TRƯỜNG ĐẠI HỌC CÔNG NGHỆ GIAO THÔNG VẬN TẢI

KHOA CÔNG NGHỆ THÔNG TIN

BÀI GIẢNG LÝ THUYẾT

KỸ THUẬT LIÊN MẠNG

Chương 1. TỔNG QUAN

1.1 Mạng máy tính và chuẩn hóa mạng máy tính

Mạng máy tính: Mạng máy tính là một hệ thống gồm nhiều máy tính và các thiết bị được kết nối với nhau bởi đường truyền vật lý theo một kiến trúc (Network Architecture) nào đó nhằm thu thập và chia sẽ tài nguyên cho nhiều người sử dụng.

Phân loại mạng:

PAP

LAN

MAN

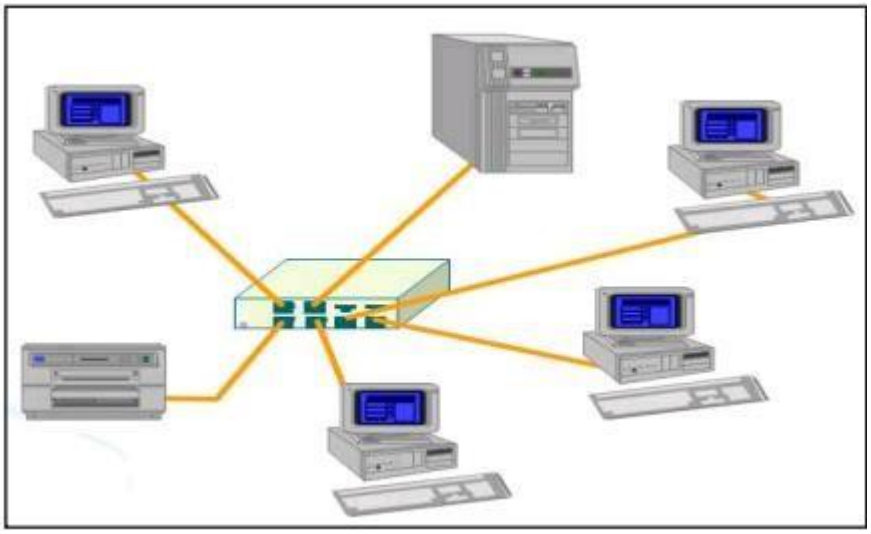
GAN

Kiến trúc mạng (Network Architecture): Cách nối các máy tính và thiết bị với nhau và tập hợp các qui tắc, qui ước mà tất cả các thực thể tham gia truyền thông trên mạng phải tuân theo. Gồm 2 thành phần:

Cách nối: Hình trạng mạng (Topolopy)

Một số Topology mạng cơ bản:

+ Dạng hình sao – Start



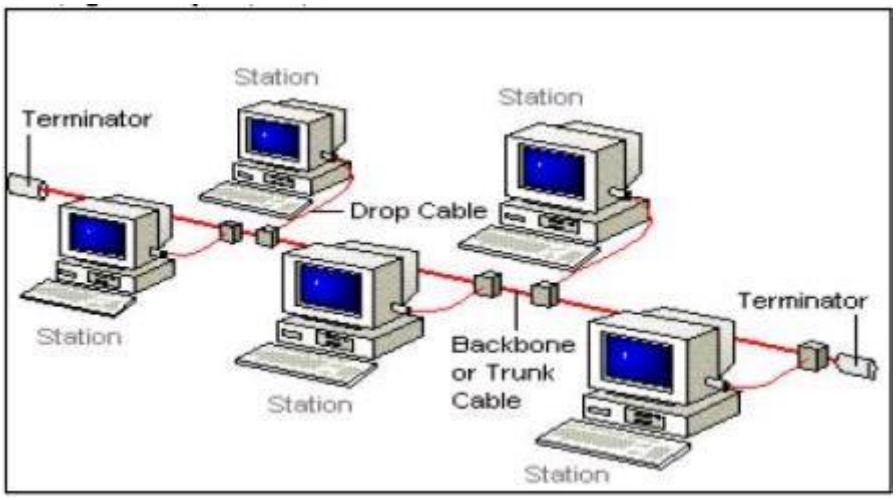
Bao gồm các thiết bị đầu cuối (terminator) được nối vào trung tâm điều khiển, theo mô hình Client/Server. Bộ môn An ninh mạng

Thiết bị trung tâm sẽ thực hiện việc bắt tay giữa các cặp trạm cần trao đổi thông tin với nhau, thiết lập các liên kết điểm - điểm (point to point), xử lý quá trình trao đổi thông tin.

Ưu điểm:

- Lắp đặt đơn giản, dễ dàng cấu hình lại
- Dễ dàng kiểm soát và khắc phục sự cố.
- Ít xảy ra va chạm, xung đột trên đường truyền
- Đạt tốc độ khá cao.
- Nhɑợc điểm:
- Khoảng cách mạng hạn chế.

+ Dạng hình tuyến – Bus



Là mạng mà các máy được nối vào một đường trục (backbone or Trunk Cable).Ở hai đầu của đường trục có các Terminator thực hiện đánh dấu kết thúc và truyền lại dữ liệu.

Ưu điểm:

- Phạm vi lớn, tốc độ truyền cao.

Nhược điểm:

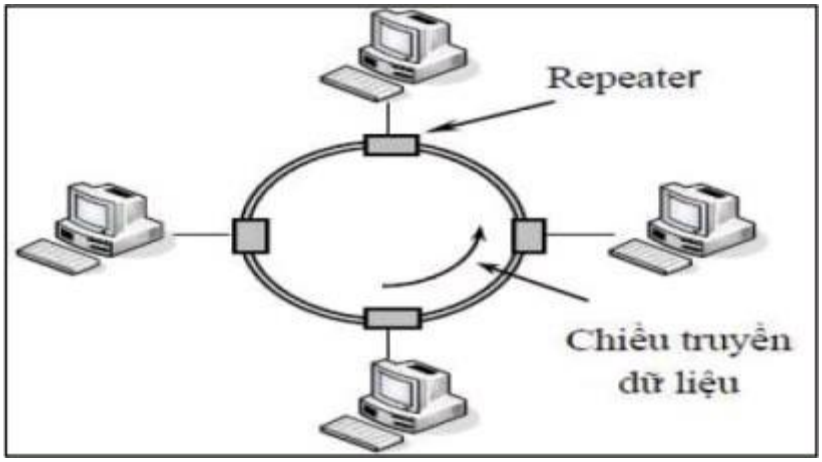
- Cần giao thức điều khiển truy cập đường truyền
- Khi có sự cố khó kiểm soát và khắc phục, dễ gây ảnh hưởng tới toàn mạng hơn mạng star.

Dễ xảy ra va chạm, xung đột trên đường truyền

+ Dạng hình vòng – Ring

Mô tả:

- Đường cáp chính làm thành một vòng khép kín.
- Các thiết bị đầu cuối được nối với vòng thông qua Repeater có nhiệm vụ nhận tín hiệu rồi chuyển tới trạm kế tiếp trên vòng.
- Tín hiệu được truyền cho nhau theo một chiều, tại một thời điểm chỉ một trạm được truyền.
- Mỗi trạm khi nhận được một gói dữ liệu có thể nhận hoặc chuyển tiếp.
- Giao thức điều khiển thẻ bài (Token)



Ưu điểm:

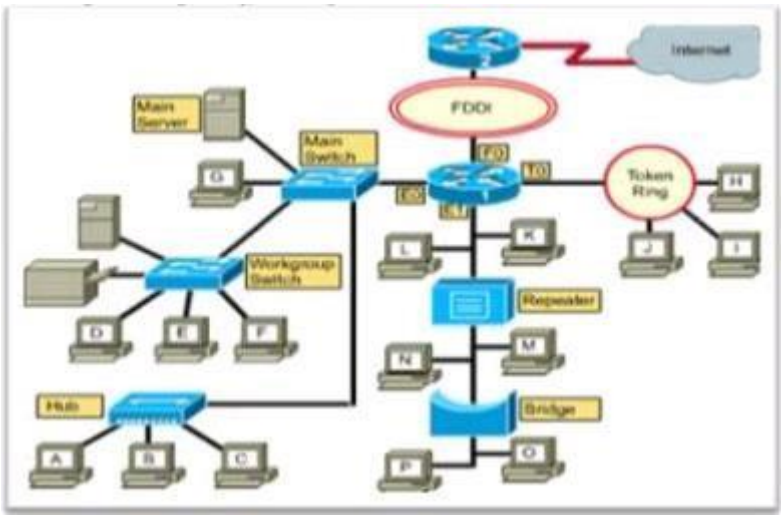
 Nới rộng vòng xa

Nhqợc điểm:

 Đường dây phải khép kín, nếu bị ngắt ở nơi nào đó

 Giao thức điều khiển truyền dữ liệu phức tạp.

+ Dạng hỗn hợp – Kết hợp các dạng trên.



Qui tắc, qui ước: Giao thức mạng (Protocol)

+ Khái niệm về giao thức mạng? : Để các máy trên mạng có thể trao đổi thông tin với nhau được thì chúng phải tuân

theo các qui tắc, qui ước về nhiều mặt: từ khuôn dạng kích thức, thủ tục gửi, thủ tục nhận,

kiểm soát, cho đến việc xử lý lôi, sự cố xảy ra và an toàn thông tin truyền như thế nào. Tập

các qui tắc, qui ước đó chính là giao thức mạng.

+ Chức năng của giao thức mạng.

- ✓ Đóng gói dữ liệu (Encapsulation)
- ✓ Phân đoạn và hợp lại
- ✓ Điều khiển liên kết
- ✓ Giám sát
- ✓ Điều khiển lưu lượng
- ✓ Điều khiển lỗi
- ✓ Đồng bộ hóa
- ✓ Địa chỉ hóa

1.2. Các giao thức và kiến trúc mạng

Kiến trúc phân tầng:

Tại sao phải chuẩn hóa mạng?

Giao thức mạng: là một phần rất quan trọng của kiến trúc mạng máy tính. Trong hệ thống mạng có rất nhiều giao thức, số giao thức và chức năng của nó phu thuộc vào mục đích xây dựng mạng.

Sự khác nhau về các qui định truyền thông trong các hệ thống mạng của các tổ chức khác nhau.

Các sản phẩm mạng do các công ty sản xuất không theo một chuẩn truyền thông chung.

Tổ chức tiêu chuẩn

ISO (International Standards Organization): đưa ra mô hình chuẩn OSI - Open Systems Interconnection

Hệ thống giao thức là một trong các thành phần cốt lõi để thiết kế nên MMT, do vậy cần được xây dựng theo một mô hình thống nhất. Mỗi hệ thống MMT hiện nay đều được coi như cấu trúc đa tầng giao thức. Trong đó mỗi tầng cung cấp một số dịch vụ nhất định. Mô hình đó được gọi là kiến trúc phân tầng.

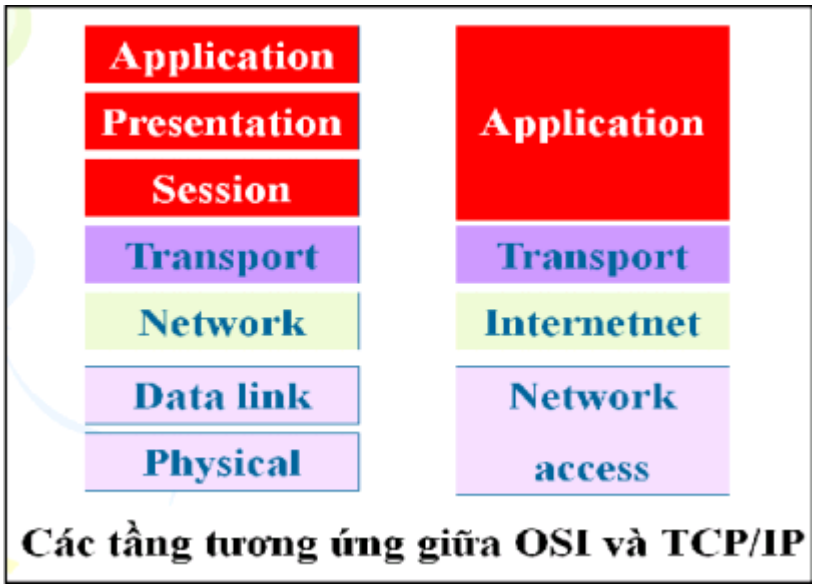
Nguyên tắc của kiến trúc phân tầng là:

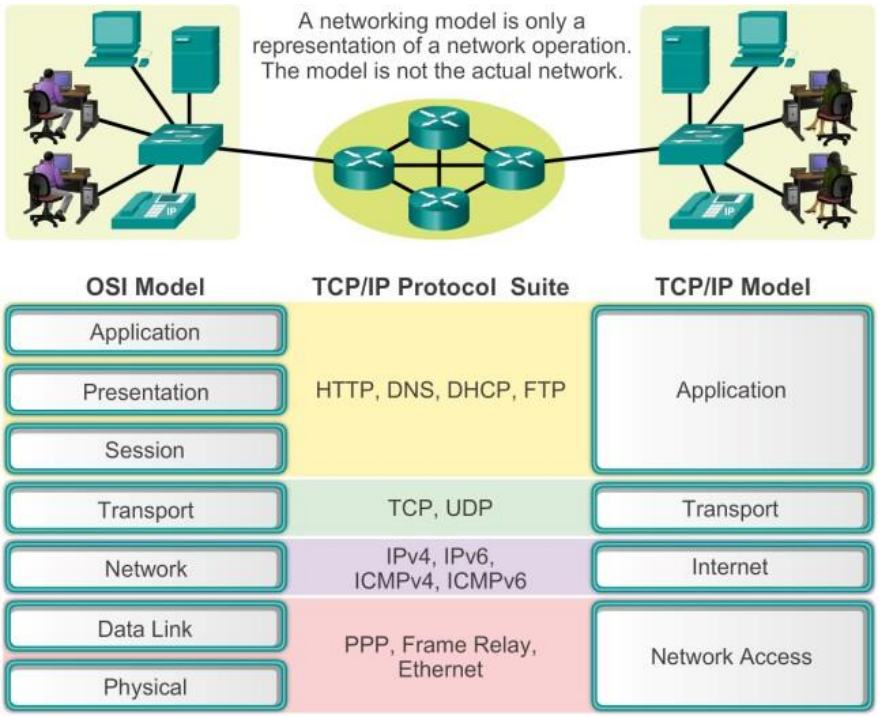
(1) Mỗi hệ thống trong mạng đều có cấu trúc tầng (số lượng tầng và chức năng của mỗi tầng là như nhau).

(2) Giữa 2 tầng liền kề trong một hệ thống giao tiếp với nhau qua 1 giao diện qua đó xác định các hàm nguyên thủy và các dịch vụ tầng dưới cung cấp.

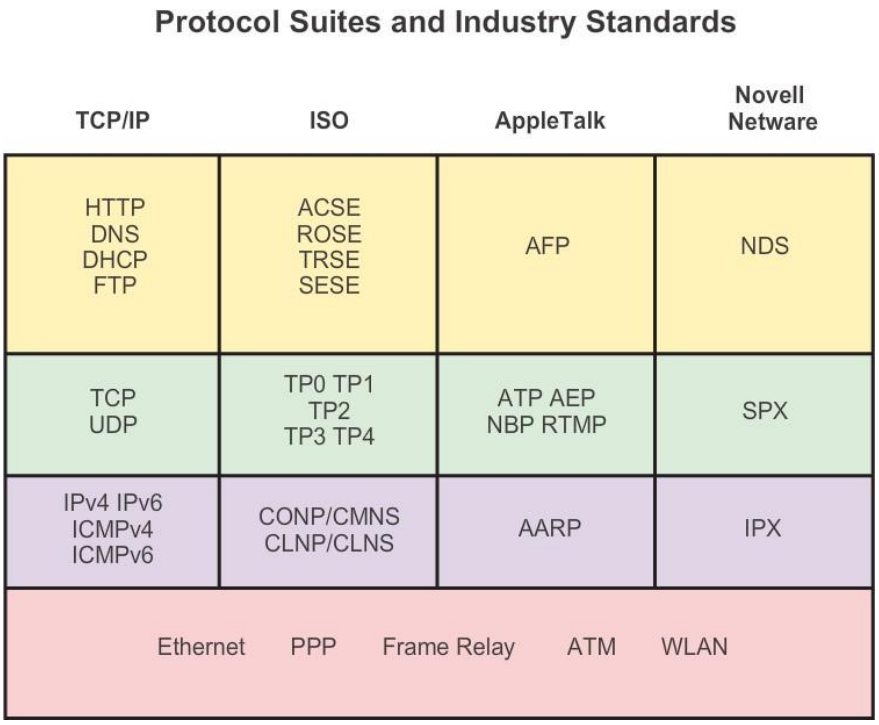
(3) Giữa hai tầng đồng mức ở hai hệ thống giao tiếp với nhau thông qua các luật lệ, qui tắc được gọi là giao thức.

(4) Trong thực tế, dữ liệu không được truyền trực tiếp từ tầng thứ i của hệ thống này sang tầng thứ i của hệ thống khác (trừ tầng thấp nhất). Mà việc kết nối giữa hai hệ thống được thực hiện thông qua hai loại liên kết: liên kết vật lý ở tầng thấp nhất và liên kết lôgic (ảo) ở các tầng cao hơn.





Một số kiến trúc và giao thức mạng tương ứng:



1.3. Mở rộng và liên kết mạng

1961-1972: Các nguyên lý mạng chuyển mạch gói

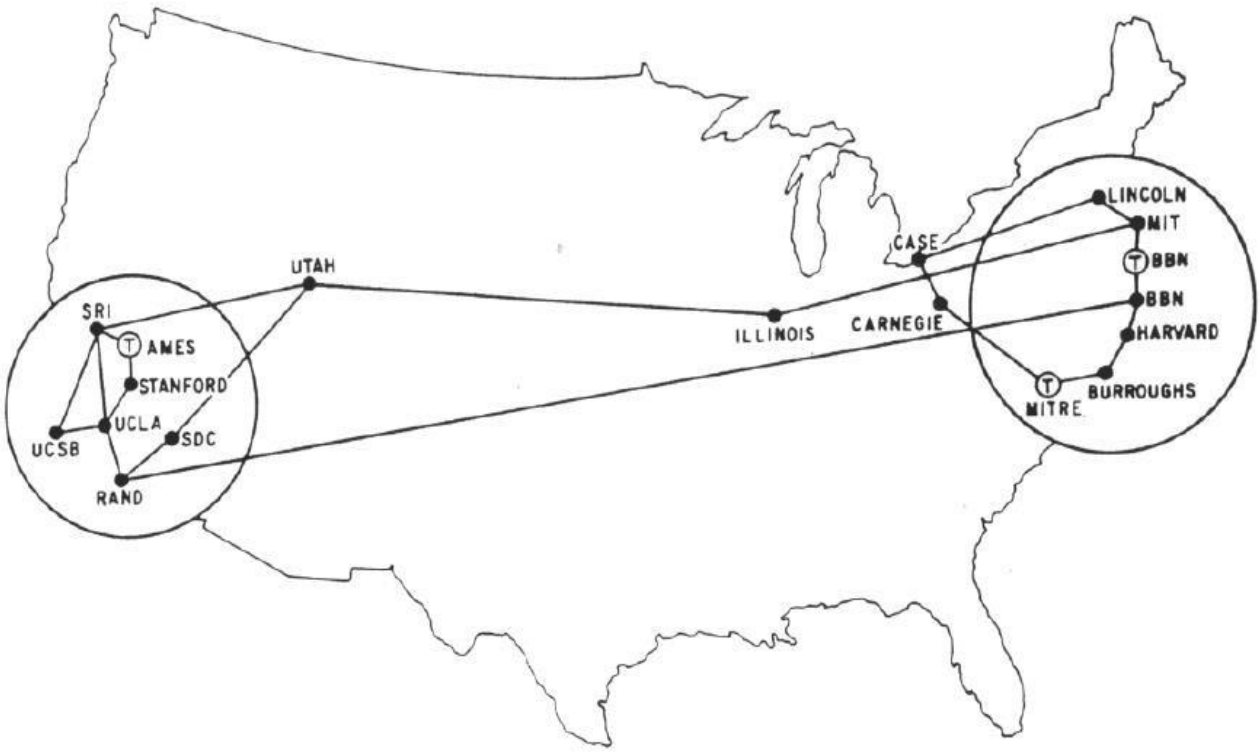
1960s: Mạng điện thoại và sự phát triển của máy tính

1961: Kleinrock – Lý thuyết hàng đợi hiệu quả của chuyển mạch gói

1964: Baran – Mạng chuyển mạch gói

1967: ARPAnet được phê duyệt (Advanced Research Projects Agency)

Một mạng hoàn chỉnh với 4 nút, 56kbps kết nối UCSB (University of California), Santa Barbara – TAH (University of Utah) - SRI



MAP 4 September 1971

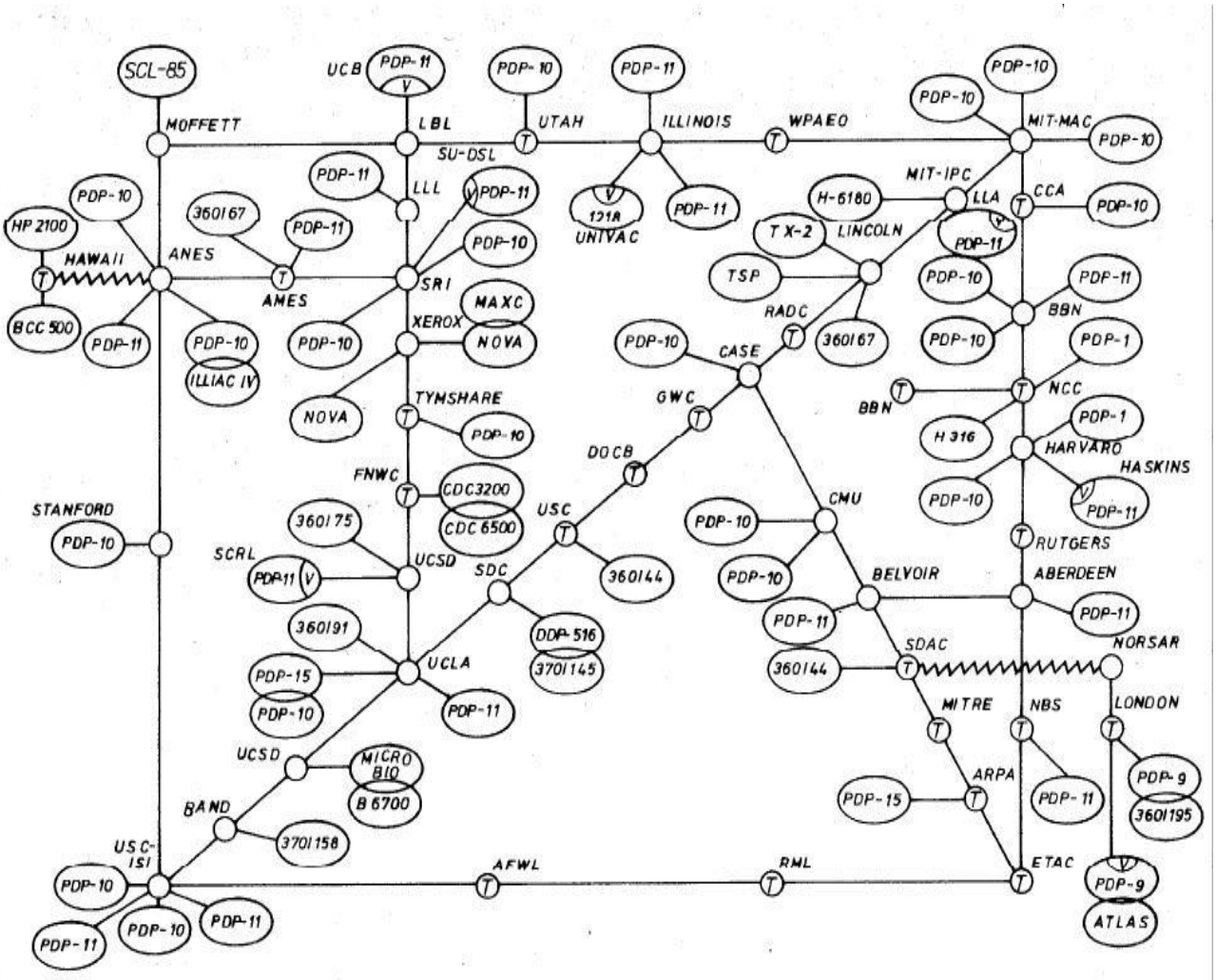


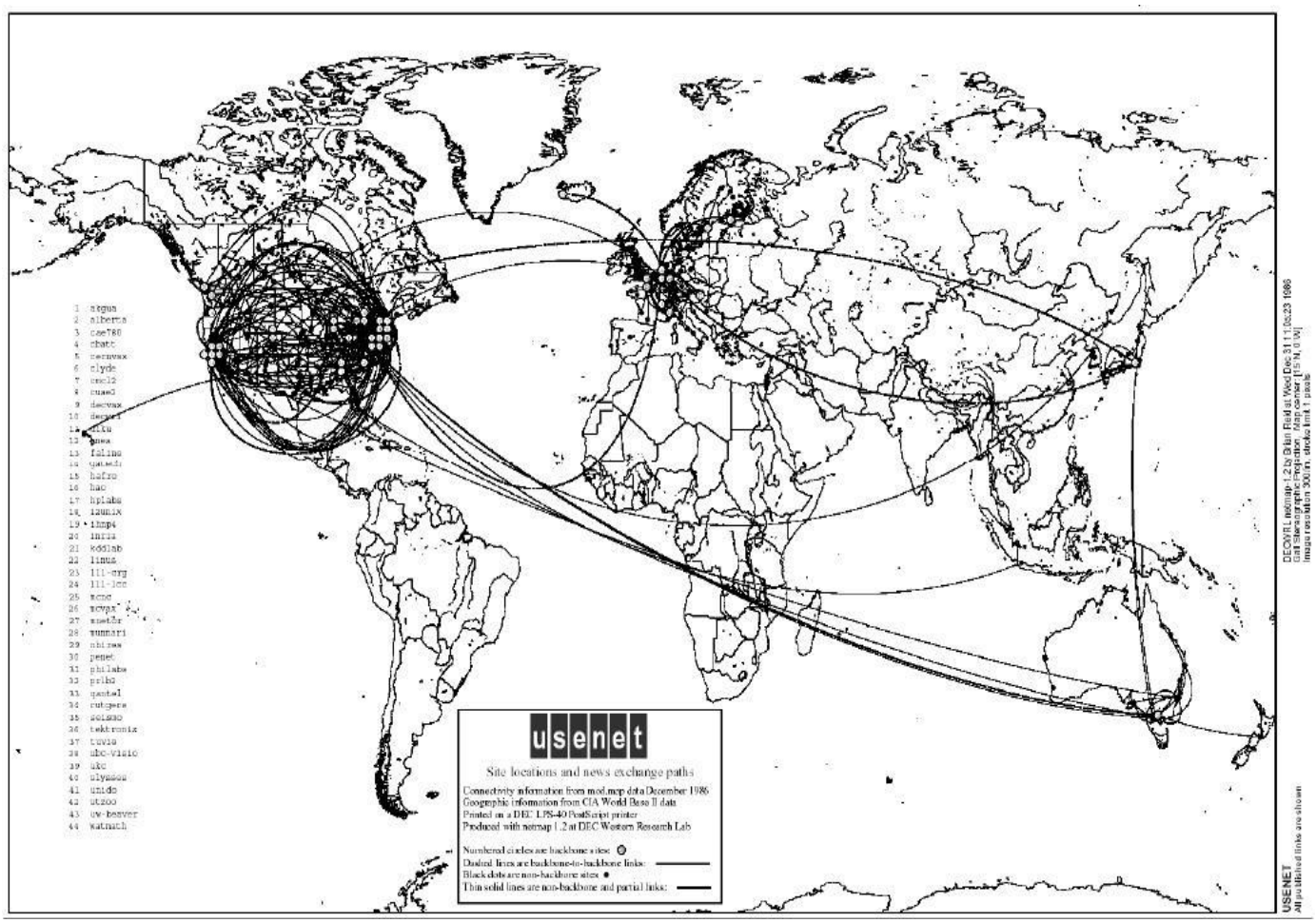
Abb. 4 ARPA NETwork, topologische Karte. Stand Juni 1974.

1974: Cerf & Kahn – nguyên lý kết nối

các hệ thống mở (Turing Awards)

1976: Ethernet, Xerox PARC

Cuối 1970: ATM



Bản đồ mạng USENET 1986 – tiền hân mạng Internet (1990)

Chương 2: LIÊN KẾT MẠNG

2.1. Định tuyến

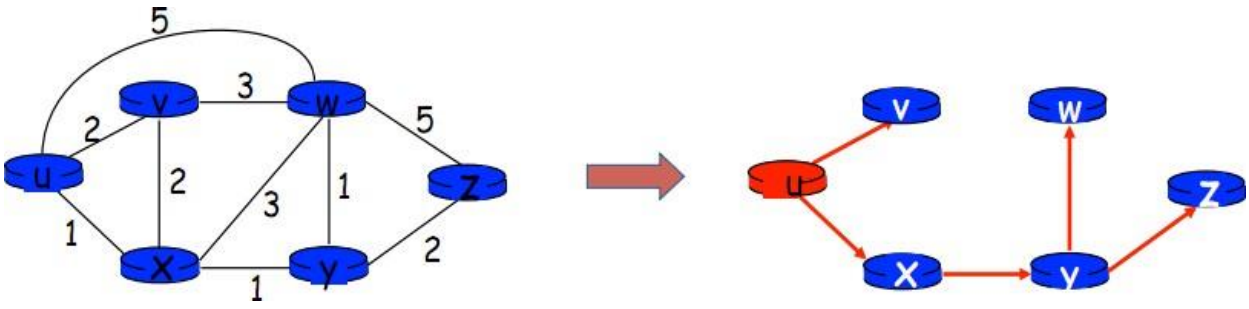
2.1.1. Các giải thuật định tuyến

- ✓ **Link-state: Dijkstra**
- ✓ **Distance vector: Bellman Ford**
- ✓ Flooding
- ✓ Giải thuật tìm đường phân cấp
- ✓ Giải thuật tìm hai đường đi phân biệt Suurball
- ✓ Giải thuật Prim-Dijktra
- ✓ Định tuyến cho các trạm di động
- ✓ Định tuyến trong mạng Ad-hoc

a. Cây đường đi ngắn nhất SPT – Shortest Path Tree

Các cạnh xuất phát từ nút gốc và tới các lá u Đường đi duy nhất từ nút gốc tới nút v, là đường đi ngắn nhất giữa nút gốc và nút v u Mỗi nút sẽ có một SPT của riêng nút đó 4 x y w u z u x y v w z 2 2 1 3 1 1 2 5 3 5 v Các giải thuật tìm đường Tìm đường đi từ 1 nguồn đến tất cả các nút khác thường dựa trên cây khung uCây khung là 1 cây có gốc là nguồn đi qua tất cả các đỉnh của một đồ thị Nguyên tắc tối ưu của các giải thuật tìm đường:

- ✓ Cây khung tối thiểu: tổng trọng số min.
- ✓ Một cây khung tối thiểu có thể không phải là duy nhất.
- ✓ Một cây khung tối thiểu không chứa bất kỳ một vòng lặp nào,
- ✓ Đồ thị với các nút (bộ định tuyến) và các cạnh (liên kết)
- ✓ Chi phí cho việc sử dụng mỗi liên kết c(x,y)
- ✓ Băng thông, độ trễ, chi phí, mức độ tắc nghẽn…
- ✓ Giả thuật chọn đường: Xác định đường đi ngắn nhất giữa hai nút bất kỳ

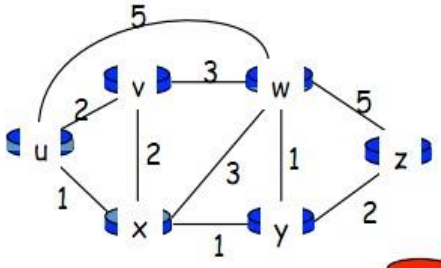


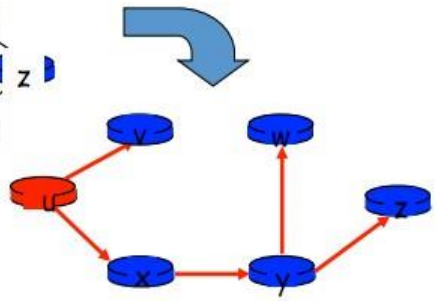
Cây đương đi ngắn nhất SPT

b. Link-State: Dijkstra (1959):

- ✓ Thuật toán Dijkstra, mang tên của nhà khoa học máy tính người Hà Lan Edsger Dijkstra, là một thuật toán giải quyết bài toán đường đi ngắn nhất nguồn đơn trong một đồ thị có hướng.
- ✓ Thuật toán thực hiện tìm đường đi từ một đỉnh đến tất cả các đỉnh còn lại của đồ thị có trọng số không âm.
- ✓ Thuật toán Dijkstra bình thường sẽ có độ phức tạp là trong đó m là số cạnh, n là số đỉnh của đồ thị đang xét.
- ✓ Để minh họa các giải thuật tìm đường, thông thường người ta ký hiệu N là số nodes trong mạng, i và j là nhãn của các node trong mạng.

Step	T	d(v),p(v)	d(w),p(w)	d(x),p(x)	d(y),p(y)	d(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					





SPT của u:

Bảng chọn đường của u:

destination	link
v	(u,v)
x	(u,x)
y	(u,x)
w	(u,x)
z	(u,x)

Ký hiệu:
G = (V,E) : Đồ thị với tập đỉnh V và tập cạnh E
c(x,y): chi phí của liên kết x tới y; = ∞ nếu không phải 2 nút kế nhau
d(v): chi phí hiện thời của đường đi từ nút nguồn tới nút đích. v
p(v): nút ngay trước nút v trên đường đi từ nguồn tới đích
T: Tập các nút mà đường đi ngắn nhất đã được xác định
Init():
Với mỗi nút v, d[v] = ∞, p[v] = NIL
d[s] = 0
Update(u,v), trong đó (u,v) u, v là một
cạnh nào đó của G
if d[v] > d[u] + c(u,v) then
d[v] = d[u] + c(u,v)

p[v] = u

Init() ;

T = Φ;

Repeat

u: u ∈ T | d(u) là bé nhất ;

T = T ∪ {u};

for all v ∈ neighbor(u) và v ∉ T

update(u,v) ;

Until T = V

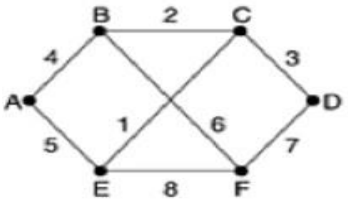
Ý nghĩa Link State (liên kết trạng thái) ứng dụng giao thức mạng

(Routing Protocol – OSPF, IS-IS)

Khám phá các láng giềng và học các địa chỉ mạng của chúng : Khám phá các routers láng giềng bằng cách gửi 1 gói tin HELLO trên mỗi đường dẫn, Khi 2 hay nhiều routers kết nối bởi một LAN, tình huống sẽ phức tạp . mỗi LAN coi như nútảo.

*Đo độ trễ (delay), hay giá (cost) tới các láng giềng : C*ác routers phải có sự ước lượng về các đường dẫn tới các routers láng giếng để làm trọng số cho giải thuật định tuyến.

Xây dựng một gói tin báo cho các trạng thái/ thông tin vừa học: Gói tin bắt đầu với định danh của máy gửi, theo sau là thứ tự trạng thái, tuổi (age) và một danh sách các láng giềng. Thông thường các gói tin trạng thái được xây dựng một cách định kỳ.



Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

Ví dụ về các gói tin trạng thái liên kết cho subnet

Gửi gói tin cập nhật đến tất cả các routers khác:

- ✓ Sử dụng thuật toán ngập lụt (flooding) để gửi các gói tin trạng thái, Các gói tin chứa thông tin về tuổi (age) để tránh trùng lặp và cập nhật thông tin. Khi bộ đếm tuổi quay về zero, thông tin về routers đấy sẽ bị hủy.
- ✓ Trường tuổi cũng giảm theo từng routers trong quá trình ngập lụt để đảm bảo không có gói tin nào có thể tồn tại vô hạn
- ✓ Các gói tin trạng thái thường được lưu vào bộ nhớ đệm để xử lý tuần tự, nếu có trùng lặp sẽ bị loại bỏ.

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Ví dụ về buffer đệm lưu trữ gói tin trạng thái của router B

Tính đường dẫn ngắn nhất cho từng routers

(Sử dụng giải thuật Dijkstra để tìm đường ngắn nhất tới từng routers)

- ✓ Sau khi các routers có đầy đủ thông tin trạng thái các đường dẫn sẽ sử dụng thuật toán Dijkstra để tính toán/ xây dựng đường dẫn ngắn nhất cho mọi nơi đến có thể,
- ✓ Chọn đường trạng thái liên kiết (link-state) được dùng nhiều trong các mạng hiện nay, Các giao thức chọn đường trạng thái liên kết phổ biến là
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System-Intermediate System).
- ✓ Bộ định tuyến dùng nhiều bộ nhớ và thực thi nhiều hơn so với các giao thức định tuyến theo vectơ khoảng cách.
- ✓ Lý do cần thiết phải lưu trữ thông tin của tất cả các láng giềng, cơ sở dữ liệu mạng đến từ các nơi khác và việc thực thi các thuật toán định tuyến trạng thái.
- ✓ Các nhu cầu về băng thông cần phải tiêu tốn để khởi động sự phát tán gói trạng thái.

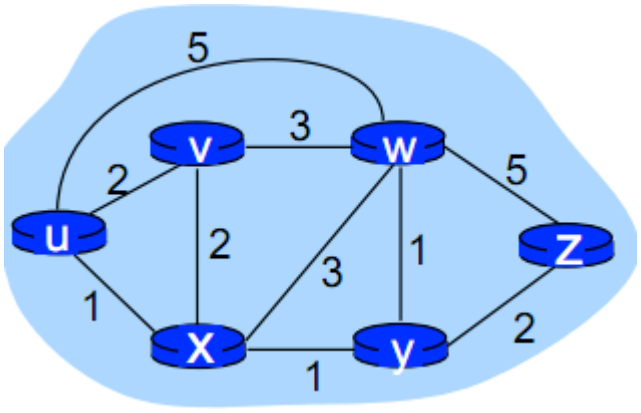
c. Distance-Vector (Bellman-Ford= phương trình quy hoạch) = RIP, IDX

Định nghĩa

dx(y) := chi phí của đường đi ngắn nhất từ x tới y

Ta có dx(y) = min {c(x,v) + dv(y) }

cho tất cả các v là hàng xóm của x



Dễ thấy, dv(z) = 5, dx(z) = 3, dw(z) = 3

du(z) = min { c(u,v) + dv(z),

c(u,x) + dx(z),

c(u,w) + dw(z) }

= min {2 + 5,

1 + 3,

5 + 3} = 4

B-F eq. cho ta biết:

Nút nào làm giá trị trên nhỏ nhất ➜ Lựa chọn là nút kế tiếp trong bảng chọn đường

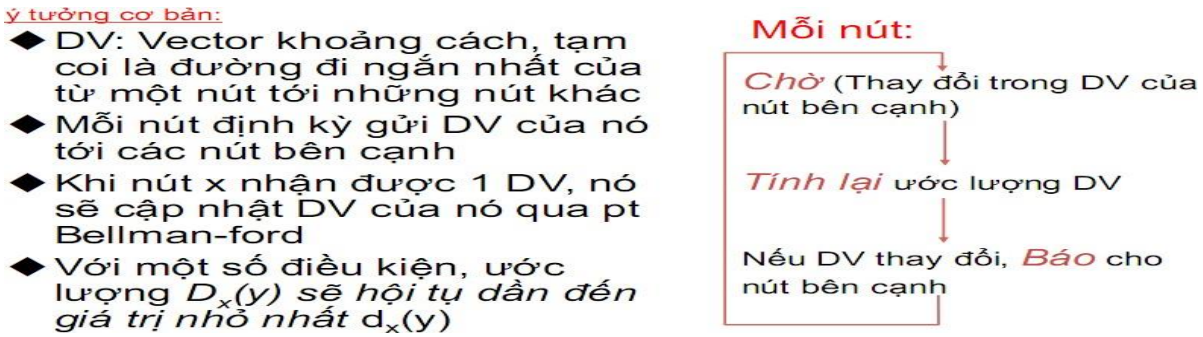
Mỗi router duy trì một bảng vector khoảng cách cho cự ly tốt nhất tới từng đích và đường truyền dùng để tới đích đó,

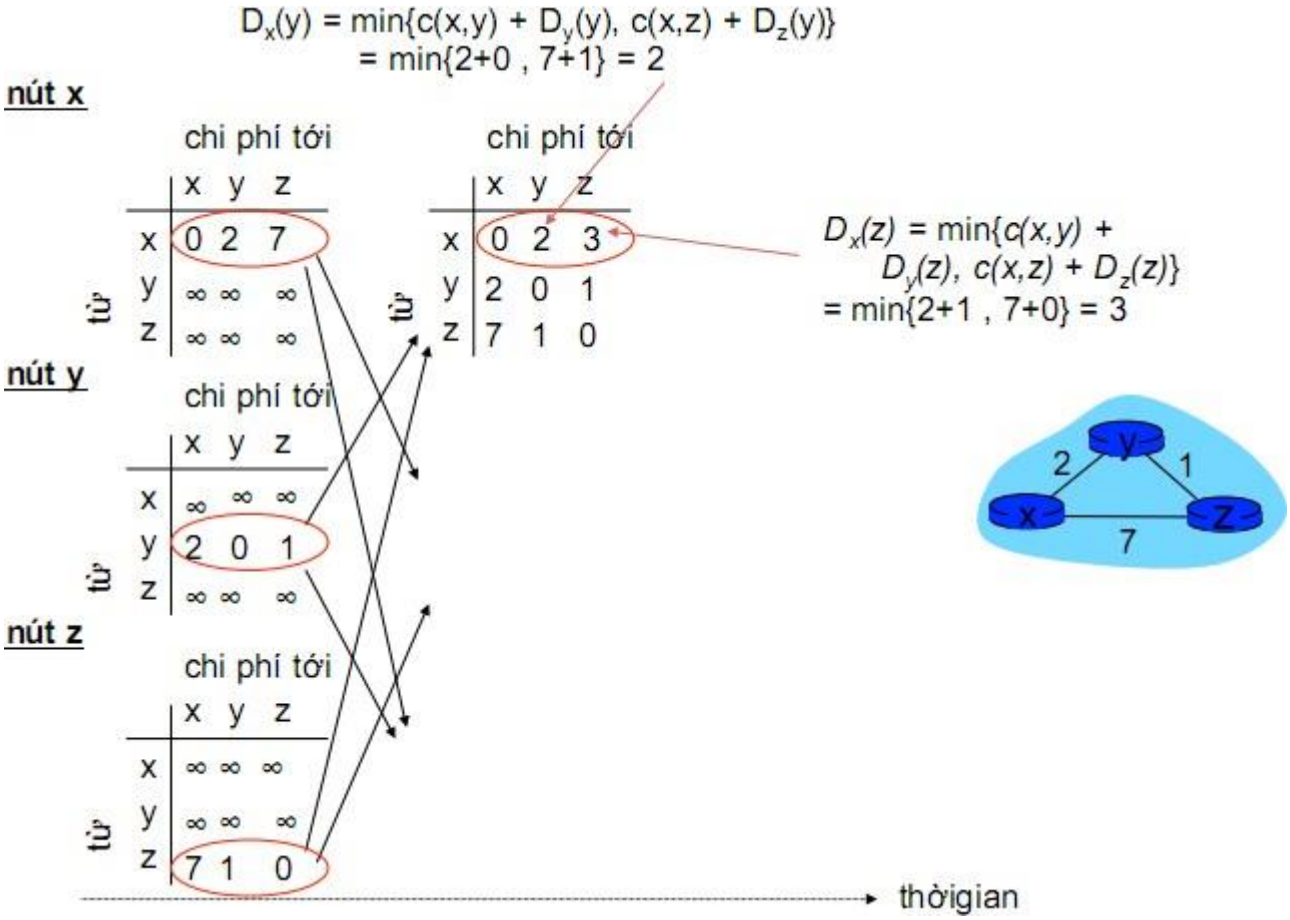
Các bảng vector khoảng cách được cập nhật thông tin nhờ trao đổi định kỳ với các láng giềng của nó, Sử dụng thuật toán Bellman-Ford Fulkerson,

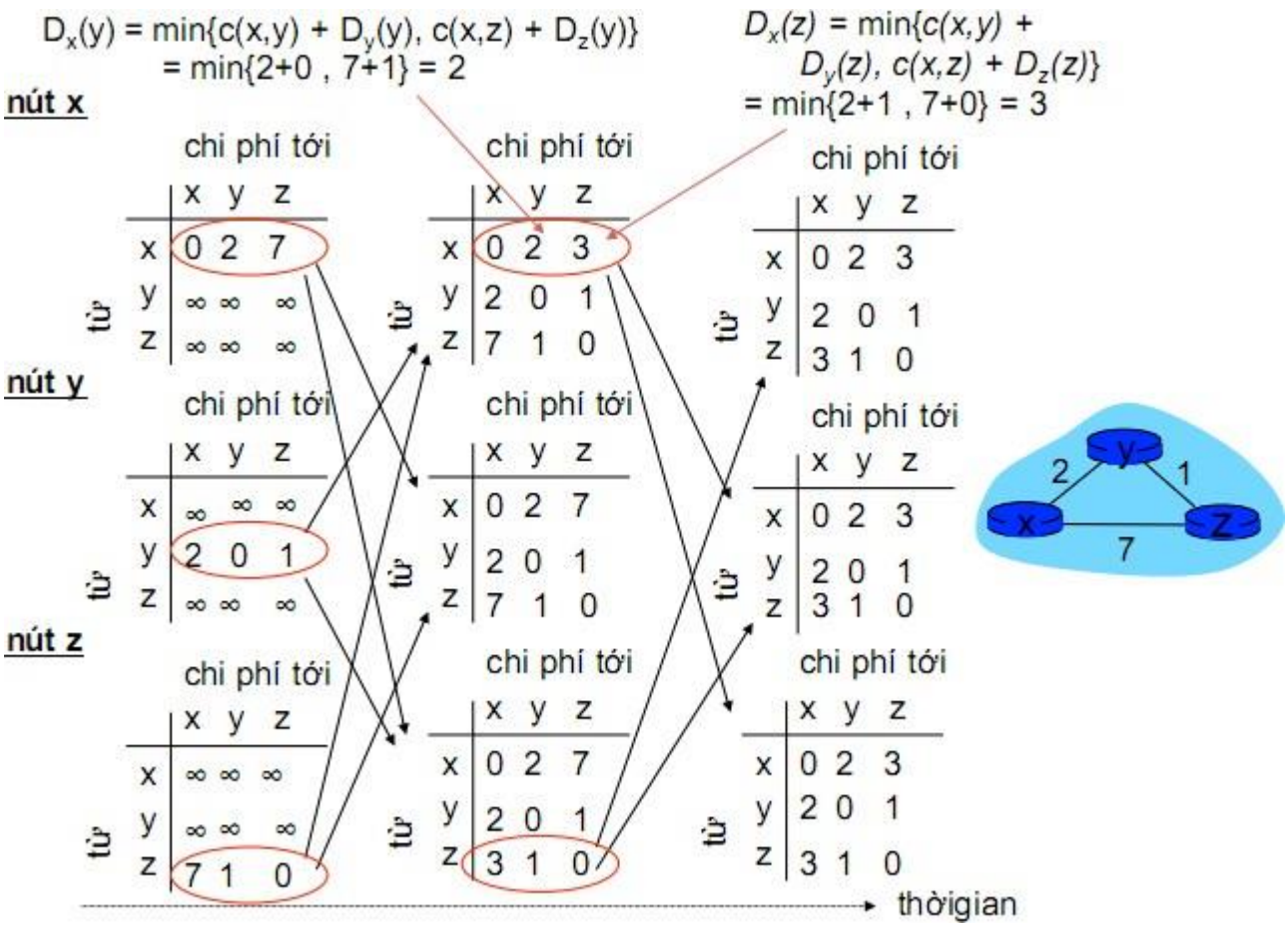
Là thuật toán chọn đường gốc cho mạng ARPANET và được dùng rộng rãi trong định tuyến IP trong giao thức định tuyến RIP (Routing Information Protocol), IDX của Novell.

Được sử dụng đến năm 1979 sau đó được thay thế bởi các giải thuật chọn đường trạng thái liên kết do độ trễ lớn, thời gian hội tụ lâu do đòi hỏi cần phải trao đổi các thông

điệp định tuyến lớn.




$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\}$
$= \min\{2+0 , 7+1\} = 2$
nút x
chi phí tới
x y z
từ
x 0 2 7
y ∞ ∞ ∞
z ∞ ∞ ∞
chi phí tới
x y z
x 0 2 3
y 2 0 1
z 7 1 0
$D_x(z) = \min\{c(x,y) + D_y(z), c(x,z) + D_z(z)\}$
$= \min\{2+1 , 7+0\} = 3$
nút y
chi phí tới
x y z
x ∞ ∞ ∞
y 2 0 1
z ∞ ∞ ∞
nút z
chi phí tới
x y z
x ∞ ∞ ∞
y ∞ ∞ ∞
z 7 1 0
y
x
z
2
1
7
thờigian



So Sánh Link – State và Distance-Vector

Chức năng	Link State	Distance Vector
Thông điệp trao đổi	n nút, E cạnh => O (nE) thông điệp	Chỉ đạo thay đổ giữa các nút kế bên (hàng xóm) Thời gian hội tụ thay đổi
Tốc độ hội tụ	Thuật toán $O(n^2)$ cần O(nE) thông điệp	Có sự thay đổi
Sự tin cậy Giả sử 1 rouer hoạt đông sai (lỗi)	Nút gửi các chi phí (giá trị Cost) sai Mỗi nút tính lại bảng chọn đường -> tối ưu	Có thể bị gửi sai Mỗi nút tính toán dựa trên các nút khác -> lỗi bi lan truyền tới các router phía sau

Tổng kết về các giao thức định tuyến phổ dụng trên mạng IP:

Đặc trưng	RIPv1	RIPv2	IRGP	EIGRP	OSPF
Distance-vector	X	X	X	X	
Link-state					X
Tự động tóm tắt định tuyến	X	X	X	X	
Hỗ trợ VLSM		X		X	X
3rd party compatible	X	X			X
Thích hợp	Nhỏ	Nhỏ	Vừa	Lớn	Lớn
Thời gian hội tụ	Chậm	Chậm	Chậm	Nhanh	Nhanh
Giá trị định tuyến	Hop count	Hop count	BW+D	BW+D	10E8/BW
Giới hạn hop	15	15	100	100	
Cân bằng tải cùng giá trị đt	X	X	X	X	X
Cân bằng tải ko cùng giá trị đt			X	X	
Thuật toán	Bellman-Ford	Bellman-Ford	Bellman-Ford	Dual	Dijkstra

Thuật toán Cisco DUAL (EIGRP)

DUAL áp dụng với IGRP, EIGRP, đọc quyền (Là trái tim của IGRP, EIGRP, chọn đường tối ưu)

Làm thế nào EIGRP xác định tuyến đường tốt nhất ?

Để hình dung đơn giản từ A đến E có ba tuyến đường: A-B-E, A-C-E, A-D-E.

Mỗi hàng xóm của A sẽ gửi một reported distance (RD) hay còn là chi phí từ những router đến đích.

B sẽ tốn chi phí là10.

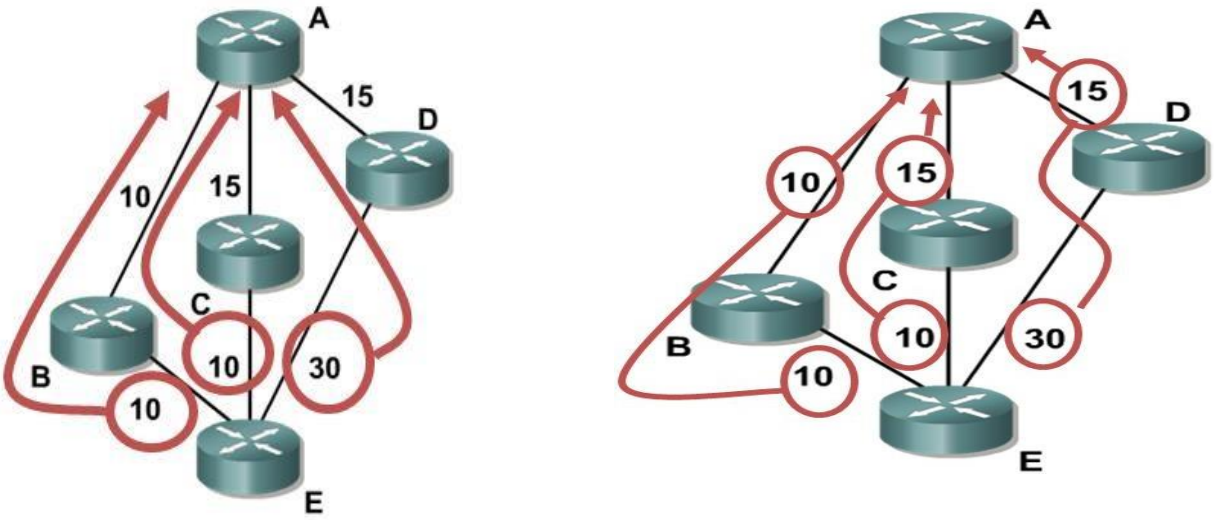
C sẽ tốn chi phí là10.

