-server, cho phép client lấy cấu hình IP từ một DHCP server.
- BOOTP là một phiên bản trước của DHCP và cũng có nhiều đặc điểm hoạt động giống DHCP nhưng BOOTP chỉ cấp phát địa chỉ cố định.
- DHCP server quản lý dải địa chỉ IP và các thông số tương ứng kèm theo. Mỗi một dải địa chỉ tương ứng với một subnet IP.
- DHCP client thực hiện 4 bước để lấy cấu hình IP từ server.
- DHCP server thường được cấu hình để phân phối nhiều địa chỉ IP.
- Lệnh show ip dhcp binding dùng để kiểm tra hoạt động của DHCP.

- Lệnh debug ip dhcp server events được dùng để tìm sự cố của DHCP.
- Khi DHCP server và client không nằm trong cùng một mạng và bị ngăn cách bởi Router, chúng ta dùng lệnh ip helper-address để router chuyển tiếp yêu cầu DHCP.

2.2. Các công nghệ WAN

2.2.1.Kênh quay số (dial-up)



Hình 2.2.1. *Kết nối WAN thông qua modem và mạng* điện *thoại.*

Modem và đường điện thoại quay số dùng tín hiệu tương tự cung cấp kết nối chuyển mạch, dung lượng thấp, phù hợp cho nhu cầu truyền dữ liệu tốc độ thấp, rẻ tiền.

Điện thoại truyền thống sử dụng cáp đồng kết nối từ máy điện thoại của thuê bao đến tổng đài mạng điện thoại chuyển mạch công cộng (PSTN – Public switched telephone network). Tín hiệu truyền đi trên đường truyền này là tín hiệu tương tự biến đổi liên tục để truyền tiếng nói. Do đó, đường truyền này không phù hợp với tín hiệu số nhị phân của máy tính. Modem tại đầu phát phải thực hiện điều chế tín nhị phân sang tính hiệu tương tự rồi mới đưa tín hiệu xuống đường truyền. Modem tại đầu thu giải điều chế tín hiệu tương tự thành tín hiệu nhị phân như ban đầu.

Đặc điểm vật lý của đường truyền và kết nối PSTN khiến tốc độ của tín hiệu bị hạn chế. Giới hạn trên khoảng 33 kb/giây. Tốc độ này có thể tăng lên khoảng 56 kb/giây nếu tín hiệu được truyền trực tiếp qua một kết nối số.

Đối với nhưng doanh nhiệp nhỏ thì đường truyền này phù hợp vì họ chỉ cần trao đổi các thông tin về bảng lương, giá cả, các báo cáo thông thường và email. Hơn nữa, họ có thể sử dụng cách quay số tự động vào ban đêm hoặc vào ngày nghỉ cuối tuần để truyền tải dữ liệu có dung lượng lớn và lưu dữ liệu dự phòng, vì trong nhưng khoảng thời gian này mức giá cước thấp hơn bình thường. Tổng chi phí cước phụ thuộc và khoảng cách giữa các điểm kết nối, thời gian trễ và thời gian thực hiện cuộc gọi.

Ưu điểm của modem và đường truyền tương tự là thực hiện đơn giản ở mọi nơi, chi phí thấp. Nhược điểm là tốc độ thấp, thời gian thực hiện kết nối lâu, có thời gian trễ và nghẽn mạch, việc truyền thoại và video không được tốt với tốc độ thấp như vậy.

2.2.2. ISDN

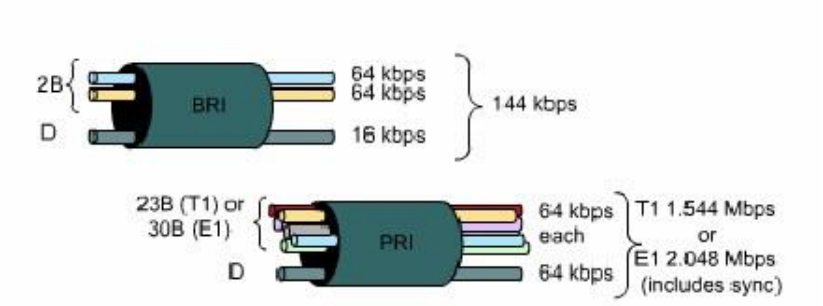
Các đường trung kế của PSTN được thay đổi từ tín hiệu tương tự phân kênh theo tần số sang tín hiệu số phân kênh theo thời gian (TDM). Bước tiếp theo là mạch vọng nội bộ kết nối từ tổng đài đến thuê bao cũng truyền tín hiệu số. Do đó, đường truyền này có dung lượng cao hơn.

ISDN (Integrated Services Digital Network) là kết nối số TDM. Kết nối này sử dụng các kênh B (Bearer) 64 Kb/giây để truyền thoại hoặc dữ liệu và một kênh báo hiệu D (Delta) dùng để thiết lập cuộc gọi và nhiều mục đích khác.

