

## Bài 1: **Frame relay**

Frame relay vẫn là công nghệ WAN được triển khai nhiều nhất có dùng router. Đã có một sự chuyển đổi dần dần từ FR sang các công nghệ như VPN dựa trên nền IP và MPLS-VPN. Tuy nhiên Frame relay sẽ vẫn đóng một vai trò lớn trong các mạng doanh nghiệp trong một tương lai trước mắt.

Chuẩn FR được phát triển bởi nhiều nhóm nghiên cứu. Ban đầu, Cisco và các công ty khác (còn được gọi là gang of four) phát triển một chuẩn giúp cho tính tương thích của FR và phát triển sản phẩm. Sau đó một diễn đàn về Frame relay Framerelay Forum được thành lập nhằm phát triển FR. IETF hiện định nghĩa vài RFC liên quan đến việc dùng FR như là giao thức lớp 2 trong mạng IP.

Tài liệu Cisco IOS thường mô tả các chuẩn của FR thông qua các thỏa hiệp hiện thực FRF, ví dụ FRF.12 liên quan đến đặc tả cho tiến trình phân mảnh. Cuối cùng, ANSI và ITU xây dựng trên các chuẩn này để chuẩn hóa FR theo chuẩn quốc gia của Mỹ và quốc tế.

### **Các mạch ảo của Frame Relay:**

Công nghệ Frame Relay thường chuyển các frame từ nguồn đến đích trên những đường dẫn kết nối ảo. Các đường đi ảo này có thể là các mạch ảo thường trực (permanent virtual circuits - PVCs) hoặc các mạch ảo chuyển mạch (switched virtual circuits - SVCs).

Một PVC thường được thiết lập bởi các nhà cung cấp dịch vụ khi họ lập trình các tổng đài Frame Relay Switch. Tùy thuộc vào thỏa thuận với nhà cung cấp, một khách hàng hoặc một PVC của người dùng có thể được cấu hình để mang lưu lượng đến một tốc độ nào đó được gọi là tốc độ thông tin cam kết (committed information rate - CIR).

CIR là tốc độ truyền mà mạng Frame Relay hoặc nhà cung cấp đồng ý truyền trong tình trạng bình thường, đây cũng là tốc độ trung bình trong một khoảng thời gian nào đó. Đơn vị của CIR là bits trên giây.

Mỗi kết nối PVC ở cuối mỗi thiết bị đầu cuối được xác định bằng một địa chỉ có chiều dài 10 bit trong phần header đầu của frame, còn được gọi là DLCI. DLCI thường được dùng để ánh xạ đến địa chỉ lớp mạng của đích đến, tức địa chỉ của router ở đầu xa của mạch PVC. Sau đó dữ liệu cần được truyền trên hạ tầng Frame relay sẽ được đóng gói trong các header này.

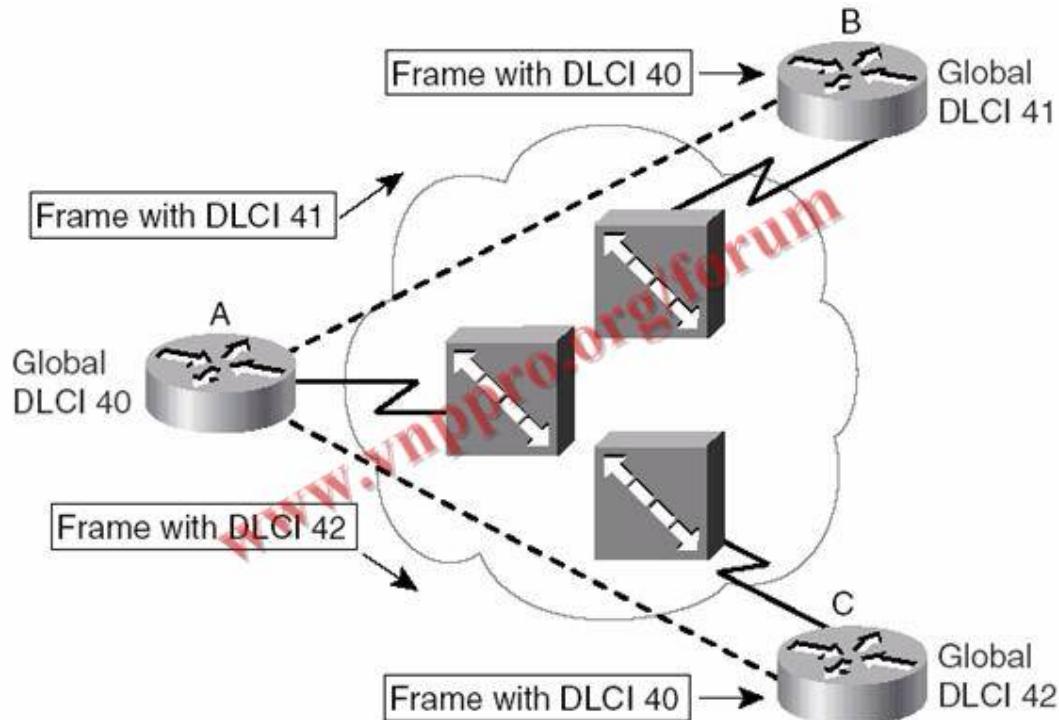
Mỗi header trong Frame Relay được chèn vào giá trị DLCI tương ứng đến địa chỉ lớp mạng của đích đến. Các frame sau đó sẽ được gửi đến tổng đài với giá trị DLCI ban đầu. Các frame này tiếp tục được trung chuyển về phía mạng đích

thông qua các tổng đài của các nhà cung cấp dịch vụ FR. Các tổng đài FR có thể thay đổi giá trị DLCI sang các PVC khác trên đường đi về đích. Kết quả là, giá trị DLCI của một frame không nhất thiết phải là giống như giá trị ban đầu khi frame đi vào mạng Frame Relay. Vì vậy, giá trị DLCI chỉ có ý nghĩa cục bộ. Ngoài ra, cả hai đầu của PVC có thể dùng cùng giá trị DLCI, ví dụ DLCI 200. Tuy nhiên, ở cuối một kết nối, một DLCI không thể tượng trưng cho nhiều hơn một PVC.

### Thông số nhận dạng kết nối lớp datalink DLCI :

Để kết nối hai thuê bao Frame Relay DTE, nhà cung cấp dịch vụ FR sẽ dùng một mạch ảo giữa hai router đầu cuối. Một router có thể gửi ra một frame Frame Relay, trong đó có một trường có chiều dài 10-bit để nhận dạng từng VC, gọi là *Data Link Connection Identifier (DLCI)*.

Các tổng đài trung gian FR chuyển các frame dựa trên thông tin trên giá trị DLCI của frame, cho đến khi frame thực sự thoát ra khỏi tổng đài để đến router trên đầu kia của kết nối. Các giá trị FR DLCI chỉ có ý nghĩa cục bộ, nghĩa là một giá trị DLCI nào đó chỉ có ý nghĩa trên một kết nối đơn. Kết quả là giá trị DLCI của một frame có thể thay đổi khi frame đi qua một mạng. Năm bước dưới đây hiển thị các giá trị DLCI cục bộ cho một mạch ảo trong hình vẽ.



- Router A gửi ra một frame với giá trị DLCI 41.
- Tổng đài FR xác định frame là một phần của mạch VC kết nối router A đến routerB.
- Tổng đài FR thay thế trường DLCI của frame bằng giá trị 40.

Trong thực tế, một vài nhà cung cấp dịch vụ dùng địa chỉ DLCI toàn cục. Qui ước DLCI truyền thống cho phép ta suy nghĩ router có một địa chỉ đơn duy nhất, cũng tương tự như vai trò của địa chỉ MAC. Tuy nhiên các địa chỉ vẫn là cục bộ và một giá trị DLCI của một mạch ảo VC vẫn có thể bị thay đổi giá trị khi nó đi qua một hệ thống mạng. Ví dụ, cho cùng một VC từ routerA đến RouterB, chỉ ra routerA có DLCI là 40 và routerB có DLCI là 41.

Ý tưởng của địa chỉ toàn cục thì cũng giống như trong LAN. Ví dụ, khi router A gửi một frame đến Router B, router A sẽ gửi frame đến địa chỉ toàn cục của router B (41). Tương tự, routerB sẽ gửi một frame đến địa chỉ toàn cục của router A (40).

### **Các thông điệp quản lý trạng thái cổng nội bộ (Local Management Interface – LMI)**

Các thông điệp LMI trong FrameRelay giúp ta quản lý trạng thái đường truyền giữa router thuê bao và tổng đài FR. Một router thuê bao dịch vụ FR có thể gửi các thông điệp truy vấn về trạng thái đến tổng đài và tổng đài sẽ trả lời bằng thông điệp trạng thái LMI Status để thông báo cho router về giá trị DLCI của mạch ảo VC cũng như là trạng thái của từng mạch VC này.

Ở chế độ mặc định, thông điệp LMI được gửi mỗi 10 giây. Cứ mỗi thông điệp thứ sáu sẽ mang đầy đủ thông tin về trạng thái, trong đó bao gồm thông tin đầy đủ hơn về từng VC.

Các thông điệp truy vấn LMI Status enquiry (từ router) và Status (từ tổng đài) cũng hoạt động như cơ chế keepalive. Một router sẽ xem các cổng của nó là bị hỏng nếu router không thể nhận thông điệp từ tổng đài trong ba chu kỳ (mỗi chu kỳ là 10 giây). Kết quả là, cơ chế LMI trong Frame Relay thực sự được cho phép hoặc không được cho phép bằng cách dùng lệnh keepalive/no keepalive trên cổng Frame Relay của router. **Nói cách khác, lệnh no keepalive sẽ tắt các thông điệp LMI.**

Có ba loại thông điệp LMI tồn tại, chủ yếu là do có nhiều nhà cung cấp thiết bị và các chuẩn khác nhau để phát triển FR. Kiểu được định nghĩa sớm nhất, được gọi là Cisco LMI thì hơi khác với các kiểu ANSI và ITU được định nghĩa sau đó. Sự khác nhau ở điểm:

- Cisco LMI cho dùng các giá trị DLCI được phép, tức dãy số DLCI cho phép.
- Các giá trị DLCI được dùng để gửi thông điệp LMI.

Nói một cách thực tế, các vấn đề này ít quan trọng. Mặc định router sẽ tự động dò tìm loại LMI. Nếu cần thiết, lệnh frame-relay lmi-type có thể được dùng để chỉ ra kiểu LMI được dùng trên đường truyền Frame Relay.

Bảng dưới đây liệt kê ba kiểu LMI, từ khóa type cùng với vài điểm so sánh liên quan đến LMI và các giá trị DLCI cho phép. Ví dụ kiểu LMI của Cisco cho phép dùng các giá trị DLCI từ 16 cho đến 1007. Kiểu LMI của ANSI cho phép dùng DLCI từ 16 đến 991. Giá trị DLCI được dùng để bởi chính LMI để truyền và nhận các thông điệp cũng khác nhau. Cisco LMI dùng DLCI 1023, còn ANSI LMI dùng DLCI 0.

Kiểu LMI	Tài liệu nguồn	Các thông số Cisco IOS LMI Type	Dãy DLCI cho phép (số lượng)	LMI DLCI
Cisco	Riêng	Cisco	16–1007 (992)	1023
ANSI	T1.617 Annex D	ANSI	16–991 (976)	0
ITU	Q.933 Annex A	q933a	16–991 (976)	0

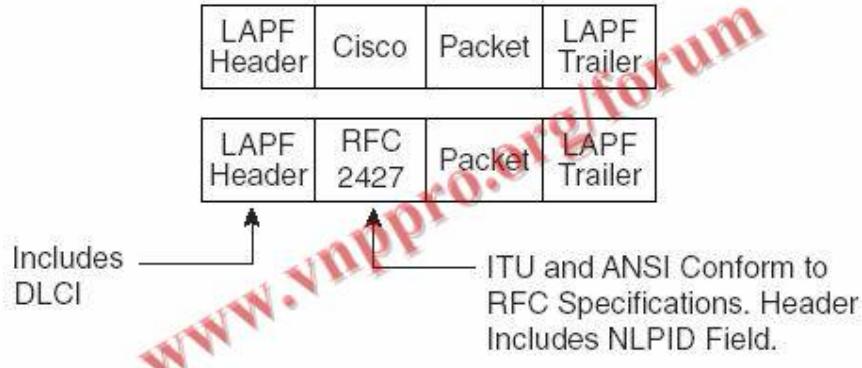
### Frame Relay Headers và quá trình đóng gói FR

Router tạo ra các frame bằng cách dùng các header liên tiếp khác nhau. Header đầu tiên là ITU *Link Access Procedure for Frame-Mode Bearer Services (LAPF)*. Header LAPF bao gồm tất cả các trường được dùng bởi tổng đài FR để phân phối các frame trên đám mây FR, các trường này bao gồm DLCI, DE, BECN và FECN.

Các trường theo sau phần LAPF sẽ chứa các thông tin quan trọng cho các router thuê bao trên đầu cuối của VC. Đối với đoạn header đóng gói, có hai tùy chọn tồn tại:

- Các loại header do Cisco định nghĩa ban đầu.
- Header được định nghĩa bởi IETF trong RFC 2427 (trước đây là RFC 1490).

Nếu ta dùng Cisco router ở cuối mỗi VC, tùy chọn Cisco là phù hợp và làm việc tốt. Trong khi, tùy chọn ietf là cần thiết trong trường hợp dùng nhiều sản phẩm của các hãng khác nhau. Cả hai header đều có một trường có tên là protocol để hỗ trợ nhiều giao thức lớp 3 trên một VC. Trường được dùng nhiều nhất là trường xác định giao thức lớp mạng *Network Layer Protocol ID*, được mô tả trong RFC2427. Hình dưới đây mô tả cấu trúc của header và trailer.



Mỗi VC mặc định đều dùng header của Cisco trừ phi được cấu hình để dùng header kiểu IETF. Có ba phương thức được dùng để cấu hình một VC dùng kiểu header IETF:

- Dùng lệnh encapsulation frame-relay ietf. Lệnh này sẽ thay đổi trạng thái mặc định của cổng đó sang IETF thay vì dùng cisco.
- Dùng lệnh frame-relay interface-dlci number ietf, bỏ qua trạng thái mặc định cho VC này.
- Dùng lệnh frame-relay map dlci...ietf. Lệnh này cũng sẽ thay đổi trạng thái mặc định của VC.

Ví dụ, trên một cổng có 10 VC, trong đó có bảy VC cần phải dùng kiểu đóng gói IETF, cổng có thể chuyển sang IETF bằng lệnh encapsulation frame-relay ietf. Sau đó, lệnh frame-relay interface-dlci number cisco có thể được dùng cho ba VC cần chạy theo kiểu đóng gói Cisco.

### Các tín hiệu báo nghẽn DE, BECN và FECN trong Frame Relay

Mạng FR, cũng giống như các mạng đa truy cập khác, có thể tạo ra nghẽn do vấn đề tốc độ không đồng bộ. Ví dụ một mạng Frame Relay có 20 thuê bao với các đường 256 kbps và một văn phòng chính có băng thông mức T1. Nếu cả 20 site gửi các frame liên tục về văn phòng chính ở cùng một thời điểm, ta sẽ có khoảng 5Mbps dữ liệu cần đi ra khỏi đường T1 1.5Mbps, làm cho hàng đợi của tổng đài FRSwitch tăng nhanh.

Tương tự, khi văn phòng chính cần gửi dữ liệu đến bất kỳ chi nhánh nào, router sẽ gửi ở tốc độ T1. Điều này là nguyên nhân tiềm tàng gây nghẽn đầu ra, các hàng đợi cũng có thể tăng nhanh chóng bên trong mạng FrameRelay.

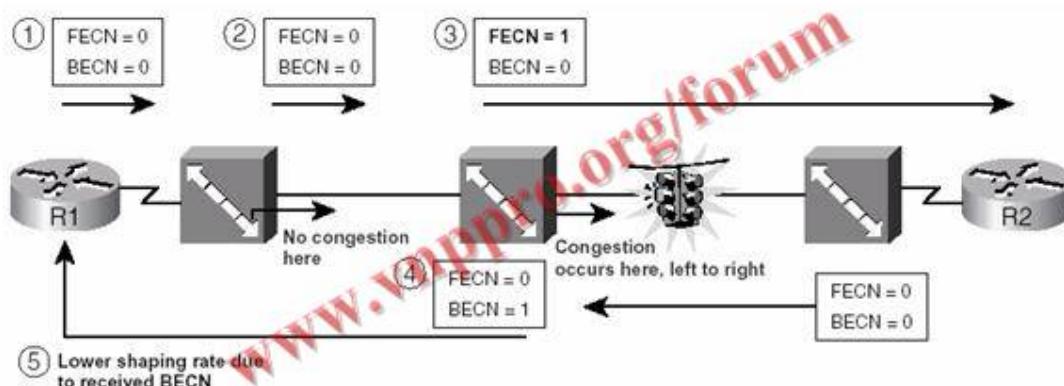
Do đó, FR cung cấp hai phương thức để phản ứng với vấn đề nghẽn.

Adaptive Shaping, FECN và BECN

Ở chương 16, “shaping và policing” đã mô tả khái niệm định hình lưu lượng

theo chế độ thích ứng, trong đó router sẽ thay đổi tốc độ định hình tùy thuộc vào mạng có nghẽn hay không. Để phản ứng với nghẽn xảy ra trong mạng FR, router phải nhận được vài dạng thông báo từ tổng đài FRSwitch rằng nghẽn đã xảy ra. Vì vậy phần header của FR sẽ bao gồm các bit *Forward Explicit Congestion Notification (FECN)* và bit *Backward Explicit Congestion Notification (BECN)* để báo hiệu nghẽn xảy ra trên một VC nào đó.

Để thực hiện việc này, khi một tổng đài FRSwitch nhận thấy có nghẽn gây ra bởi một VC, tổng đài sẽ gán bit FECN trong một frame của VC đó. Tổng đài cũng theo dõi các VC đang bị nghẽn sao cho nó có thể tìm ra frame kế tiếp đang được gửi trên VC đó nhưng đi theo chiều đối diện như trong bước 4 của hình. Tổng đài sau đó sẽ đánh dấu bit BECN trong frame đang truyền theo chiều ngược lại này. Router nhận được frame có bit BECN biết rằng một frame do router gửi ra đã chịu tình trạng nghẽn, vì vậy router có thể giảm tốc độ gửi dữ liệu của nó xuống. Hình dưới đây mô tả một ví dụ của tiến trình.



Bit FECN có thể được gán bởi tổng đài FR nhưng không thể được gán bởi bất kỳ router nào bởi vì router không cần truyền tín hiệu nghẽn. Ví dụ, nếu R1 nghĩ rằng nghẽn xảy ra từ trái sang phải, R1 có thể chỉ cần giảm tốc độ truyền xuống. Ở đầu kia của kết nối, R2 là đích đến của frame, vì vậy nó sẽ không bao giờ lưu ý về nghẽn xảy ra cho những frame đi từ trái sang phải. Vì vậy, chỉ có tổng đài cần phải thiết lập giá trị bit FECN.

BECN thì có thể được gán bởi tổng đài và bởi router. Hình trên mô tả một tổng đài gán giá trị BECN trên frame kế tiếp của người dùng. Nó cũng có thể gửi các frame kiểm tra Q.922. Động thái này giúp loại bỏ sự cần thiết phải chờ cho có lưu lượng của người dùng gửi trên VC và gán giá trị BECN trên frame đó. Cuối cùng, các router có thể được cấu hình để xem xét các frame có bit FECN, phản ứng lại bằng cách gửi ra các frame kiểm tra Q.922 trên VC đó với bit BECN được thiết lập. Đặc tính này, thỉnh thoảng còn được gọi là phản hồi FECN. Tính năng này được cấu hình bằng lệnh **shape fecn-adapt (CB Shaping)** hoặc lệnh **traffic-shape fecn-adapt (FRTS)**.

## Bit chỉ ra khả năng loại bỏ frame DE

Khi có nghẽn xảy ra, các hàng đợi trong tổng đài FRSwitch bắt đầu lấp đầy. Trong vài trường hợp, frame có thể bị loại bỏ ra khỏi hàng đợi. Tổng đài có thể (nhưng không yêu cầu) phải kiểm tra bit chỉ ra khả năng loại bỏ của frame Discard Eligibility (DE) khi frame cần phải bị loại bỏ. Tổng đài FR sẽ chủ động loại bỏ các frame có bit DE thay vì loại bỏ các frame không có bit DE.

Cả router và tổng đài FR có thể gán bit DE. Thông thường, một router sẽ ra quyết định về việc gán bit DE trong vài frame nào đó, bởi vì người quản trị có khả năng biết các lưu lượng nào là quan trọng hơn lưu lượng nào, thường là chiều inbound.

Đánh dấu các bit DE có thể được thực hiện thông qua cơ chế CB Marking, dùng lệnh set fr-de của MQC. Mặc dù router thường thực hiện việc đánh dấu bit DE, các tổng đài FR cũng có thể đánh dấu bit DE. Đối với tổng đài, động tác đánh dấu thường được thực hiện khi tổng đài không chê lưu lượng, nhưng thay vì loại bỏ các lưu lượng vượt quá giới hạn, tổng đài sẽ đánh dấu bit DE. Bằng cách này, các tổng đài bên dưới sẽ có khả năng loại bỏ các frame đã đánh dấu và gây ra nghẽn.

Bảng dưới đây tóm tắt các điểm mấu chốt về FECN, BECN và bit DE

Bit	Ý nghĩa	Được thiết lập bởi
FECN	Xảy ra nghẽn theo cùng chiều của frame	Tổng đài FRSwitch trong các frame người dùng
BECN	Xảy ra nghẽn theo chiều ngược với chiều của frame	Bởi tổng đài hay router trong các frame của người dùng hay trong các frame kiểm tra Q.922
DE	Frame này sẽ bị loại bỏ trước những frame khác	Router hay tổng đài trong các frame của người dùng

## Cấu hình Frame Relay

Phần này mô tả các cấu hình cơ bản và các lệnh hoạt động, cùng với các cơ chế nén tải trên FR và cơ chế chèn LFI trong FR.

### Cấu hình Frame Relay cơ bản

Hai chi tiết quan trọng nhất liên quan đến cấu hình Frame Relay là việc kết hợp các giá trị DLCI với các cổng hoặc subinterface và việc ánh xạ địa chỉ lớp 3 đến các giá trị này. Một điều thú vị là cả hai đặc điểm này có thể được cấu hình với cùng hai lệnh: **frame-relay map** và lệnh **frame-relay interface-dlci**.

Mặc dù một router có thể học các giá trị DLCI trên đường truyền FR thông qua các thông điệp LMI, các thông điệp này không có chức năng ngầm định rằng DLCI sẽ dùng cho cổng nào. Để cấu hình FR dùng các subinterface, các thông số DLCI phải được kết hợp với các subinterface. Bất kỳ DLCI nào được học với LMI mà không kết hợp với một cổng subinterface thì sẽ được giả sử là dùng cho cổng vật lý.

Một phương thức phổ biến hơn để thực hiện việc kết hợp này là dùng lệnh frame-relay interface-dlci trong dấu nhắc lệnh sub interface. Trên các subinterface dạng điểm-nối-điểm point-to-point, chỉ có một lệnh frame-relay interface dlci là được phép dùng, trong khi nếu cổng là dạng đa điểm multipoint, có thể nhiều lệnh được dùng.

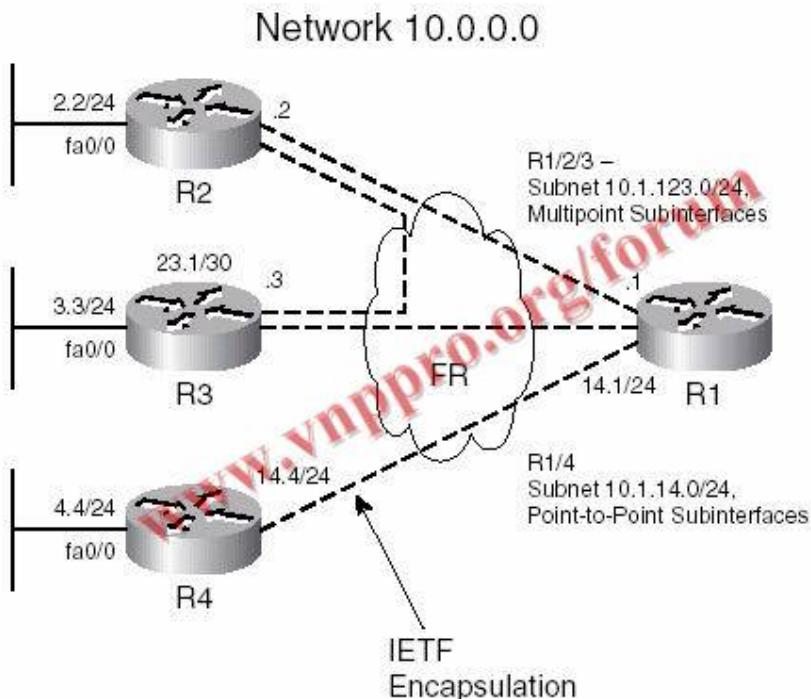
Một phương thức thay thế là dùng lệnh **frame-relay map**. Lệnh này vẫn ánh xạ địa chỉ lớp 3 sang giá trị DLCI nhưng cũng ngầm định chỉ ra rằng DLCI thuộc về cổng mà lệnh này được cấu hình. Trên các cổng subinterface dạng đa điểm, nhiều lệnh có thể được cho phép đối với từng giao thức lớp 3.

Ví dụ dưới đây mô tả các tùy chọn cấu hình của FR, dùng lệnh **frame-relay interface-dlci** và các lệnh show liên quan. Ví dụ này hiện thực các yêu cầu sau đây:

R1 dùng nhiều cổng dạng multipoint subinterface để kết nối R2 và R3.

R1 dùng các cổng subinterface dạng điểm-điểm để kết nối đến R4.

Mạch ảo VC giữa R1 và R4 dùng kiểu đóng gói IETF.



Bắt đầu bằng cấu hình của R1. Cổng subinterface s0/0.14 hiển thị tùy chọn IETF được dùng trên lệnh frame-relay interface-dlci. Cổng subinterface s0/0.123 có hai DLCI thuộc về nó, là VC kết nối đến R2 và R3.

Code:

```
interface Serial0/0/0
encapsulation frame-relay
!
interface Serial0/0.14 point-to-point
ip address 10.1.14.1 255.255.255.0
frame-relay interface-dlci 104 IETF
!
interface Serial0/0/0.123 multipoint
ip address 101.123.1 255.255.255.0
frame-relay interface-dlci 102
frame-relay interface-dlci 103
```

Tiếp theo là cấu hình R2. R2 gán giá trị DLCI cho VC từ R1 và R3 đến cổng subinterface .123. Chú ý rằng số của subinterface của router không cần phải đúng bằng giá trị DLCI.

Code:

```
interface Serial0/0/0
encapsulation frame-relay
!
interfacce Serial0/0/0.123 multipoint
ip address 101.123.2 255.255.255.0
frame-relay interface-dlci 101
frame-relay interface-dlci 103
```

Tiếp theo là cấu hình R4, trong đó đóng gói bằng lệnh frame-relay ietf. Lệnh này sẽ thiết lập kiểu đóng gói cho tất cả các VC trên cổng S0/0/0. Cũng lưu ý rằng tần suất gửi các thông điệp đã thay đổi từ giá trị mặc định (10) thành 8 thông qua lệnh keepalive 8.

Code:

```
interface Serial0/0/0
encapsulation frame-relay IETF
keepalive 8
!
interface Serial0/0/0.1 point-to-point
ip address 10.1.14.4 25.255.255.0
frame-relay interface-dlci 101
```

Lệnh show frame-relay pvc hiển thị các thông tin thống kê và trạng thái của từng VC. Lệnh kê tiếp trên R1 đã bỏ qua một số đoạn, chỉ để lại những dòng có trạng thái PVC.

Code:

```
R1# show frame-relay pvc| incl PVC STATUS
DLCI = 100, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE,
INTERFACE = Serial0/0/0
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0.123
DLCI = 103, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0.123
DLCI = 104, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0.14
DLCI = 105, DLCI USAGE = UNUSED, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0
DLCI = 106, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE,
INTERFACE = Serial0/0/0
DLCI = 107, DLCI USAGE = UNUSED, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0
DLCI = 108, DLCI USAGE = UNUSED, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0
DLCI = 109, DLCI USAGE = UNUSED, PVC STATUS = INACTIVE,
INTERFACE = Serial0/0/0
```

Code:

```
R1# show frame-relay pvc 102
PVC Statistics for interface Serial0/0/0 (Frame Relay DTE)
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0/0.123
input pkts 41 output pkts 54 in bytes 4615
out bytes 5491 dropped pkts 0 in pkts dropped 0
out pkts dropped 0 out bytes dropped 0
in FECN pkts 0 in BECN pkts 0 out FECN pkts 0
out BECN pkts 0 in DE pkts 0 out DE pkts 0
out bcast pkts 27 out bcast bytes 1587
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:29:37, last time pvc status changed 00:13:47
```

Kết quả lệnh dưới đây xác nhận rằng đường truyền của R1 đang dùng Cisco LMI. Các thông điệp trạng thái LMI sẽ xuất hiện mỗi phút trong đó thông điệp Full Status message được liệt kê sau cùng. Chú ý rằng router gửi các thông điệp truy vấn trạng thái đến tổng đài. Khi tổng đài gửi các thông điệp trạng thái, các bộ đếm này sẽ cùng tăng.

Code:

```
R1# show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE =
CISCO
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 183 Num Status msgs Rcvd 183
Num Update Status Rcvd 0 Num Status Timeouts 0
Last Full Status Req 00:00:35 Last Full Status Rcvd 00:00:35
```

Lệnh show interface liệt kê vài chi tiết, bao gồm các khoảng thời gian để gửi các thông điệp LMI, LMI stats, LMI DLCI và các trạng thái trong hàng đợi FR. Hàng đợi broadcast giữ các broadcast FR mà những broadcast này sẽ được nhận bản và gửi trên VC. Ví dụ như các OSPF LSAs.

Code:

```
R1# show int s 0/0/0
Serial0/0/0 is up, line protocol is up
! lines omitted for brevity
Encapsulation FRAME-RELAY, loopback not set
Keepalive set (10 sec)
LMI enq sent 185, LMI stat recv 185, LMI upd recv 0, DTE LMI up
LMI enq recv 0, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
FR SVC disabled, LAPF state down
Broadcast queue 0/64, broadcasts sent/dropped 274/0, interface broadcasts 228
! Lines omitted for brevity
```

Code:

```
R3# sh frame lmi |include LMITYPE
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI TYPE =
ANSI
R3# sh int s 0/0/0 | include LMI DLCI
LMI DLCI 0 LMI type is ANSI Annex D frame relay DTE
```

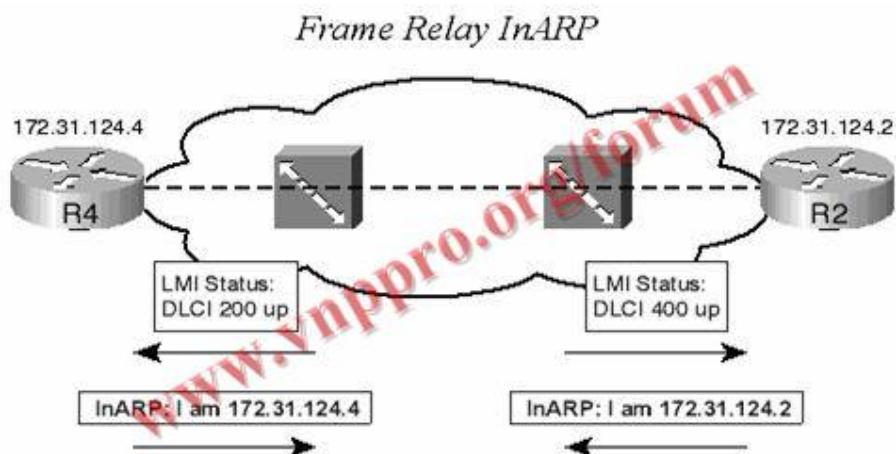
Chú ý là R3 đang dùng kiểu ANSI LMI. R3 có thể cấu hình LMI tĩnh bằng câu lệnh **frame-relay lmi-type {ansi | cisco | q933a}** trong công vật lý. Tuy nhiên R3 đã bỏ qua lệnh này, làm cho R3 có hành động mặc định là tự động tìm ra loại LMI.

## Frame Relay Inverse ARP:

IP ARP được biết đến như một giao thức phổ thông và tương đối đơn giản. Đối với kỳ thi CCIE cũng vậy. Đa số các câu hỏi trong phần IP ARP là những câu hỏi đơn giản. Do đó, những câu hỏi khó về chủ đề xây dựng CEF adjacency table sẽ tập trung vào Frame Relay Inverse ARP, cũng chính vì vậy mà phương thức Frame Relay Inverse ARP sẽ được trình bày cụ thể và chi tiết hơn.

Tương tự như IP ARP, nhiệm vụ của InARP là phân giải giữa địa chỉ L3 và địa chỉ L2. Địa chỉ L3 chính là địa chỉ IP, còn địa chỉ L2 ở đây chính là số DLCI (tương tự như địa chỉ MAC trong IP ARP). Tuy nhiên, trong phương thức InARP, router đã biết được địa chỉ L2 (DLCI), và cần phân giải ra địa chỉ L3 (IP) tương ứng.

Hình sau là một ví dụ về chức năng của InARP.



Hình 1.2

Trong môi trường LAN, đòi hỏi phải có một gói tin (ARP request) đến host và kích hoạt giao thức IP ARP trên host (trả về ARP reply). Tuy nhiên, trong môi trường WAN, không cần một gói tin nào đến router để kích hoạt InARP trên router này, thay vào đó là một thông điệp về tình trạng LMI (Local Management Interface) sẽ được dùng.

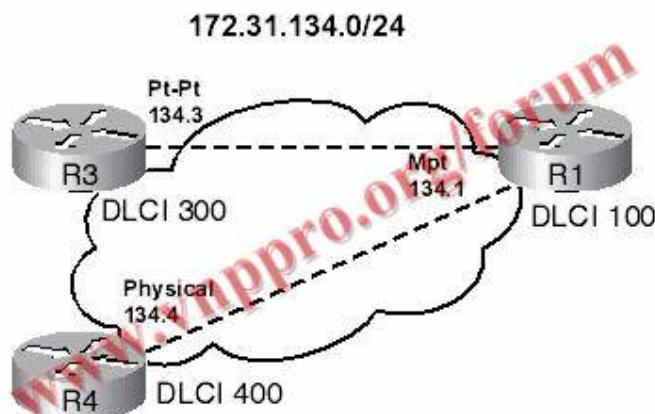
Sau khi nhận được thông điệp trạng thái LMI là LMI PVC Up, router sẽ loan báo địa chỉ IP của nó ra mạch liên kết ảo (VC - Virtual Circuit) tương ứng thông qua thông điệp InARP (định nghĩa trong RFC1293). Như vậy, một khi LMI không được thực thi thì InARP cũng không hoạt động bởi vì không có thông điệp nào nói cho router biết để gửi thông điệp InARP.

Trong mạng Frame Relay, những cấu hình chi tiết được chọn lựa với mục đích tránh một số tình trạng không mong muốn, những tình trạng này sẽ được mô tả chi tiết trong những trang kế tiếp của chương này. Ví dụ khi sử dụng point-to-point subinterface, với mỗi VC thuộc một subnet riêng, tất cả những vấn đề gấp phai trong cấu hình này sẽ được mô tả rõ ràng để có thể phòng tránh.

Bản thân giao thức InARP tương đối đơn giản. Tuy nhiên, khi triển khai InARP trên những mô hình mạng khác nhau, dựa trên những kiểu cổng khác nhau (cổng vật lý, cổng point-to-point subinterface và multipoint subinterface) thì cách thức hoạt động của InARP sẽ trở nên phức tạp hơn rất nhiều.

Sau đây là một ví dụ về hệ thống mạng Frame Relay được thiết kế theo mô hình mạng lưới không đầy đủ (partial mesh) trên cùng một subnet trong khi mỗi router sử dụng một kiểu cổng khác nhau.

### *Frame Relay Topology for Frame Relay InARP Examples*



Hình 1.3

Sơ đồ mạng trên chỉ mang tính chất là một ví dụ, nó chỉ sử dụng trong môi trường học tập để hiểu chi tiết hơn về cách thức hoạt động của InARP. Sơ đồ này không nên được áp dụng trong môi trường mạng thực tế bởi thiết kế yếu kém với nhiều hạn chế khi triển khai giao thức định tuyến bên trên.

Thông tin của một số lệnh show và debug liên quan đến Frame Relay InARP và một trong số những điều kỳ quặc về InARP liên quan đến point-to-point subinterface được mô tả trong *ví dụ 1.1*.

Đầu tiên cấu hình frame relay trên cổng multipoint của R1.

