2. Port Mirroring: Trong một hệ thống mạng lớn và chạy nhiều ứng dụng, việc xảy ra lỗi làm chậm hệ thống hoặc không thể truy nhập mạng là điều không thể tránh khỏi, nguyên nhân gây lỗi có thể từ máy tính, hệ thống cáp, cấu trúc mạng, phần mềm ứng dụng... Nhờ việc sử dụng tính năng Port Mirroring, người quản trị mạng có thể ánh xạ toàn bộ hoạt động của một cổng nào đó trên thiết bị chuyển mạch sang một cổng khác để dò lỗi một cách nhanh chóng mà không phải xuất hiện tại nơi xảy ra lỗi.

Theo dõi trạng thái hoạt động truyền và nhận của cổng. Bạn có thể ánh xạ cổng nào đó vào một cổng khác để theo dõi hoạt động về lưu lượng của các cổng theo thời gian thực. Chú ý khi ánh xạ cổng nguồn và cổng đích phải nằm trong cùng 1 Vlan. Và chúng ta có thể ánh xạ nhiều cổng vào 1 cổng để theo dõi

3. Dịch vụ QoS: Chức năng này cho phép bạn cấu hình ưu tiên loại dịch vụ tức là ưu tiên gói tin kết hợp với điều khiển luồng. Các cổng đặt chế độ ưu tiên khi gói tin đến sẽ được đánh dấu và chuyển tới đích theo mức ưu tiên đã thiết lập. QoS thường có các thuật ngữ như : TOS (Type Of Service), 802.1p Priority, Adapted Flow Control, Priority Weight Ration. Các port nào được đánh dấu ưu tiên thì sẽ được ưu tiên với các tính năng của QoS.

4. Giao thức 802.1d(STP- Spanning Tree Protocol): MAC – Bridge : Chức năng tránh dữ liệu lặp vòng qua các đường liên kết switch- hoạt động trên các switch Ethernet bao gồm các bước :

- Đọc địa chỉ MAC của card mạng kết nối với cổng switch và lưu trong bảng địa chỉ MAC.

- Đếm thời gian và thiết lập hạn chế với khoảng time-line trước khi tạo frame mới trên switch và chuẩn bị truyền đi.

- Cơ chế truyền và lọc dữ liệu khi nhận 1 frame xác nhận qua địa chỉ MAC đích lưu trong header của frame, so sánh với bảng địa chỉ MAC để xác định địa chỉ cổng truyền qua. Nếu tìm thấy, nó lập tức forward qua cổng đó, nếu không thì gửi broadcast tới mọi cổng.

5. Giao thức 802.1w (RSTP- Rapid Spanning Tree Protocol) giao thức nhanh hơn 802.1d với các tính năng như Uplink fast- Backbone Fast- Port Fast nhằm tăng tốc thời gian hội tụ trên mạng bridge.

6. Dịch vụ IntServ : bao gồm 2 dịch vụ chính :

- Quan sát dịch vụ : hỗ trợ đảm bảo băng thông và giảm trễ, chức năng giống như chuyển mạch ảo.

- Dịch vụ điều khiển tải mạng : hỗ trợ dịch vụ ứng dụng hiệu quả hơn, chức năng giống như các điều khiển băng thông mức thấp, giảm độ mất mát thông tin và độ trễ mạng.

7. Dịch vụ DiffServ

- Được biết đến để đáp ứng các yêu cầu dịch vụ hiệu quả hơn và tính mở rộng cao hơn IntServ.

- Lưu lượng được phân tách lớp thành 5 mức forwarding.

- Các lớp forwarding được mã hoá trên các điểm dịch vụ DiffServ (DSCP) tại mỗi vùng hearder gói tin.

- Các router thừa kế PHBs- Per Hop Behaviors tới các gói tin theo mã hoá theo lớp forwarding.