Giao tiếp tốc độ cơ bản BRI ISDN cung cấp hai kênh B 64 Kb/giây và một kênh D 16 Kb/giây phù hợp cho cá nhân, gia đình và các công ty nhỏ. Nếu nhu cầu lớn hơn nữa thì chúng ta có giao tiếp PRI ISDN. PRI cung cấp 23 kênh B 64 Kb/giây và một kenh Điểm 64 Kb/giây ở Bắc Mỹ, tổng tốc độ bit lên tới 1.544 Mb/giây. Ở Châu Âu, Australia và nhiều nơi khác trên thế giới, ISDN PRI cung cấp 30 kênh B và một kênh D, tổng tốc độ bit lên tới 2,048 Mb/giây. Kết nối T1 có tốc độ PRI ở Bắc Mỹ, kết nối E1 có tốc độ PRI quốc tế.

Kênh Điểm BRI không được tận dụng hết khả năng vì nó chỉ được sử dụng để điều khiển cho 2 kênh B. Một số nhà cung cấp dịch vụ cho phép kênk D truyền dữ liệu ở tốc độ thấp, ví dụ như kết nối X.25 với tốc độ 9,6 kb/giây.

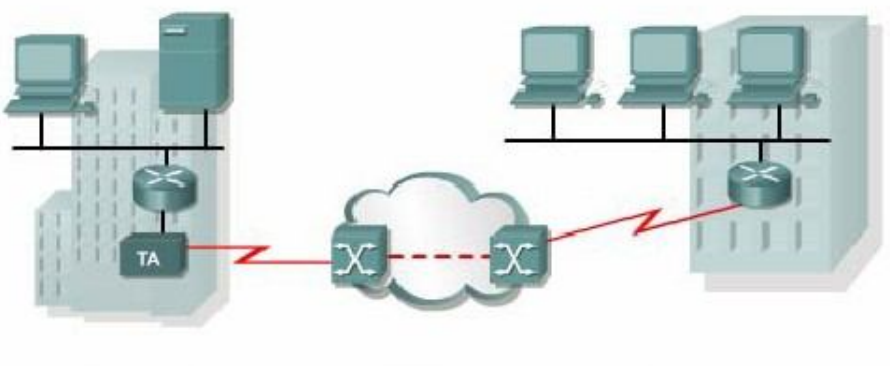
Đối với mạng WAN nhỏ thì kết nối BRI ISDN là một kết nối lý tưởng . BRI có thời gian thiết lập cuộc gọi nhỏ hơn một giây, kênh B 64 kb/giây cung cấy dung lượng lớn hơn một kết nối tương tự với modem. Nếu nhu cầu dung lương cao hơn thì kênh B thứ 2 sẽ được kích hoạt để cung cấp tốc độ 128 kb/giây. Mặc dù như vậy vẫn chưa phù hợp cho truyền video nhưng cũng đã cho phép thực hiện cùng lúc nhiều cuộc đối thoại cùng với các luồng lưu lượng khác.



Hình 2.2.a. ISDN

Một ứng dụng thông thường của ISDN là cung cấp thêm dung lượng truyền cho đường truyền thuê riêng. Đường truyền thuê riêng được sử dụng chính, trong những thời điểm nhu cầu dung lượng tăng cao thì ISDN được kích hoạt để hỗ trợ thêm. Ngoài ra, ISDN còn được sử dụng làm đường truyền dự phòng trong trường hợp đường truyền thuê riêng gặp sự cố. Chi phí cước của ISDN được tính trên từng kênh B và cũng tương tự như kết nối thoại quay số.

Với PRI ISDN, ta có thể kết nối hai điểm với nhau bằng nhiều kênh B. Do đó, ta có thể thực hiện được hội nghị truyền hình (video conference), kết nối dữ liệu tốc độ cao, không có thời gian trễ và nghẽn mạch, nhưng chi phí sẽ cao khi khoảng cách giữa các điểm khá lớn



Hình 2.2.2.b. *Cấu trúc chung của mạng WAN với ISDN, Router cần phải có cổng giao tiếp ISDN hoặc phải kết nối thông qua bộ chuyển đổi giao tiếp.*

2.2.3.Đường truyền thuê riêng (leased line)

Khi cần phải có một kết nối dành riêng cố định thì sử dụng đường truyền thuê riêng với dung lượng có thể lên tới 2,5 Gb/giây.

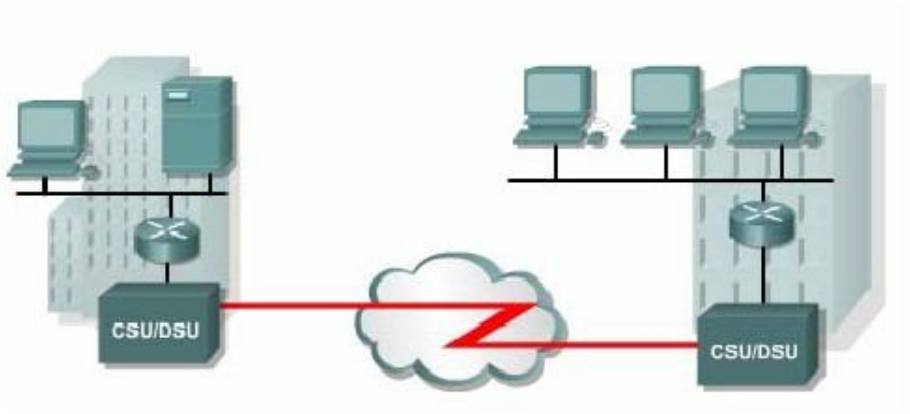
Loại	Chuẩn	Dung lượng
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Hình 2.2.3.a. *Các đường truyền WAN và băng thông tương ứng.*