Code:

```
Router1# sh run
! Lines omitted for brevity
interface Serial0/0
encapsulation frame-relay
interface Serial0/0.11 multipoint
ip address 172.31.134.1 255.255.255.0
frame-relay interface-dlci 300
frame-relay interface-dlci 400
! Lines omitted for brevity
```

Kế tiếp, cổng serial được tắt và bật và các hàng trong InARP trước đó bị xóa vì vậy ta có thể quan sát tiến trình InARP.

Code:

```
Router1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)# int s 0/0
Router1(config-if)# do clear frame-relay inarp
Router1(config-if)# shut
Router1(config-if)# no shut
Router1(config-if)# ^Z
```

Các thông điệp từ lệnh debug frame-relay event hiển thị các thông điệp nhận được InARP trên R1. Chú ý các giá trị hex 0xAC1F8603 và 0xAC1F8604, với các giá trị thập phân tương ứng là 172.31.134.3 and 172.31.134.4 (tương ứng với Router3 và Router4).

Code:

```
Router1# debug frame-relay events
*Mar 1 00:09:45.334: Serial0/0.11: FR ARP input
*Mar 1 00:09:45.334: datagramstart = 0x392BA0E, datagramsize = 34
*Mar 1 00:09:45.334: FR encap = 0x48C10300
*Mar 1 00:09:45.334: 80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00
*Mar 1 00:09:45.334: AC 1F 86 03 48 C1 AC 1F 86 01 01 02 00 00
*Mar 1 00:09:45.334:
*Mar 1 00:09:45.334: Serial0/0.11: FR ARP input
*Mar 1 00:09:45.334: datagramstart = 0x392B8CE, datagramsize = 34
*Mar 1 00:09:45.338: FR encap = 0x64010300
*Mar 1 00:09:45.338: 80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00
*Mar 1 00:09:45.338: AC 1F 86 04 64 01 AC 1F 86 01 01 02 00 00
```

Kế tiếp, chú ý lệnh show frame-relay map có bao gồm từ khóa dynamic, nghĩa là các hàng được học thông qua InARP.

Code:

```
Router1# show frame-relay map
```

```
Serial0/0.11 (up): ip 172.31.134.3 dlc 300(0x12C,0x48C0), dynamic,  
broadcast, status defined, active  
Serial0/0.11 (up): ip 172.31.134.4 dlc 400(0x190,0x6400), dynamic,  
broadcast, status defined, active
```

Trên R3, lệnh show frame-relay map chỉ liệt kê một hàng duy nhất nhưng định dạng thì khác. Bởi vì R3 dùng point-to-point subinterface, hàng này không được học thông qua InARP và kết quả lệnh không bao gồm từ khóa Dynamic. Cũng chú ý là kết quả không cho thấy địa chỉ Layer 3 nào.

Code:

```
Router3# show frame-relay map  
Serial0/0.3333 (up): point-to-point dlc, dlc 100(0x64,0x1840), broadcast  
status defined, active
```

Chú ý: Trong ví dụ trên ta thấy xuất hiện lệnh “do” trong chế độ cấu hình. Lệnh do cho phép cấu hình trong configuration mode nhưng để thực hiện chức năng ở exec mode mà không phải thoát khỏi mode configuration. Ví dụ lệnh do clear frame-relay inarp thực hiện ở configuration mode tương đương với việc ta thực hiện lệnh clear frame-relay inarp ở chế độ toàn cục.

Trong ví dụ trên, lệnh show cho thấy Router R1 đã nhận và sử dụng thông tin InARP; tuy nhiên Router R3 thì không sử dụng thông tin InARP đã nhận vào. Hệ điều hành Cisco IOS hiểu rằng chỉ một VC được thiết lập với một subinterface point-to-point; mỗi một địa chỉ IP đầu cuối khác trên cùng một subnet chỉ có thể tham chiếu đến duy nhất một số DLCI. Vì vậy, mỗi thông tin InARP nhận được liên kết đến số DLCI đó là không cần thiết.

Lấy ví dụ, khi nào Router R3 cần gửi một gói tin đến Router R1(172.31.134.1), hay đến mỗi đầu cuối khác trong subnet 172.31.134.0/24. Từ chính cấu hình của mình, Router R3 biết rằng phải gửi qua số DLCI trên point-to-point subinterface đó, nghĩa là qua DLCI 100. Vì vậy, mặc dù cả ba kiểu cổng được dùng cho cấu hình Frame Relay hỗ trợ InARP một cách mặc định, point-to-point subinterface sẽ bỏ qua thông tin InARP nhận được.

### Cấu hình ánh xạ địa chỉ tĩnh trong Frame Relay

Trong *hình 1.3*, R3 đã biết cách đẩy gói tin đến R4, nhưng ngược lại R4 chưa biết cách để đẩy gói tin ngược trở lại Router3. Theo ý nghĩa logic R3 sẽ hiểu như sau “Để những gói tin đến được next-hop router trên subnet 172.31.124.0/24, R3 sẽ gửi chúng ra theo một số DLCI trên point-to-point subinterface, ở đây chính là DLCI 100”. Những gói tin này sẽ được chuyển đến R1 và nhờ R1 chuyển đến R4.

Trong cách thiết kế yếu kém trong *hình 1.3*, mặc dù R4 và R3 sử dụng hai kiểu cổng khác nhau, R3 sử dụng point-to-point subinterface trong khi R4 sử dụng cổng vật lý. Để đến được R3, R4 cần gửi frame qua DLCI 100 đến R1 và nhờ

R1 chuyển tiếp đến R3. Trong trường hợp này InARP sẽ không giúp được gì, bởi vì thông điệp InARP chỉ cho phép qua một VC, mà không cho phép chuyển tiếp; một chú thích rằng không có VC nào tồn tại giữa R4 và R3.

Để giải quyết vấn đề này, trong cấu hình của R4 được thêm vào câu lệnh frame-relay map. *Ví dụ 1.2* mô tả chi tiết thông tin trước và sau khi sử dụng lệnh frame-relay map.

Router 4 chỉ liệt kê một hàng trong lệnh show frame-relay map bởi vì Router4 chỉ có một VC duy nhất kết nối về Router1. Chỉ với một VC, Router 4 có thể học về một router khác thông qua InARP.

Code:

```
Router4# sh run
! lines omitted for brevity
interface Serial0/0
ip address 172.31.134.4 255.255.255.0
encapsulation frame-relay

Router4# show frame-relay map
Serial0/0 (up): ip 172.31.134.1 dlci 100(0x64,0x1840), dynamic,
broadcast,, status defined, active
! Next, proof that Router4 cannot send packets to Router3's Frame Relay IP
address.

Router4# ping 172.31.134.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.134.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Kết tiếp, các thông tin ánh xạ tĩnh được thêm vào trên Router4 dùng lệnh frame-relay map trong sub-interface. Cũng chú ý rằng lệnh này dùng DLCI 100, vì vậy bất cứ gói tin nào được gửi bởi R4 về 172.31.134.3 (Router3) sẽ đi qua VC về router 1, sau đó lại cần định tuyến gói tin ngược về Router3. Từ khóa broadcast báo cho Router4 gửi các bản copy trên VC này.

Code:

```
Router4# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router4(config)# int s0/0
Router4(config-if)# frame-relay map ip 172.31.134.3 100 broadcast
Router4(config-if)# ^Z
Router4# ping 172.31.134.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.134.3, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms

### Ví dụ 1.2

Chú ý: Router R3 không cần phải sử dụng câu lệnh frame-relay map, bởi vì trong cấu hình của R3 đã sử dụng point-to-point subinterface. Phải nhớ kỹ rằng bạn đừng nên sử dụng nhiều kiểu cổng khác nhau như *hình 1.3*, cũng không nên triển khai mô hình dạng lưới không đầy đủ (non-full-mesh) với cùng một subnet, trừ khi bạn buộc phải thực hiện trên đúng không gian địa chỉ IP hạn chế của mình.

Trong trường hợp khi bạn sử dụng mô hình như *hình 1.3*, bạn có thể sử dụng cấu hình ở trên. Một sự lựa chọn khác là nếu bạn sử dụng multipoint subinterface trên cả R3 và R4, cả hai router đều phải sử dụng câu lệnh frame-relay map, bởi vì cả hai router đều không thể nghe được thông điệp InARP từ router khác. Tuy nhiên, nếu cả hai router R3 và R4 đều sử dụng point-to-point subinterface, không router nào đòi hỏi phải có câu lệnh frame-relay map, bởi vì theo nghĩa logic cả hai router đều hiểu là: “dùng một VC của nó để đến tất cả các địa chỉ trong subnet”.

### Tắt InARP

Trong hầu hết những mô hình mạng được đưa ra, việc sử dụng InARP là hợp lý. Tuy nhiên, ta có thể tắt InARP trên interface vật lý hay multipoint interface bằng cách sử dụng lệnh no frame-relay inverse-arp trên interface subcommand. Có thể ngừng hoạt động InARP trên tất cả các VC của interface/subinterface, tất cả các VC của interface/subinterface ứng với một giao thức L3 riêng biệt, hay đơn thuần là trên mỗi DLCI cụ thể.

Câu lệnh no frame-relay inverse-arp không chỉ làm cho router ngừng việc gửi thông điệp InARP ra ngoài, mà còn làm cho router không nhận thông điệp InARP. Lấy ví dụ, câu lệnh no frame-relay inverse-arp ip 400 ở mode subinterface trên Router R1 trong *ví dụ 1.2* không chỉ ngăn R1 ngừng gửi thông điệp InARP ra DLCI400 tới R4 mà còn làm cho R1 bỏ đi thông điệp InARP đã nhận trên DLCI400.

*Bảng 1.2 : Tổng hợp một số đặc tính chi tiết về Frame Relay Inverse ARP trên IOS*

Cách cài xử trên mỗi kiểu interface riêng biệt	Interface Point-to-point	Interface multipoint hoặc interface vật lý
InARP có đòi hỏi LMI không ?	Luôn luôn	Luôn luôn
InARP được kích hoạt một cách mặc định ?	Đúng	Đúng
Có thể tắt hoạt động của InARP không ?	Không	Có
Có thể bỏ qua thông điệp InARP đã nhận hay không	Luôn luôn (*)	Khi InARP bị tắt đi

(\*) Interface point-to-point luôn luôn bỏ qua thông điệp InARP, bởi vì đối với point-to-point interface, chỉ dùng một số DLCI để gửi đến tất cả địa chỉ trong cùng một subnet

### Bài 3: SPANNING TREE PROTOCOL - STP

#### 1. Tổng quan về IEEE 802.1D:

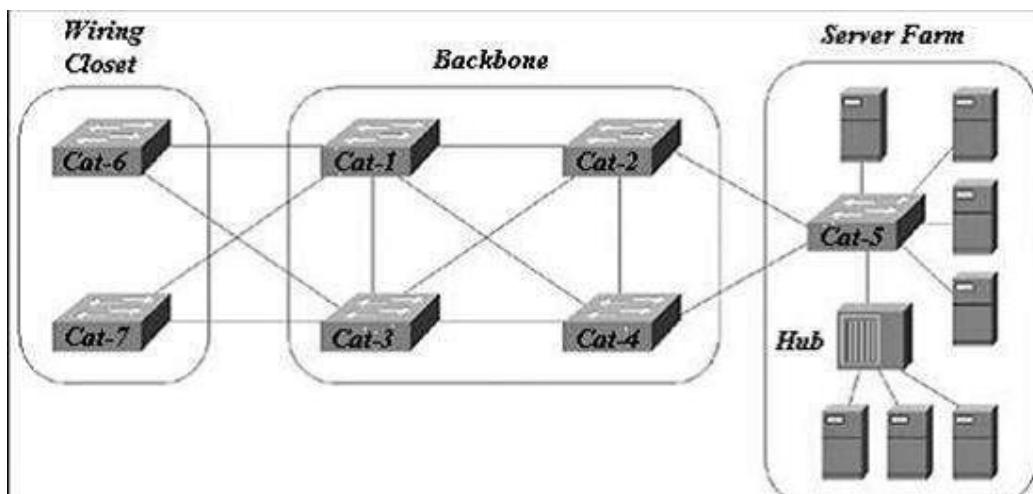
Một mạng mạnh mẽ được thiết kế không chỉ đem lại tính hiệu quả cho việc truyền các gói hoặc frame, mà còn phải xem xét làm thế nào để khôi phục hoạt động của mạng một cách nhanh chóng khi mạng xảy ra lỗi. Trong môi trường lớp 3, các giao thức định tuyến sử dụng con đường dự phòng đến mạng đích để khi con đường chính bị lỗi thì sẽ nhanh chóng tận dụng con đường thứ 2. Định tuyến lớp 3 cho phép nhiều con đường đến đích để giữ nguyên tình trạng hoạt động của mạng và cũng cho phép cân bằng tải qua nhiều con đường.

Trong môi trường lớp 2 (switching hoặc bridging), không sử dụng giao thức định tuyến và cũng không cho phép các con đường dự phòng, thay vì bridge cung cấp việc truyền dữ liệu giữa các mạng hoặc các port của switch. Giao thức Spanning Tree cung cấp liên kết dự phòng để mạng chuyển mạch lớp 2 có thể khôi phục từ lỗi mà không cần có sự can thiệp kịp thời. STP được định nghĩa trong chuẩn IEEE 802.1D.

## 1.1. Spanning Tree là gì và tại sao phải sử dụng nó?

Spanning Tree Protocol (STP) là một giao thức ngăn chặn sự lặp vòng, cho phép các bridge truyền thông với nhau để phát hiện vòng lặp vật lý trong mạng. Sau đó giao thức này sẽ định rõ một thuật toán mà bridge có thể tạo ra một topology luân lý chứa loop-free. Nói cách khác STP sẽ tạo một cấu trúc cây của free-loop gồm các lá và các nhánh nối toàn bộ mạng lớp 2.

Vòng lặp xảy ra trong mạng với nhiều nguyên nhân. Hầu hết các nguyên nhân thông thường là kết quả của việc cố gắng tính toán để cung cấp khả năng dự phòng, trong trường hợp này, một link hoặc switch bị hỏng, các link hoặc switch khác vẫn tiếp tục hoạt động, tuy nhiên các vòng lặp cũng có thể xảy ra do lỗi. Hình 3.1 biểu diễn một mạng switch điển hình và các vòng lặp có ý được dùng để cung cấp khả năng dự phòng như thế nào.

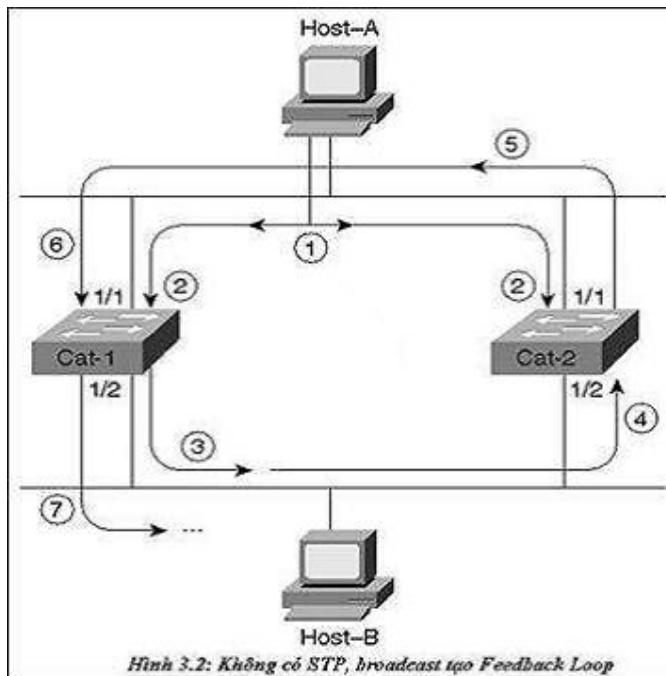


Hình 3.1: Bridging Loop trong mạng

**Hai nguyên nhân chính gây ra sự lặp vòng tai hại trong mạng chuyển mạch là do broadcast và sự sai lệch của bảng bridge.**

### Broadcast Loop

Broadcast Loop và vòng lặp lớp 2 là một sự kết hợp nguy hiểm. Hình 3.2 biểu diễn broadcast tạo ra vòng lặp phản hồi (feedback loop).



Hình 3.2: Không có STP, broadcast tạo Feedback Loop

Giả sử rằng, không có switch nào chạy STP:

- **Bước 1:** host A gửi một frame bằng địa chỉ broadcast MAC (FF-FF-FF-FF-FF-FF).
- **Bước 2:** frame đến cả hai Cat-1 và Cat-2 qua port 1/1
- **Bước 3:** Cat-1 sẽ đưa frame qua port 1/2.
- **Bước 4:** frame được truyền đến tất cả các node trên đoạn mạng Ethernet kể cả port 1/2 của Cat-2.
- **Bước 5:** Cat-2 đưa frame này đến port 1/1 của nó.
- **Bước 6:** một lần nữa, frame xuất hiện port 1/1 của Cat-1.
- **Bước 7:** Cat-1 sẽ gửi frame này đến port 1/2 lần hai. Như vậy tạo thành một vòng lặp ở đây.

**Chú ý:** frame này cũng tràn qua đoạn mạng Ethernet và tạo thành một vòng lặp theo hướng ngược lại, feedback loop xảy ra trong cả hai hướng. Một kết luận quan trọng nữa trong hình 3.2 là bridging loop nguy hiểm hơn nhiều so với routing loop. Hình 3.3 mô tả format của một DIXv2 Ethernet frame.



Hình 3.3: Format của một DIXv2 Ethernet frame

DIXv2 Ethernet Frame chỉ chứa 2 địa chỉ MAC, một trường Type và một CRC. Trong IP header chứa trường time-to-live (TTL) được thiết lập tại host gốc và nó sẽ được giảm bớt mỗi khi qua một router. Gói sẽ bị loại bỏ nếu TTL = 0, điều này cho phép các router ngăn chặn các datagram bị “run-away”. Không giống như IP, Ethernet không có trường TTL, vì vậy sau khi một frame bắt đầu

bị loop trong mạng thì nó vẫn tiếp tục cho đến khi ai đó ngắt một trong các bridge hoặc ngắt một kiêm kết.

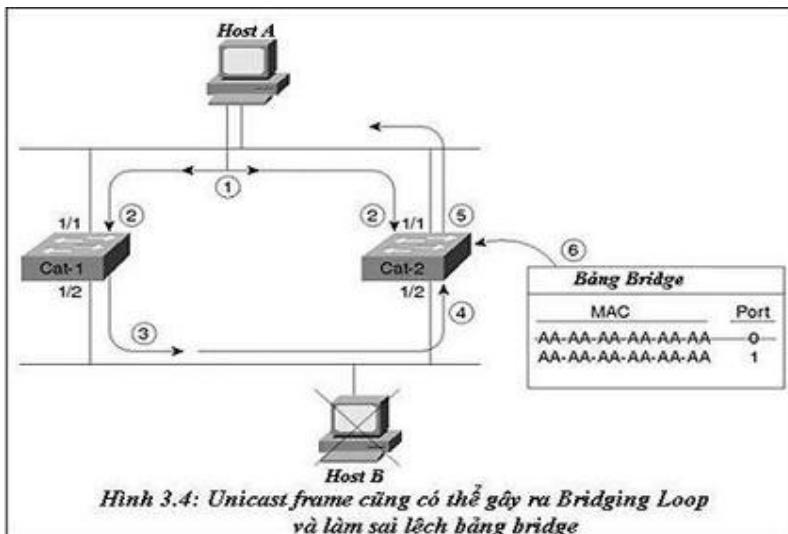
Trong một mạng phức tạp hơn mạng được mô tả trong hình 3.1, 3.2 thì có thể gây ra feedback loop rất nhanh theo tỉ lệ số mũ. Vì cứ mỗi frame tràn qua nhiều port của switch, thì tổng số frame tăng nhanh rất nhiều.

Ngoài ra cần phải chú ý đến broadcast storm trên các user của host A và B trong hình 3.2. Broadcast được xử lý bởi CPU trong tất cả các thiết bị trên mạng. Trong trường hợp này, các PC đều cố xử lý broadcast storm. Nếu ta ngắt kết nối một trong số các host từ LAN, thi nó hoạt động trở lại bình thường. Tuy nhiên, ngay khi ta kết nối nó trở lại LAN thì broadcast sẽ sử dụng 100% CPU. Nếu ta không xử lý điều này mà vẫn tiếp tục sử dụng mạng, thì sẽ tạo ra vòng lặp vật lý trong VLAN.

#### **Việc sai lệch bảng bridge:**

Nhiều nhà quản trị switch/bridge đã nhận thức vấn đề cơ bản của broadcast storm, tuy nhiên ta phải biết rằng thậm chí các unicast frame cũng có thể truyền mãi trong mạng mà chưa vòng lặp. Hình 3.4 mô tả điều này.

- **Bước 1:** host A muốn gửi gói unicast đến host B, tuy nhiên host B đã rời khỏi mạng, và đúng với bảng bridge của switch không có địa chỉ của host B.
- **Bước 2:** giả sử rằng cả hai switch đều không chạy STP, thì frame đến port 1/1 trên cả hai switch.
- **Bước 3:** vì host B bị down, nên Cat-1 không có địa chỉ MAC BB-BB-BB-BB-BB-BB trong bảng bridge, và nó tràn frame qua các port.
- **Bước 4:** Cat-2 nhận được frame trên port 1/2 . Có 2 vấn đề xảy ra.
  - **Bước 5:** Cat-2 tràn frame vì nó không học địa chỉ MAC BB-BB-BB-BB-BB-BB, điều này tạo ra feedback loop và làm down mạng.
  - Cat-2 chú ý rằng, nó chỉ nhận một frame trên port 1/2 với địa chỉ MAC là AA-AA-AA-AA-AA-AA. Nó thay đổi địa chỉ MAC của host A trong bảng bridge dẫn đến sai port.



Vì frame bị lặp theo hướng ngược lại, nên ta thấy địa chỉ MAC của host A bị lẫn giữa port 1/1 và 1/2. Điều này không chỉ làm mạng bị tràn với các gói unicast mà còn sửa sai bảng bridge. Như vậy không chỉ có broadcast mới làm hư hại mạng.

#### Bài 4:

### Spanning Tree.

Một hệ thống mạng hiện thực STP kém có thể dẫn đến rất nhiều công việc cấu hình, khôi phục lỗi trên mạng campus. Bài viết này giải thích cơ chế hoạt động của spanning-tree, chức năng ngăn ngừa loop trong mạng switch.

STP là một trong những chủ đề đậm tính kỹ thuật trong công nghệ LAN switching. Để hiểu về STP thì cũng khó khăn như là hiểu về các cơ chế hoạt động bên dưới của OSPF hay EIGRP (timers, kiểu gói tin, các giải thuật). STP đóng vai trò nền tảng trong hoạt động của mọi hệ thống mạng campus. Nó đóng vai trò then chốt trong thiết kế và triển khai mạng campus.

Spanning-tree là một giao thức lớp 2 sử dụng một giải thuật đặc biệt để tìm ra các vòng lặp trong mạng và tác động của một mạng không bị loop. STP sẽ tạo ra một cấu trúc cây bao gồm các lá và các nhánh trải rộng trên toàn bộ mạng L2. Trong phần này, thuật ngữ switch và bridge được dùng thay thế lẫn nhau. Ngoài ra, nếu không đề cập đến, kết nối giữa các switch sẽ được giả sử là kết nối trunk.

Các vòng lặp loop có thể diễn ra trong một hệ thống mạng vì nhiều lý do. Thông thường, loop là kết quả của những cố gắng xây dựng các kết nối dự phòng. Tuy nhiên, loop cũng có thể dẫn đến từ những lỗi do cấu hình.

Các kết nối vật lý theo kiểu vòng lặp mà không dùng STP có thể gây nhiều vấn đề. Có hai vấn đề cò thể dẫn đến là broadcast loop và hỏng bảng mac-address.

Một frame Ethernet chỉ chứa hai địa chỉ MAC, vùng typefield, một vùng CRC và các thông tin lớp network. Trong khi đó, header của IP có chứa vùng time-to-live (TTL) được gán bởi router nguồn và bị trừ dần mỗi khi qua một router. Bằng cách loại bỏ những gói tin có TTL=0, router sẽ ngăn ngừa các gói tin đã tồn tại quá lâu trong hệ thống mạng. Không giống như IP, Ethernet không có vùng TTL. Vì vậy, sau khi một frame bắt đầu bị lặp, frame sẽ được chuyển bất tận cho đến khi nào một switch bị tắt đi hoặc một kết nối là bị ngắt.

## **Bridge-ID**

Giải thuật spanning-tree được định nghĩa trong IEEE 802.1D. Các thông số được dùng bởi giải thuật bao gồm Bridge-ID sẽ được khảo sát trong phần này.

Giải thuật spanning-tree dựa trên một số thông số để ra quyết định. Thông số bridge-ID là thông số đầu tiên được dùng bởi STP để tìm ra trung tâm của mạng, còn gọi là root-bridge. Thông số bridge-UD là một giá trị 8-bytes bao gồm hai vùng giá trị. Giá trị đầu tiên là giá trị thập phân có độ dài 2-bytes gọi là Bridge-Priority và giá trị tiếp theo là địa chỉ MAC 6 bytes. Bridge Priority được dùng để chỉ ra độ ưu tiên của một bridge trong giải thuật spanning-tree. Các giá trị có thể là từ 0 cho đến 65535. Giá trị mặc định là 32,768.

Giá trị MAC trong BID là một trong những MAC-address của switch. Hai thông số BID không thể nào bằng nhau, bởi vì Catalyst switch được gán những giá trị MAC address khác nhau. Trong các giải thuật của spanning-tree, khi so sánh hai giá trị của switch, giá trị thấp hơn luôn được dùng.

## **Path cost**

Path cost là thông số thứ hai được dùng bởi giải thuật của spanning-tree để xác định đường đi về root. Đặc tả IEEE 802.1D ban đầu định nghĩa cost có giá trị bằng 10 lũy thừa 9 chia cho băng thông của kết nối tính theo Mbps. Ví dụ đường 10M sẽ có cost là 100 ( $1000/10$ ) và đường 100Mbps sẽ có cost là 10. Tuy nhiên, do công nghệ phát triển, có các công nghệ mới có tốc độ cao hơn cả 1Gbps nên cần định nghĩa lại công thức tính cost.

Cost được lưu như một giá trị số nguyên.

Thông số path cost sẽ đo lường các bridge sẽ gần nhau như thế nào. Path cost là tổng của các chi phí trên đường link giữa hai bridge. Đại lượng này không đo bằng hop count. Hop count cho đường đi A có thể lớn hơn hop-count cho đường đi B, trong khi đó, nếu xét theo cost, đường đi qua path A sẽ nhỏ hơn đường đi qua path B. Thông số path cost được dùng bởi các switch để xác định đường đi tốt nhất về RootBridge. Giá trị thấp nhất của đường đi sẽ là đường đi tốt nhất về root-bridge.

## **Port-ID**

Thông số PortID là thông số thứ ba được dùng bởi spanning-tree để xác định đường đi về root-bridge. Giá trị port-ID là giá trị 2-bytes bao gồm một hai chỉ số. Chỉ số đầu tiên gọi là port Priority, giá trị thứ hai được gọi là port-number. Trên một CatOS, giá trị đầu tiên là 6bits và giá trị thứ hai là 10 bits. Trên IOS-based switch, cả hai giá trị là 8 bits.

Ta không nên nhầm lẫn giữa PortID với giá trị Port Number. Giá trị port number chỉ là một phần của PortID. Giá trị PortID càng thấp thì được ưu tiên hơn giá trị portID cao trong các quyết định của STP. Hai giá trị PortID không thể nào bằng nhau, bởi vì PortNumber sẽ chỉ ra switchport trên Catalyst switch. Giá trị port priority là một thông số STP có thể thay đổi được. Tầm giá trị của nó là từ 0 cho đến 255 trên IOS-based switch, giá trị mặc định là 128.

---

Bài 5:

## **Route redistribution**

### **Redistribution**

#### *1. Định nghĩa*

Trường hợp nếu một mạng của công ty chạy nhiều giao thức định tuyến thì cần phải có một phương thức để chia sẻ thông tin định tuyến giữa các giao thức khác nhau đó. Quá trình đó gọi là redistribution.

Chú ý là trong trường hợp tồn tại nhiều giao thức định tuyến trên cùng một router không có nghĩa là redistribution tự xảy ra. Mà để quá trình redistribution này xảy ra thì ta phải cấu hình chúng.

Trường hợp có nhiều giao thức định tuyến tồn tại trên cùng một router mà không được cấu hình redistribution được gọi là ships in the night (SIN) routing. Có nghĩa là router chỉ trao đổi thông tin định tuyến với neighbor của nó trong cùng process domain. Mặc dù SIN routing thường được đề cập tới trường hợp nhiều giao thức định tuyến trên cùng một router (như là OSPF của giao thức IP và NLSP của giao thức IPX).

Một chú ý nữa là redistribution chỉ có thể xảy ra giữa các giao thức định tuyến tương ứng với cùng một giao thức lớp 3 (IP, IPX hay Apple Talk). Một vài giao thức định tuyến thì tự động redistribution mà không cần phải cấu hình, tuy nhiên thường là ta phải cấu hình thì quá trình redistribution mới diễn ra.

Hình 3.1 dưới đây sẽ miêu tả chính sách redistribution của từng giao thức định tuyến.

## Routing Protocol & Chính sách redistribution (Redistribution Policy)

Static: Phải cấu hình bằng tay vào các giao thức định tuyến khác.

Connected: Trừ phi có câu lệnh Network cho quá trình định tuyến, phải yêu cầu cấu hình redistribution bằng tay vào các giao thức định tuyến khác.

RIP: Yêu cầu cấu hình redistribution bằng tay.

IGRP: Nó sẽ tự động diễn ra giữa IGRP và EIGRP nếu giá trị AS autonomous system của chúng giống nhau. Trường hợp còn lại yêu cầu phải cấu hình bằng tay.

EIGRP: Nó sẽ tự động diễn ra giữa IGRP và EIGRP nếu giá trị autonomous system của chúng giống nhau. EIGRP cho giao thức Apple Talk sẽ tự động redistribution giữa EIGRP và RTMP. EIGRP cho IPX sẽ tự động redistribution giữa EIGRP và IPX RIP/SAP. Trường hợp còn lại yêu cầu phi cấu hình bằng tay. Trong các phiên bản sau, NLSP có thể redistribution bằng tay.

OSPF: Yêu cầu phải cấu hình redistribution giữa các OSPF process khác nhau và với giao thức định tuyến khác.

IS-IS: Yêu cầu phải cấu hình bằng tay giữa các giao thức định tuyến khác nhau.

BGP: Yêu cầu phải cấu hình bằng tay giữa các giao thức định tuyến khác nhau.

Các trường hợp dẫn tới tồn tại nhiều giao thức định tuyến trong cùng một tổ chức:

- Tổ chức chuyển từ một giao thức này sang một giao thức khác bởi vì họ cần một giao thức định tuyến phức tạp hơn. Ví dụ chuyển từ RIP sang OSPF.
- Do yêu tố lịch sử, tổ chức có rất nhiều mạng con. Công ty cần được thiết kế để chuyển sang một giao thức duy nhất trong tương lai. Ví dụ hiện tại vừa chạy RIP, IGRP. Mong muốn chuyển sang EIGRP.
- Một vài doanh nghiệp sử dụng giải pháp host-based yêu cầu nhiều giao thức định tuyến. Ví dụ, ví dụ một UNIX host sử dụng RIP để khám phá gateway.
- Sau khi 2 công ty được hợp nhất.
- Về mặt chính trị, có những tư tưởng khác nhau giữa các nhà quản trị mạng khác nhau.

- Trong một môi trường rất lớn, những vùng khác nhau có những yêu cầu khác nhau, do đó một giải pháp đơn lẻ là không hiệu quả. Ví dụ: một mạng đa quốc gia, thì EIGRP là giao thức định tuyến được sử dụng ở access layer và distribution layer nhưng BGP là giao thức định tuyến được dùng kết nối với core layer.

## 2. Các vấn đề phát sinh và giải pháp khi thực hiện redistribution.

Đặc trưng của các giao thức định tuyến mà hầu hết được mang trong redistribution là sự khác nhau trong metric và administrative distance, và khả năng classful hay classless của chúng. Nếu không xem xét cẩn thận sự khác nhau này khi redistribution các giao thức định tuyến có thể dẫn tới các vấn đề như không trao đổi một vài hoặc tất cả các tuyến (route), routing loop và black hole.

### a/ Metric

Static route không có metric đi kèm với chúng, nhưng mỗi OSPF route (tuyến OSPF) phải có một giá trị cost đi kèm. Một ví dụ khác liên quan đến metric nữa đó là redistribution của RIP route (tuyến RIP) vào IGRP. Metric của RIP là hop count, trong khi IGRP sử dụng bandwidth và delay. Metric của IGRP là một số 24 bit trong khi của RIP giá trị giới hạn là 15. Trong cả 2 trường hợp, yêu cầu đổi với giao thức định tuyến tham gia redistribution là đổi với những tuyến (route) được redistribution vào domain của nó thì nó phải kết hợp được metric của nó với metric của những tuyến đó.

Do đó cần có một giải pháp. Đó là khi router thực hiện redistribution phải gán một giá trị metric cho những tuyến tham gia redistribution, tức là chuyển đổi metric của các tuyến từ giao thức cũ (ví dụ là RIP – dùng hop count) sang giao thức mới (ví dụ là IGRP – dùng bandwidth+ delay). Quá trình chuyển đổi nên thực hiện ngay trong lúc redistribution và trên router chạy nhiều routing protocol.

Một ví dụ là EIGRP và OSPF. EIGRP được redistribution vào OSPF và ngược lại OSPF được redistribution vào EIGRP. OSPF không hiểu metric tổ hợp của EIGRP và EIGRP cũng không hiểu cost của OSPF. Kết quả là, các phần của quá trình redistribution các router phải được gán một cost cho mỗi EIGRP route trước khi tuyến đó được quảng bá sang OSPF domain. Tương tự như vậy, router cũng phải gán một cặp giá trị sau: bandwidth, delay, reliability, load và MTU cho mỗi OSPF route trước khi nó được quảng bá sang EIGRP domain. Nếu quá trình gán metric là không đúng thì quá trình redistribution sẽ thất bại.

### b. Khoảng cách quản lý (Administrative Distance)

Tính đa dạng của metric còn gây ra vấn đề sau: nếu một router chạy nhiều hơn một giao thức định tuyến và học một tuyến (route) tới cùng một đích từ mỗi giao thức tương ứng, thì tuyến nào sẽ được chọn? Mỗi giao thức định tuyến sử

dụng metric của nó để xác định ra route tốt nhất theo cách của mình. So sánh tuyến (route) với metric khác nhau chẳng hạn: hop count và cost, chẳng khác nào so sánh táo và cam.

Có một giải pháp để giải quyết vấn đề này đó là administrative distance. Đúng như metric được gán cho mỗi tuyến (route) đến mức độ ưu tiên của mỗi route có thể được xác định, administrative distance được gán cho tuyến nguồn (route source) đến mức độ ưu tiên hn của tuyến nguồn được xác định. Như trong phần hai đã giới thiệu administrative distance nó như là thước đo về độ tin cậy. Giá trị administrative distance càng nhỏ thì độ tin cậy của thông tin định tuyến trao đổi bởi giao thức tương ứng càng lớn.

Ví dụ, giả sử một router chạy 2 giao thức định tuyến là RIP và EIGRP. Khi router học một tuyến tới mạng 192.168.5.0 bằng cả 2 giao thức định tuyến thì nó sẽ nhận được thông tin về tuyến tới mạng 192.168.5.0 từ cả RIP neighbor và EIGRP neighbor. Bởi vì EIGRP sử dụng metric tổ hợp cho nên những thông tin định tuyến học được từ EIGRP sẽ chính xác hơn là thông tin định tuyến học được từ RIP. Do đó, EIGRP tin cậy hơn RIP.

Bảng 3.3 cho biết các giá trị administrative distance mặc định của các giao thức định tuyến khác nhau. EIGRP có administrative distance là 90 trong khi RIP là 120. Điều đó chứng tỏ EIGRP tin cậy hơn RIP.

### c. Redistributing từ Classless vào Classful Protocols

Sự suy xét thận trọng đã được nói rõ được nói rõ khi thực hiện redistribution từ một classless routing process domain vào một classful domain. Để hiểu được tại sao lại như vậy, đầu tiên cần hiểu một classful routing protocol phản ứng lại như thế nào với sự thay đổi của subnet. Như đã biết RIP là một classful routing protocol cho nên nó không gửi mask trong thông tin định tuyến. Đối với các route mà một classful router nhận được sẽ rI vào một trong 2 khả năng sau:

- Router sẽ có một hay nhiều hơn interface gắn với mạng chính (major network).
- Router sẽ không có interface gắn vào mạng chính.