D sẽ tốn chi phí là30.

DUAL sẽ sử dụng những thông in đó để tính toán tuyến đường tốt nhất.

- Từ A, tổng số chi phi đến E khi đi qua:

- B là 20. C là 25. D là 45.
- Ta thấy trong ba tuyến đường, từ A đi qua B đến E có chi phí thấp nhất là 20 -> A-B-E là feasible distance (FD) tuyến đường ngắn nhất tới đích.



Các giải thuật khác (tìm kiếm tài liệu tham khảo)

- ✓ Flooding
- ✓ Giải thuật tìm đường phân cấp
- ✓ Giải thuật tìm hai đường đi phân biệt Suurball
- ✓ Giải thuật Prim-Dijktra
- ✓ Định tuyến cho các trạm di động
- ✓ Định tuyến trong mạng Ad-hoc

2.2. Kiểm soát tắc nghẽn

2.2.1. Các nguyên tắc và chính sách kiểm soát tắc nghẽn

- Tắc nghẽn: Luồng dữ liệu đi trên cáp với băng thông không đủ. Nó xảy ra khi nhiều thông tin lưu chuyển trên đường truyền hoặc máy nhận có thể chấp nhận ít thông tin hơn máy gửi trong cùng 1 giây (ms)
- Điều khiển luồng: Khi xảy ra tắc nghẽn mạng phải có cơ chế điều khiển luồng (Flow Control), nó thực hiện cơ chế chuyển dữ liệu tới nơi chờ (Cacher center) nào đó trong mạng, hoặc tạo một kết nối trực tiếp giữa 2 điểm.
  - Có 2 cách để giải quyết đồng bộ dữ liệu 2 đầu để đảm bảo không bị lỗi (truyền thông)

- Cách 1: Stop and Wait (ngưng và đợi)
- Cách 2: *sliding window flow Control* (cửa sổ di động) – phổ biến gồm 2 phương pháp

PP1: *window End to End* điều khiển luồng điểm gửi – nhận trông mạng

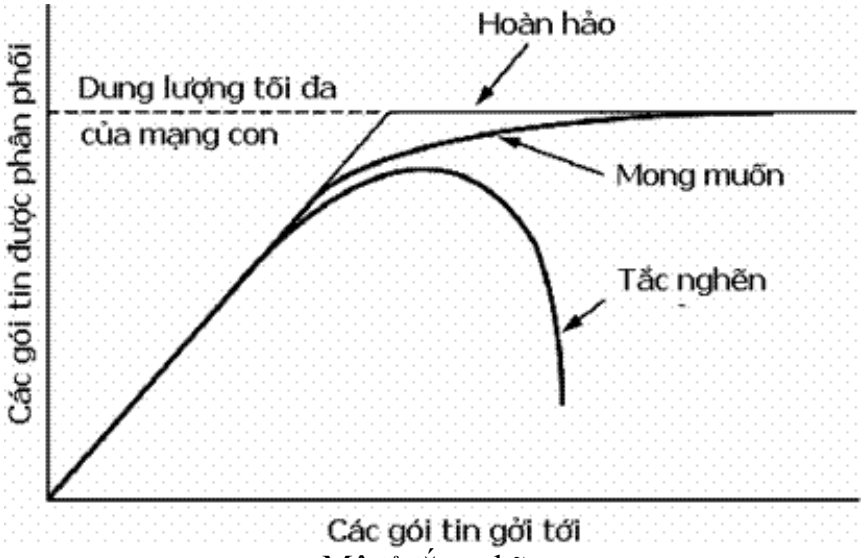
PP2: Hop by Hop- điều khiển luồng giữa hai nút liền kề

- Flow Control = Layer 1-4 (tùy theo giao thức tầng nào)

VD: TCP: flow control ở tầng transport, nhằm mục đích tránh tràn buffer ngõ vào.
Frame flow control ở tầng datalink, nhằm mục đích tránh tắc nghẽn trên đường truyền. flow control giữa máy tính và modem : tầng physical , nhằm mục đích tránh tràn buffer.

Các giải thuật chống tắc nghẽn

Khi có quá nhiều gói tin hiện diện trong một mạng con (hoặc một phần của nó), hiệu năng hoạt động của hệ thống bị giảm. Tình trạng này được gọi là "tắc nghẽn".



Mô tả tắc nghẽn

Hình H6.19 mô tả lại hiện tượng tắc nghẽn.

Khi số lượng gói tin chạy trong mạng con nằm dưới ngưỡng cho phép, chúng đều được phân phối đến đích (ngoại trừ những gói tin bị lỗi), và số lượng gói tin được phân phối tỉ lệ thuận với số lượng gói tin được phát ra lúc đầu. Tuy nhiên, khi mật độ giao thông tăng quá cao, các router không còn đáp ứng kịp nữa và chúng dần dần đánh mất một số gói tin. Điều này có xu hướng làm cho vấn đề tắc nghẽn nghiêm trọng thêm. Khi mà giao thông cực cao, hiệu năng hệ thống sụp đổ hoàn toàn và hầu như không gói tin nào được phân phát đến đích.

Có vài yếu tố góp phần gây ra tắc nghẽn. Nếu đột nhiên nhiều luồng mang các gói tin đến một nút tại nhiều ngõ vào, và tất cả các gói tin này đều cần một ngõ ra, thì một hàng đợi sẽ xuất hiện. Nếu không đủ bộ nhớ để lưu các gói tin trên hàng đợi này, một số gói tin sẽ bị mất. Tăng thêm bộ nhớ chỉ giúp không mất gói tin trong hàng đợi, nhưng Nagle (1987) đã chỉ ra rằng: nếu một router có bộ

nhớ vô hạn, sự tắc nghẽn lại càng tồi tệ hơn! Lý do là khi mà gói tin đến được đầu của hàng đợi thì nó đã bị mãn kỳ (timed out), và do đó sẽ có nhiều phiên bản trùng với gói tin đó được bên gởi gởi đến router, làm tăng thêm tải của mọi hướng đi đến đích của gói tin.

Các bộ xử lý chậm cũng có thể gây ra tắc nghẽn. Nếu CPU của router xử lý các gói tin trung chuyển qua nó chậm, hàng đợi cũng sẽ phát sinh, cho dù dung lượng các đường nối vào và ra đều vượt yêu cầu.

Tóm lại, đường truyền băng thông thấp có thể gây ra tắc nghẽn. Nâng cấp đường truyền nhưng năng lực xử lý của bộ xử lý tại router yếu cũng gây ra tắc nghẽn. Thành thử, nâng cấp một phần mà không phải là toàn bộ hệ thống chỉ đẩy sự tắc nghẽn từ nơi này đến nơi khác mà thôi. Vấn đề phát sinh từ sự bất cân đối giữa các bộ phận của hệ thống, và nó chỉ qua đi khi mà các bộ phận này được giữ cân bằng với nhau.

Các nguyên tắc chung để điều khiển tắc nghẽn

Nhiều bài toán trong các hệ thống phức tạp, ví dụ như trong mạng máy tính, có thể được xem xét theo quan điểm của lý thuyết điều khiển (control theory). Cách tiếp cận này dẫn đến việc chia các giải pháp thành hai loại: vòng đóng và vòng mở (closed loop and open loop). Các giải pháp dạng vòng đóng cố gắng giải quyết vấn đề tắc nghẽn bằng cách đưa ra thiết kế tốt cho mạng, thực chất là để đảm bảo tắt nghẽn sẽ không xảy ra. Một khi mạng được khởi động và chạy, sẽ không có việc sửa chữa giữa kỳ.

Các công cụ thực hiện việc điều khiển kiểu vòng mở bao gồm việc quyết định khi nào nên chấp nhận luồng giao thông mới, quyết định khi nào thì bỏ qua các gói tin và bỏ qua gói nào. Tất cả các công cụ trên đều có đặc điểm chung là chúng đưa ra các quyết định mà không quan tâm đến trạng thái hiện hành của mạng.

Ngược lại, các giải pháp kiểu vòng đóng dựa trên quan niệm về chu trình phản hồi thông tin. Cách tiếp cận này bao gồm 3 phần:

1. Giám sát hệ thống để phát hiện nơi nào và khi nào xảy ra tắc nghẽn.
2. Chuyển thông tin đến những nơi cần có những hành động ứng phó.
3. Điều chỉnh lại hoạt động của hệ thống để khắc phục sự cố.

Nhiều kiểu đo lường có thể được sử dụng để giám sát một mạng con để phát hiện ra tắc nghẽn ở đó. Các kiểu đo lường thường dùng nhất là tỉ lệ các gói tin bị bỏ qua do thiếu không gian trữ đệm, chiều dài trung bình của các hàng đợi, số lượng các gói tin bị mãn kỳ và được tái truyền, thời gian trì hoãn gói tin trung bình. Trong mọi tình huống, các số đo tăng đồng nghĩa với việc tăng tắc nghẽn.

Bước thứ hai trong chu trình phản hồi là chuyển thông tin về tắc nghẽn từ điểm được phát hiện bị tắc nghẽn đến điểm có trách nhiệm xử lý tình huống đó. Cách dễ nhất là để cho router phát hiện ra tắc nghẽn phát thông báo đến nút nguồn vừa gởi thông tin đến làm tắc hệ thống. Dĩ nhiên, thông báo này làm cho tắc nghẽn tăng thêm tạm thời.

Một cách thông báo tắc nghẽn khác là: Người ta dành riêng một bit hoặc một trường trong gói tin để trong trường hợp có tắc nghẽn, router có thể bật bit hoặc trường này lên và gởi nó đến mọi ngõ ra nhằm thông báo cho các láng giềng của nó biết.

Hoặc cũng có thể dùng cách phản hồi sau: Cho các host hoặc router thường xuyên gởi các gói tin thăm dò ra ngoài để hỏi thẳng về tình hình tắc nghẽn. Thông tin này có thể được sử dụng để

chuyến hướng vạch đường vòng qua khu vực bị tắc nghẽn. Ví dụ thực tế: Một số đài phát thanh thường phái một số máy bay trực thăng bay vòng quanh thành phố để báo cáo lại những trục đường bị tắc, từ đó thông báo đến thính giả giúp họ chuyển hướng lái xe tránh những điểm nóng.

Sự hiện diện của tắc nghẽn đồng nghĩa với việc: tài nguyên của hệ thống không đủ để tải gánh nặng thông tin truyền qua. Vì thế ta nghĩ ra hai giải pháp: tăng tài nguyên hoặc giảm tải. Ví dụ, một mạng con có thể bắt đầu sử dụng các đường điện thoại quay số để tạm thời tăng băng thông giữa một số điểm nào đó. Trong các hệ thống vệ tinh, việc tăng công suất truyền đồng nghĩa với việc cung cấp băng thông lớn hơn. Chia tách lưu lượng thông tin cho chúng chạy trên nhiều đường đi khác nhau cũng có thể giúp tăng băng thông. Cuối cùng, các router dự phòng (thường để dự phòng tình huống các router chính bị sự cố) có thể được mang ra chạy trực tuyến để tăng dung lượng truyền tải của hệ thống khi tắc nghẽn nghiêm trọng xảy ra.

Tuy nhiên, đôi khi ta không thể tăng tài nguyên của hệ thống lên nữa, hoặc tài nguyên đã tăng tối đa. Cách thức duy nhất để chống lại tắc nghẽn là giảm tải. Có nhiều cách giảm tải, ví dụ: từ chối phục vụ một số người dùng, giảm cấp dịch vụ đối với vài hoặc tất cả người dùng, và buộc người dùng cung cấp lịch trình phát ra yêu cầu của họ.

Các biện pháp phòng ngừa tắc nghẽn

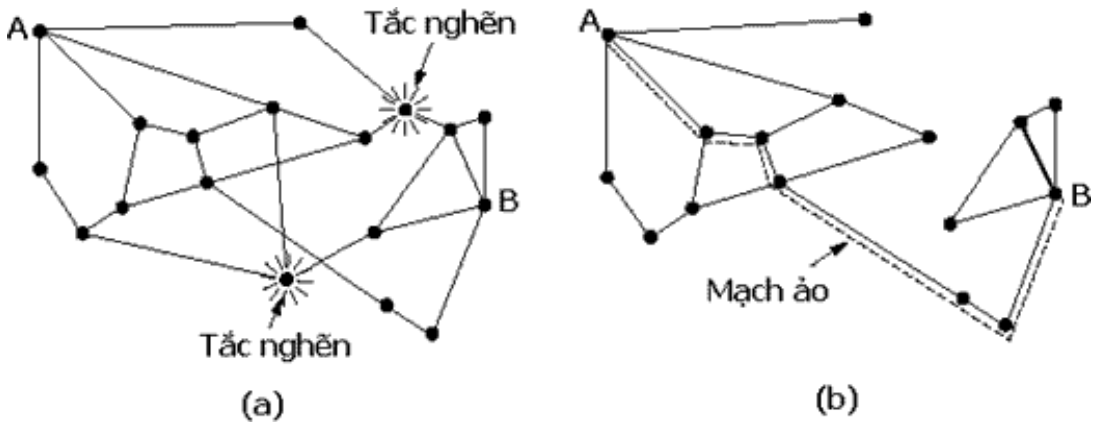
Tại tầng mạng, việc chọn sử dụng mạch ảo hay datagram sẽ tác động đến tắc nghẽn do nhiều giải thuật điều khiển tắc nghẽn chỉ chạy trên mạch ảo. Giải pháp "lập hàng đợi cho các gói tin và phục vụ chúng" liên quan đến việc một router có một hàng đợi cho mỗi ngõ vào, một hàng đợi cho mỗi ngõ ra hay cả hai. Nó cũng liên quan đến trình tự xử lý các gói tin trong hàng đợi (round-robin hay dựa trên sự ưu tiên). Chính sách hủy bỏ gói tin sẽ chỉ ra gói tin nào cần bị hủy bỏ khi không còn không gian chứa. Một chính sách tốt có thể giúp làm giảm tắc nghẽn, ngược lại có thể làm tắc nghẽn trầm trọng thêm.

Một giải thuật vạch đường tốt có thể giúp tránh được tắc nghẽn bằng cách trải đều giao thông trên tất cả đường nối, trong khi một giải thuật tồi chỉ đơn giản gởi quá nhiều thông tin lên một đường tải đã quá tải rồi. Cuối cùng, việc quản lý thời gian sống của gói tin sẽ phải đưa ra quyết định là một gói tin có thể sống bao lâu trong hàng đợi trước khi bị hủy bỏ. Thời gian sống quá dài sẽ làm trì trệ công việc rất lâu. Nhưng nếu thời gian sống quá ngắn, các gói tin thỉnh thoảng sẽ bị mãn kỳ (timed-out) trước khi chúng đến được đích, vì thế dẫn đến việc tái truyền.

Điều khiển tắc nghẽn trong các mạng con dạng mạch ảo

Một giải pháp đơn giản là điều khiển cấp phép (admission control). Ý tưởng như sau: một khi có cảnh báo về tắc nghẽn, hệ thống sẽ không thiết lập thêm mạch ảo nào nữa đến khi sự cố qua đi. Vì thế, trong lúc tắc nghẽn xảy ra, những cố gắng thiết lập mạch ảo đều thất bại. Lý do: cho phép nhiều người vào đấy sẽ làm cho vấn đề trở nên trầm trọng hơn.

Cách tiếp cận khác là cho phép tạo ra các mạch ảo mới nhưng cẩn trọng vạch đường cho các mạch ảo mới này đi vòng qua khu vực bị vấn đề tắc nghẽn. Ví dụ, xem xét mạng con như trong hình H6.20, trong đó hai router bị tắc nghẽn.



(a) Một mạng con bị tắc nghẽn.
(b) Mạng con được vẽ lại sau khi loại trừ các điểm gây tắc nghẽn

Giả sử một host được nối với router A muốn thiết lập nối kết tới một host của router B. Thường thì nối kết này sẽ chạy qua một trong hai nút bị tắc nghẽn. Để tránh chuyện này, chúng ta vẽ lại mạng con như trong hình (b), bỏ qua các router bị tắc nghẽn cùng với các đường nối của chúng. Đường chấm chỉ ra một đường đi có thể tránh được tắc nghẽn.

Một chiến lược khác liên quan đến mạch ảo là: host và mạng con thỏa thuận với nhau về việc thiết lập mạch ảo. Thỏa thuận này thường bao gồm dung lượng và đường đi của thông tin, chất lượng dịch vụ được yêu cầu và các thông số khác. Để đảm bảo thực hiện được thỏa thuận, mạng con sẽ dành riêng tài nguyên trên suốt con đường mạch ảo đi qua. Các tài nguyên này bao gồm không gian bảng vạch đường và buffer trên các router, cùng với băng thông trên các đường nối. Trong tình huống này, tắc nghẽn hầu như không xảy ra trên một mạch ảo mới bởi vì tất cả tài nguyên cần thiết đã được đảm bảo sẵn dùng.

Kiểu dành riêng tài nguyên này có thể được thực hiện toàn thời gian như là một phương thức hoạt động chuẩn, hoặc chỉ được thực hiện khi tắc nghẽn xảy ra. Nếu được thực hiện toàn thời gian sẽ có hạn chế là lãng phí tài nguyên. Nếu đường truyền 6 Mbps được tận hiến cho 6 mạch ảo, mỗi mạch ảo tiêu tốn 1 Mbps, thì đường truyền này luôn được đánh dấu là đầy, cho dù hiếm có khi nào 6 mạch ảo con của nó truyền hết công suất tại cùng thời điểm.

Điều khiển tắc nghẽn trong mạng con dạng Datagram

Trong mạng dạng Datagram, mỗi router có thể dễ dàng kiểm soát hiệu năng của các đường ra và các tài nguyên khác. Ví dụ, nó có thể gán cho mỗi đường nối một biến thực *u*, với giá trị từ 0.0 đến 1.0, dùng phản ánh hiệu năng gần đây của đường nối đó. Để duy trì độ chính xác tốt cho *u*, một mẫu hiệu năng tức thời *f* của đường nối sẽ được lấy thường xuyên, và *u* sẽ được cập nhật như sau

$$u_{mới} = a\, n_{cũ} + (1 - a)\, f$$

trong đó hằng số *a* quyết định router quên đi lịch sử gần đây nhanh như thế nào.

Khi *u* vượt qua ngưỡng, đường ra rơi vào trạng thái "cảnh báo". Mỗi gói tin mới tới sẽ được giữ lại và chờ kiểm tra xem đường ra có ở trạng thái cảnh báo không. Nếu có, một số hành động sẽ được thực hiện, và chúng ta sẽ thảo luận ngay sau đây.

Các gói tin chặn (Choke Packets)

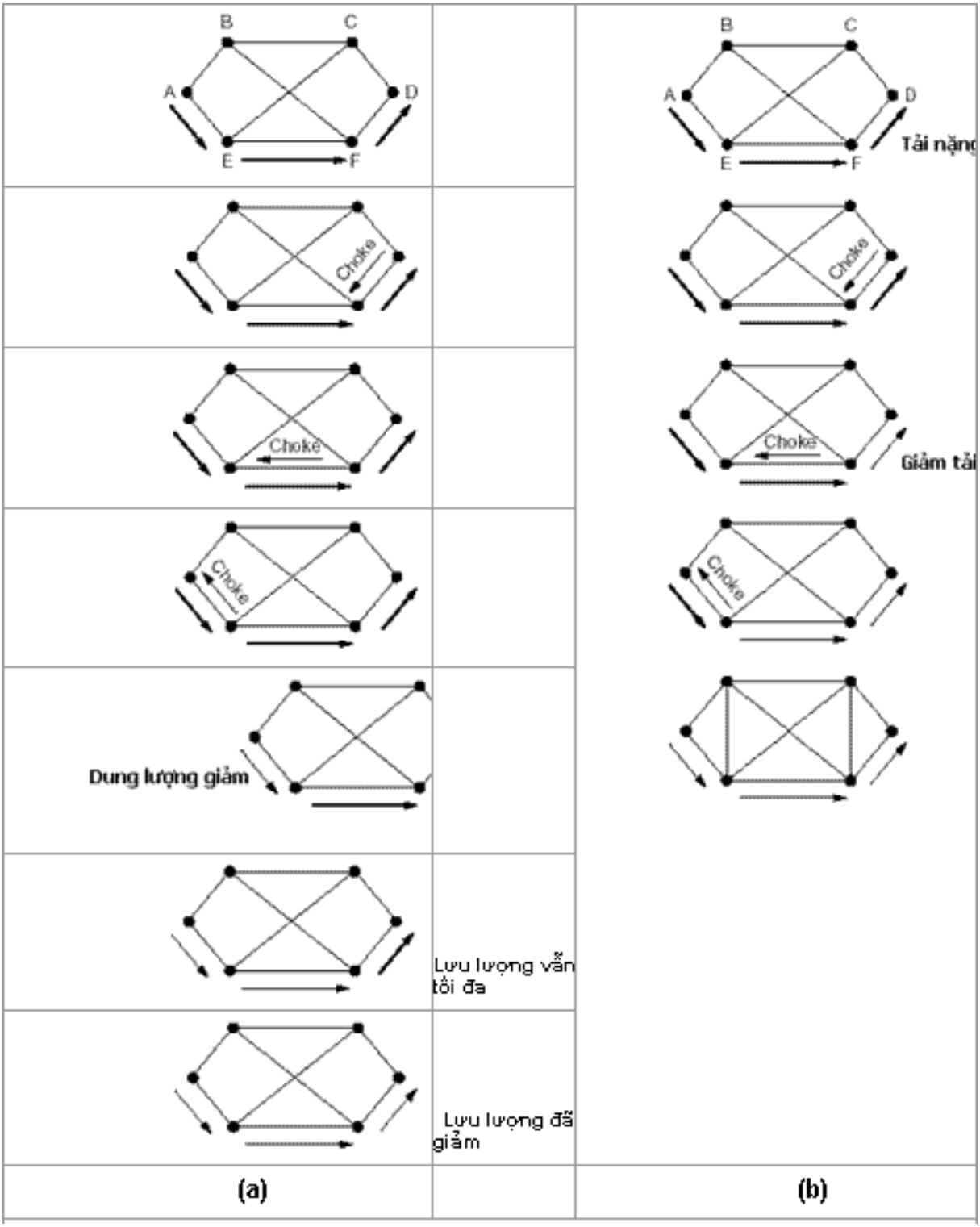
Khi một gói tin đến router và ngõ ra của nó đang ở trong trạng thái báo động, router sẽ gởi một gói tin chặn ngược về nút nguồn đã gởi gói tin đó. Gói tin gặp tắc nghẽn như đã nói sẽ được đánh dấu để nó không làm phát sinh các gói tin chặn khác nữa. Khi gói tin chặn đến được nút nguồn, nút nguồn sẽ giảm lưu lượng thông tin đến điểm bị nghẽn đi X phần trăm. Do có thể còn vài gói tin đang trên đường đi đến đích bị nghẽn, sau này nút nguồn nên bỏ qua các gói tin chặn phát ra tiếp từ đích đó.

Sau giai đoạn trên, nút nguồn bỏ thêm một khoảng thời gian để lắng nghe thêm các gói tin chặn khác. Nếu chúng còn tới, đường nối vẫn bị nghẽn, nút nguồn tiếp tục giảm dung lượng truyền. Nếu không còn gói tin chặn nào chạy ngược về nút nguồn trong thời gian lắng nghe, nó có thể từng bước tăng lưu lượng truyền lên.

Gởi các gói chặn từng bước một (Hop-by-Hop Choke Packets)

Ở tốc độ cao hoặc qua khoảng cách xa, việc gởi gói tin chặn ngược về nút nguồn là không hiệu quả, bởi vì phản ứng của nút nguồn sẽ chậm.

Một cách tiếp cận khác là làm cho gói tin chặn có tác dụng tại mọi nút trung gian mà nó đi qua. Hãy xem hình ví dụ 5.18(b).



(a) Một gói tin chặn chỉ tác động lên nút nguồn. (b) Một gói tin chặn tác động lên mọi nút mà nó đi qua (H6.21)

Ở trong hình 5.18(b), ngay khi gói tin chặn vừa đến F, F liền giảm lưu lượng truyền đến D. Tương tự, khi gói tin chặn đến E, E sẽ giảm lưu lượng truyền đến F. Cuối cùng gói tin chặn đến A và lưu lượng được giảm suốt tuyến đường từ A đến D.

Hiệu quả của sơ đồ chặn từng bước một là có thể giải phóng điểm bị nghẽn nhanh chóng. Tuy nhiên cái giá phải trả là nó tiêu tốn băng thông hướng lên cho gói tin chặn. Nhưng cái lợi cuối cùng là ở chỗ, giải pháp này bóp chết tắc nghẽn ngay trong trứng nước.

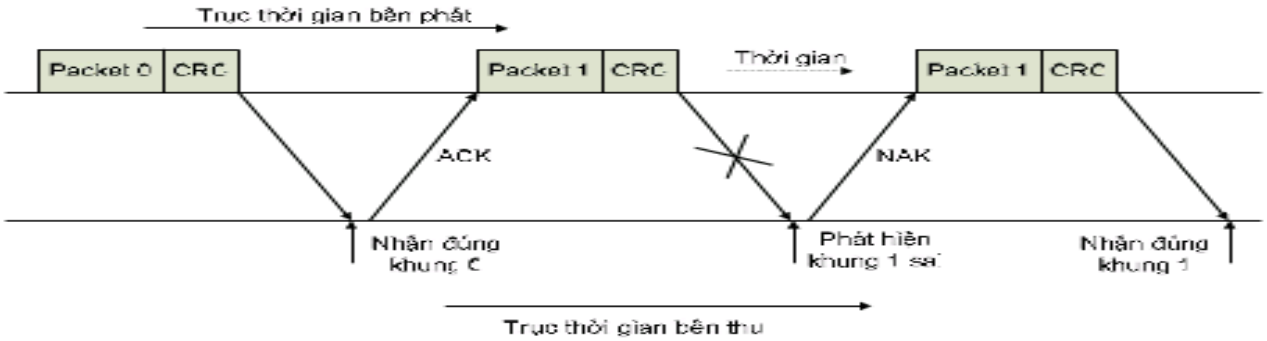
2.2.2. Các giải pháp kiểm soát tắc nghẽn

- Khống chế tắc ghẽn: là ngăn chặn xảy ra không để tắc nghẽn về lưu lượng dữ liệu trên đường truyền (*congestion control*)
- **Flow Control: Stop and Wait**

Điều khiển luồng kết hợp ARQ – Stop-and- wait (dừng và đợi)

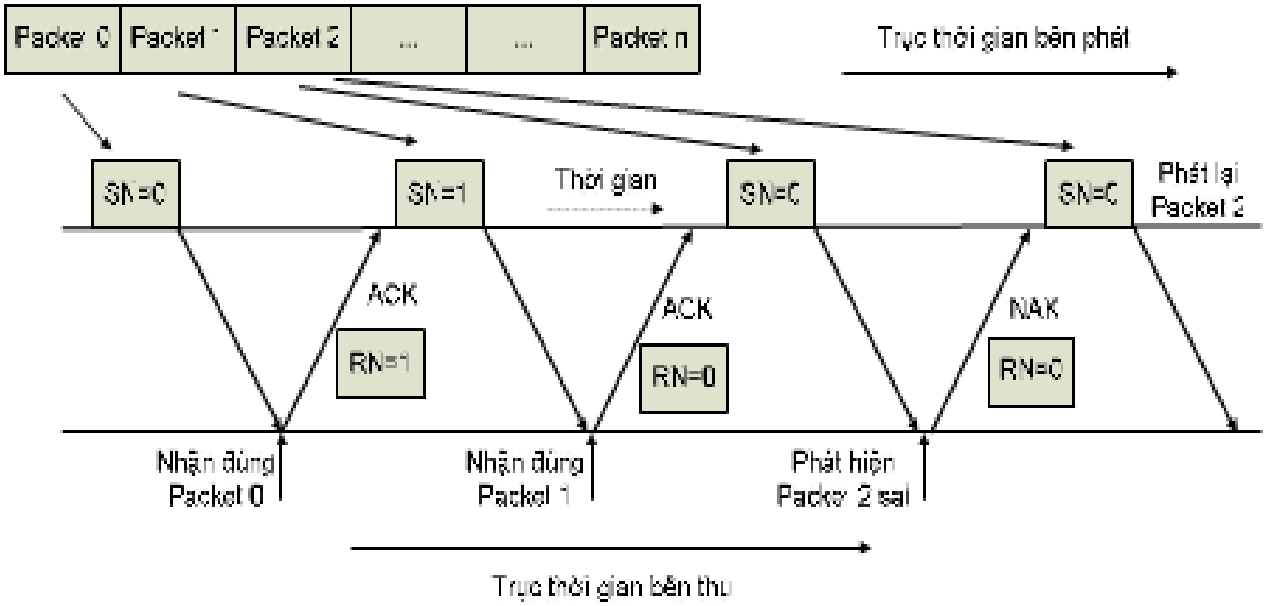
Stop - and -wait là một dạng của điều khiển dòng truyền dừng và đợi đã mở rộng để chứa các chức năng truyền lại dữ liệu trong trường hợp dữ liệu bị mất hoặc bị hư hỏng.

Hình vẽ mô tả nguyên tắc hoạt động cơ bản của cơ chế phát lại dừng và đợi:



Hình 2.1: Phát lại theo cơ chế dừng và đợi

Hình mô tả nguyên tắc hoạt động của cơ chế Stop- and- Wait:



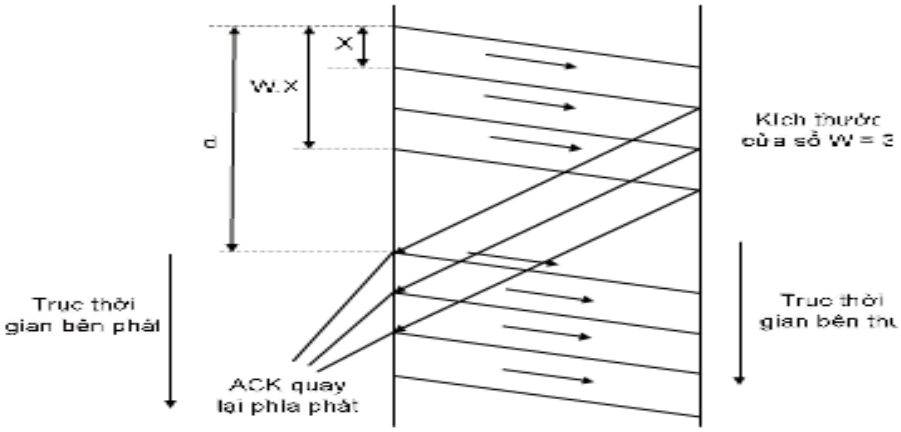
Hình 2.2: Stop-and-Wait ARQ có dùng SN/RN

Flow Control: Window end to end

Định nghĩa

Phương pháp điều khiển luồng theo cửa sổ dựa trên cơ sở phương pháp cửa sổ trượt ARQ làm việc tại lớp liên kết dữ liệu. Các khung thông tin từ phát sang thu và khung báo nhận, báo lỗi truyền từ thu sang phát được đánh số thứ tự để phân biệt, kích thước cửa sổ $W < 2^k$ với k là số bit dùng đánh số phân biệt các khung.

Bài toán 2: Trường hợp d > W.X



Hình 2.7: Ví dụ phía phát truyền tin không liên tục khi W = 3

a. Tắc nghẽn cục bộ

- Backbone (Physical)
- Bridge/ Router
- VLAN (Switch layer 2)
- IP Subnet (Subnet Mask)

b.Tắc nghẽn toàn cục

- Backbone (Physical)
- Others (tối ưu hóa thiết kế mạng, đường truyền,Server…)

2.3. Định tuyến liên mạng

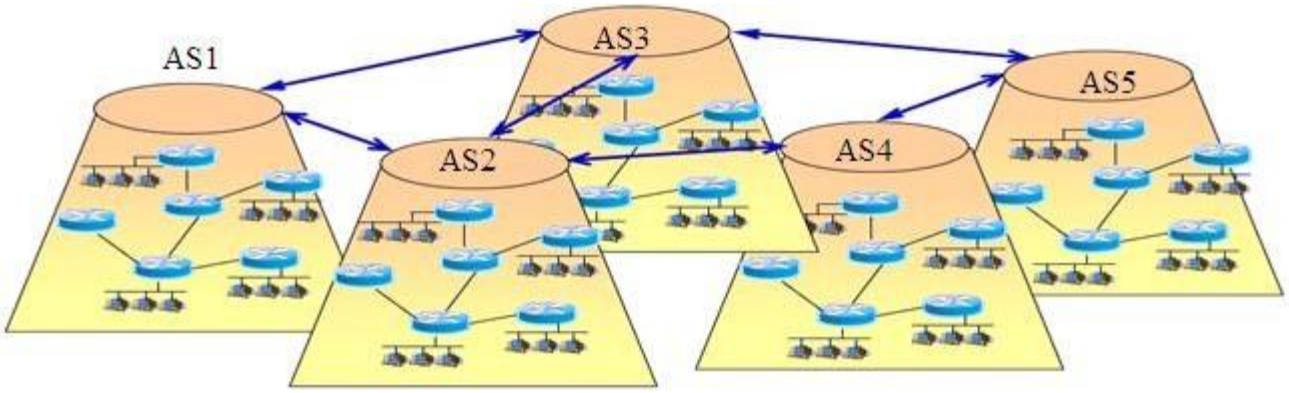
Khái niệm về liên mạng

Phân cấp định tuyến trên Internet (Internet = Mạng của các mạng)

Mỗi mạng có thể lựa chọn riêng cho mình một chiến lược chọn đường riêng.

Mỗi mạng như vậy có thể gọi là một hệ tự trị - Autonomous System (AS)

Mô hình kết nối liên mạng



Mô hình internet kết nối các AS

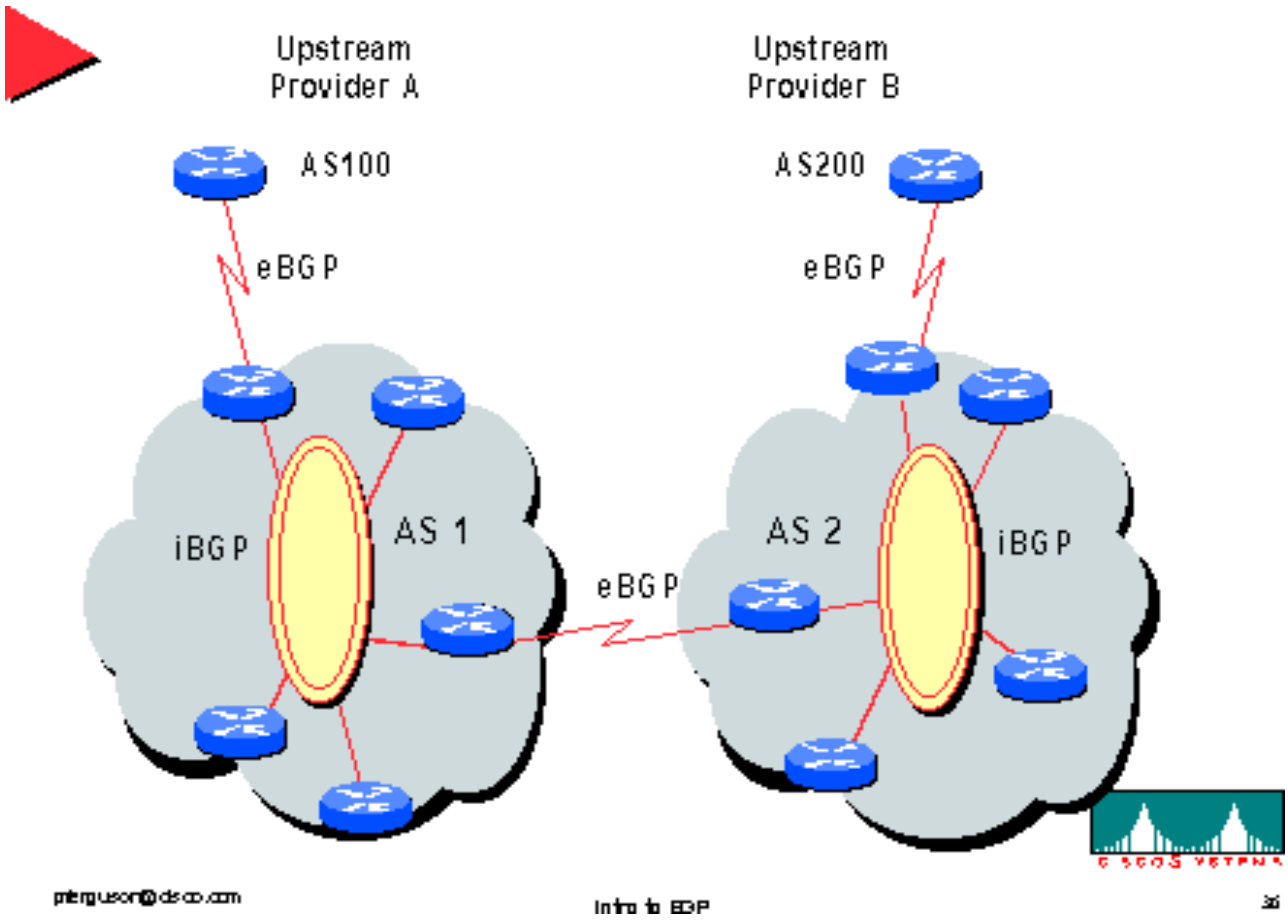
Khái niệm về AS (Autonomous System)

Cơ chế chống loop là một ASN- AS number. Khi một cập nhật về một mạng đi ra khỏi 1 AS, ASN của AS đó được đính kèm vào bản cập nhật. Khi một AS nhận một cập nhật, nó sẽ xem trong AS list. Nếu nhận ra ASN của chính nó, cập nhật sẽ bị loại bỏ.

ASN – Autonomous system number
Gồm 16 bit nằm trong range 1→ 65635 gồm có:

- **Private**: 64512-65535 → chỉ sử dụng trong một AS local và bị remove khi đi qua AS khác. Do IANA cấp. (hiện tại VPNT vẫn đang sử dụng AS private cho 64 tỉnh thành và chỉ có 1 AS kết nối ra bên ngoài, ở VN thì chỉ có 5 sô AS).

Giao thức GBP (iBGP, eBGP)



Đinh tuyến nội (iBGP) , là định tuyến giữa các router trong 1 AS

Định tuyến ngoại (eBGP) là định tuyến kết nối AS (thông qua router)

- iBgp (internal BGP) là BPG chạy trong cùng 1 AS.
- eBGP (external BGP) là BGP chạy giữa các AS.

+ Các kiểu thông điệp BGP: Có 4 kiểu thông điệp

- *Open:* sau khi một láng giềng được cấu hình, BGP gửi một thông điệp open để cố gắng kết nối với láng giềng đó. Bao gồm thông tin như ASN, RIB, và hold time.

- *Update:* thông điệp này được sử dụng để trao đổi thông tin định tuyến giữa các peers. Chứa thông tin về các routes mới, các routes bị down, và các thuộc tính của đường (path attributes).

- *Keepalive:* mặc định, các BGP peers trao đổi thông điệp này sau mỗi 60 giây. Chúng sẽ giữ phiên làm việc giữa các peer được active.

- *Notification:* khi xảy ra 1 vấn đề làm cho Router phải kết thúc phiên làm việc BGP, một thông điệp notification sẽ được gửi đến BGP neighbor và việc kết nối sẽ chấm dứt.

Cập nhập BGP

+ *BGP Database:* BGP dùng 3 loại database, 2 loại dùng riêng cho giao thức, 1 loại dùng cho toàn bộ quá trình routing trên router

- Neighbor database: một danh sách tất cả các BGP láng giềng được cấu hình.

- BGP database, hay còn gọi RIB (Routing Information Base): một danh sách các mạng mà BGP biết, kèm theo là paths (đường đi) và attributes.

Chương 3. GIAO THỨC LIÊN MẠNG

3.1. Tầng mạng trong mô hình OSI và giao thức tầng mạng

3.1.1. Các vấn đề trong thiết kế tầng mạng

+ Router có chức năng tại tầng mạng (Network Layer); vì lý do đó việc thiết kế tầng mạng là việc lắp đặt các router một cách tối ưu sao cho mạng hoạt động hiệu quả nhất

+ Việc lắp đặt thừa router sẽ làm cho mạng phải xử lý tại các nút và có độ trễ (delay)

+ Thêm một router kem theo một chi phí lắp đặt; phải thực hiện cấu hình router

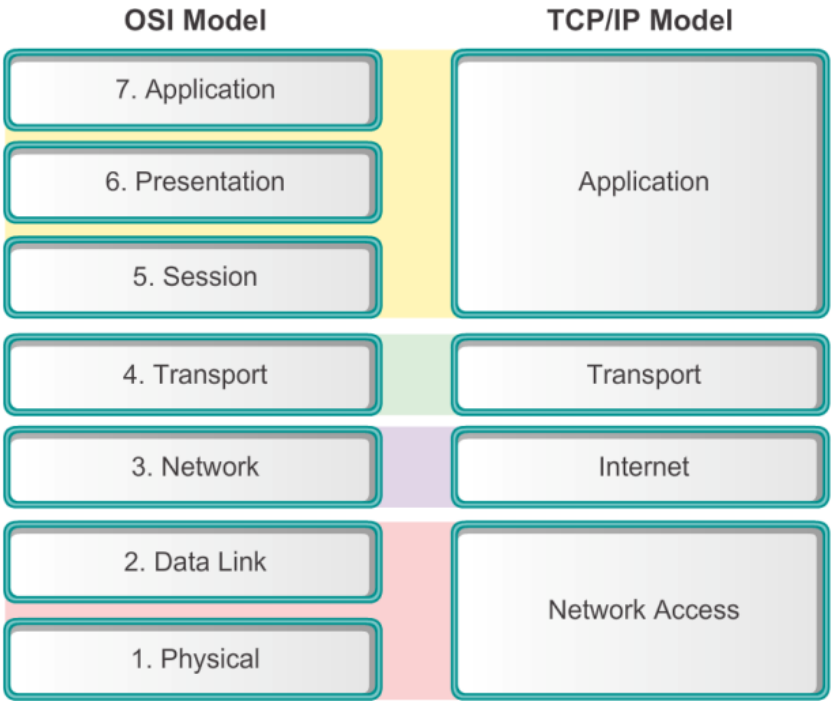
+ Tối thiểu hóa trong lắp đặt router: Việc xử lý gói tin trong liên mạng phải vận hành ổn định trách tắc nghẽn:

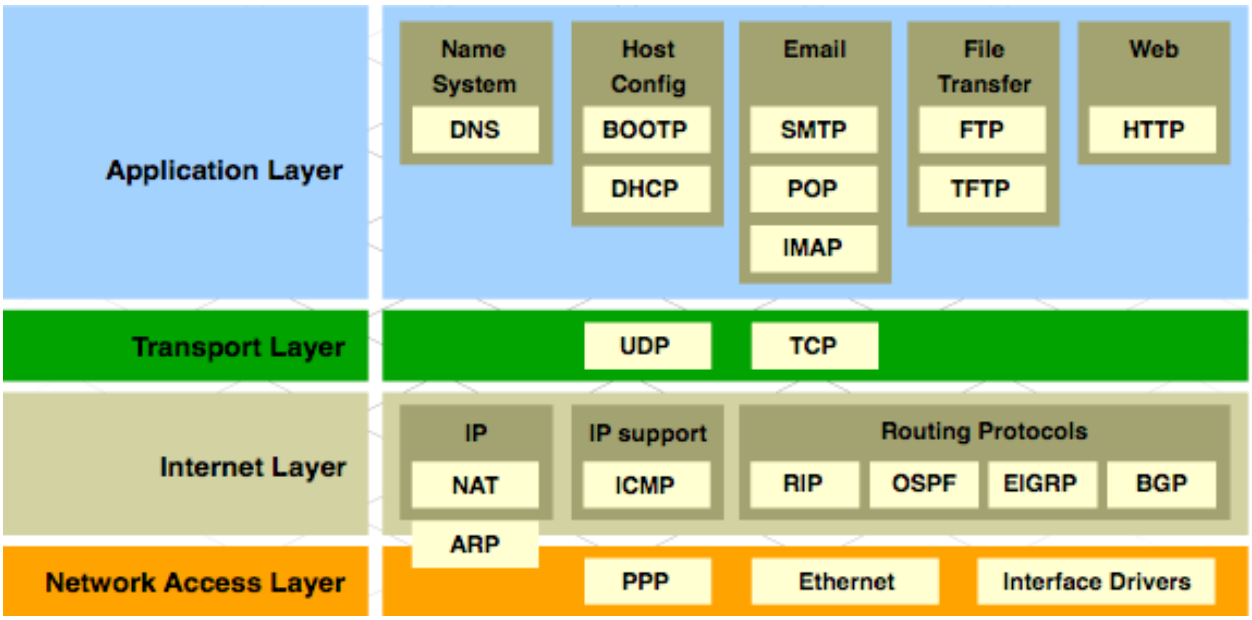
Bao nhiêu router la đủ?

+ căn cứ vào số lượng mạng con vật lý trong liên mạng

+ Căn cứ vào khoảng cách của mỗi mạng

3.1.2. Giao thức tầng mạng (định tuyến và điều khiển)





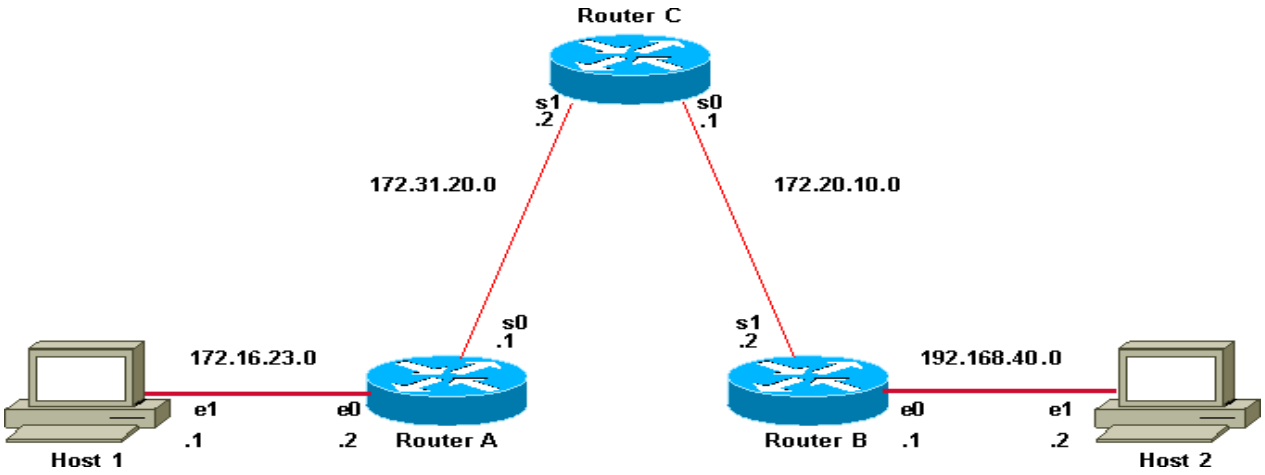
a. Giao thức IP – ICMP

+ ICMP ?? là giao thức điều khiển

- ICMP (Internet Control Message Protocol)
  - là giao thức điều khiển của tầng IP
- Chức năng của ICMP
  - Điều khiển lưu lượng
  - Thông báo lỗi
  - Định hướng lại các tuyến
  - Kiểm tra các trạm ở xa

Router gửi thông điệp ICMP cho một trạm thông báo nên dung router khác (trạm nguồn ở cùng một mạng với 2 thiết bị định tuyến)

Nhóm	Loại bản tin	Kiểu - Type
Thông điệp truy vấn (ICMP Queries)	Hỏi và phúc đáp Echo (Echo request và Echo reply)	8/0
	Hỏi và phúc đáp nhãn thời gian (Timestamp request và Timestamp reply)	13/14
	Yêu cầu và phúc đáp mặt nạ địa chỉ (Address mask request và Address mask reply)	17/18
	Yêu cầu quảng bá bộ định tuyến (Router soliciation và router advertisement)	10/9
Thông điệp báo lỗi (ICMP Error reports)	Khổng thể tới đích (Destination Unreachable)	3
	Yêu cầu ngừng hoặc giảm tốc độ phát (Source quench)	4
	Định hướng lại (Redirection)	5
	Vượt ngưỡng thời gian (Time Exceeded)	11



- ❖ Tìm hiểu lệnh Ping (một ứng dụng của ICMP)
  - Khi Host 1 ping tới Host 2 tức là host 1 gửi một loạt các gói tin ICMP echo request.
  - Host 2 nhận được lập tức gửi lại các gói tin trả lời ICMP echo reply
- ❖ Tìm hiểu lệnh Ping (một ứng dụng của ICMP)
  - Khi Host 1 ping tới Host 2 tức là host 1 gửi một loạt các gói tin ICMP echo request.
  - Host 2 nhận được lập tức gửi lại các gói tin trả lời ICMP echo reply
- ❖ Các thông số

Ping thành công

- Bytes: kích thước gói tin
- Time: thời gian hồi đáp
- TTL: thời gian sống, cứ đi qua 1 router giá trị giảm đi 1

Ping không thành công

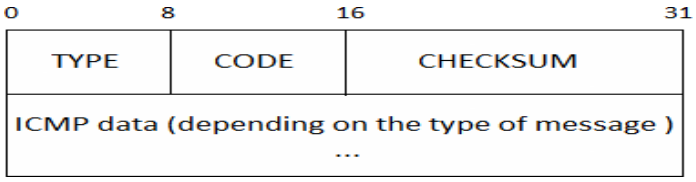
- Request time out: hết thời gian mà không thấy gói tin trở về
- Destination host unreachable:

Hoạt động ICMP

Chuyển phát thông điệp bằng IP Datagram

- Không hề có thêm độ tin cậy và ưu tiên
- ICMP không tạo ra thông báo lỗi về thông báo lỗi khác
- ICMP không phải là giao thức cấp cao hơn IP, mà là phần bắt buộc của IP

Khuôn dạng thông điệp ICMP



- TYPE (8 bit): mang kiểu thông điệp ICMP
- CODE (8 bit): them thông tin về thông điệp
- CHECK SUM (16 bit): ICMP sử dụng thuật giải checksum như IP nhưng Checksum ICMP chỉ tính đến thông điệp ICMP
- ICMP data: header và 64 bit dữ liệu đầu của datagram gây nên lỗi
- **Một số kiểu (TYPE) của ICMP:**

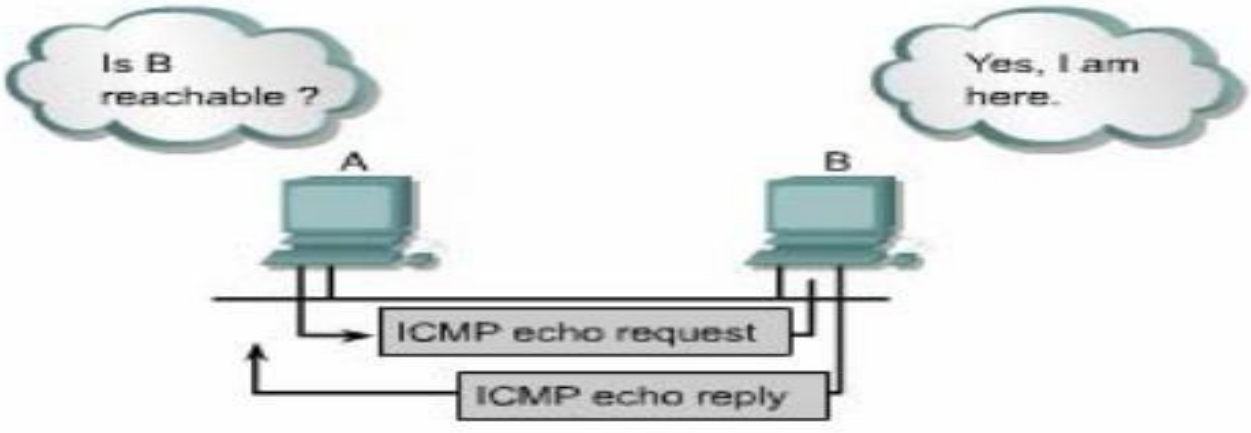
✓ *0: Echo Reply*
✓ *3: Destination Unreachable*
✓ *4: Source Quench*
✓ *5: Redirect*
✓ *6: Alternate Host Address*

- ✓ *8: Echo Request*
- ✓ *9: Router Advertisement*
- ✓ *10: Router Selection*
- ✓ *11: Time Exceeded*
- ✓ *12: Parameter Problem*
- ✓ *13: Timestamp*
- ✓ *14: Timestamp Reply*
- ✓ *15: Information Request*
- ✓ *16: Information Reply*
- ✓ *17. Address Mask Request*
- ✓ *18. Address Mask Reply*

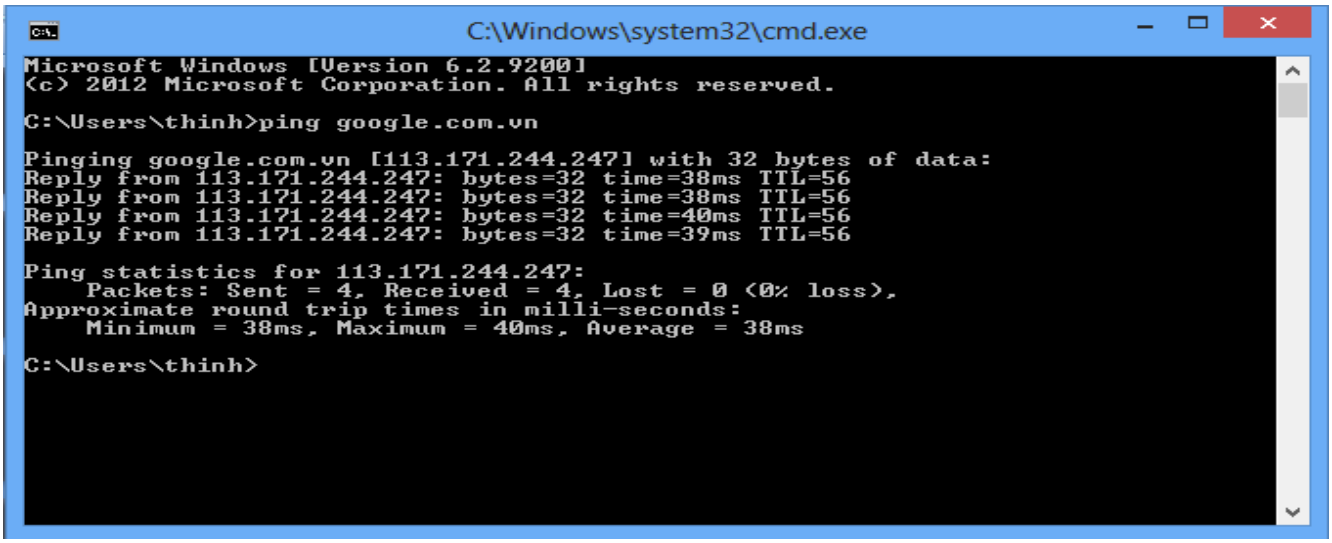
Các thông điệp quan trọng ICMP quan trọng

- ✓ Thông điệp ICMP kiểm tra khả năng đến đích (Ping ICMP)
- ✓ Thông điệp ICMP báo lỗi các đích không đến được
- ✓ Thông điệp ICMP làm nguội nguồn phát (Source Quench)
- ✓ Thông điệp ICMP yêu cầu thay đổi định tuyến từ bộ định tuyến
- ✓ Thông điệp ICMP nhận biết vòng kín hoặc định tuyến quá dài
- ✓ Thông điệp ICMP báo lỗi có vấn đề tham số của Datagram
- ✓ Thông điệp ICMP đồng bộ đồng hồ và ước lượng thời gian
- ✓ Thông điệp ICMP tìm mặt nạ mạng con
- ✓ Thông điệp ICMP tìm ra bộ định tuyến
- ✓ Thông điệp ICMP yêu cầu bộ định tuyến cấp thông tin tức thì

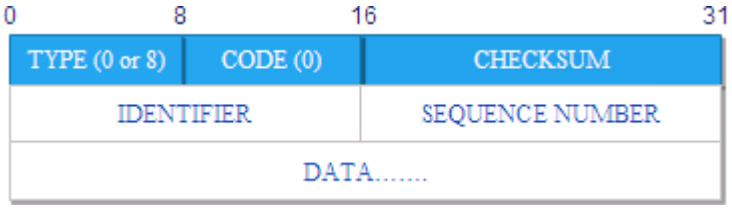
Thông điệp ICMP kiểm tra khả năng đến đích (Ping ICMP)



Chứng minh được những phần chính của hệ thống làm việc tốt nêu như máy nguồn nhận được đúng thông điệp "echo reply".