DiffServ so sánh với IntServ :

DiffServ tập trung tài nguyên hơn là xử lí theo luồng,

DiffServ di chuyển theo lớp, cơ chế và hoạt động chức năng hoá đồng bộ tới các điểm mạng,

DiffServ định dạng các đối tượng forwarding theo trạm (PHBs) không phải các dịch vụ đầu cuối,

DiffServ đảm bảo được dựa theo cơ chế cung cấp chứ không phải đặt trước,

DiffServ hỗ trợ trên các miền (domain) riêng lẻ hơn là thiết lập đầu cuối.

8. "Jumbo Frames" mở rộng dung lượng gói tin tới 9000 byte trong môi trường Ethernet. Bởi vì thứ nhất chế độ CRC 32bít lên tới 12000byte, thứ hai 9000byte là đủ cho các data gram ứng dụng lên khoảng 8KB (ví dụ : NFS) và cộng thêm các gói tin overhead. Rất thích hợp với cơ chế truyền file dung lượng lớn chẳng hạn như Media hay dữ liệu lớn giảm tải và tránh quá tải mạng.

Các Jumbo Frame và các gói tin 1500 byte cùng song song tồn tại theo 2 cơ chế :

- trên 1 cổng đơn được quy định, các dữ liệu được down xuống là hỗ trợ jumbo frames,

- sử dụng 802.1q VLAN, khi mà các thiết bị hoạt động jumbo frame và non-jumbo frame theo các vùng khác nhau.

9. Chức năng 802.3x: Hỗ trợ đặc tính mới, điều khiển luồng full-duplex. Khi 1 switch dò biết được bộ đệm truyền thông sắp tràn thì lập tức tạm dừng một vài quá trình truyền tin tránh mất mát thông tin và nghẽn mạng.

10. Chức năng 802.3p: Nhu cầu khi trong mạng sử dụng nhiều dịch vụ ứng dụng như email, file transfer, database, VoiP.. kết quả lưu lượng mạng chậm trong các quá trình xử lí dữ liệu. Chuẩn IEEE 802.3p cho phép các gói tin mạng phân mức ưu tiên thông qua các Tag (phần đính kèm sau gói tin) phân biệt và nhận dạng gói tin để tách các lưu lượng theo quyền truyền thông qua mạng.

11. Chức năng 802.3q - VLAN: giúp đỡ IT nâng cao hiệu quả mạng và bảo mật an toàn mạng bằng cách phân vùng mạng thành các mạng LAN ảo. Chức năng còn giúp đỡ cho việc chặn các gói tin broadcast giữa lưu lượng các VLAN.

12. PPPoE: chuẩn giao thức point to point trên đường Ethernet

PPPoA : chuẩn giao thức point to point trên đường truyền không đồng bộ ATM

13. Simple Network Management Protocol:

SNMPv1 : giao thức quản lí mạng đơn giản : phát triển trên nền giám sát các trạm agent (server, PC workstation, router, switches và hub...) sử dụng giao thức UDP để truyền thông tin.

Một hệ thống được SNMP quản lí gồm các thành phần chính :

- hệ thống quản lí mạng ,

- các trạm (thành phần mạng như switch, hub, router...) và các thành phần phần mềm mạng kèm theo,

- các thiết bị được quản lí (nút mạng bao gồm trạm tồn tại trên mạng),

SMNPv2 : cải tiến hoạt động hiệu quả hơn so với v1, định dạng message khác với v1.

Có thêm 2 dịch vụ mới:

Get Bulk : sử dụng phục hồi block dữ liệu lớn với chất lượng tin cậy.

Inform : cho phép 1 NMS (hệ thống quản lí mạng) gửi thông tin tới một NMS khác và nhận phản hồi.

14. Dịch vụ MIB II: Management Information Base : thích hợp với các hệ thông quản lí mạng liên kết sử dụng giao thức TCP/IP (1 tập các định

nghĩa dự án quản lý mạng theo TCP/IP) sử dụng một cơ sở dữ liệu ghi lại các cấu hình, trạng thái và thông tin lưu trữ cho từng thiết bị.

15. DVMRP: giao thức định tuyến theo vector khoảng cách đa đích

IGMP : Internet group management protocol.