Giải pháp 1: cho việc redistribution giữa classful routing protocol và classless routing protocol là sử dụng định tuyến tĩnh để phân phối các route vào trong classful routing domain.

Giai pháp 2: thực hiện route summary để nhóm các subnet con thành một subnet to hơn mà classful routing domain hiểu được.

## Bài 6:

### **Thảo luận các vấn đề về cáp quang**

#### **Hỏi:**

1. *Cho em hỏi về sự khác nhau giữa cáp quang SM và MM?*
2. *Các thiết bị đầu cuối để hàn sợi cáp quang trước khi gắn nó vào switch. Trên một số switch, em thấy có giao tiếp FX; đôi khi em thấy giao tiếp cáp quang là SX hoặc LX. Vậy trong trường hợp nào thì mình sẽ dùng fx, và trong trường hợp nào mình dùng sx. Sợi cáp patch-cable để dùng cho fx là st/sc. Tuy nhiên em không phân biệt được trong trường hợp nào em dùng st/st hoặc sc/sc. Các anh có thể giải thích cho em được không?*
3. *Các bạn thử lý giải tại sao sợi đơn mode cần đến các bộ suy hao 5dB, 10dB ở khoảng cách gần?*

#### **Trả lời:**

1. Sợi quang là những dây nhỏ và dẻo truyền các ánh sáng nhìn thấy được và các tia hồng ngoại. Chúng có 3 lớp: lõi (core), áo (cladding) và vỏ bọc (coating). Để ánh sáng có thể phản xạ một cách hoàn toàn trong lõi thì chiết suất của lõi lớn hơn chiết suất của áo một chút. Vỏ bọc ở phía ngoài áo bảo vệ sợi quang khỏi bị ẩm và ăn mòn, đồng thời chống xuyên âm với các sợi đi bên cạnh. Lõi và áo được làm bằng thủy tinh hay chất dẻo (Silica), chất dẻo, kim loại, fluor, sợi quang kết tinh). Thành phần lõi và vỏ có chiết suất khác nhau. Chiết suất của những lớp này như thế này sẽ quyết định tính chất của sợi quang. Chúng được phân loại thành các loại sợi quang đơn mode (Single Mode – SM) và đa mode (Multimode -MM) tương ứng với số lượng mode của ánh sáng truyền qua sợi quang. Mode sóng là một trạng thái truyền ổn định của sóng ánh sáng (cũng có thể hiểu một mode là một tia).

Sợi quang đơn mode hay sợi quang đa mode đều chỉ truyền một tín hiệu (là dữ liệu mà ta cần truyền). Muốn truyền nhiều dữ liệu từ các kênh khác nhau, ta phải dùng đến công nghệ WDM (truyền nhiều bước sóng trên cùng một sợi quang). Sợi đa mode có thể truyền cùng lúc nhiều ánh sáng với góc anpha khác nhau, còn sợi đơn mode chỉ có thể truyền 1 ánh sáng với 1 bước sóng nhất định. Do sợi quang là vật liệu truyền thông tin dựa trên định luật phản xạ ánh sáng. Tia sáng khi đi từ môi trường có chiết suất cao qua môi trường chiết suất thấp thì không đi thẳng (hay còn gọi là tán xạ) mà sẽ phản xạ lại. Do đó, khi ánh sáng mang thông tin, sẽ được truyền đi mà không bị suy hao gì cả (vì nó cứ chạy lòng vòng trong đó, phản xạ bên này, rồi phản xạ bên kia. Sợi quang đơn mode thì lõi có chiết suất là một hằng số và chiết suất của vỏ cũng là 1 hằng số. Khi đó ánh sáng sẽ truyền đi theo đường ziczac trong sợi quang (độ lệnh pha của tín hiệu khi đó sẽ đáng kể). Sợi đa mode là công nghệ tiên tiến hơn, chiết suất từ lõi ra đến vỏ sẽ giảm từ từ (nhưng vẫn đảm bảo một tỉ số chiết suất để

ánh sáng chỉ phản xạ chứ không tán xạ), khi đó thì ánh sáng sẽ đi theo đường cong, độ lệnh pha sẽ ít hơn nhiều so với hình ziczac của loại đơn mode. Đa mode còn chia làm 2 loại, đó là step mode và grade mode. Step mode thì chiết suất từ lõi đến vỏ giảm dần, nhưng theo từng nấc, còn grade mode thì giảm liên tục và dĩ nhiên là grade mode sẽ tốt hơn step mode. Dĩ nhiên là việc dùng đa mode thì còn phụ thuộc nhiều yếu tố nữa như là giá thành, các thiết bị đầu cuối (ghép kênh quang). Sợi SM chỉ truyền được một mode sóng do đường kính lõi rất nhỏ (khoảng 10 micromet). Do chỉ truyền một mode sóng nên SM không bị ảnh hưởng bởi hiện tượng tán sắc và thực tế SM thường được sử dụng hơn so với MM. Sợi MM có đường kính lõi lớn hơn SM (khoảng 6-8 lần), có thể truyền được nhiều mode sóng trong lõi.

Thông số vật lý của hai loại cáp này:

Đường kính lõi sợi (phần truyền tin):

Core.

SM: 9/125;

MM: 50/125 và 62.5/125.

Đường kính vỏ phản xạ: Cladding thì cả SM và MM đều nhau là 125um.

Hiện nay, cáp quang single mode chỉ dùng cho đường trực, ngoài việc giá thành ra, công nghệ của cáp single mode rất khắc khe, và rất khó trong việc thi công cũng như sử dụng. Lý do chính là do lớp lõi của cáp single mode rất nhỏ (khoảng 27 Micromet) còn của multi mode thi lớn hơn rất nhiều (khoảng 130 Micromet). Ngoài ra, do kết cấu lõi single mode cho ánh sáng đi theo đường thẳng, mà giá thành chế tạo, cũng như độ chính xác trong thi công, thiết bị công nghệ cao... làm cho cáp SM khó thực hiện trong các công trình dân sự.

Về Coating thì tùy thuộc vào đặc tính cần bảo vệ mà người ta làm lớp này, tuy nhiên thông thường đối với cáp outdoor thì nó là 250, với cáp indoor thì nó là 900, điều này không phụ thuộc vào cáp SM hay MM. Về sử dụng thì tùy thuộc vào công suất phát, độ nhạy thu, khoảng cách truyền dẫn, tốc độ yêu cầu và giá thành mà người ta quyết định dùng SM hoặc MM.

Minh họa hình đường đi của ánh sáng truyền trong lõi (mà nguyên nhân là do kết cấu của lõi Single Mode Multi Mode):

===== > ----- > - - đường ánh sáng

=====  
Single Mode

Multi mode

Tiếp cận theo quang học tia (ray optic), mode của sợi quang được hiểu là một tia sóng ánh sáng đơn sắc. Sợi quang đa mode là sợi quang truyền nhiều tia sáng cùng một lúc, trong khi sợi quang đơn mode chỉ truyền duy nhất một mode dọc trực. Tiếp cận theo quang học lượng tử, ánh sáng là một loại sóng điện từ (hai thành phần E, H) và truyền dẫn của nó trong sợi quang phải tuân thủ các phương trình của định luật Maxoen. Người ta nhận thấy rằng thành phần điện (véc tơ E) và thành phần từ (véc tơ H) tại lõi và vỏ của sợi quang không độc lập với nhau mà có mối liên hệ thông qua điều kiện biên lõi-vỏ. Bất cứ cặp nghiệm nào của hệ phương trình Maxoen ở lõi và vỏ thoả mãn điều kiện biên được gọi là một mode truyền sóng.

Ngoài cách phân loại như trên, còn vài cách phân loại cáp quang khác. Theo Mode thì có: SM và MM (MM có 2 loại: 62.5 và 50). Theo môi trường lắp đặt thì có Outdoor và In door. Outdoor lại chia ra thành các loại: F8 và Underground.

2. Tại sao sợi quang đơn mode có khả năng truyền tốt hơn sợi đa mode?

Sợi đơn mode truyền xa và tốt hơn sợi đa mode. Trong Single mode, ánh sáng đi theo gần như một đường thẳng trùng với trực cáp, còn trong Multi Mode, ánh sáng đi theo một chùm tia sáng có dạng đồ hình sin đồng trục (vì thế mà ta có thể ghép thêm nhiều ánh sáng có các bước sóng khác nhau). Sợi quang đa mode sẽ gặp hiện tượng tán sắc trong sợi quang giữa các mode truyền dẫn. Đây là yếu điểm chính của đa mode so với đơn mode. Do đó mà tín hiệu trong sợi quang đa mode dễ bị tán xạ hơn, tốc độ truyền kém hơn và khoảng cách truyền gần hơn.

Sợi quang có chỉ số bước và chỉ số lớp tùy theo hình dạng và chiết suất của các phần của lõi sợi. Sợi quang đơn mode hay đa mode phụ thuộc vào bước sóng của ánh sáng truyền trong đó. Cùng một sợi quang nhưng nó có thể là sợi đơn mode với bước sóng này và là sợi đa mode với bước sóng khác. Tuy nhiên trong sợi quang, người ta chỉ truyền một số bước sóng nhất định. Những bước sóng này gọi là các cửa sổ quang. Ba bước sóng đó là 850nm, 1330nm, 1550nm. Thường thì bước sóng 850nm ít được dùng. MM có các bước sóng chuẩn là: 780, 850 và 1300. Hiện nay các thiết bị ít dùng bước sóng 780. SM có các bước sóng: 1310, 1550, 1627. Các thiết bị SM dùng công nghệ DWM thì còn có thể sử dụng nhiều bước sóng khác nữa. Do đó khái niệm sợi đa mode và đơn mode phải gắn liền với bước sóng truyền. Khoảng cách truyền (theo

khuyến cáo) của cáp đa mode là 500m. Khoảng cách truyền (theo khuyến cáo) của cáp đơn mode là 3000m. Sợi quang đơn mode được dùng chủ yếu do ko có hiện tượng tán sắc giữa các mode là nguyên nhân chủ yếu gây nhiễu ở sợi quang. Sợi đơn mode được dùng để làm mạng backbone còn sợi đa mode chỉ dùng truyền giữa các mạng trong vùng. Thêm nữa cả đơn mode và đa mode đều dùng ánh sáng laser hoặc led được, còn sử dụng cái nào là tuỳ vào từng trường hợp cụ thể do nhu cầu và yêu cầu của mạng.

Khi truyền trong sợi quang, sóng ánh sáng bị chi phối bởi một số hiện tượng sau:

(\*) Suy giảm (attenuation): Suy giảm trong sợi quang do hai nguyên nhân chính, là hấp thụ của vật liệu và tán xạ ReyLeng. Hấp thụ vật liệu nhỏ hơn tán xạ ReyLeng nên có thể bỏ qua. Tán xạ ReyLeng do các thăng giáng vi sai trong cấu trúc vật liệu, và giảm khi bước sóng tăng. Đồ thị tổng hợp của các nguyên nhân suy giảm giúp tìm ra ba cửa sổ truyền sóng sử dụng rộng rãi ngày nay (800nm, 1300nm và 1550nm)

(\*) Tán sắc (dispersion): Tán sắc là hiện tượng các thành phần khác nhau của tín hiệu cần truyền truyền đi với các tốc độ khác nhau trong sợi quang. Tán sắc do đó gây ra hiện tượng giãn xung ánh sáng ở đầu ra, gây ra nhiễu chồng phô và là nguyên nhân chính dẫn đến hạn chế của khoảng cách truyền trong sợi quang ngày nay. Có một số loại tán sắc khác nhau, gồm tán sắc mode (sợi quang đa mode mới có), tán sắc phân cực và tán sắc đơn sắc (gồm tán sắc vật liệu + tán sắc ống dẫn sóng), mỗi loại có một ảnh hưởng khác nhau đến quá trình truyền của tín hiệu. Các loại sợi quang dịch tán sắc hạn chế được một phần vấn đề này nên có khoảng cách truyền xa (longhaul).

(\*) Các hiệu ứng phi tuyến: Khi truyền nhiều mode trong sợi quang, hiện tượng phi tuyến gây ra hiện tượng sinh ra các hài từ các mode truyền cơ bản, dẫn đến nhiễu tại đầu thu và giảm công suất tín hiệu truyền.

Các hiện tượng này có ảnh hưởng càng rõ rệt ở khoảng cách càng lớn, và khoảng cách cũng không phải là tham số duy nhất. Chúng làm ảnh hưởng tiêu cực đến biên độ, tần số, các tham số khác về xung truyền, và do đó ảnh hưởng đến khả năng nhận dạng của đầu thu. Hơn nữa, các ảnh hưởng này lại không giống nhau, ví dụ bộ khuyếch đại có thể dùng để hạn chế vấn đề attenuation, nhưng vô hiệu với giãn xung, và các bộ tái tạo xung không thể đảm bảo công suất ngưỡng của đầu thu...gây ra nhiều khó khăn trong khắc phục

Trong số các ảnh hưởng thì tán sắc là nghiêm trọng nhất, và trong số các loại tán sắc thì tán sắc mode là đáng kể nhất. Hãy tưởng tượng hai mode sóng ở lõi và ở ngoài nhất. Khoảng cách về thời gian khi đến đích của chúng là yếu tố quyết định đến khoảng cách truyền. Thông thường khoảng cách này không được vượt quá 1/2 chu kỳ xung cần truyền để bộ thu có khả năng hồi phục tín hiệu như cũ. Đó là lý do chính để sợi đơn mode truyền tốt hơn sợi đa mode trên các tham số kỹ thuật chung. Ngoài ra, còn rất nhiều vấn đề nếu muốn thực sự

hiểu được vấn đề mode và phân biệt giữa chúng. Truyền dẫn quang với power budget là bài toán cần phải cân thận khi tính toán thiết kế. Ngày nay, công nghệ WDM và các phát hiện mới trong kỹ thuật quang đã và đang hướng thế hệ mạng đến một kỷ nguyên mới, kỷ nguyên của Optical Internet.

Đường kính lõi của sợi quang đơn mode nhỏ hơn đường kính lõi của sợi quang đa mode. Điều này xuất phát từ điều kiện đảm bảo tính đơn mode của sợi quang cho bởi công thức sau:

$$(2*\pi/\lambda)*a*\sqrt{n_1*n_1-n_2*n_2} < 2.405$$

Trong đó  $\lambda$  là bước sóng,  $a$  là đường kính lõi sợi quang và  $n_1, n_2$  lần lượt là chiết suất lõi vỏ. Trên đồ thị biểu diễn số mode và diameter, bạn cần kéo dài a để có thêm số mode truyền sóng.

Rõ ràng với một bước sóng đơn mode tới hạn  $\lambda$ , chiết suất lõi vỏ xác định, thì đường kính sợi quang bị hạn chế bởi công thức trên.

Thực tế ánh sáng có lưỡng tính sóng hạt, và đó đã trở thành một cuộc tranh cãi lớn nhất trong lịch sử Vật lý những năm cuối thế kỷ 19. Tiếp cận theo quang học tia và quang học lượng tử đều cần thiết để lý giải các hiện tượng truyền sóng ánh sáng trong sợi quang, tuy nhiên, bản chất điện từ của sóng ánh sáng giúp giải quyết các vấn đề sáng tố và dễ hiểu hơn nhiều so với các lý giải trong quang học tia. Đơn cử với mode sóng, tiếp cận theo quang học lượng tử giúp bạn có thể hiểu được vấn đề tán sắc phân cực (trong chế độ đơn mode về bản chất vật lý vẫn là dẫn xuất của hai nghiệm độc lập nhưng cùng hằng số truyền sóng, tức vẫn “đa mode”), vấn đề tán sắc ống dẫn sóng (phân bố năng lượng của mode khi truyền trong sợi quang ở lõi và vỏ, phân bố này không giống nhau với các mode khác nhau, dẫn đến năng lượng của sóng đi trong các vùng có chiết suất  $n$  thay đổi, và là nguyên nhân của tán sắc). Chúng ta không cần hiểu sâu sắc đến độ hệ Maxwell giải ntn, nhưng nắm được phương pháp tiếp cận này giúp chúng ta hiểu tốt hơn về sợi quang và các vấn đề truyền dẫn trên sợi quang. Ngoài ra, đưa 2 sợi quang tràn thì không thể phân biệt được SM và MM đâu. Để phân biệt được thì bạn phải có Microscope hoặc Fusion Splicer.

### 3. Về phần gắn thiết bị đầu cuối, hàn và đấu nối cáp quang

Thông thường có hai kỹ thuật đấu nối cáp quang: mài đầu Connector và hàn hồ quang.

#### 3.1. Kỹ thuật mài đầu Connector cáp quang:

Lấy đầu Connector gắn vào sợi quang rồi mài mòn đầu cho phẳng đầu. Có nhiều loại đầu connector của các hãng khác nhau nhưng ở VN thì chủ yếu là đầu connector AMP. Loại đầu này không cần dùng keo gắn mà nó có khóa sợi ở trong. Thi công theo kỹ thuật này thì đơn giản nhưng suy hao cao do làm thủ công và chi phí sửa chữa và xử lý sự cố cáp bằng chi phí làm ban đầu do các đầu Connector chỉ dùng được 1 lần duy nhất.

### 3.2. Kỹ thuật hàn nối bằng hồ quang:

Dùng máy hàn cáp quang chuyên dụng hàn một sợi dây nối vào cáp (dây nối là loại dây đã có 1 đầu Connector gắn sẵn rồi).

Kỹ thuật này có nhược điểm là ít người làm vì chi phí đầu tư máy khá cao (khoảng 12K USD) nhưng ưu điểm của nó là chi phí sửa chữa và xử lý sự cố khá rẻ do dây nối có thể sử dụng nhiều lần (mỗi sợi dây nối dài trung bình 2,5 mét. Mỗi lần xử lý phải cắt đi 3 cm). Bạn kéo cáp quang tới nơi sử dụng, hàn vào pittel, từ pittel gắn vào converter.

Có 2 cách hàn:

- + Hàn bằng máy : \$20/mỗi
- + Hàn bằng tay (bấm) : \$8/mỗi

Một mỗi hàn cáp quang khoảng \$12 (tùy bạn ở xa hay gần, số lượng mỗi hàn....), pigtail FC 1.5m khoảng \$8/ 1 sợi simplex, patch cord FC-SC 5m khoảng \$12/ sợi simplex, ODF 12 port khoảng \$85 / cái.

Khi hàn thì sẽ có một thông số gọi là sai số suy hao. Bạn không thể trên cùng một đường truyền dẫn có quá nhiều mối nối (khoảng 6 mối hàn tay và 10 mối hàn máy). Cáp quang không bị nhiễu bởi từ trường nên không cần thiết phải có khoảng cách.

Dây Patch cord/Pigtail của cáp quang thì cũng giống tác dụng như dây Patch cord bình thường thôi, là đoạn cáp nhảy hai đầu có Connector để kết nối thiết bị quang với sợi quang trên ODF. Sợi pig tail thực chất là một đoạn cáp quang ngắn để nối từ fiber-enclosure đến thiết bị. Sợi cáp quang khi được kéo sẽ kết thúc ở các box gọi là enclosure. Các enclosure này có thể được gắn trên tường nên thing thoáng còn được gọi là wall-mount. Trong giáo trình academy này hay gọi fiber enclose là ODF. Cáp quang sẽ được hàn với các connector trong các ODF/WALLMOUT/ENCLOSURE này. Từ các ODF, anh có thể dùng các sợi pig-tail/patch-cord để gắn vào switch. Giao diện trên switch cho các quang có thể là SC/ST/FC. Dây Pigtail là sợi cáp quang một đầu có Connector, một đầu để hàn vào một sợi cáp quang. Đầu nối quang trên các switch thường là đầu SC (đầu vuông). Có thể thuê các công ty làm dịch vụ như Saicom, Nhân Sinh Phúc, An Minh Phát, Lạc Việt, SPT... hàn cho bạn (hàn sợi pigtail vào cáp quang, đầu còn lại của sợi pigtail cắm vào ODF) ODF thường dùng đầu nối FC (đầu tròn, vặn) vì vậy bạn cần mua thêm ít nhất 4 sợi patch cord FC – SC để nối từ ODF ra switch.

Thật ra giải pháp tốt nhất là hàn thêm sợi quang nếu khoảng cách xa, nếu không chúng ta có thể mua Jumper cord có khoảng cách dài (được biết có một số nhà cung cấp chào hàng dài đến 300 mét). Sau đó chúng ta có thể mua về cắt bỏ một đầu để làm pigtail. Hiện tại máy hàn cáp quang rất phổ dụng, các công ty viễn thông trên địa bàn thành phố đều có khả năng thực hiện công việc này. Một số nơi chọn cách bấm đầu cáp quang thay vì hàn, như vậy rẻ hơn chút ít

nhưng suy hao nhiều hơn là hàn. Dùng kiểu bấm đầu thì mang tính chất tạm thời, khó kiểm soát được hệ thống, nhất là hệ thống mạng trực.

Về thiết bị đầu cuối (Switch/Router) thì cũng đơn giản thôi, bạn học CCNA thì quan tâm đến Ethernet, Media Converter, nếu bạn quan tâm đến viễn thông thì quan tâm đến PDH, SDH, thiết bị DWM. Nói chung hệ thống thông tin quang không có gì phức tạp đâu, đơn giản nó cũng chỉ là Layer 1 thôi. Khoảng cách 1Km thì dùng Switch ở 2 đầu là được, dùng được cá MM và SM. Không cần phải dùng Router, dùng Switch nào có thể config được L2 hay L3 thì tốt mà giá lại rẻ. Hệ thống quang khi đã chạy được rồi thì không có chuyện chập chờn. Nếu dùng Cisco thì có thể dùng con 2960 là được rồi. Nên dùng 2 con 2960 không có cổng GBIC rồi dùng thêm 2 con Media Converter 100Mbps thì giá thành hợp lý nhất, còn nếu không thì dùng con 2960 có cổng Gbic cũng được nhưng không tối ưu về giá tiền. Khoảng cách giữa 2 thiết bị đầu nối bằng cáp quang không quy định cụ thể là bao nhiêu KM. Khoảng cách giữa 2 thiết bị căn cứ vào tính toán suy hao toàn tuyến, công suất phát, độ nhạy thu và công suất dự phòng của thiết bị. Thông thường mỗi thiết bị đều có khuyến cáo chạy ở cự ly nhất định, Chú ý cự ly quang của các loại module, nếu gần quá cần phải gắn thêm bộ suy hao quang để tránh làm hỏng con laser receiver, tuy nhiên đó chỉ là tính tương đối thôi.

### 3.3. Về giá thành của hai giải pháp:

Cả hai giải pháp đều dùng phụ kiện như nhau. Gồm hộp chứa phụ kiện (patchpanel/ ODF), Adaptor, Patchcord.

Đối với giải pháp hàn sợi quang pigtail (giả sử là 6 sợi quang)

pigtail MM: 7 USD/ 1 pcs  
tray :14 USD/ tray 12 or 24 soi  
Công hàn : 4 USD/ moi han

---

Tổng cộng cho 6 sợi:  $42 + 14 + 24 = 80$  USD

Đối với giải pháp bấm đầu connector:

Connector :4 USD/ 1 pcs  
Công bấm đầu: 4 USD/ dau

---

Tổng cộng cho 6 đầu:  $24+24 = 48$  USD

Như vậy chênh lệch cho một điểm tập kết cáp quang có 6 core là  $80 - 48 = 32$  USD.

## Bài 7:

### **Leased line**

#### Câu hỏi liên quan đến leased line:

1. Công ty mình đang xài leased-line 256Kbps, thời gian đầu thì có thể download file và duyệt web rất nhanh nhưng hiện nay rất chậm (có thể nói là chậm như dial-up). Minh cần biết 2 điều là :
  - Làm cách nào để mạng internet chạy nhanh trở lại
  - Làm cách nào để biết được đường leased-line mà mình đang sử dụng có phải là 256Kbps không?
2. DDN là gì? Mời các bạn có hiểu biết về DDN dành chút thời gian post lên cho anh em trong diễn đàn những kiến thức của mình về DDN.
3. Cách cấu hình leased line trên thiết bị của CISCO không?
4. Băng thông của một đường truyền ( ví dụ leased-line) có phải bằng tổng của tốc độ truyền (bit/s) của cả hai chiều (IN/OUT) cộng lại không?

#### Trả lời:

Bạn có thể dùng MRTG để kiểm tra lưu lượng băng thông vào ra, chương trình miễn phí và hỗ trợ khá nhiều phần cứng, chỉ phải cài là cài đặt hơi thủ công mà thôi nhưng dùng rất tốt. Mrtg download tại mrtg.org để kiểm tra tốc độ. Ngay lúc này anh có thể kiểm tra thông số Reliability của cổng Serial bằng cách anh dùng lệnh #show interface Serial X/X ..... Nếu thông số này có tỉ lệ quá thấp thì có thể đường truyền chở anh không tốt. Đây là một thiết bị để kết nối leased line, đúng hơn là thiết bị HDSL Modem.

Thiết bị đầu cuối bạn cần trang bị khi đầu nối leased line tại mạng DDN của Tp HCM là dùng các NTU. NTU thì có rất nhiều loại ví dụ ASM 31 chẳng hạn. Thiết bị này cũng có datarate = 128K. Loại Timeplex AD3, IDSL Max datarate= 128K NTU Timeplex AD3 có datarate =128K, chính xác hơn nếu dưới 128K thì bưu điện sẽ chỉ định khách hàng dùng thiết bị theo bưu điện chỉ định, còn nếu > 128K thì khách hàng dùng loại nào cũng được miễn là > 128K. Thường tất cả các loại thiết bị này có một đầu là V.35, còn một đầu kia nối vào đường line cáp đồng kéo từ bưu điện. TimePlex AD3 được đề cập ở trên đã ngừng sản xuất và được thay thế bằng TimePlex SYNCHRONY® AD7 và hiện tại là AD-10/FR2. Hàng cung cấp NTU thì nhiều lắm, vấn đề là bạn được bưu điện ‘khuyến cáo’ sử dụng loại gì tương thích.

DDN là 1 network hoàn chỉnh dùng để cung cấp các dịch vụ về data. Hiện tại mạng DDN sử dụng công nghệ ghép kênh TDM (TDM-based). Trong tương lai có lẽ sẽ chuyển dần sang các công nghệ mới như DPT/RPR hoặc chuyển sang ATM-based, IP-based. Mạng DDN là một tập hợp các access node (sử dụng các bộ mini MUX, DACS ...) dùng mạng truyền dẫn nội tỉnh hiện có để kết nối các access node lại với nhau (cái định nghĩa này không chắc chắn). Theo em thì DDN (Digital Data Network) là một hệ thống mạng chỉ dựa trên truyền dẫn cáp

đồng. Hiện nay mạng của bưu điện là mạng DDN (tất nhiên là backbone thì vẫn là Optical rồi)

Các access node có 2 nhiệm vụ:

1. Cung cấp dịch vụ data tới người dùng cuối. ví dụ như dịch vụ leasedline.
2. Tập trung lưu lượng (multiplexer) để truyền đi trên mạng truyền dẫn.

Dưới đây so sánh Leased lines (LL) với một số công nghệ khác như FrameRelay và MPLS/VPN.

Việc chọn LL hay FrameRelay tùy thuộc chủ yếu vào nhu cầu sử dụng. Sau đây là bảng so sánh 1 cách cơ bản nhất:

LL: độ bảo mật cao nhất vì có đường truyền dành riêng. Thích hợp cho các ứng dụng rất quan trọng hay các ứng dụng đòi hỏi cao, không chấp nhận delay (như VoIP, SAP,...). Không phụ thuộc vào khả năng và trình độ kỹ thuật của nhà cung cấp dịch vụ, vì LL hoạt động ở lớp 1 chi phí rất cao

FrameRelay: độ bảo mật thấp hơn vì ở mạng FR, dữ liệu được truyền đi chung với các dữ liệu của những khách hàng khác. Thích hợp cho các ứng dụng không đòi hỏi cao. Phụ thuộc vào khả năng và trình độ kỹ thuật của nhà cung cấp dịch vụ, vì FR hoạt động ở lớp 2 chi phí rẻ hơn LL rất nhiều

So sánh giữa leased line (TDM) và MegaWAN (VPN/MPLS), giả sử tốc độ đường truyền cần thuê như nhau. Kết nối 1 văn phòng và 2 chi nhánh.

Leased line:

Ưu điểm:

- Băng thông đảm bảo 100%
- Delay nhỏ
- Jitter nhỏ
- Đa dịch vụ (có thể sử dụng cho các dịch vụ non-IP và IP).

Khuyết điểm:

- Giá thuê rất đắt.
- Thiết bị đầu cuối rất đắt, ít thông dụng, khó tìm.
- Buộc phải sử dụng 1 cặp thiết bị cho mỗi kênh → ở văn phòng cần 2 thiết bị để phục vụ cho 2 điểm chi nhánh.

MegaWAN:

Ưu điểm:

- Băng thông đảm bảo (chỉ sợ nó không khai CBR -Constant Bit Rate cho bácthôi).
- Giá thuê rất rẻ
- Thiết bị đầu cuối thông dụng, dễ mua (modem ADSL bình thường hoặc

SHDSL). HDSL và G.shdsl cho các kết nối data 128Kbps< n x 64Kbps &lt;= 2048Kbps.

- Chỉ cần 1 modem ở văn phòng để phục vụ cho nhiều điểm chi nhánh.
- Phù hợp để kết nối mạng tin học và các dịch vụ trên nền IP.

Khuyết điểm:

- Delay lớn
  - Jitter lớn
- 

Bài 8:

### Xài cáp quang với RJ45

Câu hỏi:

Xin chào,

Tôi có một vấn đề mong được giải đáp. Công ty có 2 buiding cách nhau >200m (cách con đường). Để nối giữa 2 building, cty dùng cáp quang (cách này hợp lý nhất chưa?) để nối 2 đầu. Ở 2 đầu sử dụng LAN router cisco 26xx (để tách rời 2 mạng LAN) chỉ có 2 port FE 10/100. Vậy bây giờ dùng cách nào để nối được cáp quang vào cái đầu Rj-45 của router? Nếu nối thẳng vào Switch 29xx có đầu cho cáp quang ở 2 đầu building thì có thể tách rời 2 mạng không?

Rất cảm ơn

Trả lời từ các thành viên diễn đàn:

Nếu muốn nối 2 văn phòng với khoảng cách gần (< 3km) có rất nhiều giải pháp phụ thuộc vào các thiết bị đầu cuối mà công ty các bạn đang có:

1. Cáp đồng công nghệ G.SHDSL hay công nghệ VDSL:

Có thể kết nối hai tòa nhà bằng dây cáp đồng (loại cáp điện thoại). Dùng thiết bị hai đầu VC102 (Planet VDSL Converter).

- \* Thiết bị này có nhiều chế độ để lựa chọn
- \* Khoảng cách tối đa 1km2
- \* Băng thông khoảng 11mb
- \* Giá cũng khoảng hơn 800usd cho 1 cặp.

Thiết bị cần thiết là hai modem sử dụng công nghệ trên có port Lan (1 hoặc 4 port)

vd: Loại modem G.SHDSL Paradyn 1740 A2 giá tầm 500usd, Zyxel P 792H giá tầm 400usd. Loại modem VDSL Zyxel P972.

Nếu dùng cáp đồng công nghệ G.SHDSL và muốn đấu vào Router: các bạn mua các loại NTU đang có trên thị trường có Interface V35 là ok, tốc độ Syn 2Mbps. Lúc này mạng của bạn giống như một Wan kết nối hai LAN. Nếu công ty dư dả thì mua Interface E1 (modem và cả Router).

vd: sản phẩm của Telindus, CTC ...

Lưu ý: bạn phải có chức năng kéo được cáp đồng nếu ngoài đường, trong khuôn viên công ty thì miễn bàn.

## 2. Cáp quang:

Để kết nối bằng cáp quang bạn cần có:

- Cáp quang: nên xài loại outdoor, có armoured càng tốt. Với khoảng cách khoảng 200-500m thì dùng cáp multimode 50/125um là tốt nhất. Số core thì tùy bạn nhưng tối thiểu là 2 core (Tx & Rx), thông thường là 4 hoặc 8 core để dự phòng.
- ODF x 2 pcs cho 2 building: Tùy vị trí đấu nối/ phòng thiết bị bạn có thể chọn loại rack mount hoặc wall mount, FO adapter chọn loại thông dụng như ST hoặc SC
- Connector quang: tối thiểu là 4 (2 cho mỗi đầu), có thể chọn ST hay SC cho thông dụng cũng như dễ hàn đầu và phải cùng loại với adapter của ODF
- Patch cord quang: nối từ ODF sang media converter, dài khoảng 3m là đủ. Chú ý 2 đầu connector phải cùng loại với adapter của ODF và FO connector của media converter.
- Media converter:tùy nhu cầu băng thông giữa 2 building bạn có thể chọn FE hoặc GE. Chú ý các thông số: Công suất phát tối thiểu, Công suất phát tối đa, độ nhạy đầu thu, ngưỡng công suất thu tối đa, kiểu FO connector.
- Cuối cùng là 2 sợi patch cord RJ45 để nối từ media converter tới switch. Dùng Media Converter là hay nhất và giá rẻ nhất. Trên thị trường có nhiều loại các bạn có thể dò giá để được giá tốt nhất.

Ở hai đầu của đường cáp quang các bạn có thể dùng switch layer 2 hoặc dùng router hoặc một bên là switch và một bên là router.

Bạn kết nối hai switch bằng cáp quang thì hai mạng LAN trở thành một nếu bạn không cấu hình VLAN. Đầu kia nối thẳng vào switch L2. Trang bị 01 Switch có 02 cổng cáp quang là ổn. Mạng chạy thoải mái 1000Mbps.

### RJ45 cáp quang

(LAN)————[SWITCH có cổng cáp quang]————-[SWITCH có cổng cáp quang]————(LAN)

Nếu dùng cáp quang và muốn đấu vào Router ở hai đầu: Các bạn có thể dùng modem quang. Trên Modem quang có nhiều lựa chọn hơn vì nó ra nhiều

Interface hơn : LAN, E1 và V35. Nếu bạn muốn dùng cáp quang trực tiếp trên router bạn có thể mua thêm module NM-1FE-FX.

Nếu không muốn đầu tư thêm switch có cổng quang bạn có thể sử dụng Converter của hãng Planet Fast Ethernet Media Converters. Hiện nay trên thị trường có các dòng media converter 100base FX/100base TX của PlanNet. Giá rẻ (từ 100-300\$ tùy loại). Dùng cáp Multimode thì media converter rẻ hơn Single Mode, khoảng cách từ 500m->80km. Thiết bị này có thể cho băng thông là 100Mbps, khoảng cách 2km với multimode và khoảng 35 km với cáp singlemode.

Sử dụng 01 cặp converter là ổn nhất, giá cả cũng bình thường mà ưu điểm nhất vẫn là dễ lắp đặt và sử dụng, khai thác. Giải pháp cáp quang rất tốt nhưng chi phí cao cho mô hình mạng cho 2 tòa nhà chỉ cách nhau 200m. Dùng cáp quang là giải pháp có băng thông cao và ổn định nhất, ko bị ảnh hưởng bởi môi trường như wireless bridge. Tuy nhiên chi phí có thể cao hơn cũng như thi công sẽ rắc rối hơn. Với khoảng cách trên 2 Km thì bạn dùng cáp quang đơn mốt.

Tốc độ của đường kết nối lúc này không phụ thuộc vào cáp quang mà chỉ phụ thuộc vào thiết bị đầu cuối (router/switch) của bạn. Bạn chạy được tốc độ Gb bình thường hoặc thậm chí 10Gb.

Khoảng cách 200m thì không nên dùng cáp 50/125 mà dùng cáp 62.5/125 thì ổn hơn. Về mặt lý thuyết thì cáp quang 50/125 có độ suy hao ít hơn cáp 62.5/125 nên cáp 50 được dùng cho cự ly xa hơn, tuy nhiên hiện nay công suất phát quang của thiết bị đã được cải thiện đáng kể và giá thành cũng đã giảm nhiều rồi. Lý do nên dùng cáp 62.5/125 vì loại này rất phổ thông và có nhiều nhà cung cấp nên bạn có thể mua được các phụ kiện đi kèm như dây nối, dây nhảy một cách dễ dàng và giá thành cũng rẻ, chắc bạn biết giá thành SP ở VN không phụ thuộc nhiều vào giá SX mà chủ yếu phụ thuộc vào có bao nhiêu người bán thôi. Một điều nữa là hiện nay ở VN vẫn sử dụng kiểu bấm đầu cáp quang mà ít khi hàn, kiểu bấm đầu già thành vừa đắt mà lại không linh hoạt khi cần thay đổi.

Sau cùng, vẫn còn giải pháp Wireless. Bạn có thể chỉ cần dùng 1AP cho cự ly 200m để xây dựng 1 wireless Lan. Lúc này anh cần thêm các wireless card cho các client. Ở khoảng cách lớn hơn, anh cần dùng 2 AP bridge để thiết lập 1 point – to-point connection. Khi này anh vẫn có 1 LAN duy nhất. Trong giải pháp này không cần đến các wireless card, từ PC đến bridge ta sẽ dùng UTP. Chức năng của AP là kết nối hai LAN với nhau.