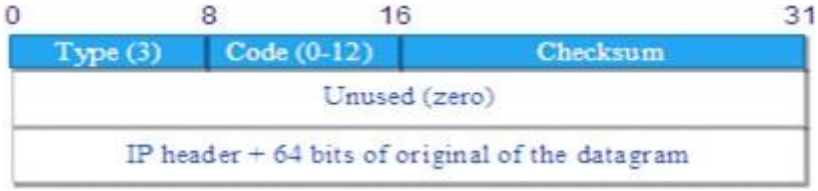


Trên nhiều hệ thống, lệnh thực hiện việc gửi thông điệp ICMP "echo request" có tên là PING

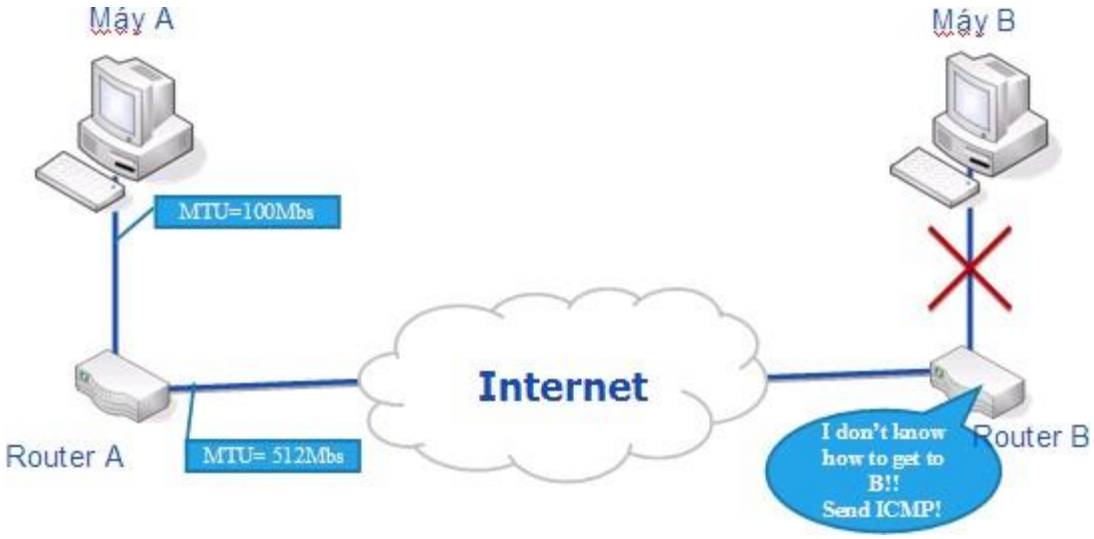


IDENTIFIER và SEQUENCE NUMBER được sử dụng để máy gửi so sánh giữa lời yêu cầu và lời đáp

Thông điệp ICMP báo lỗi các đích không đến được.

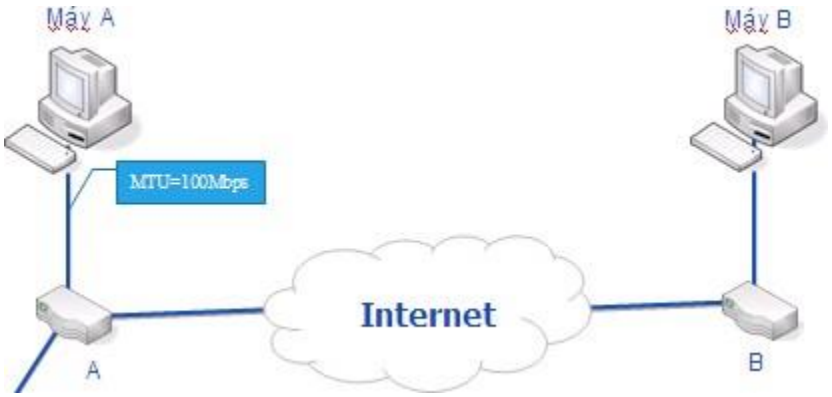


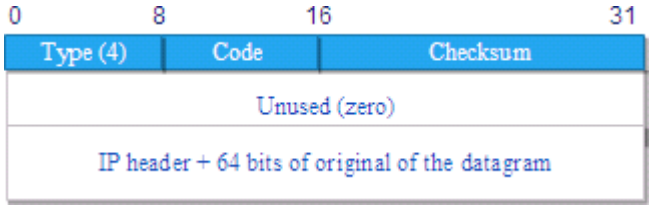
Khi bộ định tuyến không thể truyền hay chuyển phát datagram, nó gửi thông báo "đích không thể đến được" ngược trở về nguồn, thông qua định dạng Data Option như sau:



Thông điệp ICMP làm nguội nguồn phát (Source Quench)

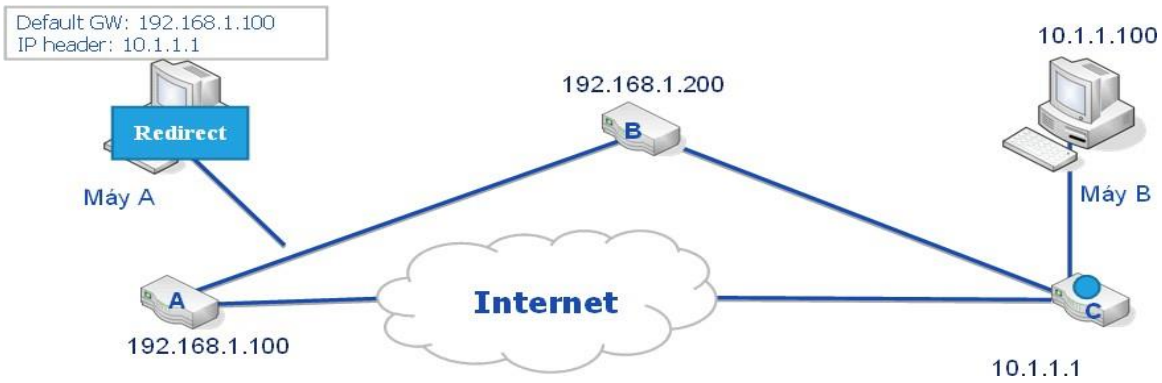
- Khi datagram đến quá nhanh mà máy tính hoặc bộ định tuyến không xử lý kịp.
- Bộ định tuyến sẽ gửi thông điệp ICMP "source quench" yêu cầu nguồn giảm cường độ truyền datagram.
- Không có thông điệp ngược lại.





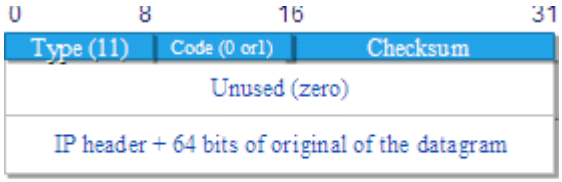
Các thông điệp "Source quench" có một vùng để chứa tiền tố của Datagram.

Thông điệp ICMP yêu cầu thay đổi định tuyến từ bộ định tuyến



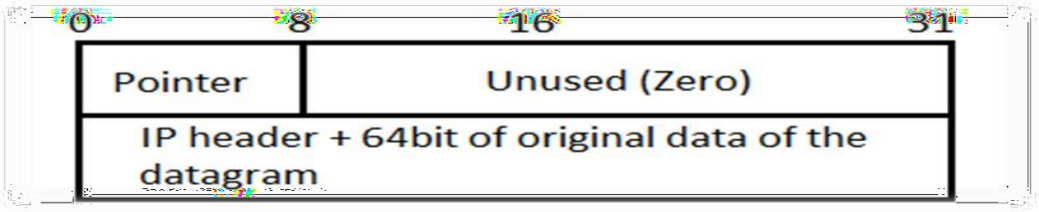
Thông điệp ICMP nhận biết vòng kín hoặc định tuyến quá dài

- Khi bộ định tuyến hủy bỏ một datagram vì TTL của nó về 0 hoặc vì hết thời gian đợi fragment của một datagram, nó sẽ gửi thông điệp ICMP *"quá thời hạn"* (time exceeded) ngược về nguồn của datagram đó.
- Data Option:



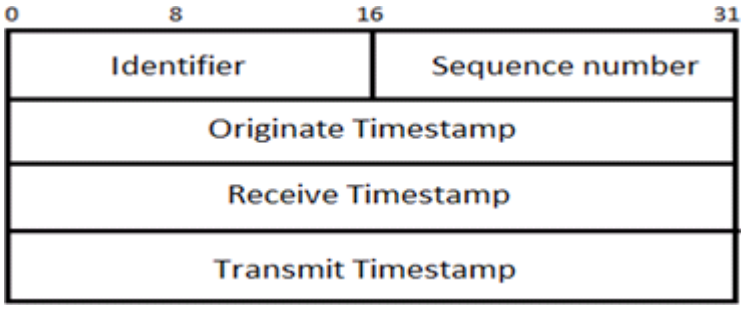
Code = 0: Bộ đếm thời gian sống bằng zero
Code = 1: Quá thời gian đợi kết hợp các fragment

Thông điệp ICMP báo lỗi có vấn đề tham số



- Thông điệp "*Parameter Problem"* được sử dụng khi bộ định tuyến nhận thấy có vấn đề với header của datagram.
- Phần Data Option được định dạng và chỉ được gửi khi có vấn đề quá nghiêm trọng
- Sử dụng vùng POINTER để xác định byte trong datagram đã gây ra lỗi.

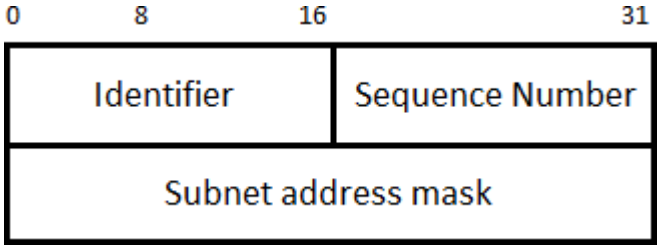
Thông điệp đồng bộ đồng hồ và ước lượng thời gian



- Type: Xác định yêu cầu (13) hay trả lời (14)
- Code: Nhận giá trị 0.
- Identifier và Sequence number: được dung bởi máy nguồn
- Originate timestamp: thời gian do máy ban đầu điền
- Receive timestamp: được điền ngay khi nhận được yêu cầu
- Transmit Timestamp: điền ngay khi lời đáp chuyển đi

Thông điệp ICMP tìm mặt nạ mạng con

- Để tham gia vào một mạng con, một máy tính cần biết mặt nạ mạng con.
- ICMP cung cấp khả năng gửi yêu cầu trực tiếp từ một máy tính



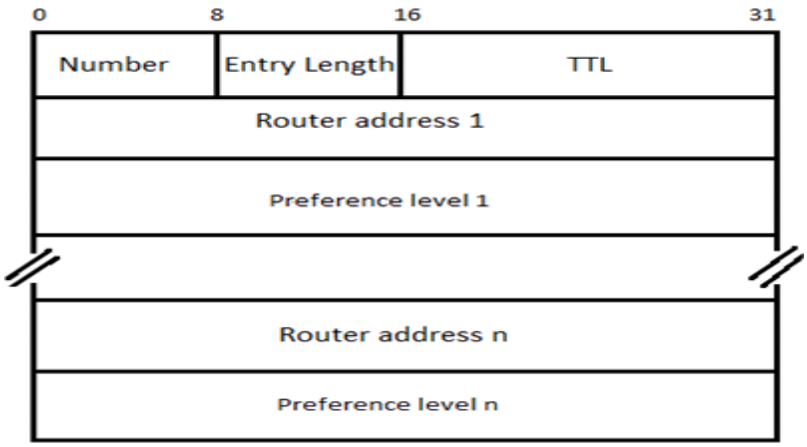
- TYPE: thông điệp là yêu cầu(17) hay (18)
- SUBNET ADDRESS MASK: mặt nạ mạng con của lời đáp
- IDENTIFIER & SEQUENCE NUMBER: cho phép máy phối hợp với lời đáp với yêu cầu

Thông điệp ICMP tìm ra bộ định tuyến

Cung cấp hai cơ chế khắc phục nhược điểm của BOOTRAP và DHCP để cho phép một máy tính tìm ra một địa chỉ một bộ định tuyến

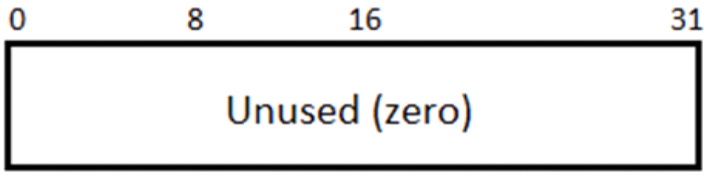
Lấy thông tin trực tiếp từ chính bộ định tuyến

Sử dụng kỹ thuật trạng thái mềm với bộ đếm thời gian.



- Number: Số lượng các địa chỉ để sử dụng
- Entry length: Kích thước của một vùng
- TTL: Thời gian được sử dụng địa chỉ quảng bá
- Router address & Preference level: tương ứng một con đường

Thông điệp ICMP yêu cầu bộ định tuyến cấp thông tin tức thì



- Khi máy mới khởi động sẽ gửi thông điệp "khẩn khoản bộ định tuyến" yêu cầu router cấp thông tin.
- Router đáp lại bằng thông điệp "router advertisement"
- Máy tính có thể gửi "lời khẩn khoản" tới tất cả các địa chỉ multicast hoặc tới địa chỉ quảng bá

IPv6 –ICMPv6

Internet Control Message Protocol version 6 (ICMPv6) là phiên bản được biến đổi và nâng cấp của Internet Control Message Protocol (ICMP) cho giao thức liên mạng thế hệ 6 (IPv6). ICMPv6 được định nghĩa trong RFC 4443. ICMPv6 là một phần gắn liền với IPv6 và thực hiện

thông báo lỗi mạng và chức năng chẩn đoán (ví dụ, ping), và có một khuôn khổ cho các phần mở rộng để thực hiện những thay đổi trong tương lai.

Một số phần mở rộng đã được công bố, xác định các loại thông điệp ICMPv6 mới cũng như tùy chọn mới với nhiều loại thông điệp có ở ICMPv6. Giao thức Neighbor Discovery (NDP) là một giao thức phát hiện các nút trong IPv6 thay thế và mở rộng các chức năng của ARP.[2]Secure Neighbor Discovery (SEND) là một phần mở rộng của NDP thêm những chức năng an ninh. Multicast Listener Discovery (MLD) được sử dụng bởi các bộ định tuyến IPv6 để khám phá multicast listener trên một đường kết nối trực tiếp, giống như Internet Group Management Protocol (IGMP) được sử dụng trong IPv4. Multicast Router Discovery (ĐBSCL) cho phép phát hiện các multicast router.

Cũng như ICMP, các thông điệp ICMPv6 được chia ra làm hai loại: *thông điệp lỗi* và *thông điệp thông tin*. Các thông điệp ICMPv6 được các gói IPv6 chuyên chở trong đó giá trị của Next Header cho ICMPv6 là 58.

Gói tin ICMPv6

Gói tin ICMPv6

Bit offset	0–7	8–15	16–31
0	Type	Code	Checksum
32	Thông điệp		

Gói tin ICMPv6 bao gồm phần header và phần thông điệp. ICMPv6 header bao gồm ba trường: Type (8 bít), Code (8 bít) và Checksum (16 bít).

- *type* xác định loại thông điệp. Giá trị từ 0 tới 127 (bít đầu tiên là 0) chỉ thông điệp lỗi, từ 128 tới 255 (bít đầu tiên là 1) thông điệp thông tin.
- *code* phân dạng sâu hơn gói tin ICMPv6, định rõ đây là gói tin dạng gì trong từng loại thông điệp ICMPv6.
- *checksum* cung cấp giá trị sử dụng để kiểm tra lỗi cho toàn bộ gói tin ICMPv6.

b. Giao thưc định tuyến:

RIP, OSPF, EIGRP, BGP, IS_IS

IS-IS là 1 giao thức thường được dùng trong các ISP vì nó có nhiều tính năng nổi trội. Có thể nói IS-IS là 1 giao thức khá phức tạp nên khi các bạn đọc IS-IS hãy bình tĩnh.
Sau đây sẽ là loạt bài về IS-IS

1. Lịch sử IS IS

- Được phát triển vào thập niên 80 bởi công ty DEC và được công nhận bởi tổ chức ISO
- IS-IS (**Intermediate System to Intermediate System**) là một *giao thức định*

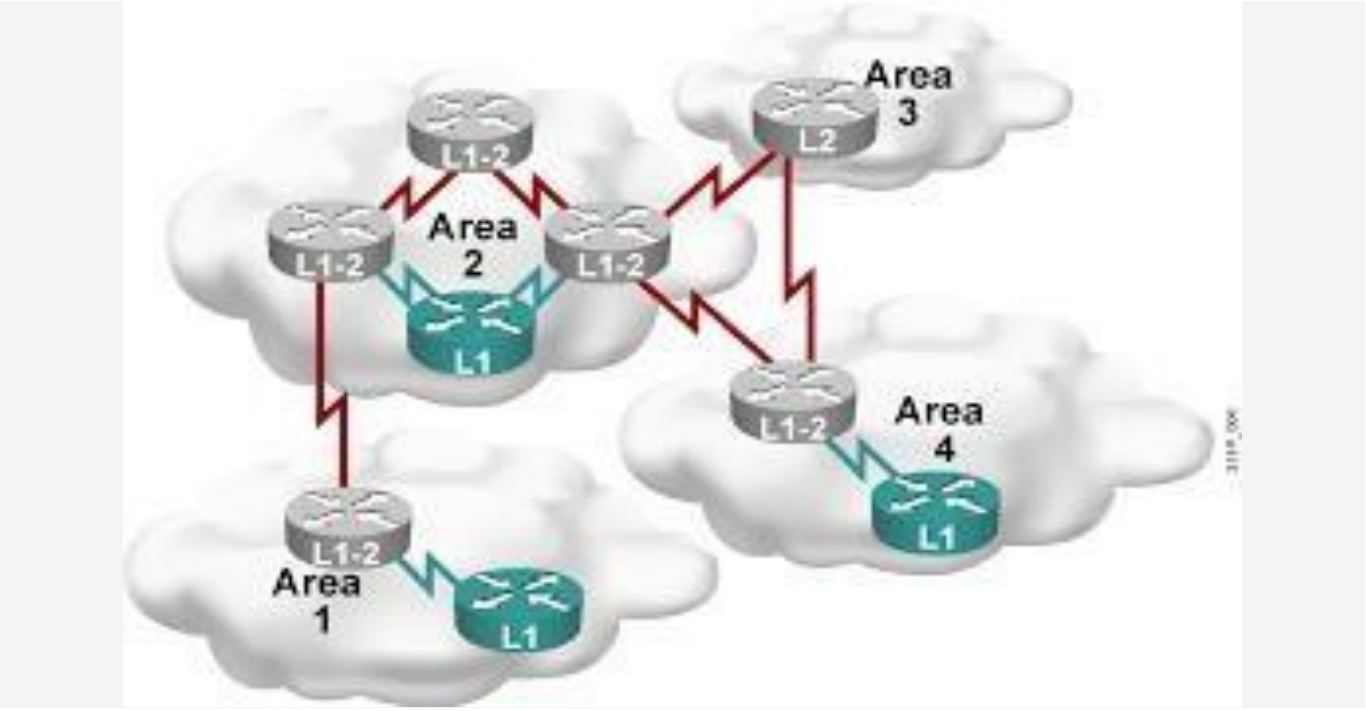
tuyến IGP.
- IS-IS được xem là *giao thức định tuyến cho mô hình OSI*
- Việc tạo ra IS-IS là một phần trong sự nỗ lực tạo ra một giao thức chuẩn quốc tế có thể cạnh tranh với TCP/IP. IS-IS được phát triển để đáp ứng:

- Một giao thức không mang tính độc quyền.
- Hỗ trợ dải địa chỉ rộng và phân cấp
- Một giao thức hiệu quả, cho phép hội tụ nhanh, chuẩn xác và ít gây quá tải mạng.

- Tuy nhiên, sau này internet được xây dựng trên nền TCP/IP đã chiếm ưu thế nên IS-IS đã thay đổi để hỗ trợ IP với tên gọi *Integrated IS-IS* (IS-IS tích hợp)
- Những năm gần đây, IS-IS vươn lên như một giao thức định tuyến cho IPv6 hay sử dụng với MPLS. Thêm vào đó là các ưu điểm của IS-IS cũng được nhắc tới
như: *IS-IS là một giao thức độc lập, mở rộng tốt, và có khả năng xác lập định tuyến theo ToS* (Type of Service - Kiểu dịch vụ)

2. Tính năng
- Là giao thức Link state
- Hỗ trợ VLSM
- Sử dụng thuật toán Dijkstra's SPF
- Hội tụ nhanh
- Sử dụng gói tin *Hello để thiết lập Adjacencies* và *LSP để trao đổi thông tin bảng định tuyến* (link-state information)
- Hiệu quả trong việc sử dụng Bandwidth, RAM, CPU
- Hỗ trợ 2 mức định tuyến

- **Level 1**: Xây dựng topology chung của các *system ID trong cùng 1 area* với đường đi tốt nhất
- **Level 2**: Trao đổi thông tin *giữa các Area*. Xác định traffic đến 1 area với đường đi tốt nhất



3. Intergrated IS-IS

- Trong mô hình OSI

- **Router** được coi như một IS **(Intermediate System** - Hệ thống trung gian)
- **PC** được coi như một ES (**End System** - Hệ thống đầu cuối).

=>IS-IS là giao thức định tuyến Router tới Router.

- **CLNP** (Connectionless Network Protocol)**:** Lớp Network trong mô hình OSI được gọi là CLNP và được sử dụng cho CLNS
- **CLNS** (Connectionless Network Service)**:** IS-IS là 1 giao thức hoạt động trên OSI, nó sử dụng CLNS như 1 Router-ID để nhóm các Router vào các Area. Thực tế CLNS chỉ có ý nghĩa tượng trưng

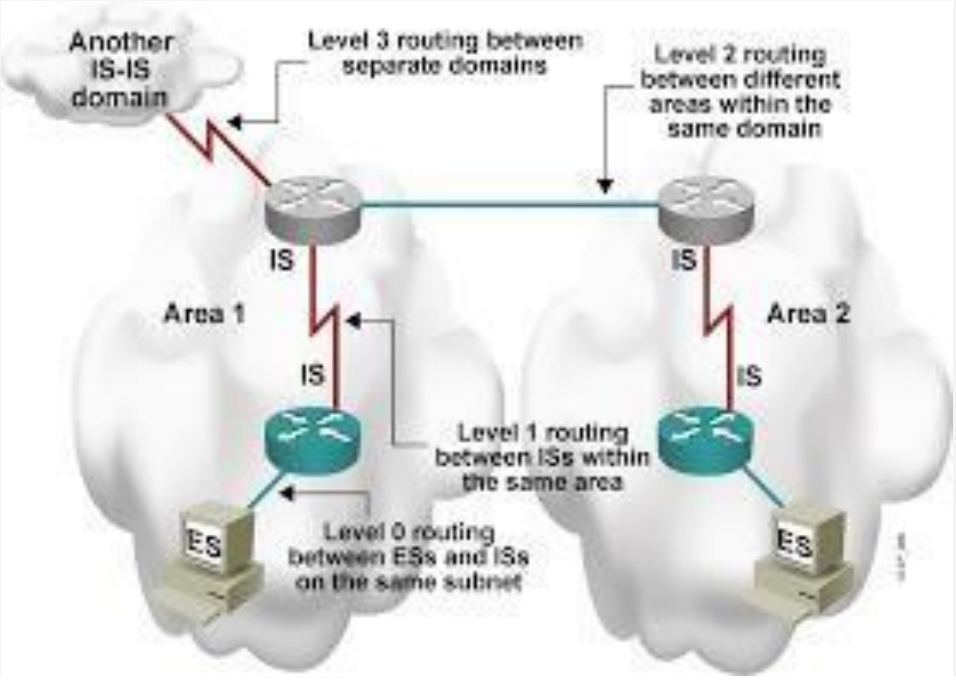
3. Routing level:

- Hỗ trợ 4 mức level routing

- **level 0**: dùng giao tiếp End system tới Intermediate System (ES –IS: router với máy)

- **Level 1**: dùng để trao đổi thông tin trong một Area. Sử dụng LSP level 1 tương tự như LSA 1&2 trong OSPF (internal area)
- **Level 2**: dùng để trao đổi thông tin backbone giữa các Area. Sử dụng LSP level 2 tương tự như LSA 3,4,5 trong OSPF (other area)
- **Level 3**: được sử dụng giữa Autonomous System (AS) và khu vực Interdomain Routing Protocol (IDRP). => Giữa các IS-IS domain

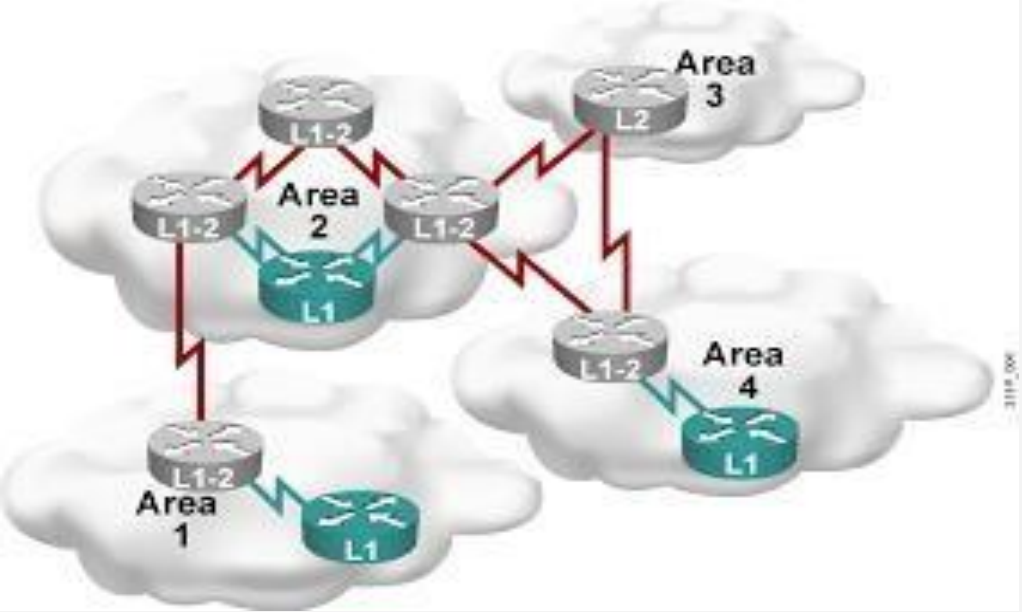
- Nhưng *cisco chỉ hỗ trợ 2 level routing: level 1 và level 2*.



4. Router Level:

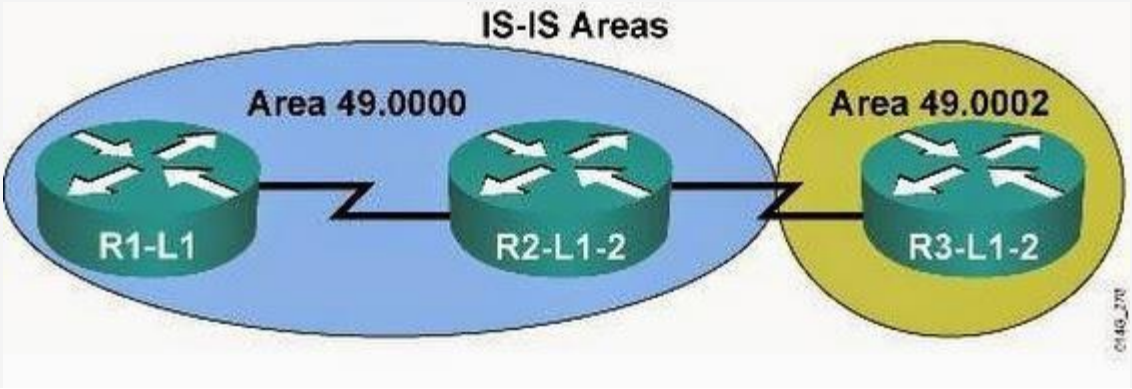
- *Router có thể ở trong level 1, level 2 hoặc trong cả hai*

- **Router level 1:** sử dụng LSP để xây dựng topology cho khu vực nó thuộc về, area local
- **Router Level 2:** sử dụng LSP để xây dựng topology giữa các area khác nhau (tương đương router backbone trong OSPF)
- **Router level 1-2** làm chức năng của cả 2 con trên. (tương đương ABR trên OSPF)



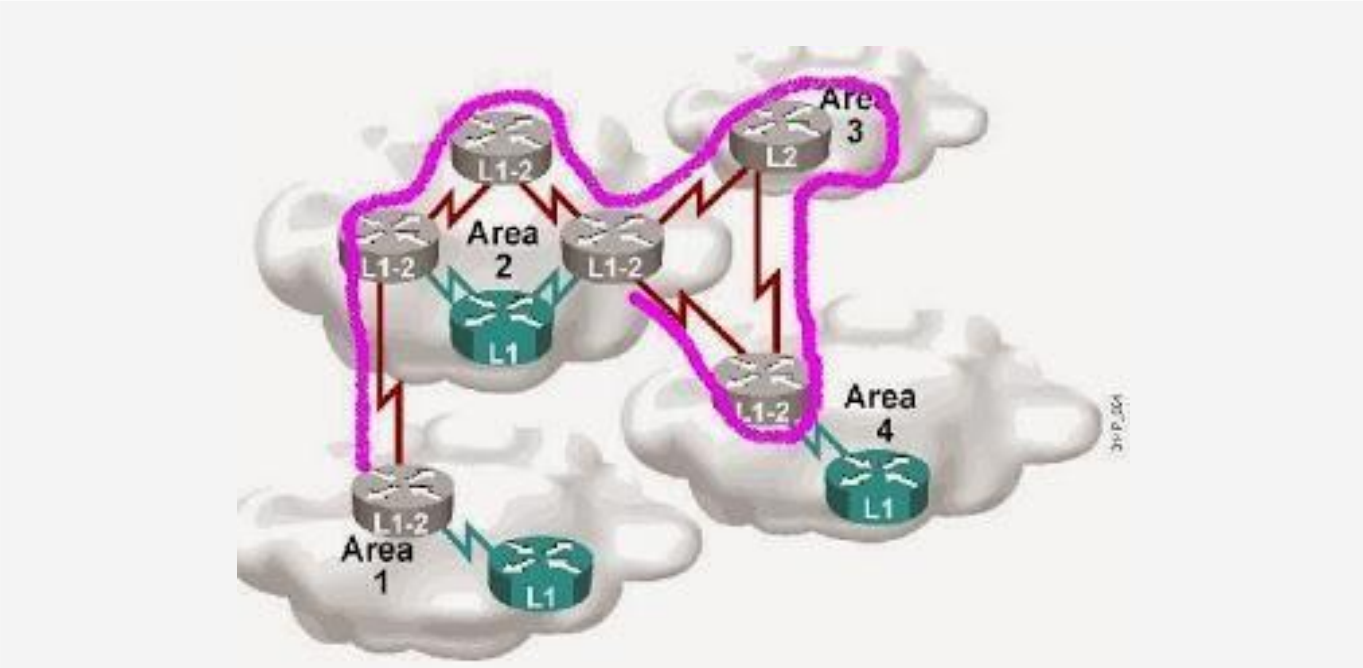
5. Area

- *Trong IS-IS mỗi Router chỉ thuộc 1 area* (khác với OSPF)
- IS-IS thì flexible (linh hoạt) hơn khi mở rộng backbone



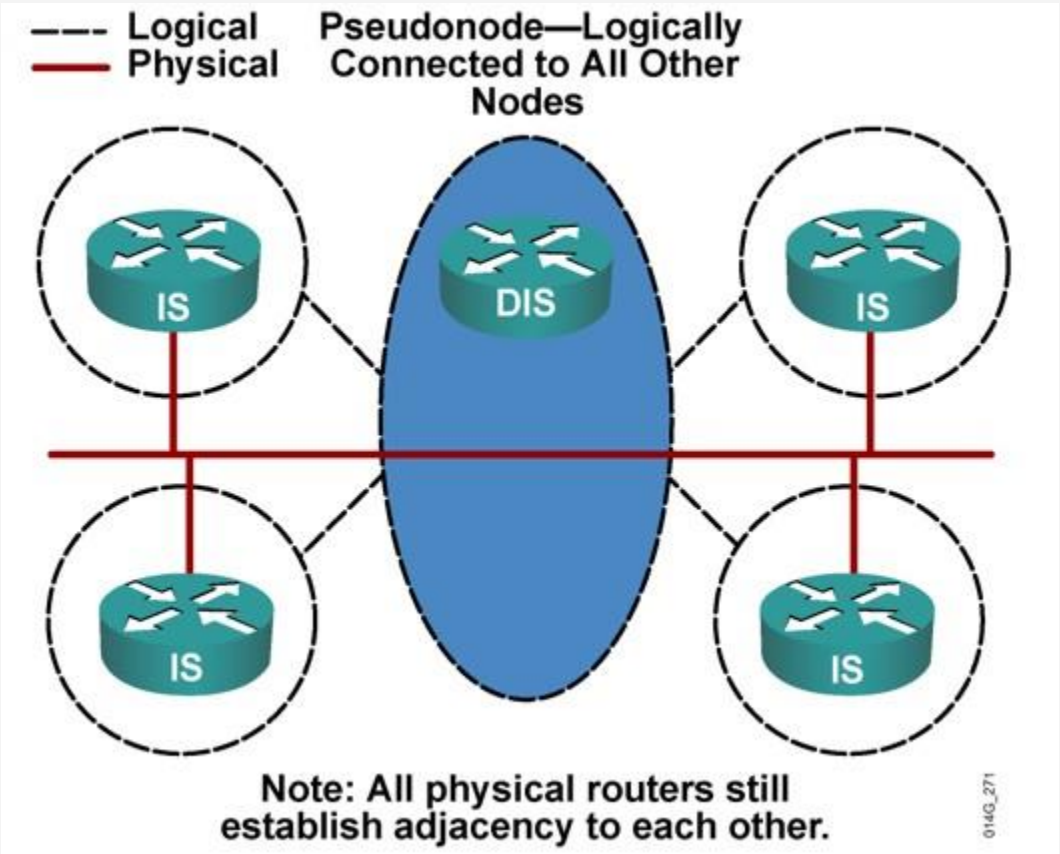
- OSPF thì mỗi link thuộc 1 area nhưng Router thì có thể thuộc nhiều area

- Đường màu hồng là backbone, tất cả router nằm trên đường màu hồng sẽ có thể thấy nhau.



6. DIS

- Giống như một DR trong OSPF, ở IS-IS một DIS được dùng để mô phỏng các kết nối point to point đi qua môi trường multi-point. Do vậy một DIS đôi khi còn được gọi là một pseudonode (nút ảo).



- Mặc dù có nhiều điểm giống nhau, nhưng DIS vẫn có nhiều điểm hơi khác so với OSPF:

- DIS nằm cả ở level 1 và level 2, và *không có một DIS dự phòng*.
- Trong IS-IS cho phép một Router mới khi có priority cao hơn DIS sẽ *được phép cướp quyền* và trở thành DIS mới.
- Trong OSPF, số lượng adjacency ít vì mỗi Router chỉ thiết lập mối quan hệ Adjacency với DR và BDR, còn trong IS-IS, mỗi Router đều thiết lập Adjacency với mọi Router khác trên đường dây.
- *Các gói tin LSP chỉ được gửi bởi DIS* với vai trò của một psenudonode.

- Bầu chọn DIS dựa trên các tiêu chí

- Priority của interface nào cao nhất
- SNPA (MAC) lớn nhất

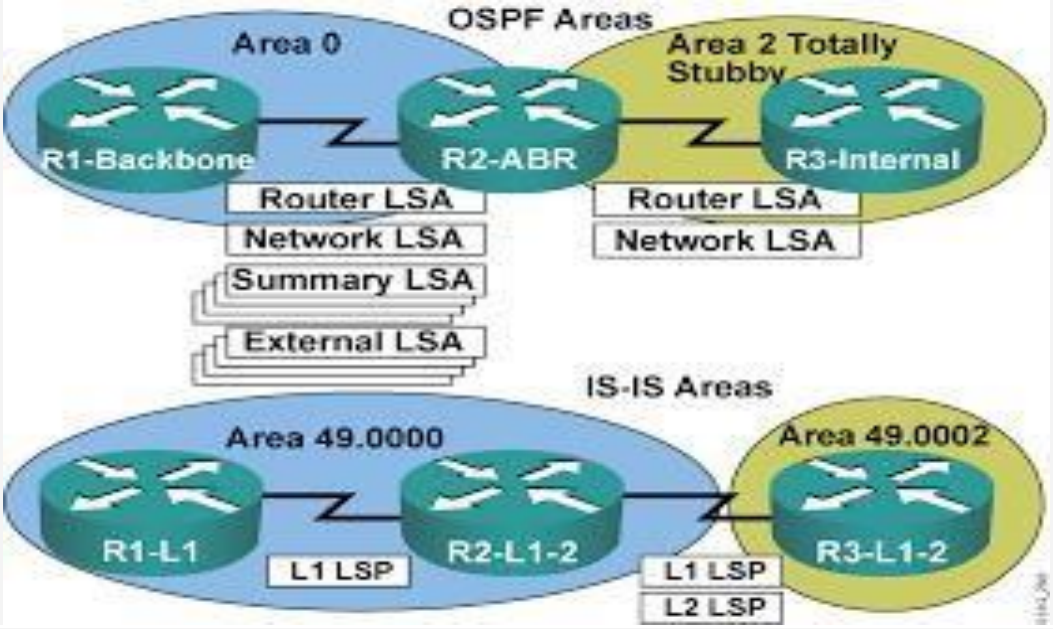
7. intergrated (or dual) IS-IS

- Ban đầu IS-IS thì chỉ dành cho có CLNS protocol (chỉ dành cho chuẩn OSI).
- Nhưng vì sau này IP phổ biến hơn nên IS-IS hỗ trợ luôn ip nên nó được gọi chính xác là intergrated IS-IS.

=> *IS-IS tạo ra 2 bảng: 1 cho IP và một cho CLNS*.

- Khi đẩy gói đi nó sẽ tra vào bảng routing IP tương ứng với con router nào.
- Sau đó nó sẽ tra bảng CLNS address để tìm ra chính xác vị trí con router định tuyến IS-IS.

- Tất cả thông tin *IP thực chất sẽ được bọc trong PDU (CLNS protocol)* để chuyển gói đi chứ không send trong ip packet.
- Mỗi router chạy IS-IS chỉ có duy nhất một address CLNP (CLNP address đại diên cho một router, chứ không đại diện cho từng interface).



Kết luận: Từ bài viết trên chúng ta có thể rút ra 1 vài điểm tương đồng và khác nhau giữa OSPF và IS-IS

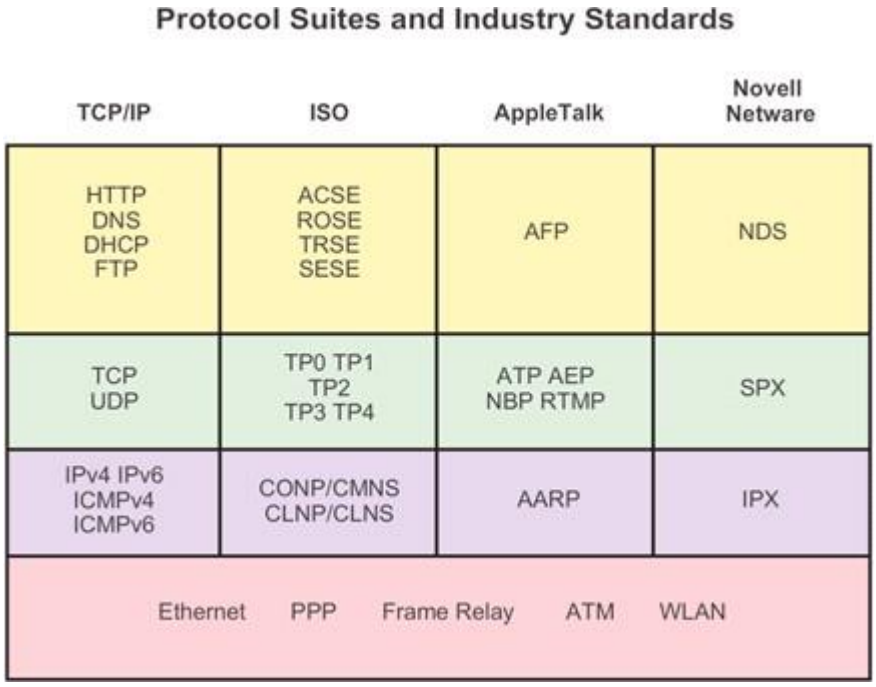
- Giống nhau giữa IS-IS và OSPF

- **Link-state representation, aging timers, and LSDB synchronization**
- **SPF algorithms**
- **Update, decision, and flooding processes**
- **VLSM support**

- Chỉ khác là aging timers của OSPF thì đếm lên từng giây tại thời điểm nó vừa nhận LSA. Còn IS-IS thì đếm ngược từ khi nó nhận LSP.

Tham khảo chương 5.

c. Một số giao thức tầng mạng phát triển bởi ISO, Apple, Novell



+ Novell:

IPX/ SPX

Bộ giao thức IPX/SPX (Internetwork Packet eXchange/Sequence Packet eXchange) là bộ giao thức chủ yếu của Novell trên mạng Novell Netware. Bộ giao thức giúp cho các máy tính có thể giao tiếp và truyền thông với nhau trên mạng.

Bộ giao thức IPX/SPX (Internetwork Packet eXchange/Sequence Packet eXchange) là bộ giao thức chủ yếu của Novell trên mạng Novell Netware. Bộ giao thức giúp cho các máy có thể giao tiếp và truyền thông với nhau trên mạng. Với những bài toán truyền thông lớn, thường giao thức rất phức tạp. Để đơn giản, bài toán truyền thông lớn được chia thành các phần nhỏ và người ta thiết kế giao thuwccs trên từng phần. Tất cả các giao thức trên từng tầng tạo nên một bộ giao thức. Tương tự như TCP/IP, giao thức IPX và SPX hợp lại tạo thành bộ giao thức IPX/SPX với sự hỗ trợ của các giao thức : SAP (Service Advertising Protocol), NCP (Netware Core Protocol), RIP, NLSP (Netware Link Service Protocol)).

IPX là giao thức hoạt động trên tầng mạng, chịu trách nhiệm về địa chỉ và định tuyến dựa trên sự hỗ trợ của các giao thức định tuyến, để nhận được thông báo về điểm đến của gói tin.

SPX hoạt động trên tầng giao vận và kết nối theo định hướng, điều này làm cho SPX đáng tin cậy hơn.

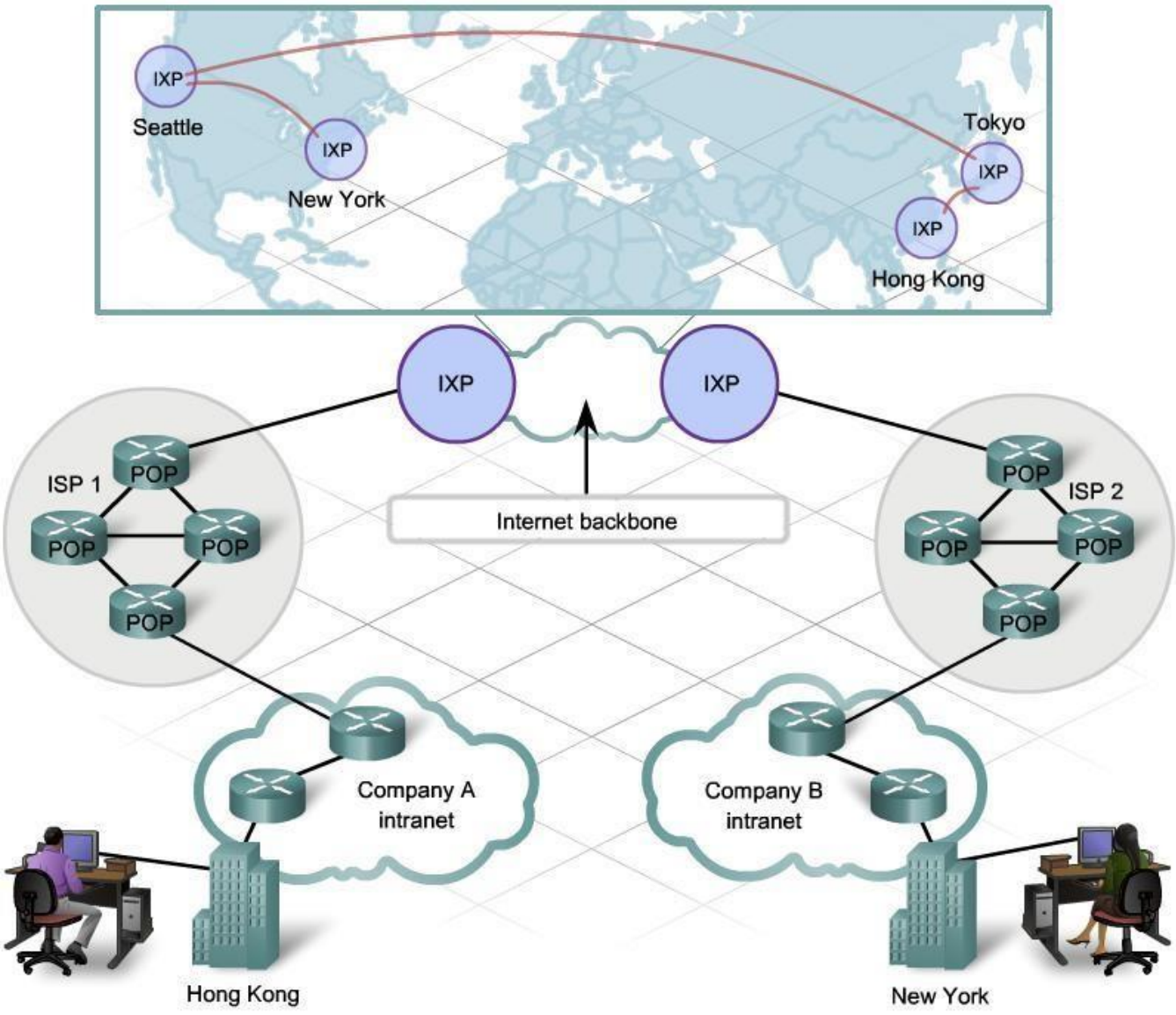
IPX đưa các gói tin đến dích chủa nó, và SPX tập trung vào việc làm sao cho các gói tin đến đích đầy đủ và trong tình trạng tốt. SPX xử lý trình tự và số lượng các gói tin truyền, đảm bảo giao hàng bằng cách kiểm tra các dữ liệu nhận được.