Một kết nối điểm-đến-điểm thiết lập một đường truyền WAN từ vị trí của thuê bao thông qua mạng của nhà cung cấp dịch vụ đến điểm đích. Đường truyền điểm-đến-điểm này thường được thuê từ nhà cung cấp dịch vụ nên được gọi là đường truyền thuê riêng. Đường truyền thuê riêng có thể được cung cấp với nhiều mức dung

lượng khác nhau. Giá cả phụ thuộc vào mức băng thông yêu cầu và khoảng cách giữa hai điểm kết nối. Đương nhiên, giá thuê một đường truyền riêng điểm-đến-điểm sẽ cao hơn nhiều so với các đường chia sẻ khác như Frame Relay. Đôi khi chi phí cho đường thuê riêng quá cao so với nhu cầu mà ta sử dụng được. Chi phí này sẽ hiệu quả hơn nếu các kết nối này được sử dụng để nối nhiều vị trí trung tâm. Dung lượng cố định có ưu điểm là không có thời gian trễ và nghẽn mạch giữa hai điểm cuối, phù hợp cho nhiều ứng dụng như thương mại điện tử.

Để thực hiện kết nối thuê riêng ta cần phải có CSU/DSU và đường truyền từ nhà cung cấp dịch vụ, router phải có cổng Serial, mỗi cổng tương ứng với một kết nối.



Hình 2.3.b. *Mạng WAN với đường truyền thuê riêng.*

Đường kết nối trực tiếp thường được sử dụng để kết nối giữa các toà nhà, cung cấp dung lượng truyền cố định. Đường truyền thuê riêng là một chọn lựa truyền thống từ trước tới nay, tuy nhiên nó cũng có nhiều nhược điểm. Lưu lượng WAN luôn biến đổi nhưng dung lượng đường truyền cố định. Do đó, băng thông đường truyền ít khi nào bằng với lưu lượng thực tế. Mỗi router tại mỗi điểm cuối cần phải có một

cổng Serial cho một kết nối, do đó chi phí cho thiết bị sẽ tăng thêm. Mỗi lần muốn thay đổi dung lượng đường truyền ta cần phải liên hệ với nhà cung cấp dịch vụ.

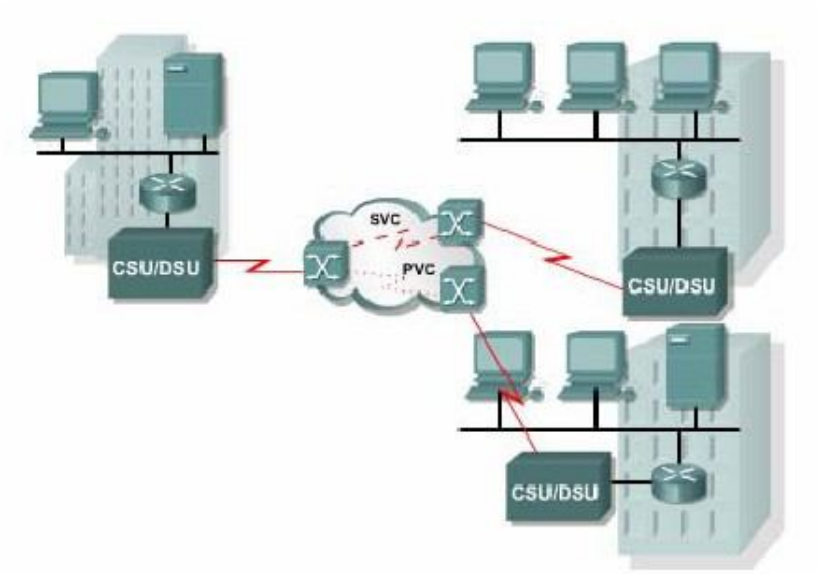
Đường truyền thuê riêng cung cấp kết nối trực tiếp điểm-đến-điểm giữa các LAN và kết nối nhiều chi nhánh riêng lẻ vào mạng chuyển mạch gói.

2.2.4.X.25

Do đường truyền thuê riêng có chi phí cao nên các nhà cung cấp dịch vụ đã giới thiệu mạng chuyển mạch gói sử dụng đường truyền chia sẻ để giảm bớt chi phí. Mạng chuyển mạch gói đầu tiên là mạng X.25. X.25 cung cấp tốc độ bit thấp, dung lượng chia sẻ qua dịch vụ chuyển mạch hoặc cố định.

X.25 là một giao thức lớp Mạng và các thuê bao được cung cấp một địa chỉ mạng. Khi có yêu cầu từ một tập hợp các địa chỉ, mạch ảo SVC sẽ được thiết lập, mỗi SVC được phân biệt bằng một địa chỉ số kênh. Các gói dữ liệu được dán nhãn theo chỉ số kênh này, dựa vào đó các gói dữ liệu được truyền đến đúng địa chỉ mạng đích. Trên một kết nối vật lý có thể thiết lập nhiều kênh truyền.

Thuê bao có thể kết nối vào mạng X.25 bằng kết nối thuê riêng hoặc bằng kết nối quay số. Mạng X.25 cũng có thể cung cấp kênh truyền cố định PVC cho các thuê bao.