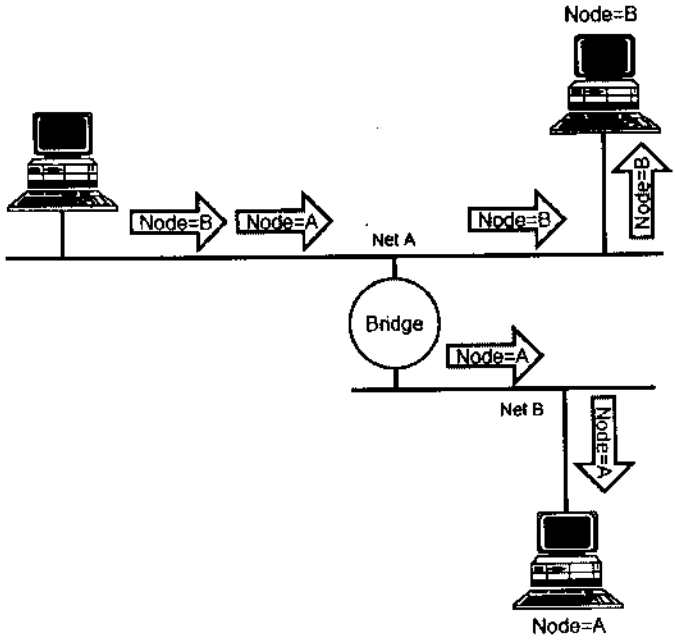
4.1.6. WIRELESS

Chi tiết xem chương 7 của quyển sách này.

4.1.7. BRIDGE

Bridge có thể dùng để mở rộng kích thước tối đa của một mạng máy và đồng thời nó là một thiết bị linh hoạt hơn nhiều so với repeater. Các bridge hoạt động ở tầng con MAC của tầng Data Link (Tầng 2) trong mô hình OSI. Trong khi repeater chuyển đi tất cả các tín hiệu mà nó nhận được, thì bridge lại lựa chọn kỹ lưỡng và chỉ cho phép các tín hiệu được yêu cầu đi qua nó. Sở dĩ Bridge làm được điều này là vì mỗi một thiết bị trong mạng đều được xác định danh tính bởi một địa chỉ duy nhất. Mỗi một gói tin được truyền trên mạng đều chứa địa chỉ của thiết bị mà gói tin này cần phải được gửi đến. Bridge thế hệ mới ngày nay còn được gọi là learning bridge. Các bridge này tự động xây dựng các bảng ghi địa chỉ của các thiết bị trong mạng và cũng tự động cập nhật các bảng địa chỉ này mỗi khi một thiết bị mạng bị loại bỏ hay được cài thêm vào mạng.

Bridge được dùng để chia nhỏ mạng thành các segment mạng riêng lẻ. Mạng được thiết kế sao cho phần lớn các gói tin được chuyển đến đích mà không cần phải đi qua một bridge nào. Khi đó, lưu lượng truyền thông và khả năng đụng độ trong mỗi segment mạng đơn lẻ sẽ được giảm thiểu. Các gói tin sẽ phải đi qua một bridge chỉ khi hai host tham gia trao đổi các gói tin này thuộc về hai segment mạng khác nhau.



Hình 4.9. *Sơ đồ hoạt động của Bridge*

Bridge có thể được sử dụng để mở rộng kích thước vật lý của mạng. Mặc dù kích thước của mỗi một segment mạng đơn lẻ vẫn bị hạn chế bởi kích thước tối đa do các giới hạn thiết kế mạng áp đặt, bridge cho phép người thiết kế mạng có thể mở rộng khoảng cách giữa các segments và do đó mở rộng được kích thước chung của mạng.

Tuy nhiên, bridge không thể kết nối các mạng LAN khác loại với nhau. Lý do là vì hoạt động của các bridge phụ thuộc vào các địa chỉ vật lý của các thiết bị mạng. Các địa chỉ này là các chức năng của tầng Data Link và các mạng khác nhau sử dụng các giao thức tầng Data Link khác nhau. Vì vậy mà một bridge không thể dùng để kết nối một segment mạng ETHERNET với một segment mạng Token Ring.