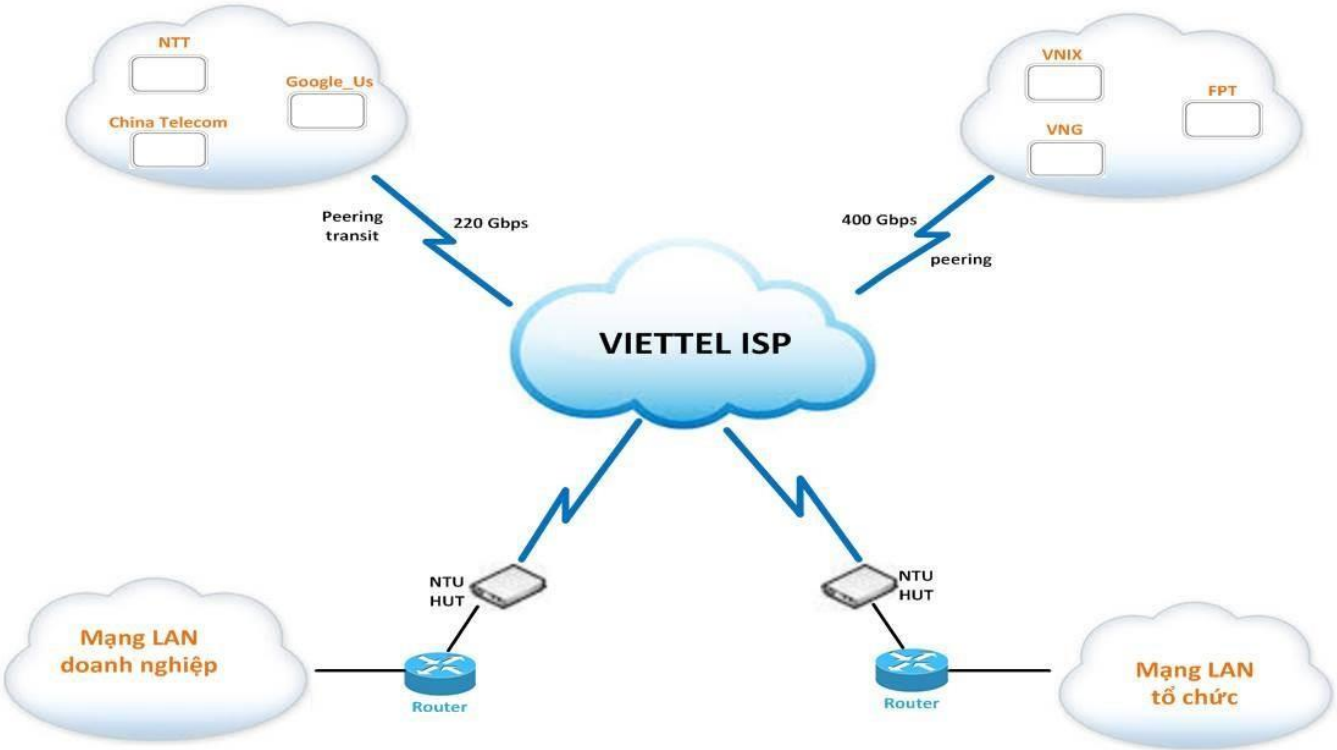
Tham khao thêm ;
+ ISO (CONP/CMNS và CLNP/CLNS) ;

+ AppleTalk: AARP Appletalk Address Resolution Protocol

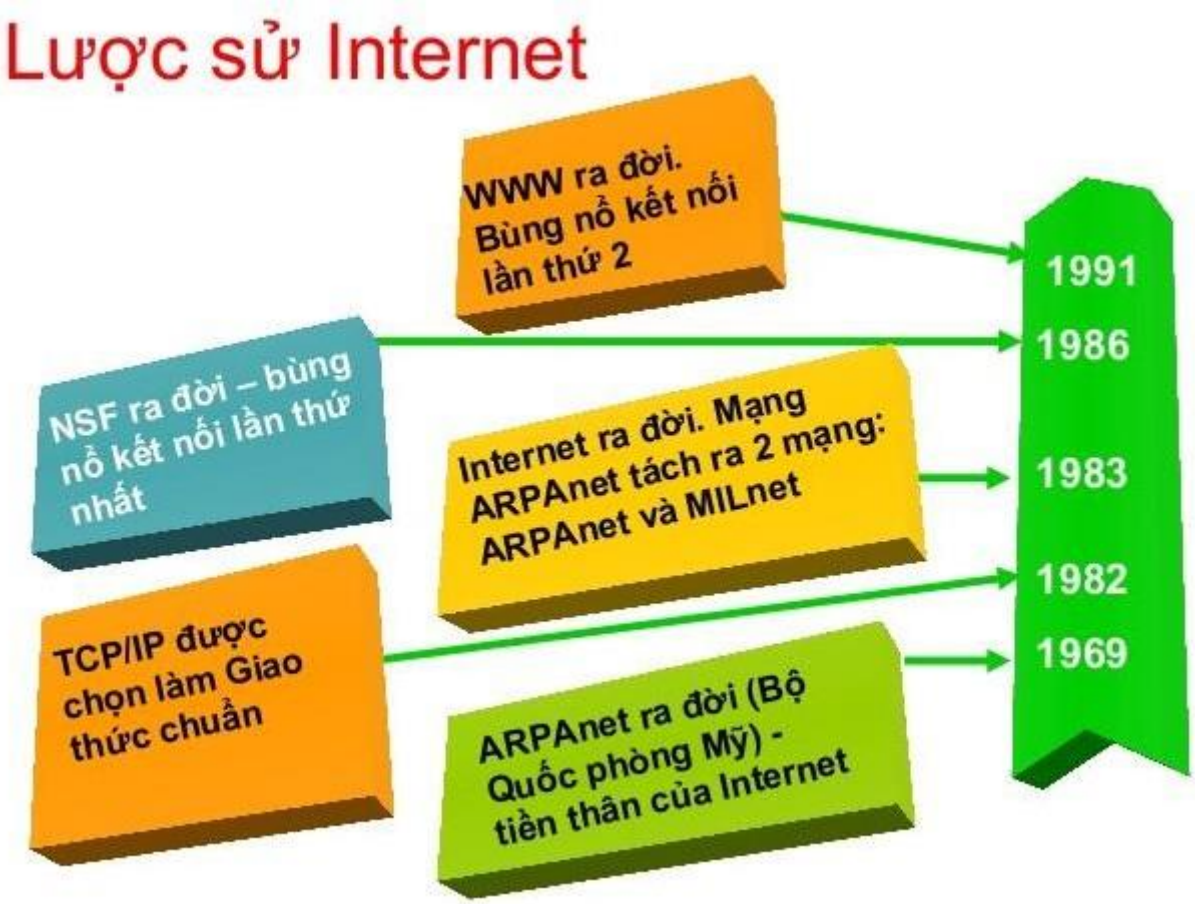
3.2. Mạng Internet và họ giao thức TCP/IP

3.2.1. Mạng Internet và mô hình kiến trúc mạng Internet





Lịch sử ra đời Internet:



Mạng Internet ra đời vào khoảng năm 1974, tiền thân của nó là mạng ARPANET. Cơ quan quản lý dự án nghiên cứu phát triển mạng ARPA thuộc bộ quốc phòng Mỹ liên kế 4 địa điểm đầu tiên vào tháng 7/1969 là Viện nghiên cứu Stanford, Đại học California, Los Angeles, Đại học Utah và Đại học California, Santa Barbara. Đó chính là mạng liên khu vực (Wide Area Network – WAN) đầu tiên được xây dựng.

Đến năm 1983, tất cả máy tính nối với ARPANET phải sử dụng giao thức TCP/IP, giao thức này cũng được coi như một chuẩn mực đối với ngành quân sự Mỹ.

Một năm sau đó, mạng ARPANET được chính thức chia làm 2 phần: một phần được sử dụng cho việc nghiên cứu khoa học và phát triển, một phần được sử dụng cho mục đích quân sự.

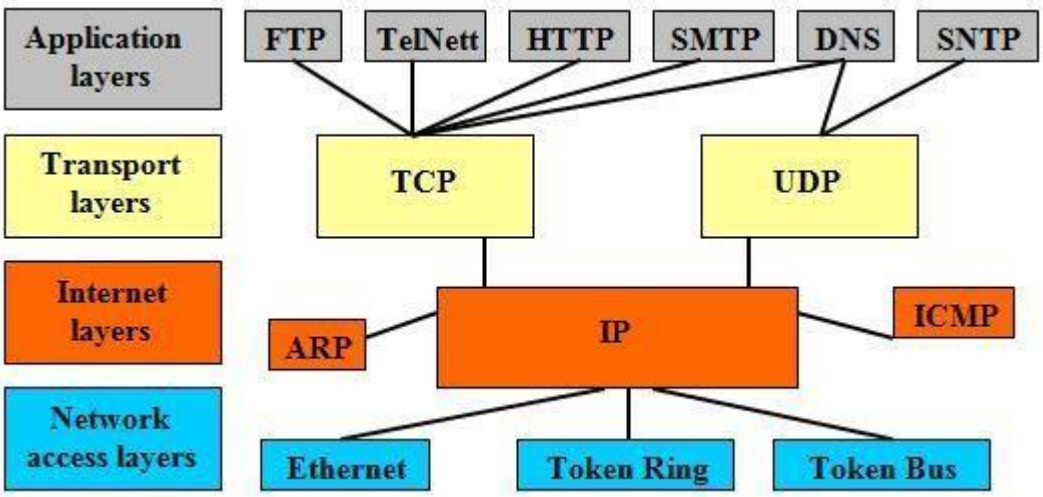
Theo đó giao thức trên ngày càng thể hiện rõ điểm mạnh của mình và khả năng liên kết, kết nối tối ưu của nó. Chính điều này đã thúc đẩy tạo nên một siêu mạng.

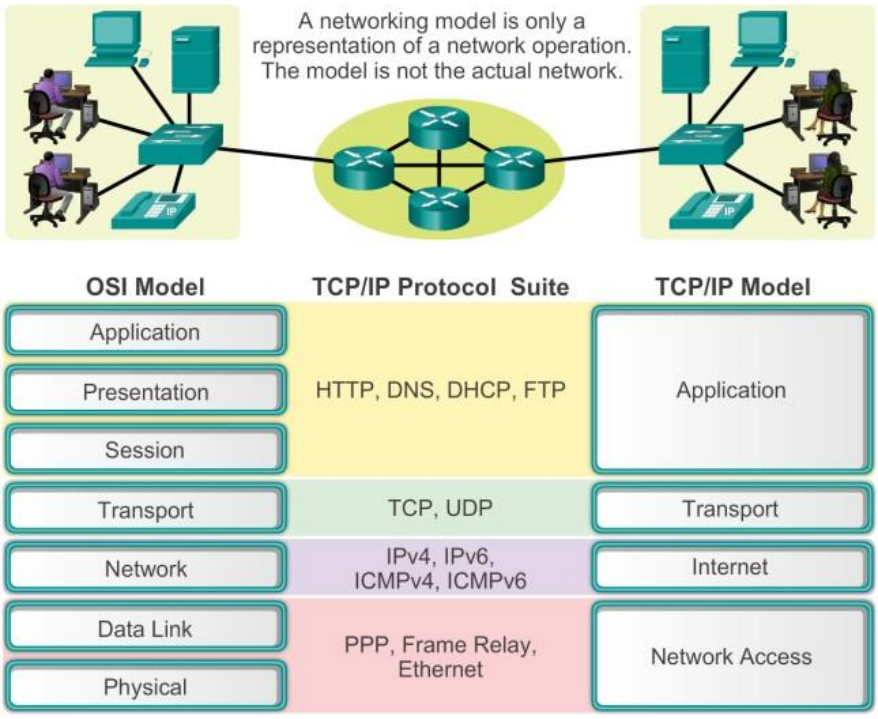
Năm 1980, mạng Internet chính thức ra đời được xác lập và liên kết các máy tính lớn với nhau gọi NSFNET.

Sự hình thành của mạng xương sống NSFNET đã tạo dựng một môi trường thuận lợi cho sự phát triển của Internet. Tuy nhiên NSFNET đã không còn hiệu quả sau gần 20 năm hoạt động và chuyển thành mạng nghiên cứu, còn Internet vẫn tiếp tục phát triển đến ngày nay.

Hy vọng những thông tin hữu ích trên sẽ giúp ích cho bạn trả lời được câu hỏi " mạng Internet ra đời năm nào?" Nhà bác học Albert Einstein từng có câu "Tôi sợ rằng trong tương lai, công nghệ sẽ lấn lướt sự tương tác giữa con người. Thế giới lúc đó sẽ là thế hệ của những kẻ đần độn". Internet có rất nhiều lợi ích nhưng đừng phụ thuộc vào nó, hãy biến nó thành công cụ để hỗ trợ con người. Đừng khiến Internet biến bạn thành kẻ đần độn vô cảm hoạt động như cái máy hãy sử dụng Internet một cách hữu ích nhất.

3.2.2. Họ giao thức TCP/IP





Giao thức IPv4

Mục đích của giao thức IP là kết nối các mạng con thành dạng Internet để truyền dữ liệu. Giao thức IP cung cấp bốn chức năng:

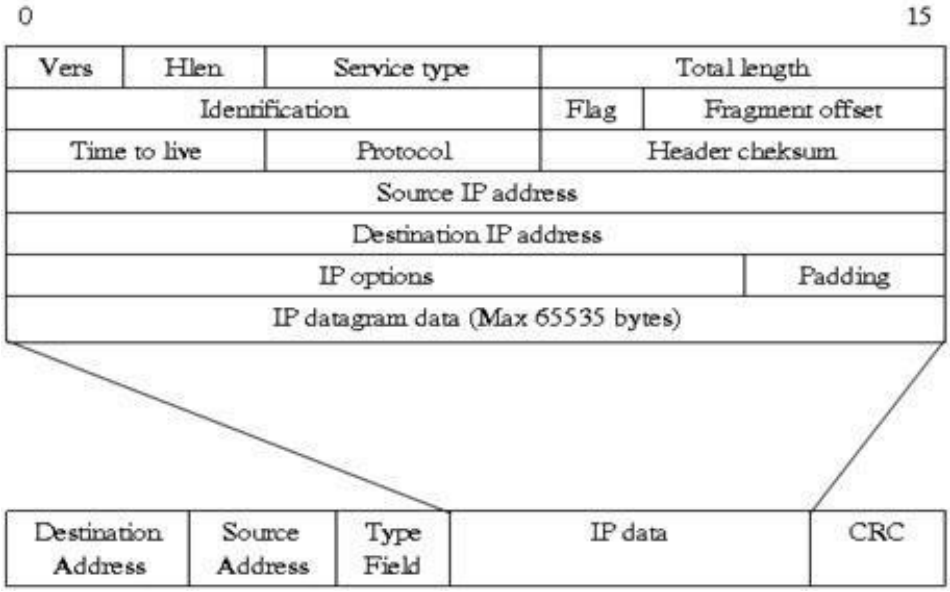
- Đơn vị cơ sở cho truyền dữ liệu
- Đánh địa chỉ
- Chọn đường
- Phân đoạn các datagram

Mục đích đầu tiên của IP là cung cấp các thuật toán truyền dữ liệu giữa các mạng. Nó cung cấp một dịch vụ phân phát không kết nối cho các giao thức tầng cao hơn. Nghĩa là nó không thiết lập

phiên (session) làm việc giữa trạm truyền và trạm nhận. IP gói (encapsulate) dữ liệu và phát nó với một sự nỗ lực nhất. IP không báo cho người nhận và người gửi về tình trạng gói dữ liệu mà cố gắng phát nó, do đó gọi là dịch vụ nỗ lực nhất. Nếu tầng liên kết dữ liệu bị lỗi thì IP cũng không thông báo mà cứ gửi lên tầng trên. Do đó, tới tầng TCP dữ liệu phải được phục hồi lỗi. Nói cách khác, tầng TCP phải có cơ chế timeout đối với việc truyền đó và sẽ phải gửi lại (resend) dữ liệu.

Trước khi phát dữ liệu xuống tầng dưới, IP thêm vào các thông tin điều khiển để báo cho tầng 2 biết có thông báo cần gửi vào mạng. Đơn vị thông tin IP truyền đi gọi là datagram, còn khi truyền trên mạng gọi là gói. Các gói được truyền với tốc độ cao trên mạng.

Giao thức IP không quan tâm kiểu dữ liệu trong gói. Các dữ liệu phải thêm các thông tin điều khiển gọi là đầu IP (IP header). Hình 2.3 chỉ ra cách IP gói thông tin và một đầu gói chuẩn của một datagram IP.



Khuôn dạng của IP header

Các trường trong IP header được định nghĩa như sau:

- **VERS**: Định nghĩa phiên bản hiện thời của IP trên mạng. Phiên bản này là Version 4 còn phiên bản sau cùng là Version 6.
- **HLEN**: Chiều dài của đầu IP. Không phải tất cả các trường trong phần đầu đều được sử dụng. Trường đo bằng đơn vị từ 32 bit. Đầu IP ngắn nhất là 20 bytes. Nó cũng có thể dài hơn phụ thuộc trường option.
- **Service Type**: Đặc tả các tham số về dịch vụ, có dạng cụ thể như sau:

0 1 2	3	4	5	6 7
Precedence	D	T	R	unused

+ **Precedence**: Trường này có giá trị từ 0 (mức ưu tiên bình thường) tới 7 (mức kiểm soát mạng) qui định việc gửi datagram. Nó kết hợp với các bit D (trễ), T (thông lượng), R (độ tin cậy) thành thông tin để chọn đường, được xem như định danh kiểu dịch vụ (Type of Service – TOS).

+ **Bit D** – Thiết lập là 1 khi yêu cầu trễ thấp.

+ **Bit T** – Yêu cầu thông lượng cao.

+ **Bit R** – Yêu cầu độ tin cậy cao.

Ví dụ, nếu có nhiều đường tới đích, bộ chọn đường sẽ đọc trường này để chọn một đường. Điều này đã trở nên quan trọng trong giao thức chọn đường OSPF, giao thức chọn đường đầu tiên của IP. Nếu giao dịch đã chiếm vị trí truyền file bạn có thể thiết lập các bit là 0 0 1 để báo rằng bạn không muốn độ trễ thấp và thông lượng cao nhưng cần độ tin cậy cao. Các trường của TOS được thiết lập bởi các ứng dụng như (TELNET, FTP) và không chọn đường. Các bộ chọn đường chỉ đọc trường này và dựa vào đó chọn ra đường tối ưu cho datagram. Nó yêu cầu một bộ chọn đường có nhiều bảng chọn, mỗi bảng ứng với một kiểu dịch vụ.

- **Total length:** Đây là chiều dài của datagram đo bằng byte (trường này dài 16 bit do đó khu vực IP datagram dài 65535 byte).

  Khi phải truyền một gói từ mạng rất lớn sang mạng khác, bộ chọn đường TCP/IP phải phân đoạn gói lớn thành các gói nhỏ hơn. Xét ví dụ, truyền một khung từ mạng Token Ring (kích thước truyền tối đa 4472 byte) tới mạng Ethernet (tối đa 1518 byte). TCP/IP sẽ thiết lập kích thước gói cho một liên kết. Nhưng nếu hai trạm đang thông tin bằng nhiều loại phương tiện, mỗi loại hỗ trợ kích thước truyền khác nhau? Việc phân đoạn thành các gói nhỏ thích hợp hơn cho truyền trên mạng LAN hoặc mạng LAN phức hợp dùng tầng IP. Các trường sau được sử dụng để đạt được kết quả này.

- **Idetification, flags, frement offset:** Các trường này biểu thị cách phân đoạn một datagram quá lớn. IP cho phép trao đổi dữ liệu giữa các mạng có khả năng phân đoạn các gói.

  Mỗi đầu IP của mỗi datagram đã phân đoạn hầu như giống nhau. Trường Identification để nhận dạng các datagram được phân đoạn từ cùng một datagram lớn hơn. Nó kết hợp với địa chỉ IP nguồn để nhận dạng.

  Trường flags biểu thị:

- Dữ liệu đang tới có được phân đoạn hay không.
- Phân đoạn hoặc không đối với một datagram.

  Việc phân đoạn rất quan trọng khi truyền trên các mạng có kích thước khung khác nhau. Ta đã biết cầu (bridge) không có khả năng này. Khi nhận một gói quá lớn nó sẽ phát (forward) lên mạng và không làm gì cả. Các giao thức tần trên sẽ timeout gói và trả lời theo. Khi một phiên làm việc thiết lập, hầu hết các giao thức có khả năng thương lượng khích thước gói tối đa mà mỗi trạm có thể quản lý, do đó không ảnh hưởng tới hoạt động của cầu.

  Các trường total length (tổng chiều dài) và fragment offset IP có thể xây dựng lại một datagram và chuyển nó tới phần mềm tầng cao hơn. Trường total length biểu thị tổng độ dài của một gói. Trường fragment offset biểu thị độ lệch từ đầu gói tới điểm mà tại đó dữ liệu sẽ được đặt vào trong đoạn dữ liệu để xây dựng lại gói (reconstruction).

- **Trường Time to live (TTL):** Có nhiều điều kiện lỗi làm cho một gói lặp vô hạn giữa các router (bộ chọn đường) trên Internet. Khởi đầu gói được thiết lập tại trạm gốc (originator). Các router sử dụng trường này để đảm bảo các gói không bị lặp vô hạn trên mạng. Tại trạm phát trường này được thiết lập thời gian là một số giây, khi datagram qua mỗi router trường này sẽ bị giảm. Với tốc độ hiện nay của các router thường giảm. Một thuật toán là router đang nhận sẽ ghi thời gian một gói đến, và sau đó, khi phát (forward) gói, router sẽ giảm trường này đi một số giây mà datagram phải đợi để được phát đi. Không phải tất cả các thuật toán đều làm việc theo cách này. Thời gian giảm ít nhất là 1 giây. Router giảm trường này tới 0 sẽ hủy gói tin và báo cho trạm gốc đã phát đi datagram.

  Trường TTL cũng được thiết lập một thời gian xác định (ví dụ số khởi tạo thấp nhất 64) để đảm bảo một gói tồn tại trên mạng trong một khoảng thời gian xác định. Nhiều router cho phép người quản trị mạng thiết lập trường này một số bất kỳ từ 0 đến 255.

- **Trường Protocol:** Trường này dùng để biểu thị giao thức mức cao hơn IP (ví dụ TCP hoặc UDP). Có nhiều giao thức tồn tại trên giao IP. IP không quan tầm tới giao thức đang chạy trên nó. Thường các giao thức này là TCP hoặc UDP. Theo thứ tự IP biết phải chuyển đúng gói tin tới đúng thực thể phía trên, đó là mục đích của trường này.
- **Trường Checksum:** Đây là mã CRC – 16 bit (kiểm tra dư thừa vòng). Nó đảm bảo tính toàn vẹn (integrity) của header. Một số CRC được tạo ra từ dữ liệu trong trường IP data và được đặt trong

trường này bởi trạm truyền (transmitting station). Khi trạm nhận đọc dữ liệu, nó sẽ tính số CRC. Nếu hai số CRC không giống nhau, có một lỗi trong header và gói tin sẽ bị hủy. Khi mỗi router nhận được datagram, nó sẽ tính lại checksum. Bởi vì, trường TTL bị thay đổi bởi mỗi router khi datagram truyền qua.

- **Trường IP option:** Về cơ bản, nó gồm thông tin về chọn đường (source routing), tìm vết (tracing a route), gán nhãn thời gian (time stamping) gói tin khi nó truyền qua các router và các đầu mục bí mật quân sự. Trường này có thể có hoặc không có trong header (nghĩa là cho phép độ dài header thay đổi).
- **Các trường IP source và IP destination address (địa chỉ nguồn và đích):** Rất quan trọng đối với người sử dụng khi khởi tạo trạm làm việc của họ hoặc cố định truy nhập các trạm khác không sử dụng dịch vụ tên miền (DNS) hoặc cập nhật file host (up-to-date host file). Nó cho biết địa chỉ trạm đích gói tin phải tới và địa chỉ trạm gốc đã phát gói tin.

  Tất cả các host trên internet được định danh bởi địa chỉ. Địa chỉ IP rất quan trọng sẽ được bàn tới đầy đủ dưới đây.

  ### Địa chỉ IP

  Ta đã biết với mạng Ethernet và Token Ring có các địa chỉ MAC. Với giao thức TCP/IP các host được định danh bởi địa chỉ IP 32-bit. Đây được xem như một giao thức địa chỉ.

  Mục đích đánh địa chỉ để IP thông tin với các host trên mạng hoặc Internet. Địa chỉ IP xác định cả nút đặc biệt và số hiệu mạng của nó. Địa chỉ IP dài 32 bit chia làm 4 trường, mỗi trường 1 byte. Địa chỉ này có thể biểu diễn dưới dạng thập phân, cơ số 8, 16 và nhị phân. Thường địa chỉ IP viết dưới dạng thập phân cùng các dấu chấm.

  Có hai cách gán địa chỉ IP, phụ thuộc cách kết nối của bạn. Nếu bạn nối với Internet, địa chỉ mạng được gán thông qua điều hành trung tâm, như trung tâm thông tin mạng (Network Information Centrer – NIC). Nếu bạn không nối với Internet, địa chỉ IP của bạn được gán một cách địa phương thông qua người quản trị mạng của bạn.

  Khi NIC gán địa chỉ mạng của bạn, đó chỉ là số hiệu mạng còn phần địa chỉ host được gán một cách địa phương bởi người quan trị mạng.

XNS sử dụng địa chỉ MAC 48-bit như địa chỉ host của nó. IP được phát triển trước khi có LAN tốc độ cao, do đó, nó có sơ đồ số hiệu của riêng nó. Địa chỉ IP tương thích với địa chỉ tầng vật lý của Ethernet và Token Ring.

- Khuôn dạng địa chỉ IP

  Mỗi host trên mạng TCP/IP có một định danh duy nhất tại tầng IP với một địa chỉ có dạng <NetID, HostID>. Toàn bộ địa chỉ thường dùng để định danh một host, không có sự tách biệt giữa các trường. Thực tế, khó phân biệt giữa các trường khi không viết tách. Dạng tổng quát của địa chỉ IP có dạng:

  <*Network Number, Host Number*>

- Các lớp IP (IP classes):

  128.4.70.9 là một ví dụ địa chỉ IP. Nhìn vào địa chỉ này khó mà biết được đâu là phân số hiệu mạng, đâu là phân số hiệu host. Địa chỉ IP bao gồm 4 byte, phần số hiệu mạng có thể chiếm một, hai hoặc ba byte đầu, phần còn lại là số hiệu host. Tùy thuộc vào điều đó, địa chỉ IP chia làm 5 lớp: A, B, C, D và E. Các lớp A, B và C được sử dụng cho địa chỉ mạng và host. Lớp D là kiểu địa chỉ đặc biệt dùng cho multicast. Lớp E được để dành.

- Định danh lớp IP trong IPv4:

  Lớp A: Địa chỉ lớp A chỉ sử dụng byte đầu cho số hiệu mạng, ba byte sau cho địa chỉ host. Địa chỉ lớp A cho phép phân biệt 126 mạng, mỗi mạng tới 16 triệu host ứng với 24 bits. Tại sao chỉ có 126 mạng ứng với 8 bit? Thứ nhất, 127.x (01111111 nhị phân) được dành cho chức năng loop-back nên không gán cho số hiệu mạng. Thứ hai, bit đầu tiên thiết lập 0 để nhận dạng lớp A. Địa chỉ mạng lớp A thường trong phạm vi từ 1 tới 126, còn ba byte cuối được gán một cách địa phương cho các host. Địa chỉ lớp A có dạng:

  <**Số hiệu mạng.host.host.host**>

  Lớp B: Địa chỉ lớp B dùng hai byte đầu cho số hiệu mạng và hai byte cuối dành cho số hiệu host. Nó được nhận dạng bởi hai bit đầu tiên là 10. Cho phép phân biệt 16384 số hiệu mạng, mỗi mạng tới 65354 host. Do đó dịch địa chỉ số hiệu mạng từ 128 tới 191. Nên nó sẽ có dạng:

  <**Số hiệu mạng.Số hiệu mạng.host.hos**>

Lớp C: Địa chỉ lớp C sử dụng ba byte đầu cho số hiệu mạng và byte cuối cho địa chỉ host. Nhận dạng bởi ba bit đầu tiên là 110. Cho phép địa chỉ mạng trong phạm vi 192-223 của trường thứ nhất. Do đó có tới hai triệu mạng và mỗi mạng có thể chứa 254 host. Thường địa chỉ lớp C được gán bởi NIC. Nó có dạng:

<**Số hiệu mạng.Số hiệu mạng.Số hiệu mạng.Host**>

Địa chỉ IP không thể đặt bốn bit đầu tiên 1111 vì dành cho lớp E.

Các địa chỉ lớp D hoặc multicast dùng để gửi một IP datagram tới một nhóm các host trên mạng.

Các địa chỉ IP dành riêng

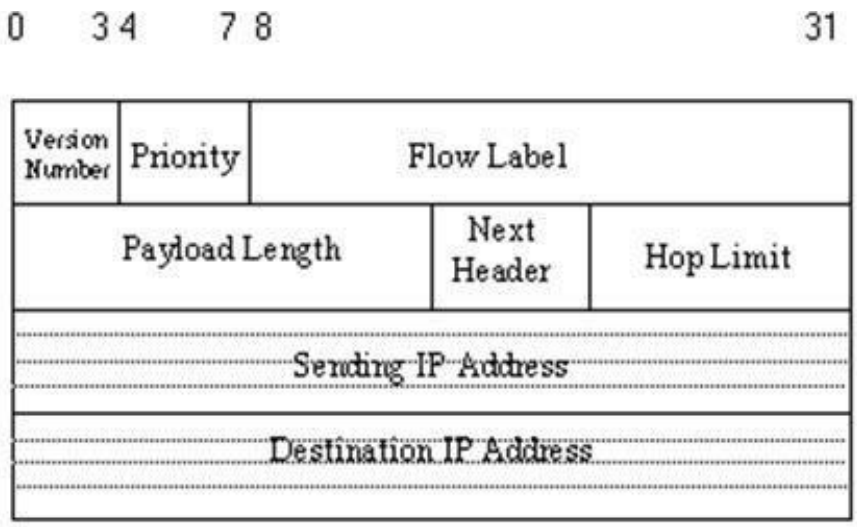
Các địa chỉ host nào đó được dành riêng và không thể gán cho các thiết bị trên mạng. Các địa chỉ host dành riêng này bao gồm:

Địa chỉ mạng: Được dùng để định danh chính mạng đó. Một địa chỉ IP có tất cả vị trí bit ở phần host đều chứa nhị phân 0 được dành riêng cho địa chỉ mạng.

ĐịachỉBroadcast: Được dùng để quảng bá (broadcasting) các gói đến tất cả các thiết bị trên một mạng. Để truyền số liệu đến tất cả các thiết bị trên mạng, cần một địa chỉ broadcast. Một hoạt động broadcast diễn ra là khi một nguồn truyền số liệu đến tất cả các thiết bị trên mạng. Để đảm bảo tất cả các thiết bị khác trên mạng xử lý broadcast này, máy gửi phải dùng một địa chỉ IP đích mà chúng có thể chấp nhận và xử lý. Các địa chỉ broadcast kết thúc bằng toàn là nhị phân 1 trong phần host của địa chỉ.

IPv6

IPv6 là tập hợp những đặc tả về nâng cấp IPv4 và được IETF soạn thảo. Nó được coi là giao thức Internet thế hệ mới và được thiết kế để gói thông tin được định dạng cho IPv4 có thể làm việc được. Những giới hạn về dung lượng địa chỉ và tốc độ tìm đường đi thấp đã thúc đẩy việc phát triển IPv6. Với dung lượng 128 bit và cách đánh địa chỉ đơn giản hơn, giao thức mới này sẽ giải quyết phần nào những vấn đề trên. Các tính năng được tăng cường này sẽ giải quyết phần nào những vấn đề trên. Các tính năng được tăng cường khác là mã hóa 64 bit và tự động cấu hình được thiết kế sẵn của địa chỉ IP. Khuôn dạng của IPv6 header được miêu tả ở hình ?



Khuôn dạng của IPv6 header

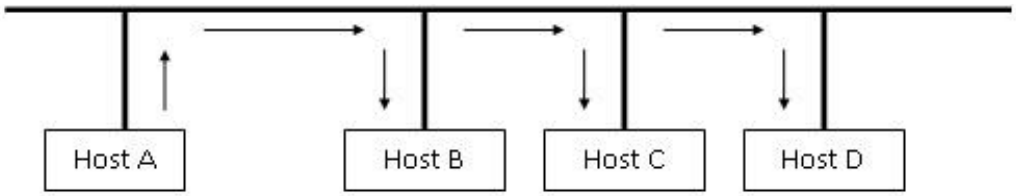
- Mở rộng địa chỉ và tính năng dẫn đường: Kích thước địa chỉ IP lên đến 128 đảm bảo rằng IPv6 sẽ là giao thức Internet lâu dài. Khả năng mở rộng của việc định tuyến một chiều được cải tiến để truyền một cách hiệu quả các ứng dụng băng thông cao như video và audio.
- Tốc độ mạng: Những thay đổi thực hiện trong định dạng địa chỉ giúp giảm yêu cầu về băng thông và cho phép tăng tính hiệu quả và linh hoạt của việc định tuyến và phát tiếp thông tin.
- Khả năng bảo mật thiết kế sẵn: Những mở rộng để hỗ trợ khả năng kiểm tra tính hợp lệ, tích hợp và bảo mật dữ liệu là một phần của IPv6.

Gói tin ARP

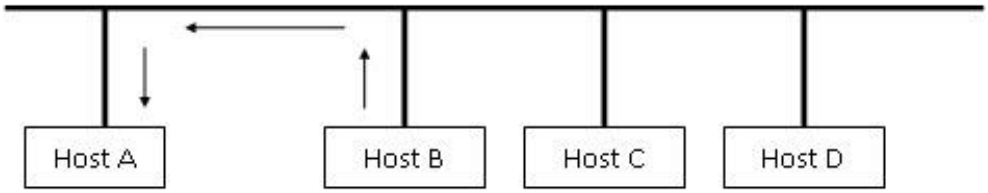
Mọi máy tính cùng nằm trên một mạng có cùng một network id và các máy tính trên một mạng vật lý có thể gửi frame vật lý trực tiếp cho nhau nên việc truyền thông tin giữa hai máy tính trong cùng một mạng vật lý không cần sử dụng gateway. Trạm gửi chỉ việc kết khối dữ liệu vào frame, chuyển địa chỉ IP của trạm đích thành địa chỉ vật lý và gửi trực tiếp nó tới máy nhận.

Một cơ chế sử dụng để chuyển địa chỉ IP thành địa chỉ vật lý là ARP (Address Resolusion Protocol). Khi hai máy tính cùng nối vào một mạng vật lý, chúng biết được địa chỉ IP của nhau nhưng để truyền thông giữa hai máy, chúng phải biết được địa chỉ vật lý của nhau. ARP giải quyết vấn đề chuyển từ địa chỉ IP 32 bit sang địa chỉ Ethernet 48 bit. Người ta sử dụng hai cơ chế đó là:

- Chuyển giao trực tiếp: địa chỉ vật lý là một hàm của địa chỉ IP ví du sử dụng trên mạng token ring proNET-10 là mạng cho phép đặt địa chỉ IP và địa chỉ vật lý thoải mái. Người ta có thể đặt địa chỉ IP là 192.5.48.3 và địa chỉ vật lý là 3, khi đó ta có $P_A=f(I_A)$.
- Chuyển giao địa chỉ động được thực hiện bằng cách máy tính muốn gửi thông tin gửi một thông báo tới toàn bộ các máy tính trên mạng, trong thông báo đó có chứa địa chỉ IP của máy tính nó cần liên lạc, mọi máy sẽ nhận được thông báo và máy nào thấy địa chỉ IP của mình thì trả lại một thông báo chứa địa chỉ vật lý, khi đó, hai máy tính có thể "nói chuyện" với nhau.



ARP Request



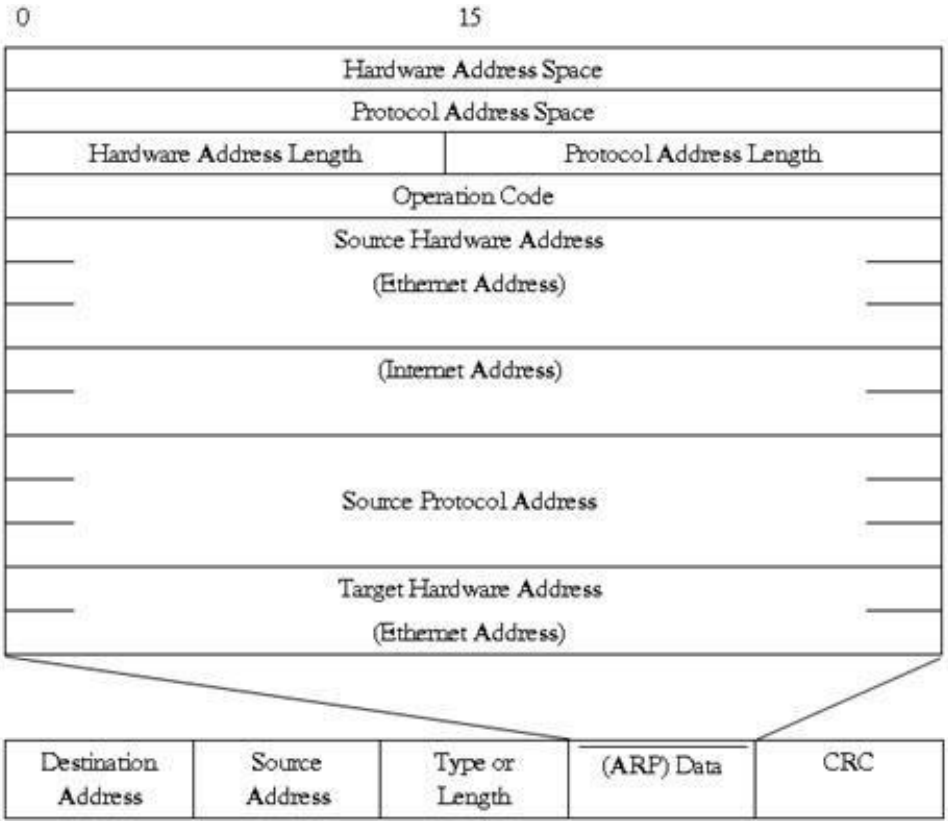
ARP Reply

Quá trình hỏi đáp của gói tin ARP

- Ngoài ra, người ta còn sử dụng bảng chỉ đường để lưu trữ tạm thời các địa chỉ sử dụng mới nhất (Address Reslution Cache) để tăng tốc độ của việc chuyển giao địa chỉ.

  Một gói thông tin ARP là một Ethernet Frame được truyền trực tiếp từ máy này tới máy khác. Vì không phải sử dụng IP, gói tin này không có địa chỉ IP cũng như không cần được dẫn đường, nó phải được gửi broadcasts tới tất cả các máy trên mạng Ethernet (với địa chỉ FFFFFFFFFFFF)

  Gói thông tin ARP được mô tả như sau:



Cấu trúc gói tin ARP

Không giống phần lớn các giao thức khác, dữ liệu trong ARP không có một định dạng chuẩn cho header. Để ARP có thể làm việc với nhiều công nghệ khác nhau, người ta dùng một trường để chứa độ dài của những trường đi sau nó.

Trong trường hợp máy trạm không có thiết bị nhớ phụ, nó không biết địa chỉ IP của chính mình khi khởi động, người ta sử dụng cơ chế có tên (RARP) để giải quyết vấn đề này đó là có một máy chủ chứa bảng địa chỉ IP của các máy trạm, khi máy trạm khởi động, nó gửi một request tới tất cả các máy và máy chủ trả lời nó bằng một gói tin chứa địa chỉ IP.

Cơ chế thông báo lỗi (Internet Control Message Protocol – ICMP)

Một giao thức trong tầng Internet là ICMP được định nghĩa trong RFC 792. ICMP sử dụng gói tin IP để chuyển thông báo của nó. ICMP gửi các thông báo làm các công việc: Điều khiển, thông báo lỗi và chức năng thông tin cho TCP/IP.

Gói tin ICMP

Mặc dầu mỗi thông báo ICMP có một kiểu định dạng riêng của nó, chúng đều chứa 3 trường đầu tiên giống nhau.

- **TYPE**: Định nghĩa thông báo đi sau.
- **CODE**: Cung cấp thông tin thêm về thông báo.
- **CHECKSUM**: Chưa checksum của thông báo.

Bảng 2.1 Bảng mã gói tin thông báo ICMP

Type Field	ICMP Message Type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (Change o router)
8	Echo Request
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Điều khiển dòng dữ liệu

Khi dữ liệu gửi tới trạm nhận quá nhanh không kịp xử lý, trạm đích - hay một thiết bị dẫn đường gửi trả trạm nguồn một thông báo để nó tạm ngừng việc truyền thông tin.

Thông báo lỗi

Khi không tìm thấy trạm đích, một thông báo lỗi Destination Unreachable được được gateway gửi trả lại trạm nguồn. Nếu một cổng không nhận ra, trạm đích gửi thông báo lỗi lại cho trạm nguồn (chúng ta sẽ nói về cổng trong phần giao thức tầng giao vận).

Giao thức TCP:

Bít 0 - 3	4 - 9	10 - 15	16 - 31
Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
Data Offset	Reserved	Flags	Window
Checksum			Urgent Pointer
Options (optional)			
Data			

Source port: Số hiệu của cổng tại máy tính gửi.

Destination port: Số hiệu của cổng tại máy tính nhận.

Sequence number: Trường này có 2 nhiệm vụ. Nếu cờ SYN bật thì nó là số thứ tự gói ban đầu và byte đầu tiên được gửi có số thứ tự này cộng thêm 1. Nếu không có cờ SYN thì đây là số thứ tự của byte đầu tiên.

Acknowledgement number: Nếu cờ ACK bật thì giá trị của trường chính là số thứ tự gói tin tiếp theo mà bên nhận cần.

Data offset : Trường có độ dài 4 bít quy định độ dài của phần header (tính theo đơn vị từ 32 bít). Phần header có độ dài tối thiểu là 5 từ (160 bit) và tối đa là 15 từ (480 bít).

Reserved: Dành cho tương l; ai và có giá trị là 0.

Flags (hay Control bits): Bao gồm 6 cờ:

URG: Cờ cho trường Urgent pointer

ACK: Cờ cho trường Acknowledgement

PSH: Hàm Push

RST: Thiết lập lại đường truyền

SYN:Đồng bộ lại số thứ tự

FIN: Không gửi thêm số liệu

Window:Số byte có thể nhận bắt đầu từ giá trị của trường báo nhận (ACK)

Checksum

16 bít kiểm tra cho cả phần header và dữ liệu. Phương pháp sử dụng được mô tả trong RFC 793:

16 bít của trường kiểm tra là bổ sung của tổng tất cả các từ 16 bít trong gói tin. Trong trường hợp số octet (khối 8 bít) của header và dữ liệu là lẻ thì octet cuối được bổ sung với các bít 0. Các bít này không được truyền. Khi tính tổng, giá trị của trường kiểm tra được thay thế bằng 0,

Nói một cách khác, tất cả các từ 16 bít được cộng với nhau. Kết quả thu được sau khi đảo giá trị từng bít được điền vào trường kiểm tra. Về mặt thuật toán, quá trình này giống với IPv4.

Điểm khác nhau chỉ ở chỗ dữ liệu dùng để tính tổng kiểm tra. Dưới đây là một header của IP:

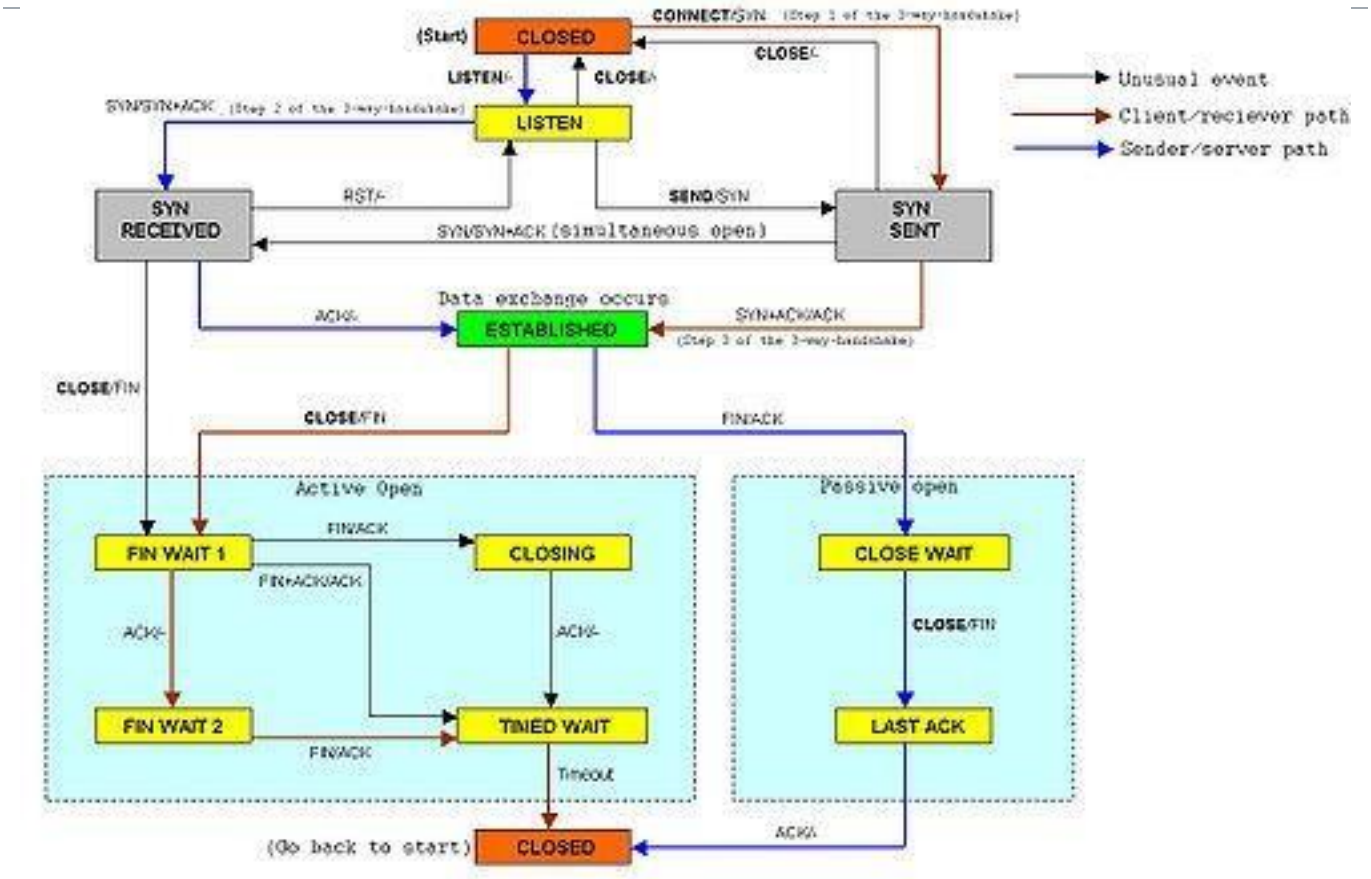
Urgent pointer

Nếu cờ URG bật thì giá trị trường này chính là số từ 16 bít mà số thứ tự gói tin (*sequence number*) cần dịch trái.

Options

Đây là trường tùy chọn. Nếu có thì độ dài là bội số của 32 bít.

Hoạt động của giao thức



Trước khi miêu tả các pha này, ta cần lưu ý các trạng thái khác nhau của một socket:

1. LISTEN
2. SYN-SENT
3. SYN-RECEIVED
4. ESTABLISHED
5. FIN-WAIT
6. CLOSE-WAIT
7. CLOSING
8. LAST-ACK
9. TIME-WAIT

10. CLOSER

LISTEN

đang đợi yêu cầu kết nối từ một TCP và cổng bất kỳ ở xa (trạng thái này thường do các TCP server đặt)

SYN-SENT

đang đợi TCP ở xa gửi một gói tin TCP với các cờ SYN và ACK được bật (trạng thái này thường do các TCP client đặt)

SYN-RECEIVED

đang đợi TCP ở xa gửi lại một tin báo nhận sau khi đã gửi cho TCP ở xa đó một tin báo nhận kết nối (*connection acknowledgment*) (thường do TCP server đặt)

ESTABLISHED

cổng đã sẵn sàng nhận/gửi dữ liệu với TCP ở xa (đặt bởi TCP client và server)

TIME-WAIT

đang đợi qua đủ thời gian để chắc chắn là TCP ở xa đã nhận được tin báo nhận về yêu cầu kết thúc kết nối của nó. Theo RFC 793, một kết nối có thể ở tại trạng thái TIME-WAIT trong vòng tối đa 4 phút.

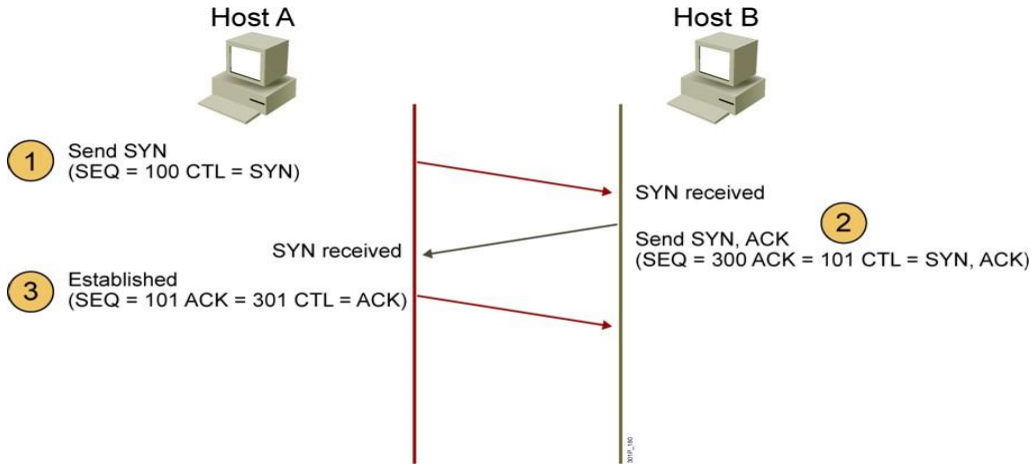
Thiết lập kết nối

Để thiết lập một kết nối, TCP sử dụng một quy trình bắt tay 3 bước (*3-way handshake*) Trước khi client thử kết nối với một server, server phải đăng ký một cổng và mở cổng đó cho các kết nối: đây được gọi là mở bị động. Một khi mở bị động đã được thiết lập thì một client có thể bắt đầu mở chủ động. Để thiết lập một kết nối, quy trình bắt tay 3 bước xảy ra như sau:

1. Client yêu cầu mở cổng dịch vụ bằng cách gửi gói tin SYN (gói tin TCP) tới server, trong gói tin này, tham số**sequence number** được gán cho một giá trị ngẫu nhiên **X**.
2. Server hồi đáp bằng cách gửi lại phía client bản tin SYN-ACK, trong gói tin này, tham số **acknowledgment number**được gán giá trị bằng X + 1, tham số **sequence number** được gán ngẫu nhiên một giá trị **Y**
3. Để hoàn tất quá trình **bắt tay ba bước**, client tiếp tục gửi tới server bản tin ACK, trong bản tin này, tham số**sequence number** được gán cho giá trị bằng X + 1 còn tham số **acknowledgment number** được gán giá trị bằng Y + 1

Tại thời điểm này, cả client và server đều được xác nhận rằng, một kết nối đã được thiết lập.

Bắt tay 3 bước TCP



TCP là giao thức thuộc dạng connection-oriented (hướng kết nối). Có nghĩa là nó thiết lập kênh kết nối trước khi truyền data đi.

- UDP là giao thức thuộc dạng connectionless (nghĩa là không hướng kết nối). Nó không cần thiết lập kênh truyền trước khi truyền dữ liệu đi.

TCP thiết lập kết nối bằng 3 bước bắt tay (3-way handshake)

sender_____receiver

SYN seq=X ----------> SYN received (step 1)

SYN received <------- send ACK X+1 and SYN Y (step 2)

Send ACK Y+1-------- > (step 3)

Một gói dữ liệu TCP chứa các code bits (6) dùng để xác định các loại segment. Có 6 loại segment: URG, ACK, PSH, RST, SYN, FIN

* SYN (synchronization) dùng để bắt đầu một connection.
* ACK (acknowledgement).
* FIN (finish) dùng để ngắt một connection.
* URG và PSH là gói tin ưu tiên
* RST là gói tin cắt ngang

Bây giờ là các bước thực hiện việc thiết lập kết nối (giả sử A là người gởi và B là người nhận)
- Bước 1. A gởi cho B một SYN segment, trong đó chứa Sequence number của A
- Bước 2. Khi B nhận được B sẽ gởi lại một SYN – ACK Segment, trong đó chứa Sequence number của B và vùng ACK= Sequence number của B + 1
- Bước 3. Khi A nhận được sẽ gởi lại một ACK Segment chứa Sequence number A bằng giá trị vùng ACK của B gởi tới và vùng ACK của A có giá trị bằng Sequence number +1
Sau bước 3, kết nối được thiết lập và sẵn sàng truyền Data. Mục đích là để trao đổi Sequence Number và ACK Number.

Mục đích của Phương pháp bắt tay 3 bước là để thiết lập kết nối giữa bên gởi và bên nhận để tránh bị mất dữ liệu

Truyền dữ liệu

Một số đặc điểm cơ bản của TCP để phân biệt với UDP:

- Truyền dữ liệu không lỗi (do có cơ chế sửa lỗi/truyền lại)
- Truyền các gói dữ liệu theo đúng thứ tự
- Truyền lại các gói dữ liệu mất trên đường truyền
- Loại bỏ các gói dữ liệu trùng lặp
- Cơ chế hạn chế tắc nghẽn đường truyền

Ở hai bước đầu tiên trong ba bước bắt tay, hai máy tính trao đổi một số thứ tự gói ban đầu (*Initial Sequence Number* -ISN). Số này có thể chọn một cách ngẫu nhiên. Số thứ tự này được dùng để đánh dấu các khối dữ liệu gửi từ mỗi máy tính. Sau mỗi byte được truyền đi, số này lại được tăng lên. Nhờ vậy ta có thể sắp xếp lại chúng khi tới máy tính kia bất kể các gói tới nơi theo thứ tự thế nào.

Trên lý thuyết, mỗi byte gửi đi đều có một số thứ tự và khi nhận được thì máy tính nhận gửi lại tin báo nhận (ACK). Trong thực tế thì chỉ có byte dữ liệu đầu tiên được gán số thứ tự trong trường số thứ tự của gói tin và bên nhận sẽ gửi tin báo nhận bằng cách gửi số thứ tự của byte đang chờ.

Ví dụ: Máy tính A gửi 4 byte với số thứ tự ban đầu là 100 (theo lý thuyết thì 4 byte sẽ có thứ tự là 100, 101, 102, 103) thì bên nhận sẽ gửi tin báo nhận có nội dung là 104 vì đó là thứ tự của byte tiếp theo nó cần. Bằng cách gửi tin báo nhận là 104, bên nhận đã ngầm thông báo rằng nó đã nhận được các byte 100, 101, 102 và 103. Trong trường hợp 2 byte cuối bị lỗi thì bên nhận sẽ gửi tin báo nhận với nội dung là 102 vì 2 byte 100 và 101 đã được nhận thành công.

Giả sử ta có 10.000 byte được gửi đi trong 10 gói tin 1.000 byte và có 1 gói tin bị mất trên đường truyền. Nếu gói bị mất là gói đầu tiên thì bên gửi sẽ phải gửi lại toàn bộ 10 gói vì không có cách nào để bên nhận thông báo nó đã nhận được 9 gói kia. Vấn đề này được giải quyết trong giao thức SCTP (*Stream Control Transmission Protocol* - "Giao thức điều khiển truyền vận dòng") với việc bổ sung báo nhận chọn lọc.

Số thứ tự và tin báo nhận giải quyết được các vấn đề về lặp gói tin, truyền lại những gói bị hỏng/mất và các gói tin đến sai thứ tự. Để phục vụ mục đích kiểm tra, các gói tin có trường giá trị tổng kiểm (*checksum* - Xem thêm phần #Cấu trúc gói).

Với trình độ hiện tại, kỹ thuật kiểm tra tổng trong TCP không đủ mạnh. Các tầng liên kết dữ liệu với xác suất lỗi bit cao có thể cần được bổ sung các khả năng phát hiện lỗi tốt hơn. Nếu như TCP được thiết kế vào thời điểm hiện tại, nhiều khả năng nó sẽ bao gồm trường kiểm tra độ dư tuần hoàn (*cyclic redundancy check* - CRC) với độ dài 32 bit. Điểm yếu này một phần được bù đắp bằng CRC hay những kỹ thuật khác tại tầng thứ 2 (trong mô hình 7 lớp OSI) ở bên dưới cả TCP và IP như trong các giao thức điểm-điểm (PPP) hoặc Ethernet. Tuy nhiên điều này cũng không có nghĩa là trường kiểm tra tổng của TCP là không cần thiết: thống kê cho thấy các sai sót do cả phần cứng và phần mềm gây ra giữa các điểm áp dụng kỹ thuật kiểm tra CRC là khá phổ biến và kỹ thuật kiểm tra tổng có khả năng phát hiện phần lớn các lỗi (đơn giản) này.