Hình 2.2.4. *Mạng X25*

X.25 có chi phí thấp và hiệu quả vì chi phí cước được tính theo lưu lượng dữ liệu chứ không tính theo thời gian kết nối và khoảng cách của kết nối. Dữ liệu được truyền đi với bất kỳ tốc độ nào lên tới mức độ tối đa của đường truyền. Nhưng mạng X.25 thường có dung lượng thấp, tối đa là 48 Kb/giây. Ngoài ra thời gian truyền gói dữ liệu cũng bị trễ do đặc trưng của mạng chia sẻ.

Công nghệ X.25 từ lâu đã không còn được sử dụng rộng rãi. Frame Relay đã thay thế cho X.25

Ứng dụng thường thấy của X.25 là trên các máy đọc thẻ tín dụng. Tại các trung tâm thương mại, siêu thị, khi khach hàng sử dụng thẻ để thanh toán thì các máy đọc thẻ sẽ sử dụng X.25 để liên hệ với máy tính trung tâm xác định giá trị của thẻ, thực hiện giao dịch thanh toán. Một số công ty còn sử dụng X.25 trên mạng VAN (Value-add network). VAN là một mạng riêng được các công ty thuê từ nhà cung cấp dịch vụ để thực hiện trao đổi dữ liệu về tài chính và nhiều thông tin thương mại

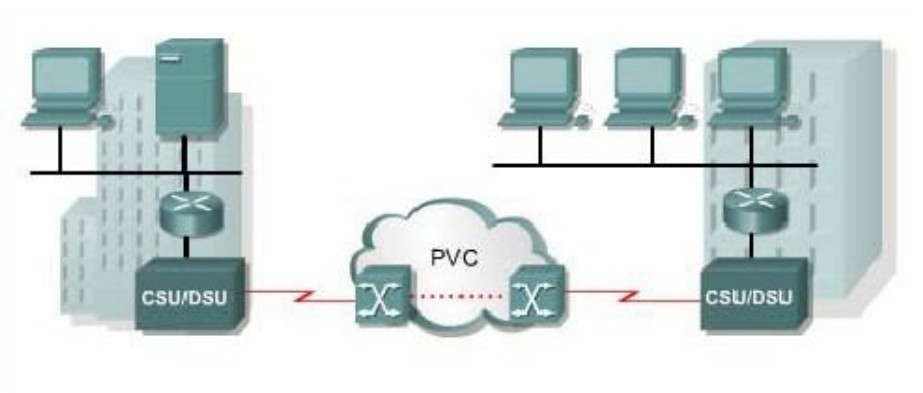
khác. Đối với những ứng dụng này, băng thông thấp và thời gian trễ cao không phải là vấn đề lớn, trong khi đó chi phí thấp lại là một ưu điểm của X.25.

2.2.5. Frame Relay.

Do nhu cầu băng thông ngày càng cao và yêu cầu thời gian chuyển mạch gói nhanh hơn, nhà cung cấp dịch vụ đã giới thiệu Frame Relay, Frame Relay cũng hoạt động như X.25 nhưng có tốc độ cao hơn, lên đến 4 Mb/giây hoặc hơn nữa.

Frame Relay có một số đặc điểm khác với X.25. Trong đó, điểm khác biệt quan trọng nhất là: Frame Relay là giao thức đơn giản hơn, hoạt động ở lớp liên kết dữ liệu thay vì ở lớp Mạng.

Frame Relay không thực hiện điều khiển luồng và kiểm tra lỗi. Do đó, thời gian trễ do chuyển mạch frame giảm đi.



Hình 2.2.5. *Mạng Frame Relay*

Hầu hết các kết nối Frame Relay đều là kết nối PVC, chứ không phải là SVC. Kết nối từ mạng của khách hàng vào mạng của nhà cung cấp dịch vụ thường là kết nối thuê riêng hoặc cũng có thể là kết nối quay số nếu nhà cung cấp dịch vụ có sử dụng đường ISDN, Kênh D ISDN được sử dụng để thiết lập kết nối SVC trên một hay

nhiều kênh B. Giá cước Frame Relay được tính theo dung lượng kết nối và dung lượng thoả thuận trên các PVC>

Frame Relay cung cấp kết nối chia sẻ có băng thông truyền cố định, có thể truyền được cả tiếng nói. Frame Relay là một chọn lựa lý tưởng cho kết nối giữa các LAN. Router trong LAN chỉ cần một cổng vật lý, trên đó cầu hình nhiều kết nối ảo VC. Kết nối thuê riêng để kết nối vào mạng Frame Relay khá ngắn nên chi phí cũng tương đối hiệu quả khi nối giữa các LAN.

2.2.6. ATM

Các nhà cung cấp dịch vụ đã nhìn thấy nhu cầu cần phải có công nghệ cung cấp mạng chi sẻ cố định với thời gian trễ thấp, ít nghẽn mạch và băng thông cao. Giải pháp của họ chính là ATM (Asychronous Transfer Mode) với tốc độ 155 Mb/giây. So với các công nghệ chia sẻ khác như X.25, Frame Relay thì sơ đồ mạng WAN ATM cũng tương tự.