Bài 9:

## **Khôi phục mật khẩu cho router Cisco**

### **Đặt vấn đề:**

Khi cấu hình một router, người quản trị thiết bị thường đặt các mật khẩu để ngăn chặn việc đăng nhập không hợp lệ vào thiết bị do mình quản lý. Ví dụ, để ngăn chặn việc đăng nhập vào mode privileged từ đó đi đến các mode cấu hình sâu hơn ở bên trong, người quản trị có thể sử dụng enable password hoặc enable secret:

```
Router(config)#enable password vnpro (cấu hình enable password là vnpro)
```

```
Router(config)#enable secret cisco (cấu hình enable secret là cisco)
```

Hoặc thậm chí có thể đặt mật khẩu ngăn chặn đăng nhập không hợp lệ ngay từ cổng console:

```
Router(config)#line console 0  
Router(config-line)#password vnpro  
Router(config-line)#login
```

Việc đặt các mật khẩu như vậy là cần thiết nhằm đảm bảo một mức độ bảo mật cơ bản nhất cho thiết bị. Tuy nhiên, đôi lúc vì bất cẩn, người quản trị có thể đánh nhầm một vài ký tự khi khai báo mật khẩu hoặc có thể quên mất mật khẩu đăng nhập do đó không đăng nhập được vào thiết bị do mình quản lý. Trong trường hợp này, người quản trị cần phải thực hiện một số thao tác nhằm khôi phục lại mật khẩu cho thiết bị. Bài viết này sẽ trình bày nguyên lý cơ bản được sử dụng để khôi phục mật khẩu cho các router của tập đoàn Cisco, kèm theo đó là sự hướng dẫn cụ thể các thao tác để khôi phục mật khẩu trên các dòng router Cisco phổ biến hiện nay là các dòng 2600, 2800.

### **Nguyên lý cơ bản:**

Việc khôi phục mật khẩu dựa trên việc can thiệp vào bước cuối cùng của tiến trình khởi động của router. Để can thiệp vào tiến trình này, người quản trị phải thực hiện thay đổi giá trị của một thông số kỹ thuật trên router có tên gọi là *thanh ghi cấu hình (configuration register)*. Thanh ghi này bao gồm một chuỗi nhị phân 16 bit với mỗi bit đều mang một ý nghĩa, chức năng riêng. Thiết lập các giá trị 0 hay 1 cho các bit có thể ảnh hưởng đến tiến trình khởi động của router. Thanh ghi cấu hình thường được hiển thị dưới dạng số hexa (hệ đếm 16), ví dụ; 0x2102, 0x2142, 0x2100, v.v... (kí hiệu “0x” được sử dụng để chỉ ra đây là các số hexa). Ta xem xét tiến trình khởi động của router:

1. POST (Power On Self Test): Đây là bước đầu tiên, diễn ra ngay sau khi bật nguồn của router, quy trình POST sẽ kiểm tra toàn bộ phần cứng của router để đảm bảo các phần cứng hoạt động đúng.
2. Nạp chương trình bootstrap từ ROM vào RAM để chạy, chương trình này chịu trách nhiệm thực hiện quy trình nạp hệ điều hành (IOS) cho router.
3. Nạp IOS (hệ điều hành của router) từ bộ nhớ Flash vào RAM để chạy.
4. Sau khi được nạp, IOS sẽ nạp file cấu hình startup-config từ bộ nhớ NVRAM vào bộ nhớ RAM thành file running-config và thực hiện file cấu hình này.

Tất cả các mật khẩu sau khi khai báo đều được lưu lại trong file cấu hình startup-config trên bộ nhớ NVRAM và vì thế sau khi file này được nạp và chạy thì các mật khẩu sẽ phát huy tác dụng. Do đó, để bỏ qua các mật khẩu thì phải điều khiển router bỏ qua file startup-config trong bước này và nạp vào một cấu hình trống. Sử dụng cấu hình trống và vào được các mode cấu hình sâu hơn, có thể chỉnh sửa hoặc xóa bỏ các mật khẩu đã lưu trong file cấu hình cũ, từ đó có thể sử dụng lại file cấu hình cũ trong lần khởi động tiếp theo nhưng với các mật khẩu đã được sửa lại theo ý của người quản trị.

Để thực hiện được việc này, cần phải thiết lập giá trị là 1 cho bit thứ 6 của thanh ghi cấu hình (tính từ phải sang trái, bit đầu tiên đứng ngoài cùng bên phải có số thứ tự là 0). Giá trị của cả thanh ghi khi đã thiết lập giá trị 1 cho bit số 6 thường được dùng là : 0x2142 , có ý nghĩa bỏ qua startup-config trong NVRAM khi khởi động. Bình thường, thanh ghi này có giá trị mặc định là 0x2102 (trong đó bit số 6 bằng 0 có ý nghĩa: sử dụng file startup-config trong NVRAM).

### **Các bước cụ thể khôi phục mật khẩu trên router Cisco các dòng 2600, 2800:**

Đầu tiên, giả thiết router đã bị cấu hình sai mật khẩu hoặc mật khẩu bị quên dẫn đến đăng nhập thiết bị không thành công:

```
Vnpro>enable  
Password:  
Password:  
Password:  
% Bad passwords
```

```
Vnpro>
```

Ta tiến hành các bước như sau để khôi phục mật khẩu cho router:

1. Tắt công tắc router và sau khoảng 30s thì bật trở lại, khi router khởi động, màn hình sẽ hiển thị các dòng sau:

```
System Bootstrap, Version 12.4(1r) [hqluong 1r], RELEASE SOFTWARE (fc1)
Copyright (c) 2005 by cisco Systems, Inc.
```

```
Initializing memory for ECC
```

```
c2811 processor with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled
```

```
 Readonly ROMMON initialized
```

( Nhấn Ctrl + Break tại đây)

2. Ctrl + Break là tổ hợp phím ngắt có tác dụng đưa router vào một chế độ đặc biệt gọi là chế độ rommon. Tại chế độ rommon, router sử dụng hệ điều hành phụ trong bộ nhớ ROM để chạy chứ không sử dụng hệ điều hành chính IOS trong flash để chạy:

```
rommon 1 >
```

**Lưu ý:** Nhấn Ctrl + Break ngay khi bật router có thể làm đứng router. Tốt nhất là chờ nhấn ngắt khi router hiện thông báo về kích thước bộ nhớ chính. Ta cũng có thể nhấn Ctrl +Break trong 15 giây đầu tiên. Lưu ý rằng đối với các chương trình terminal khác nhau, tổ hợp phím ngắt có thể khác nhau. Chương trình terminal phổ biến nhất là Window Hyper Terminal sử dụng tổ hợp phím Ctrl+Break để ngắt.

3. Tại rommon, ta thực hiện lệnh đổi giá trị của thanh ghi cấu hình thành 0x2142.

```
rommon 1 > confreg 0x2142
```

```
You must reset or power cycle for new config to take effect
rommon 2 > _
```

4. Sau khi đổi xong giá trị của thanh ghi cấu hình, phải khởi động lại router. Trong rommon, lệnh khởi động lại router là lệnh reset.

```
rommon 2 > reset
c2811 processor with 262144 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled
```

```
 Readonly ROMMON initialized
```

5. Sau khi khởi động lại, router sau khi nạp xong IOS, sẽ bỏ qua không nạp cấu hình từ NVRAM để chạy nữa mà đi vào mode setup, cho phép ta sử dụng một cấu hình trống để chạy.

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Press RETURN to get started!
```

Ta nhập phần trả lời là “no” để sử dụng cấu hình trắng. Khi sử dụng cấu hình trắng, ta đi vào được mode privileged của router, từ đó có thể tiếp tục đi vào các mode cấu hình sâu hơn để chỉnh sửa hoặc loại bỏ mật khẩu trong file cấu hình cũ.

```
Router>enable  
Router#_
```

6. Tiếp theo, copy file startup-config vào thành file running-config. Sau khi copy file startup-config vào, ta có thể thay đổi chỉnh sửa lại mật khẩu cũ nằm trên file này.

```
Router#copy startup-config running-config  
Destination filename [running-config]?
```

```
1058 bytes copied in 0.404 secs (2619 bytes/sec)  
Vnpro#_
```

Ta thấy tên router đã được đổi từ tên mặc định là “Router” thành “Vnpro”. Như vậy, ta đã làm việc trên file cấu hình cũ và bỏ qua được mật khẩu.

7. Kế tiếp, ta chỉ việc xem mật khẩu nào cần chỉnh sửa hoặc loại bỏ để làm các thao tác chỉnh sửa, loại bỏ tương ứng. Ở đây, ví dụ mật khẩu cần sửa lại là enable password, sửa lại thành “vnpro”.

```
Vnpro(config)#enable password vnpro  
Vnpro(config)#exit  
Vnpro#co  
*Feb 25 17:10:17.383: %SYS-5-CONFIG_I: Configured from console by console  
Vnpro#copy  
Vnpro#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
Vnpro#_
```

Sau khi sửa xong, nhớ lưu đè cấu hình lên cấu hình cũ để từ nay về sau sử dụng mật khẩu mới.

8. Bước cuối cùng, ta phải sửa lại thanh ghi cấu hình về mặc định như cũ là 0x2102 để tiến trình khởi động sau này được diễn ra bình thường.

```
Vnpro#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Vnpro(config)#config-register 0x2102  
Vnpro(config)#_
```

Thanh ghi cấu hình sau khi được sửa vẫn giữ nguyên giá trị 0x2142, ta phải khởi động lại router thì giá trị mới 0x2102 mới được sử dụng.

Trên đây là nguyên lý và các bước dùng để khôi phục mật khẩu lỗi hoặc bị quên cho router các dòng 2600, 2800 của hãng Cisco. Đối với các dòng khác có thể có biến đổi chút ít về cách thức và dòng lệnh nhưng nguyên tắc thì vẫn giống như vậy, có thể tham khảo thêm trong các tài liệu hướng dẫn đi kèm hoặc trên trang hỗ trợ của Cisco.

---

Bài 10:

### Clockrate vs bandwidth.

#### Tổng kết các thảo luận được đưa ra về “bandwidth và clockrate”

Các câu hỏi xung quanh vấn đề này:

-Câu lệnh clock rate tạo xung nhịp, vậy nếu chúng ta gõ clockrate càng lớn thì tốc độ truyền dữ liệu giữa DCE và DTE càng cao phải không?

-Còn câu lệnh Bandwidth khi gõ vào một interface nào đó thì có tác dụng gì?

- Cấp xung Clockrate là dùng để đồng bộ 2 đầu (1 là DCE – trên thực tế là nhà cung cấp dịch vụ, 1 là DTE- là người sử dụng), nhưng đồng bộ để làm gì? Còn tốc độ đường truyền là phụ thuộc vào Bandwidth, BW càng cao thì tốc độ đường truyền nhanh và ngược lại. Clockrate ảnh hưởng đến đường truyền? Nếu nói như bạn thì 1 đường có BW=256 với Clockrate = 9600 và 1 đường có BW = 64 với Clockrate = 128000 thì đường nào sẽ nhanh hơn.

Một số ý kiến trả lời:

- Lệnh bandwidth thực chất là tạo một tham số đầu vào để tính ra composite metric (của IGRP). khi bandwidth càng lớn thì metric tính ra càng nhỏ( như vậy con đường sẽ có độ tin cậy cao hơn, và sẽ được ưu tiên so với các con đường khác đến cùng mạng đích để router chọn update vào bảng định tuyến). Lệnh này không có tác dụng làm tăng tốc độ truyền giữa DCE và DTE.

- Còn lệnh clockrate, sẽ làm thay đổi tốc độ truyền dữ liệu vì xung nhịp cao thì dữ liệu sẽ được truyền với tốc độ cao hơn.

- Clock rate càng cao thì dĩ nhiên sẽ cho bạn tốc độ càng cao, nhưng với điều kiện DTE và DCE phải đáp ứng được. Hơn thế nữa tốc độ clockrate không phải là con số bất kỳ bạn nghĩ ra, rồi gõ vào ! Mà nó có những con số cố định sẵn, ví dụ như 9600,19200,56000,64000,115200,... và tùy thuộc vào truyền sync hay async mà những con số quy định này khác nhau. Nhưng dù sao đi nữa thì clockrate này cũng không quyết định hoàn toàn tốc độ truyền trong 1 số trường hợp, thí dụ như modem async, frame relay,... Đối với modem async thì clock rate chỉ quyết định được tốc độ từ DTE đến DCE mà tốc độ thực thì phụ thuộc vào carrier của DCE (modem) . Còn frame relay thì clock rate ảnh hưởng đến access rate mà thôi, data truyền nhanh hay chậm thì còn phụ thuộc CIR. Nhưng dù sao đi nữa thì khi truyền async ta nên cho clockrate > tốc độ carrier vì như vậy giúp cho DTE sẽ giúp CPU trên DTE nhẹ tải hơn cho công việc truyền có thời gian trống nhiều hơn cho những việc khác. Clock Rate chỉ có ý nghĩa trong chế độ truyền đồng bộ, không có ý nghĩa trong truyền bất đồng bộ. Trong chế độ truyền bất đồng bộ, đồng hồ xung nhịp ở hai đầu khác nhau – hay nói cách khác là ko đồng bộ với nhau – thì việc cấp xung nhịp sẽ ko có ý nghĩa gì cả. Khi dùng lệnh clock rate, gõ ? sẽ ra các tốc độ phù hợp. Con số này luôn là bội số của 9600 bps.

- Trong truyền dẫn FR, CIR có ý nghĩa là tốc độ đảm bảo của nhà cung cấp dịch vụ cho khách hàng. Trong điều kiện mạng bị nghẽn thì nhà cung cấp dịch vụ vẫn đảm bảo tốc độ truyền = CIR mà ko thấp hơn. Do đó, thông số CIR cũng ko ảnh hưởng đến tốc độ truyền của FR.

- Bandwidth thì có tác dụng giúp các routing protocol tính các composite metric, không có tác dụng về vấn đề tốc độ trong truyền data.

- Clockrate thể hiện tần số trên đó số liệu được chuyển đi. Tần số càng cao thì số liệu được chuyển đi càng nhanh. Clockrate làm việc ở layer 1.

Còn bandwidth thì hoàn toàn không quan gì đến layer 1 cả. Nó chỉ giúp cho người quản trị theo dõi dễ dàng hơn. Ngoài ra, bandwidth còn được một số dynamic routing protocols như OSPF, EIGRP dùng để tính toán best route đến destination.

Trong ví dụ trên thì đường có clockrate 128k sẽ nhanh hơn rất nhiều so với đường có clockrate 9.6k

- Khả năng truyền số liệu không chỉ phụ thuộc vào clockrate mà còn lệ thuộc vào những yếu tố khác nữa như đường kết nối vật lý, công nghệ truyền dẫn.

- Trong trường hợp dùng dial-up, công nghệ hiện tại chỉ cho phép đến 56K. Xin lưu ý là 56K chỉ là tốc độ kết nối lý thuyết. Tốc độ thực tế khi kết nối sẽ thấp hơn, ví dụ như 48k. Lưu ý là đây không phải là tốc độ truyền số liệu, chỉ là tốc

độ “ở thời điểm kết nối” mà thôi. Trong quá trình truyền số liệu, 2 modems ở 2 đầu sẽ liên tục trao đổi với nhau và tìm ra tốc độ kết nối ổn định cao nhất. Tùy theo đường vật lý (xa hay gần, tốt hay xấu,...) mà tốc độ truyền số liệu “thực tế” sẽ thay đổi, chẳng hạn như chỉ còn 33.6k, 19.2k hay thậm chí không thể truyền được vì có quá nhiều lỗi

Trong trường hợp của ADSL, công nghệ mới này cho phép truyền số liệu ở một tốc độ cao hơn so với trường hợp dùng dial-up. Trong trường hợp dùng lease line, tốc độ 128k được bảo đảm và đồng bộ trên toàn bộ đường đi từ điểm A đến điểm B. Thiết bị ở 2 đầu phải có khả năng hỗ trợ để hoạt động ở tốc độ nay. Tốc độ này sẽ cố định và không thay đổi theo thời gian.

- Khi chúng ta sử dụng router Cisco, có hai câu lệnh thường dùng liên quan đến băng thông. Thứ nhất là lệnh clock rate, lệnh này định nghĩa tỉ lệ bit lớp 1 thực sự. Câu lệnh được sử dụng khi router cung cấp xung đồng hồ, điển hình khi kết nối router sử dụng interface serial với một vài thiết bị lân cận(ví dụ như với router khác).

- Câu lệnh bandwidth thiết lập lượng băng thông sẵn có trên interface. Ví dụ: giao thức định tuyến EIGRP (Enhanced Interior Gateway Routing Protocol) lựa chọn các metric cho interface dựa theo câu lệnh bandwidth, không dựa theo câu lệnh clock rate. Nói tóm lại, băng thông chỉ thay đổi hoạt động của các tool trên interface nhưng không bao giờ thay đổi tốc độ gửi bit thật sự trên một interface.

- Một số tool QoS liên quan đến băng thông của interface, được định nghĩa bởi câu lệnh bandwidth. Các kỹ sư nên xem xét băng thông mặc định khi cho phép các yếu tố QoS. Đối với các interface serial của router Cisco, băng thông mặc định được thiết lập với tốc độ T1 – bất kể băng thông thực sự. Nếu sử dụng subinterface, chúng thừa hưởng băng thông được thiết lập cho interface vật lý tương ứng.

Bài 11:

## AAA

### 1.1.Giới thiệu tổng quan AAA

#### 1.1.1.Việc sử dụng AAA trong vđè bảo mật và điều khiển truy cập mờ rộng mạng

Các nhà quản trị mạng ngày nay phải điều khiển việc truy cập cũng như giám sát thông tin mà người dùng đầu cuối đang thao tác. Những việc làm đó có thể đưa đến thành công hay thất bại của công ty. Với ý tưởng đó, AAA là cách thức tốt nhất để giám sát những gì mà người dùng đầu cuối có thể làm trên

mạng. Ta có thể xác thực (authentication) người dùng, cấp quyền (authorization) cho người dùng, cũng như tập hợp được thông tin như thời gian bắt đầu hay kết thúc của người dùng (accounting). Như ta thấy, bảo mật là vấn đề rất quan trọng.

Với mức độ điều khiển, thật dễ dàng để cài đặt bảo mật và quản trị mạng. Ta có thể định nghĩa các vai trò (role) đưa ra cho user những lệnh mà họ cần để hoàn thành nhiệm vụ của họ và theo dõi những thay đổi trong mạng. Với khả năng log lại các sự kiện, ta có thể có những sự điều chỉnh thích hợp với từng yêu cầu đặt ra. Tất cả những thành phần này là cần thiết để duy trì tính an toàn, bảo mật cho mạng. VỚI THÔNG TIN THU THẬP ĐƯỢC, TA CÓ THỂ TIỀN ĐOÁN VIỆC CẬP NHẬT CẦN THIẾT THEO THỜI GIAN. Yêu cầu bảo mật dữ liệu, gia tăng băng thông, giám sát các vấn đề trên mạng,... tất cả đều có thể tìm thấy trên dịch vụ AAA.

### 1.1.2. Tổng quan AAA

AAA [1] cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. Nó cung cấp việc xác thực (authentication) người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng. Một khi đã nhận dạng người dùng, ta có thể giới hạn thẩm quyền (authorization) mà người dùng có thể làm. Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm. AAA với ba phần xác thực (authentication), cấp quyền (authorization), tính cước (accounting) là các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng, cần thiết để mở rộng và bảo mật mạng. AAA có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Ta có thể bật các dịch vụ AAA trên router, switch, firewall, các thiết bị VPN, server, ...

### 1.1.3. Định nghĩa AAA

Các dịch vụ AAA được chia thành ba phần, xác thực (authentication), cấp quyền (authorization), tính cước (accounting). Ta sẽ tìm hiểu sự khác nhau của ba phần này và cách thức chúng làm việc như thế nào. Điều quan trọng nhất là hiểu về các kiểu khác nhau của tính cước (accounting).

#### 1.1.3.1. Xác thực (Authentication)

Xác thực dùng để nhận dạng (identify) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong AAA Server. Tất nhiên, tùy thuộc vào giao thức mà AAA hỗ trợ mã hóa đến đâu, ít nhất thì cũng mã hóa username và password. Xác thực sẽ xác định người dùng là ai. Ví dụ: Người dùng có username là vnpro và mật khẩu là L@bOnlin3 sẽ là hợp lệ và được xác thực thành công với hệ thống. Sau khi xác thực thành công thì người dùng đó có thể truy cập được vào mạng. Tiến trình này chỉ là một trong các thành phần để điều khiển người dùng với

AAA. Một khi username và password được chấp nhận, AAA có thể dùng để định nghĩa thẩm quyền mà người dùng được phép làm trong hệ thống.

### 1.1.3.2.Thẩm quyền (Authorization)

Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức. AAA cho phép nhà quản trị tạo ra các thuộc tính mô tả các chức năng của người dùng được phép làm. Do đó, người dùng phải được xác thực trước khi cấp quyền cho người đó. AAA Authorization làm việc giống như một tập các thuộc tính mô tả những gì mà người dùng đã được xác thực có thể có. Ví dụ: người dùng vnpro sau khi đã xác thực thành công có thể chỉ được phép truy cập vào server VNLABPRO\_SERVER thông qua FTP. Những thuộc tính này được so sánh với thông tin chưa trong cơ sở dữ liệu của người dùng đó và kết quả được trả về AAA để xác định khả năng cũng như giới hạn thực tế của người đó. Điều này yêu cầu cơ sở dữ liệu phải giao tiếp liên tục với AAA server trong suốt quá trình kết nối đến thiết bị truy cập từ xa (RAS).

### 1.1.3.3.Tính cước (Accounting)

Accounting cho phép nhà quản trị có thể thu thập thông tin như thời gian bắt đầu, thời gian kết thúc người dùng truy cập vào hệ thống, các câu lệnh đã thực thi, thông kê lưu lượng, việc sử dụng tài nguyên và sau đó lưu trữ thông tin trong hệ thống cơ sở dữ liệu quan hệ. Nói cách khác, accounting cho phép giám sát dịch vụ và tài nguyên được người dùng sử dụng. Ví dụ: thống kê cho thấy người dùng có tên truy cập là vnpro đã truy cập vào VNLABPRO\_SERVER bằng giao thức FTP với số lần là 5 lần. Điểm chính trong Accounting đó là cho phép người quản trị giám sát tích cực và tiên đoán được dịch vụ và việc sử dụng tài nguyên. Thông tin này có thể được dùng để tính cước khách hàng, quản lý mạng, kiểm toán sổ sách.

---

Bài 12:

## Vấn đề duplex trong Ethernet

### Chế độ full-duplex trong Ethernet

Cũng giống như trong Ethernet, để cải thiện performance ta có thể dùng chế độ fullduplex. Fast Ethernet có thể cung cấp tốc độ truyền lên đến 100Mbps trong mỗi chiều truyền, dẫn đến kết quả 200Mbps throughput. Thông lượng tối đa 200Mbps này chỉ đạt được khi một thiết bị (trạm làm việc, server, routers hay một switch khác) kết nối trực tiếp đến một switchport. Nói cách khác, các thiết bị đầu cuối của một kết nối phải hỗ trợ fullduplex, có khả năng truyền mà không phải chờ phát hiện và khôi phục khỏi xung đột.

Đặc tả của FastEthernet cũng cho phép tương thích ngược với 10Mbps Ethernet truyền thống. Trong trường hợp 100BaseTX, các switchport thường được gọi là 10/100 để chỉ ra tốc độ dualspeed. Khi này, hai thiết bị ở hai đầu kết nối sẽ tự động dò tìm tốc độ sao cho cả hai có thể hoạt động ở tốc độ cao nhất. Quá trình dò tìm này bao gồm việc phát hiện và chọn lựa công nghệ ở lớp vật lý, tìm chế độ halfduplex hay fullduplex. Nếu cả hai đầu của kết nối được cấu hình theo kiểu autonegotiate, tốc độ chung cao nhất giữa hai thiết bị sẽ được dùng.

Trong quá trình bắt tay dò tìm chế độ duplex của một kết nối, một số thông tin sẽ được trao đổi qua lại giữa hai thiết bị. Điều này có nghĩa là, để cho quá trình dò tìm tự động là thành công, cả hai đầu phải được thiết lập ở chế độ autonegotiate. Nếu khác đi (nghĩa là chỉ có một đầu thiết lập ở autonegotiate), một đầu của kết nối sẽ không nhận được thông tin từ đầu kia và sẽ không có khả năng xác định chế độ chính xác đang được dùng. Nếu quá trình autonegotiation là thất bại, một switchport sẽ trở về chế độ tự động của nó là halfduplex.

Cần chú ý về vấn đề duplex mismatch khi cả hai đầu của kết nối đều không cấu hình cho autonegotiation. Khi có mismatch xảy ra, một đầu của kết nối sẽ dùng full-duplex trong khi đầu kia dùng halfduplex. Kết quả là máy trạm đang hoạt động ở chế độ half-duplex sẽ luôn phát hiện ra collision khi cả hai đều muốn truyền. Máy trạm đang chạy ở full-duplex sẽ giả sử là nó có quyền truyền ở bất kỳ thời điểm nào. Máy trạm này sẽ không dừng lại và chờ. Tình trạng này dẫn đến lỗi trên kết nối và tốc độ đáp ứng rất chậm giữa các máy.

Quá trình bắt tay sẽ dùng bảng các độ ưu tiên dưới đây. Khi cả hai đầu kết nối có thể bắt tay nhau ở nhiều tốc độ, tốc độ nào có độ ưu tiên cao nhất sẽ được dùng. Ví dụ, nếu cả hai thiết bị có thể chạy ở mức 6 (100BbaseTX fullduplex) và mức 2 (10base2full), mức 6 sẽ được dùng.

độ ưu tiên	Chế độ ethernet
7	100Base-t2 (full duplex)
6	100Base-TX (full duplex)
5	100BASE-t2 (half duplex)
4	100Base-T4
3	100Base-TX
2	10base-T (full duplex)
1	10Base-T

Để đảm bảo cấu hình chính xác ở cả hai đầu của kết nối, Cisco khuyến cáo các giá trị về tốc độ truyền, duplex mode phải được cấu hình thủ công (manually) trên các switchports. Yếu tố này giúp loại trừ khả năng một bên thay đổi các cài đặt, dẫn đến kết nối có thể không dùng được. Nếu bạn đã cấu hình thủ công switchport, hãy thiết lập luôn cho thiết bị trên đầu kia của kết nối các thông số tương ứng. Nếu khác đi, vấn đề speed mismatch hay duplex mismatch sẽ xảy ra.

Bài 13:

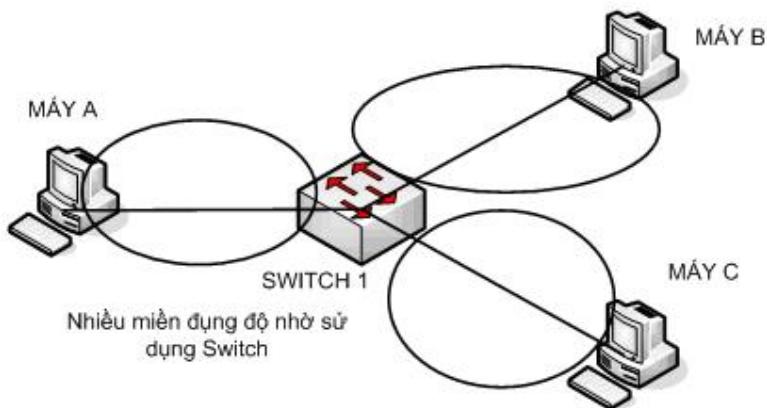
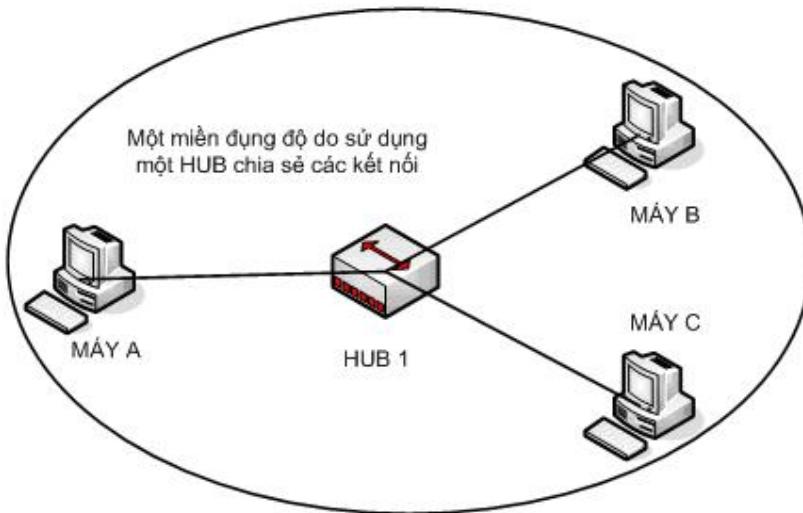
## **Collision domain**

### **Miền đụng độ và bộ đệm chuyển mạch:**

Một miền đụng độ (Collision domain) là một tập hợp các thiết bị có thể gửi các khung tin mà các khung tin này có thể bị đụng độ với các khung tin của một thiết bị khác. Trước khi switch được phát minh, Ethernet thường dùng hub hoặc các đoạn cáp dùng chung như 10Base2 và 10Base5. Switch trong công nghệ Ethernet giúp giảm khả năng đụng độ thông qua quá trình lưu các khung tin trong bộ đệm và cơ chế hoạt động ở lớp 2 của nó.

Theo định nghĩa, Hub trong công nghệ Ethernet sẽ bao gồm các đặc điểm sau:

- Hoạt động chỉ ở lớp 1 của mô hình tham chiếu OSI.
- Khuyếch đại, tái tạo tín hiệu điện để nâng chiều dài đường truyền.



*Miền đụng độ (Collision Domain)*

Chuyển tín hiệu nhận được trên một cổng ra tất cả những cổng khác ngoại trừ cổng nhận vào, và không có bộ đệm.

Như vậy hub sẽ tạo ra một miền đụng độ. Ngược lại, switch sẽ giới hạn miền đụng độ trên từng cổng của nó.

Switch cũng dùng cùng loại cáp và khuếch đại tín hiệu giống như hub, nhưng switch làm nhiều việc hơn. Độ đụng độ sẽ giảm thiểu do các khung tin được đệm, khi switch nhận được các khung tin trên các cổng khác nhau, switch lưu khung tin trong các bộ nhớ đệm để ngăn ngừa xung đột. Ví dụ, giả sử một switch nhận ba khung tin ở cùng một thời điểm đi vào ba cổng khác nhau và nó phải được đưa ra cùng một cổng của switch. Lúc này switch sẽ lưu hai khung tin trong bộ nhớ, và chuyển các khung tin đó đi một cách tuần tự. Khi một cổng của switch kết nối đến một thiết bị không phải là HUB, đụng độ sẽ không thể xảy ra. Thiết bị duy nhất có thể tạo ra đụng độ là bản thân cổng switch và một thiết bị kết nối

vào nó và nếu mỗi bên có một cặp cáp riêng để truyền. Vì dung độ không thể xảy ra, những phân đoạn mạng trên có thể sử dụng chế độ song công.

---

Bài 14:

## Các phương thức chống loop của RIP

### Hội tụ (Convergence) và chống loop:

Phần quan trọng nhất và cũng phức tạp nhất của RIP nằm ở những phương thức chống loop. Giống như những giao thức định tuyến distance vector khác, RIP sử dụng kết hợp những công cụ chống loop khác nhau, nhưng đáng tiếc rằng những công cụ này cũng làm tăng thời gian hội tụ (convergence) một cách đáng kể. Sự thật, đó là một hạn chế rất lớn của RIP (kể cả RIPv2). Bảng 8.3 tổng hợp những tính năng và phương thức liên quan đến sự hội tụ và chống loop của RIP.

Tính năng	Mô tả
Split horizon	Thay vì quảng bá tất cả các route ra một interface, RIP không quảng bá những route mà router học được từ interface này.
Triggered update	Router sẽ gửi một update mới ngay khi thông tin định tuyến bị thay đổi, thay vì phải chờ hết thời gian update time. Trigger update còn có tên gọi khác là flash update. Khi một giá trị metric thay đổi tốt hơn hoặc kém hơn, router ngay lập tức sẽ gửi ra một thông điệp cập nhật mà không cần chờ cho khoảng thời gian update timers bị hết. Quá trình tái hội tụ diễn ra nhanh hơn so với trường hợp phải chờ những khoảng thời gian cập nhật định kỳ. Các thông điệp cập nhật định kỳ vẫn diễn ra cùng với các thông điệp trigger update. Như vậy một router có thể nhận một thông tin kém về một route từ một router chưa hội tụ sau khi đã nhận một thông tin chính xác từ một trigger update. Tình huống này xảy ra và các lỗi định tuyến vẫn có thể xảy ra trong quá trình tái hội tụ.  Một sự hiệu chỉnh xa hơn nữa là trong thông điệp cập nhật, chỉ bao gồm các địa chỉ mạng làm cho việc trigger xảy ra. Kỹ thuật này làm giảm thời gian xử lý và giảm ảnh hưởng đến băng thông.
Route poisoning	khi route bị lỗi, router sẽ gửi update về route đó đi với infinity-metric (hop count = 16).
Poison reverse	Router nhận được quảng bá về một poisoned route (metric 16) trên một interface, router sẽ hồi đáp lại thông điệp

	poison reverse trên cùng interface đó.
Update timer	Qua mỗi khoảng thời gian update timer, router sẽ gửi update một lần qua một interface, mỗi interface có một update timer riêng, mặc định trên tất cả interface là 30 giây.
Holddown timer	<p>Đối với mỗi route đến một subnet trong bảng định tuyến, nếu như metric của route thay đổi đến một giá trị lớn hơn, thời gian holddown timer sẽ bắt đầu. Trong khoảng thời gian này (mặc định là 180 giây) router sẽ không cập nhật route nào khác đến subnet đó trong bảng định tuyến cho đến khi thời gian holddown timer kết thúc.</p> <p>Trigger update sẽ làm tăng khả năng đáp ứng một hệ thống mạng đang hội tụ. Holddown timers sẽ giúp kiểm soát các thông tin định tuyến xấu.</p> <p>Nếu khoảng cách đến một mạng đích tăng (ví dụ số hop count tăng từ hai lên bốn), router sẽ gán một giá trị thời gian cho route đó. Cho đến khi nào thời gian hết hạn, router sẽ không chấp nhận bất kỳ cập nhật nào cho route đó.</p> <p>Rõ ràng có một sự đánh đổi ở đây. Khả năng các thông tin định tuyến kém bị đưa vào bảng định tuyến là giảm nhưng bù lại thời gian hội tụ sẽ tăng lên. Nếu thời gian holdown là quá ngắn, nó sẽ không hiệu quả. Nếu khoảng thời gian là quá dài, quá trình định tuyến thông thường sẽ bị ảnh hưởng.</p>
Invalid timer	Đối với mỗi route tồn tại trong bảng định tuyến, thời gian invalid timer sẽ tăng cho đến khi router nhận được update thông báo về route đó. Nếu như nhận được update, thời gian invalid sẽ được đặt về 0. Nếu như router không nhận được update, mà thời gian invalid đã hết (mặc định là 180 giây), route đó được xem như là không dùng được.
Flush (Garbage) timer	Thời gian flush timer mặc định là 240 giây, cũng giống như thời gian invalid timer, tuy nhiên thời gian flush timer mặc định sẽ tăng thêm 60 nữa, trong thời gian này nếu không nhận được update về route, router sẽ loại route đó ra khỏi bảng định tuyến.

## Tắt Frame Relay InARP

### Tắt InARP:

Trong hầu hết những mô hình mạng được đưa ra, việc sử dụng InARP là hợp lý. Tuy nhiên, ta có thể tắt InARP trên interface vật lý hay multipoint interface đi bằng cách sử dụng lệnh no frame-relay inverse-arp trên interface subcommand. Có thể ngừng hoạt động InARP trên tất cả các VC của interface/subinterface, tắt cả các VC của interface/subinterface ứng với một giao thức L3 riêng biệt, hay đơn thuần là trên mỗi DLCI cụ thể.

Câu lệnh no frame-relay inverse-arp không chỉ làm cho router ngừng việc gửi thông điệp InARP ra ngoài, mà còn làm cho router không nhận thông điệp InARP. Lấy ví dụ, câu lệnh no frame-relay inverse-arp ip 400 ở mode subinterface trên Router R1 trong ví dụ 1.2 không chỉ ngăn R1 ngừng gửi thông điệp InARP ra DLCI400 tới R4 mà còn làm cho R1 bỏ đi thông điệp InARP đã nhận trên DLCI400.

*Bảng 15.1 : Tổng hợp một số đặc tính chi tiết về Frame Relay Inverse ARP trên IOS*

Cách cài đặt trên mỗi kiểu interface riêng biệt	Interface Point-to-point	Interface multipoint hoặc interface vật lý
InARP có đòi hỏi LMI không ?	Luôn luôn	Luôn luôn
InARP được kích hoạt một cách mặc định ?	Đúng	Đúng
Có thể tắt hoạt động của InARP không ?	Có	Không
Có thể bỏ qua thông điệp InARP đã nhận hay không	Luôn luôn (*)	Khi InARP bị tắt đi

(\*) Interface point-to-point luôn luôn bỏ qua thông điệp InARP, bởi vì đối với point-to-point interface, chỉ dùng một DLCI để gửi đến tất cả địa chỉ trong cùng một subnet.

Bài 16:

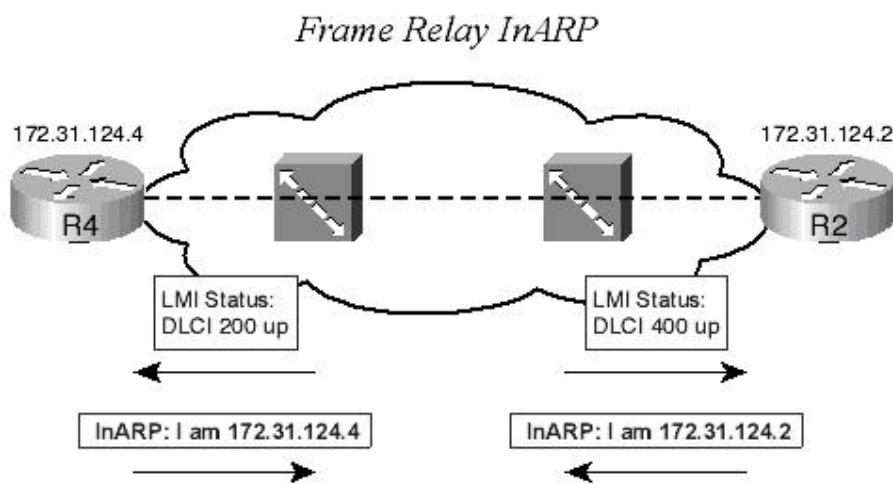
## Giao thức Frame Relay Inverse ARP

### Frame Relay Inverse ARP:

IP ARP được biết đến như một giao thức phổ thông và tương đối đơn giản. Đối với kỳ thi CCIE cũng vậy. Đa số các câu hỏi trong phần IP ARP là những câu hỏi đơn giản. Do đó, những câu hỏi khó về chủ đề xây dựng CEF adjacency table sẽ tập trung vào Frame Relay Inverse ARP, cũng chính vì vậy mà phương thức Frame Relay Inverse ARP sẽ được trình bày cụ thể và chi tiết hơn.

Tương tự như IP ARP, nhiệm vụ của InARP là phân giải giữa địa chỉ L3 và địa chỉ L2. Địa chỉ L3 chính là địa chỉ IP, còn địa chỉ L2 ở đây chính là số DLCI (tương tự như địa chỉ MAC trong IP ARP). Tuy nhiên, trong phương thức InARP, router đã biết được địa chỉ L2 (DLCI), và cần phân giải ra địa chỉ L3 (IP) tương ứng.

Hình sau là một ví dụ về chức năng của InARP.



Trong môi trường LAN, đòi hỏi phải có một gói tin (ARP request) đến host và kích hoạt giao thức IP ARP trên host (trả về ARP reply). Tuy nhiên, trong môi trường WAN, không cần một gói tin nào đến router để kích hoạt InARP trên router này, thay vào đó là một thông điệp về tình trạng LMI (Local Management Interface) sẽ được dùng.

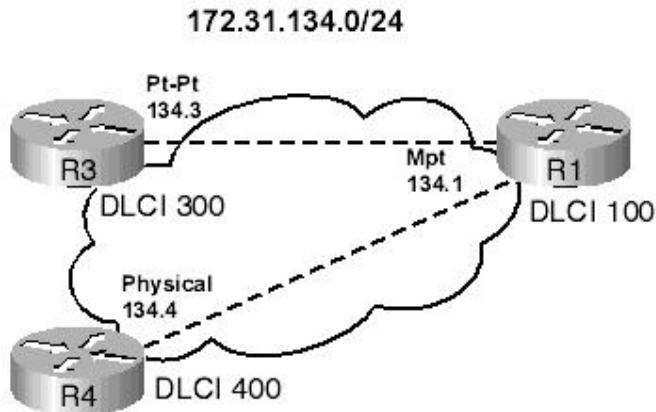
Sau khi nhận được thông điệp trạng thái LMI là LMI PVC Up, router sẽ loan báo địa chỉ IP của nó ra mạch liên kết ảo (VC – Virtual Circuit) tương ứng thông qua thông điệp InARP (định nghĩa trong RFC1293). Như vậy, một khi LMI không được thực thi thì InARP cũng không hoạt động bởi vì không có thông điệp nào nói cho router biết để gửi thông điệp InARP.

Trong mạng Frame Relay, những cấu hình chi tiết được chọn lựa với mục đích tránh một số tình trạng không mong muốn, những tình trạng này sẽ được mô tả chi tiết trong những trang kế tiếp của chương này. Ví dụ khi sử dụng point-to-point subinterface, với mỗi VC thuộc một subnet riêng, tất cả những vấn đề gấp phai trong cấu hình này sẽ được mô tả rõ ràng để có thể phòng tránh.

Bản thân giao thức InARP tương đối đơn giản. Tuy nhiên, khi triển khai InARP trên những mô hình mạng khác nhau, dựa trên những kiểu cổng khác nhau (cổng vật lý, cổng point-to-point subinterface và multipoint subinterface) thì cách thức hoạt động của InARP sẽ trở nên phức tạp hơn rất nhiều.

Sau đây là một ví dụ về hệ thống mạng Frame Relay được thiết kế theo mô hình mạng lưới không đầy đủ (partial mesh) trên cùng một subnet trong khi mỗi router sử dụng một kiểu cổng khác nhau.

#### *Frame Relay Topology for Frame Relay InARP Examples*



Sơ đồ mạng trên chỉ mang tính chất là một ví dụ, nó chỉ sử dụng trong môi trường học tập để hiểu chi tiết hơn về cách thức hoạt động của InARP. Sơ đồ này không nên được áp dụng trong môi trường mạng thực tế bởi thiết kế yếu kém với nhiều hạn chế khi triển khai giao thức định tuyến bên trên.

Đầu tiên cấu hình frame relay trên cổng multipoint của R1.