Một bridge đôi khi cũng được sử dụng để liên kết một segment mạng LAN thông qua một kết nối dùng modem đồng bộ với một segment mạng LAN khác ở cách xa.

4.1.8. KẾT NỐI HOST

Để nối một thiết bị Host vào môi trường mạng cần một thiết bị gọi là các giao tiếp mạng NIC (Network Interface Card). Hiện nay, NIC thường có trong các dạng sang sau: NIC sử dụng trong PC loại Server, Desktop là chuẩn PCI cắm vào khe mở rộng hoặc nằm trong Bo mạch chủ với các

chuẩn cho cả cáp BNC, UTP, quang, với tốc độ trải từ 10 Mbps đến Gigabit, đối với máy Notebook là chuẩn PCMCIA cắm vào khe mở rộng của máy hoặc nằm luôn trong bo mạch chủ với các chuẩn và tốc độ giống loại cho máy chủ và Desktop, ngoài ra NIC còn sử dụng cho cả trong máy in (Print Server), chuyển đổi từ các cổng USB, RS232 sang mạng.

Trong mô hình OSI, NIC được xem như là thiết bị lớp 2 bởi mỗi NIC chứa một mã duy nhất được gọi là địa chỉ MAC (địa chỉ này do một tổ chức trên thế giới cấp cho từng nhà sản xuất). Địa chỉ này được dùng để điều khiển hoạt động truyền số liệu cho host trên mạng. Chúng ta sẽ tìm hiểu kỹ về địa chỉ MAC trong chương 5 của quyển sách này.

Để có thể kết nối các chuẩn khác nhau của NIC, ta phải dùng các bộ chuyển đổi, ví dụ khi nối NIC có đầu ra là RJ45 vào chuyển mạch sử dụng cho cáp quang ta phải dùng bộ chuyển đổi quang điện.

Trong lược đồ, các NIC không có ký hiệu chuẩn. Điều này ngụ ý rằng, khi các thiết bị nối mạng được gắn vào trong đường truyền mạng thì đương nhiên có một NIC hay một thiết bị tương tự như NIC hiện diện ở đó. Bất cứ ở đâu có một dấu chấm trên bản đồ cấu hình thì đó là biểu diễn cho một giao tiếp NIC hoặc một port, chúng đóng vai trò như một NIC.

4.1.9. PEER-TO-PEER

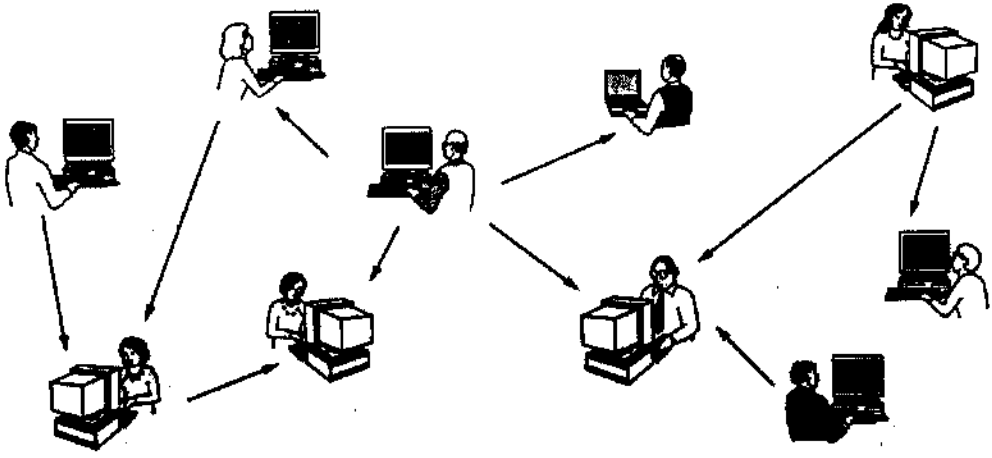
Với các thiết bị mạng LAN ở trên hay ở WAN phần 4.2, các máy tính được liên kết để cung cấp các dịch vụ phục vụ cho công việc cũng như đời sống hàng ngày cho người dùng. Để có được điều này, các máy tính nối mạng thực hiện các vai trò hay chức năng riêng trong mối quan hệ với nhau. Trong mạng, các máy tính thực hiện các chức năng độc lập, không có ưu tiên cho bất cứ máy nào và đối xử với nhau như các đối tác ngang hàng. Trong mạng ngang hàng, cũng có các loại ứng dụng chp phép một máy tính thực hiện chức năng để phục vụ cho một số các máy tính khác trong một mối quan hệ không ngang hàng nhau. Trong cả hai loại ứng dụng, hai máy tính truyền tin cho nhau bằng cách dùng các giao thức yêu cầu / đáp ứng (request/response). Một máy tính phát ra một yêu cầu dịch vụ, máy tính thứ hai tiếp nhận và đáp ứng cho yêu cầu này.