Điểm cuối cùng là khả năng hạn chế tắc nghẽn.

Tin báo nhận (hoặc không có tin báo nhận) là tín hiệu về tình trạng đường truyền giữa 2 máy tính. Từ đó, hai bên có thể thay đổi tốc độ truyền nhận dữ liệu phù hợp với điều kiện. Vấn đề này thường được đề cập là điều khiển lưu lượng, kiểm soát tắc nghẽn. TCP sử dụng một số cơ chế nhằm đạt được hiệu suất cao và ngăn ngừa khả năng nghẽn mạng. Các cơ chế này bao gồm: cửa sổ trượt (*sliding window*), thuật toán slow-start, thuật toán tránh nghẽn mạng (*congestion avoidance*), thuật toán truyền lại và phục hồi nhanh,... Hiện nay, vấn đề cải tiến TCP trong môi truyền truyền dẫn tốc độ cao đang là một hướng nghiên cứu được quan tâm.

Kích thước cửa sổ TCP

Chuỗi số thứ tự gói và cửa sổ trong TCP hoạt động giống như một cái đồng hồ. Kích thước của cửa sổ (đo bằng byte) được thiết lập bởi khả năng tiếp nhận của máy tính nhận. Cửa sổ này được dịch đi mỗi khi máy tính nhận nhận được dữ liệu và gửi tin báo nhận. Khi chuỗi thứ tự tăng đến tối đa thì lại quay lại về 0.

Kích thước của cửa sổ là chiều dài (byte) của khối dữ liệu có thể lưu trong bộ đệm của bên nhận. Bên gửi chỉ có thể gửi tối đa lượng thông tin chứa trong cửa sổ này trước khi nhận được tin báo nhận.

Dãn kích thước cửa sổ

Để tận dụng khả năng truyền dẫn của mạng thì cửa sổ dùng trong TCP cần được tăng lên. Trường điều khiển kích thước cửa sổ của gói TCP có độ dài là 2 byte và do đó kích thước tối đa của cửa sổ là 65.535 byte.

Do trường điều khiển không thể thay đổi nên người ta sử dụng một hệ số dãn nào đó. Hệ số này được định nghĩa trong tài liệu RFC 1323 có thể sử dụng để tăng kích thước tối đa của cửa sổ từ 65.535 byte lên tới 1 gigabyte. Tăng kích thước cửa sổ lớn hơn nữa cũng cần thiết trong TCP Tuning.

Việc tăng kích thước cửa sổ chỉ được dùng trong giao thức bắt tay 3 pha. Giá trị của trường co giãn cửa sổ thể hiện số bit cần được dịch trái đối với trường kích thước cửa sổ. Hệ số dãn có thể thay đổi từ 0 (không dãn) tới 14 (dãn tối đa).

Kết thúc kết nối

Để kết thúc kết nối hai bên sử dụng quá trình bắt tay 4 bước và chiều của kết nối kết thúc độc lập với nhau. Khi một bên muốn kết thúc, nó gửi đi một gói tin FIN và bên kia gửi lại tin báo nhận ACK. Vì vậy, một quá trình kết thúc tiêu biểu sẽ có 2 cặp gói tin trao đổi.

Một kết nối có thể tồn tại ở dạng "nửa mở": một bên đã kết thúc gửi dữ liệu nên chỉ nhận thông tin, bên kia vẫn tiếp tục gửi.

Các cổng TCP

TCP sử dụng khái niệm số hiệu cổng (*port number*) để định danh các ứng dụng gửi và nhận dữ liệu. Mỗi đầu của một kết nối TCP có một số hiệu cổng (là số không dấu 16-bit) được gán cho ứng dụng đang nhận hoặc gửi dữ liệu. Các cổng được phân thành ba loại cơ bản: nổi tiếng, được đăng ký và động/cá nhân. Các cổng nổi tiếng đã được gán bởi tổ chức Internet Assigned Numbers Authority (IANA) và thường được sử dụng bởi

các tiến trình mức hệ thống hoặc các tiến trình của root. Ví dụ: FTP (21), TELNET (23), SMTP (25) và HTTP (80). Các cổng được đăng ký thường được sử dụng bởi các ứng dụng người dùng đầu cuối (*end user application*) với vai trò các cổng phát tạm thời (khi dùng xong thì hủy đăng ký) khi kết nối với server, nhưng chúng cũng có thể định danh các dịch vụ có tên đã được đăng ký bởi một bên thứ ba. Các cổng động/cá nhân cũng có thể được sử dụng bởi các ứng dụng người dùng đầu cuối, nhưng không thông dụng bằng. Các cổng động/cá nhân không có ý nghĩa gì nếu không đặt trong một kết nối TCP. Có 65535 cổng được chính thức thừa nhận.

TCP trên mạng không dây

TCP cũng được sử dụng cho mạng không dây. Ở đây trường hợp mất gói tin cũng được xem là nghẽn mạng và kích thước cửa sổ do đó cũng sẽ được giảm xuống. Tuy nhiên trong nhiều trường hợp đối với các mạng không dây thì việc mất các gói tin thường xảy ra một cách ngẫu nhiên do ảnh hưởng của fading, chuyển giao giữa các cell... và chúng ta không thể xem đây là nghẽn mạng. Do đó, việc giảm kích thước cửa sổ không đúng sẽ làm cho hiệu quả sử dụng đường truyền giảm một cách đáng kể. Nhiều nghiên cứu đã tập trung để giải quyết vấn đề này. Các giải pháp được đề ra có thể phân loại thành các nhóm: giải pháp đầu cuối (liên quan tới việc thay đổi tại client/server), giải pháp tại tầng liên kết dữ liệu (chẳng hạn giao thức RLP trong chuẩn CDMA2000) và giải pháp dựa trên proxy (thay đổi trong mạng mà không cần thay đổi các thiết bị đầu cuối).

Gỡ rối trong TCP

Các phần mềm đọc gói (*packet sniffer*) TCP có thể sử dụng để gỡ rối/theo dõi bằng cách đọc tất cả các gói TCP được truyền trong mạng. Ví dụ: Wireshark(trên Windows và Linux), tcpdump(trên Linux)...

Đối với một số ứng dụng thì TCP không thích hợp. Vấn đề lớn nhất là phía nhận không thể tiếp nhận các gói tin đến sau một gói bị lỗi trước khi chính gói bị lỗi được truyền lại. Điều này khiến TCP không thích hợp cho các ứng dụng thời gian thực (*real-time*) chẳng hạn như đa phương tiện trực tuyến, trò chơi trực tuyến và thoại trên nền IP (VoIP) bởi vì các ứng dụng này cần các gói tin kịp thời hơn là nhận đủ các gói tin theo đúng thứ tự.

Ngoài ra sự phức tạp của TCP cũng gây ra vấn đề với các hệ thống nhúng (*embedded system*). Ví dụ tiêu biểu là netbooting sử dụng giao thức TFTP. Cuối cùng, độ phức tạp của TCP cũng gây khó khăn cho một số vấn đề khác như truyền thông tin giữa 2 máy tính nằm sau hệ thống chuyển đổi địa chỉ (NAT).

Thông thường, khi TCP không thích hợp thì UDP được sử dụng. UDP cung cấp một số tính năng giống TCP như đa công và kiểm tra tổng nhưng nó không đảm bảo việc truyền lại gói tin lỗi hay thứ tự các gói tin. Vì thế, người phát triển ứng dụng có thể áp dụng các phương thức khác ở các tầng trên để giải quyết vấn đề tùy theo yêu cầu cụ thể.

Giao thức điều khiển truyền vận dòng (*Stream Control Transmission Protocol* - SCTP) cũng là một giao thức dựa trên nền IP không khác nhiều so với TCP. SCTP được phát triển sau và có cấu trúc phức tạp hơn TCP.

SCTP được thiết kế để sử dụng trong điều kiện yêu cầu độ tin cậy và gần thời gian thực. Tuy nhiên SCTP chưa được sử dụng rộng rãi.

TCP cũng bộc lộ một số vấn đề khi dùng trong môi trường truyền dẫn tốc độ cao. Thuật toán tránh nghẽn mạng làm việc tốt trong môi trường không dự tính trước nhưng đối với môi trường xác định hơn chẳng hạn như ATM (*Asynchronous Transfer Mode*) thì TCP không tận dụng được khả năng của hệ thống bên dưới.

Giao thức UDP:

Bits 0 - 15	16 - 31
Source Port	Destination Port
Length	Checksum
Data	

UDP là giao thức hướng thông điệp nhỏ nhất của tầng giao vận hiện được mô tả trong RFC 768 của IETF.

Trong bộ giao thức TCP/IP, UDP cung cấp một giao diện rất đơn giản giữa tầng mạng bên dưới (thí dụ, IPv4) và tầng phiên làm việc hoặc tầng ứng dụng phía trên.

UDP không đảm bảo cho các tầng phía trên thông điệp đã được gửi đi và người gửi cũng không có trạng thái thông điệp UDP một khi đã được gửi (Vì lý do này đôi khi UDP còn được gọi là *Unreliable* Datagram Protocol).

UDP chỉ thêm các thông tin multiplexing và giao dịch. Các loại thông tin tin cậy cho việc truyền dữ liệu nếu cần phải được xây dựng ở các tầng cao hơn.

Phần header của UDP chỉ chứa 4 trường dữ liệu, trong đó có 2 trường là tùy chọn (ô nền đỏ trong bảng).

Source port

Trường này xác định cổng của người gửi thông tin và có ý nghĩa nếu muốn nhận thông tin phản hồi từ người nhận. Nếu không dùng đến thì đặt nó bằng 0.

Destination port

Trường xác định cổng nhận thông tin, và trường này là cần thiết.

Length

Trường có độ dài 16 bit xác định chiều dài của toàn bộ datagram: phần header và dữ liệu. Chiều dài tối thiểu là 8 byte khi gói tin không có dữ liệu, chỉ có header.

Checksum

Trường checksum 16 bit dùng cho việc kiểm tra lỗi của phần header *và dữ liệu*. Phương pháp tính checksum được định nghĩa trong RFC 768.

Do thiếu tính tin cậy, các ứng dụng UDP nói chung phải chấp nhận mất mát, lỗi hoặc trùng dữ liệu. Một số ứng dụng nhưTFTP có nhu cầu phải thêm những kỹ thuật làm tin cậy cơ bản vào tầng ứng dụng. Hầu hết các ứng dụng UDP không cần những kỹ thuật làm tin cậy này và đôi khi nó bị bỏ đi. Streaming media, game trực tuyến và voice over IP (VoIP) là những thí dụ cho các ứng dụng thường dùng UDP. Nếu một ứng dụng

đòi hỏi mức độ cao hơn về tính tin cậy, những giao thức nhưTCP hoặc mã erasure có thể được sử dụng để thay thế.

Thiếu những cơ chế kiểm soát tắc nghẽn và kiểm soát luồng, các kỹ thuật dựa trên mạng là cần thiết để giảm nguy hiệu ứng cơ tắc nghẽn dây chuyền do không kiểm soát, tỷ lệ tải UDP cao. Nói cách khác, vì người gởi gói UDP không thể phát hiện tắc nghẽn, các thành phần dựa trên mạng như router dùng hàng đợi gói (packet queueing) hoặc kỹ thuật bỏ gói như là những công cụ để giảm tải của UDP. Giao thức Datagram Congestion Control Protocol (DCCP) được thiết kế như một giải pháp cho vấn đề bằng cách thêm hành vi kiểm soát tắc nghẽn cho thiết bị đầu cuối cho các dòng dữ liệu UDP như streaming media.

Mặc dù tổng lượng lưu thông của UDP trên mạng thường chỉ vài phần trăm, nhưng có nhiều ứng dụng quan trọng dùng UDP, bao gồm DNS, SNMP, DHCP và RIP.

Tham khảo cổng kết nối TCP/ UDP trên Internet

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

3.3. Các giao thức liên quan khác

Mỗi kiến trúc mạng sử dụng bộ giao thức chuẩn khác nhau; có nhiều giao thức liên quan tương ứng (để tương thích trong truyền thông)

Giao thức chủ đạo TCP/IP; bộ giao thức này có một số giao thức chuẩn liên quan để hỗ trợ trong truyền thông mạng máy tính

Giao thức ARP/ RARP

Nguyên tắc làm việc của ARP trong một mạng LAN

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng network (IP, IPX…) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng network của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một gói tin (trong đó có chứa địa chỉ MAC của mình). Trong một hệ thống mạng đơn giản, ví dụ như PC A muốn gửi gói tin đến PC B và nó chỉ biết được địa chỉ IP của PC B. Khi đó PC A sẽ phải gửi một ARP broadcast cho toàn mạng để hỏi xem "địa chỉ MAC của PC có địa chỉ IP này là gì ?" Khi PC B nhận được broadcast này, nó sẽ so sánh địa chỉ IP trong gói tin này với địa chỉ IP của nó. Nhận thấy địa chỉ đó là địa chỉ của mình, PC B sẽ gửi lại một gói tin cho PC A trong đó có chứa địa chỉ MAC của B. Sau đó PC A mới bắt đầu truyền gói tin cho B.

Nguyên tắc hoạt động của ARP trong môi trường hệ thống mạng:

Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C. Máy A thuộc mạng A muốn gửi gói tin đến máy B thuộc mạng B. Do

các broadcast không thể truyền qua Router nên khi đó máy A sẽ xem Router C như một cầu nối hay một trung gian (Agent) để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (routing table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của Router C. Bảng định tuyến sẽ có chứa địa chỉ IP của port X. Quá trình truyền dữ liệu theo từng bước sau :

Máy A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.

Router C trả lời, cung cấp cho máy A địa chỉ MAC của port X.

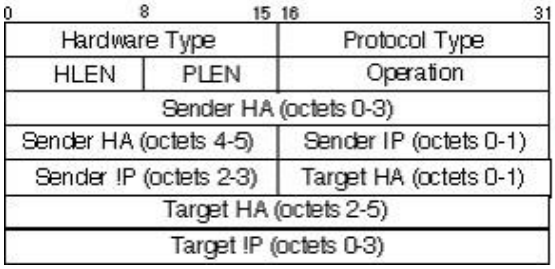
Máy A truyền gói tin đến port X của Router.

Router nhận được gói tin từ máy A, chuyển gói tin ra port Y của Router. Trong gói tin có chứa địa chỉ IP của máy B. Router sẽ gửi ARP request để tìm địa chỉ MAC của máy B.

Máy B sẽ trả lời cho Router biết địa chỉ MAC của mình. Sau khi nhận được địa chỉ MAC của máy B, Router C gửi gói tin của A đến B.

Trên thực tế ngoài dạng bảng định tuyến này người ta còn dùng phương pháp proxyARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác.Theo đó các máy trạm không cần giữ bảng định tuyến nữa Router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy .

Address Resolution Protocol (ARP). Dưới đây là cấu trúc gói tin sử dụng trong giao thức ARP.



Ý nghĩa các trường trong header gói tin ARP:

- Hardware Type:
- xác định kiểu bộ giao tiếp phần cứng máy gửi cần biết
- với giá trị 1 cho Ethernet

Protocol Type:

- Xác định kiểu giao thức địa chỉ cấp cao máy gửi cung cấp
- Có giá trị 080016 cho giao thức IP

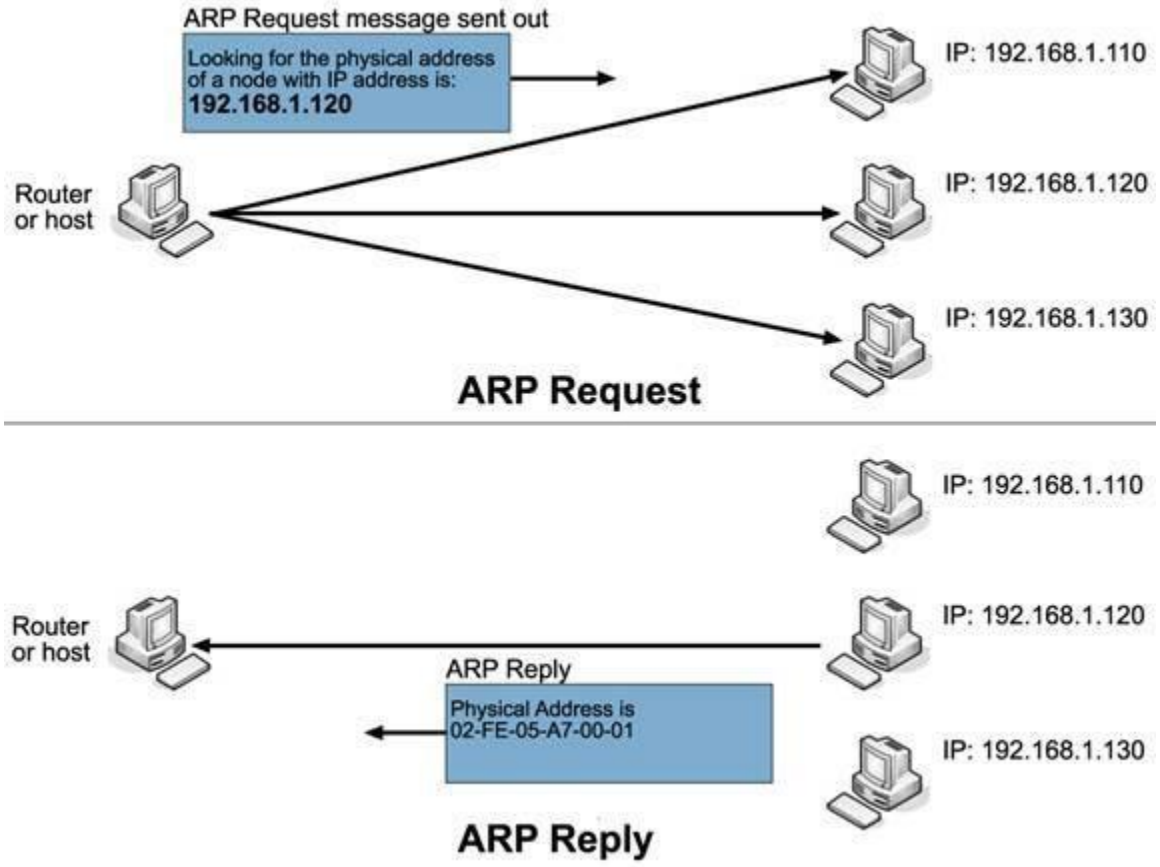
HLEN: độ dài địa chỉ vật lý (bit)

PLEN: độ dài địa chỉ logic (bit)

- 1: là một ARP request.
- 2: là một ARP reply.
- 3: là một RARP request.
- 4: là một RARP reply.

Sender HA (sender hardware address): địa chỉ MAC của máy gửi
Sender Protocol Address: địa chỉ IP máy gửi
Target HA (target hardware address): địa chỉ MAC của máy nhận
Target Protocol Address: địa chỉ IP máy nhận

Vậy cơ chế hoạt động của ARP ra sao?



Thử tưởng tượng bạn bước vào một phòng học và biết được rằng có một bạn gái tên Lina đang ở trong đó. Bạn muốn đến ngồi cạnh để trò chuyện nhưng lại không biết bạn ấy ngồi ở đâu. Khi ấy giải pháp đơn giản chúng ta sẽ thực hiện là đứng lên nói cho tất cả mọi người cùng nghe: "xin cho hỏi bạn Lina đang ngồi ở vị trí nào ạ?" Sau khi bạn Lina nghe thấy như vậy sẽ giơ tay cho biết vị trí bạn ấy đang ngồi. Sau khi đã biết vị trí của Lina bạn sẽ lại gần bạn ấy và cuộc trò chuyện bắt đầu.

Trong môi trường mạng LAN cũng như vậy. Và đây là cách hoạt động của ARP.

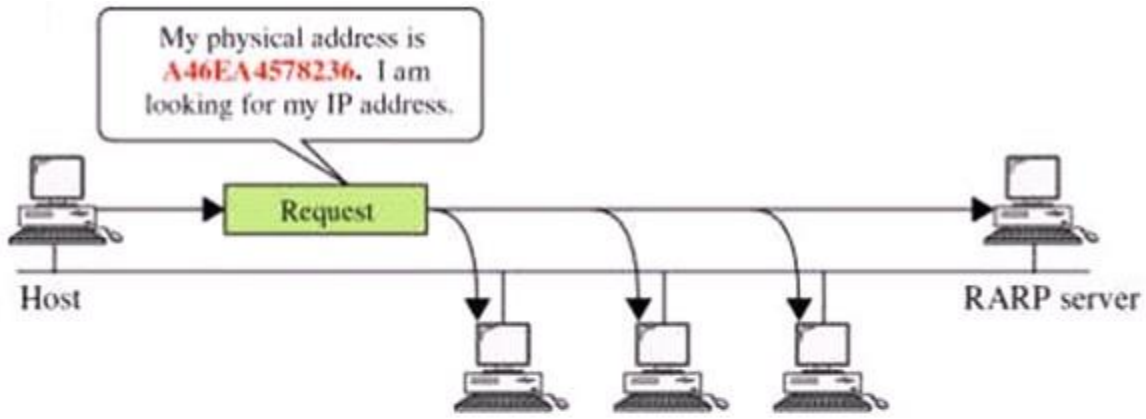
- Bước 1: Thiết bị A sẽ kiểm tra cache của mình (giống như quyển sổ danh bạ nơi lưu trữ tham chiếu giữa địa chỉ IP và địa chỉ MAC). Nếu đã có địa chỉ MAC của IP 192.168.1.120 thì lập tức chuyển sang bước 9.
- Bước 2: Bắt đầu khởi tạo gói tin ARP Request. Nó sẽ gửi một gói tin broadcast đến toàn bộ các máy khác trong mạng với địa chỉ MAC và IP máy gửi là địa chỉ của chính nó, địa chỉ IP máy nhận là 192.168.1.120, và địa chỉ MAC máy nhận là ff:ff:ff:ff:ff:ff.
- Bước 3: Thiết bị A phân phát gói tin ARP Request trên toàn mạng. Khi switch nhận được gói tin broadcast nó sẽ chuyển gói tin này tới tất cả các máy trong mạng LAN đó.

- Bước 4: Các thiết bị trong mạng đều nhận được gói tin ARP Request. Máy tính kiểm tra trường địa chỉ Target Protocol Address. Nếu trùng với địa chỉ của mình thì tiếp tục xử lý, nếu không thì hủy gói tin.
- Bước 5: Thiết bị B có IP trùng với IP trong trường Target Protocol Address sẽ bắt đầu quá trình khởi tạo gói tin ARP Reply bằng cách:
- lấy các trường Sender Hardware Address và Sender Protocol Address trong gói tin ARP nhận được đưa vào làm Target trong gói tin gửi đi.
- Đồng thời thiết bị sẽ lấy địa chỉ MAC của mình để đưa vào trường Sender Hardware Address
  Bước 6: Thiết bị B đồng thời cập nhật bảng ánh xạ địa chỉ IP và MAC của thiết bị nguồn vào bảng ARP cache của mình để giảm bớt thời gian xử lý cho các lần sau (hoạt động cập nhật danh bạ).
  Bước 7: Thiết bị B bắt đầu gửi gói tin Reply đã được khởi tạo đến thiết bị A.
  Bước 8: Thiết bị A nhận được gói tin reply và xử lý bằng cách lưu trường Sender Hardware Address trong gói reply vào địa chỉ phần cứng của thiết bị B.
  Bước 9: Thiết bị A update vào ARP cache của mình giá trị tương ứng giữa địa chỉ IP (địa chỉ network) và địa chỉ MAC (điac chỉ datalink) của thiết bị B. Lần sau sẽ không còn cần tới request. Như vậy máy A đã biết được địa chỉ MAC của máy B, tương tự như việc chúng ta đã biết địa chỉ cụ thể của ai đó. Và khi A cần gửi một gói tin cho B thì sẽ điền địa chỉ này vào trường Target Hardware Address. Gói tin sẽ được gửi thằng đến B mà không cần gửi đến các máy khác trong mạng LAN nữa.

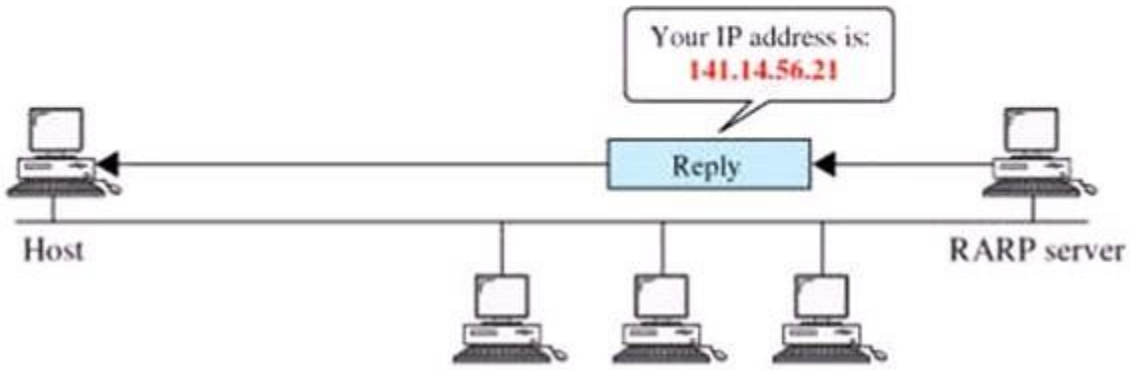
Giao thức RARP

Định Nghĩa : Giao thức RARP (Reverse Address ResolutionProtocol) hay còn gọi là giao thức phân giải địa chỉ ngược là một giao thức được sử dụng bởi một máy chủ yêu cầu giao thức Internet(IPv4) dùng để xác định địa chỉ IP (địa chỉ logic) từ địa chỉ MAC của thiết bị.

Mục Đích : Sử dụng giao thức RARP để tìm địa chỉ IP (Thực chất là việc ánh xạ cho Host một địa chỉ IP) khi đã biết địa chỉ vật lý (MAC) của Host.



RARP request is broadcast



RARP Request Uniscast

Qúa trình thực hiện RARP được bắt đầu khi một máy muốn gửi đi một gói tin đến một máy khác, để làm được điều này trước tiên là máy đó phải xác định được địa chỉ IP của mình trong mạng. Như chúng ta đã biết việc gửi gói tin trong cùng một mạng thông qua Switch là dựa vào địa chỉ MAC tuy nhiên để biết được chúng có cùng trong cùng một mạng hay không thì cần xác định IP của mạng đó, RARP làm nhiệm vụ này.

Khi một máy trong mạng cục bộ gửi yêu cầu xác định địa chỉ IP từ cổng của máy chủ ARP (Address Resolution Protocol) thì chúng sẽ kiểm tra tại các bảng hoặc bộ nhớ đệm (Cache) tại đó. Một quản trị mạng (Network Administrator) có trách nhiệm tạo ra bảng tại cổng định hướng của mạng cục bộ này. Bảng này sẽ ánh xạ địa chỉ MAC của máy sang địa chỉ IP tương ứng.

Khái niệm RARP Server: Tất cả ánh xạ giữa địa vật lý (MAC) với địa chỉ logic(IP) của các Hosts được lưu trữ vào tệp cấu hình của một Host nào đó trong mạng. Host này được gọi là RARP Server. Host này đáp ứng tất cả các yêu cầu của RARP Request. Còn tệp cấu hình này nằm trên vùng đĩa cứng của RARP Server.

RARP Client : là một hệ thống máy tính không đĩa (Hosts), nơi phát ra các yêu cầu để xác định IP của Host với đầu vào là địa chỉ MAC.

Hoạt động:

- Khi một hệ thống không đĩa khởi động, nó phát đi một gói tin Broadcast yêu cầu RARP với địa chỉ MAC của nó. Gói tin này được nhận bởi tất cả các Hosts trong mạng. Khi RARP Server nhận được gói tin này nó nhìn lên địa chỉ MAC trong tệp cấu hình và xác định địa chỉ IP tương ứng.

Sau đó nó gửi địa chỉ IP trong gói trả lời tin RARP (RARP Reply) và chỉ gửi từ một Host đến Host đích cần tới vì vậy gọi là gói Unicast. Hệ thống không đĩa ban đầu nhận được gói tin này và có được địa chỉ IP.

- Một gói tin RARP Request thường được được tạo ra trong quá trình khởi động của Host. Khi RARP Server nhận được gói RARPRequest, nó thực hiện các bước sau.
- Địa chỉ MAC trong gói tin yêu cầu được tìm kiếm trong tệp cấu hình, và được ánh xạ sang địa chỉ IP tương ứng .
- Nếu việc ánh xạ không tìm thấy thì gói tin sẽ bị loại.
- Nếu việc ánh được tìm thấy, một gói tin RARP Reply được tạo ra với địa chỉ MAC và IP của máy nguồn. Sau đó gói này được gửi trả lại Host mà đã đưa ra gói RARP Request.

Lúc này khi Host nhận được RARP Reply, nó nhận được địa chỉ IP từ gói tin RARP ban đầu và hoàn tất quá trình khởi động (Boot), địa chỉ IP được sử dụng để giao tiếp với các Hosts khác trong mạng cho đến khi nó khởi động lại.

Một số đặc điểm của giao thức RARP:

- Giao thức này xuất hiện đầu tiên trong việc giải quyết nhiệm vụ ánh xạ từ địa chỉ vật lý sang địa chỉ logic.
- Sử dụng trong các hệ thống không có đĩa (DisklessWorkstation).
- Sử dụng nhiều trong các mạng LAN qui mô nhỏ, đặc biệt là trong mạng Ethernet .
- Hiện tại RARP không còn sử dụng nữa mà đã thay thế bằng giao thức khác đó là BOOTP và DHCP. Chúng ta sẽ cùng tìm hiểu những giao thức này trong bài viết sau.
- RARP cùng với ARP nằm trên lớp DataLink Layer của mô hình OSI .

+ HTTP (HTTPS), DNS, DHCP, FTP, POP3, SMTP, TELNET, SSH, IMAP4,….

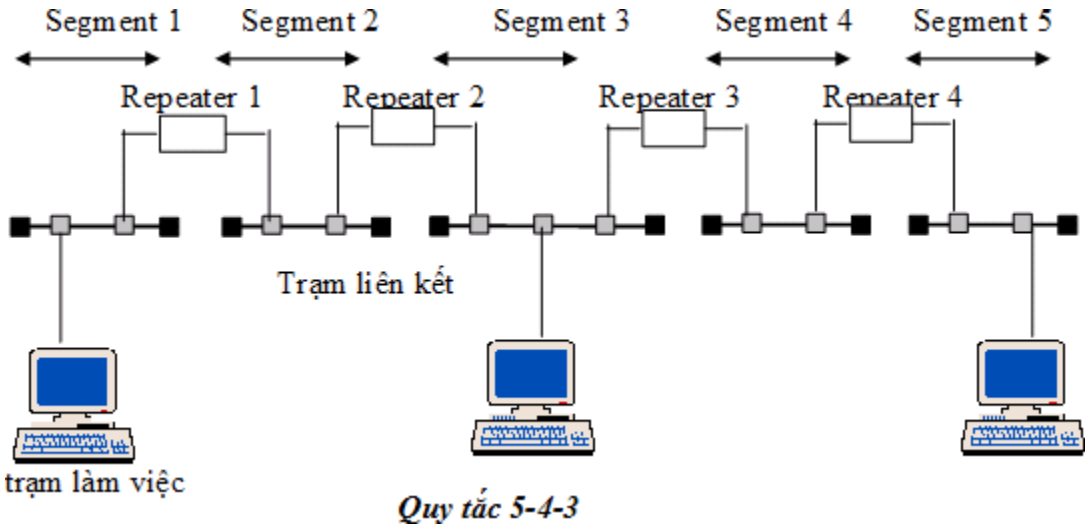
Tham khảo thêm phụ lục 1

Chương 4. CÔNG NGHỆ TRUYỀN THÔNG LIÊN MẠNG

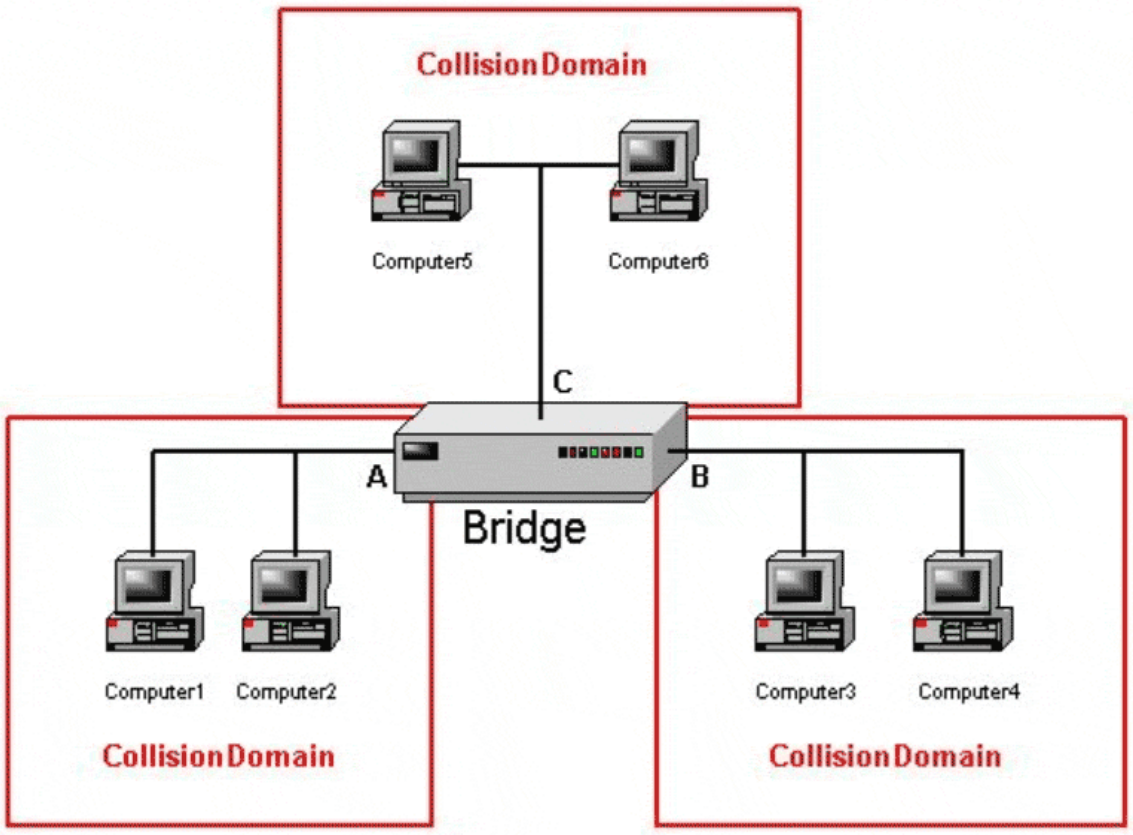
4.1. Các thiết bị liên kết mạng

4.1.1. Mở rộng và liên kết các mạng cục bộ

+ **Mở rộng theo quy tắc Cisco:** Mở rộng bằng cách thêm các thiết bị liên kết trong LAN



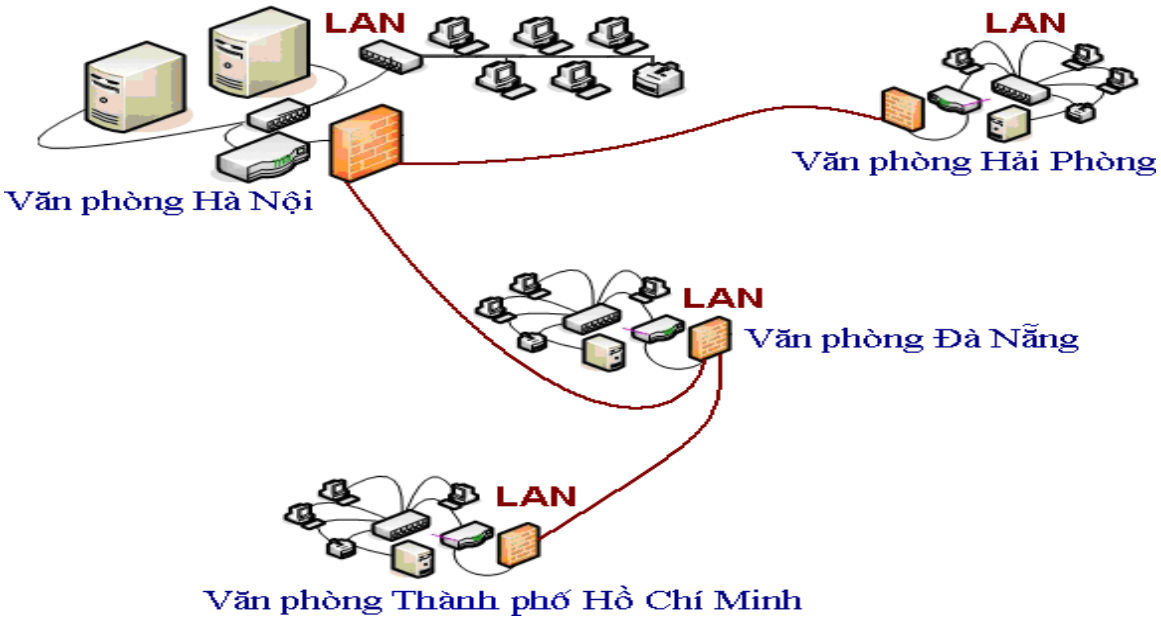
Quy tắc 5-4-3



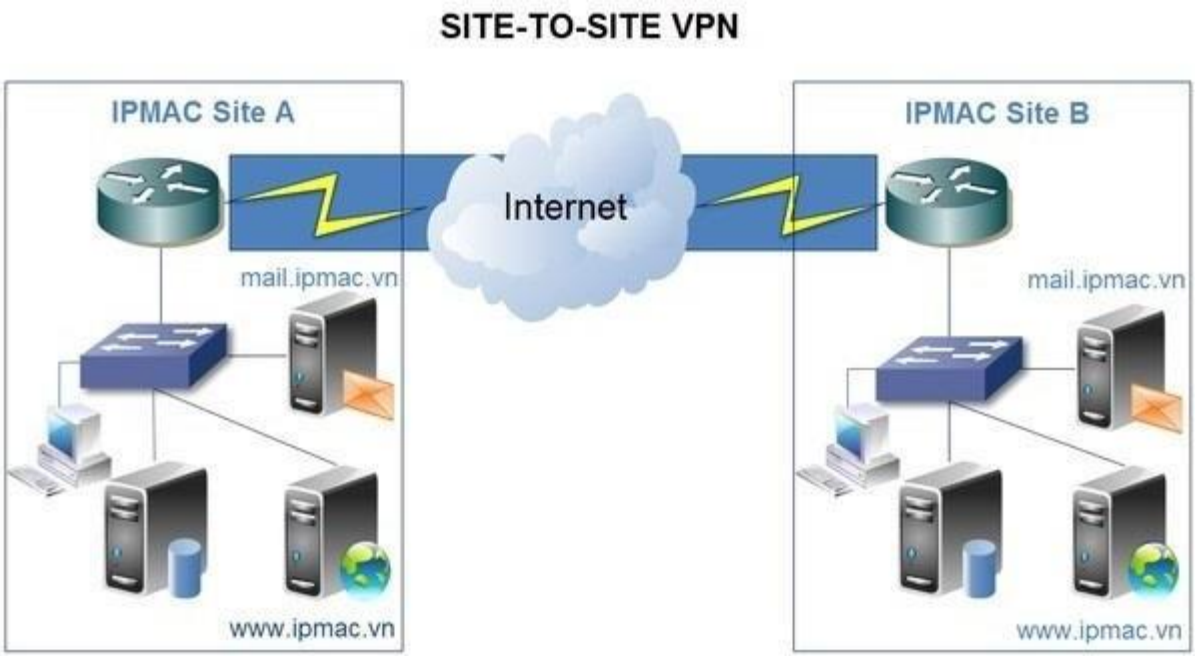
+ Mở rộng mạng WIFI (WLAN)

Cần thiết bị chuyển tiếp sóng

+ Mở rộng kết nối nhiều MAN tạo thành WAN



+ Mở rộng mạng WAN qua đường Internet (VPN- Mạng riêng ảo)



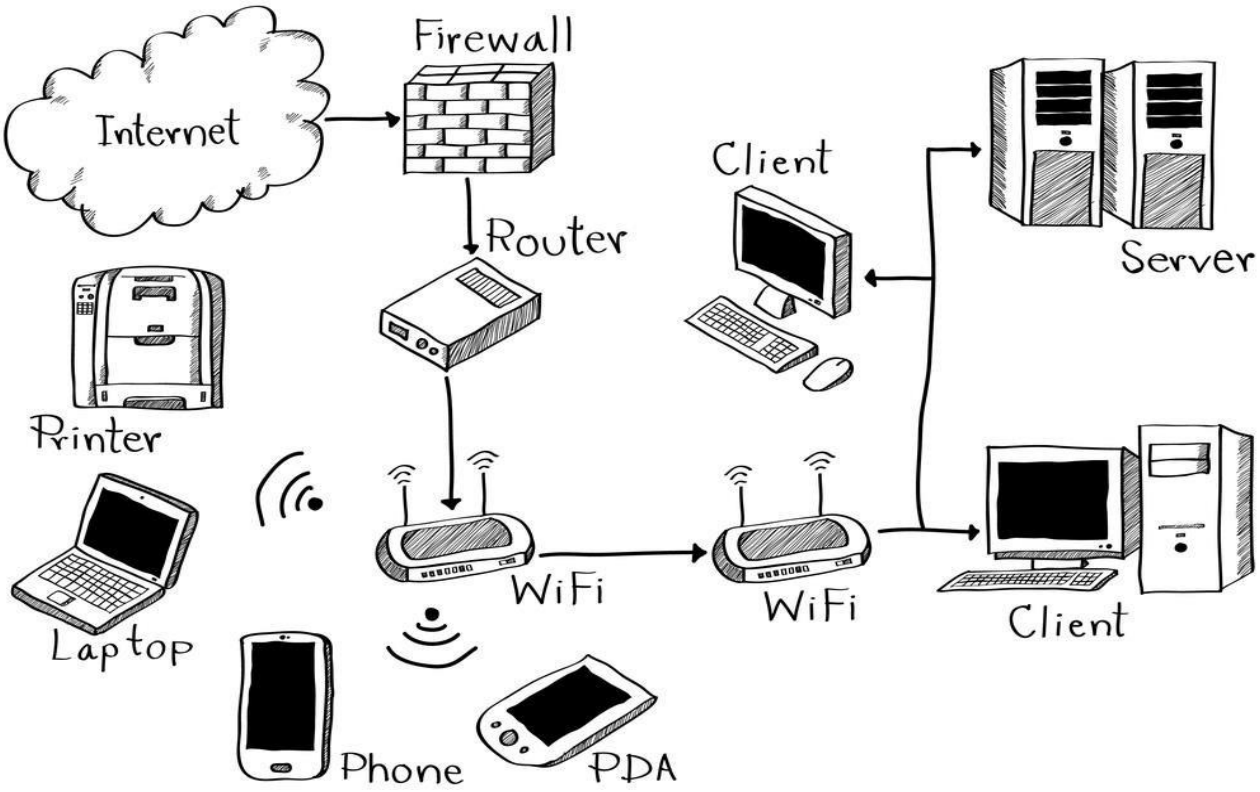
+ Mô hình mở rộng mạng kết nối đa thiết bị

Cho phép các thiết bị kết nối với nhau thông qua nhiều kênh truyền dẫn Hồng ngoại; Wifi, Bluetooth, GSM, được phép shared tài nguyên mạng và kết nối tới các dịch vụ tích hợp như điện toán đám maay (cloud) và chia sẻ đường truyền Internet.

+ Mở rộng mạng kết nối với thiết bị thông minh:

Các thiết bị kết nối SmartTV; smartphone; Ipad, Mobile,…


SMARTPHONE
LAPTOP
TABLET
INTERNET
Hệ thống điện
An ninh
Hệ thống camera
Báo cháy
LAN
Điều hòa nhiệt độ
Hệ thống giải trí
Hệ thống chiếu sáng
Hệ thống tưới cây
Thiết bị nhà bếp
Hệ thống kiểm soát ra vào
BỘ XỬ LÝ TRUNG TÂM
Hệ thống cấp thoát nước
www.vinteligroup.com



4.1.2. Vai trò của các thiết bị liên kết mạng

Các thiết bị liên kết mạng là thiết bị trung gian, có nhiệm vụ tạo ra kết nối vật lý gữa các mạng (không dây hoặc có dây), đảm baaor một mậng rộng hơn kết nối tương thích với nhau theo một thiết kế nào đó.

+ Repeater chính là thiết bị có khả năng khuếch đại, truyền tín hiệu xa và ổn định hơn. Trong mô hình OSI thì thiết bị này nằm ở lớp 1. Nguyên lý hoạt động của thiết bị này đó là sẽ giúp những tín hiệu vật lý ở đầu vào được khuếch đại. Từ đó sẽ giúp đường truyền sóng wifi được mạnh và đến những thiết bị nằm cách xa Modem wifi.

Chính vì vậy, nếu bạn sử dụng máy tính trong không gian lớn và muốn tốc độ truy cập internet bằng wifi được mạnh thì nên chọn Repeater. Thiết bị này sẽ giúp tốc độ truy cập internet nhanh hơn ngay cả ở những vị trí xa

+ HUB/ Switch Bộ tập trung – liên kết các máy với nhau theo kết nối hình sao (Star Topology)

Hub là thiết bị nhiều cổng và được ví như một Repeater nhiều cổng, có khả năng truyền tín hiệu tới nhiều thiết bị khác nhau. Nghĩa là nếu một cổng trên Hub được truyền tín hiệu thì những cổng khác cũng sẽ nhận được thông tin ngay lập tức.

Trên thị trường hiện nay có 2 loại Hub phổ biến đó là Active Hub và Smart Hub, mỗi loại sẽ có những đặc điểm và tính năng riêng. Ví dụ như Active Hub có khả năng khuếch đại tín hiệu, giúp tốc độ truyền tin được ổn định. Smart Hub cũng có những tính năng tương tự như Active Hub nhưng còn có khả năng dò lỗi trên mạng một cách tự động.

Switch có khả năng kết nối được nhiều hơn tùy thuộc vào số cổng có trên thiết bị này. Chức năng chính của thiết bị Switch đó là chuyển dữ liệu từ nguồn đến đích và xây dựng các bảng Switch.

+ Bridge: Liên kết các đoạn mạng LAN tạo ra mạng lớn hơn (MAN)

Bridge nằm ở lớp thứ hai trong mô hình OSI. Chức năng của thiết bị mạng này chính là để nối hai mạng Ethernet với nhau để tạo thành một mạng lớn. Nghĩa là Bridge sẽ giúp sao chép lại gói tin và chuyển dữ liệu tới máy tính cần nhận kể cả khi hai máy tính này lại sử dụng hai mạng khác nhau.

Tóm lại, cho dù bạn sử dụng nhiều hệ thống mạng khác nhau nhưng chỉ Bridge thì những tín hiệu vẫn có thể trao đổi qua lại một cách dễ dàng. Không chỉ có khả năng kết nối hai mạng với nhau mà Bridge còn có thể xử lý được nhiều luồng thông tin từ nhiều mạng khác nhau trong cùng một lúc.

+ Router: Thiết bị cho phép định tuyến; tìm đường đi cho dữ liệu trong một mang lớn đảm baaor các gói tin đến đích một cách nhanh nhất

Trong mô hình OSI thì Router nằm ở lớp thứ 3. Hay còn gọi là thiết bị định tuyến hay bộ định tuyến, thiết bị này dùng để đóng gói và chuyển các gói dữ liệu từ một liên mạng đến các thiết bị đầu cuối.

Router wifi: Đối với thiết bị này thường sẽ có các cổng LAN, cổng WAN, đặc biệt hơn sẽ có thêm cổng USB để chia sẻ dữ liệu trực tuyến.

+ Gateway

Chức năng chính của thiết bị mạng Gateway là kết nối các máy tính với nhau một cách dễ dàng ngay cả khi những thiết bị này không sử dụng chung một giao thức. Ví dụ như Gateway có thể kết nối máy tính sử dụng giao thức IP với máy tính sử dụng giao thức SNA, IPX,..

Ngoài ra, thiết bị này còn có khả năng phân biệt các giao thức. Vì vậy, thường được ứng dụng trong việc chuyển thư điện tử từ mạng này sang mạng khác kể cả đường truyền xa.

Chức năng của Gateway trong hệ thống mạng IP [01/06/2015]

Gateway là một phần tử không nhất thiết phải có trong một giao tiếp H.323. Nó đóng vai trò làm phần tử cầu nối và chỉ tham gia vào một cuộc gọi khi có sự chuyển tiếp từ mạng H.323 (ví dụ như mạng LAN hay mạng Internet) sang mạng phi H.323 (ví dụ mạng chuyển kênh hay PSTN). Một **Gateway** có thể kết nối vật lý với một hay nhiều mạng IP hay với một hay nhiều mạng chuyển mạch kênh. Một Gateway có thể bao gồm: Gateway báo hiệu, Gateway truyền tải kênh thoại, Gateway điều khiển truyền tải kênh thoại. Một hay nhiều chức năng này có thể thực hiện trong một Gatekeeper hay một Gateway khác.

- Gateway báo hiệu SGW: cung cấp kênh báo hiệu giữa mạng IP và mạng chuyển mạch kênh. Gateway báo hiệu là phần tử trung gian chuyển đổi giữa báo hiệu trong mạng IP (ví dụ H.323) và báo hiệu trong mạng chuyển mạch kênh (ví dụ R2, CCS7). Gateway báo hiệu có các chức năng sau:

- Chức năng kết nối các giao thức điều khiển cuộc gọi.
- Chức năng kết cuối báo hiệu từ mạng chuyển mạch kênh: phối hợp hoạt động với các chức năng báo hiệu của Gateway điều khiển truyền tải kênh thoại.
- Chức năng báo hiệu: chuyển đổi báo hiệu giữa mạng IP với báo hiệu mạng chuyển mạch kênh phi phối hợp hoạt động với**Gateway** điều khiển truyền tải kênh thoại.
- Chức năng giao diện mạng chuyển mạch gói: kết cuối mạng chuyển mạch gói.
- Chức năng bảo mật kênh báo hiệu: đảm bảo tính bảo mật của kênh báo hiệu nối với thiết bị đầu cuối.
- Chức năng quản lý: giao tiếp với hệ thống quản lý mạng.
- Chức năng ghi các bản tin sử dụng: xác định hoặc ghi lại các thông tin về sự kiện (truy nhập, cảnh báo) và tài nguyên.
- Chức năng báo cáo các bản tin sử dụng: báo các các bản tin đã được sử dụng ra thiết bị ngoại vi.

Gateway truyền tải kênh thoại MGM: cung cấp phương tiện để thực hiện chức năng chuyển đổi mã hóa. Nó sẽ chuyển đổi giữa các mã hóa trong mạng IP với các mã hóa truyền trong mạng chuyển mạch kênh. Gateway truyền tải kênh thoại bao gồm các khối chức năng sau:

- Chức năng chuyển đổi địa chỉ kênh thông tin: cung cấp địa chỉ IP cho các kênh thông tin truyền và nhận.
- Chức năng chuyển đổi luồng: chuyển đổi giữa các luồng thông tin giữa mạng IP và mạng chuyển mạch kênh bao gồm việc chuyển đổi mã hóa và triệt tiếng vọng.
- Chức năng dịch mã hóa: định tuyến các luồng thông tin giữa mạng IP và mạng chuyển mạch kênh.
- Chức năng giao diện với mạng chuyển mạch kênh: kết cuối và điều khiển các kênh mang thông tin từ mạng chuyển mạch kênh.
- Chức năng chuyển đổi kênh thông tin giữa mạng IP và mạng chuyển mạch kênh: chuyển đổi giữa kênh mang thông tin thoại, Fax, dữ liệu của mạng chuyển mạch kênh và các gói dữ liệu trong mạch IP. Nó cũng thực hiện các chức năng xử lý tín hiệu thích hợp như: nén tín hiệu thoại, triệt tiếng vọng, mã hóa, chuyển đổi tín hiệu Fax và điều tiết tốc độ modem tương tự. Thêm vào đó, nó còn thực hiện việc chuyển đổi giữa tín hiệu mã đa tần DTMF trong mạng chuyển mạch kênh và các tín hiệu thích hợp trong mạng điện thoại IP khi các bộ mã hóa tín hiệu thoại không mã hóa tín hiệu mã đa tần DTMF. Chức năng chuyển đổi kênh thông tin giữa mạng IP và mạng chuyển mạch kênh cũng có thể thu nhập thông tin về lưu lượng gói và chất lượng kênh đối với mỗi cuộc gọi để sử dụng trong việc báo cáo chi tiết và điều khiển cuộc gọi.
- Chức năng quản lý: giao tiếp với hệ thống quản lý mạng.
- Chức năng ghi các bản tin sử dụng: xác định hoặc ghi lại các thông tin về sự kiện (truy nhập, cảnh báo) và tài nguyên.
- Chức năng báo cáo các bản tin sử dụng: báo cáo các bản tin đã được sử dụng ra thiết bị ngoại vi.