```
Router1# sh run

! Lines omitted for brevity

interface Serial0/0

encapsulation frame-relay

interface Serial0/0.11 multipoint

ip address 172.31.134.1 255.255.255.0

frame-relay interface-dlci 300

frame-relay interface-dlci 400

! Lines omitted for brevity
```

Kết nối, cổng serial được tắt và bật và các hàng trong InARP trước đó bị xóa vì vậy ta có thể quan sát tiến trình InARP.

```
Router1# conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)# int s 0/0

Router1(config-if)# do clear frame-relay inarp

Router1(config-if)# shut

Router1(config-if)# no shut

Router1(config-if)# ^Z
```

Các thông điệp từ lệnh debug frame-relay event hiển thị các thông điệp nhận được InARP trên R1. Chú ý các giá trị hex 0xAC1F8603 và 0xAC1F8604, với các giá trị thập phân tương ứng là 172.31.134.3 and 172.31.134.4 (tương ứng với Router3 và Router4).

```
Router1# debug frame-relay events
```

```
*Mar 1 00:09:45.334: Serial0/0.11: FR ARP input  
*Mar 1 00:09:45.334: datagramstart = 0x392BA0E, datagramsize = 34  
*Mar 1 00:09:45.334: FR encap = 0x48C10300  
*Mar 1 00:09:45.334: 80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00  
*Mar 1 00:09:45.334: AC 1F 86 03 48 C1 AC 1F 86 01 01 02 00 00  
*Mar 1 00:09:45.334:  
*Mar 1 00:09:45.334: Serial0/0.11: FR ARP input  
*Mar 1 00:09:45.334: datagramstart = 0x392B8CE, datagramsize = 34  
*Mar 1 00:09:45.338: FR encap = 0x64010300  
*Mar 1 00:09:45.338: 80 00 00 00 08 06 00 0F 08 00 02 04 00 09 00 00  
*Mar 1 00:09:45.338: AC 1F 86 04 64 01 AC 1F 86 01 01 02 00 00
```

Kết tiếp, chú ý lệnh show frame-relay map có bao gồm từ khóa dynamic, nghĩa là các hàng được học thông qua InARP.

```
Router1# show frame-relay map
```

```
Serial0/0.11 (up): ip 172.31.134.3 dlci 300(0x12C,0x48C0), dynamic,  
broadcast, status defined, active  
Serial0/0.11 (up): ip 172.31.134.4 dlci 400(0x190,0x6400), dynamic,  
broadcast, status defined, active
```

Trên R3, lệnh show frame-relay map chỉ liệt kê một hàng duy nhất nhưng định dạng thì khác. Bởi vì R3 dùng point-to-point subinterface, hàng này không được học thông qua InARP và kết quả lệnh không bao gồm từ khóa Dynamic. Cũng chú ý là kết quả không cho thấy địa chỉ Layer 3 nào.

```
Router3# show frame-relay map
```

```
Serial0/0.3333 (up): point-to-point dlc1, dlci 100(0x64,0x1840), broadcast  
status defined, active
```

Chú ý: Trong ví dụ trên ta thấy xuất hiện lệnh do trong chế độ cấu hình. Lệnh do cho phép cấu hình trong configuration mode nhưng để thực hiện chức năng ở exec mode mà không phải thoát khỏi mode configuration. Ví dụ lệnh do clear frame-relay inarp thực hiện ở configuration mode tương đương với việc ta thực hiện lệnh clear frame-relay inarp ở chế độ toàn cục.

Trong ví dụ trên, lệnh show cho thấy Router R1 đã nhận và sử dụng thông tin InARP; tuy nhiên Router R3 thì không sử dụng thông tin InARP đã nhận vào. Hệ điều hành Cisco IOS hiểu rằng chỉ một VC được thiết lập với một subinterface point-to-point; mỗi một địa chỉ IP đầu cuối khác trên cùng một subnet chỉ có thể tham chiếu đến duy nhất một số DLCI. Vì vậy, mỗi thông tin InARP nhận được liên kết đến số DLCI đó là không cần thiết.

Lấy ví dụ, khi nào Router R3 cần gửi một gói tin đến Router R1(172.31.134.1), hay đến mỗi đầu cuối khác trong subnet 172.31.134.0/24. Từ chính cấu hình của mình, Router R3 biết rằng phải gửi qua số DLCI trên point-to-point subinterface đó, nghĩa là qua DLCI 100. Vì vậy, mặc dù cả ba kiểu công được dùng cho cấu hình Frame Relay hỗ trợ InARP một cách mặc định, point-to-point subinterface sẽ bỏ qua thông tin InARP nhận được.

---

Bài 17:

## Giới thiệu về IPv6

Hai vấn đề lớn mà IP v.4 đang phải đổi mới là việc thiếu hụt các địa chỉ, đặc biệt là các không gian địa chỉ tầm trung (lớp B) và việc phát triển về kích thước rất nguy hiểm của các bảng định tuyến trong Internet.

Trong những năm 1990, CIDR được xây dựng dựa trên khái niệm mặt nạ địa chỉ (address mask). CIDR đã tạm thời khắc phục được những vấn đề nêu trên. Khía cạnh tổ chức mang tính thứ bậc của CIDR đã cải tiến khả năng mở rộng của IPv4. Mặc dù có thêm nhiều công cụ khác ra đời như kỹ thuật subnetting (1985), kỹ thuật VLSM (1987) và CIDR (1993), các kỹ thuật trên đã không cứu vớt IP v.4 ra khỏi một vấn đề đơn giản: không có đủ địa chỉ cho các nhu cầu tương lai. Có khoảng 4 tỉ địa chỉ IPv4 nhưng khoảng địa chỉ này là sẽ không đủ trong tương lai với những thiết bị kết nối vào Internet và các thiết bị ứng dụng trong gia đình có thể yêu cầu địa chỉ IP.

Một vài giải pháp tạm thời, chẳng hạn như dùng RFC1918 trong đó dùng một phân không gian địa chỉ làm các địa chỉ dành riêng và NAT là một công cụ cho phép hàng ngàn hosts truy cập vào Internet chỉ với một vài IP hợp lệ. Tuy nhiên giải pháp mang tính dài hạn là việc đưa vào IPv6 với cấu trúc địa chỉ 128-bit. Không gian địa chỉ rộng lớn của IPv6 không chỉ cung cấp nhiều không gian địa chỉ hơn IPv4 mà còn có những cải tiến về cấu trúc. Với 128 bits, sẽ có 340,282,366,920,938,463,374,607,431,768,211,456 địa chỉ.

Trong năm 1994, IETF đã đề xuất IPv6 trong RFC 1752. IPv6 khắc phục vào một số vấn đề như thiếu hụt địa chỉ, chất lượng dịch vụ, tự động cấu hình địa chỉ, vấn đề xác thực và bảo mật. Đối với một doanh nghiệp đã dùng hạ tầng mạng theo IPv4, để chuyển sang IPv6 không phải là việc dễ dàng. Một giao thức IP mới sẽ yêu cầu các phần mềm mới, các phần cứng mới và các phương pháp quản trị mới. Cũng có thể, IPv4 và IPv6 sẽ cùng tồn tại, ngay cả bên trong một Autonomous System trong khoảng thời gian sắp tới.

IP v.6 có các đặc điểm và lợi ích như sau:

Không gian địa chỉ rộng lớn

Địa chỉ unicast và địa chỉ multicast

Tổng hợp địa chỉ (address aggregation)

Tự động cấu hình

Renumbering

Cấu trúc header đơn giản, hiệu quả

Bảo mật

Cơ động

Các tùy chọn để chuyển đổi từ IPv4 sang IPv6

Như được định nghĩa trong RFC1884 và RFC2373, các địa chỉ IPv6 là 128-bit dùng để nhận dạng cho các cổng của routers và tập các cổng của routers. Có ba kiểu địa chỉ tồn tại:

- Unicast: là địa chỉ cho một giao tiếp. Một gói dữ liệu được gửi tới một địa chỉ Unicast sẽ được phân phối tới cổng giao tiếp được chỉ ra bởi địa chỉ đó.

- Anycast: là địa chỉ cho tập hợp các cổng giao tiếp. Các tập này thông thường thuộc về các node khác nhau. Một gói dữ liệu được gửi tới một địa chỉ anycast sẽ được phân phối đến cổng giao tiếp gần nhất hay đầu tiên trong nhóm anycast.

- Multicast: địa chỉ cho một tập hợp các cổng giao tiếp (thông thường thuộc về các node khác nhau). Khi một gói được gửi đến một địa chỉ multicast, tất cả các cổng giao tiếp sẽ nhận được gói dữ liệu này.

Để viết một địa chỉ dạng 128-bit ở dạng dễ đọc hơn, kiến trúc của IPv6 đã loại bỏ dạng cú pháp dấu chấm thập phân của IPv4 mà chỉ dùng dạng thập lục phân. Vì vậy, IPv6 có thể được viết bao gồm 32 ký tự dạng hex với dấu hai chấm ‘::’ tách địa chỉ ra thành tám phần, mỗi phần có chiều dài 16-bit.

Theo các kế hoạch hiện tại, các node chạy IPv6 kết nối vào Internet sẽ dùng một kỹ thuật gọi là địa chỉ khả kết toàn cục (aggregatable global unicast address). Trong đó có nhiều điểm tương đồng với kỹ thuật summary như trong version 4.

Địa chỉ tích hợp của IPv6 có ba mức:

Mức public topology: là tập hợp các nhà cung cấp kết nối Internet.

Mức vùng: mức này là cục bộ đối với các tổ chức.

Mức cổng giao tiếp: mức này ảnh hưởng đến các cổng giao tiếp riêng lẻ. Link-local address là địa chỉ chỉ được sử dụng trên 1 kết nối (hay 1 cổng của router) và địa chỉ này phải duy nhất trong liên kết đó. Địa chỉ này có thể được sử dụng trong mạng cục bộ (các máy có chung địa chỉ mạng) và có thể không có router trong mạng này. Địa chỉ này có dạng :FE80::<MAC>. Subnet ID của loại địa chỉ này được gán =0. Do đó loại địa chỉ này không thể được sử dụng để giao tiếp ra khỏi subnet cục bộ được.

---

Bài 18:

## **Khái niệm Vlan (CCNA level)**

Trong môi trường Ethernet LAN, tập hợp các thiết bị cùng nhận một gói broadcast bởi bất kỳ một thiết bị còn lại được gọi là một broadcast domain. Trên các switch không hỗ trợ VLAN, switch sẽ đẩy tất cả các broadcast ra tất cả các cổng, ngoại trừ cổng mà nó nhận frame. Kết quả là, tất cả các interface trên loại switch này là cùng broadcast domain. Nếu switch này kết nối đến các switch và các hub khác, các cổng trên switch này cũng sẽ trong cùng broadcast domain.

Một VLAN đơn giản là một tập hợp của các switchport nằm trong cùng broadcast domain. Các cổng có thể được nhóm vào các vlan khác nhau trên từng switch và trên nhiều switch. Bằng cách tạo ra nhiều VLAN, các switch sẽ tạo ra nhiều broadcast domains. Khi đó, khi có một broadcast được gửi bởi một thiết bị nằm trong một vlan sẽ được chuyển đến những thiết bị khác trong cùng

vlan, tuy nhiên broadcast sẽ không được forward đến các thiết bị trong vlan khác.

Mỗi Vlan nên có một ip subnet hay nói cách khác, các thiết bị trong một vlan thường dùng chung một dãy địa chỉ IP. Tuy nhiên, ta vẫn có thể đặt nhiều dãy chỉ trong một vlan và dùng secondary address trên các routers để định tuyến giữa các vlan và các subnets. Bạn cũng có thể thiết kế một mạng dùng chỉ một subnets trên nhiều vlan và dùng routers với chức năng proxy-arp để chuyển traffic giữa các hosts trong các vlan này.

Private vlan có thể được xem như gồm một subnet trên nhiều vlan. Các L2 switch chuyển các frame giữa các thiết bị trên cùng một vlan nhưng nó không chuyển frame giữa các thiết bị khác vlan. Để chuyển dữ liệu giữa hai vlan, một thiết bị L3 switch hoặc routers phải được dùng.

### VLAN Trunking Protocol:

VTP quảng bá các thông tin cấu hình vlan đến các switch láng giềng để các cấu hình vlan có thể được thực hiện trên một switch, trong khi tất cả các switch khác trong hệ thống mạng sẽ học thông tin vlan. VTP thường quảng bá các thông tin như vlan ID, vlan name và kiểu vlan cho từng vlan. Tuy nhiên, VTP thường không quảng bá bất cứ thông tin nào về các switchport nào trong từng vlan nào, vì vậy cấu hình kết hợp switch interface nào với vlan nào vẫn phải được cấu hình trên từng switch. Ngoài ra, sự tồn tại của vlan ID được dùng cho private vlan cũng được quảng bá, nhưng các thông tin chi tiết bên trong private vlan cũng sẽ không được quảng bá bởi VTP.

Chức năng	Server mode	Client	Transparent
Gửi ra các thông tin quảng bá VTP	Yes	No	No
Xử lý các thông tin VTP nhận được để cập nhật cấu hình vlan	Yes	Yes	No
Trung chuyển các thông tin quảng bá của VTP	Yes	Yes	Yes
Lưu thông tin vlan trong NVRAM hay vlan.dat	Yes	No	Yes
Có thể tạo, thay đổi và xóa vlan dùng các lệnh cấu hình	Yes	No	Yes

## Các tiến trình VTP và chỉ số revision number:

Tiến trình cập nhật của VTP bắt đầu khi người quản trị thêm vào hoặc xóa cấu hình của vlan trên VTP server. Khi cấu hình mới xuất hiện, VTP sẽ tăng giá trị VTP revision lên 1 và quảng bá toàn bộ cơ sở dữ liệu vlan với giá trị revision number mới. Khái niệm chỉ số VTP cho phép các switch biết khi nào có sự thay đổi trong cơ sở dữ liệu vlan. Khi nhận được một cập nhật VTP, nếu chỉ số VTP trong cập nhật VTP là cao hơn chỉ số revision number hiện hành, switch sẽ cho rằng có một phiên bản mới của cơ sở dữ liệu vlan.

Mặc định Cisco switch dùng chế độ VTP server nhưng switch sẽ không gửi các cập nhật VTP cho đến khi nào nó được cấu hình VTP domain name. Ở thời điểm này, server bắt đầu gửi các cập nhật VTP với các phiên bản cơ sở dữ liệu khác nhau và các chỉ số revision number khác nhau khi có thông tin cấu hình vlan database thay đổi. Tuy nhiên các VTP client thật sự không được cấu hình VTP domain name. Nếu không được cấu hình, client sẽ giả sử là nó sẽ dùng VTP domain name trong gói tin cập nhật VTP đầu tiên mà nó nhận được. Tuy nhiên, client vẫn phải cần cấu hình VTP mode. Khi cấu hình VTP, để tăng tính dự phòng, các hệ thống mạng dùng VTP thường dùng tối thiểu hai VTP server. Trong điều kiện bình thường, một sự thay đổi về vlan có thể chỉ thực hiện trên switch server và các VTP server khác sẽ cập nhật sự thay đổi này. Sau khi cập nhật xong, VTP server sẽ lưu các thông tin cấu hình vlan thường trực (ví dụ như trong NVRAM) trong khi client không lưu thông tin này.

Việc hỗ trợ nhiều VTP server gây ra một khả năng khác là việc vô tình thay đổi cấu hình vlan của hệ thống mạng. Khi một VTP Client hoặc một VTP transparent switch kết nối lần đầu vào một hệ thống mạng thông qua kết nối trunk, nó không thể ảnh hưởng đến cấu hình hiện tại bởi vì các chế độ hoạt động này không tạo ra các gói tin cập nhật VTP. Tuy nhiên nếu một switch mới hoạt động ở chế độ VTP server được gắn vào mạng thông qua kết nối trunk, switch đó có khả năng thay đổi cấu hình vlan của các switch khác bằng chính thông tin của switch mới. Nếu switch mới có các đặc điểm sau, nó sẽ có thể thay đổi cấu hình các switch khác:

- Kết nối là trunk.
- Switch mới có cùng VTP domain.
- Chỉ số revision number là cao hơn các switch hiện có.
- Nếu mật khẩu của VTP domain là được cấu hình, mật khẩu của switch mới phải là giống. Chỉ số revision number và tên VTP domain có thể được thấy thông qua các phần mềm sniffer. Để ngăn ngừa kiểu tấn công DoS dùng VTP, hãy cài đặt mật khẩu cho VTP. Mật khẩu này thường được mã hóa dạng MD5. Ngoài ra, vài nơi triển khai chỉ đơn giản dùng VTP transparent mode trên tất cả các switch, ngăn ngừa switch khỏi việc lắng nghe các cập nhật VTP từ các switch khác.

## Gigabit Ethernet và 10Gigabit Ethernet

### Gigabit Ethernet:

Ở GE, lớp vật lý đã được bổ sung để tăng tốc độ truyền. Có hai công nghệ đã được kết hợp với nhau để đạt được ưu điểm của từng công nghệ: IEEE 802.3 và ANSI X3T11 FibreChannel. Các yếu tố của 802.3 như định dạng frame, CSMA/CD, fullduplex và các đặc điểm khác vẫn được giữ lại. FibreChannel thì cung cấp một nền tảng mạch ASIC tốc độ cao, các thành phần cáp quang, các cơ chế mã hóa, giải mã.... Kết quả của hai giao thức này là IEEE 802.3z Gigabit Ethernet.

Gigabit Ethernet hỗ trợ vài loại cabling, được gọi là 1000BaseX.

Kiểu GE	Kiểu cáp	Số cặp	Chiều dài
1000BASE-CX	Shield twisted-pair (STP)	1	25m
1000Base-T	EIA/TIA Cat5 UTP	4	100m

Trong mạng campus, bạn có thể dùng Gigabit Ethernet trong switch block, core block và server block. Trong switch block, GE có thể dùng để kết nối access layer switch lên distribution switch. Trong core block, GE dùng để kết nối distribution lên core switch và kết nối các thiết bị core với nhau. Trong server block, GE có thể cung cấp các kết nối tốc độ cao đến từng server riêng lẻ.

Trên Cisco switch, các cổng Gigabit luôn được thiết lập ở chế độ fullduplex. Do đó quá trình tự động bắt tay duplex mode là không thể.

Các switch Catalyst đã chuẩn hóa các giao tiếp GBIC và SFP. GBIC và SFP cho phép các loại cáp khác nhau có thể kết nối. Các module giao tiếp là hotswappable và có khả năng cắm vào switch để hỗ trợ loại media khác. Các giao tiếp GBIC có thể dùng giao tiếp cáp quang SC và RJ45, SFP có thể dùng LC và MT-RJ fiber optic. GBIC và SFP được hỗ trợ trên những cổng Gigabit Ethernet sau:

1000BaseSX dùng SC connector và cáp quang multimode MMF cho khoảng cách lên đến 550m.

1000BaseLX/LH dùng SC connector và có thể dùng với cáp quang MMF đến 550m còn SMF với khoảng cách lên đến 10km.

1000BaseZX dùng SC connector và SMF, có khoảng cách lên đến 70km thậm chí đến 100km với loại cáp quang tốt.

Gigastack dùng một loại connector đặc biệt với tốc độ truyền dữ liệu cao giúp bảo toàn tín hiệu và chống nhiễu, cho phép kết nối GBIC-GBIC giữa các switch. Kết nối là fullduplex nếu chỉ có một stacking connector được dùng. Nếu cả hai connector được dùng, kết nối này trở thành halfduplex trên shared bus.

1000BaseT hỗ trợ kết nối RJ45 dùng cả 4 pair, hoạt động với khoảng cách lên đến 100m. Sơ đồ bấm dây là các chân 1,2,3,6,4,5,7,8 sẽ kết nối đến 3,6,1,2,7,8 và 4,5 trong trường hợp bấm cáp chéo.

Các module quang luôn có chân nhận dữ liệu bên trái và chân truyền dữ liệu bên phải. Các module này có thể tạo ra các bức xạ, vì vậy phải luôn che các chân bằng các nút cao su và không nên nhìn trực tiếp vào connector.

### **10-Gigabit Ethernet:**

Các đặc điểm lớp 2 của Ethernet vẫn được bảo toàn: định dạng frame, MAC protocol vẫn không thay đổi. 10GbE khác với các công nghệ Ethernet tiền bối của nó chỉ ở lớp PHYSICAL. 10GbE hoạt động chỉ ở full duplex. Chuẩn này định nghĩa vài kiểu transceiver có thể được dùng như các giao tiếp phần cứng độc lập (PMD – Physical media dependent).

LAN PHY: Kết nối các switch trong mạng campus, chủ yếu là ở lớp core.

WAN PHY: Giao tiếp với các mạng SONET/SDH trong các mạng MAN.

Các giao tiếp PMD cũng có một cách đặt tên chuẩn chung, giống như GigabitEthernet. Chuẩn 10-Gigabit sẽ có ký hiệu là 10GBASE-X. Bảng dưới đây sẽ liệt kê các loại PMD khác nhau. Tất cả các loại PMD dùng cáp quang có thể được dùng trong LAN PHY hay WAN PHY ngoại trừ loại 10Gbase-LX4, chỉ dùng cho LAN PHY. Ngoài ra, bạn cần biết rằng các loại PMD có bước sóng dài thường có chi phí cao hơn các loại khác.

Kiểu PMD	Fiber media	Khoảng cách tối đa	Catalyst switch
10Gbase-SR/SW (9850 nm serial)	MMF 50 micron	66m	N/A
	MMF: 50 micron (2 GHz* km modal bandwidth)	300m	
	MMF: 62.5 micron	33m	
10Gbase-LR/LW (1310 nm serial)	SMF: 9 micron	10km	Catalyst 6500
10Gbase-ER/EW (1550 nm serial)	SMF 9 micron	40 km	Catalyst 6500
10GBase-	MMF 50 micron	300m	N/A

LX4/LW4 (1310 nm WWDM)			
	MMF 62.5 micron	300m	N/A
	SMF 9 micron	10 km	

---

Bài 20:

## Ethernet 10Mbps

Ethernet là một công nghệ LAN dựa trên chuẩn IEEE 802.3. Ethernet cung cấp băng thông 10Mbps giữa các người dùng cuối. Ở dạng đơn giản nhất, Ethernet sử dụng một thiết bị chia sẻ băng thông (hub). Thiết bị này bị xem như là một collision domain và broadcast domain. Khi số lượng người dùng tăng lên, khả năng một người dùng truyền dữ liệu ở một thời điểm cũng tăng lên. Nếu có một người dùng khác cũng cố gắng truyền dữ liệu, xung đột (collision) sẽ xảy ra. Nói cách khác, cả hai người dùng không thể truyền dữ liệu ở cùng một thời điểm nếu cả hai cùng dùng chung một hub. Ethernet hoạt động dựa trên công nghệ CSMA/CD. Theo đó, không có độ xung đột xảy ra, một máy truyền phải lui về một khoảng thời gian ngẫu nhiên. Switched Ethernet giải quyết vấn đề này bằng cách cấp một phần băng thông 10Mbps đến từng port. Lúc này, collision ít xảy ra và collision domain sẽ giảm. Do đó, các máy trạm không còn phải chờ đến lượt để truyền. Thay vào đó, các máy trạm có thể hoạt động ở chế độ fullduplex: truyền và nhận đồng thời. Chế độ fullduplex sẽ tăng hiệu năng của hệ thống mạng, cung cấp một thông lượng 20Mbps.

Một mối quan tâm khác khi nói về mạng Ethernet 10-Mbps là vấn đề cáp. Ethernet thường dùng cáp UTP, có giới hạn khoảng cách 100m. Trong mạng campus, Ethernet thường được dùng ở lớp access, giữa các thiết bị của người dùng cuối. Ethernet 10Mbps không được dùng ở lớp distribution hay lớp core.

## Fast Ethernet

Fast Ethernet hoạt động ở tốc độ 100Mbps và được đặc tả trong IEEE802.3u. Các nguyên tắc CSMA/CD, vấn đề cáp và các giao thức lớp cao hơn đều được duy trì giống như trong Ethernet. Mạng campus thường dùng FE ở các switch lớp access hoặc distribution nếu như không có sẵn các kết nối tốc độ cao hơn. Cáp được dùng cho FastEthernet thường là UTP hoặc cáp quang.

Công nghệ	Kiểu cáp	Số cáp	Chiều dài cáp
100Base-TX	EIA/TIA cat 5 UTP	2	100m
100Base-T2	EIA/TIA Cat 3 4 5 UTP	2	100m
100BaseT4	EIA/TIA Cat 3 4 5 UTP	4	100m
100Base FX	Cáp quang đa mode MMF: 62.5	4	100m

micron core, 125 micron core (62.5/125)		
Single mode fiber SMF	1	10k

### Chế độ full-duplex:

Cũng giống như trong Ethernet, để cải tiến performance ta có thể dùng chế độ fullduplex. FE có thể cung cấp tốc độ truyền lên đến 100Mbps trong mỗi chiều truyền, dẫn đến kết quả 200Mbps throughput. Thông lượng tối đa 200Mbps này chỉ đạt được khi một thiết bị (trạm làm việc, server, routers hay một switch khác) kết nối trực tiếp đến một switchport. Nói cách khác, các thiết bị đầu cuối của một kết nối phải hỗ trợ fullduplex, có khả năng truyền mà không phải chờ phát hiện và khôi phục khỏi xung đột.

Đặc tả của FastEthernet cũng cho phép tương thích ngược với 10Mbps Ethernet truyền thống. Trong trường hợp 100BaseTX, các switchport thường được gọi là 10/100 để chỉ ra tốc độ dualspeed. Khi này, hai thiết bị ở hai đầu kết nối sẽ tự động dò tìm tốc độ sao cho cả hai có thể hoạt động ở tốc độ cao nhất. Quá trình dò tìm này bao gồm việc phát hiện và chọn lựa công nghệ ở lớp vật lý, tìm chế độ halfduplex hay fullduplex. Nếu cả hai đầu của kết nối được cấu hình theo kiểu autonegotiate, tốc độ chung cao nhất giữa hai thiết bị sẽ được dùng.

Trong quá trình bắt tay dò tìm chế độ duplex của một kết nối, một số thông tin sẽ được trao đổi qua lại giữa hai thiết bị. Điều này có nghĩa là, để cho quá trình dò tìm tự động là thành công, cả hai đầu phải được thiết lập ở chế độ autonegotiate. Nếu khác đi (nghĩa là chỉ có một đầu thiết lập ở autonegotiate), một đầu của kết nối sẽ không nhận được thông tin từ đầu kia và sẽ không có khả năng xác định chế độ chính xác đang được dùng. Nếu quá trình autonegotiation là thất bại, một switchport sẽ trở về chế độ tự động của nó là halfduplex.

Cần chú ý về vấn đề duplex mismatch khi cả hai đầu của kết nối đều không cấu hình cho autonegotiation. Khi có mismatch xảy ra, một đầu của kết nối sẽ dùng full-duplex trong khi đầu xa dùng halfduplex. Kết quả là máy trạm đang hoạt động ở chế độ half-duplex sẽ luôn phát hiện ra collision khi cả hai đều muốn truyền. Máy trạm đang chạy ở full-duplex sẽ giả sử là nó có quyền truyền ở bất kỳ thời điểm nào. Máy trạm này sẽ không dùng lại và chờ. Tình trạng này dẫn đến lỗi trên kết nối và tốc độ đáp ứng rất chậm giữa các máy.

Quá trình bắt tay sẽ dùng bảng các độ ưu tiên dưới đây. Khi cả hai đầu kết nối có thể bắt tay nhau ở nhiều tốc độ, tốc độ nào có độ ưu tiên cao nhất sẽ được dùng. Ví dụ, nếu cả hai thiết bị có thể chạy ở mức 6 (100BbaseTX fullduplex) và mức 2 (10base2full), mức 6 sẽ được dùng.

độ ưu tiên	Chế độ ethernet
7	100Base-t2 (full duplex)
6	100Base-TX (full duplex)
5	100BASE-t2 (half duplex)
4	100Base-T4
3	100Base-TX
2	10base-T (full duplex)
1	10Base-T

Để đảm bảo cấu hình chính xác ở cả hai đầu của kết nối, Cisco khuyến cáo các giá trị về tốc độ truyền, duplex mode phải được cấu hình thủ công (manually) trên các switchports. Yếu tố này giúp loại trừ khả năng một bên thay đổi các cài đặt, dẫn đến kết nối có thể không dùng được. Nếu bạn đã cấu hình thủ công switchport, hãy thiết lập luôn cho thiết bị trên đầu kia của kết nối các thông số tương ứng. Nếu khác đi, vẫn đề speed mismatch hay duplex mismatch sẽ xảy ra.

---

Bài 21:

## Kinh nghiệm học thi wireless

### Kinh nghiệm cho các bạn muốn học thi chứng chỉ CWNA

Như các bạn cũng đã biết, CWNA cũng là một chứng chỉ quốc tế nên nói chung việc học nó cũng tương tự như học các chứng chỉ khác, ở đây tôi sẽ đưa ra cách học tổng quát để các bạn có thể áp dụng khi học bất kỳ chứng chỉ nào chứ không riêng gì CWNA.

+ Đọc sách: tất nhiên rồi, học bất cứ cái gì cũng cần phải đọc sách. Mặc dù biết đây là một vấn đề “biết rồi, khổ lăm, nói mãi” nhưng đa số chúng ta đều mắc phải một “bệnh kinh niên” đó là lười. Chúng ta lười trong mọi chuyện chứ không riêng gì việc đọc sách, bệnh lười này đặc biệt khó chữa đối với đại đa số nam giới, điều này cũng dễ hiểu thôi, bản tính đàn ông là vậy mà. (Một lý do nữa khiến chúng ta ít đọc sách là không có thời gian đặc biệt là với những người đã đi làm, còn đối với các bạn sinh viên có lẽ vẫn còn mãi “bận” chơi). Nếu như có cố gắng lăm ngòi được vào bàn để đọc sách thì cũng chỉ được vài tiếng là cùng nhưng như vậy cũng là tốt lắm rồi. Ở đây tôi muốn nhấn mạnh không phải số lượng mà là chất lượng. Đúng vậy, cho dù các bạn ngồi lâu, đọc nhiều sách nhưng các bạn không biết mình đọc cái gì, để làm gì thì các bạn có đọc xong rồi cũng chẳng hiểu thêm được gì, chỉ mất thời gian. Như vậy trước

khi đọc các bạn phải xác định xem mình sẽ đọc về cái gì, điều này giúp chúng ta tập trung chú ý về cái mình đang đọc. Trong quá trình đọc các bạn có thể chú thích, gạch chân hay tô màu những đoạn quan trọng hoặc bạn có thể ghi lại vào một quyển sổ nhỏ (khuyến khích cách này vì có ghi thì chúng ta mới nhớ được và nó cũng rất tiện khi chúng ta ôn lại thì chỉ cần xem quyển sổ này thôi, khỏi cần lật nguyên cả quyển sách). Và cuối cùng, sau khi đọc xong một đoạn, một mục, một phần hay một chương thì bạn nên ngẫm lại xem mình đã đọc được những gì, hiểu được gì không, đây là cách rất tốt giúp chúng ta nhớ lâu. Các bạn thấy tôi nói dài dòng lắm phải không, thật sự nếu như các bạn đã hình thành một thói quen rồi thì mọi việc sẽ trở nên rất đơn giản.

+ Học nhóm: đây có lẽ là phương thuốc hữu hiệu nhất để chữa bệnh lười. Khi học nhóm, ta có thể tận dụng tối đa kiến thức của nhiều người khác nhau để cùng giải quyết một bài toán hay một vấn đề lý thuyết phức tạp mà khi nghiên cứu một mình ta không tài nào hiểu được. Hơn nữa, mỗi người một ý trong quá trình tranh luận sẽ giúp cho buổi học thêm sinh động, hấp dẫn, không nhảm chán nhu khi ta tự học. Các bạn lưu ý là hãy chủ động tham gia vào các cuộc tranh luận, nếu không có chủ kiến của mình thì hãy thể hiện kỹ năng lắng nghe của bạn để xem ý kiến của những người khác có đúng hay không, nếu sai thì hãy lập tức phản biện ngay, nó sẽ giúp bạn nhớ một vấn đề rất lâu đó.

+ Tham gia diễn đàn: đây là cách học tiết kiệm nhất, thể hiện tính hiện đại, dịch chuyển của các bạn trẻ ngày nay. Một khó khăn của cách học này là đôi khi có một vấn đề ta đưa lên diễn đàn cả tuần thậm chí cả tháng trời vẫn không có ai trả lời giúp bạn, trong trường hợp này thì chỉ còn cách duy nhất là “tự mình cứu lấy ta” mà thôi. Nếu các bạn muốn mọi người giúp mình thì trước tiên mình hãy giúp mọi người, các bạn hãy trả lời những bài viết trên diễn đàn trong khả năng của các bạn, diễn đàn là nơi mọi người giúp đỡ lẫn nhau, không có ai chỉ nhận thôii mà không bao giờ cho cả. Hiện nay có rất nhiều diễn đàn về các chủ đề khác nhau, nếu như bạn chỉ quan tâm đến mạng nói chung cũng như mạng không dây nói riêng thì chúng ta có thể vào <http://www.wimaxpro.org>, <http://vnpro.org/forum> ... (tiếng Việt), còn đối với các bạn khá tiếng Anh thì có thể vào <http://cwnp.com/phpBB2/index.php> hoặc <http://www.sadikhov.com/forum/>

+ Đăng ký một khóa học: đây là cách học tồn tiền nhất phù hợp với những người không có khả năng tự học, tuy nhiên nó đảm bảo cho bạn có được khả năng làm việc thực tế nhiều hơn so với các cách còn lại vì trong một khóa học đã bao gồm luôn cả phần lý thuyết lẫn thực hành nên bạn có thể hiểu được, nắm bắt được vấn đề ngay sau khi thực hành. Sau khi hoàn thành khóa học thì bạn có thể bắt tay vào làm việc được ngay mà không cần phải mò mẫm như những người tự học. Một thuận lợi nữa của cách học này đó là nếu như bạn học ở một trung tâm uy tín thì khi đi xin việc, các nhà tuyển dụng sẽ tin tưởng khả năng thực sự của bạn hơn các ứng viên khác. Tất nhiên, việc học ở một trung tâm uy tín không bảo đảm bạn sẽ là một người giỏi, mọi việc vẫn do chính bạn quyết định mà thôi. Trước khi đến lớp học, bạn hãy đọc về chủ đề mà bạn sẽ

được học, trong lớp học bạn hãy thể hiện tính năng động của mình bằng cách tích cực lắng nghe giảng viên rồi cố gắng đặt ra những câu hỏi mang tính xây dựng giúp chúng ta hiểu bài hơn. Còn trong giờ thực hành thì các bạn hãy cố suy nghĩ tìm cách giải quyết bài toán đặt ra theo cách của riêng mình chứ đừng chép nguyên câu hình trong sách lab lại, nếu như vậy thì chẳng có gì để nói, chẳng còn gì để học cả. Sau khi câu hình xong, các bạn nên lưu file câu hình lại để về nhà còn đọc lại ngay sau buổi thực hành hôm đó, nó sẽ giúp các bạn hiểu được vấn đề của bài toán và nhớ lâu hơn.

+ Trước khi thi: khoảng 1 hay 2 tuần trước khi thi là thời gian tốt nhất để chúng ta ôn lại những kiến thức đã học, việc này giúp bạn có một cái nhìn tổng quan về tất cả những điều mà bạn đã học trong suốt thời gian vừa qua, kết nối lại các kiến thức mà trong quá trình học ta cứ tưởng như chúng chẳng có liên quan gì nhau. Đọc lại các file câu hình mà bạn đã từng làm, sau khi đọc, có thể bạn sẽ “ngộ” ra được nhiều điều thú vị đấy. Việc cuối cùng và khá quan trọng đó chính là luyện thi mà cụ thể hơn chính là làm các câu hỏi trắc nghiệm giúp cho chúng ta làm quen với đề thi để khi vào thi chúng ta không bị “choáng” trước các câu hỏi của đề. Các đề thi mẫu các bạn có thể mua từ Tesking, Pass4sure, Actualtest ... Một điều lưu ý cho các bạn đó là các bạn không nên tin hoàn toàn vào cách giải của các đề thi mẫu này vì theo kinh nghiệm của tôi, nó sai khá nhiều. Có những câu nó trả lời sai rồi giải thích rất ngon khiến mình không thể không tin vào nó. Các bạn nên vận dụng kiến thức đã học của mình để trả lời các câu hỏi trước khi xem kết quả và giải thích của nó có phù hợp không.

+ Trong lúc thi: điều quan trọng nhất tôi muốn nói đó chính là “bình tĩnh” và “tự tin” rồi các bạn sẽ “chiến thắng”.

+ Sau khi thi: còn gì hạnh phúc bằng việc ta đã vượt bao nhiêu gian khổ, tốn thời gian tiền bạc, giờ đây mình đã đạt được cái mình muốn rồi. Có một câu mà tôi thường hay nghe các bạn nói mỗi lần thi xong đó là “nhậu thõi”, hy vọng hai từ sẽ luôn được vang lên mỗi khi các bạn thi xong.

Lời cuối cùng tôi muốn nhắn nhủ đến các bạn đó là “Hãy học bằng tất cả sự đam mê của mình”, hãy làm sao đó để mỗi lần học chúng ta lại nói là “được học” chứ không phải là “phải học”. Không có ai ép buộc bạn làm việc gì cả, chỉ có bạn mới biết được việc gì là tốt nhất cho mình, hãy làm nó với tất cả sự đam mê của mình, đừng bao giờ bỏ cuộc và cuối cùng thành công sẽ đến với bạn mà thôi!

Bài 22:

## **Qui trình khôi phục password cho router Cisco.**

### **I. Đối với Cisco 1600, 1700 and 2600 Series Routers:**

1. Vào HyperTerminal (Private Edition 5.0 or higher) console.

2. Tắt router, sau đó bật lại. Nhấn Ctrl-Break trong vòng 60 giây

monitor: command "boot" aborted due to user interrupt  
rommon 1 >

3. Dùng lệnh confreg để đổi nội dung thanh ghi sang 2142.

rommon 1 >confreg 0x2142

4. Reboot the router with the reset command.

rommon 2 >reset

5. Sau khi reboot, dùng Ctrl-C để vào user mode:

router>

6.

router>enable  
router#copy startup-config running-config

7.

router>enable  
router#show startup-config

8. Đặt lại password mới:

```
router#config term
router(config)#enable secret newpassword
router(config)#enable password newpassword
router(config)#line con 0
router(config-line)#login
router(config-line)#password newpassword
router(config)#line aux 0
router(config-line)#login
```

```
router(config-line)#password newpassword  
router(config)#line vty 0 4  
router(config-line)#login  
router(config-line)#password newpassword
```

9. #copy run start

10. Khôi phục giá trị thanh ghi về 0x2102

```
router#config term  
router(config)#config-register 0x2102  
router(config)#exit  
router#copy running-config startup-config
```

11. Kiểm tra nội dung thanh ghi

```
router#show version  
Cisco Internetwork Operating System Software  
IOS (tm) C2600 Software (C2600-DO3S-M), Version 12.0(5)T1, RELEASE  
SOFTWARE (fc1)  
Copyright (c) 1986-1999 by cisco Systems, Inc.  
Compiled Tue 17-Aug-99 13:18 by cmong  
Image text-base: 0x80008088, data-base: 0x80CB67B0  
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)  
1 FastEthernet/IEEE 802.3 interface(s)  
2 Low-speed serial(sync/async) network interface(s)  
32K bytes of non-volatile configuration memory.  
8192K bytes of processor board System flash (Read/Write)
```

Configuration register is 0x2142 (will be 0x2102 at next reload)

## **II. Cisco 2500 Series Routers:**

1. Thiết lập HyperTerminal (Private Edition 5.0 or higher) console .
2. Tắt routers, sau đó bật lại. Nhấn CTRL-BREAK trong vòng 60 giây.

```
Abort at 0x10EA884 (PC)  
>
```

3. Đổi nội dung thanh ghi thành 0x2142

>o/r 0x2142 (lower case of the letter O for o/r and zero for 0x2142)

4. Reboot router

>i

5. Nhấn Ctrl-C để vào user mode khi router khởi động lại

router>

6. Vào enable mode

router>enable

router#copy startup-config running-config

7. Thực hiện các lệnh show running-config or show startup-config  
router#show startup-config

8.

```
router#config term
router(config)#enable secret newpassword
router(config)#enable password newpassword
router(config)#line con 0
router(config-line)#login
router(config-line)#password newpassword
router(config)#line aux 0
router(config-line)#login
router(config-line)#password newpassword
router(config)#line vty 0 4
router(config-line)#login
router(config-line)#password newpassword
```

9. Copying the startup-configuration to running-configuration. Thực hiện lệnh no shutdown trên tất cả các interface được dùng.

10. Chuyển nội dung thanh ghi về giá trị ban đầu. Lưu cấu hình

```
router#config term
router(config)#config-register 0x2102
router#copy running-config startup-config
```

11. Kiểm tra thanh ghi có giá trị là 2102 bằng lệnh show version