Trong mạng máy tính ngang hàng, Khi một máy tính yêu cầu máy tính khác, thì chúng ta có thể coi máy tính yêu cầu là máy trạm, còn máy tính được yêu cầu có thể đóng vai trò máy chủ, khái niệm chủ và trạm sẽ chỉ là tương đối và vai trò thay đổi liên tục

Trong mạng ngang hàng, các người dùng tự kiểm soát tài nguyên của mình, quyết định chia sẻ hay không chia sẻ các tài nguyên đó, và chia sẻ các thông tin đó với các quyền tự mình quyết định. Các người dùng cá thể đưa ra các quyết định về chính sách cho tài nguyên của mình, do đó không hề có điểm điều khiển trung tâm hay sự quản trị tập trung nào trong mạng. Ngoài ra, các người dùng phải tự dự phòng các hệ thống của mình để có thể phục hồi các dữ liệu bị mất trong trường hợp hỏng hóc. Khi một máy tính đóng vai trò server, user của máy này có thể phải chịu sự giảm hiệu suất khi máy này phục vụ yêu cầu từ các hệ thống khác.

Hệ thống mạng ngang hàng rất dễ lắp đặt. Không cần thêm thiết bị nào ngoại trừ một hệ điều hành thích hợp trên mỗi máy tính. Vì người dùng tự kiểm soát tài nguyên của họ nên không cần người quản trị riêng.

Khi hệ thống mạng ngang hàng phát triển với số lượng nhiều lên, các quan hệ ngang hàng trở nên khó cộng tác và phức tạp. Mạng ngang hàng chỉ làm việc tốt với 10 máy tính hay ít hơn. Vì các mạng ngang hàng không có khả năng mở rộng nên hiệu suất của nó sẽ giảm nhanh khi số lượng máy tính trên mạng gia tăng. Do người dùng kiểm soát truy xuất tài nguyên trên máy tính của họ, cho nên điều này có nghĩa là khó duy trì tính an toàn. Mô hình client/server có thể được dùng để khắc phục các hạn chế này của mạng ngang hàng.



Hình 4.10. Mạng ngang hàng (peer-to-peer).

4.1.10. CLIENT/SERVER

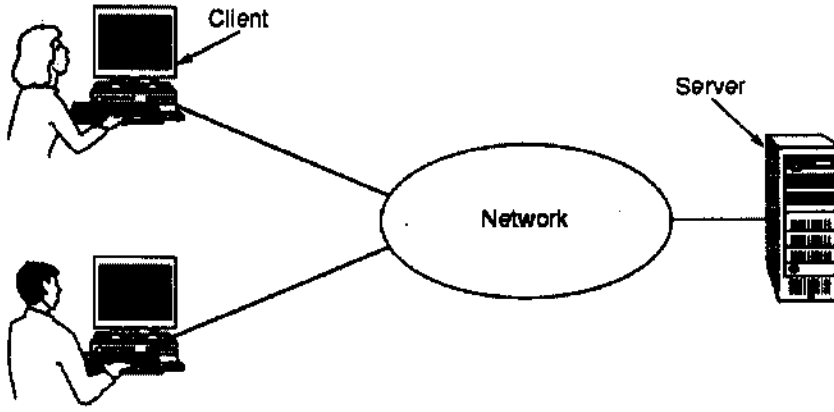
Trong mô hình mạng Client/Server, các dịch vụ mạng, tài nguyên mạng được tập trung vào một máy tính và máy tính đó gọi là Server. Các máy tính trạm gửi yêu cầu sử dụng các dịch vụ lên máy chủ và máy chủ sẽ đáp