Gateway điều khiển truyền tải kênh thoại MGWC: đóng vai trò phần tử kết nối giữa Gateway báo hiệu và Gatekeeper. Nó cung cấp chức năng xử lý cuộc gọi cho Gateway, điều khiển Gateway truyền tải kênh thoại, nhận thông tin báo hiệu của mạng chuyển mạch

kênh từ Gateway báo hiệu và thông tin báo hiệu của mạng IP từ Gatekeeper. **Gateway** điều khiển truyền tải kênh thoại bao gồm các chức năng sau:

- Chức năng truyền và nhận các bản tin
- Chức năng xác nhận: thiết lập các đặc điểm nhận dạng của người sử dụng, thiết bị hoặc các phần tử mạng.
- Chức năng điều khiển cuộc gọi: lưu giữ các trạng thái cuộc gọi của Gateway. Chức năng này bao gồm tất cả các điều khiển kết nối logic của Gateway.
- Chức năng báo hiệu: chuyển đổi giữa báo hiệu mạng IP và báo hiệu mạng chuyển mạch kênh trong quá trình phối hợp hoạt động với **Gateway** báo hiệu.
- Chức năng quản lý: giao tiếp với hệ thống quản lý mạng.
- Chức năng ghi các bản tin sử dụng: xác định hoặc ghi lại các thông tin về sự kiện (truy nhập, cảnh báo) và tài nguyên.
- Chức năng báo cáo các bản tin sử dụng: báo cáo các bản tin đã được sử dụng ra thiết bị ngoại vi.

+ **Modem:** là thiết bị kết nối Internet

Modem là thiết bị giao tiếp với mạng lưới của các nhà cung cấp dịch vụ Internet (ISP) thông qua hệ thống cáp nối đồng trục, cáp quang hay đường dây điện thoại (DSL). Đây chính là cánh cổng để giúp bạn kết nối với internet quốc tế.

Chức năng Modem

Modem là viết tắt của từ "modulator và demodulator" có nghĩa là thiết bị mã hóa và giải mã các xung điện, mang nhiệm vụ chuyển tín hiệu số của máy tính, điện thoại thành tín hiệu tương tự mà hạ tầng Internet toàn cầu đang sử dụng và ngược lại.

Nói rõ hơn, modem đóng vai trò chuyển hóa các gói dữ liệu do ISP cung cấp thành kết nối Internet cho router hoặc các thiết bị có liên kết mạng khác qua địa chỉ IP.

Modem wifi: Đa số các modem wifi mà các nhà cung cấp dịch vụ Internet hiện này cấp cho khách hàng đều có tích hợp tính năng phát wifi để người dùng tiện lợi sử dụng và tiết kiệm thêm chi phí mua thêm router wifi.

Access Point:

Access point WiFi repeater: kích sóng, mở rộng mạng qua sóng Wifi

Access point là gì? Access point (AP) là một thiết bị tạo ra một mạng không dây cục bộ, hoặc WLAN, thường trong một văn phòng hoặc tòa nhà lớn. Một điểm truy cập access point là một trạm truyền và nhận dữ liệu. Có thể gọi chúng là bộ thu phát wifi.

Một điểm truy cập Access Point kết nối người dùng với những người dùng khác trong cùng một mạng. Ngoài ra chúng còn đóng vai trò là điểm kết nối giữa mạng WLAN và mạng dây cố định. Trong một khu vực mạng được xác định thì mỗi điểm truy cập Access Point có thể phục vụ

nhiều người dùng. Nếu khi mọi người di chuyển ra ngoài phạm vi của một điểm truy cập, thì chúng sẽ tự động được chuyển sang điểm tiếp theo.

Firewall:

Tường lửa Firewall là gì?

Tường lửa (Firewall) là một hệ thống an ninh mạng, có thể dựa trên phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát traffic vào, ra khỏi hệ thống. Tường lửa hoạt động như một rào chắn giữa mạng an toàn và mạng không an toàn. Nó kiểm soát các truy cập đến nguồn lực của mạng thông qua một mô hình kiểm soát chủ động. Nghĩa là, chỉ những traffic phù hợp với chính sách được định nghĩa trong tường lửa mới được truy cập vào mạng, mọi traffic khác đều bị từ chối.

Bất kì máy tính nào kết nối tới Internet cũng cần có firewall, giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng. Việc có một "người gác cổng" như vậy để giám sát mọi việc xảy ra rất quan trọng bởi 2 lý do:

Thứ nhất, bất kì máy tính kết nối mạng nào thường kết nối vĩnh viễn với Internet. Thứ 2, mỗi máy tính trực tuyến lại có một chữ ký điện tử riêng, được gọi là **Internet Protocol address** (hay còn gọi là địa chỉ IP): Nếu không có firewall hỗ trợ, nó chẳng khác gì chuyện bạn bật tất cả đèn lên và mở rộng cửa để đón trộm vào.

Một firewall được cấu hình chính xác sẽ ngăn chặn điều này xảy ra và giúp máy tính "ẩn" một cách hiệu quả, cho phép người dùng thoải mái thưởng thức những gì thế giới trực tuyến mang lại. Firewall không giống chương trình diệt virus. Thay vào đó, nó làm việc cùng với những công cụ này nhằm đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến.

Firewall hoạt động như thế nào?

Công việc của một firewall khá khó khăn, bởi có rất nhiều dữ liệu hợp pháp cần được cấp phép cho ra hoặc vào máy tính kết nối mạng. Ví dụ, khi chúng ta truy cập vào trang web Quantrimang.com, đọc tin tức, tips công nghệ mới thì thông tin và dữ liệu của trang web cần được truyền từ và tới máy thông qua mạng để hoàn thành quá trình này.

Một firewall cần biết được sự khác biệt giữa lưu lượng hợp pháp như trên với những loại dữ liệu gây hại khác.

Firewall sử dụng rule hoặc ngoại lệ để làm việc với những kết nối tốt và loại bỏ những kết nối xấu. Nhìn chung, quá trình này được thực hiện ẩn, người dùng không thấy được hoặc không cần tương tác gì cả.

Tường lửa có trạng thái (Stateful firewall)

Khi tường lửa được tạo ra lần đầu tiên, chúng không có trạng thái, nghĩa là phần cứng mà lưu lượng truy cập đi qua trong khi được kiểm tra sẽ theo dõi từng gói lưu lượng mạng riêng và chặn hoặc cho phép nó.

Bắt đầu từ giữa đến cuối những năm 1990, những tiến bộ đầu tiên về tường lửa đã được ra đời. Tường lửa có trạng thái kiểm tra lưu lượng truy cập, liên quan đến trạng thái hoạt động và đặc điểm kết nối

mạng để cung cấp tường lửa toàn diện hơn. Việc duy trì trạng thái này cho phép tường lửa cho lưu lượng nhất định truy cập đến người dùng cụ thể trong khi chặn lượng truy cập tương tự đến người dùng khác.

Tường lửa thế hệ tiếp theo (Next-generation firewalls - NGFW)

Qua nhiều năm tường lửa đã bổ sung thêm vô số tính năng mới, bao gồm phân tích sâu các gói (Deep Packet Inspection - DPI), phát hiện xâm nhập, ngăn và kiểm tra lưu lượng được mã hóa. Tường lửa thế hệ tiếp theo đề cập đến tường lửa được tích hợp nhưng tính năng tiên tiến này.

Tường lửa dựa trên proxy (Proxy-based firewall)

Các tường lửa này hoạt động như một cổng nối giữa những người dùng cuối yêu cầu dữ liệu và nguồn của dữ liệu đó. Tất cả lưu lượng truy cập được lọc qua proxy này trước khi được chuyển cho người dùng cuối. Điều này nhằm bảo vệ máy khách khỏi tiếp xúc với các mối đe dọa bằng cách che giấu danh tính của người yêu cầu thông tin ban đầu.

Tường lửa ứng dụng web (Web application firewall - WAF)

Các tường lửa được sử dụng cho các ứng dụng cụ thể thay vì được đặt trên một điểm vào hoặc ra của một mạng lưới rộng hơn. Trong khi các tường lửa dựa trên proxy thường bảo vệ máy khách người dùng cuối, thì tường lửa ứng dụng web bảo vệ máy chủ ứng dụng.

Phần cứng tường lửa

Phần cứng tường lửa thường là một máy chủ đơn giản có thể hoạt động như một router lọc lưu lượng truy cập và chạy phần mềm tường lửa. Những thiết bị này được đặt ở trong mạng công ty, giữa router và điểm kết nối của nhà cung cấp dịch vụ Internet. Một doanh nghiệp có thể triển khai hàng chục tường lửa vật lý trong một trung tâm dữ liệu. Người dùng cần xác định dung lượng thông qua mà họ cần tường lửa hỗ trợ dựa trên kích thước cơ sở người dùng và tốc độ kết nối Internet.

Phần mềm tường lửa

Thông thường người dùng cuối triển khai nhiều điểm cuối phần cứng tường lửa và hệ thống phần mềm tường lửa trung tâm để quản lý việc triển khai. Hệ thống trung tâm này là nơi các chính sách và tính năng được cấu hình, nơi có thể thực hiện phân tích và phản hồi lại các mối đe dọa.

4.1.3. Một số thiết bị điển hình

(1) Hub

Hình 4.? Thiết bị HUB

Thông số kỹ thuật:
Số Port/ Link up port
Speed: 10Mbps
Nguồn: DC 5v

(2) Switch

Switch 1950 48G 2SFP+ 2XGT PoE+, JG963A

Hình 4.? thiết bị HUB

Thông tin sản phẩm Thiết bị chuyển mạch HPE Switch 1950 48G 2SFP+ 2XGT PoE+, JG963A

Differentiator
Smart web-managed PoE-enabled Gigabit Ethernet switch with 52 total ports: 48-ports PoE+ Gigabit 10/100/1000, 2-ports 10GBASE-T and 2-ports SFP+. Layer 3 static routing, ACLs, 802.1X network login. PoE+ power budget of 370W. True stacking.

Ports
(48) RJ-45 auto-negotiating 10/100/1000 PoE+ ports
(2) SFP+ fixed 1000/10000 SFP+ ports
(2) RJ-45 1/10GBASE-T ports

Memory and processor
128 MB flash
Packet buffer size: 3 MB
1 GB SDRAM

Latency
100 Mb Latency: < 5 µs
1000 Mb Latency: < 5 µs
10 Gbps Latency: < 1.5 µs

Throughput
up to 130.9 Mpps

Routing/switching capacity
176 Gbps

PoE capability
370 W PoE+

Stacking capabilities
Virtual
4 switches

Management features
IMC - Intelligent Management Center
Limited command-line interface
Web browser
SNMP manager
HTTPS
RMON1
FTP
Supported by HPE IMC and generic SNMP management platforms. Refer to documentation for MIB support details.

Input voltage
100 - 240 VAC, rated (depending on power supply chosen)

Power consumption
470 W (maximum)

(3) Bridger

Hình 4.? Bridge Planet VDSL2 (VC234)

Đặc tính kỹ thuật

Ports	10/100Base-TX: 4 RJ-45, Auto-Negotiation and Auto-MDI/MDI-X
	VDSL: 1 RJ-11, female Phone Jack
	PHONE: 1 RJ-11, Built-in splitters for POTS connection
DIP Switch	4 position DIP switch
Functionality	CO / CPE mode select
	Selectable fast and interleaved mode
	Selectable target 17a / 30a profiles
	Selectable target SNR mode
Encoding	VDSL-DMT: ITU-T G.993.1 VDSL, ITU-T G.997.1, ITU-T G.993.2 VDSL2 (Profile 17a/30a Support)
LED Indicators	One Power
	4 for RJ-11/VDSL2
	1 for per RJ45 10/100Base-TX port
Cabling	Ethernet
	10Base-T: 2-pair UTP Cat.3,4,5 up to 100m (328ft)
	100Base-TX: 2-pair UTP Cat.5, up to 100m (328ft)
	VDSL
	Twisted-pair telephone wires (AWG24 or better) up to 1.4km

Performance (Downstream / Upstream)	17a profile
	300m -> 99/70Mbps
	400m -> 99/60Mbps
	600m -> 90/45Mbps
	800m -> 50/28Mbps
	1000m -> 40/12Mbps
	1200m -> 20/7Mbps
	1400m -> 20/4Mbps
	30a profile
	300m -> 100/100Mbps
	400m -> 90/90Mbps
	600m -> 69/55Mbps
	800m -> 48/9Mbps
Switch Specifications	
Switch Processing Scheme	Store-and-Forward
Address Table	2K entries
Flow Control	Back pressure for half duplex
	IEEE 802.3x Pause Frame for full duplex
Switch fabric	0.8Gbps
Throughput (packet per second)	0.59Mpps
Network cables	10/100Base-TX:
	2-Pair UTP Cat. 3, 4, 5 (100meters, max.)
	EIA / TIA-568 100-ohm STP (100meters, max.)
Standard Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T
	IEEE 802.3u 100Base-TX
	ITU-T: G.993.1 (VDSL), G.997.1, G.993.2 VDSL2 (Profile 17a/30a)
Power Requirements	5V DC, 2A
Power Consumption	7.2 Watts/ 24 BTU
Dimensions	155 x 86 x 26 mm
Weight	368g

(4) Router

Thông số sản phẩm Router Cisco ISR4351/K9

Mã sản phẩm: **Cisco ISR4351 / K9**

Tổng thông lượng: 200 Mb / giây đến 400 Mb / giây

Tổng số cổng WAN hoặc LAN 10/100/1000 trên bo mạch: 3

Cổng dựa trên RJ-45: 3

Cổng dựa trên SFP: 3

Khe cắm mô-đun dịch vụ nâng cao (SM-X): 2

Các khe NIM (Môđun Giao diện Mạng): 3

Khe ISC trên bo mạch: 1

Ký ức: 4 GB (mặc định) / 16 GB (tối đa)

Bộ nhớ flash: 4 GB (mặc định) / 16 GB (tối đa)

Tùy chọn cung cấp điện: Nội bộ: AC, DC (lộ trình) và PoE

Chiều cao rack: 2 RU

Kích thước (H x W x D): 43,9 x 438,15 x 507,2 mm

(5) Access Point

Hình 4.? Bộ thu phat sóng wifi Access Point

Wifi	IEEE 802.11ac/n/a 5GHz IEEE 802.11b/g/n 2.4GHz
Giao tiếp	4 x cổng LAN 10/100/1000Mbps 1 x cổng WAN 10/100/1000Mbps 1 x cổng USB 2.0
Dải tần số	2.4GHz và 5GHz
Button	Nút WPS/Reset Nút Tắt/ Mở Wi-Fi Nút Tắt/ Mở Nguồn
Kích thước	243.5 × 186.5 × 32.7 mm
Bảo hành	24 tháng (thiết bị), 12 tháng (adapter)
Hãng sản xuất	TP-LINK

(6) <u>Kích sóng Repeater Wifi</u>

Hình 4.? Thiết bị kích sóng Repeater Wifi

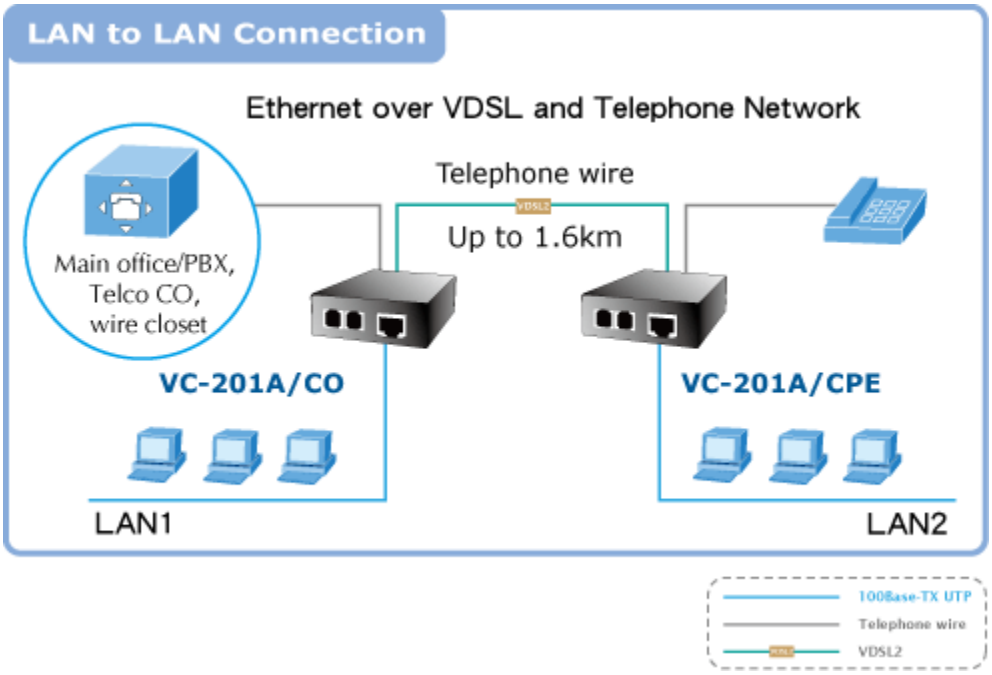
<u>Thông số kỹ thuật</u>

Băng tần 2.4~2.4835GHz
Tốc độ: 300Mbps
Ăng ten: 2 ăng ten 4 dBi
Tính bảo mật cao với WPS

(7) <u>Gateway</u>

Hình 4.? Thiết bị cổng vào/ra mạng gateway

(7) Mở rộng LAN VC-201A



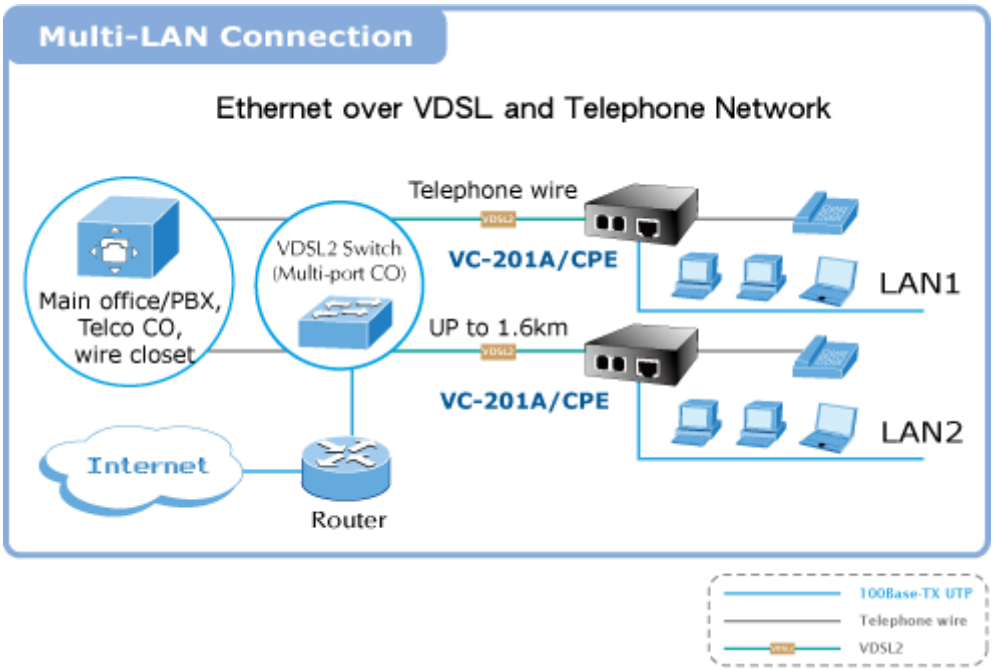
Hình 4.? Mở rộng mạng LAN Thiết bị mạng Planet VC-201A

Mở rộng khoảng cách Ethernet

Hai VC-201A hoạt động như một cặp độc lập tốt cho việc mở rộng khoảng cách Ethernet qua các dây điện thoại hiện có. Chỉ với một cặp dây đồng AWG-24, bạn có thể dễ dàng kết nối hai mạng Ethernet cùng với tốc độ dữ liệu tối đa 100 / 55Mbps. Dịch vụ điện thoại vẫn có thể được sử dụng trong khi các modem đang hoạt động. Hai giải pháp được liệt kê dưới đây là các ứng dụng điển hình cho bộ chuyển đổi Ethernet qua VDSL.

Giải pháp MTU / MDU / Khách sạn

VC-201A là một giải pháp hoàn hảo để nhanh chóng cung cấp các dịch vụ mạng tốc độ cao và hiệu quả về chi phí cho các tòa nhà nhiều tầng như nhà ở (nhà ở nhiều căn hộ), tòa nhà thương mại (các tòa nhà nhiều người), khách sạn hoặc bệnh viện. Bằng cách sử dụng các cơ sở hạ tầng điện thoại hiện có, cài đặt mạng là đơn giản và không đòi hỏi dây mới. Với khả năng truyền tải lên tới 100 / 55Mbps, Video on Demand, điện thoại IP và các dịch vụ băng thông rộng khác nhau có thể dễ dàng được cung cấp.



** Giá sản phẩm trên Tiki đã bao gồm thuế theo luật hiện hành. Tuy nhiên tuỳ vào từng loại sản phẩm hoặc phương thức, địa chỉ giao hàng mà có thể phát sinh thêm chi phí khác như phí vận chuyển, phụ phí hàng cồng kềnh, ..*

(8) Lưu trư mạng QNAP TS-253A-4G

Hìn 4.? Thiết bị lưu trữ QNAP TS-253A-4G

Thông tin sản phẩm Thiết bị lưu trữ QNAP TS-253A-4G

QTS-Linux Combo NAS: a well-rounded Private Cloud solution centralizing storage and IoT applications

Để đáp ứng tốt nhu cầu của thời gian IoT – Internet of Thing sắp tới, TS-253 là mẫu ổ cứng mới, tiên phong hỗ trợ nền tảng mã nguồn mở Linux, xem đây như là 1 gateway để điều khiển từ các thiết bị IoT cho đến thiết bị thông minh khác. TS-253 cho phép User sử dụng các ứng dụng hỗ trợ Linux, trải nghiệm hệ thống Private Cloud kết hợp cac ứng dụng lưu trữ và IoT; các Developer chuyên nghiệp có thể lập trình và chạy các ứng dụng IoT ngay trên TS-253. Tính ổn định, bảo mật đi cùng các tính năng hỗ trợ doanh nghiệp như Volume/LUN Snapshot – cho phép Files/Folder được khôi phục lại phiên bản trước (previous state), trong trường hợp File/Folder bị lỗi. TS-253 được trang bị chip xử lý "khủng" nhất Quad-Core Intel Celeron, cho phép User tận hưởng các Video 4k (chuẩn H.264) và chuyển mã video 1080p/4K theo thời gian thực (real-time) từ TS-253 tới màn hình hiển thị HD/4k.

Hỗ trợ Linux OS và xuất hình ảnh trực tiếp bằng HDMI

Tính năng Dual HDMI để chuyển đổi màn hình, dulicate hoặc thêm màn hình desktop

Tăng cường mã hoá phần cứng với chuẩn AES-NI, hiệu suất mã hoá lên đến 412MB/s

Hỗ trợ thiết bị phần cứng chuyển mã/giải mã video 4K (H.264) với gia thức on-the-fly hoặc cả offline

Tìm kiếm các file nhanh chóng bằng Nature Search với Qsirch 2.1

Giải pháp lưu trữ hợp nhất NAS và iSCSI-SAN, phục vụ cho việc ảo hoá

Hỗ trợ VMware®, Citrix®, Microsoft® Hyper-V và các tính năng ảo hoá nâng cao khác.

Hỗ trợ các giải pháp Hybrid và ảo hoá chỉ với 1 NAS; Virtualzation Station và Container Station.

Khách hang có thể tự xây dựng 1 hệ thống Karaoke cá nhân, với audio chất lượng cao bằng ứng dụng OceanKTV.

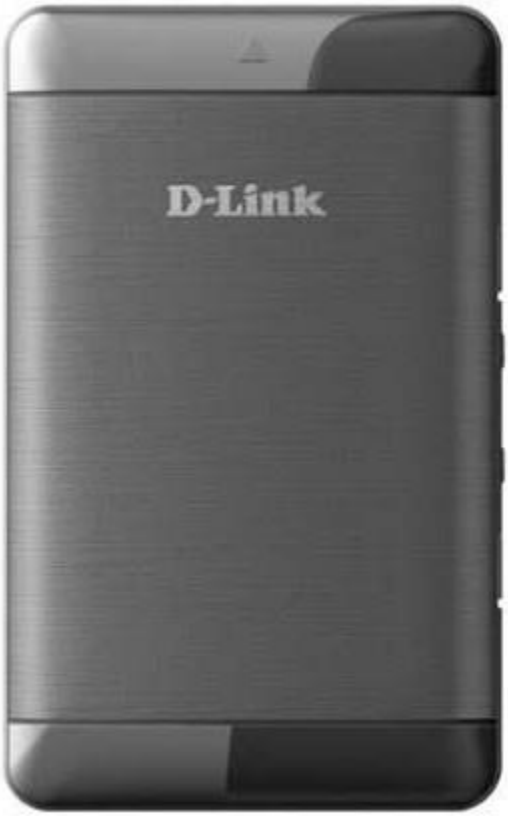
QTS-Linux dual systems, tiến tới kỷ nguyên IoT

Hệ thống dual-system (2 hệ điều hành) QTS-Linux được xây dựng trên nền tảng công nghệ ảo hoá của chính QNAP. Kiến trúc của TS-253 cho phép người dung không chỉ download nhiều ứng dụng trên kho QTS Apps Center, mà còn có thể phát triển hoặc tận dụng các gói IoT cho Linux và hiển thị thông qua HDMi. Với TS-253, người dung có thể phát triển và cài đặt các gói IoT theo nhu cầu và lưu trữ tập trung data trên TS-253. Giờ đây người có thể tận hưởng 1 kho lưu trữ riêng của mình và giải pháp lập trình tiên tiến nhất. Người dung chỉ cần cắm keyboard, chuột và màn hình (hỗ trợ cổng HDMI) vào TS-253 và sử dụng Linux Station như đang dùng trên PC*. Người dung cũng có thể dung Linux Station như là remote desktop thông qua trình duyệt Web cho công việc quản lý

Intel® Celeron® quad-core 1.6GHz CPU đáp ứng hiệu quả nhu cầu xử lý đa tác vụ (Multi-Tasking)

Công nghệ lưu trữ NAS, SAN, DAS

(9) Bộ phát Wifi 3G/4G



Hình 4.? Bộ phát sóng WiFi 3G/4G

Thông số kỹ thuật

Băng tần:	LTE: Band 1,3,7,8,20,38,40. WCDMA B1/B8. GSM: 850/900/1800/1900 MHz
Trọng lượng:	100g
Tốc độ kết nối:	150Mbps Down, 50Mbps Up (LTE Cat

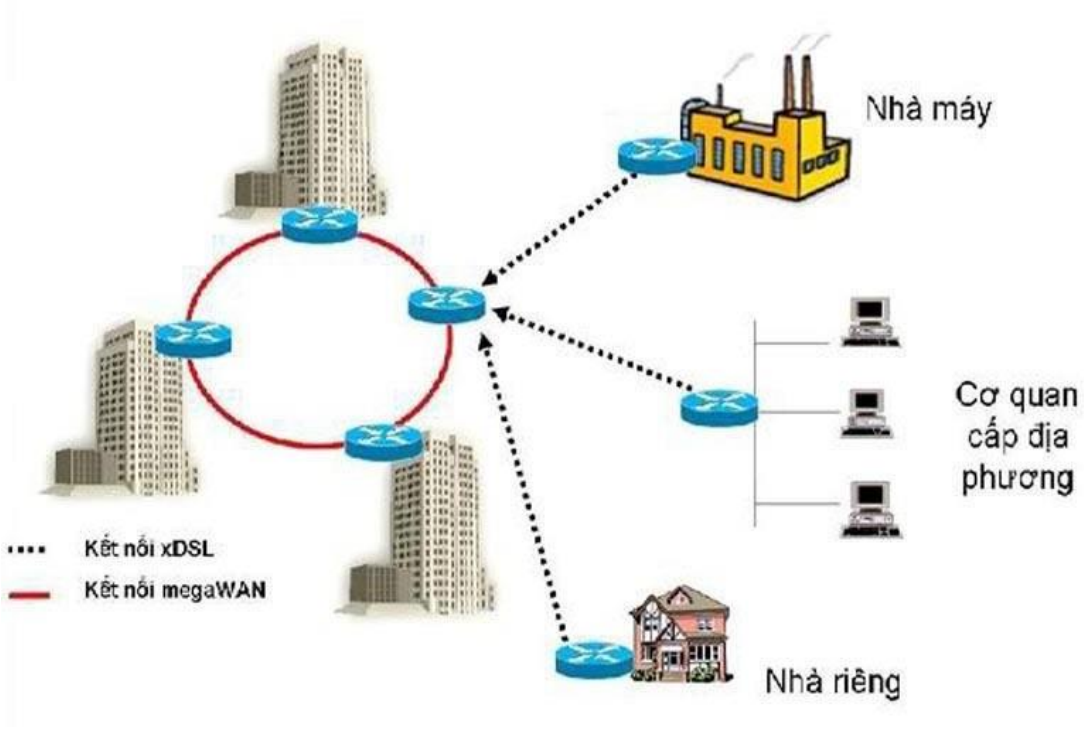
	4)
Bảo hành:	36 tháng
Thông tin thêm về sản phẩm:	Chuẩn Wi-Fi: 802.11b/g/n, bảo mật WPA/WPA2. Khe cắm: mini SIM (hay còn gọi là SIM to) và microSD

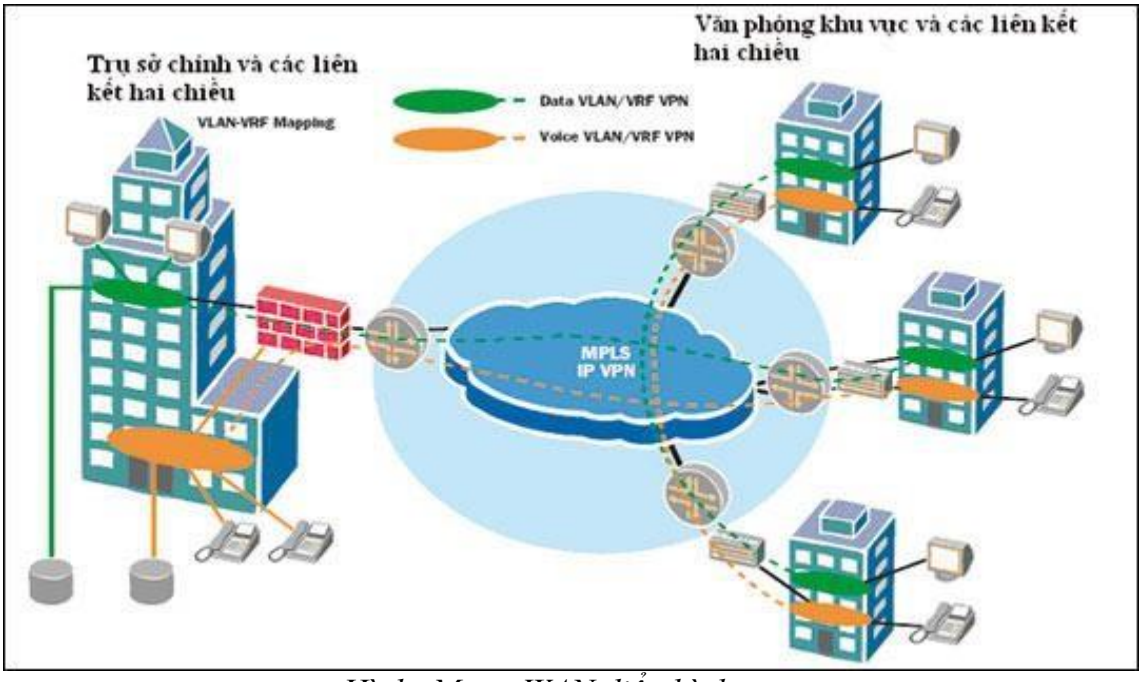
4.2. Các công nghệ truyền thông liên mạng

4.2.1. Truyền thông qua mạng diện rộng

Tổng quan về truyền thông trong mạng WAN

Mạng WAN sử dụng hạ tầng truyền dẫn của một nhà cung cấp dịch vụ bên thứ 3, chủ yếu là các công tyđiện thoại, để cung cấp dịch vụ kết nối khoảng cách xa. Cấu hình phổ biến nhất của một mạng WAN bao gồm các thành phần như hình dưới. Một thông điệp được khởi tạo từ phía khách hàng và được gửi đi bởi một thiết bị gọi là DTE tới nhà cung cấp dịch vụ mạng WAN. Các thiết bị DCE ở văn phòng trung tâm của nhà cung cấp dịch vụ sẽ "đẩy" gói tin tới mạng WAN, sau đó đi qua các thiết bị chuyển mạch để tới đích. Các thiết bị tương tự ở phía đầu nhận sẽ kết thúc hành trình.





Hình: Mạng WAN điển hình

Thiết bị đầu cuối dữ liệu (DTE - Data Terminal Equipment): Thiết bị ở phía lề của liên kết mạng WAN có chức năng gửi và nhận dữ liệu. DTE được đặt tại vị trí của người thuê bao, chính là điểm kết nối giữa mạng LAN của thuê bao và mạng WAN của nhà cung cấp dịch vụ. DTE thông thường là một bộ định tuyến (router), nhưng trong một số trường hợp có thể là một máy tính hay một bộ dồn kênh (multiplexer). Các DTE ở đầu bên này sẽ thực hiện việc truyền thông với thiết bị DTE tương ứng ở đầu bên kia.

Điểm ranh giới (Damarcation Point): Điểm kết nối giữa đường dây điện thoại của công ty điện thoại với đường dây của thuê bao. Điểm ranh giới còn được gọi là giao diện mạnghay điểm hiện

diện (point of presence). Thông thường, khách hàng sẽ chịu trách nhiệm cho tất cả các thiết bị bên trong điểm ranh giới và công ty viễn thông sẽ chịu trách nhiệm về tất cả các thiết bị ở phía bên kia.

Cáp nối chặng cuối (Local Loop): Cáp nối từ Điểm ranh giới tới Văn phòng trung tâm của công ty điện thoại. Thông thường đó là cáp đôi xoắn (UTP), nhưng cũng có thể là kết hợp cáp đôi xoắn, cáp sợi quang và các loại phương tiện truyền dẫn khác.

Văn phòng trung tâm (Central Office): Trạm tổng đài gần nhất,cũng là điểm cung cấp dịch vụ mạng WAN gần nhất với người thuê bao. Văn phòng trung tâm cung cấp điểm vàocho các cuộc gọi đi vào "đám mây mạng WAN" và cung cấp các điểm ra cho các cuộc gọi từ đám mây mạng WAN tới người sử dụng điện thoại.Ngoài ra, nó còn đóng vai trò như một điểm chuyển mạng để chuyển các gói dữ liệu tới các văn phòng trung tâm khác. Nó cũng cung cấp dòng điện một chiều ổn định cho hệ thống cáp nối chặng cuối để thiết lập mạch điện.

Thiết bị đóng mạch dữ liệu (DCE – Data Circuit-terminating Equipment)

Thiết bị truyền thông với cả DTE và đám mây mạng WAN. DCE thông thường là một bộ định tuyến của nhà cung cấp dịch vụ có chức năng chuyển tiếp dữ liệu giữa khách hàng và đám mây mạng WAN.Theo nghĩa hẹp, DTE là bất cứ thiết bị nào cung cấp tín hiệu xung cho DTE. DCE cũng có thể là một thiết bị tương tự DTE (thường là một bộ định tuyến) ngoại trừ mỗi loại thiết bị đóng một vai trò riêng.

Đám mây mạng WAN (WAN cloud): Một loạt các trung kế, tổng đài và văn phòng trung tâm tạo thành hạ tầng truyền dẫn của công ty điện thoại. Nó được thể hiện trong hình như một đám mây bởi vì có cấu trúc vật lý thay đổi thường xuyên và chỉ những người có trách nhiệm quản trị mạng mới biết dữ liệu sẽ đi tới đâu tại các tổng đài. Đối với khách hàng, điều quan trọng là dữ liệu đã được chuyển qua đường dây để tới đích.

Tổng đài chuyển mạch gói (Packet-switching exchange): Các tổng đài chuyển mạch trên mạng chuyển mạch gói của công ty viễn thông. PSE là các điểm trung gian trong đám mây mạng WAN.

Dữ liệu truyền trên mạng LAN chủ yếu được gửi từ một thiết bị số (máy tính) tới một thiết bị số khác thông qua kết nối trực tiếp. Trong khi đó, bởi vì một số mạng WAN sử dụng mạng điện thoại tương tự sẵn có, nên việc truyền số liệu có thể sử dụng một hay kết hợp những phương pháp dưới đây:

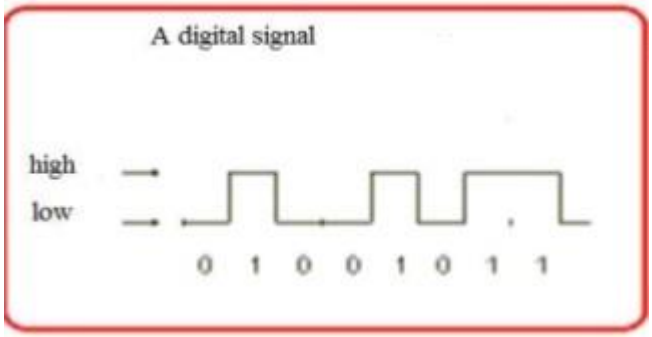
Truyền tín hiệu tương tự

Các tín hiệu tương tự thường được thể hiện dưới dạng sóng. Cường độ và tần số của tín hiệu tương tự thay đổi liên tục nên nó có thể thể hiện một cách chính xác sự chuyển động liên tục hay âm thanh hay những chuyển động đa trạng thái. Cường độ và tần số của tín hiệu tăng lên và giảm xuống tương ứng với cao độ và cường độ của âm thanh. Các tín hiệu tương tự thường dùng để biểu diễn các dữ liệu thời gian thực. Truyền thanh, điện thoại và các phương tiện truyền thông thường sử dụng tín hiệu tương tự.

Hình 2: Truyền tín hiệu tương tự

Truyền tín hiệu số

Thay vì dòng thay đổi liên tục, các tín hiệu số chỉ sử dụng 2 trạng thái, 0 và 1, để biểu diễn các bit dữ liệu. Đây là phương pháp truyền tín hiệu lý tưởng cho các mạng máy tính. Các máy tính sẽ cần tới modem, thiết bị chuyển đổi tín hiệu số của máy tính thành tín hiệu tương tự để truyền dữ liệu qua đường dây điện thoại tương tự.



Hình 3: Truyền tín hiệu số

Lưu ý: Trước đây, mạng điện thoại PSTN là mạng tương tự hoàn toàn. Các tín hiệu tương tự từ máy điện thoại tới công ty viễn thông và sẽ tiếp tục được chuyển qua các hệ thống sử dụng tín hiệu tương tự để tới đích. Ngày nay, các hệ thống điện thoại hiện nay sử dụng kết hợp hai phương pháp. Phần lớn các mạng chuyển mạch (swithced network) kết nối mạng của các công ty viễn thông đều đã được số hoá, riêng chặng cuối nối phần lớn hộ gia đình và một số doanh nghiệp vẫn sử dụng tín hiệu tương tự. Sơ đồ dưới đây cho ta thấy hai máy tính số có thể được kết nối qua mạng WAN có cả các thành phần số và thành phần tương tự. Khi một máy tính gửi tín hiệu qua mạng WAN, modem sẽ chuyển tín hiệu số thành tín hiệu tương tự để chuyển tín hiệu tới công ty điện thoại. Modem của công ty điện thoại sẽ lại chuyển dữ liệu thành dạng số để truyền qua mạng chuyển mạch. Tín hiệu lại được chuyển ngược trở lại thành tín hiệu tương tự tại phía đầu đích của công ty viễn thông để chuyển tới modem của máy tính nhận dữ liệu. Cuối cùng, modem này sẽ chuyển tín hiệu tương tự thành dạng số cho máy tính.

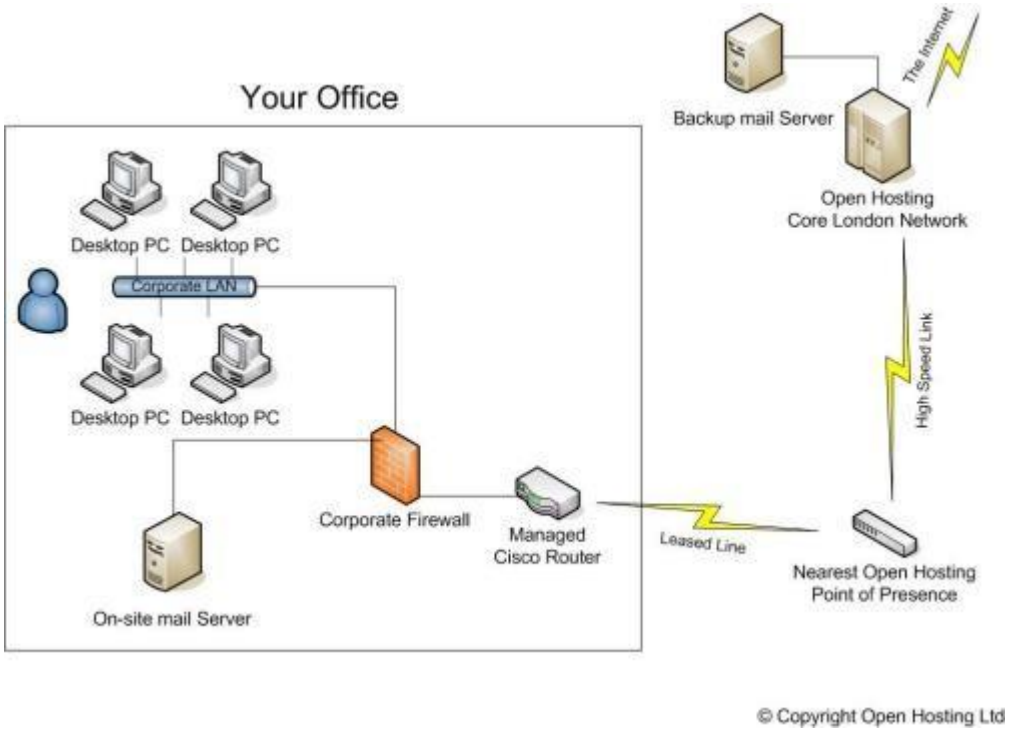
Hình 4: Mạng PSTN sử dụng kết hợp 2 phương pháp truyền tín hiệu

Các loại hình kết nối trong mạng WAN

Khi một thông điệp di chuyển qua đám mây mạng WAN, cách thức nó di chuyển từ điểm này tới điểm khác trên đường đi của nó sẽ khác nhau phụ thuộc vào kết nối vật lý và giao thức sử dụng. Các kết nối mạng WAN thường được phân thành những dạng sau:

Kết nối dành riêng (Dedicated Connection)

Đây là kết nối mang tính thường trực, kết nối trực tiếp một thiết bị với một thiết bị khác. Kết nối dành riêng có tính ổn định và nhanh nhưng có thể rất đắt. Thuê một đường dây từ nhà cung cấp dịch vụ mạng WAN có nghĩa là bạn phải trả tiền kết nối ngay cả khi bạn không sử dụng nó. Hơn nữa, bởi vì các đường dây dành riêng thiết lập kết nối trực tiếp chỉ giữa 2 điểm, nên số đường dây cần thiết sẽ tăng theo hàm số mũ các vị trí cần kết nối. Ví dụ, nếu bạn muốn kết nối 2 vị trí, bạn cần một đường dây nhưng muốn kết nối 4 vị trí bạn sẽ cần tới 6 đường dây.



Hình: Kết nối dành riêng – kenh Leased Line

Các đặc trưng của kết nối dành riêng:

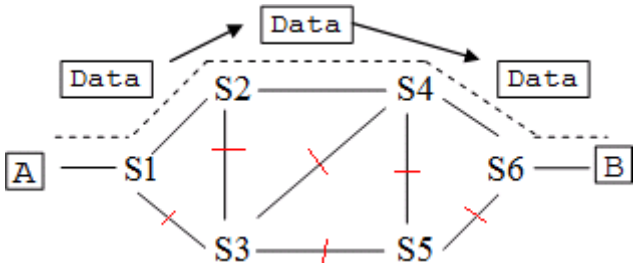
- Luôn luôn sẵn có
- Sử dụng đường dây người thuê bao thuê của nhà cung cấp dịch vụ mạng WAN
- Đắt hơn so với các giải pháp mạng WAN khác
- Sử dụng các kết nối riêng biệt giữa các điểm

Sử dụng kết nối dành riêng khi:

- Có lưu lượng cao dữ liệu luân chuyển qua mạng LAN
- Cần kết nối thường xuyên
- Có ít địa điểm cần kết nối với nhau

Mạng chuyển mạch (circuit- switched network)

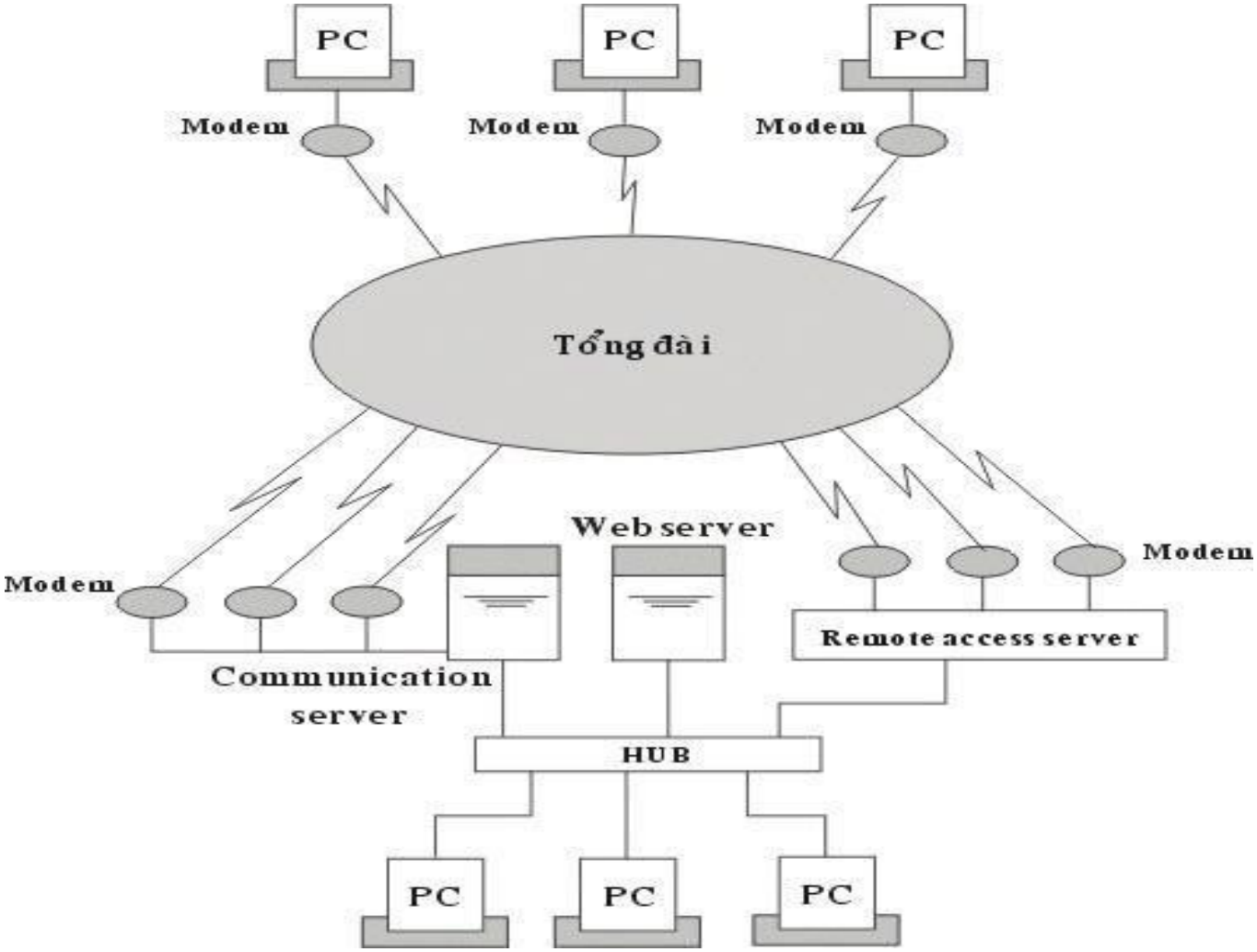
Mạng chuyển mạch cho bạn một giải pháp thay thế đối với đường thuê riêng (kết nối dành riêng), cho phép bạn sử dụng các đường dây dùng chung. Mạng chuyển mạch làm việc hai chiều, cho phép thiết lập cả các kết nối quay số vào (dial-in) và quay số ra (dial-out).



Hình : Mạng chuyển mạch

Mạng chuyển mạch (Circuit Swiching Network)

Để thực hiện được việc liên kết giữa hai điểm nút, một đường nối giữa điểm nút này và điêm nút kia được thiết lập trong mạng thể hiện dưới dạng cuộc gọi thông qua các thiết bị chuyển mạch.



Mô hình mạng chuyển mạch

Một ví dụ của mạng chuyển mạch là hoạt động của mạng điện thoại, các thuê bao khi biết số của nhau có thể gọi cho nhau và có một đường nối vật lý tạm thời được thiết lập giữa hai thuê bao.

Với mô hình này mọi đường đều có thể một đường bất kỳ khác, thông qua những đường nối và các thiết bị chuyên dùng người ta có thể liên kết một đường tạm thời từ nơi gửi tới nơi nhận một đường nối vật lý, đường nối trên duy trì trong suốt phiên làm việc và chỉ giải phóng sau khi phiên làm việc kết thúc. Để thực hiện một phiên làm việc cần có các thủ tục đầy đủ cho việc thiết lập liên kết trong đó có việc thông báo cho mạng biết địa chỉ của nút nhận.

Hiện nay có 2 loại mạng chuyển mạch là chuyển mạch tương tự (analog) và chuyển mạch số (digital)

Chuyển mạch tương tự (Analog): Việc chuyển dữ liệu qua mạng chuyển mạch tương tự được thực hiện qua mạng điện thoại. Các trạm sử dụng một thiết bị có tên là modem, thiết bị này sẽ chuyển các tín hiệu số từ máy tính sao tín hiệu tuần tự có trễ truyền đi trên mạng điện thoại và ngược lại.

Mô hình chuyển mạch tương tự

Khi sử dụng đường truyền điện thoại để truyền số liệu thì các chuẩn của modem và các tính chất của nó sẽ quyết định tốc độ của đường truyền. Cùng với các kỹ thuật chuyển đổi tín hiệu các tính năng mới như nén tín hiệu cho phép nâng tốc độ truyền dữ liệu lên rất cao.

Loại	Tốc độ (bps)	Loại nén	Tốc độ thực tế (bps)
Bell 212A	1200		
CCITT V22	1200		
CCITT V22 bis	2400	MNP Class 5	2400 - 3600
CCITT V32	9600	MNP Class 5, V42 bis	9600 - 19200
CCITT V32 bis	14400	MNP Class 5, V42 bis	14400 - 33600

Bảng kỹ thuật modem

Các kỹ thuật nén thường dùng là MNP Class 5 và V42 bis, MNP Class 5 cho phép nén với tỷ lệ 1.5:1 và V42 bis nén với tỷ lệ 2:1. Tuy nhiên trên thực tế tỷ lệ nén có thể thay đổi dựa vào dạng dữ liệu được truyền.

Chuyển mạch số (Digital): Đường truyền chuyển mạch số lần đầu tiên được AT&T thiệu vào cuối 1980 khi AT&T giới thiệu mạng chuyển mạch số Acnet với đường truyền 56 kbs. Việc sử dụng đường chuyển mạch số cũng đòi hỏi sử dụng thiết bị phục vụ truyền dữ liệu số (Data Service Unit - DSU) vào vị trí modem trong chuyển mạch tương tự. Thiết bị phục vụ truyền dữ liệu số có nhiệm vụ chuyển các tín hiệu số đơn chiều (unipolar) từ máy tính ra thành tín hiệu số hai chiều (bipolar) để truyền trên đường truyền.

Mô hình chuyển mạch số

Mạng chuyển mạch số cho phép người sử dụng nâng cao tốc độ truyền (ở đây do khác biệt giữa kỹ thuật truyền số và kỹ thuật truyền tương tự nên hiệu năng của truyền mạch số cao hơn nhiều so với truyền tương tự cho dù cùng tốc độ), độ an toàn.

Vào năm 1991 AT&T giới thiệu mạng chuyển mạch số có tốc độ 384 Kbps. Người ta có thể dùng mạng chuyển mạch số để tạo các liên kết giữa các mạng LAN và làm các đường truyền dự phòng.

Khi bạn sử dụng mạng chuyển mạch:

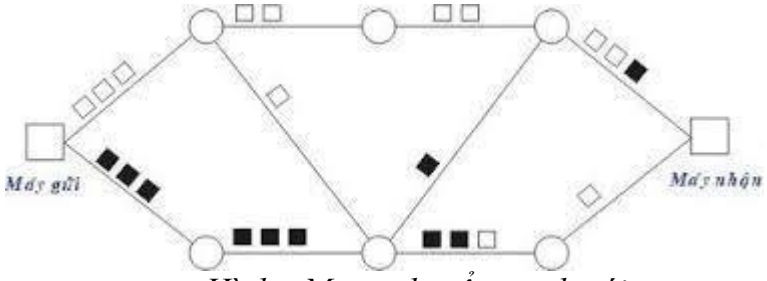
1. Máy tính gửi dữ liệu quay số vào đường dây và kết nối được thiết lập
2. Máy tính nhận dữ liệu gửi xác nhận và khoá đường dây
3. Máy tính gửi dữ liệu truyền dữ liệu qua kết nối được thiết lập
4. Sau khi hoàn tất việc truyền dữ liệu, kết nối được giải phóng cho những người sử dụng khác

Mạng chuyển mạch sử dụng các mạch ảo chuyển mạch (SVC – switched virtual circuit). Một đường truyền dữ liệu dành riêng được thiết lập khi bắt đầu quá trình truyền thông nhờ một loạt các bộ chuyển mạch điện tử. Con đường riêng này sẽ còn cho tới khi kết thúc quá trình truyền thông).