```
router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(4), RELEASE
SOFTWARE
(fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
```

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE  
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a),  
RELEASE  
SOFTWARE (fc1)  
1 Ethernet/IEEE 802.3 interface(s)  
2 Serial network interface(s)  
1 ISDN Basic Rate interface(s)  
32K bytes of non-volatile configuration memory.  
8192K bytes of processor board System flash (Read ONLY)  
Configuration register is 0x2142 (will be 0x2102 at next reload)

12. Reboot the router.  
router#reload

---

Bài 23:

## Các khái niệm routing cơ bản

Khi trong bảng routing-table của router có 2 hoặc nhiều đường đi đến một destination network, việc chia tải (load-balancing) sẽ diễn ra. Quá trình chia tải có thể chia thành hai kiểu:

1. Per packet: từng packet khi đi vào router sẽ được xử lý riêng lẻ (process switching). Router sẽ đọc destination network của packet, search bảng routing table và sau đó sẽ switch packet ra interface phù hợp. Do đó nếu bảng route của router có hai đường đi đến cùng một địa chỉ network, các packet sẽ được chia tải đều trên cả hai đường.
2. Per destination: chỉ có packet đầu tiên thực hiện theo qui trình trên. tất cả các packet còn lại sẽ dùng kết quả đã được lưu trong cache. bảng routing-table sẽ không được tham khảo cho các packet sau. Chế độ mặc định của router là fast-switching. Bạn có thể chuyển sang process-switching bằng lệnh no ip route-cache.

cần chú ý là chỉ có thể thực hiện debug ip packet nếu router hoạt động ở process switching.

### 1. AS ( Autonomous System):

Một nhóm các routers có chung chính sách quản lý, có chung một nguồn quản lý kỹ thuật duy nhất và thông thường dùng một IGP (Interior Gateway Protocol). Mỗi AS được gán bằng một số duy nhất từ 1 đến 65535, trong đó giá trị từ 64512 đến 65535 được dùng làm giá trị riêng, được gán cho các AS cục bộ

## 2. Hội tụ (convergence):

Quá trình tính toán bảng routing-table trên các router sao cho tất cả các bảng có chung một trạng thái nhất quán.

## 3. chia tải (load balancing):

Cho phép việc truyền packet đến một network đích diễn ra trên hai hoặc nhiều đường đi khác nhau.

## 4. Metric:

tất cả các routing protocols dùng metric để định lượng đường đi nhằm tìm ra đường đi tốt nhất. Một vài protocol dùng metric rất đơn giản, ví dụ như RIP dùng hop-count. EIGRP dùng metric phức tạp hơn, bao gồm băng thông, delay, reliability...

## 5. Passive interface:

Ngăn ngừa các routing update gửi ra một interface nào đó. Tuy nhiên, interface này vẫn có thể lắng nghe các routing update do các router khác gửi về. Lệnh này được dùng trong router mode.

## 6. Redistribution:

Quá trình chia sẻ route được học từ các nguồn khác nhau. Ví dụ bạn có thể redistribute route được học từ RIP vào OSPF (trong trường hợp này bạn có thể gặp vấn đề với VLSM). Hoặc bạn có thể redistribute static route vào EIGRP. Quá trình redistribution này phần lớn phải cấu hình bằng tay (manually)

## 7. Route flapping:

Trạng thái thay đổi thường xuyên của route. Quá trình này có thể gây ra những vấn đề nghiêm trọng. Ví dụ như những hệ thống mạng chạy ospf có thể phải liên tục tính toán lại database và broadcast những thay đổi này.

## 8. Static route:

static route có thể chỉ đến một host, một network. Bạn cũng có thể dùng floating static route, trong đó route này được thay đổi giá trị AD cao hơn giá trị của các routing protocol đang dùng.

## 9. AD: là một đại lượng chỉ sự tin cậy của các routing protocol.

Bài 24:

## So sánh chức năng Routing và Switching trong Router

Phần này so sánh vai trò của routing và switching và làm thế nào để kết hợp hai chức năng này để chuyển gói tin đi trên mạng. Cisco phân biệt rất rõ sự khác nhau giữa các chức năng này của một router. Sự khác nhau thật ra khá đơn giản. Để di chuyển một gói tin bên trong một router từ một cổng giao tiếp này đến một cổng giao tiếp kia, đường đi về đích phải được xác định và sau đó gói tin này sẽ được gửi ra interface hướng ra. Quá trình tìm đường là chức năng của routing trong khi đó quá trình gửi một gói tin đi ra interface là chức năng của switching.

### Chức năng routing

Chức năng routing chịu trách nhiệm học các đồ hình dạng logic của mạng và sau đó ra quyết định dựa trên kiến thức đó. Các quyết định được thực hiện bởi router sẽ xác định khi nào thì một gói tin đi vào có thể được route và nếu như vậy, sẽ được route như thế nào. Khi một gói tin được nhận, quá trình định tuyến sẽ trải qua vài bước. Các bước này có thể tóm tắt trong các câu hỏi như sau:

- Giao thức routed và giao thức routing cho gói tin (thuộc về giao thức đó) có được cài đặt trên router hay không?
- Nếu có cài đặt, có một đường đi nào cho một hệ thống mạng ở xa tồn tại trong bảng định tuyến hay không?
- Nếu mạng đích là không có trong bảng định tuyến, có tuyến đường mặc định nào được cấu hình hay không?
- Nếu có một tuyến đường mặc định tĩnh hoặc động, địa chỉ đích có đến được không?
- Đường đi tốt nhất về một mạng nào đó là như thế nào?
- Có nhiều đường đi có chi phí bằng nhau hay không?
- Nếu có nhiều đường đi có chi phí bằng nhau, interface nào sẽ được dùng để đẩy gói đi ra.

### Chức năng Switching

Chức năng switch liên quan đến việc di chuyển dữ liệu trên một router. Chức năng này sẽ chịu trách nhiệm chuyển gói tin. Switching chỉ được thực hiện sau khi những quyết định về routing đã được thực hiện. Mặc dù router đã ra quyết định, vẫn còn một vài quyết định phải thực hiện bằng phần cứng. Chức năng switching này thực hiện những việc sau:

1. Kiểm tra frame đầu vào xem có hợp lệ
2. Kiểm tra có phải frame này có địa chỉ đích là địa chỉ L2 của router hay

không

3. Kiểm tra kích thước frame có hợp lệ hay không?
4. Kiểm tra phần CRC của frame
5. Gỡ bỏ phần mào đầu và phần cuối của frame. Sau đó kiểm tra địa chỉ đích với các thông tin trong cache
6. Tạo ra các header và trailer mới và đưa ra cổng ra của router

### Mối quan hệ giữa routing và switching trong Cisco Router

Một gói tin sẽ được router chấp nhận nếu cấu trúc frame của nó chứa địa chỉ L2 của một trong những cổng của router. Nếu cấu hình địa chỉ là đúng, sau khi frame được kiểm tra, frame và nội dung của frame được đưa vào bộ đệm. Bộ đệm được chứa trong bộ nhớ hoặc trong một vài phần cứng đặc biệt của router.

Nếu địa chỉ nguồn và địa chỉ đích L3 của gói tin đó không nhận thấy bởi router trước đó, gói tin sẽ được process switch hoặc routed. Hành động này bao gồm  
- Khi một gói phải được chuyển đi, một quá trình tìm kiếm trong bảng định tuyến sẽ được kích hoạt và router sẽ quyết định gói tin đi như thế nào.

- Gói tin sau đó sẽ được đóng gói với giao thức L2 phù hợp.
- Nếu cơ chế fast-switching được dùng, gói tin sẽ được kiểm tra lại một lần nữa. Một tuyến sẽ được đưa vào cache. Một entry trong cache sẽ bao gồm: IP Prefix, cổng đi ra của router, phần header lớp 2 được dùng để chuyển gói tin đi. Các gói tin theo sau đó trong cùng luồng dữ liệu, nếu phần địa chỉ đích là so trùng trong route-cache, gói tin sẽ được chuyển đi dùng thông tin trong cache. Chức năng routing lúc này không bị ảnh hưởng. Kiểu cache được dùng phụ thuộc vào kiểu phần cứng được dùng. Các kiểu switching là fast switching, autonomous switching, silicon switching và CEF.

---

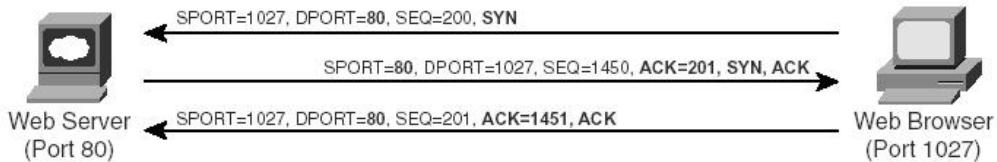
Bài 25:

### TCP: quá trình thiết lập kết nối và hủy kết nối

#### Các kết nối TCP và các cổng

Hai ứng dụng dùng TCP phải thiết lập một kết nối TCP trước khi dữ liệu có thể được truyền. Mỗi kết nối sẽ tồn tại giữa một cặp TCP sockets với socket được định nghĩa như là một kết hợp của địa chỉ IP, cổng được dùng, giao thức lớp transport. Quá trình thiết lập kết nối, khởi tạo socket bao gồm giá trị cổng nguồn và cổng đích, chỉ số tuần tự và ACK. Hình 6-2 mô tả tiến trình bắt tay ba lần trong thiết lập TCP và quá trình hủy một kết nối TCP.

### TCP Connection Establishment, Initiated by Client



### TCP Connection Termination, Initiated by Client

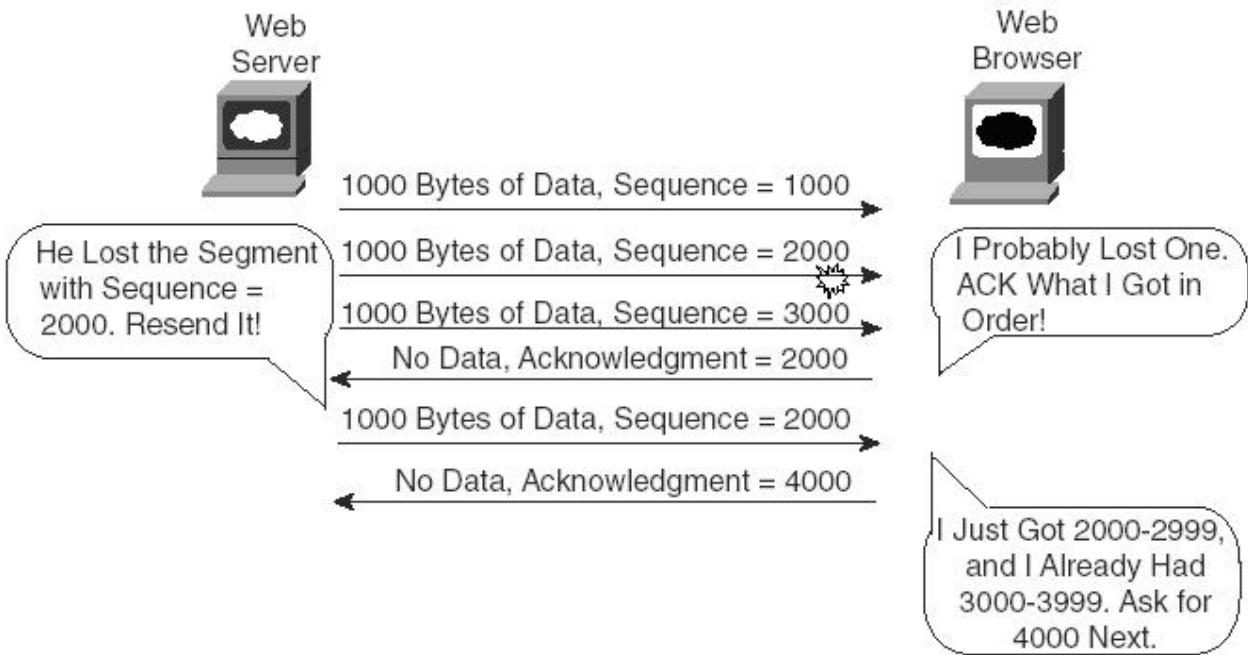


Trong quá trình thiết lập kết nối, hai host sẽ chọn lựa cổng, chọn lựa chỉ số tuần tự sequence-number và dùng các chỉ số của TCP để nhận ra thông điệp trong quá trình bắt tay ba chiều. Đầu tiên, đối với vấn đề cổng, bên server phải lắng nghe các yêu cầu kết nối từ client, trong trường hợp này là cổng 80. Phía client sẽ chọn một cổng chưa dùng làm source port, thường là giá trị 1024 hoặc lớn hơn. Lưu ý rằng khi so sánh các segment trong tiến trình trên, giá trị port là không đổi.

Trong phần header của TCP có bao gồm vài trường có giá trị 1-bit, gọi là các cờ. Các cờ này phục vụ cho các mục đích khác nhau. Các cờ SYN và ACK sẽ chỉ ra một segment có phải là segment đầu tiên hay là thứ hai trong một kết nối TCP mới. Một segment có cờ SYN sẽ là segment đầu tiên trong một kết nối TCP. Một segment có cả SYN và ACK sẽ là segment thứ hai trong một kết nối. Các cờ này cho phép các host dễ dàng nhận ra các yêu cầu kết nối mới. Chỉ số ban đầu có thể được gán về bất kỳ giá trị hợp lệ nào và thường không được gán về 0. Hãy nhớ rằng trong quá trình khôi phục lỗi, việc sử dụng các giá trị này là độc lập trong cả hai chiều.

### Quá trình khôi phục lỗi

Để thực hiện quá trình khôi phục lỗi, TCP sẽ gửi các công nhận ACK khi nhận được dữ liệu. Khi dữ liệu gửi đi không được ACK, bên gửi có thể gửi lại dữ liệu. Hình dưới đây mô tả tiến trình một web server gửi ra 1000-bytes trong đó khi segment thứ hai bị mất, dữ liệu sẽ được khôi phục lại.



Ví dụ trên mô tả một tiến trình khôi phục lỗi trong đó bên gửi (máy web) nhận được một ACK trong đó chỉ ra rằng một segment đã bị mất. Lưu ý rằng trường ACK sẽ chỉ ra byte mong đợi kế tiếp- chứ không phải là byte nhận được cuối cùng. Cũng lưu ý rằng trường ACK và trường sequence chỉ ra số bytes, chứ không phải chỉ ra TCP segment. Bên máy gửi sẽ gửi ra một bộ định thời timers, dựa trên giá trị TCP Measured Round Trip Time (MRTT) sao cho nếu một ACK là không nhận được, máy gửi sẽ gửi lại tất cả nhưng dữ liệu không được công nhận mà không chờ cho bên máy nhận gửi một yêu cầu truyền lại.

Bài 26:

### Dạng địa chỉ của IPv6

Địa chỉ IPv6 thì rất khác so với địa chỉ IPv4. Không chỉ khác nhau về kích thước (dài hơn gấp 4 lần) mà sự khác nhau còn trong dạng biểu hiện ở dạng thập lục phân so với dạng thập phân. Các dấu ‘:’ sẽ tách các số dạng thập lục phân là các thành phần của địa chỉ 128-bit. Một ví dụ của địa chỉ Ipv6 là như sau:

4021:0000:240E:0000:0000:0AC0:3428:121C

Để tránh nhầm lẫn, lỗi và các trạng thái phức tạp không cần thiết, các luật sau sẽ được xác định:

Các số dạng thập lục phân không phân biệt chữ thường và chữ hoa.  
Bất cứ một số 0 nào đứng trước các vùng 16 bit có thể được bỏ qua và được

tương trưng bằng dấu ‘::’. Một cặp dấu :: chỉ ra rằng các giá trị 16 bit của các số 0 đã được rút gọn. Quá trình nhận dạng số sẽ dễ dàng nhận ra số chữ số 0 đã bị thu gọn bằng cách thêm vào số chữ số 0 cho đến khi nào thu được một địa chỉ dài 128-bit

Chỉ có một cặp các dấu ‘::’ là cho phép tồn tại trong một địa chỉ bởi vì quá trình nhận dạng sẽ không thể chỉ ra có bao nhiêu số 0 trong mỗi vị trí.

Ví dụ địa chỉ 4021:0000:240E:0000:0000:0AC0:3428:121C có thể được viết ở dạng 4021:0:240E::0AC0:3428:121C

Mặc dù không thể có hai phiên bản của hai dấu ‘::’, các vùng với nhiều chữ số 0 chỉ có thể được biểu diễn như 0. Trong ví dụ nêu trên, các chữ số 0 trong vùng thứ hai của địa chỉ được thu gọn lại thành một chữ số 0. Nếu một địa chỉ không có phần host, địa chỉ có thể kết thúc ở dạng ‘::’. Ví dụ 4021:0:240E::

IPv6 có thể có nhiều dạng và nó có khả năng giải quyết các hạn chế của IPv4.

Cấu trúc ba mức này được thể hiện thông qua cấu trúc của địa chỉ tích hợp của IPv6, trong đó bao gồm các vùng sau:

Vùng tiền tố FP: 3 bit của FP sẽ được dùng để chỉ ra kiểu của địa chỉ (là unicast. Multicast...). Giá trị 001 chỉ ra đây là địa chỉ toàn cục

Vùng TLA ID (top level aggregation) được dùng để chỉ ra mức thẩm quyền cho địa chỉ này. Các Internet Router sẽ duy trì các bảng cần thiết cho tất cả các giá trị TLA. Với 13-bit, vùng này có thể có đến 8,192 TLAs.

RES field (8 bits): kiến trúc của IPv6 định nghĩa vùng dành riêng sao cho các giá trị TLA hoặc NLA có thể mở rộng. Hiện tại, giá trị này bằng zero

NLA ID (24 bits): vùng này được dùng để chỉ ra ISP. Vùng này có thể được sắp xếp để phản ánh mối quan hệ giữa các ISP.

LSA ID (16 bits): được dùng bởi các tổ chức để tạo ra các kiến trúc địa chỉ bên trong của nó và để chỉ ra các mạng con.

Interface ID (64 bits): chỉ ra các cổng giao tiếp riêng lẻ trên một kết nối. Vùng này là tương tự như vùng host trên IPv4 nhưng nó được dẫn xuất từ dạng địa chỉ IEEE EUI-64 bit. Dạng địa chỉ này tương tự như địa chỉ MAC nhưng thêm vào một vùng 16 bit.

Thêm vào dạng địa chỉ tích hợp toàn cục nêu trên, IPv6 hỗ trợ các địa chỉ nội bộ, tương tự như các địa chỉ RFC1918. Nếu một node không được gán một địa chỉ toàn cục hay một địa chỉ cục bộ nêu trên, nó có thể được định vị bằng địa chỉ kết nối cục bộ, chỉ ra một phân đoạn mạng. Local-Use Unicast address: được gọi là địa chỉ đơn hướng dùng nội bộ, được dùng cho một tổ chức có mạng máy tính riêng (dùng nội bộ) chưa nối với mạng Internet toàn cầu hiện tại nhưng sẵn sàng nối được khi cần. Ngoài ra địa chỉ này còn được chia thành 2 loại là Link-Local (nhận dạng đường kết nối local) và Site local (nhận dạng trong phạm vi nội bộ có thể nhiều nhóm Node – Subnet). Link-local, sẽ được sử dụng ngay lần đầu khi thiết bị IPv6 bật lên. Do khả năng tự cấu hình của

IPv6, nên khi thiết bị được bật lên, tự động một địa chỉ link-local sẽ được gán. Chú ý là địa chỉ này không phải do ta gán mà do máy tự gán để giao tiếp trong nội bộ kết nối, nghĩa là với các host có chung địa chỉ subnet. Sau đó, khi thấy có router tồn tại trong mạng thì máy sẽ gửi các gói tin router solicitation và advertising để xin router 1 subnet ID để tạo site-local để sử dụng giao tiếp giữa các subnet. Chú ý là 2 địa chỉ này không được định tuyến ra internet.

## IPv6 Multicast Addresses

Một địa chỉ multicast là một địa chỉ xác định một nhóm các cổng của router, thông thường trên các hệ thống đầu cuối khác nhau. Các gói tin sẽ được phân phối đến tất cả các hệ thống được chỉ ra trong địa chỉ multicast. Sử dụng địa chỉ multicast thì hiệu quả hơn địa chỉ broadcast, trong đó yêu cầu tất cả các hệ thống đầu cuối phải ngưng tất cả các việc đang xử lý. Bởi vì một địa chỉ multicast là một địa chỉ của một nhóm các máy tính, nếu một máy tính không phải là thành viên của nhóm địa chỉ này, nó sẽ drop các gói ở layer 2. Tuy nhiên broadcast vẫn được xử lý trước khi các hệ thống xác định rằng dạng broadcast này là không liên quan đến nó. Các thiết bị lớp 2 thường lan truyền các broadcast bởi vì các địa chỉ broadcast không được lưu trữ trong bảng CAM. Không giống như router (hành động mặc định của router là drop các gói tin trong đó phần địa chỉ là không biết), switch sẽ phát tán tất cả các frame với phần địa chỉ không xác định ra tất cả các cổng của switch. Về mặt lý thuyết, điều này cũng đúng với các địa chỉ multicast mặc dù một vài thiết bị có các cơ chế thông minh để giới hạn các dạng truyền multicast.

IPv6 không dùng cơ chế broadcast mà chỉ dựa vào địa chỉ multicast. Mặc dù IPv4 dùng địa chỉ multicast như định nghĩa RFC2356, nó sử dụng theo một cách khác. Các địa chỉ IPv6 có các dãy địa chỉ khác nhau. Tất cả các địa chỉ IPv6 bắt đầu với 8 bit đầu tiên gán bằng 1. Vì vậy tất cả các địa chỉ multicast sẽ bắt đầu với giá trị F. Dãy địa chỉ multicast là FF00::/8 - FFFF::/8

Giá trị octet thứ hai, theo sau octet đầu tiên, chỉ ra tầm vực và thời gian sống của địa chỉ multicast. Theo cách này, IPv6 có hàng triệu nhóm địa chỉ multicast.

## Tóm tắt địa chỉ (Address Aggregation)

Quá trình tóm tắt các route, bắt cứ khi nào có thể, là quan trọng trong Internet. Bảng định tuyến thì dễ quản lý hơn với cách hiện thực CIDR. Mặc dù tất cả các sơ đồ địa chỉ trong IPv6 cho phép cấp phát hầu như vô tận các địa chỉ, kiến trúc của IPv6 vẫn cho phép triển khai theo dạng có cấu trúc sao cho nó không bị quá tải. Như trong IPv4, các bit bên trái của địa chỉ được dùng để tóm tắt các địa chỉ mạng xuất hiện ở phía phải của cấu trúc địa chỉ. Như vậy, địa chỉ IPv4 140.108.128.0/17 có thể bao gồm các subnets 140.108.225.0/24. Điều này có nghĩa là bảng định tuyến có thể route đến tất cả các subnets nhưng thay vì có 128 địa chỉ subnet nằm trong bảng định tuyến, chỉ còn 1 dòng duy nhất tượng

trung cho tất cả các route. Để chỉ ra một subnet nhỏ hơn, các qui luật thông thường trong định tuyến vẫn được tuân theo và gói tin được gửi tới cho router quảng bá network 140.108.128.0/17. Router này trong bảng định tuyến của nó có nhiều thông tin chi tiết hơn, sẽ chuyển gói cho đến khi nó đến được network đích.

Trong IPv6, kiến trúc địa chỉ cho phép điều chỉnh tốt hơn dạng địa chỉ được dùng trong Internet. Địa chỉ thì rất dài và mỗi phần phục vụ một chức năng khác nhau. 48-bit đầu tiên của địa chỉ được dùng bởi IANA cho quá trình định tuyến động trong Internet để tạo ra các địa chỉ khả kết toàn cục. Ba bit đầu tiên được gán giá trị 001 để chỉ ra một địa chỉ toàn cục.

---

## Bài 27: **Giới thiệu về WinPCap**

Trong rất nhiều phần mềm ứng dụng mạng, các bạn hay gặp phần mềm WinPCap, đặc biệt trong quá trình cài đặt Dynamips/Dynagen.

### **1. Giới thiệu về Winpcap:**

#### Định nghĩa:

Winpcap là một thư viện mã nguồn mở cho việc bắt gói (capture packet) và phân tích mạng, trên nền tảng (platform) win32. Winpcap hỗ trợ những chức năng sau:

- Thu thập những gói dữ liệu thô, một là ngay trên chính máy đang chạy truyền dữ liệu đi và một là sự trao đổi bởi những máy khác trên môi trường chia sẻ.
- Lọc gói dữ liệu theo những luật của người dùng trước khi chúng được truyền tới ứng dụng
- Truyền những gói dữ liệu thô tới mạng
- Thu thập thông tin thống kê lưu lượng mạng

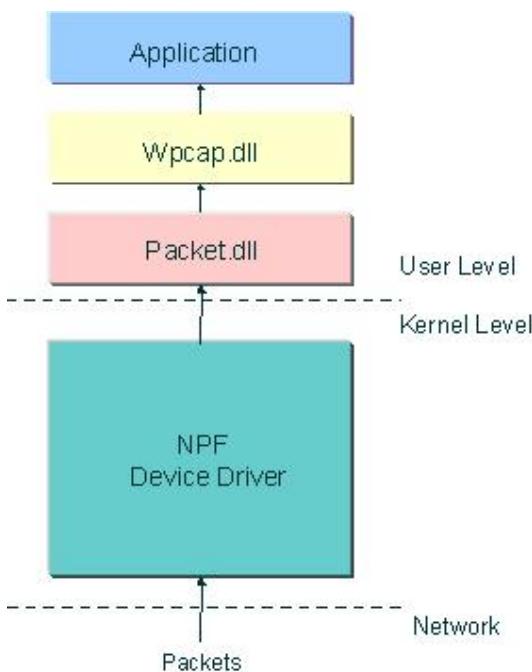
Một tập các tính năng này được được cung cấp, khi mà bạn cài đặt nó như là một trình điều khiển thiết bị (device driver), và nó được cài đặt bên trong phần hoạt động mạng của phần nhân win32 (win32 kernel) cùng với một cặp thư viện động DLL.

## Loại chương trình sử dụng winpcap

Những chương trình mà dựa trên winpcap:

- Bộ máy phân tích mạng và giao thức
- Giám sát mạng
- Traffic logger
- Traffic generator
- user-level bridges and routers
- Hệ thống phát hiện xâm nhập mạng NIDS
- Network scanner
- Công cụ bảo mật

## Cấu trúc của winpcap



Nó bao gồm ba thành phần chính: bộ lọc gói mức kernel, một thư viện packet.dll mức thấp, và một thư viện độc lập với hệ thống wpcap.dll mức cao.

### Packet.dll:

cung cấp một API mức thấp (application program interface) truy xuất trực tiếp tới trình điều khiển, độc lập với hệ điều hành microsoft. Sẽ cung cấp các chức năng sau:

- Cài đặt, khởi tạo và dừng trình điều khiển NPF (NPF device driver)
- Nhận gói từ trình điều khiển NPF
- Gởi gói đến trình điều khiển NPF
- Thu được một danh sách các card mạng

- Lấy lại thông tin khác nhau về mạng: miêu tả, danh sách địa chỉ, netmask
- Truy vấn và thiết lập các thông số cho một card điều hợp

Source code packet.dll. (nằm trong thư mục packet)

#### Wpcap:

cung cấp một tập các chức năng bắt gói mức cao mà nó tương thích với libpcap (dùng trên linux), mà nó hoạt động độc lập với phần cứng mạng và hệ điều hành. Source wpcap.dll (nằm trong thư mục wincap)

NPF (netgroup packet filter) device driver: mã nguồn nằm trong thư mục driver dành cho hệ điều hành NT

Hoạt động quan trọng nhất của NPF là capture gói. Bộ điều khiển phát hiện gói trên NIC và phân phối chúng nguyên vẹn đến ứng dụng người dùng.

Bài 28:

## **wireless cho người mới bắt đầu**

### **Cơ bản về Wireless LAN**

#### **Giới thiệu**

Các hệ thống mạng switched Ethernet thường được dùng trong các mạng doanh nghiệp ngày nay. Các kết nối Ethernet thường được dùng từ thiết bị lớp lõi (core layer device), xuống đến lớp phân phối (distribution), xuống dần đến lớp truy cập (access layer). Theo truyền thống, các người dùng đầu cuối phải dùng dây mạng để kết nối vào hệ thống mạng campus. Tuy nhiên, công nghệ mạng không dây cho phép các thiết bị ở lớp access của mạng campus có thể mở rộng đến người dùng cuối mà không cần dùng dây. Với việc dùng các thiết bị mạng không dây, người dùng cuối có thể trở nên cơ động và có thể di chuyển dễ dàng mà không hề bị mất kết nối mạng.

Bài viết này sẽ giới thiệu một cái nhìn tổng quan về các công nghệ được dùng trong mạng không dây WLAN. Khi đã hiểu và quen thuộc với một vài lý thuyết cơ bản của mạng không dây, bạn sẽ có khả năng hiểu, thiết kế và dùng các thiết bị mạng không dây để mở rộng hệ thống mạng để kết nối với người dùng.

### **Cơ bản về mạng không dây**

Bài viết này sẽ giới thiệu mạng không dây nội bộ WLAN từ góc nhìn thực tế. Tài liệu trình bày dựa trên những kiến thức bạn đã có trong các chủ đề về mạng chuyển mạch LAN trong khóa học ccnp switching. Sau cùng, mục tiêu của bài viết này giúp bạn có kiến thức đủ về wireless để có thể tích hợp công nghệ này vào mạng của bạn.

## **So sánh mạng có dây và mạng không dây**

Một mạng không dây được tích hợp một cách chính xác vào mạng switched có dây như thế nào? Ngược lại, chức năng switching sẽ tích hợp vào mạng không dây như thế nào? Trước khi trả lời các câu hỏi này, bạn có thể cần so sánh hai công nghệ này với nhau.

Ở mức cơ bản nhất, mạng có dây thì sẽ dùng dây và mạng không dây sẽ không có dây. Điều này thoạt nghe có vẻ khôi hài, nhưng thật ra nó cho thấy một vài khác nhau cơ bản ở mức vật lý mà bài viết sẽ đề cập đến ở phần sau.

Mạng Ethernet truyền thống được định nghĩa bởi các chuẩn IEEE 802.3. Mọi kết nối Ethernet phải hoạt động trong tình trạng được kiểm soát nghiêm ngặt, đặc biệt đối với những cơ chế liên quan đến lớp vật lý. Ví dụ, các cơ chế về trạng thái kết nối, tốc độ kết nối và chế độ duplex phải hoạt động theo đúng chuẩn mô tả. Wireless LAN cũng phải có yêu cầu tương tự nhưng lại được định nghĩa trong 802.11.

Những thiết bị Ethernet dùng dây phải truyền và nhận các Ethernet frame theo phương thức Carrier Sense Multiple Access/Collision Detect (CSMA/CD). Theo đó, trên một phân đoạn mạng dùng chung, khi các máy PC truyền thông theo chế độ half duplex, từng PC có thể nói chuyện tự do với nhau trước, và sau đó bị xung đột hay còn gọi là đụng độ (collision) nếu các thiết bị khác cũng đang nói chuyện. Toàn bộ tiến trình phát hiện xung đột (collision) dựa trên việc các kết nối có dây có một chiều dài tối đa và có một độ trễ tối đa khi một frame đi từ một đầu của phân đoạn mạng này đến một đầu kia của phân đoạn. Khi hạ tầng mạng là dùng chung, bất kỳ một tín hiệu điện này cũng được truyền dẫn trên đường dây cũng có thể xung đột với một tín hiệu của một thiết bị khác. Khi hai hoặc nhiều Ethernet frame chồng lấp lên đường truyền ở một thời điểm nào đó, collision xảy ra. Collision sẽ dẫn đến các lỗi bit và mất frame (bit error).

Những kết nối Ethernet hoạt động theo chế độ full duplex sẽ không gặp phải vấn đề collision hay cạnh tranh nhau về băng thông. Mặc dù vậy, các kết nối này vẫn phải tuân thủ theo cùng một đặc tả. Ví dụ, những Ethernet frame vẫn phải truyền và nhận trong một khoảng thời gian trên một kết nối full duplex. Điều này sẽ áp đặt chiều dài của đoạn cáp dùng trong full duplex và half duplex phải là giống nhau.

Mặc dù các mạng WLAN cũng dựa trên một tập hợp các chuẩn khắt khe, chính yếu tố phương tiện truyền cũng là một thách thức. Nói chung, khi một PC kết nối đến một mạng có dây, PC đó sẽ chia sẻ kết nối mạng đó với một số lượng máy biết trước cũng kết nối vào mạng có dây đó. Khi cùng một PC dùng một mạng không dây, nó cũng chia sẻ tương tự, nhưng thông qua không khí. Trong mạng không dây, hạ tầng rõ ràng là không tồn tại các đoạn dây cáp mạng hay

các ô cắm mạng. Thật ra các người dùng mạng không dây wireless khác cũng toàn quyền sử dụng cùng không gian truyen chung đó.

Mạng wireless LAN sau đó trở thành một mạng dùng chung, trong đó có một số lượng máy cạnh tranh với nhau để dùng “không khí”, tức hạ tầng mạng ở mọi thời điểm. Vấn đề xung đột (collision) là một vấn đề muôn thửa trong lĩnh vực không dây bởi vì mọi thiết bị không dây đều trong chế độ half-duplex.

Mạng 802.11 luôn luôn hoạt động ở chế độ half duplex bởi vì các trạm truyền và nhận sử dụng cùng một tần số. Chỉ có một máy truyền ở một thời điểm, nếu không, sẽ có collision xảy ra. Để có thể trở thành full duplex, tất cả các máy phải truyền trong một tần số khác và sẽ nhận trong một tần số khác. Mặc dù điều này nghe có vẻ khả thi, chuẩn 802.11 không cho phép hoạt động ở chế độ full duplex.

---

Bài 29:

### Tránh nghẽn trong mạng không dây WLAN

Khi hai hoặc nhiều trạm không dây cùng truyền ở một thời điểm, tín hiệu trở thành bị nhiễu. Máy trạm bên phía nhận chỉ có thể nhận kết quả như những dữ liệu rác, nhiễu hay bị lỗi. Thật ra, không có một cách thức rõ ràng để xác định là xung đột collision đã xảy ra. Ngay cả với máy truyền đang gây ra xung đột cũng không nhận ra, vì lúc đó phần nhận của nó phải tắt đi. Để có một cơ chế phản hồi hiệu quả, trong mạng không dây, bất cứ khi nào một trạm truyền đi một frame, bên trạm nhận phải gửi một frame ACK để xác nhận là frame đã được nhận chính xác, không bị lỗi.

Các frame ACK hoạt động như một công cụ cơ bản phát hiện xung đột, tuy nhiên, công cụ này không giúp ngăn ngừa xung đột xảy ra. Chuẩn 802.11 dùng một phương pháp gọi là Carrier Sense Multiple Access Collision Avoidance (CSMA/CA). Chú ý rằng mạng có dây 802.3 phát hiện (detect) xung đột, trong khi 802.11 cố gắng tránh (avoid) xung đột.

Tránh nghẽn hoạt động bằng cách yêu cầu tất cả các máy trạm lắng nghe trước khi nó truyền đi một frame. Khi một máy trạm có một frame cần phải truyền, một trong hai trạng thái sau có thể xảy ra:

- Không có thiết bị nào khác đang truyền: lúc này máy trạm có thể truyền frame đi ngay lập tức. Bên máy nhận dự kiến phải gửi một frame ACK để xác nhận rằng frame ban đầu đến đúng và không bị đụng độ.
- Có một thiết bị khác đang truyền một frame: lúc này máy của ta phải chờ cho đến khi nào frame đang truyền là hoàn tất, sau đó nó phải chờ một khoảng thời gian ngẫu nhiên trước khi có thể truyền frame của chính nó.

Các frame wireless có thể thay đổi về kích thước. Khi một frame được truyền,

làm thế nào để các máy khác biết là frame đã được truyền hoàn tất và đường truyền (sóng vô tuyến) là rảnh cho các máy khác sử dụng? Rõ ràng, các máy trạm chỉ có thể lắng nghe trong yên lặng, nhưng nếu làm thế thì không phải luôn luôn là hiệu quả. Các máy trạm không dây khác có thể cũng lắng nghe và cũng có thể truyền ở cùng một thời điểm. Chuẩn 802.11 yêu cầu tất cả các máy trạm phải chờ một khoảng thời gian. Khoảng thời gian này được gọi là khoảng thời gian giữa các frame DCF (DCF interframe space). Sau khoảng thời gian này, các máy trạm mới có thể truyền.

Bên máy truyền có thể chỉ ra một khoảng thời gian dự kiến để gửi đi hết một frame bằng cách chỉ ra trong một trường của frame 802.11. Khoảng thời gian này chứa số timeslot (thường tính bằng đơn vị microseconds) cần thiết để truyền frame. Các máy trạm khác phải xem giá trị chứa trong header này và phải chờ khoảng thời gian đó trước khi truyền cho chính nó.

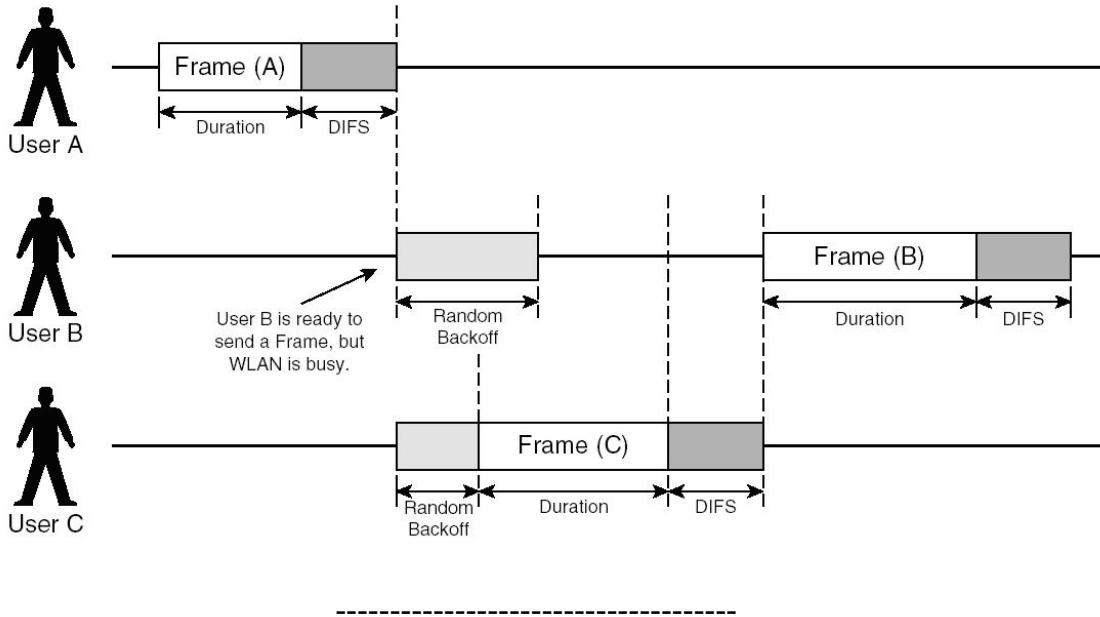
Bởi vì tất cả các frame phải chờ cùng một khoảng thời gian chỉ ra trong frame, tất cả các máy đó có thể sẽ quyết định cùng truyền khi khoảng thời gian đó trôi qua. Điều này có thể dẫn đến hiện tượng xung đột, chính là một hiện tượng cần tránh.

Bên cạnh thông số thời gian nêu trên, các trạm không dây cũng phải triển khai một bộ định thời ngẫu nhiên. Trước khi truyền một frame, máy tính đó phải chọn một số ngẫu nhiên time slot phải chờ. Con số này sẽ nằm trong khoảng từ zero đến kích thước tối đa cửa sổ cạnh tranh. Ý tưởng cơ bản của cách làm này là khi một máy muốn truyền, mỗi máy sẽ chờ một khoảng thời gian ngẫu nhiên, giảm số trạm cố gắng truyền đồng thời cùng lúc.

Toàn bộ tiến trình này được gọi là chức năng phối hợp phân phối. Chức năng này được mô tả trong hình dưới đây. Ba người dùng wireless có cùng một frame phải truyền ở các khoảng thời gian khác nhau. Một chuỗi các sự kiện sau sẽ xảy ra:

1. Người dùng A lắng nghe và xác định rằng không có người dùng nào khác đang truyền. Người dùng A truyền frame của nó, đồng thời quảng bá khoảng thời gian để truyền frame.
2. Người dùng B cũng có frame để truyền. Anh ta phải chờ cho đến khi nào frame của người dùng A là hoàn tất, sau đó, phải chờ hết khoảng thời gian DIFS (thời gian phối hợp phân phối) hoàn tất.
3. Người dùng B phải chờ một khoảng thời gian ngẫu nhiên trước khi cố gắng truyền.
4. Khi người dùng B đang chờ, người dùng C có frame phải truyền. Anh ta lắng nghe và phát hiện rằng không có ai đang truyền. Người dùng C phải chờ một khoảng thời gian ngẫu nhiên. Khoảng thời gian này là ngắn hơn khoảng thời gian ngẫu nhiên của người dùng B.
5. Người dùng C truyền frame và quảng bá khoảng thời gian để truyền.
6. Người dùng B phải chờ khoảng thời gian truyền frame của người dùng C

cộng với khoảng thời gian giữa các frame DIFS trước khi cố gắng truyền lại một lần nữa.



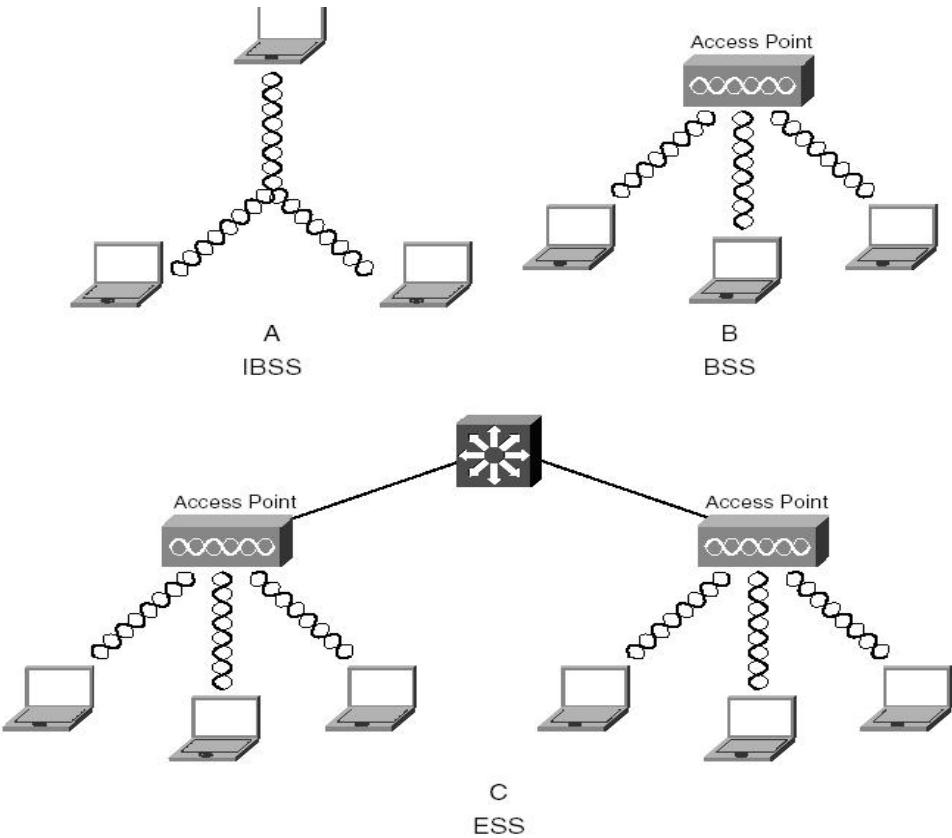
Bài 30:

### Các khối WLAN trong mạng campus

Ở mức độ cơ bản nhất, hạ tầng của mạng không dây không có một tổ chức nhất quán nếu so sánh với mạng có dây. Ví dụ, một máy PC với một card wireless có thể sẽ bật kết nối không dây của nó mọi lúc mọi nơi. Một điều tự nhiên là, để PC có thể truyền và nhận dữ liệu, một vài hoạt động phải diễn ra.

Trong các thuật ngữ của 802.11, một nhóm các thiết bị mạng không dây bất kỳ được gọi là một tập hợp các dịch vụ (service set). Các thiết bị không dây phải có cùng tên tập hợp dịch vụ (service set identified SSID). Đây là một chuỗi được chứa trong mọi frame được gửi ra. Nếu SSID giữa thiết bị gửi và thiết bị nhận là giống nhau, hai thiết bị có thể giao tiếp với nhau.

Chuẩn 802.11 cho phép hai hoặc nhiều các thiết bị không dây giao tiếp trực tiếp với nhau mà không cần thêm bất kỳ phương tiện hay thiết bị nào khác. Mô hình mạng này được gọi là mô hình mạng ad-hoc, hoặc còn gọi là tập hợp các dịch vụ cơ bản độc lập (Independent Basic Service Set IBSS). Mô hình được mô tả trong hình vẽ bên dưới:



Không có một cách kiểm soát cố định với số thiết bị có thể truyền và nhận trên một hạ tầng không dây. Ngoài ra, có nhiều thông số có thể ảnh hưởng đến việc một máy trạm có thể truyền hoặc nhận đến các máy trạm khác. Điều này khiến cho việc tạo ra một kết nối tin cậy đến tất cả các trạm khác trở nên khó khăn.

Một tập hợp dịch vụ mức cơ bản BSS sẽ tập trung giải quyết vấn đề truy cập và vấn đề kiểm soát một nhóm các thiết bị mạng không dây bằng cách đặt một access point – AP là một thiết bị đóng vai trò tập trung. Bất kỳ thiết bị không dây nào cố gắng dùng hạ tầng mạng đầu tiên phải sắp xếp trở thành thành viên của AP. Thiết bị AP có thể sẽ yêu cầu một trong những điều kiện sau, trước khi cho phép một máy trạm tham gia vào:

- SSID phải giống nhau.
- Một tốc độ truyền dữ liệu tương thích.
- Hoàn tất vấn đề xác thực.

Mối quan hệ của một client với một AP được gọi là một kết hợp (association). Máy client phải gửi một thông điệp có chứa yêu cầu kết hợp. Sau đó AP sẽ gán quyền hay từ chối yêu cầu trên bằng cách gửi ra một thông điệp trả lời. Khi đã được kết hợp thành công, tất cả các truyền thông vào/ra từ máy trạm phải thông qua AP. Hoạt động này minh họa ở hình B trong hình vẽ bên trên. Các máy trạm không còn có thể giao tiếp với nhau như trong mô hình adhoc trước đây nữa (còn gọi là mô hình IBSS).

Thiết bị AP không phải là một thiết bị hoàn toàn bị động giống như một Ethernet hub. Một AP quản lý mạng không dây của nó, quảng bá sự tồn tại của chính nó sao cho các máy trạm có thể kết hợp, sau đó AP sẽ kiểm soát tiến trình kết hợp này. Ví dụ, bạn hãy nhớ lại rằng mọi khung dữ liệu khi được gửi thành công thông qua kết nối không dây đều phải được nhận ACK. AP sau đó chịu trách nhiệm gửi ACK ngược về cho máy truy cập.

Bạn cũng nên nhớ rằng, bất chấp trạng thái kết hợp là như thế nào, một máy trạm có khả năng lắng nghe hoặc nhận các frame được gửi thông qua hạ tầng không dây. Các frame thì “trôi nổi” trong không khí, và có thể truy cập bởi bất cứ thiết bị nào nằm trong dãy tần số cho phép để nhận chúng.

Bạn chú ý rằng mô hình tập hợp dịch vụ cơ bản BSS bao gồm một AP và không có một kết nối rõ ràng đến một mạng Ethernet thông thường. Nếu ta triển khai mô hình như trên, Access Point và các máy trạm của nó tạo thành một mạng cô lập.

Một AP cũng có thể kết nối uplink vào một hệ thống mạng Ethernet bởi vì trên AP có hỗ trợ các kết nối không dây và có dây. Nếu AP đặt trong các vị trí vật lý khác nhau, nó có thể dùng để kết nối vào hạ tầng mạng của doanh nghiệp. Mô hình kết nối này được gọi là mô hình dịch vụ mở rộng 802.11 Extended Service Set.

Trong mô hình ESS, một máy trạm chỉ có thể kết nối vào một AP khi máy đó ở gần AP đó. Nếu máy trạm sau đó di chuyển sang vị trí khác, nó có thể kết nối với các AP gần đó. Chuẩn 802.11 cũng định nghĩa một cách thức cho phép các máy trạm trung chuyển (roaming) từ AP này sang AP khác khi vị trí của máy trạm không dây thay đổi.

---

Bài 31:

## **Hoạt động của AP**

Chức năng cơ bản của một AP là làm cầu nối (bridge) cho những dữ liệu mạng không dây từ không khí (mỗi trường sóng vô tuyến) vào mạng có dây bình thường. Một AP có thể chấp nhận những kết nối từ một số các máy trạm không dây sao cho nó có thể trở thành các thành viên bình thường của một mạng LAN dùng dây.

Một AP cũng có thể hoạt động như một cầu nối (bridge) để hình thành một kết nối không dây giữa một mạng LAN này và một mạng LAN khác trên một khoảng cách xa. Trong tình huống đó, ở mỗi đầu của kết nối không dây cần một access point. Kiểu kết nối này gọi là AP-to-AP hoặc kết nối line-of-sight, thường được dùng để kết nối giữa các tòa nhà.

Cisco cũng đã phát triển một loại AP có thể làm cầu nối cho các loại lưu lượng trong mạng không dây từ AP này sang AP kia, theo kiểu một chuỗi các cầu nối.

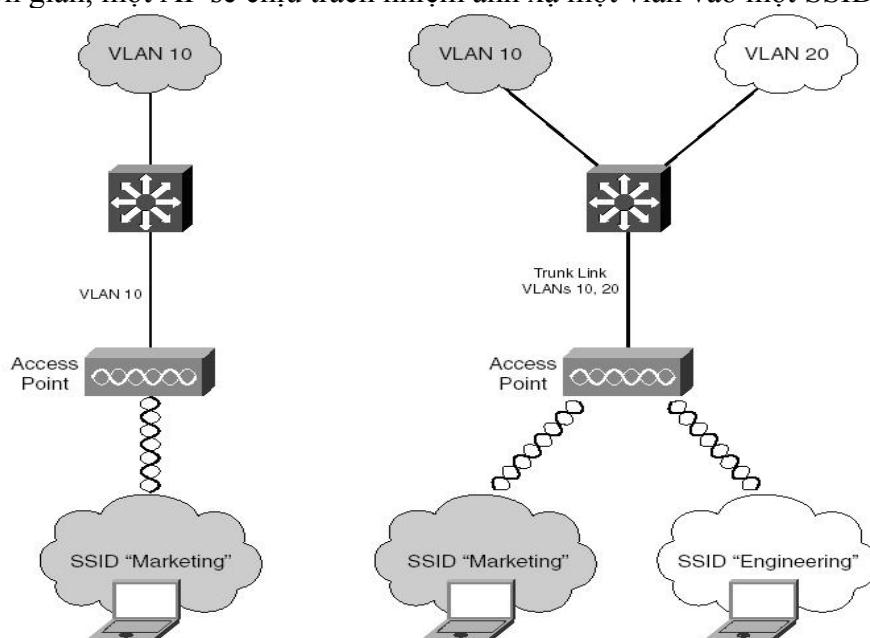
Kiểu kết nối này cho phép một vùng không gian lớn có thể được bao phủ bởi mạng không dây. Các AP lúc này sẽ hình thành nên sơ đồ mess, rất giống với mô hình ESS, trong đó các AP kết nối liên hoàn với nhau thông qua các kết nối không dây khác.

AP hoạt động như một điểm truy cập trung tâm, kiểm soát các truy cập từ các máy trạm. Bất kỳ máy trạm nào khi cố gắng dùng WLAN thì trước hết phải thiết lập một kết nối với một AP. AP có thể cho phép kết nối theo dạng mở sao cho bất kỳ máy trạm nào cũng có thể kết hợp, hoặc có thể kiểm soát chặt chẽ hơn bằng cách yêu cầu xác thực, hoặc có thể dùng các tiêu chuẩn khác trước khi cho phép kết hợp.

Hoạt động của WLAN thì liên quan chặt chẽ đến quá trình phản hồi từ đầu bên kia của kết nối không dây. Ví dụ, các máy trạm phải bắt tay với AP trước khi nó có thể kết nối và sử dụng mạng không dây. Ở mức độ cơ bản nhất, yêu cầu này đảm bảo một kết nối hai chiều bởi vì cả máy trạm và AP đều có khả năng truyền và nhận frame thành công. Tiến trình này sẽ loại bỏ khả năng truyền thông một chiều, khi máy trạm chỉ có thể nghe AP nhưng AP thì không thể nghe máy trạm.

Ngoài ra, AP có thể kiểm soát nhiều khía cạnh của phạm vi mạng không dây của nó bằng cách yêu cầu một số điều kiện phải được đáp ứng trước khi máy trạm có thể kết nối vào. Ví dụ, AP có thể yêu cầu máy client hỗ trợ một tốc độ truyền dữ liệu cụ thể, đáp ứng các biện pháp bảo mật và các yêu cầu xác thực trong quá trình kết hợp.

Bạn có thể nghĩ một AP là một thiết bị bắt cầu, trong đó frame từ các phương tiện, hạ tầng khác nhau sẽ được chuyển đổi và chuyển đi ở lớp 2. Nói một cách đơn giản, một AP sẽ chịu trách nhiệm ánh xạ một VLAN vào một SSID.



Trong phần bên trái của sơ đồ trên minh họa cho tình huống ta muốn mở rộng vlan 10 ra một AP, dùng một cổng của switch ở chế độ access. AP sau đó sẽ ánh xạ vlan 10 sang mạng wireless dùng SSID là “marketing”. Các người dùng kết hợp với SSID “marketing” sẽ được các máy khác xem như đang kết nối vào vlan 10.

Khái niệm này có thể được mở rộng để nhiều vlan được ánh xạ vào nhiều SSID. Để làm được điều này, AP phải kết nối đến switch thông qua kết nối trunk trong đó mang nhiều vlan. Trong phần bên phải của hình trên, vlan 10 và vlan 20 đều được trunk đến AP. AP dùng 802.1q để ràng buộc vlan với SSID. Ví dụ, vlan 10 được ánh xạ đến SSID “marketing” trong khi vlan 20 thì ánh xạ đến SSID “Engineering”.

Kết quả là, khi một AP dùng nhiều SSID, nó sẽ mang nhiều vlan thông qua sóng vô tuyến đến người dùng cuối. Người dùng cuối phải chọn SSID phù hợp đã được ánh xạ vào vlan tương ứng.

---

Bài 32:

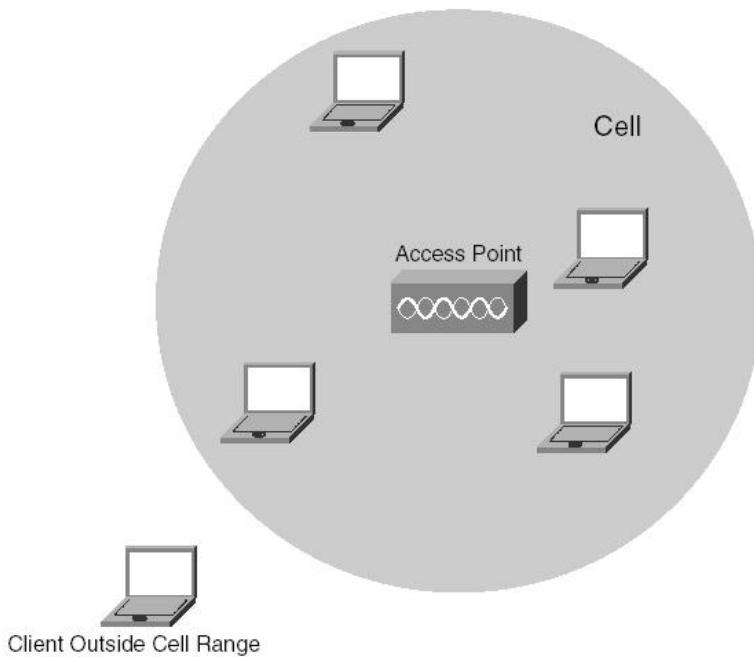
## Wireless LAN cells

Một AP có thể cung cấp kết nối WLAN đến các client chỉ trong tầm vực phát sóng của nó. Phạm vi tín hiệu có thể được định nghĩa một cách tương đối bởi loại ăng ten đang được dùng cho AP. Trong môi trường không khí, phạm vi này có thể là một hình cầu bao bọc xung quanh một ăng ten vô hướng. Ít nhất, phạm vi phủ sóng sẽ xuất hiện như một vòng tròn trên mặt bằng của sàn. Bạn cũng cần nhớ rằng, phạm vi phủ sóng là ba chiều, nghĩa là cũng ảnh hưởng đến các sàn bên trên và bên dưới, trong trường hợp bạn triển khai trong một tòa nhà nhiều tầng.

Vị trí đặt AP phải được hoạch định kỹ lưỡng sao cho phạm vi phủ sóng đạt được mức cần thiết. Mặc dù bạn thiết kế vị trí đặt AP theo một sơ đồ nào đó, hoạt động thật sự của wireless lan sẽ luôn hoạt động trong tình trạng thay đổi. Điều đó là do mặc dù vị trí của AP là cố định, các máy trạm không dây có thể thay đổi vị trí thường xuyên.

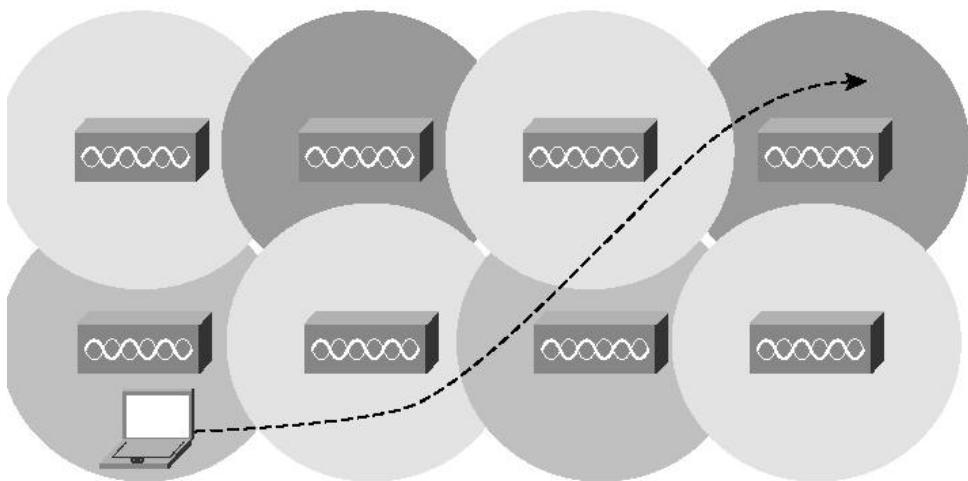
Vấn đề di chuyển của các máy trạm có thể làm cho phạm vi phủ sóng của AP trở nên khó khăn hơn dự kiến. Các máy trạm có thể di chuyển vòng quanh và phía sau những vật cản trong một phòng, phía sau tường, cửa...trong một tòa nhà. Giải pháp tốt nhất để thiết kế vị trí đặt AP và phạm vi phủ sóng là thực hiện một site survey - khảo sát mạng. Trong tiến trình site survey, một AP dùng để kiểm tra sẽ được đặt ở vị trí mong muốn hoặc dự kiến, trong khi một máy trạm không dây sẽ di chuyển xung quanh để đo chất lượng và độ mạnh của tín hiệu. Ý tưởng là thử nghiệm AP bằng chính môi trường thật, với những vật cản thật. Những vật cản thật này có thể gây ảnh hưởng lên hoạt động của máy client.

Phạm vi phủ sóng của một AP được gọi là một cell. Các client trong một cell có thể kết hợp với AP và sau đó truy cập mạng wlan. Khái niệm trên được mô tả trong hình dưới đây. Một máy ra khỏi cell bởi vì nó ra ngoài tầm tín hiệu của AP.



Giả sử một AP loại dùng trong nhà có bán kính phủ sóng là 100 feet, bao phủ vài phòng hay một phần của hành lang. Máy client có thể di chuyển thoải mái bên trong phạm vi (cell) đó và truy cập mạng không dây từ bất kỳ vị trí nào. Tuy nhiên, chỉ có một vùng phủ sóng thì hơi bị hạn chế bởi vì các máy trạm có thể hoạt động trong những phòng lân cận hoặc trên những tầng lầu khác. Các máy này dĩ nhiên không muốn mất kết nối khi đang ở những vị trí khác nhau.

Để mở rộng toàn bộ vùng phủ sóng của WLAN, các cell khác có thể che phủ các phòng lân cận bằng cách đặt thêm các AP trong toàn bộ khu vực tòa nhà. Ý tưởng là ta sẽ đặt AP sao cho các cell có thể bao phủ mọi vùng mà một máy client có thể đặt ở vị trí đó. Thật ra, các cell nên có những vùng chồng lấp lên nhau theo một tỉ lệ phần trăm nhỏ, như trong hình vẽ dưới đây:



Khi các cell là chồng lấp lên nhau, các AP láng giềng không thể dùng cùng tần số.

Nếu hai AP láng giềng sử dụng cùng một tần số, tự nó sẽ gây nhiễu lẫn nhau. Thay vào đó, các tần số được dùng trên các AP láng giềng phải không trùng lắp hoặc phải lệch nhau cho toàn khu vực.

Khi một máy trạm đã kết nối đến một AP, nó có thể tự do di chuyển xung quanh. Khi một máy trạm di chuyển từ một cell của AP sang một cell khác, kết nối cũng sẽ được chuyển từ AP sang AP khác. Việc di chuyển từ một AP sang một AP khác được gọi là chuyển vùng (roaming).

Sự chuyển động này được mô tả trong hình vẽ bên dưới. Khi máy trạm di chuyển dọc theo con đường, nó đi qua vùng phủ sóng của vài AP. Khi một máy trạm di chuyển từ một AP sang một AP khác, nó phải thiết lập lại kết nối với AP mới. Ngoài ra, các dữ liệu mà một máy trạm đang gửi trước khi ở trong trạng thái roaming cũng sẽ được tạm trung chuyển từ AP cũ sang AP mới. Theo cách này, bất kỳ máy trạm không dây nào khi thực hiện kết nối thì chỉ thông qua một AP ở một thời điểm. Điều này cũng giảm thiểu khả năng mất dữ liệu đang gửi hoặc đang nhận khi quá trình roaming diễn ra.

Khi bạn thiết kế một mạng không dây, bạn có thể cố gắng bao phủ một vùng lớn nhất có thể cho một AP. Bạn có thể cấu hình AP ở công suất phát tối đa của nó. Nếu làm như vậy, có thể bạn sẽ giảm số lượng AP cần thiết để bao phủ một vùng. Và vì vậy, sẽ giảm chi phí tổng thể. Tuy nhiên, bạn cũng nên xem xét một số yếu tố bất lợi khác nếu làm như trên.

Khi một AP được cấu hình để bao phủ một vùng rộng lớn, nó cũng tiềm tàng một khả năng là có quá nhiều máy kết nối vào. Tuy nhiên, bạn cần nhớ rằng một cell thì chỉ là một môi trường dùng chung mà tất cả các máy đều phải chia sẻ theo chế độ bán song công (half duplex). Khi số lượng máy trạm kết nối vào tăng lên, tổng số băng thông và thời gian cho mỗi máy sẽ giảm xuống.

Thay vào đó, hãy xem xét việc giảm kích thước của cell (bằng cách giảm công suất phát) sao cho chỉ có những máy trạm trong khoảng cách đủ gần có thể kết nối và dùng băng thông. Lúc này, AP cũng có thể giúp kiểm soát số lượng máy trạm đang kết nối ở một thời điểm bất kỳ nào đó. Điều này trở nên quan trọng cho các ứng dụng đòi hỏi băng thông cao hay thời gian đáp ứng thấp như voice, video hay các phần mềm y tế.

Khi kích thước của cell là giảm nhỏ, nó được gọi là microcells. Khái niệm này có thể được mở rộng trong những môi trường cần kiểm soát cao như các sàn chứng khoán. Trong những trường hợp này, công suất phát của AP và kích thước cell được giảm thiểu, lúc này các cell được gọi là picocell.

---

Bài 33:

### **Một số phương thức để cập nhật bảng định tuyến**

Sử dụng một giao thức định tuyến là cách dễ dàng nhất để tạo và duy trì một bảng định tuyến. Tuy nhiên đây không phải là cách duy nhất hoặc cách hiệu quả nhất để thông báo cho router biết về những mạng hiện có trong một AS. Nếu một router có rất ít tài nguyên, một cách hiệu quả là định nghĩa một đường đi mặc định đến một router có đủ thông tin về các mạng khác. Do đó ngoài cách dùng các giao thức định tuyến, còn có những cách khác để cập nhật.

#### **Dùng định tuyến tĩnh (Static Routes)**

Cấu hình bảng định tuyến tĩnh có nghĩa là thêm vào các tuyến đường tĩnh vào trong bảng định tuyến. Thuận lợi của cách dùng định tuyến tĩnh là giúp tiết kiệm tài nguyên mạng. Nhược điểm của cách dùng này là người quản trị phải chịu trách nhiệm cập nhật cho từng dòng định tuyến tại mọi router nếu có một thay đổi trong mạng. Theo định nghĩa, các tuyến đường tĩnh không thể tự điều chỉnh động mỗi khi có thay đổi xảy ra. Do đó các mạng sẽ không hội tụ cho đến khi nào các router được cấu hình. Có một vài tình huống cần phải dùng định tuyến tĩnh:

- Các đường truyền có băng thông thấp.
- Người quản trị mạng cần kiểm soát các kết nối.
- Kết nối dùng định tuyến tĩnh là dự phòng cho đường kết nối dùng các giao thức động.
- Chỉ có một đường duy nhất đi ra mạng bên ngoài. Tình huống này gọi là mạng stub.
- Router có rất ít tài nguyên và không thể chạy một giao thức định tuyến động.
- Người quản trị mạng cần kiểm soát bảng định tuyến và cho phép các giao thức định tuyến classful và classless.

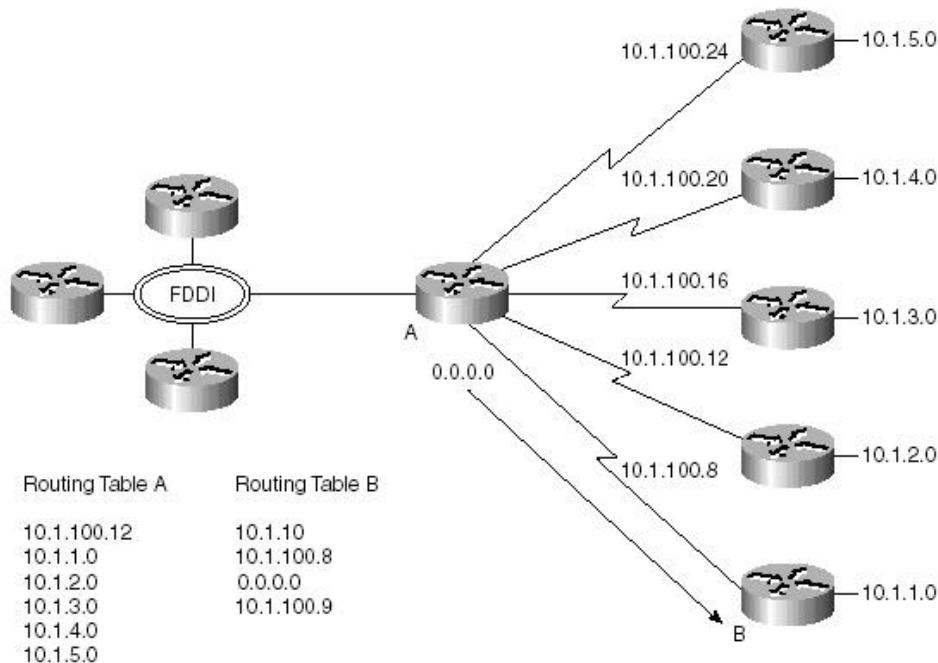
## Dùng định tuyến tĩnh với giá trị AD thay đổi (floating static route)

Cơ chế dùng định tuyến tĩnh với giá trị AD thay đổi là một cơ chế khác để đưa thông tin vào bảng định tuyến. Giải pháp này khắc phục một số giới hạn trong thiết kế mạng. Một floating static route cho phép một đường đi dự phòng nằm chờ cho đến khi nào tuyến đường chính bị chết. Sau đó đường dự phòng sẽ được kích hoạt. Khi đường chính được sửa chữa, đường backup sẽ lui về chế độ dự phòng. Một ví dụ là một đường quay số sẽ làm đường dự phòng cho đường frame-relay.

## Định tuyến theo yêu cầu (On Demand Routing)

Tất cả các vấn đề định tuyến đều quan tâm đến vấn đề phí tổn quản lý. Trong trường hợp các routing update, dùng định tuyến tĩnh thì có chi phí quản trị cao, còn dùng định tuyến động thì tiêu tốn tài nguyên. Thông thường, việc chọn lựa khi nào thì dùng định tuyến tĩnh, khi nào dùng định tuyến động là một quyết định dễ dàng. Định tuyến tĩnh thường được dùng để chia sẻ thông tin định tuyến giữa classful và classless hoặc để định nghĩa một tuyến đường mặc định. Tuy nhiên trong một vài dạng mạng có sơ đồ phân bố lớn, định tuyến tĩnh hay động đều không phù hợp. Trong một hệ thống mạng như vậy, các kết nối thường có băng thông thấp và rất ít thông tin cần gửi trên các kết nối này. Trong tình huống này, có vẻ như định tuyến tĩnh và tuyến đường mặc định default-route là các giải pháp phù hợp. Tuy nhiên nếu có rất nhiều mạng ở xa trong mô hình hub-and-spoke, giải pháp này có thể trở nên không thể quản lý được. Trong giải pháp dùng ODR, tất cả các spoke router có thể có cấu hình giống nhau, mặc dù các địa chỉ IP phải là duy nhất cho từng router.

ODR dùng CDP để gửi các địa chỉ mạng của các mạng kết nối trực tiếp từ spokes hoặc từ stub về hub router. Hub router sẽ gửi các địa chỉ IP của các kết nối chung như là một tuyến mặc định về stub router. ODR có thuận lợi là chỉ gửi các thông tin tối thiểu, chẳng hạn như phần prefix và phần mask, mặc định là mỗi 60 giây. Thông tin này sẽ được cập nhật vào bảng định tuyến của hub router và có thể được redistribute vào các giao thức định tuyến. Bởi vì giá trị netmask được gửi trong cập nhật, VLSM có thể được dùng.



Trong hình vẽ trên, routerA có đầy đủ thông tin về tất cả các mạng kết nối đến từng spoke. Các thiết bị còn lại trong AS chưa được đặt trong bảng định tuyến của router A nhằm đơn giản hóa cấu hình. tất cả các spoke router, tượng trưng ở đây là routerB, sẽ gửi một tuyến mặc định đến phần còn lại của hệ thống mạng. Route mặc định 0.0.0.0 với giá trị next hop là địa chỉ IP của cổng kết nối về A. Router B sẽ có hai mạng kết nối trực tiếp tới nó. Một mạng là tuyến mặc định 0.0.0.0 và giá trị next-hop là địa chỉ của routerA.

#### Khi cấu hình ODR, ta cần phải nhớ các điểm quan trọng sau:

- Không có giao thức định tuyến nào cấu hình trên stub router. IP routing được bật lên ON ở chế độ mặc định. Cho phép sử dụng đường đi mặc định.
- Bất kỳ một địa chỉ phụ (secondary) nào được cấu hình trên stub router sẽ không được truyền bởi CDP về hub router.
- ODR phải được cấu hình trên hub router.
- Mặc dù CDP là cho phép ở chế độ mặc định trên tất cả các cổng, một vài cổng giao tiếp WAN chẳng hạn như ATM đòi hỏi phải cấu hình CDP bằng lệnh cdp enable.
- CDP dùng cơ chế multicast. Với những công nghệ WAN yêu cầu phát biểu mapping (ví dụ như trong frame-relay), hãy dùng từ khóa broadcast để đảm bảo rằng các CDP là được truyền.
- Có thể hiệu chỉnh CDP timers để gửi các cập nhật thường xuyên hơn chu kỳ mặc định 60s.

Bài 34:

## Một số thuộc tính của IPv6

### Tóm tắt địa chỉ (Address Aggregation)

Quá trình tóm tắt các route, bắt cứ khi nào có thể, là quan trọng trong Internet. Bảng định tuyến thì dễ quản lý hơn với cách hiện thực CIDR. Mặc dù tất cả các sơ đồ địa chỉ trong IPv6 cho phép cấp phát hầu như vô tận các địa chỉ, kiến trúc của IPv6 vẫn cho phép triển khai theo dạng có cấu trúc sao cho nó không bị quá tải. Như trong IPv4, các bit bên trái của địa chỉ được dùng để tóm tắt các địa chỉ mạng xuất hiện ở phía phải của cấu trúc địa chỉ. Như vậy, địa chỉ IPv4 140.108.128.0/17 có thể bao gồm các subnets 140.108.225.0/24. Điều này có nghĩa là bảng định tuyến có thể route đến tất cả các subnets nhưng thay vì có 128 địa chỉ subnet nằm trong bảng định tuyến, chỉ còn 1 dòng duy nhất tượng trưng cho tất cả các route. Để chỉ ra một subnet nhỏ hơn, các qui luật thông thường trong định tuyến vẫn được tuân theo và gói tin được gửi tới cho router quảng bá network 140.108.128.0/17. Router này trong bảng định tuyến của nó có nhiều thông tin chi tiết hơn, sẽ chuyển gói cho đến khi nó đến được network đích.

Trong IPv6, kiến trúc địa chỉ cho phép điều chỉnh tốt hơn dạng địa chỉ được dùng trong Internet. Địa chỉ thì rất dài và mỗi phần phục vụ một chức năng khác nhau. 48-bit đầu tiên của địa chỉ được dùng bởi IANA cho quá trình định tuyến động trong Internet để tạo ra các địa chỉ khả kết toàn cục. Ba bit đầu tiên được gán giá trị 001 để chỉ ra một địa chỉ toàn cục.

### Tự động cấu hình (Autoconfiguration)

Các địa chỉ cục bộ hay các router kết nối trực tiếp gửi prefix ra các kết nối cục bộ và ra tuyến đường mặc định. Các thông tin này được gửi đến tất cả các node trên hệ thống mạng, cho phép các host còn lại tự động cấu hình địa chỉ IPv6. Router cục bộ sẽ cung cấp 48-bit địa chỉ toàn cục và SLA hoặc các thông tin subnet đến các thiết bị đầu cuối. Các thiết bị đầu cuối chỉ cần đơn giản thêm vào địa chỉ lớp 2 của nó. Địa chỉ L2 này, cùng với 16-bit địa chỉ subnet tạo thành một địa chỉ 128-bit. Khả năng gắn một thiết bị vào mà không cần bắt cứ một cấu hình nào hoặc dùng DHCP sẽ cho phép các thiết bị mới thêm vào Internet, chẳng hạn như dùng cellphone, dùng các thiết bị wireless và. Mạng Internet trở thành plug-and-play.

### Tái cấu hình địa chỉ (Renumbering)

Khả năng kết nối đến các thiết bị ở xa một cách tự động cho phép đơn giản hóa nhiều tác vụ trước đây là các cơn ác mộng cho các nhà quản trị. Tính năng tự động cấu hình của IPv6 cho phép các router cung cấp tất cả các thông tin cần thiết đến tất cả các host trên mạng của nó. Điều này có nghĩa là các thiết bị có thể cấu hình lại địa chỉ của nó dễ dàng hơn. Trong IPv6, các thay đổi này là trong suốt đối với người dùng cuối.

## Header đơn giản và hiệu quả

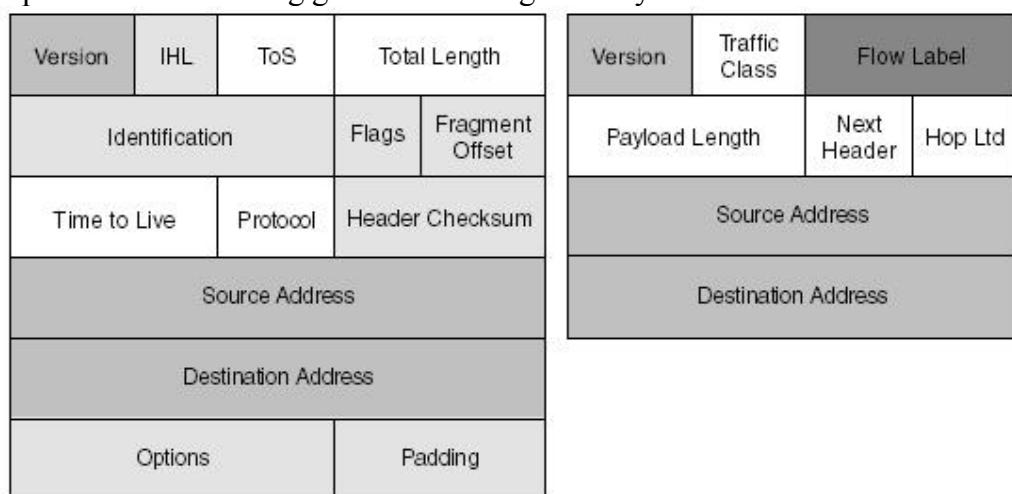
Phần header của IPv6 đã được đơn giản hóa để tăng tốc độ xử lý và tăng hiệu quả cho router. Các cải tiến bao gồm:

Có ít vùng hơn trong header.

Các vùng bao gồm 64bits.

Không còn phần kiểm tra lỗi checksum.

Do có ít vùng hơn, quá trình xử lý cũng ngắn hơn. Bộ nhớ dùng hiệu quả hơn với các field 64 bits. Điều này cho phép quá trình tìm kiếm trở nên rất nhanh bởi vì các bộ xử lý ngày nay cũng là các bộ xử lý 64 bit. Trở ngại duy nhất là việc sử dụng địa chỉ 128-bit, lớn hơn kích thước một word hiện hành. Việc loại bỏ phần check sum cũng giảm thiểu thời gian xử lý nhiều hơn nữa.



- Name Change but Same Functionality in IPv6
- No Change in IPv6
- Removed in IPv6
- New to IPv6

## Bảo mật (Security)

Với các kết nối trực tiếp thông qua các không gian địa chỉ rộng lớn, vấn đề bảo mật là một chọn lựa nhiều thực tế cho IPv6. Bởi vì nhu cầu dùng firewall và các quá trình NAT giữa các thiết bị đầu cuối là giảm, các giải pháp về bảo mật có thể được thực hiện bằng cách mã hóa giữa các hệ thống. Mặc dù IPSec đã sẵn có trong IPv4, nó đã trở thành một thành phần trong IPv6. Việc sử dụng các thành phần mở rộng cho phép một giao thức cung cấp giải pháp end-to-end.

## Tính cơ động

Địa chỉ IPv6 được thiết kế với tính cơ động được tích hợp vào trong Mobile IP. Mobile IP cho phép các hệ thống đầu cuối thay đổi vị trí mà không mất các kết nối. Đặc điểm này rất cần thiết cho những sản phẩm wireless chẳng hạn như IP phone và các hệ thống GPS trong xe hơi. Định dạng phần header cho phép các thiết bị đầu cuối thay đổi địa chỉ IP bằng cách dùng một địa chỉ gốc như là nguồn của gói tin. Địa chỉ gốc này là ổn định, cho phép các địa chỉ duy trì tính cơ động.

Bài 35:

## Bảo mật lớp 2

Tài liệu Cisco SAFE Blueprint (có ở địa chỉ <http://www.cisco.com/go/safe>) đề nghị một số giải pháp sau cho bảo mật switch. Trong phần lớn các trường hợp, việc khuyến cáo phụ thuộc vào một trong ba đặc điểm sau trên các cổng của switch.

Các port không được dùng của switch: Là các port không kết nối đến bất kỳ thiết bị nào. Ví dụ như các switchport có thể được gắn cáp sẵn vào các ổ mạng trên tường.

Các port của người dùng: Là các port gắn vào các thiết bị đầu cuối của end-user hoặc bất cứ port nào có gắn cáp dẫn đến một vài khu vực không được bảo vệ.

Các port tin cậy hay các port trunks: Là các port kết nối đến những thiết bị tin cậy, chẳng hạn như các switch khác hoặc các switch đặt trong các khu vực có bảo mật vật lý tốt.

Danh sách dưới đây tóm tắt các khuyến cáo áp dụng cho các cổng đang dùng và chưa được dùng của switch. Các điểm chung của những kiểu port này là một người dùng có thể truy cập được đến switch sau khi họ đã đi vào bên trong tòa nhà mà không cần đi vào wiring closet hay data center.

- \* Tắt các giao thức cần thiết như CDP hay DTP.
- \* Tắt các giao thức trunking bằng cách cấu hình các port này như là access port.
- \* Bật tính năng BPDU Guard và root Guard để ngăn ngừa các kiểu tấn công STP và giữ một sơ đồ mạng STP ổn định.
- \* Dùng các tính năng như Dynamic ARP Inspection (DAI) hoặc private VLAN để ngăn ngừa frame sniffing.
- \* Bật tính năng port security để giới hạn số địa chỉ MAC cho phép và để cho phép những MAC cụ thể nào đó.
- \* Dùng xác thực 802.1X.
- \* Dùng DHCP snooping và IP source Guard để ngăn ngừa DHCP DOS và kiểu tấn công man-in-the-middle.

Bên cạnh các khuyên cáo trên, Cisco SAFE Blueprint còn có thêm các khuyên cáo sau:

- \* Đối với bất cứ port nào (bao gồm cả trusted port), hãy xem xét khả năng triển khai private vlan để bảo vệ mạng khỏi bị sniffing, bao gồm cả việc ngăn ngừa các routers hay các L3 switch không định tuyến các gói tin giữa các thiết bị trong private LAN.
- \* Cấu hình xác thực VTP ở chế độ toàn cục cho từng switch để ngăn ngừa kiểu tấn công DOS.
- \* Tắt bất cứ cổng nào không dùng của switch và đặt các cổng này vào trong các vlan không dùng.
- \* Tránh sử dụng VLAN 1. Đối với các kết nối trunk, không dùng native vlan.

### **Bảo mật cho switch trên các cổng đang dùng và chưa dùng**

Ví dụ dưới đây mô tả một cấu hình trên switch Cat 3560, với cách cấu hình từng đặc điểm được nêu ra. Trong ví dụ này, cổng F0/1 là cổng không được dùng. CDP đã được tắt trên các cổng nhưng CDP vẫn còn chạy ở chế độ toàn cục vì giả thuyết là một vài cổng vẫn còn cần dùng CDP. DTP đã được tắt và STP RootGuard và BPDU Guard được bật. Lệnh cdp run cho phép CDP vẫn chạy ở chế độ toàn cục nhưng CDP đã bị tắt trên cổng F0/1 là cổng không được sử dụng.