Hình 2.2.6. *ATM.*

ATM là một công nghệ có khả năng truyền thoại, video và dữ liệu thông qua mạng riêng và mạng công cộng. ATM được xây dựng dựa trên cấu trúc tế bào (cell) chứ không dựa trên cấu trúc frame. Gói dữ liệu được truyền đi trên mạng ATM không được gọi là frame mà gọi là tế bào (cell). Mỗi tế bào ATM luôn có chiều dài cố định là 53 byte. Tế bào ATM 53 byte này chứa 5 byte phần ATM header, tiếp theo

sau là 48 byte của phần dữ liệu. Tất cả các tế bào ATM đều có kích thước nhỏ, cố định như nhau. Do đó, không có các gói dữ liệu khác lơn hơn trên đường truyền, mọi tế bào đều không phải chờ lâu. Thời gian truyền của mỗi gói là như nhau. Do đó, các gói đến đích cách nhau đều đặn, không có gói nào đến quá chậm so với gói trước. Cơ chế này rất phù hợp cho truyền thoại và video vì những tín hiệu này vốn rất nhạy cảm với vấn đề thời gian trễ.

So với các frame lơn hơn của Frame Relay và X.25 thì tế bào ATM 53 byte không được hiệu quả bằng. Khi có một packet lớn của lớp Mạng cần phải phân đoạn nhỏ hơn thì cữ mỗi 48 byte phải có 5 byte cho phần ATM header. Công việc ráp các phân đoạn lại thành packet ban đầu ở ATM switch đầu thu sẽ phức tạp hơn. Hơn nữa, việc đóng gói như vậy làm cho đường truyền ATM phải tốn nhiều hơn 20% băng thông so với Frame Relay để truyền cùng một lượng dữ liệu lớp Mạng.

ATM cung cấp cả kết nối PVC và SVC mặc dù PVC được sử dụng nhiều hơn trong WAN. Cũng như các công nghệ chia sẻ khác, ATM cho phép thiết lập kết nối ảo trên một kết nối vật lí.

2.2.7. DSL

Digital Subscriber Line – DSL là một công nghệ truyền băng rộng sử dụng đường truyền hai dây xoắn của hệ thống điện thoại để truyền dữ liệu với băng thông lớn đến thuê bao dùng dịch vụ. Kỹ thuật truyền băng rộng ghép nhiều dải tần số khác nhau trên cùng một đường truyền vật lý để truyền dữ liệu xDSL bao gồm các công nghệ DSL như sau:

Asymmetric DSL (ADSL)

Symmetric DSL (SDSL)

High Bit Rate DSL (HDSL)

ISDN DSL (IDSL)

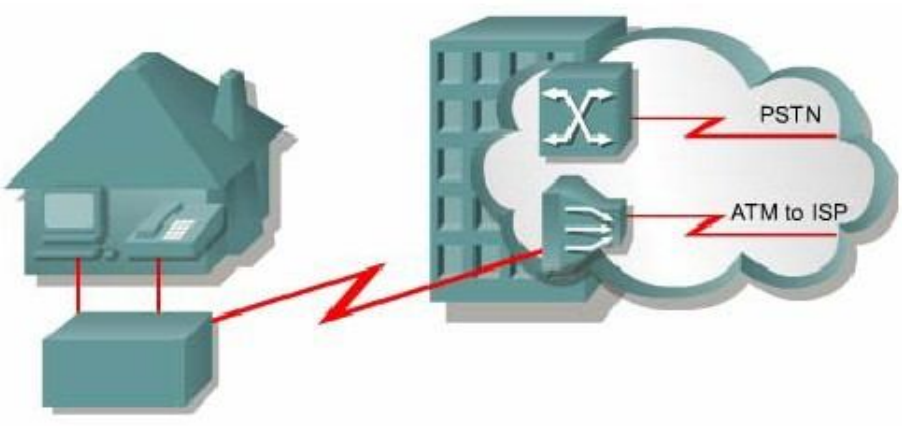
Consumer DSL (CDSL), cũng được gọi là DSL-lite hay G.lite

Service	Download	Upload
ADSL	64 kbps - 8.192 Mbps	16 kbps - 640 kbps
SDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
HDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
IDSL	144 kbps	144 kbps
CDSL	1 Mbps	16 kbps - 160 kbps

Hình 2.2.7.a.

Với công nghệ DSL, các nhà cung cấp dịch vụ có thể cung cấp cho khách hàng dịch vụ mạng tốc độ cao trên đường dây thoại cáp đồng. Công nghệ DSL cho phép đường dây này thực hiện song song đồng thời chức năng của một kết nối điện thoại và một kết nối mạng thường trực cố định. Nhiều kết nối của thuê bao DSL được ghép kênh vào một đường kết nối có dung lượng cao tại trung tâm cung cấp dịch vụ thông qua thiết bị ghép kênh truy cập DSL (DSLAM – DSL Access Multiplexer). Nhiều kết nối DSL của thuê bao được DSLAM tích hợp vào một kết nối T3/DS3 duy nhất. Các công nghệ DSL hiện nay sử dụng nhiều kỹ thuật mã hoá và điều chế phức tạp để đạt được tốc độ dữ liệu lên đến 8,192 Mb/giây.

Kênh truyền thoại chuẩn trên đường dây điện thoại nằm trong dải tần 300 Hz đến 3,3 KHz. Như vậy, dải tần số 4 KHz được dành để truyền thoại trên đường dây điện thoại. Công nghệ DSL sử dụng dải tần cao hơn 4 KHz để truyền tải dữ liệu. Bằng cách này thoại và dữ liệu có thể được truyền tải song song đồng thời trên cùng một đường truyền.