Hệ thống điện thoại công cộng là một mạng chuyển mạch. Khi bạn thực hiện một cuộc gọi, PSTN sử dụng các bộ chuyển mạch để tạo ra một kết nối vật lý, trực tiếp và dành riêng cho suốt thời gian diễn ra cuộc gọi. Khi bạn ngưng cuộc gọi, các bộ chuyển mạch giải phóng đường dây cho những người sử dụng khác. Các máy tính kết nối qua mạng làm việc theo cách thức tương tự như vậy. Khi máy tính quay số vào mạng, trước tiên con đường qua mạng được thiết lập để sau đó dữ liệu sẽ được chuyển qua con đường dành riêng tạm thời này.

Mạng chuyển mạch gói (packet-swiched)

Mạng chuyển gói không yêu cầu một đường thuê riêng hay đường dành riêng tạm thời. Thay vào đó, đường đi của thông điệp được thiết lập một cách cơ động khi dữ liệu chuyển qua mạng. Kết nối chuyển mạch gói là kết nối thường xuyên bật. Điều đó có nghĩa là bạn không cần quan tâm tới việc thiết lập kết nối hay giữ riêng đường dây. Mỗi gói tin bao gồm cả thông tin cần thiết để tới đích.



Hình : Mạng chuyển mạch gói

Mạng chuyển mạch gói có những đặc trưng sau đây:

- Thông điệp được chia thành những đơn vị nhỏ, gọi là gói
- Các gói được chuyển độc lập qua liên mạng (có thể theo những con đường khác nhau)
- Các gói được sắp xếp lại theo thứ tự ban đầu tại nơi nhận
- Thiết bị gửi và thiết bị nhận mặc định xem kết nối là thường trực (không cần quay số)

Mạng chuyển mạch gói sử dụng các mạch ảo thường trực (PVC- permanent virtual circuit). Mặc dù PVC giống như kết nối dành riêng, trực tiếp, con đường mỗi gói tin đi trong liên mạng có thể khác nhau.

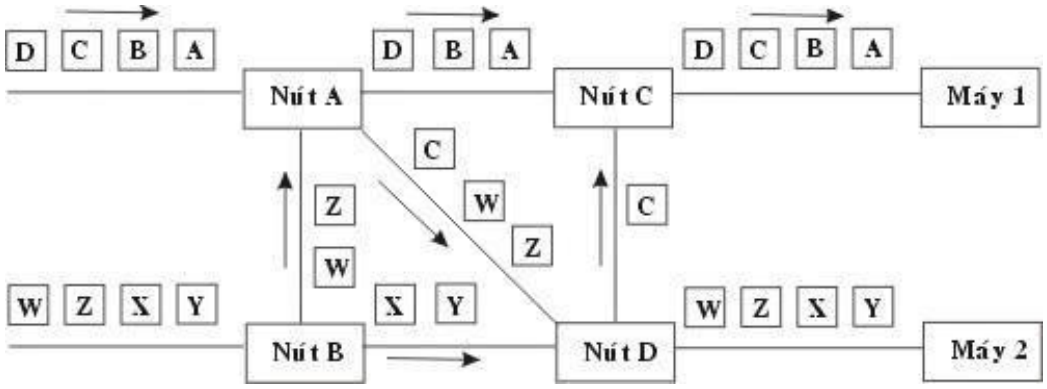
Mạng chuyển mạch gói hoạt động theo nguyên tắc sau : Khi một trạm trên mạng cần gửi dữ liệu nó cần phải đóng dữ liệu thành từng gói tin, các gói tin đó được đi trên mạng từ nút này tới nút khác tới khi đến được đích. Do việc sử dụng kỹ thuật trên nên khi một trạm không gửi tin thì mọi tài nguyên của mạng sẽ dành cho các trạm khác, do vậy mạng tiết kiệm được các tài nguyên và có thể sử dụng chúng một cách tốt nhất.

Người ta chia các phương thức chuyển mạch gói ra làm 2 phương thức:

Phương thức chuyển mạch gói theo sơ đồ rời rạc.

Phương thức chuyển mạch gói theo đường đi xác định.

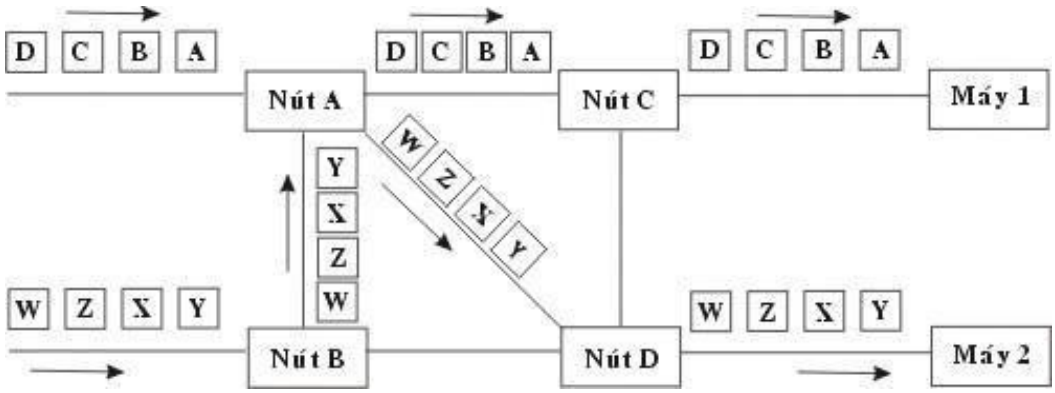
Với phương thức chuyển mạch gói theo sơ đồ rời rạc các gói tin được chuyển đi trên mạng một cách độc lập, mỗi gói tin đều có mang địa chỉ nơ i gửi và nơi nhận. Mỗi nút trong mạng khi tiếp nhận gói tin sẽ quyết định xenm đường đi của gói tin phụ thuộc vào thuật toán tìm đường tại nút và những thông tin về mạng mà nút đó có. Việc truyền theo phương thức này cho ta sự mềm dẻo nhất định do đường đi với mỗi gói tin trở nên mềm dẻo tuy nhiên điều này yêu cầu một số lượng tính toán rất lớn tại mỗi nút nên hiện nay phần lớn các mạng chuyển sang dùng phương chuyển mạch gói theo đường đi xác định.



Ví dụ phương thức sơ đồ rời rạc.

Phương thức chuyển mạch gói theo đường đi xác định:

Trước khi truyền dữ liệu một đường đi (hay còn gọi là đường đi ảo) được thiết lập giữa trạm gửi và trạm nhận thông qua các nút của mạng. Đường đi trên mang số hiệu phân biệt với các đường đi khác, sau đó các gói tin được gửi đi theo đường đã thiết lập để tới đích, các gói tin mang số hiệu củ đường ảo để có thể được nhận biết khi qua các nút. Điều này khiến cho việc tính toán đường đi cho phiên liên lạc chỉ cần thực hiện một lần.



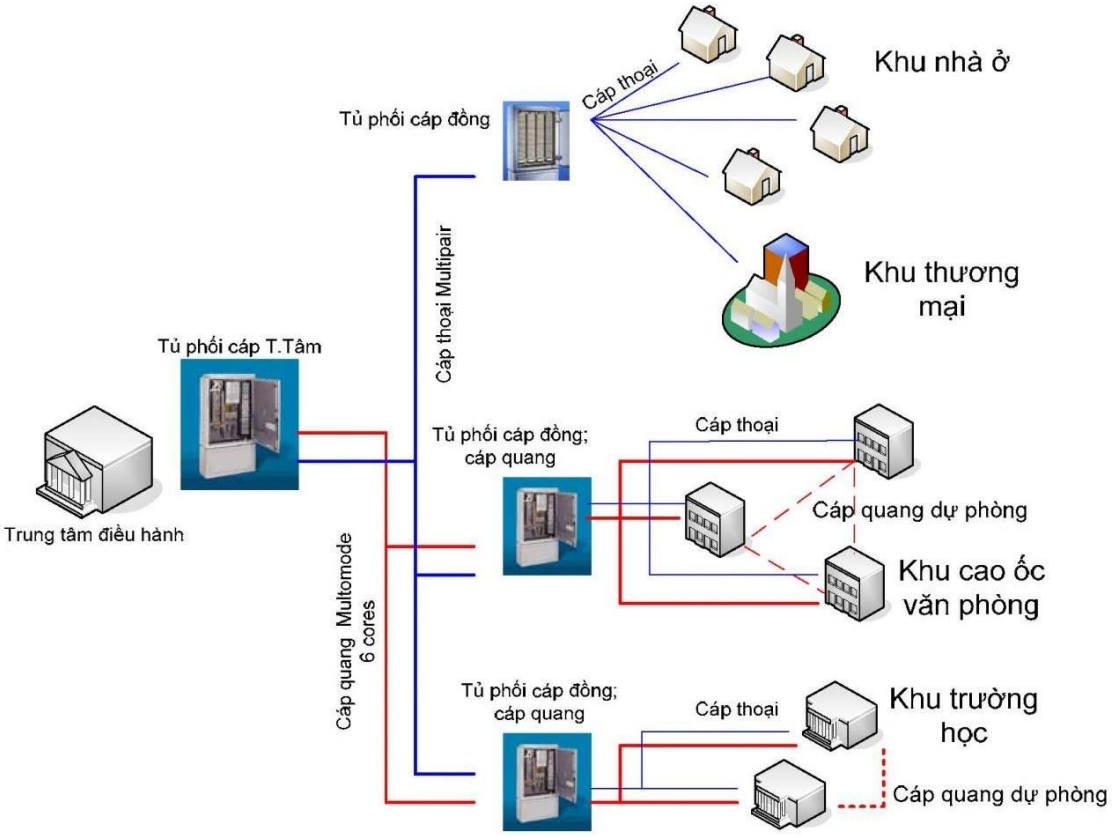
Ví dụ phương thức đường đi xác định

Các dịch vụ mạng diện rộng

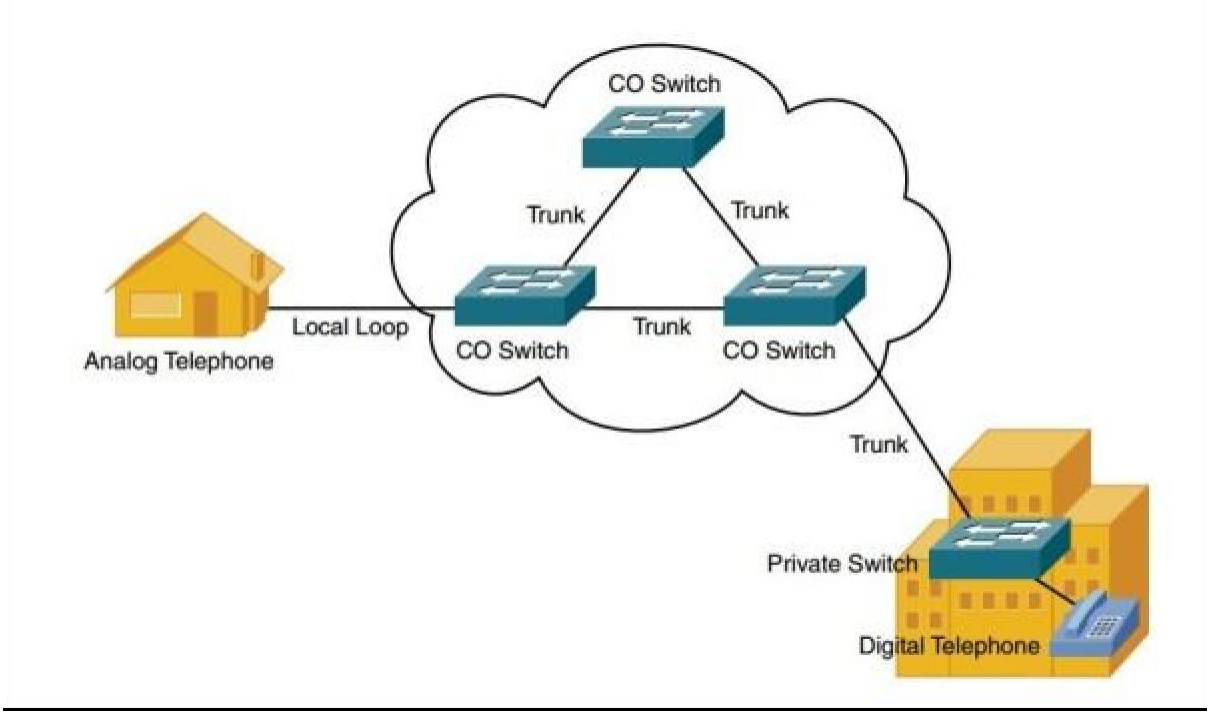
(1) PSTN (Public Switch telephoneNetwork)

Mạng điện thoại chuyển mạch công cộng là mạng lâu đời nhất và có qui mô lớn nhất có thể sử dụng cho truyền thông mạng WAN. Các đặc trưng của PSTN bao gồm:

- Đây là mạng chuyển mạch, có phạm vi toàn cầu
- Giao diện với PSTN là tương tự, vì vậy các máy tính sử dụng modem để kết nối với PSTN
- Tốc độ trên PSTN thường bị giới hạn ở ngưỡng 56 Kbit/s
- Bạn có thể sử dụng PSTN khi có nhu cầu (on demand) hay thuê một mạch riêng



Hình ?: Mạng điện thoại PSTN



Các thành phần trong hệ thống PSTN

• Điện thoại Analog (Analog telephone): là thiết bị "truyền thống" được sử dụng để kết nối đến hệ thống PSTN. Và là thiết bị chuyển đổi từ tín hiệu analog (âm thanh người nói) sang tín hiệu số (Digital) để truyền đi trên đường dây cáp đồng hai lõi (còn được gọi là Tip-Ring).

• Tín hiệu đầu-cuối (Local loop): là đường dây dẫn liên kết giữa nhà cung cấp dịch vụ trạm (PSTN) tới người dùng cuối.

• Mạch chuyển CO (CO Switch): Cung cấp các dịch vụ từ nhà cung cấp tới người dùng. (như là: đảm bảo tín hiệu cuộc gọi, chuyển hướng cuộc gọi,…)

• Đường trung kế (Trunk): là đường dây trung gian giữa nhà cung cấp dịch vụ trạm PSTN đến các CO Switch.

• Mạch chuyển nội bộ (Private Switch): Dùng cho các doanh nghiệp

Đường truyền PSTN cho tốc độ tối đa 64Kbps; khi kết nối chiếm kêh chuyền (kết nối Internet thì dừng cấc kết nối tín hiệu thoại hoặc tín hiệu fax); phải thực hiện một kết nối từ điểm đầu đến cuối (thông qua tổng đài chuyên mạch Analog);

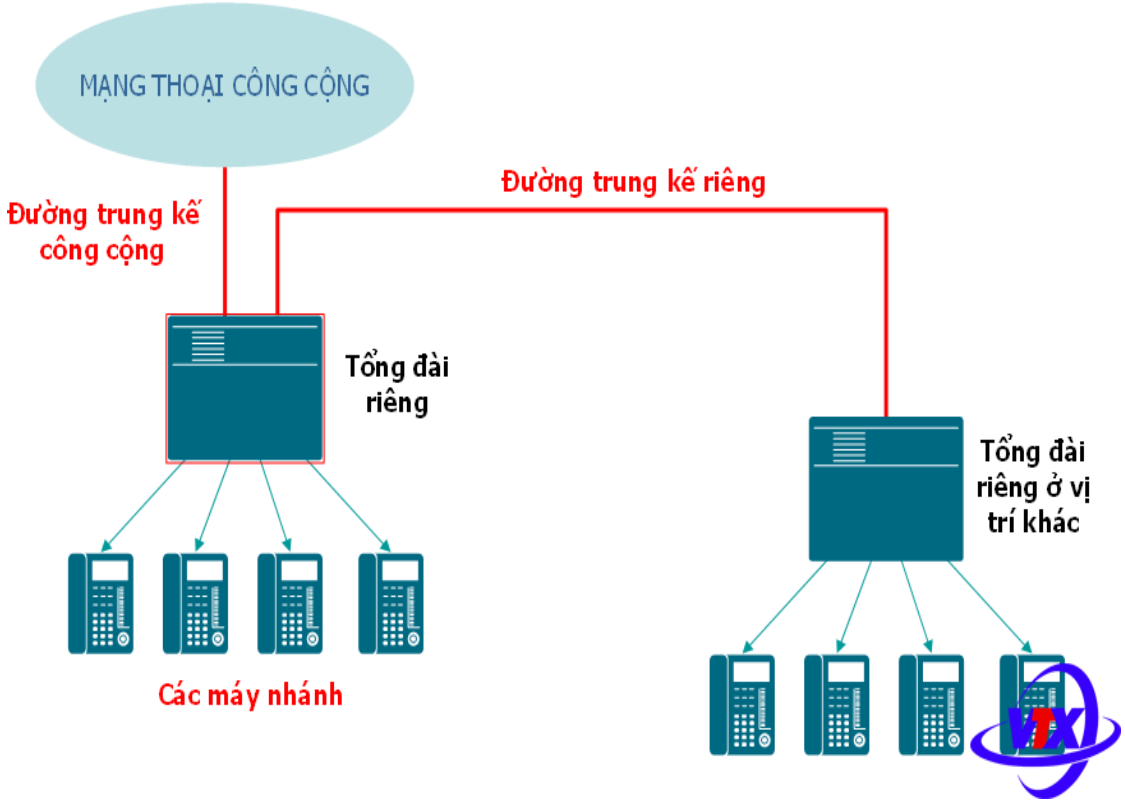
Nhược điểm: đường Analog – tốc độ thấp, chiếm giữ đường truyền; không hiệu quả

Đường thuê riêng (Leased Line)

Đối với một số công ty, lợi ích của một đường thuê riêng có thể cao hơn rất nhiều so với chi phí phải bỏ ra. Đường thuê riêng là đường độc lập và có tốc độ cao hơn so với đường PSTN thông thường. Tuy nhiên nó khá đắt nên thường chỉ có các công ty lớn sử dụng. Các đặc trưng khác của đường thuê riêng bao gồm:

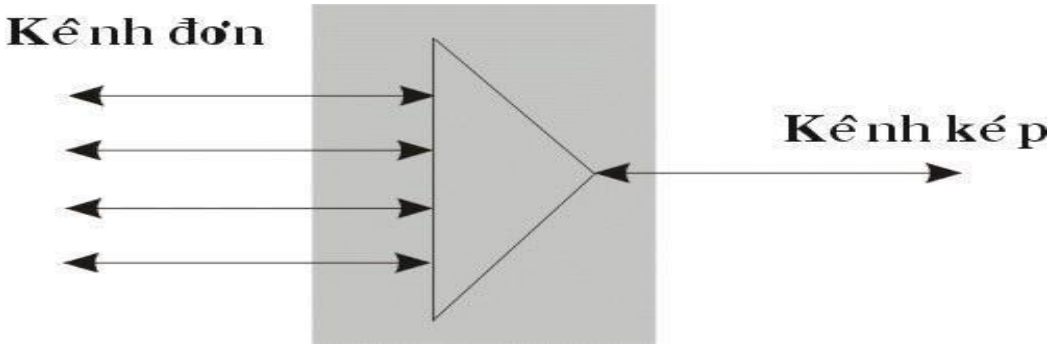
- Cung cấp kết nối thường xuyên, chất lượng ổn định

- Bạn có thể bỏ thêm chi phí để nâng cấp đường thuê riêng



Hình : Đường dây thuê riêng

Với kỹ thuật chuyển mạch giữa các nút của mạng (tương tự hoặc số) có một số lượng lớn đường dây truyền dữ liệu, với mỗi đường dây trong một thời điểm chỉ có nhiều nhất một phiên giao dịch, khi số lượng các trạm sử dụng tăng cao người ta nhận thấy việc sử dụng mạng chuyển mạch trở nên không kinh tế. Để giảm bớt số lượng các đường dây kết nối giữa các nút mạng người ta đưa ra một kỹ thuật gọi là ghép kênh.



Mô hình ghép kênh

Mô hình đó được mô tả như sau: tại một nút người ta tập hợp các tín hiệu trên của nhiều người sử dụng ghép lại để truyền trên một kênh nối duy nhất đến các nút khác, tại nút cuối người ta phân kênh ghép ra thành các kênh riêng biệt và truyền tới các người nhận.

Có hai phương thức ghép kênh chính là ghép kênh theo tần số và ghép kênh theo thời gian, hai phương thức này tương ứng với mạng thuê bao tuần tự và mạng thuê bao kỹ thuật số. trong thời gian hiện nay mạng thuê bao kỹ thuật số sử dụng kỹ thuật ghép kênh theo thời gian với đường truyền T đang được sử dụng ngày một rộng rãi và dần dần thay thế mạng thuê bao tuần tự.

Phương thức ghép kênh theo tần số FDM:

Để sử dụng phương thức ghép kênh theo tần số giữa các nút của mạng được liên kết bởi đường truyền băng tần rộng. Băng tần này được chia thành nhiều kênh con được phân biệt bởi tần số khác nhau. Khi truyền dử liệu, mỗi kênh truyền từ người sử dụng đến nút sẽ được chuyển thành một kênh con với tần số xác định và được truyền thông qua bộ ghép kênh đến nút cuối và tại đây nó được tách ra thành kênh riêng biệt để truyền tới người nhận. Theo các chuẩn của CCITT có các phương thức ghép kênh cho phép ghép 12, 60, 300 kênh đơn.

Người ta có thể dùng đường thuê bao tuần tự (Analog) nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất. Khi máy của người sử dụng gửi dữ liệu thì kênh dữ liệu được ghép với các kênh khác và truyền trên đường truyền tới nút đích và được phân ra thành kênh riêng biệt trước khi gửi tới máy của người sử dụng. Đường nối giữa máy trạm của người sử dụng tới nút mạng thuê bao cũng giống như mạng chuyển mạch tuần tự sử dụng đường dây điện thoại với các kỹ thuật chuyển đổi tín hiệu như V22, V22 bis, V32, V32 bis, các kỹ thuật nén V42 bis, MNP class 5.

Phương thức ghép kênh theo thời gian TDM:

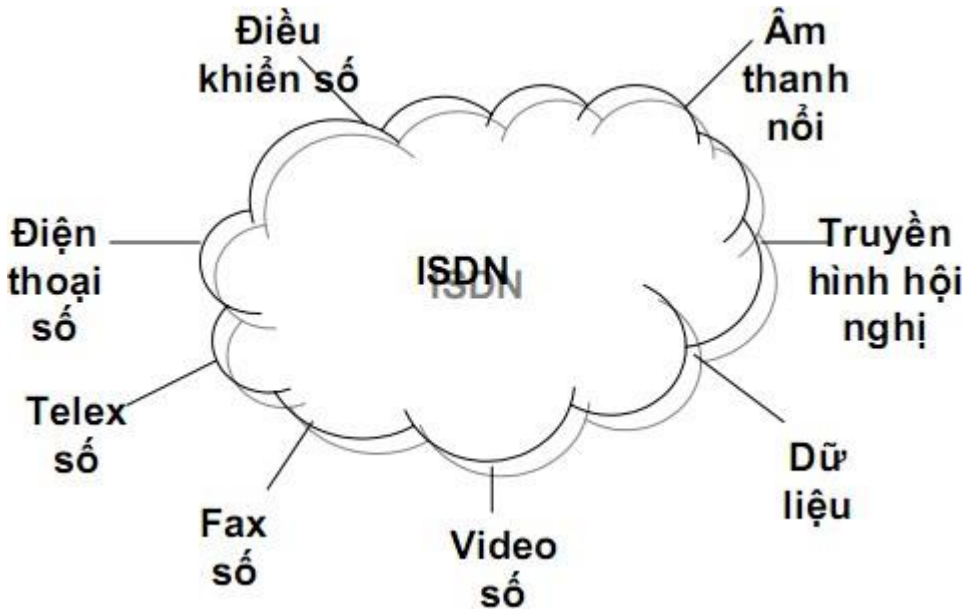
Khác với phương thức ghép kênh theo tần số, phương thức ghép kênh theo thời gian chia một chu kỳ thời gian hoạt động của đường truyền trục thành nhiều khoảng nhỏ và mỗi kênh tuyền dữ liệu được một khoảng. Sau khi ghép kênh lại thành một kênh chung dữ liệu được truyền đi tương tự như phương thức ghép kênh theo tần số. Người ta dùng đường thuê bao là đường truyền kỹ thuật số nối giữa máy của người sử dụng tới nút mạng thuê bao gần nhất.

Hiện nay người ta có các đường truyền thuê bao như sau :

Đường T1 với tốc độ 1.544 Mbps nó bao gồm 24 kênh vớp tốc độ 64 kbps và 8000 bits điều khiển trong 1 giây.

Phương thức ghép kênh theo mã (CDM):

(2) ISDN (Intergrated Services Digital Network)



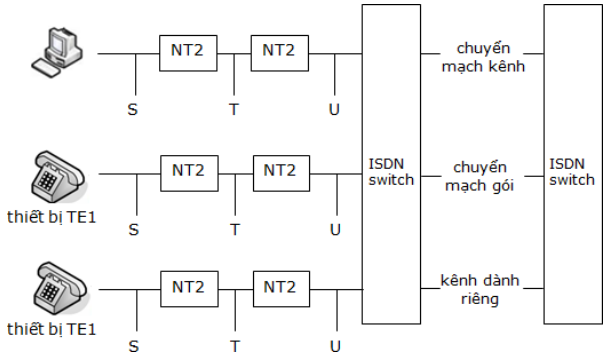
Các thiết bị cơ bản trong mạng ISDN bao gồm: (modem ISDN)

- **Terminal equipment type 1** (**TE1**): Các thiết bị đầu cuối mang tính năng ISDN (điện thoại số ISDN, digital fax…).
- **Terminal equipment type 2** (**TE2**): Các thiết bị đầu cuối không mang tính năng ISDN. Các thiết bị này để có thể liên kết được với ISDN cần phải có thêm các bộ phối ghép đầu cuối Terminal Adapter (TE).
- **Network Termination 1** (**NT1**): Thực hiện các chức năng thuộc tầng Physical trong mô hình OSI (các chức năng về điện, giao tiếp giữa ISDN và người sử dụng, chức năng kiểm soát chất lượng đường truyền…).

- **Network Termination 2** (**NT2**): Các thiết bị có khả năng đáp ứng các chức năng liên quan đến tầng mạng của mô hình OSI (các tổng đài riêng PBX).

ISDN quy định cụ thể các điểm chuẩn phân cách để xác định giao diện giữa các nhóm thiết bị, ví dụ như giữa TA và NT1. Các điểm này bao gồm:

- R: Giữa các thiết bị không có tính năng ISDN và thiết bị TA.
- S: Giữa các thiết bị đầu cuối của người dùng và thiết bị NT2.
- T: Giữa thiết bị NT1 và thiết bị NT2.
- U: Giữa thiết bị NT1 và thiết bị mạng đầu cuối.



Các điểm phân cách giữa các nhóm thiết bị trong ISDN

ISDN là gì?

Mạng số đa dịch vụ tích hợp ISDN là một tập các giao thức chuẩn được định nghĩa bởi tổ chức chuẩn quốc tế về Viễn thông ITU-T (CCITT), các giao thức này được tiếp nhận như những chuẩn cho các nhà cung cấp dịch vụ trên toàn thế giới.

ISDN tương thích với hệ thống mạng thoại truyền thống, trên một đôi dây đồng thông thường có thể truyền tải các tín hiệu thoại và phi thoại đồng thời. Nó là mạng số hoàn hảo cho tất cả các ứng dụng và thiết bị hoạt động dựa trên tín hiệu số.

Sự khác nhau cơ bản giữa mạng ISDN và mạng thoại truyền thống là số và tương tự. Với mạng ISDN tín hiệu được truyền dưới dạng các bít nhị phân. Hơn nữa, nó có thể truyền nhiều luồng bít của các tín hiệu khác nhau tại cùng một thời điểm, điều đó cho phép mạng cung cấp đến người dùng nhiều ứng dụng mà mạng thoại truyền thống PSTN rất hạn chế.

ISDN phục vụ cho tất cả các loại hình thông tin như thoại, số liệu, âm thanh chất lượng cao, truyền hình, tín hiệu truyền trên mạng dưới dạng số tốc độ cao.

ISDN có thể sử dụng nhiều thiết bị và nhiều số điện thoại trên cùng một đường dây. Nó cho phép tối đa đến 8 máy thoại, fax hoặc máy tính có thể liên kết trên một kênh ISDN băng tần cơ sở (BRI ~ 2B+D ~ 128+16Kbps) và có thể đặt cho 8 số khác nhau.

Một kênh cơ sở BRI có thể hỗ trợ đến 2 cuộc gọi đồng thời, có thể là thoại, fax hoặc kết nối PC thông qua một kênh ISDN.

Từ một kênh số ISDN, người dùng có thể thiết lập một cuộc gọi đến máy tương tự trên mạng PSTN và ngược lại. Cả hai mạng được liên kết bằng các tổng đài của nhà cung cấp dịch vụ, tương tự như vậy với kết nối giữa mạng ISDN và mạng di động

Trong ISDN, đường truyền thông tin giữa người sử dụng và mạng gọi là một kênh. Kênh chỉ truyền các tín hiệu số. Bao gồm 3 loại kênh D, kênh B và kênh H khác nhau về chức năng và tốc độ.

- Kênh D: Dùng để truyền các báo hiệu và dữ liệu. Kênh D hoạt động ở tốc độ 16Kbps hoặc 64Kbps.
- Kênh B: Dùng để truyền tín hiệu tiếng nói, âm thanh, số liệu và hình ảnh. Kênh B luôn hoạt động ở tốc độ 64Kbps.
- Kênh H: Cung cấp các dịch vụ tốc độ cao và ghép các luồng thông tin. Có 4 loại kênh H (H0, H10, H11, H12) với tốc độ lần lượt là 384Kbps, 1.472Kbps, 1.536Kbps, 1.920Kbps.

Dựa vào các kênh truyền mà ISDN bao gồm hai loại hình dịch vụ: ISDN Basic Rate Interface (BRI) và Primary Rate Interface (PRI). BRI bao gồm 2 kênh B kết hợp với một kênh D (16Kbps). Do đó, BRI có tốc độ là 144Kbps. BRI dành cho các thuê bao nhỏ để cung cấp các dịch vụ truy cập mạng. PRI bao gồm 2 tiêu chuẩn, bao gồm 23 kênh B kết hợp với 1 kênh D và 30 kênh B kết hợp với 1 kênh D. PRI dùng cho thuê bao có dung lượng lớn như tổng đài PBAX hoặc các mạng cục bộ LAN.

Mạng ISDN là sự tích hợp kỹ thuật chuyển mạch kênh và chuyển mạch gói. Cấu trúc của ISDN ở tầng Physical phụ thuộc vào hướng liên kết từ thiết bị đầu cuối đến mạng (Terminal to Netowrk) hoặc từ mạng đến thiết bị đầu cuối (Netowrk to Terminal). Tầng Data-link là sự hoạt động của giao thức LAP-D (Link Access Protocol – D channel). LAP-D thực hiện các chức năng như: thiết lập một hay nhiều liên kết trên kênh D cho sự hoạt động ở tầng Network, tạo frame, kiểm soát đồng bộ, kiểm soát luồng, phát hiện lỗi…

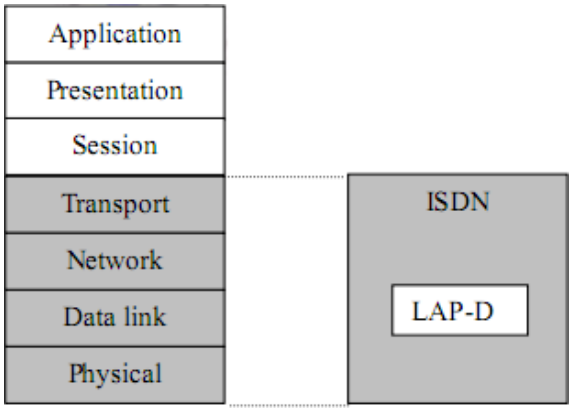
1	2	2	< 260 Byte	2	1
Flag	Address	Control	Information	CRC	Flag

Cấu trúc khung của LAP-D

Theo cấu trúc trên:

- Flag: Đánh dấu bắt đầu và kết thúc một khung.
- Address: Địa chỉ ISDN.
- Control: Trường điều khiển.
- Information: Trường dữ liệu.
- CRC: Trường kiểm tra lỗi.

Ở tầng Network, cung cấp 2 kỹ thuật ITU-T I.450 (còn được gọi là ITU-T Q.930) và ITU-T I.451 (còn được gọi là ITU-T Q.931). 2 kỹ thuật này giúp thiết lập, duy trì và kết thúc các liên kết với các thông điệp như SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS và DISCONNECT.



Kiến trúc ISDN và mô hình OSI

Ứng dụng cho ISDN

Mạng số đa dịch vụ tích hợp sử dụng chính đôi dây cáp đồng của đường dây điện thoại truyền thống trước đây vẫn chỉ dùng kết nối một kênh thoại. ISDN có thể thực hiện nhiều kết nối trên đôi dây này tại cùng một thời điểm với tốc độ cao. Các ứng dụng bao gồm: Voice, Fax, Data, và email đồng thời; hội nghị truyền hình giá thấp; quảng bá từ xa và truyền audio chất lượng cao.

Mạng ISDN đưa đến cho người dùng kênh tốc độ như thế nào?

Có hai dạng kênh chính được hỗ trợ trong ISDN

Kênh tốc độ cơ sở BRA (Basic Rate Access)

Được cung cấp thông qua một kênh giao diện tốc độ cơ sở

Kênh này có thể gọi là kênh giao diện S0

Có 2 kênh người dùng có thể sử dụng đồng thời

Tốc độ kết nối tối đa 144Kbps (2B + D)

Tốc độ này được chọn do các công ty điện thoại lắp đặt

Kênh tốc độ sơ cấp PRA (Primary Rate Access)

Được cung cấp thông qua một kênh giao diện tốc độ sơ cấp

Kênh này có thể gọi là kênh giao diện S2

Có thể sử dụng đồng thời 30 kênh khác nhau (chuẩn Châu Âu) hoặc 23 kênh (chuẩn Bắc Mỹ, Nhật bản...)

Tốc độ tối đa 2048Kbps (E1: 30B + D) với chuẩn Châu Âu và 1536Kbps với chuẩn Bắc Mỹ và Nhật bản.

Kênh này thường được cài đặt cho các đường tốc độ cao đến thiết bị trước khách hàng.

Thông thường tốc độ cơ sở sử dụng cho các trạm thông tin ở xa hoặc văn phòng nhỏ, kênh sơ cấp sử dụng cho các Server lớn đặt tại trung tâm phục vụ truy cập từ xa, fax Server hoặc PBX cỡ vừa hoặc văn phòng cỡ lớn. Hiện tại hầu hết các nhà cung cấp dịch vụ Internet ISP sử dụng kênh PRI cung cấp kết nối tương tự và ISDN cho các thuê bao

Các dịch vụ ISDN

Mạng ISDN cung cấp 2 loại hình dịch vụ chính :

Dịch vụ mạng thực hiện chuyển giao giữa người dùng và mạng

Ví dụ: thiết lập cuộc gọi và kết thúc cuộc gọi

Dịch vụ mạng định nghĩa cách mà người dùng và mạng tương tác qua lại nhằm mục đích quản lý các kết nối

Người dùng có thể sử dụng các dịch vụ mạng để yêu cầu mạng thực hiện các chức năng như thiết lập và xoá cuộc gọi, chuyển giao cuộc gọi đến người dùng khác và một số các chức năng khác. Chức năng này được xem như báo hiệu

Dịch vụ chuyển tải (Bearer)

Dịch vụ này thực hiện chuyển dữ liệu giữa hai người dùng

Ví dụ: thông tin thoại hoặc fax được mã hoá thành các dòng bit

Dịch vụ chuyển tải thực hiện các chức năng cuộc gọi mà người dùng đang thực hiện

Các dịch vụ bao gồm thoại, fax, kết nối modem và Internet.

Nói rộng hơn có hai loại hình dịch vụ chuyển tải :

Dữ liệu có cấu trúc (Structured Data): thông tin truyền trên dịch vụ này được quản lý dễ dàng bởi mạng, tín hiệu thoại là một ví dụ của dạng này. Do mạng nhận biết được kết nối, do vậy nó có thể chuyển dữ liệu sang tín hiệu tương tự trong trường hợp cuộc gọi được kết nối đến một máy thoại tương tự

Dữ liệu không có cấu trúc (Unstructured Data): dạng của dữ liệu không được nhận biết qua mạng, nhưng được nhận biết qua hai người dùng tại các điểm đầu cuối của dịch vụ

Như vậy

Dịch vụ chuyển tải cung cấp kết nối giữa các người dùng qua mạng

Dịch vụ mạng cung cấp điều khiển và báo hiệu giữa người dùng và mạng

Mạng ISDN cung cấp 2 kênh tốc độ chính: BRI và PRI

Kênh cơ sở BRI cung cấp 2 kênh người dùng (kênh B)

Kênh sơ cấp PRI cung cấp 30 kênh hoặc 23 kênh người dùng

Kênh B và kênh D

Kênh B và D làm chức năng gì?

Kênh B và D chia sẻ đường truyền như thế nào?

So sánh về cấu trúc giữa kênh BRI và PRI

Chúng mang khả năng gì và tập trung trên những kênh nào?

Dung lượng băng thông cung cấp cho người dùng là bao nhiêu?

Kênh B làm chức năng gì?

Kênh B thực hiện các dịch vụ ISDN qua mạng và truyền tin tức (thoại và phi thoại) giữa các người dùng.

Kênh B là kênh truyền độc lập cho các Bits và truyền tại tốc độ 64Kbps

Kênh B không cần biết các thông tin dạng bit truyền qua nó. Nhiệm vụ của mạng là tiếp nhận các bits được cung cấp bởi một người dùng tại một đầu cuối của kênh B và gửi chúng đến người dùng bên kia kênh.

Trong một giao diện, kênh B được đánh số. Trong giao diện cơ sở chúng được đánh số là 1 & 2; trong giao diện sơ cấp, chúng được đánh số từ 1 đến 30 (hoặc 1 đến 23). Khi hai người dùng kết nối, không có sự liên quan giữa các kênh tại các đầu cuối. Người dùng có thể kết nối kênh B số 17 với kênh B số 2. ISDN chịu trách nhiệm quản lý sự liên quan này.

Lưu ý rằng kênh số 17 chỉ tồn tại với kênh PRI, trong khi kênh 2 có thể tồn tại trên cả kênh PRI và BRI. Mạng ISDN không hạn chế các kết nối các kênh B giữa 2 loại giao diện BRI & PRI.

Kênh D làm chức năng gì?

Kênh D thực hiện dịch vụ ISDN giữa người dùng và mạng. Nó giám sát sự liên quan giữa người dùng và mạng, bao gồm:

Các yêu cầu và trả lời được sử dụng khi người dùng thiết lập hoặc nhận một cuộc gọi

Thông báo tiến trình cuộc gọi

Thông báo người dùng, nhóm cuộc gọi bị ngắt

Thông báo lỗi khi không thiết lập được cuộc gọi

Kênh D hoạt động tại tốc độ 16Kbps với kênh BRI và 64Kbps với kênh PRI

Đặc điểm của kênh B và D

Một kênh ISDN có đầu cuối, kênh B định giới hạn tại một người dùng, như vậy một kênh B kết nối chỉ 2 đầu cuối, không thể vận hành với mô hình dạng Y- shaped, có thể mô tả kênh B là end to end

Kênh D không là end - to - end:

Lưu ý kênh D không qua mạng, mỗi một người dùng chỉ có một kênh D và nó không kết nối với kênh D của người dùng khác.

Kênh B truyền trực tiếp qua mạng

Kênh B & D trong BRI chia sẻ đường như thế nào:

2 kênh B và một kênh D tạo lên một đường cơ sở BRI , sự kết hợp này sử dụng công nghệ ghép kênh phân chia theo thời gian TDM.

Kênh B & D trong PRI chia sẻ đường như thế nào:

Với giao diện kênh sơ cấp chuẩn Châu Âu 30 kênh B và một kênh D, 23 kênh B và một kênh D chuẩn Bắc Mỹ.

Kênh B hoạt động ở tốc độ 64Kbps

Kênh B hoạt động ở tốc độ 64Kbps trong giao diện kênh sơ cấp, đây là sự khác nhau giữa kênh BRI và PRI, trong kênh BRI kênh D chỉ có tốc độ là 16Kbps.

Giao diện kênh sơ cấp sử dụng cân bằng thời gian truyền số liệu cho mỗi kênh B và cho kênh D tất cả chúng hoạt động ở cùng tốc độ.

Lưu ý: có một khe thời gian không mang chức năng kênh. Khe này dành riênh cho mạng mà nhà cung cấp sử dụng cho mục đích chẩn đoán. Kênh xuất hiện giữa kênh B số 15 và kênh B số 16

Kênh sơ cấp PRI 30B+D

Fractional PRI

Dịch vụ ISDN có khả năng cung cấp các giao diện trong đó chỉ sử dụng một số kênh. Tại một số nước, khi người dùng sử dụng giao diện sơ cấp, chỉ phải tính cước các kênh B sử dụng thực tế.

Nếu người dùng không cần tất cả các kênh, họ có thể yêu cầu không kích hoạt một số kênh này, có nghĩa là tốc độ sơ cấp được phân đoạn (Fractional). Số kênh người dùng có thể yêu cầu phụ thuộc vào chính sách của nhà cung cấp dịch vụ.

Điều gì sẽ xảy ra nếu người dùng cố gắng dùng hơn số kênh mà họ thuê bao? Với mạng ISDN lúc đó chính sách của mạng ISDN được thiết lập bởi nhà cung cấp dịch vụ sẽ can thiệp. Khi người dùng muốn đặt cuộc gọi thông qua mạng ISDN thì gửi yêu cầu trong kênh D đến mạng. Mạng sẽ đáp ứng yêu cầu này hoặc từ chối.

Nếu sử dụng một kênh B, người dùng sẽ được đáp ứng, nếu yêu cầu tiếp cuộc gọi thứ hai trong khi cuộc gọi đầu vẫn hoạt động, mạng sẽ từ chối yêu cầu

- Giao diện T1: 24 kênh thoại / 1 đường (Dải 24 số); sử dụng theo chuẩn Mỹ
- Giao diện E1: 30 Kênh thoại / 1 đường (Dải 30 số); Sử dụng theo chuẩn châu Âu
- Giao diện BRI: 2 kênh thoại / 1 đường (Dải 2 số)
- Giao diện PRI30 : 30 kênh thoại / 1 đường (Dải 30 số)

Luồng T1 là gì:

Luồng T1 là luồng truyền dữ liệu có khả năng kết nối đồng thời 24 kết nối đồng thời chạy với tốc độ truyền 1,544 Mbps. Luồng T1 kết nối 24 kênh này về một điểm liên kết duy nhất. Luồng T1 được chia thành các khung với tốc độ 8000 lần/ s, và mỗi khung có tổng cộng 193 bit từ 24 kênh. Tổng dung lượng truyền dữ liệu của T1 bằng 8.000 x 193 = 1.544 Mbps.

Tốc độ luồng T2 = T1x2 , T3, T4…

Luồng E1 là gì:

E1 là định dạng truyền dữ liệu chuẩn châu âu, sử dụng tại hầu hết các nước trên thế giới ngoại trừ Mỹ và Nhật Bản. E1 cũng có đặc điểm như T1 nhưng có tốc độ đường truyền 2.048 Mbps. Luồng E1 có 32 kênh và mỗi kênh có tốc độ 64kb/ s. Luồng E1 có tốc độ băng thông nhanh hơn so với luồng T1 nhờ không sử dụng bit đầu cho phí tổn điều khiển. Trông khi đó T1 sử dụng trong mỗi kênh 1 bit.

Tốc độ luồng E2=2xE1; ….

Sự khác nhau giữa truyền tín hiệu giữa luồng E1 và T1

Giao thức truyền dữ liệu E1 và T1 gồm 2 đường dữ liệu, 1 đường dữ liệu truyền và 1 đường dữ liệu nhận. Tín hiệu đồng hồ xác định khi các dữ liệu được truyền trong T1 và E1.

Các tín hiệu kỹ thuật số điển hình hoạt động bằng cách gửi các tín hiệu định dạng số 0 hoặc 1 , thường được biểu thị bằng sự vắng mặt hoặc hiện diện của điện áp trên đường dây. Thiết bị nhận chỉ cần phát hiện sự hiện diện của điện áp trên đường dây và kiểm tra cụ thể để xác định xem tín hiệu là 0 hay 1. Luồng T1 và E1 sử dụng các xung điện lưỡng cực. Tín hiệu được biểu thị không có điện áp (0), điện áp dương và âm là 1. Tín hiệu lưỡng cực cho phép các máy thu T1 và E1 phát hiện các điều kiện lỗi trong đường truyền, tùy thuộc vào loại mã hóa đang được sử dụng.

Mã Hoá T1 và E1:

Các mã hoá phổ biến đang được sử dụng hiện nay:

- Alternate mark inversion (AMI) có trên T1 và E1
- Bipolar with 8-zero substitution (B8ZS) chỉ có trên T1
- High-density bipolar 3 code (HDB3)— chỉ có trên E1

Khung dữ liệu và tín hiệu Loopback luồng E1 và T1

Khung dữ liệu:

- Luồng T1 sử dụng khung mở rộng ESF cho phép mở rộng D4 từ 12 lên 24 khung
- Luồng E1 sử dụng khung dữ liệu chuẩn E704 hoặc G704 không có khung CRC4 hoặc để ở chế độ không có khung dữ liệu

Tín hiệu Loopback luồng E1 và T1:

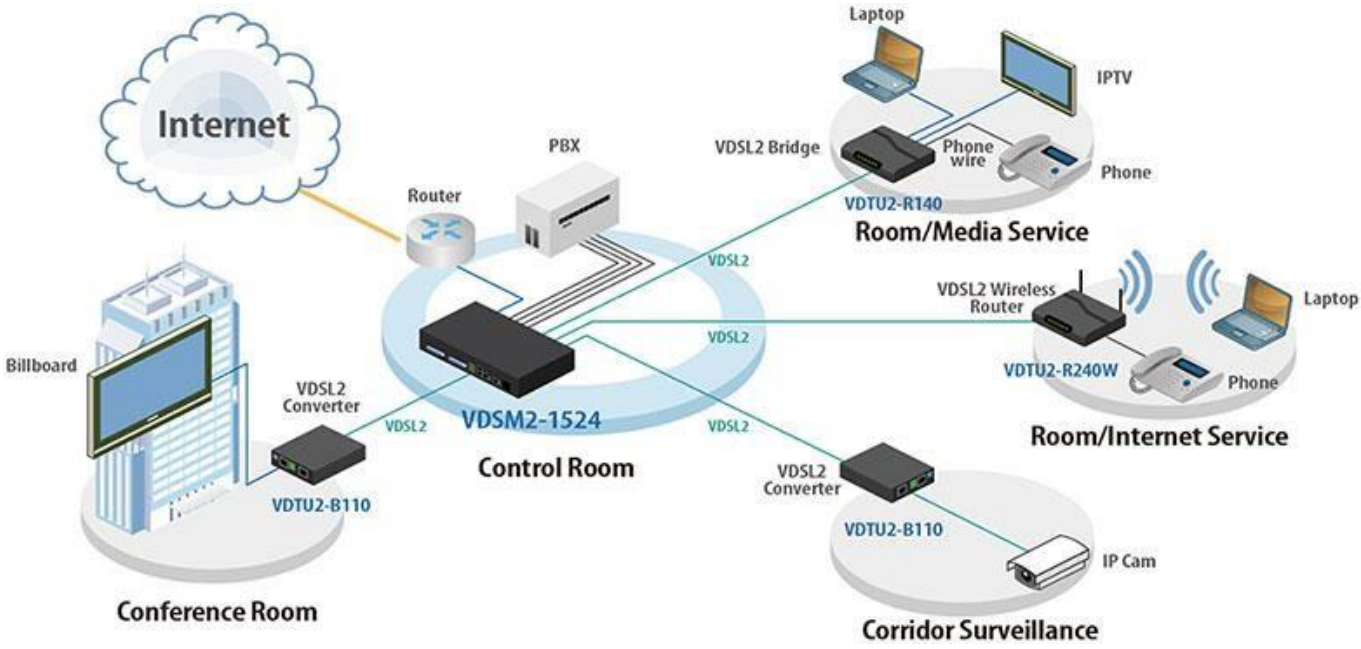
Tín hiệu điều khiển trên các định dang kỹ thuật số T1 và E1 là tín hiệu Loopback. Khi sử dụng tín hiệu Loopback các nhà cung cấp dịch mạng có thể buộc các thiết bị từ xa của một liên kết để truyền lại tín hiệu nhận được của nó trở lại đường truyền, Sau đó, thiết bị truyền có thể xác minh rằng các tín hiệu nhận được khớp với các tín hiệu được truyền không, để thực hiện kiểm tra đầu cuối trên liên kết.

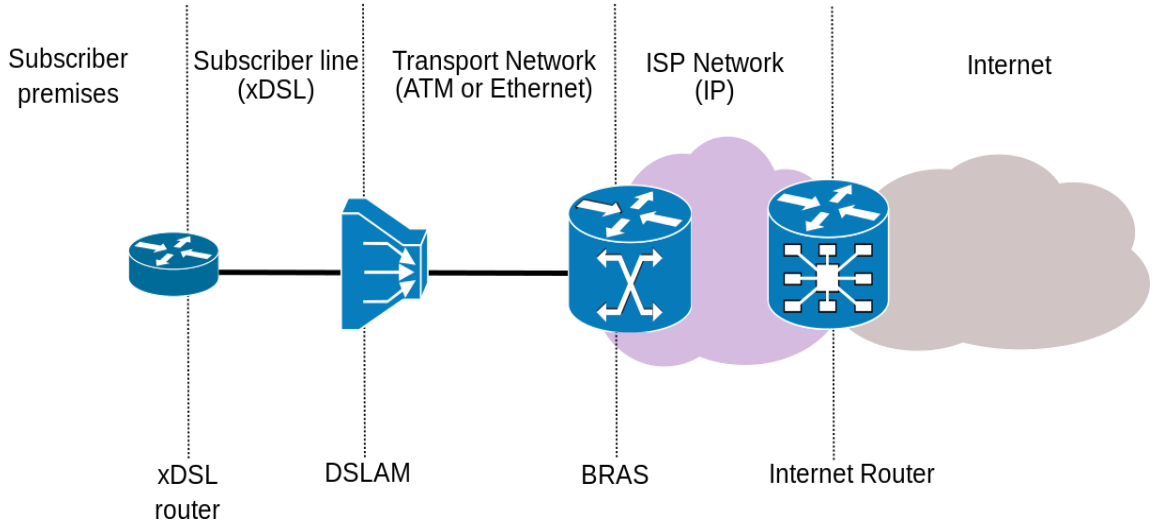
DSL (Digital Subcriber Line - Kênh thuê bao số)

Tổng quan:

Công nghệ Intenet DSL ra đời nhằm mục đích tạo ra một đừng truyền có chất lượng tốt về dịch vụ , đáp ứng nhu cầu truyền thông phủ rộng tới các hộ gia đình; văn phòng. Coong nghệ thay thế ISDL, PSTN vì cho phép truyền tín hiệu số và thực hiện tách tín hiệu qua thiết bị DSLAM (đồng thời truyền nhiều dạng tín hiệu : thoại, Internet; Fax, VoiIP..) **ADSL** là 'liên tục/always-on'' kết nối trực tiếp, sử dụng dải tần số từ 300 Hz tới 3400 Hz.

Ghi chú **ISDN** chạy ở tốc độ cơ sở 64kbps hoặc 128kbps.





DSLAM là gì?

Một thiết bị **DSLAM** có thể tập hợp nhiều kết nối thuê bao ADSL - có thể nhiều tới hàng trăm thuê bao - và tụ lại trên một kết nối cáp quang. Sợi cáp quang này thường được nối tới thiết bị gọi là BAS - Broadband Access Server, nhưng nó cũng có thể không nối trực tiếp tới BAS vì BAS có thể được đặt tại bất cứ đâu.

DSLAM là thiết bị đặt ở phía tổng đài, là điểm cuối của kết nối ADSL. Nó chứa vô số các **Modem ADSL** bố trí về một phía hướng tới các mạch vòng và phía kia là kết nối cáp quang.

BRAS là gì?

Broadband Remote Access Server (BRAS) là thiết bị đặt giữa DSLAM và POP của ISP. Một thiết bị BAS có thể phục vụ cho nhiều DSLAM. Các giao thức truyền thông được đóng gói để truyền dữ liệu thông qua kết nối ADSL, vì vậy mục đích của BAS là mở gói để hoàn trả lại các giao thức đó trước khi đi vào Internet. Nó cũng đảm bảo cho kết nối của bạn tới ISP được chính xác giống như khi bạn sử dụng Modem quay số hoặc ISDN. Như chú giải ở trên, ADSL không chỉ rõ các giao thức được sử dụng để tạo thành kết nối tới Internet. Phương pháp mà PC và Modem sử dụng bắt buộc phải giống như BAS sử dụng để cho kết nối thực hiện được. Thông thường ADSL sử dụng hai giao thức chính là : PPPoE - PPP over Ethernet Protocol. PPPoA - Point to Point Protocol over ATM.