ứng các yêu cầu trên. Server là máy tính trung tâm hoạt động liên tục để đáp ứng các yêu cầu từ các client về tập tin, in ấn, ứng dụng và các dịch vụ khác. Hầu hết các hệ điều hành mạng đều tuân theo dạng quan hệ client/ server. Thông thường, các máy tính để bàn đóng vai trò là các client và một hay nhiều máy tính có cấu hình mạnh như CPU có tốc độ xử lý cao, bộ nhớ lớn, phần mềm có chức năng đặc biệt đóng vai trò là server. Trong mô hình client/server vẫn tồn tại mô hình mạng ngang hàng, các máy tính trạm trong mô hình vẫn có thể trao đổi dữ liệu, tài nguyên cho nhau.

Hệ thống sever được thiết kế để kiểm soát yêu cầu từ nhiều client cung một lúc, số các client, dịch vụ sẽ quyết định số máy chủ tối thiểu cần dùng trên mạng, người thiết kế mạng giỏi là phải tính toán sao cho các máy chủ chịu tải từ client đồng đều và đảm bảo tốc độ hoạt động trên mạng ổn định và đáp ứng được các yêu cầu băng thông tối thiểu của từng dịch vụ. Trước khi một client truy xuất các tài nguyên của server, client phải được nhận dạng và được xác thực để dùng tài nguyên đó trên server. Điều này được thực hiện bằng cách gán cho mỗi client một account name và password, cặp này sẽ được thẩm tra bởi một dịch vụ xác thực. Dịch vụ xác thực đóng vai trò như một lính gác để canh phòng hoạt động truy xuất tài nguyên. Với sự tập trung các account, bảo vệ và điều khiển truy xuất, các mạng theo mô hình client/ server đơn giản trong việc quản trị các mạng lớn.

Việc các tài nguyên trên mạng như hệ thống file, máy in và các ứng dụng được lưu trữ và quản lý tập trung, giúp chúng ta bảo dưỡng và backup dễ dàng hơn rất nhiều. Thay vì trải rộng tài nguyên này ra một số các máy tính cá nhân, các tài nguyên này được đặt trên các server trung tâm làm cho truy xuất dễ dàng hơn. Hầu hết các hệ thống client/server đều có các tiện ích tăng cường nhằm bổ sung dịch vụ mới gia tăng sự hữu dụng của mạng.

Việc tập trung các dịch vụ trên máy chủ cũng tạo ra các cơ hội cho những kẻ tấn công truy xuất bất hợp pháp có thể dễ dàng tìm những thông tin cần lấy, đồng thời các server tỏ ra là một điểm hỏng hóc nóng trên hệ thống mạng. Không có server hoạt động, mạng không thể thực hiện bất kỳ chức năng nào. Các server yêu cầu nhóm chuyên viên phải được huấn luyện để quản trị và điều hành. Điều này làm tăng chi phí hoạt động của mạng. Các hệ thống server cũng yêu cầu sự bổ sung phần cứng và phần mềm đặc biệt làm tăng chi phí đầu tư.



Hình 4.11. Mạng gồm có hai client và một server.