Hình 2.2.7.b. *Mạch vòng nội bộ của hệ thống điện thoại kết nối modem DSL của từng thuê bao đến DSLAM đặt tại trung tâm cung cấp dịch vụ. Thoại và dữ liệu sử dụng hai dải tần số riêng biệt.*

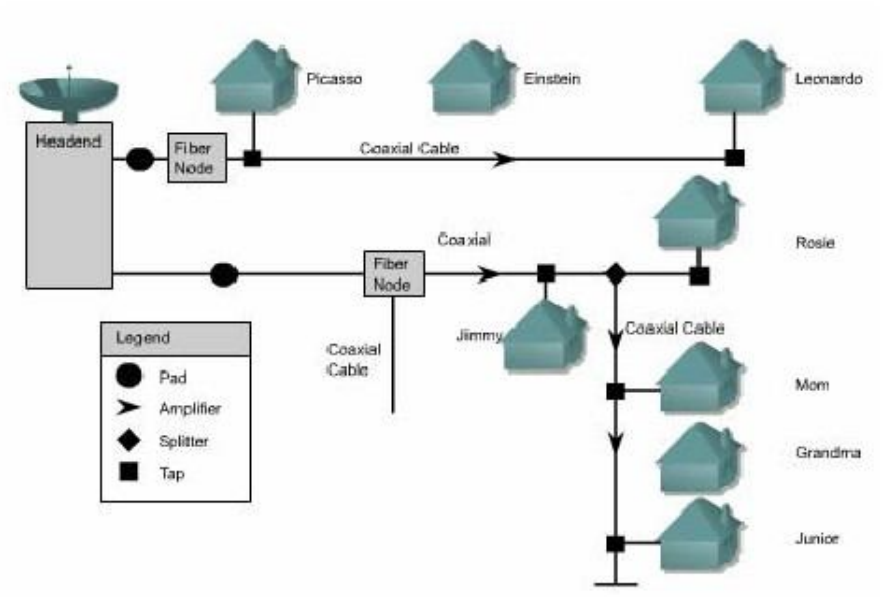
Có 2 loại công nghệ DSL cơ bản là ADSL (Asymmetric DSL – DSL bất đối xứng) và SDSL (Symmetric DSL – DSL đối xứng). Dịch vụ bất đối xứng cung cấp kênh tải dữ liệu (download) lớn hơn kênh truyền dữ liệu (upload). Dịch vụ đối xứng cung cấp cả hai kênh truyền này có dung lượng như nhau.

Không phải tất cả các công nghệ DSL đều cho phép sử dụng đường dây điện thoại. Ví dụ SDSL không cung cấp dịch vụ điện thoại trên cùng một đường truyền. Do đó phải có riêng một đường truyền cho SDSL.

Các loại DSL khác nhau cung cấp băng thông khác nhau với dung lượng có thể vượt qua đường thuê riêng T1 hoặc E1. Tốc độ truyền phụ thuộc vào chiều dài thực tế của mạch vòng nội bộ, loại cáp và điều kiện đi dây cáp. Để dịch vụ được cung cấp tốt thì mạch vòng nội bộ nên ngắn hơn 5,5 km. DSL thường không được chọn làm kết nối giữa nhà riêng và hệ thống mạng trong công ty vì thuê bao không thể từ nhà riêng kết nối trực tiếp vào mạng trung tâm của công ty, mà phải thông qua một nhà cung cấp dịch vụ Internet (ISP – Internet Service Provider). Từ đây, một kết nối IP mới được thực hiện thông qua Internet để đến mạng trung tâm của công ty. Như vậy rất nguy hiểm về mặt bảo mật. Để đảm bảo tính an toàn, dịch vụ DSL có cung cấp khả năng sử dụng mạng riêng ảo VPN (Virtual Private Network) để kết nối vào server VPN đặt tại công ty.

2.2.8. Cable modem

Cáp đồng trục được sử dụng rộng rãi trong các thành phố để truyền tín hiệu truyền hình. Hệ thống mạng được xây dựng dựa trên hệ thống cáp đồng trục này có băng thông cao hơn so với hệ thống mạng trên cáp đồng điện thoại.