Kết nối mạng

Các thành phần kết nối như thế nào?

Dưới đây sẽ trình bày về những giao thức truyền thông được sử dụng trên kết nối ADSL. Khi kết nối vào Internet, bạn sử dụng các giao thức chạy ở tầng vận chuyển TCP/IP (chẳng hạn như HTTP - giao thức được sử dụng bởi các Web Browser). Quá trình này là giống nhau với các kiểu truy nhập quay số qua PSTN, ISDN và ADSL.

Các giao thức được sử dụng giữa Modem và BAS

Khi quay số PSTN/ISDN để truy nhập vào Internet, chúng ta sử dụng giao thức gọi là PPP để vận chuyển dữ liệu TCP/IP và kiểm tra cũng như xác thực tên và mật khẩu người truy nhập. Trong ADSL, PPP cũng thường được sử dụng để kiểm tra tên và mật khẩu truy nhập, và ATM thì luôn được sử dụng ở mức thấp nhất. Kết nối điển hình như dưới đây :

Vai trò của ATM

ATM - Asynchronous Transfer Mode - được sử dụng như là công cụ chuyển tải cho ADSL ở mức thấp. Lý do vì đó là cách thuận tiện và mềm dẻo đối với các công ty thoại muốn kéo dài khoảng cách kết nối từ DSLAM tới BAS giúp họ có thể đặt BAS ở bất cứ đâu trên mạng. Các tham số thiết lập cấu hình ATM Có hai tham số cần phải thiết lập cấu hình một cách chính xác trên Modem ADSL để đảm bảo kết nối thành công tại mức ATM với DSLAM:

VPI - the Virtual Path Identifier.

VCI - the Virtual Channel Identifier.

Cấu trúc của ADSL

- Vai trò của PPP

PPP là giao thức dùng để vận chuyển lưu lượng Internet tới ISP dọc theo các kết nối Modem và ISDN. PPP kết hợp chặt chẽ các yếu tố xác thực - kiểm tra tên/mật khẩu - và đó là lý do chính mà người ta dùng PPP với ADSL. Mặc dù BAS thực thi giao thức PPP và tiến hành việc xác thực, nhưng thực ra việc đó được thực hiện bằng cách truy nhập vào các cơ sở dữ liệu khách hàng đặt tại ISP. Bằng cách đó, ISP biết được rằng các kết nối do BAS định tuyến tới - đã được xác thực thông qua giao dịch với cơ sở dữ liệu riêng của ISP.

Modem ADSL trên thực tế

Các loại **modem ADSL** thông minh và thụ động

Modem ADSL thông minh bản thân nó đã tích hợp sẵn các giao thức truyền thông cần thiết (Như thiết bị Modem ADSL Router hoặc Modem được sử dụng kết nối qua cổng Card Ethernet 10/100Mb) nên chỉ việc lựa chọn và khai báo VPI/VCI cho Modem.

Còn *Modem ADSL* thụ động thì phải hoạt động dựa trên hệ điều hành của máy tính để cung cấp các giao thức cần thiết. Các loại Modem này bắt buộc phải cài đặt phần mềm điều khiển Modem và thiết lập các giao thức PPP, VPI/VCI. Việc cấu hình như vậy phức tạp và đòi hỏi thời gian nhiều hơn. Chỉ có Windows 98SE, Windows ME và Windows 2000/XP là có cài sẵn cơ chế thực thi ATM, vì thế người ta ít sử dụng các Modem thụ động trên thực tế. Mặc dù các Modem thông minh có hỗ trợ các giao thức cần thiết nhưng chúng vẫn có thể được dùng cho các hệ điều hành nói trên. Các Modem thụ động có thể nối với PC thông qua giao diện USB, hoặc có thể được sản xuất dưới dạng PCI Card để cắm thẳng trên bảng mạch chủ của PC. Lưu ý là việc khai thác giao thức ATM không có nghĩa là cần phải có Card mạng ATM cho PC - đó chỉ là cơ chế hỗ trợ bằng phần mềm trong hệ điều hành.

Mối tương quan giữa thoại và ADSL

Thoại và ADSL cùng chung sống ra sao?

ADSL cho phép cùng lúc vừa truy nhập Internet tốc độ cao lại vừa có thể thực hiện cuộc gọi cũng trên đường dây đó. Thiết bị chuyên dụng Splitters được sử dụng để tách riêng các tần số cao dùng cho ADSL và các tần số thấp dùng cho thoại. Như vậy, người ta thường đặt các Splitters tại mỗi đầu của đường dây - phía thuê bao và phía **DSLAM.**

Tại phía thuê bao, các tần số thấp được chuyển đến máy điện thoại còn các tần số cao đi đến **modem ADSL**. Tại các tổng đài, các tần số thấp được chuyển sang mạng thoại PSTN còn các tần số cao đi đến ISP.

Tốc độ đa dạng

Tốc độ của kết nối giữa modem ADSL và DSLAM phụ thuộc vào khoảng cách đường truyền và tốc độ tối đa được cấu hình sẵn trên cổng của DSLAM. Còn tốc độ kết nối vào Internet lại còn phụ thuộc vào nhiều yếu tố khác nữa như dưới đây :

Số người dùng kết nối vào cùng một DSLAM và thực tế có bao nhiêu người dùng đang khai thác kết nối.

Tốc độ kết nối giữa DSLAM và BAS.

Bao nhiêu card DSLAM cùng nối vào một BAS và bao nhiêu người dùng đang khai thác thực tế kết nối.

Tốc độ kết nối giữa BAS và ISP.

Bao nhiêu BAS kết nối vào ISP và bao nhiêu người dùng thực tế đang khai thác.

Tốc độ của kết nối từ ISP tới mạng Internet toàn cầu.

Bao nhiêu thuê bao của ISP đang khai thác (qua các giao tiếp khác nhau như quay số **PSTN/ ISDN và ADSL**).

ISP tổ chức Caching và Proxy ra sao, liệu thông tin mà bạn cần khai thác đã được lưu trữ trên Cache chưa hay phải tải về từ Internet

ADSL (Download / Upload = 8/2 Mbps) Bất đối xứng

ADSL (*Asymmetrical DSL*) chính là một nhánh của công nghệ xDSL. ADSL cung cấp một băng thông bất đối xứng trên một đôi dây. Thuật ngữ bất đối xứng ở đây để chỉ sự không cân bằng trong dòng dữ liệu tải xuống và tải lên. Dòng dữ liệu tải xuống có băng thông lớn hơn băng thông dòng dữ liệu tải lên. ADSL ra đời vào năm 1989 trong phòng thí nghiệm. ADSL1 cung cấp 1,5 Mbps cho đường dữ liệu tải xuống và 16 kbps cho đường đường dữ tải lên, hỗ trợ chuẩn MPEG-1. ADSL2 có thể cung cấp băng thông tới 3 Mbps cho đường xuống và 16 kbps cho đường lên, hỗ trợ 2 dòng MPEG-1. ADSL3 có thể cung cấp 6 Mbps cho đường xuống và ít nhất 64 kbps cho đường lên, hỗ trợ chuẩn MPEG-2. Dịch vụ ADSL mà chúng ta hay sử dụng hiện nay theo lý thuyết có thể cung cấp cung cấp 8 Mbps cho đường xuống và 2 Mbps cho đường lên, tuy nhiên vì nhiều lý do từ phía các ISP nên chất lượng dịch vụ sử dụng ADSL tại các đầu cuối của chúng ta thường không đạt được như sự quảng cáo ban đầu.

SDSL(Symmetrical DSL) – (Download / Upload = 1.5 Mbps) Đối xứng
Truyền ữ liệu đối xứng với các kiểu tốc độ đường lên = đường xuống 128Kbps, tốc độ trung bình là 256Kbps, 512Kbps, 768Kbps và các mạch dung lượng lớn thường là 1Mbps, 1.5Mbps.

HDSL (Dựa trên chuẩn ISDN T1/E1)
HDSL (high bit-rate DSL) có tốc độ 1.544Mbps và một đôi đôi

HDSL (high bit-rate DSL) có tốc độ 2048Mbps và dùng hai hoặc ba đôi dây

Ra đời trong phòng thí nghiệm vào năm 1986. Thực chất các thiết bị thu phát HSDL là sự kế thừa của ISDN nhưng ở mức độ phức tạp hơn. HDSL ra đời dựa trên chuẩn T1/E1 của Mỹ/châu Âu. HDSL1 cho phép truyền 1,544Mbps hoặc 2,048Mbps trên 2 hay 3 đôi dây. HDSL2 ra đời sau đó cho phép dùng 1 đôi dây để truyền 1,544Mbps đối xứng. HDSL2 ra đời mang nhiều ý tưởng của ADSL. Ưu thể của HDSL là loại công nghệ không cần các trạm lặp, tức là có độ suy hao thấp hơn các loại khác trên đường truyền. Do vậy HDSL có thể truyền xa hơn mà vẫn đảm bảo được chất lượng tín hiệu. HDSL được ưa dùng do có các đặc tính chẩn đoán nhiễu (đo SNR) và ít gây nhiễu xuyên âm. HDSL được dùng bởi các nhà khai thác nội hạt (các công ty điện thoại) hay cung cấp các đường tốc độ cao giữa nhiều tòa nhà hay các khu công sở với nhau.

VDSL

VDSL (*very-high-bit-rate digital subscriber line*) là một công nghệ xDSL cung cấp đường truyền đối xứng trên một đôi dây đồng. Dòng bit tải xuống của VDSL là cao nhất trong tất cả các công nghệ của xDSL, đạt tới 52Mbps, dòng tải lên có thể đạt 2,3 Mbps. VDSL thường chỉ hoạt động tốt trong các mạng mạch vòng ngắn. VDSL dùng cáp quang để truyền dẫn là chủ yếu, và chỉ dùng cáp đồng ở phía đầu cuối.

VDSL là Very High Speed DSL (12.9 tới 52.8Mbps luồng xuống và 1.5 tới 2.3Mbps luồng lên).

RADSL

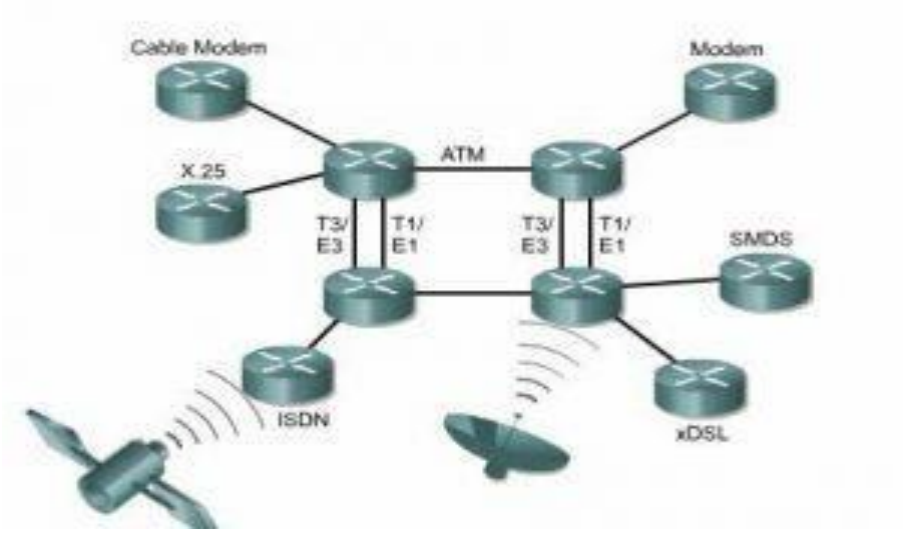
RADSL (*rate-adaptive digital subscriber line*) là một phiên bản của ADSL mà ở đó các modem có thể kiểm tra đường truyền khi khởi động và đáp ứng lúc hoạt động theo tốc độ nhanh nhất mà đường truyền có thể cung cấp. RADSL còn được gọi là ADSL có tốc độ biến đổi.

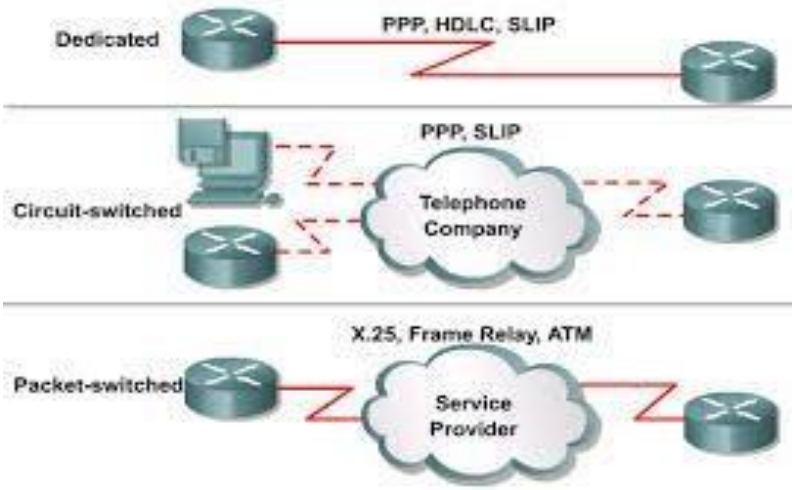
IDSL *(ISDN DSL) có cùng tốc độ 128Kbps hoặc 144Kbps như dịch vụ ISDN*

SL Lite *(còn gọi là G-Lite) là kiểu tốc độ thấp nhất của ADSL*

4.2.2. Một số công nghệ điển hình

Mô hình Tổng quát





Vai trò của router trong mạng WAN

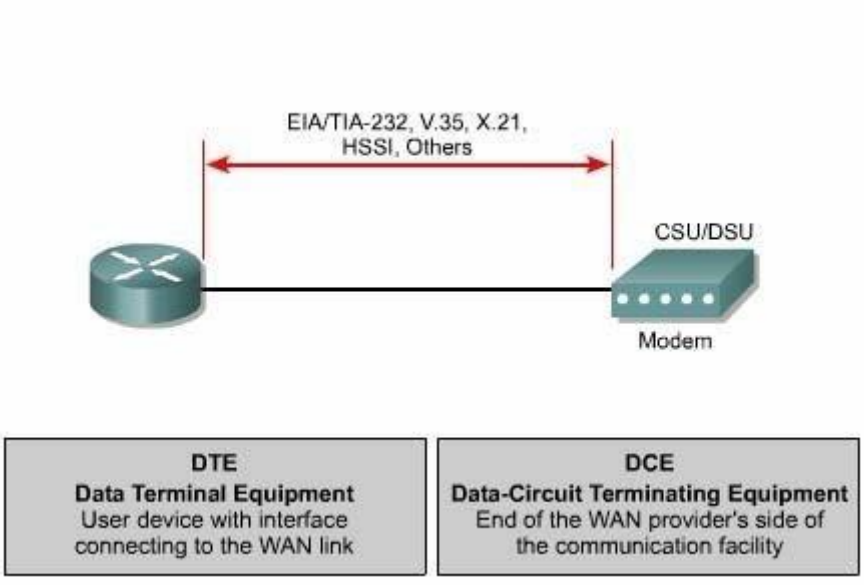
Mạng WAN hoạt động chủ yếu ở lớp vật lý và lớp liên kết dữ liệu. Điều này không có nghĩa là năm lớp còn lại của mô hình OSI không có trong mạng WAN. Điều này đơn giản có nghĩa là mang WAN chỉ khác với mạng LAN ở lớp Vật lý và lớp Liên kết dữ liệu. Hay nói cách khác là các tiêu chuẩn và giao thức sử dụng trong mạng WAN ở lớp 1 và lớp 2 là khác với mạng LAN.

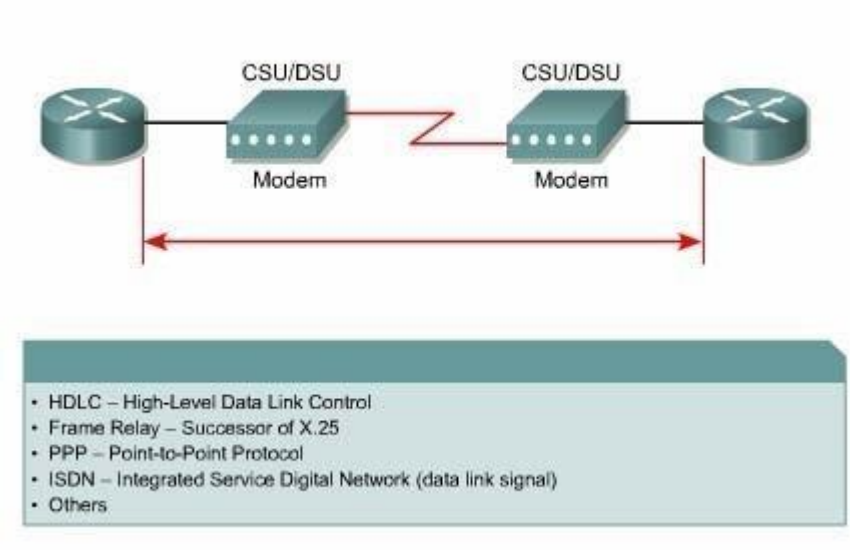
Lớp Vật lý trong mạng WAN mô tả các giao tiếp thiết bị dữ liệu đầu cuối DTE (Data Terminal Equipment) và thiết bị đầu cuối mạch dữ liệu DCE (Data Circuitterminal Equipment). Thông thường, DCE là thiết bị ở phía nhà cung cấp dịch vụ và DTE là thiết bị kết nối vào DCE. Theo mô hình này thì DCE có thể là modem hoặc CSU/DSU.

Chức năng chủ yếu của router là định tuyến. Hoạt động định tuyến diễn ra ở lớp 3 – lớp Mạng trong khi WAN hoạt động ở lớp 1 và 2. Vậy router là thiết bị LAN hay WAN? Câu trả lời là cả hai. Router có thể là thiết bị LAN, hoặc WAN, hoặc thiết bị trung gian giữa LAN và WAN hoặc có thể là LAN và WAN cùng một lúc.

Một trong những nhiệm vụ của router trong mạng WAN là định tuyến gói dữ liệu ở lớp 3, đây cúng là nhiệm vụ của router trong mạng LAN. Tuy nhiên, định tuyến không phải là nhiệm vụ chính yếu của router trong mạng WAN. Khi router sử dụng các chuẩn và giao thức của lớp Vật lý và lớp Liên kết dữ liệu để kết nối các mạng WAN thì lúc này nhiệm vụ chính yêú của router trong mạng WAN không phải là định tuyến nữa mà là cung cấp kết nối giữa các mạng WAN với các chuẩn vật lý và liên kết dữ liệu khác nhau. Ví dụ: một router có thể có một giao tiếp ISDN sử dụng kiểu đóng gói PPP và một giao tiếp nối tiếp T1 sử dụng kiểu đóng gói FrameRelay. Router phải có khả năng chuyển đổi luồng bit từ loại dịch vụ này sang dịch vụ khác. Ví dụ: chuyển đổi từ dịch vụ ISDN sang T1, đồng thời chuyển kiểu đóng gói lớp Liên kết dữ liệu từ PPP sang FrameRelay.

Chi tiết về các giao thức lớp 1 và 2 trong mạng WAN sẽ được đề cập ở tập sau của giáo trình này. Sau đây chỉ liệt kê một số chuẩn và giao thức WAN chủ yếu để các bạn tham khảo:





Các chuẩn và giao thức WAN lớp vật lý: EIA/TIA-232,449, V24, V35, X21, EIA530, ISDN, T1, T3, E1, E3, Xdsl, sonet (oc-3, oc-12, oc-48, oc-192).

Các chuẩn và giao thức WAN lớp liên kết dữ liệu: HDLC, FrameRelay, PPP, SDLC, SLIP, X25, ATM, LAMB, LAPD, LAPF.

Mạng X.25 (Chuyển mạch kênh => Chuyển mạch gói tin)

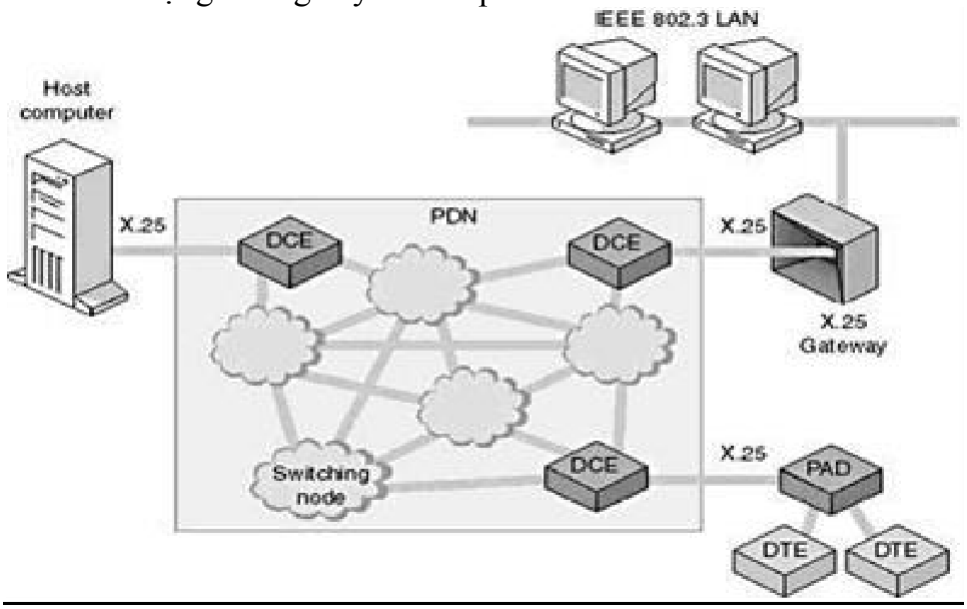
X.25 ra đời vào những năm 1970. Mục đích ban đầu của nó là kết nối các máy chủ lớn (mainframe) với các máy trạm (terminal) ở xa. Ưu điểm của X.25 so với các giải pháp mạng WAN khác là nó có cơ chế kiểm tra lỗi tích hợp sẵn. Chọn X.25 nếu bạn phải sử dụng đường dây tương tự hay chất lượng đường dây không cao.

Hình Mạng X25 trên phương tiện truyền dẫn không ổn định

X.25 là chuẩn của ITU-T cho truyền thông qua mạng WAN sử dụng kỹ thuật chuyển mạch gói qua mạng điện thoại. Thuật ngữ X.25 cũng còn được sử dụng cho những giao thức thuộc Lớp vật lý và Lớp liên kết dữ liệu để tạo ra mạng X.25. Theo thiết kế ban đầu, X.25 sử dụng đường dây tương tự để tạo nên một mạng chuyển mạch gói, mặc dù mạng X.25 cũng có thể được xây dựng trên cơ sở một mạng số. Hiện nay, giao thức X.25 là một bộ các qui tắc xác định cách thức thiết lập và duy trì kết nối giữa các DTE và DCE trong một mạng dữ liệu công cộng (PDN – public data network). Nó qui địch các thiết bị DTE/DCE và PSE (Packet-swiching exchange) sẽ truyền dữ liệu như thế nào.

- Bạn cần phải trả phí thuê bao khi sử dụng mạng X.25
- Khi sử dụng mạng X.25, bạn có thể tạo kết nối tới PDN qua một đường dây dành riêng

- Mạng X.25 hoạt động ở tốc độ 64 Kbit/s (trên đường tương tự)
- Kích thước gói tin (gọi là frame) trong mạng X.25 không cố định
- Giao thức X.25 có cơ chế kiểm tra và sửa lỗi rất mạnh nên nó có thể làm việc tương đối ổn định trên hệ thống đường dây điện thoại tương tự có chất lượng thấp
- X.25 hiện đang được sử dụng rộng rãi ở nhiều nước trên thế giới nơi các mạng số chưa phổ biến cũng như chất lượng đường dây còn thấp



X25 có 2 kiểu LAP và LAPB (LAPB hoàn thiện hơn LAP)
DCE/ DTE là các thiết bị đầu cuối
DTE (Data Terminal Equipment): là thiết bị đầu cuối hoặc máy tính (đóng vai trò đầu cuối)
DEC (Data Circuit-terminating Equipment): đóng vai trò như một Modem

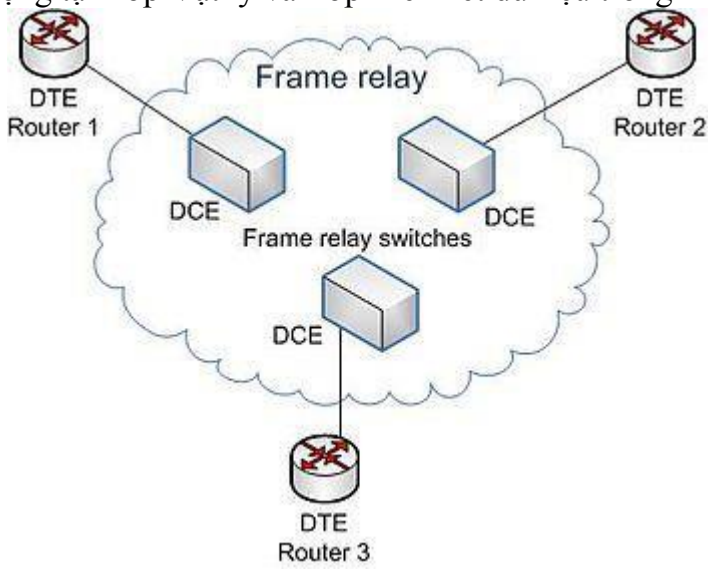
***FRAME RELAY NETWORK* (chuyển mạch gói tin)**

Frame Relay hiệu quả hơn so với X.25 và đang dần dần thay thế chuẩn này. Khi sử dụng Frame Relay, bạn trả phí thuê đường dây tới node gần nhất trên mạng Frame Relay. Bạn gửi dữ liệu qua đường dây của bạn và mạng Frame Relay sẽ định tuyến nó tới node gần nhất với nơi nhận và chuyển dữ liệu xuống đường dây của người nhận. Frame Relay nhanh hơn so với X.25

Frame Relay là một chuẩn cho truyền thông trongmạng WAN chuyển mạch gói qua các đường dây số chất lượng cao. Một mạng Frame Relay có các đặc trưng sau:

- Có nhiều điểm tương tự như khi triển khai một mạng X.25
- Có cơ chế kiểm tra lỗi nhưng không có cơ chế khắc phục lỗi
- Tốc độ truyền dữ liệu có thể lên tới 1.54 Mbit/s
- Cho phép nhiều kích thước gói tin khác nhau
- Có thể kết nối như một kết nối đường trục tới mạng LAN
- Có thể triển khai qua nhiều loại đường kết nối khác nhau (56K, T-1, T-3)

- Hoạt động tại Lớp Vật lý và Lớp Liên kết dữ liệu trong mô hình OSI.



Hình ? Mạng Frame Relay trên phương diện truyền dẫn ổn định

Khi đăng ký sử dụng dịch vụ Frame Relay, bạn được cam kết về mức dịch vụ gọi là CIR (Committed Information Rate). CIR là tốc độ truyền dữ liệu tối đa được cam kết bạn nhận được trên một mạng Frame Relay. Tuy nhiên, khi lưu lượng trên mạng thấp, bạn có thể gửi dữ liệu ở tốc độ nhanh hơn CIR. Khi lưu lượng trên mạng cao, ưu tiên sẽ dành cho những khách hàng có mức CIR cao.

Trong Frame relay, khi gửi thông tin trên mạng WAN thì các thông tin đó được phân thành các frame, mỗi frame sẽ có địa chỉ riêng biệt để xác định đích đến.

Frame relay hoạt động hoàn toàn ở lớp 2 và có 1 số tính năng được dùng như : kiểm tra tính đúng đắn của frame lỗi frame rỗng…nhưng không yêu cầu gửi lại frame khi phát hiện ra frame hỏng.

Chiều dài của frame thay đổi tuỳ theo dữ liệu của người gửi.

Do Frame relay được xây dựng bắt nguồn từ ý tưởng của HDLC (High Data Link Control) nên cấu trúc của gói tin Frame relay cũng tương tự như cấu trúc của HDLC. Nó chứa các trường cờ (flag) bắt đầu và kết thúc dùng để phân định và thừa nhận frame trên liên kết các truyền thông và bảo vệ thông tin đi giữa. Nó không chứa một trường địa chỉ riêng biệt, mà nó kết hợp trường địa chỉ và trường điều khiển lại với nhau và được thiết kế như là header trong Frame relay. Trương thông tin chứa dữ liệu của người dùng. Và FCS (frame check sequence) dùng để kiểm tra các frame có bị hỏng hay không trong lúc truyền trên liên kết của các thiết bị truyền thông.

Header của frame trong Frame relay co 6 trường :

+ DLCI : Bit nhận dạng đường nối dữ liệu

+ C/R : Bit trao đổi thông tin

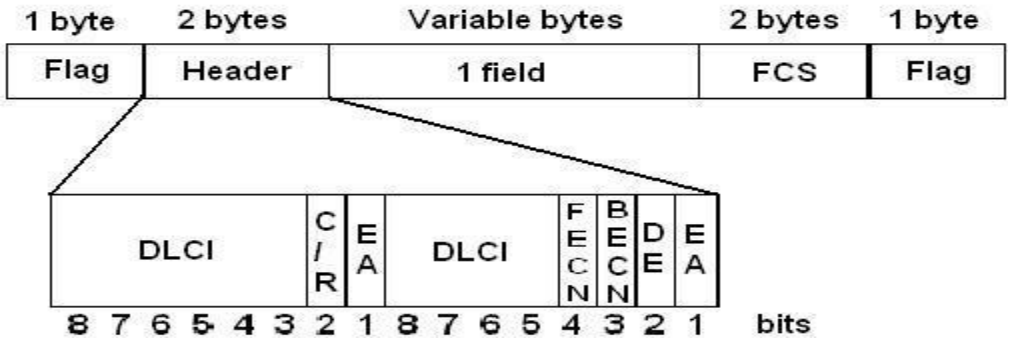
+ EA : Bit mở rộng địa chỉ

+ FECN : Bit thông báo tắc nghẽn tới

+ BECN : Bit thông báo tắc nghẽn lùi

+ DE : Bit hủy frame

Figture :
The Frame relay PDU (frame)

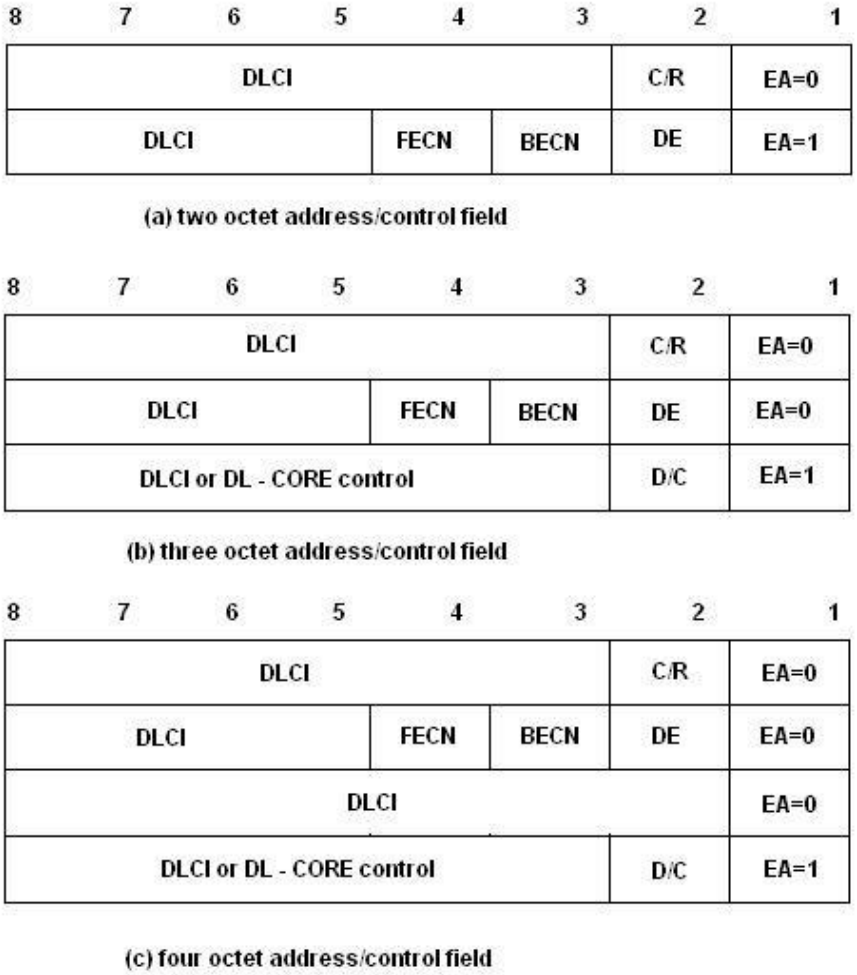


PDU Frame relay

lượng qua mạng giữa mạng cục bộ UNI đến mạng UNI từ xa :

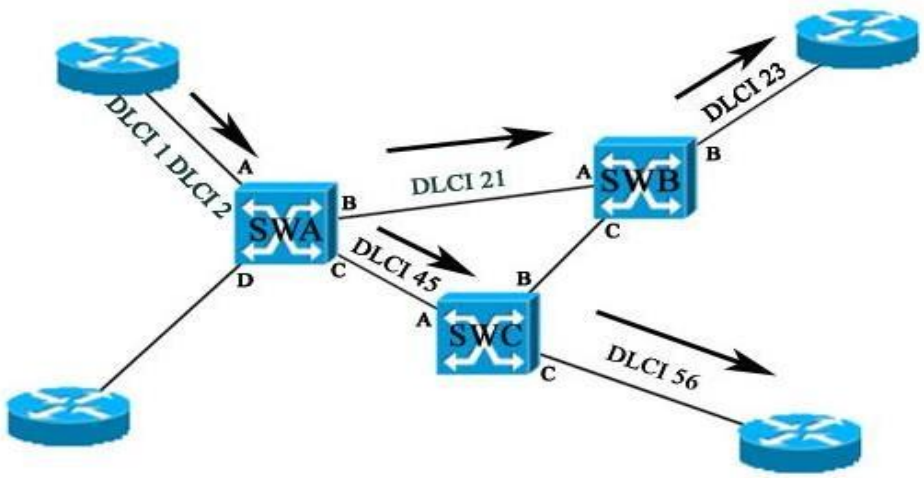
Frame Relay Header

Figture : Frame relay header formats



Hình ? Các định dạng của header Frame relay

DLCI trong mạng Frame Relay:



SWA

In Port	DLCI	Out Port	DLCI
A	1	B	21
A	2	C	45

SWB

In Port	DLCI	Out Port	DLCI
A	21	B	23

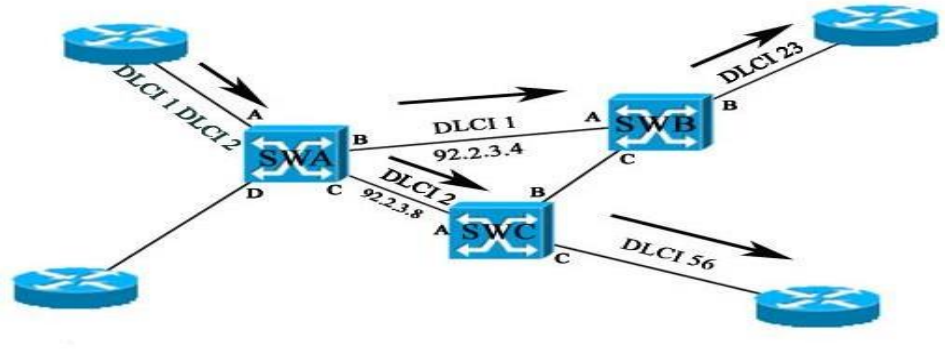
SWC

In Port	DLCI	Out Port	DLCI
A	45	C	56

Hình ? Ánh xạ DLCI

Trong hình trên: SWA chấp nhận các frame từ port A có chứa DLCI 1 va DLCI 2 trong header của frame. Khi truy xuất tới bảng định tuyến và tìm thấy có chứa DLCI 1 nên chuyển đến port B và DLCI1 này được ánh xạ thành DLCI 21. frame có chứa DLCI2 sẽ được chuyển đến port C và được ánh xạ thành DLCI 45. Các frame này sẽ được chuyển đến SW B và SW C. qua bảng định tuyến SW B và SW C sẽ thực hiện tương tự SW A và phân phát đến các UNI từ xa để đến thiết bị người dùng cuối cùng, mà trong ví dụ này là các router.

<u>Sử dụng header mạng nội địa trong mạng.</u>



SWA

In Port	DLCI	Out Port	Add
A	1	B	92.2.3.4
A	2	C	92.2.3.8

SWB

In Port	Add	Out Port	DLCI
A	92.2.3.4	B	23

SWC

In Port	DLCI	Out Port	DLCI
A	45	C	56

Hình ? Dùng các Header bên trong mạng nội bộ

Các chuẩn của Frame relay thiết lập các thủ tục cho sự ánh xạ của các DLCI giữa các máy tại UNI và NNI. Các hoạt động xảy ra trong 1 mạng có thể chắc chắn theo sự chỉ đạo của Frame relay. Tuy nhiên vài đại lý và các nhà cung cấp sử dụng 1 hệ thống độc quyền cho các hoạt động trong 1 mạng nếu như các phần chuyển đổi được sản xuất bởi cùng 1 đại lý.Với điều này các thiết bị chuyển đổi được cấu hình với các giao thức sở hữu riêng và có thể kết nối 1 cách khá dể dàng. Các header của mạng nội địa thường hỗ trợ các hoạt động kết nối không kênh (connectionless), cho phép chức năng, thích ứng trong mạng.

Ý nghĩa của DLCI :

+ ý nghĩa cục bộ (local significance):

Các DLCI có thể được quản lý như là các con số và có thể được tái sử dụng bởi 1 mạng. Điều này được biết như là ý nghĩa cục bộ, và có thể các mạch ảo (virtual circuit) được thiết lập nhiều hơn để được tạo ra trong 1 mạng Frame relay. Bởi vì các giá trị của các DLCI có thể được tái sử dụng tại mỗi interface vật lý (hay còn gọi là logical port) tại mỗi UNI. Tuy nhiên phải cẩn thận khi lấy số DLCI có ý nghĩa cục bộ và không biết đến các router khác.

+ ý nghĩa toàn cầu (Global significance) :

Một số các tuỳ chọn thêm vào là phần của chuẩn Frame relay. Tuỳ chọn ý địa chỉ toàn cầu sẽ cho phép một DLCI chỉ định như là một con số có ý nghĩa chung. Điều này có nghĩa là số point này sẽ đến cùng 1 đích bất chấp router nguồn nào.

Với hai octet trong header của frame thì cho phép tói 1024 DLCI trong toàn thể mạng, bởi vì các DLCI có thể không được tái sử dụng tại một port khác. Thực tế theo chuẩn thì chỉ có 992 DLCI được tạo ra, bởi vì 32 DLCI đã được dành riêng cho quản lý mạng bên trong.

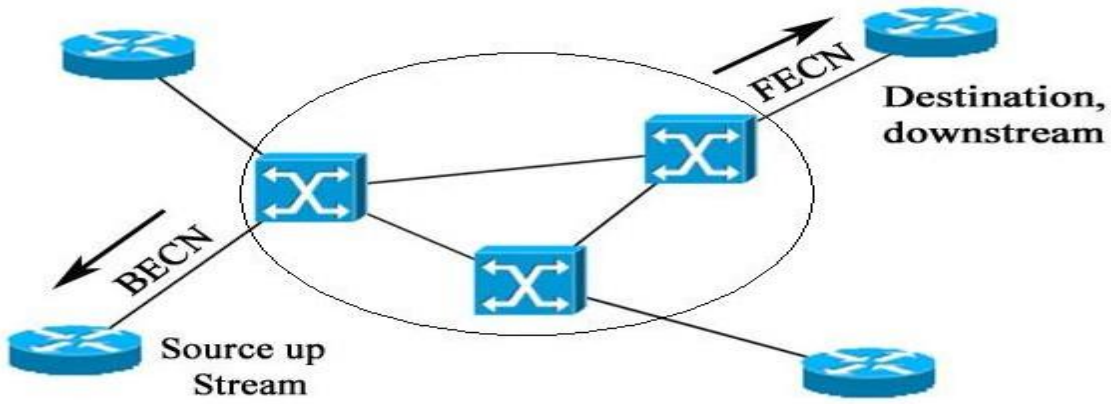
Sử dụng DLCI toàn cầu trên PVC, thì mỗi phần chuyển đổi Frame relay phải có các bảng để cung cấp chỉ thị là lảm thế nào để chuyên lưu lượng giữa các thiết bị chuyển đổi và các thiết bị cuối.

C/R – Command/respond

Bit này dùng o thủ tục hỏi và đáp, nhưng mạng Frame relay không dùng đến mà chi dành cho các thiết bị đầu cuối (FRAD) sử dụng mỗi khi cần trao đổi thông tin cho nhau, Bit C/R do FRAD đặt giá trị và được giữ nguyên khi truyền qua mạng.

Bit FECN và Bit BECN

Hai kỹ thuật dùng để thông báo cho user, router hay là các phần chuyển đổi về sự tắc nghẽn. Các khả năng đó có thể thực hiện được bởi bit báo tắc nghẽn tiến FECN (forward explicit congestion notification) và bit báo tắc nghẽn lùi BECN (backward explicit congestion notification). Xem hình :



Hình ? Các bit thông báo tắc nghẽn

Các phần chuyển đổi của Frame relay bắt đầu tắc nghẽn khi xảy ra vấn đề như bộ nhớ đệm của nó trở nên đầy hay có vấn đề về quản lý bộ nhớ. Các phần chuyển đổi phải thông báo cho các node theo hướng tiến của luồng data và các node theo hướng ngược lại của luồng data về các vấn đề xảy ra bằng cách dùng các bit FECN và BECN.

Bit BECN sẽ được bật lên (tức là set nó thành 1) trong frame và gửi nó theo hướng ngược lại (tức là hướng có frame đi tới) để dùng báo cho nguồn của lưu lượng rằng tắc nghẽn đang tồn tại ở các phần chuyển đổi trong kết nối. Thông báo này cho phép các máy nguồn để điều khiển lưu lượng cho đến khi tắc nghẽn được giải quyết.

Bit FECN có thể set bằng 1 trong frame, và gửi đến node theo hướng tiến để dùng báo rằng tắc nghẽn đang xảy ra ở hướng phía ngược lại. Bit FECN được truyền đến giao thức của lớp phía trên (như là lớp transport) để cho phép nó làm chậm lại các xác nhận đến lớp transport của

hướng ngược lại của luồng data (tức là hướng có frame đi tới) hoặc để hạn chế giới hạn điều khiển luồng ở các máy nguồn

ATM (Chuyển Mạch gói tin) – Cell Relay

Giới thiệu chung về ATM

-ATM(Asynchronous Transfer Mode) là công nghệ chuyển mạch gói tương thích với mọi loại hình dịch vụ hiện nay. Nó được dùng trong cả mạng truy nhập lẫn mạng lõi.
-Dữ liệu cần gởi được chia thành các gói có độ dài cố định là 53 bytes, được gọi là một tế bào (cell).

ATM (Asynchronous Transfer Mode) là công nghệ chuyển mạch gói tương thích với mọi loại hình dịch vụ hiện nay. Nó được dùng trong cả mạng truy nhập lẫn mạng lõi. Hoạt động ở tầng 2 datalink của OSI

-Dữ liệu cần gởi được chia thành các gói có độ dài cố định là 53 bytes, được gọi là một tế bào (cell).

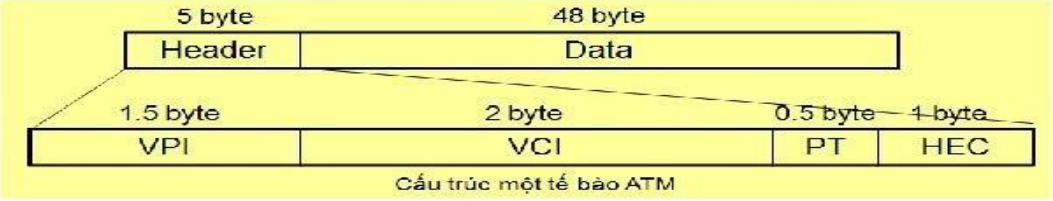
ATM (Asynchronous Transfer Mode – Chế độ truyền không đồng bộ) là hệ thống chuyển mạch gói tiên tiến, có thể truyền đồng thời dữ liệu, âm thanh và hình ảnh số hoá trên cả mạng LAN và mạng WAN.

Đây là một trong những phương pháp kết nối mạng WAN nhanh nhất hiện nay, tốc độ đạt từ 155 Mbit/s đến 622 Mbit/s. Trên thực tế, theo lý thuyết nó có thể hỗ trợ tốc độ cao hơn khả năng hiện thời của các phương tiện truyền dẫn hiện nay. Tuy nhiên, tốc độ cao có nghĩa là chi phí cũng cao hơn, ATM đắt hơn nhiều so với ISDN, X25 hoặc FrameRelay. Các đặc trưng của ATM bao gồm:

Sử dụng gói dữ liệu (cell) nhỏ, có kích thước cố định (53 byte), dễ xử lý hơn so với các gói dữ liệu có kích thước thay đổi trong X.25 và Frame Relay.

- Tốc độ truyền dữ liệu cao, theo lý thuyết có thể đạt 1,2 Gbit/s
- Chất lượng cao, độ nhiễu thấp nên gần như không cần đến việc kiểm tra lỗi
- Có thể sử dụng với nhiều phương tiện truyền dẫn vật lý khác nhau (cáp đồng trục, cáp dây xoắn, cáp sợi quang)
- Có thể truyền đồng thời nhiều loại dữ liệu

Chuyển mạch ATM

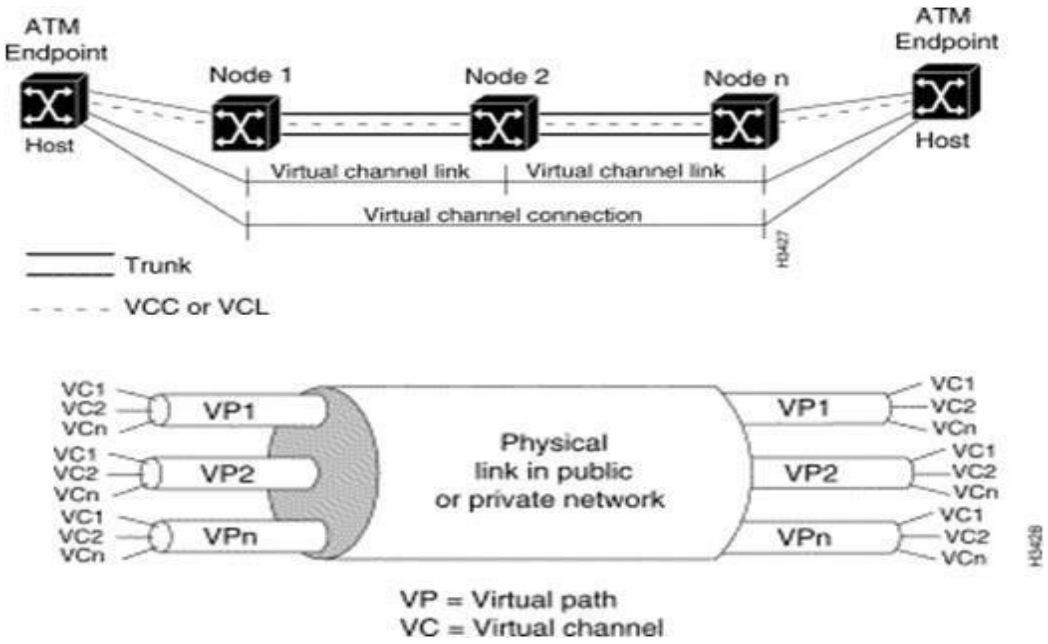


Cấu trúc một tế bào ATM

- VPI (Virtual Path Indentifier): nhận dạng đường ảo, dùng để phân biệt đường truyền nào trong số các đường nối tới một nút
- VCI (Virtual Channel Indentifier): nhận dạng kênh ảo, dùng để phân biệt kênh nào được dùng trong đường truyền trên
- PT (Payload Type): phân biệt dữ liệu của dịch vụ hay người dùng mà được đóng gói trong cell ATM đang gửi
- HEC (Header Error Check): Dùng CRC kiểm tra lỗi bit của trường header
-Tại mỗi nút ATM sẽ dựa vào 2 trường VPI và VCI để chuyển mạch gói tin.
-Chỉ thực hiện kiểm tra lỗi của header nên tốc độ rất nhanh
- Vì cấu trúc của 1 cell là cố định 53 bytes nên có thể thiết kế hệ thống chuyển mạch ngay trong thiết bị phần cứng chứ không cần dùng phần mềm như các công nghệ chuyển mạch gói khác. Điều này làm tăng đáng kể tốc độ chuyển mạch
- Đảm bảo chất lượng dịch vụ thông qua việc thiết lập các kênh ảo thường trực PVC (Permanent Virtual Channel) ưu tiên để cấp băng thông cho từng loại dịch vụ hay thông qua thõa thuận với người dùng.

- Khả năng nhóm một vài kênh ảo(VC) thành một đường ảo nhằm giúp cho việc định tuyến được dễ dàng

Hoạt động ATM



Chuyển mạch ATM có một số đặc điểm như sau:

-Công nghệ chuyển mạch lớp 2 trong mô hình OSI

-Chuyển tiếp gói tin theo cơ chế định hướng kết nối (Connection Operation).

-Kích thước gói tin cell nhỏ, cố định giúp chuyển mạch nhanh

-Truyền tải các dữ liệu nhạy theo thời gian: tiếng nói, dữ liệu, video và dữ liệu đa phương tiện

-Xếp chồng hoạt động layer3 (IP) lên layer2 (ATM)

+Đáp ứng thời gian thực

+Tốc độ cao

+Chất lượng dịch vụ

+Điều khiển lưu lượng

+Triển khai trên các mạng trục xương sống tốc độ cao

-Ưu điểm của giải pháp này là sử dụng ATM có khả năng truyền nhiều loại tín hiệu khác nhau trong cùng đường truyền với yêu cầu chất lượng dịch vụ khác nhau. Một ưu điểm khác khi sử dụng ATM là tính mềm dẻo khi cung cấp dịch vụ mạng.

Hạn chế

-Thiết lập các liên kết PVC(permanent virtual circuits - các mạch ảo cố định) tại N điểm nút

-Phân cắt mạng IPoATM ra thành nhiều mạng logic nhỏ (LIS:logical IP subnet), giữa các LIS dùng bộ định tuyến trung gian để liên kết.

-Không đảm bảo QoS thực sự

-Hai giao thức này riêng lẽ nên phải dùng một loạt các giao thức phức tạp khác để kết nối.
-Quản lý và điều khiển IP over ATM phức tạp hơn so với quản lý và điều khiển IP qua mạng thuê riêng (IP - Leased line)

Chương 5. LẬP TRÌNH LIÊN MẠNG SOCKET

5.1. Mô hình và cơ chế giao tiếp mạng

5.1.1. Mô hình giao tiếp client/server

5.1.2. Socket và cơ chế giao tiếp mạng

5.2. Lập trình client/server hướng kết nối

5.2.1. Thủ tục trao đổi dữ liệu theo mô hình client/server hướng kết nối

5.2.2. Cấu trúc ứng dụng theo mô hình client/server hướng kết nối

5.3. Lập trình client/server không hướng kết nối

5.3.1. Thủ tục trao đổi dữ liệu theo mô hình client/server không hướng kết nối

5.3.2. Cấu trúc ứng dụng theo mô hình client/server không hướng kết nối

Tham khảo phụ Lục 1

Phụ lục 1. LẬP TRÌNH LIÊN MẠNG SOCKET

https://learn.vtc.edu.vn/courses/lap-trinh-mang-can-ban/lectures/3548630

https://learn.vtc.edu.vn/courses/lap-trinh-mang-can-ban/lectures/3548625

https://learn.vtc.edu.vn/courses/lap-trinh-mang-can-ban/lectures/4144126

http://dotnet.edu.vn/ChuyenMuc/Trong-lap-trinh-Socket-dung-de-lam-gi-985.aspx

https://kipalog.com/posts/Tim-hieu-ve-lap-trinh-socket---Buoc-dau-lam-quen

https://giai-ma.blogspot.com/2016/04/so-sanh-2-giao-thuc-tcp-va-udp.html

https://topdev.vn/blog/socket-la-gi-websocket-la-gi/

Phụ lục 2. GIAO THỨC ĐỊNH TUYẾN

https://vnpro.vn/thu-vien/khai-niem-va-phan-loai-dinh-tuyen-2346.html

https://vnpro.vn/thu-vien/lua-chon-giao-thuc-dinh-tuyen-trong-mang-phan-1-2384.html

http://svuit.vn/threads/bai-11-tim-hieu-cac-giao-thuc-dinh-truyen-mang-42/

http://svuit.vn/threads/bai-13-tim-hieu-ve-giao-thuc-dinh-tuyen-rip-78/

http://svuit.vn/threads/bai-14-tim-hieu-giao-thuc-dinh-tuyen-ospf-101/

http://svuit.vn/threads/bai-15-tim-hieu-giao-thuc-dinh-tuyen-eigrp-114/

http://svuit.vn/threads/chapter-4-1-overview-is-is-protocol-part-1-627/

https://vnpro.vn/thu-vien/so-luoc-ve-giao-thuc-dinh-tuyen-bgp-2061.html

http://svuit.vn/threads/bgp-ba%CC%80i-1-co-ba%CC%89n-bgp-1089/

Chuyển đổi tốc độ Mbps – Mb/s

https://www.gbmb.org/mbps-to-mbs