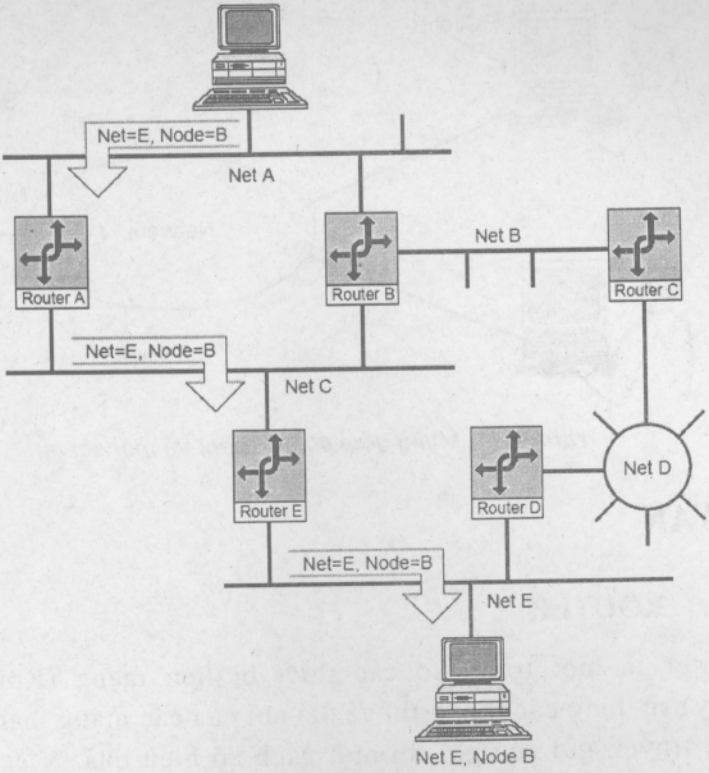
4.2. WAN

4.2.1. ROUTER

Router là một trong số các thiết bị liên mạng (Router, Brouter, Gateway) sử dụng các thông tin về địa chỉ của các mạng thành phần để hỗ trợ việc truyền gửi các gói tin một cách có hiệu quả. Việc sử dụng các thông tin về địa chỉ của mạng để gửi các gói tin được gọi là việc định tuyến. Router thực hiện việc định tuyến.

Router tổ chức một mạng lớn dưới dạng các segment mạng logic. Mỗi một segment mạng đều được gán địa chỉ sao cho tất cả các gói tin đều có cả hai địa chỉ là địa chỉ của mạng đích đến và địa chỉ của thiết bị đích đến.

Router hoạt động "thông minh" hơn bridge rất nhiều. Router không những xây dựng bảng địa chỉ của các mạng, mà nó còn sử dụng các thuật toán để xác định đường truyền có hiệu suất cao nhất để gửi gói tin đến bất kỳ một mạng nào. Ngay cả trong trường hợp một segment mạng đặc biệt nào đó không được gắn kết trực tiếp với một router, thì router này vẫn xác định được cách tốt nhất để gửi gói tin đến một thiết bị nào đó trong mạng tách biệt này. Router còn có thể kết nối các loại mạng khác nhau lại thành một liên mạng (ví dụ như kết nối ETHERNET với Token Ring).



Hình 4.12. *Sơ đồ hoạt động của Router*

Vì các router có thể xác định được hiệu suất định tuyến nên chúng thường được sử dụng để kết nối mạng LAN với mạng WAN (Wide Area Network). Các mạng WAN thường xuyên được thiết kế với đa đường truyền dẫn (multiple paths- các đường truyền đa kênh), và khi đó các router sẽ bảo đảm cho việc các đường truyền được sử dụng một cách có hiệu quả nhất (với hiệu suất cao nhất). Có hai loại router là router tĩnh (static router) và router động (dynamic router):

Router tĩnh (static router): các router tĩnh không thể tự xác định được đường dẫn. Thay vào đó, người sử dụng phải thiết lập bảng định tuyến chỉ rõ các tuyến dẫn tiềm năng cho các gói tin.

Router động (dynamic router): các router loại này có khả năng tự xác định được các tuyến và tìm ra đường dẫn tối ưu trong số các đường dẫn khả dĩ dựa trên các thông tin của bản thân gói tin và các thông tin thu được từ các router khác.

Để xác định đường dẫn tốt nhất cho một gói tin các router sử dụng một số thuật toán định tuyến. Một vài thuật toán định tuyến thông dụng được trình bày dưới đây.