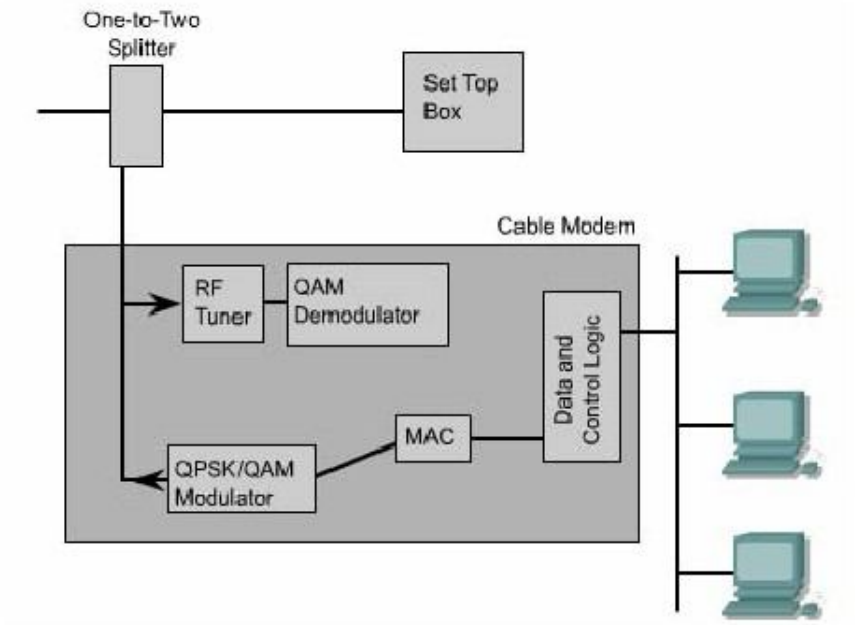
Hình 2.2.8.a. *Cable modem*

Cable modem thực hiện truyền dữ liệu hai chiều tốc độ cao, sử dụng cáp đồng trục trong hệ thống mạng cáp truyền hình. Một số nhà cung cấp dịch vụ còn cam kết tốc độ truyền dữ liệu cao gấp 6,5 lần đường thuê riêng T1. Tốc độ này cho phép truyền được nhanh chóng một lượng lớn thông tin số bao gồm video clip, audio… Lượng thông tin cần phải mất 2 phút nếu tải bằng đường truyền ISDN BRI thì bây giờ chỉ mất 2 giây thông qua kết nối cable modem.

Cable modem cũng cung cấp kết nối thường trực và lắp đặt kết nối này đơn giản. Một kết nối thường trực cũng có nghĩa là máy tính luôn luôn đứng trước mối nguy hiểm về mặt bảo mật, do đó cần phải được bảo vệ bằng bức tường lửa (firewalls). Để đảm bảo về mặt an toàn, dịch vụ cable modem cũng cho phép sử dụng mạng riêng ảo VPN để kết nối vào VPN server đặt tại mạng trung tâm của một công ty.

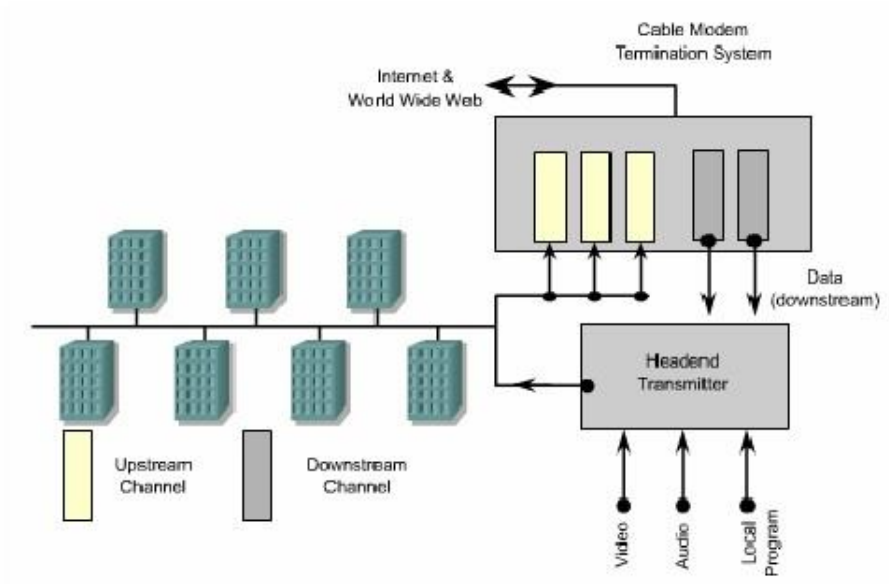
Một kết nối cable modem có dung lượng có thể lên đến 30 – 40 Mb/giây trên kênh truyền 6 MHz. Đường truyền này nhanh gần gấp 500 lần so với đường truyền modem thường (56 Kb/giây).

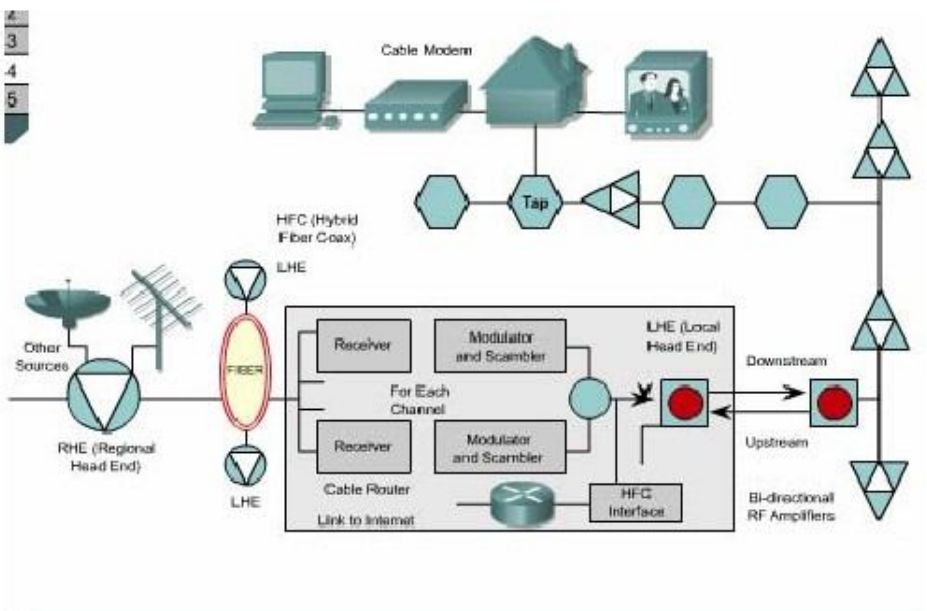
Với cable modem, thuê bao vẫn có thể nhận song song đồng thời dịch vụ truyền hình cáp và dữ liệu cho máy tính thông qua một bộ phân giải 1-2 đơn giản.

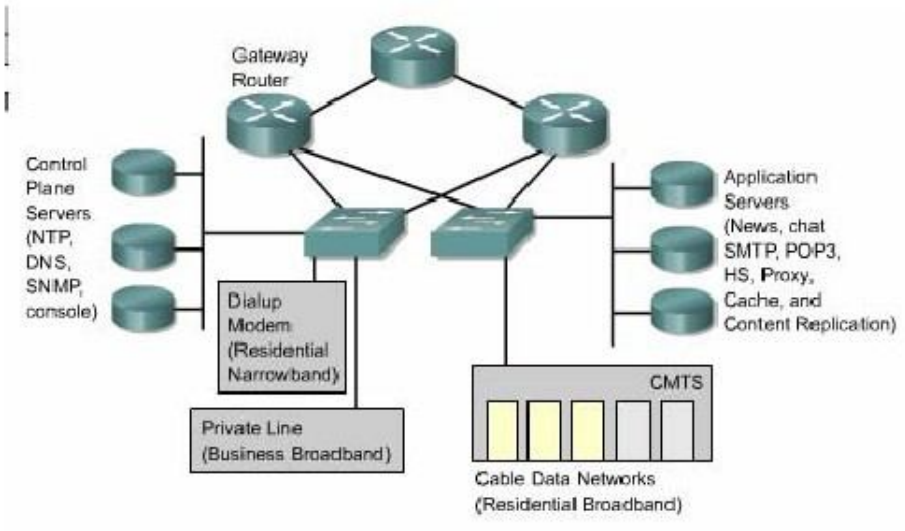


Hình 2.2.8.b. *Cấu trúc bộ phân giải 1-2.*

Thuê bao cable modem phải sử dụng ISP liên kết với nhà cung cấp dịch vụ truyền hình cáp. Tất cả các thuê bao nội bộ đều chia sẻ cùng một băng thông cáp. Do đó càng nhiều người tham gia vào dịch vụ thì lượng băng thông cho mỗi người sẽ giảm xuống.







Hình 2.2.8.c. *Cấu trúc mạng cable modem.*

2.3. Thiết kế WAN

2.3.1. Thông tin liên lạc bằng WAN

WAN là một tập hợp các đường liên kết dữ liệu kết nối các router trong các LAN khác nhau.

Vì lý do chi phí và pháp định nên chỉ có các nhà cung cấp dịch vụ thông tin liên lạc - viễn thông mới sở hữu các đường truyền dữ liệu của WAN. Khách hàng thuê các đường liên kết này để kết nối các mạng LAN của mình hoặc kết nối đến các mạng ở xa. Tốc độ truyền dữ liệu trong WAN thường thấp hơn tốc độ 100 Mb/giây trong LAN. Chi phí thuê bao đường truyền là chi phí lớn nhất cho một mạng WAN. Do đó, việc thiết kế WAN phải đảm bảo cung cấp băng thông lớn nhất trong khả năng chi trả chấp nhận được. Đối với người sử dụng, việc cân đối giữa chi phí và nhu cầu dịch vụ tốc độ cao là một điều không dễ dàng.

WAN truyền tải rất nhiều loại lưu lượng khác nhau như dữ liệu, thoại và video. Do đó thiết kế được đưa ra phải cung cấp đủ dung lượng, thời gian truyền đáp ứng được với yêu cầu của toàn bộ hệ thống. Ngoài ra, người thiết kế còn phải quan tâm đến cấu trúc của mạng nối giữa các trung tâm với nhau, về đặc tính tự nhiên, về băng thông và khả năng của các kết nối này.

Mạng WAN cũ trước đây thường bao gồm các đường kết nối giữa các máy tính lớn (mainframe) ở cách xa nhau. Mạng WAN ngày nay kết nối các LAN ở xa lại với nhau. Tất cả các máy tính đầu cuối, server và router nằm trong cùng một phạm vi được kết nối với nhau thông qua LAN và WAN kết nối các router của từng LAN lại với nhau. Thông qua sự trao đổi thông tin địa chỉ lớp 3 router có thể định tuyến cho mọi luồng dữ liệu. Ngoài ra, router còn cung cấp chế độ quản lý chất lượng dịch vụ (QoS) cho phép định tuyến và chuyển mạch các luồng dữ liệu khác nhau với các mức ưu tiên khác nhau.

WAN thường chỉ là tập hợp các kết nối giữa các router để liên kết các LAN với nhau, do đó không có dịch vụ nào thực hiện trên WAN. WAN hoạt động ở 3 lớp dưới của mô hình OSI. Router quyết định chọn đường đến đích cho dữ liệu từ thông tin lớp Mạng nằm trong gói dữ liệu rồi sau đó chuyển gói dữ liệu xuống kết nối vật lý tương ứng.