```
cdp run  
int fa0/0  
no cdp enable
```

Lệnh switchport mode access ngăn ngừa port không trở thành trunking và lệnh switchport nonegotiate ngăn ngừa bất kỳ thông điệp nào của DTP được gửi hay nhận.

```
switchport mode access  
switchport nonegotiate
```

Hai lệnh cuối cùng bật tính năng Root Guard và BPDU Guard trên từng cổng. BPDU cũng có thể được bật trên tất cả các cổng bằng tính năng PortFast. Tính năng này được cấu hình bằng lệnh ở chế độ toàn cục spanning-tree portfast bpduguard enable.

```
spanning-tree guard root  
spanning-tree bpduguard enable
```

## **Port Security**

Tính năng switchport port security giám sát một cổng của switch để giới hạn số địa chỉ MAC kết hợp với port đó trong bảng switching L2. Tính năng này cũng áp đặt giới hạn số địa chỉ MAC bằng cách chỉ cho vài địa chỉ MAC có thể dùng trên cổng đó.

Để hiện thực tính năng port security, switch sẽ thêm vào vài bước trong tiến trình xử lý bình thường của các frame đi vào. Thay vì tự động thêm vào bảng MAC địa chỉ MAC nguồn và số cổng, switch xem xét cấu hình port security và sẽ quyết định nó có cho phép địa chỉ đó không. Bằng cách ngăn ngừa các địa chỉ MAC khỏi việc thêm vào switch, port security có thể ngăn ngừa không đầy frame về các địa chỉ MAC đó trên một cổng.

Tính năng port security hỗ trợ những đặc điểm chủ chốt sau:

Giới hạn số địa chỉ MAC có thể kết hợp với một cổng của switch.

Giới hạn địa chỉ MAC thật kết hợp với cổng, dựa trên ba phương thức sau:

Cấu hình tĩnh địa chỉ MAC.

Học động địa chỉ MAC, số địa chỉ MAC có thể lên đến giá trị định nghĩa tối đa, trong đó các hàng trong bảng định tuyến sẽ bị mất khi reload.

Học động các địa chỉ MAC nhưng các địa chỉ này sẽ được lưu trong cấu hình (còn được gọi là sticky).

Chức năng port security bảo vệ vài kiểu tấn công. Khi một bảng CAM điền thông tin mới vào, các thông tin cũ sẽ bị xóa ra. Khi một switch nhận được một frame đi về địa chỉ MAC đích không còn trong bảng CAM, switch sẽ phát tán frame đó ra tất cả các cổng. Một kẻ tấn công có thể làm cho các switch điền lại thông tin trong bảng CAM bằng cách gửi ra rất nhiều frame, mỗi frame có một địa chỉ MAC nguồn khác nhau, làm cho switch xóa các thành phần trong bảng CAM cho hầu hết các host hợp lệ. Kết quả là, switch sẽ phát tán các frame hợp lệ bởi vì địa chỉ MAC đích không còn trong bảng CAM, làm cho máy tấn công thấy tất cả các frame.

---

Bài 36:

## **Một số tính năng nâng cao của NAT**

**Cấu hình pool uyển chuyển hơn:**

Cú pháp cấu hình dãy địa chỉ đã được mở rộng để cho phép một dãy không liên tục các địa chỉ. Cú pháp sau đây là cho phép:

```
ip nat pool <name> { netmask <mask> | prefix-length <length> } [ type { rotary } ]
```

Lệnh này sẽ đưa người dùng vào IP NAT pool, trong đó một dãy địa chỉ có thể được cấu hình. Chỉ có một lệnh được cấu hình trong chế độ này:

address <start> <end>

Example:

*Router(config)#ip nat pool fred prefix-length 24*

*Router(config-ipnat-pool)#address 171.69.233.225 171.69.233.226*

*Router(config-ipnat-pool)#address 171.69.233.228 171.69.233.238*

Cấu hình tạo ra một dãy chứa các địa chỉ 171.69.233.225-226 và dãy địa chỉ 171.69.233.228-238 (địa chỉ 171.69.233.227 đã bị loại bỏ).

### **Dịch sang địa chỉ của công:**

Để giúp các người dùng muốn dịch tất cả các địa chỉ bên trong gán đến một công trên router, NAT cho phép ta đặt tên cho công của router khi cấu hình nat động.

*ip nat inside source list <number> interface <interface> overload*

Nếu không có địa chỉ nào trên công, hay nếu công là không up, NAT sẽ không xảy ra.

Ví dụ:

*ip nat inside source list 1 interface Serial0 overload*

### **Cấu hình NAT tĩnh với các công:**

Khi chuyển dịch địa chỉ đến địa chỉ của một công, các kết nối đến router xuất phát từ bên ngoài (chẳng hạn như email) sẽ cần các cấu hình thêm để có thể chuyển các kết nối vào các máy bên trong. Lệnh này cho phép người dùng ánh xạ vài dịch vụ đến vài máy bên trong.

*ip nat inside source static { tcp | udp } <localaddr> <localport> <globaladdr> <globalport>*

Ví dụ:

*ip nat inside source static tcp 192.168.10.1 25 171.69.232.209 25*

Trong ví dụ này, các kết nối SMTP từ bên ngoài đến công 25 sẽ được gửi vào máy bên trong ở địa chỉ 192.168.10.1.

### **Hỗ trợ cho route maps:**

Các lệnh thực hiện NAT động có thể chỉ ra một route map để xử lý thay vì là một access-list. Một route map cho phép người dùng lựa ra một kết hợp của access-list, next-hop và địa chỉ công ra (output interface) để xác định dãy địa chỉ nào sẽ được dùng.

```
ip nat inside source route-map <name> pool <name>
Example:
ip nat pool provider1-space 171.69.232.1 171.69.232.254 prefix-length 24
ip nat pool provider2-space 131.108.43.1 131.108.43.254 prefix-length 24
ip nat inside source route-map provider1-map pool provider1-space
ip nat inside source route-map provider2-map pool provider2-space
!
interface Serial0/0
ip nat outside
!
interface Serial0/1
ip nat outside
!
interface Fddi1/0
ip nat inside
!
route-map provider1-map permit 10
match ip address 1
match interface Serial0/0
!
route-map provider2-map permit 10
match ip address 1
match interface Serial0/1
```

#### Từ khóa “extendable”:

Từ khóa extandable cho phép người dùng cấu hình vài luật chuyển đổi không rõ ràng, ví dụ như các luật có cùng địa chỉ local và global.

```
ip nat inside source static <localaddr> <globaladdr> extendable
```

Một vài khách hàng muốn dùng nhiều hơn một nhà cung cấp dịch vụ và sẽ dịch vào từng không gian địa chỉ của nhà cung cấp dịch vụ. Ta có thể dùng route map để việc chọn lựa dựa trên địa chỉ toàn cục hay trên những cổng ra hoặc dựa vào access list. Dưới đây là một ví dụ:

```
ip nat pool provider1-space ...
ip nat pool provider2-space ...
ip nat inside source route-map provider1-map pool provider1-space
ip nat inside source route-map provider2-map pool provider2-space
!
route-map provider1-map permit 10
match ip address 1
match interface Serial0/0
!
```

```
route-map provider2-map permit 10
match ip address 1
match interface Serial0/1
```

Ta cũng muốn định nghĩa các ánh xạ tĩnh cho một host đặc biệt trên từng không gian địa chỉ của người dùng. Hệ điều hành Cisco IOS không cho phép hai câu lệnh cấu hình tĩnh có cùng địa chỉ cục bộ vì nó sẽ gây ra sự nhập nhằng từ phía bên trong. Router sẽ chấp nhận các câu lệnh tĩnh này và giải quyết việc nhập nhằng bằng cách tạo ra các câu lệnh ánh xạ đầy đủ và nếu việc ánh xạ được đánh dấu như là “extendable”. Đối với một dòng từ bên ngoài vào, các luật route map động sẽ được dùng để tạo ra việc chuyển đổi.

### **Tạo ra các tên cho các dãy địa chỉ:**

Nhiều khách hàng muốn cấu hình NAT để dịch các địa chỉ cục bộ sang địa chỉ toàn cục được cấp phát từ những địa chỉ không dùng trong một dãy địa chỉ mạng. Điều này yêu cầu router trả lời những ARP request cho những địa chỉ này để các gói tin đi về địa chỉ toàn cục được chấp nhận bởi router và được thực hiện NAT. Tiến trình định tuyến routing trong router sẽ quản lý gói tin này khi địa chỉ toàn cục được cấp phát từ một địa chỉ ảo, không kết nối vào đâu. Khi một dãy địa chỉ NAT dùng một địa chỉ inside global hoặc outside local bao gồm các địa chỉ trên một subnet, phần mềm sẽ tạo ra một tên giả cho địa chỉ mà router sẽ trả lời ARP.

Quá trình đặt tên tự động này cũng diễn ra cho các địa chỉ inside global hay outside global trong các hàng cấu hình tĩnh. Cơ chế này có thể tắt bằng cách dùng lệnh no-alias:

```
ip nat inside source static <local-ip-address> <global-ip-address> no-alias
```

### **Host Number Preservation: Lưu giữ địa chỉ host**

Để dễ cho việc quản trị, một vài site chỉ muốn đổi phần địa chỉ mạng, không đổi phần địa chỉ. Nghĩa là họ muốn phần địa chỉ đã chuyển đổi phải có cùng địa chỉ phần host giống như ban đầu. Dĩ nhiên là hai địa chỉ mạng phải có cùng prefix length. Đặc điểm này có thể được bật bằng cách cấu hình nat động như thường lệ nhưng cấu hình phần dãy địa chỉ thêm vào từ khóa match-host.

```
ip nat pool fred <start> <end> prefix-length <len> type match-host
```

### **Cài tiến thời gian timeouts:**

Các lệnh sau đây đã được hỗ trợ để mở rộng thời gian chuyển dịch

```
ip nat translation ?
icmp-timeout Specify timeout for NAT ICMP flows
syn-timeout Specify timeout for NAT TCP flows after a SYN and no further data
```

### **Giới hạn số lượng NAT sessions:**

Dùng các lệnh sau, Cisco IOS NAT có thể được cấu hình để giới hạn số lượng NAT tạo ra. Mặc định là không giới hạn.

*ip nat translation max-entries <n>*

Bài 37:

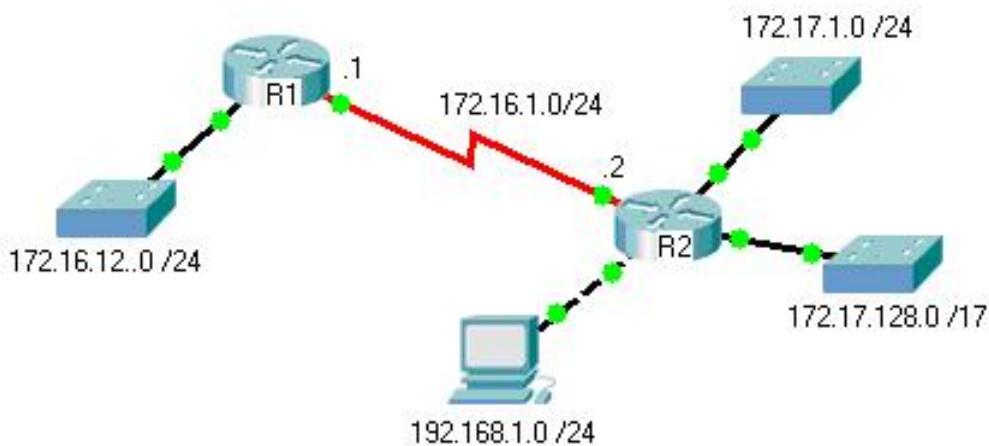
### **Cách xem thông tin bảng định tuyến**

#### **Cấu trúc bảng định tuyến và tiến trình tra bảng định tuyến của router:**

Một khi đã quyết định trở thành người quản trị mạng bạn phải thực sự hiểu về cấu trúc của bảng định tuyến và quá trình tìm đường đi dựa vào bảng định tuyến (lookup process). Kiến thức này rất quan trọng khi người quản trị giải quyết những vấn đề liên quan tới bảng định tuyến.

Để hiểu được quá trình router thực hiện tra bảng định tuyến như thế nào, ta phải hiểu được định dạng của bảng định tuyến, layer 1 route và layer 2 route.

Ta sử dụng mô hình mạng với 2 router, R1 gồm 1 mạng chính 172.16.0.0 /16 được chia subnet 172.16.0.0 /24. R2 gồm 3 mạng chính (major network) 172.17.0.0/16, 172.16.0.0/16, 192.168.1.0/24.



*Hình 37.1: Mô hình lab gồm 2 router.*

Để đơn giản ta chỉ xét thông tin bảng định tuyến trên Router 2

```
R2#sho ip rout
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C 172.16.0.0/24 is subnetted, 2 subnets
   C 172.16.1.0 is directly connected, Serial0/0/0
      2 172.16.12.0 [120/1] via 172.16.1.1, 00:00:05, Serial0/0/0
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
         C 172.17.1.0/24 is directly connected, FastEthernet0/0
         C 172.17.128.0/17 is directly connected, FastEthernet0/1
      192.168.1.0/24 is directly connected, Ethernet0/1/0
R2#
```

Hình 37.2: Thông tin bảng định tuyến của Router 2

Khi show bảng định tuyến cơ bản ta sẽ thấy được những thông tin sau:

Cho biết tuyến đường này có được do người quản trị chỉ ra (static route), router học được nhờ các giao thức định tuyến (dynamic route) hay là mạng kết nối trực tiếp tới router (connected route).

Router có thể gửi được dữ liệu tới mạng này

Để tới được mạng mong muốn Router phải gửi gói tin ra interface nào hay gửi gói tin tới địa chỉ IP nào (IP next-hop)

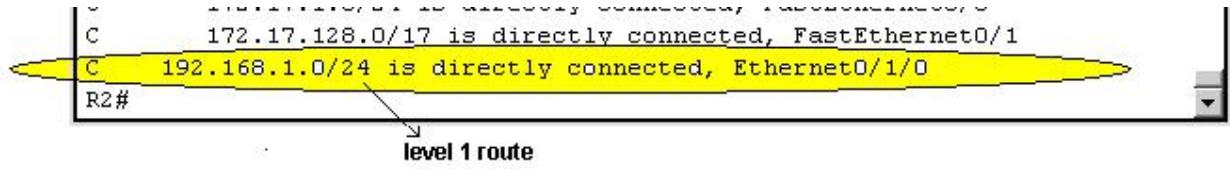
**Ví dụ:** như trên hình 2, router 2 muốn gửi gói tin tới mạng 172.16.12.0 thì sẽ gửi ra cổng (interface) serial0/0/0 hay gửi tới cổng của router có địa chỉ IP 172.16.1.1. Thông tin này được học nhờ giao thức định tuyến RIP

### I/ Cấu trúc phân cấp của bảng định tuyến.

Bảng định tuyến của router có cấu trúc phân cấp, việc này rất quan trọng giúp router không cần phải tra hết tất cả tuyến đường trong bảng định tuyến để chọn đường đi. Đơn giản ta chỉ tìm hiểu tuyến đường với 2 cấp lever 1 và 2.

**Level 1 ultimate route:** là những tuyến có subnet mask bằng hoặc nhỏ hơn classfull mask của địa chỉ mạng và bao gồm thông tin về next-hop IP address hay interface mà router sẽ gửi gói tin ra để đi đến mạng mong muốn.

Như trong hình 3, 192.168.1.0 /24 là tuyến đường cấp 1 vì nó có subnet mask là 24 bằng với classful mask của địa chỉ mạng lớp C /24 và interface trên router để đi ra mạng này là serial Ethernet0/1/0.



Hình 37.3: level 1 route

#### ***Parent and child routes ( level 1 parent route and level 2 route)***

Khi một mạng có chia subnet được add vào bảng định tuyến, tuyến đường này được phân thành 2 cấp: *parent route* và *child route* hay còn được gọi *parent route cấp 1 (level 1 parent route)* và *route cấp 2*.

**Level 1 parent route:** là địa chỉ **classfull** không mang thông tin về địa chỉ IP next-hop hay exit interface. (xem tiếp bên dưới)

**Level 2 route:** Là tuyến đường chỉ ra mạng con của địa chỉ mạng chính

Như trong hình 4

```
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
C        172.16.1.0 is directly connected, Serial0/0/0
R        172.16.12.0 [120/1] via 172.16.1.1, 00:00:05, Serial0/0/0
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C          172.17.1.0/24 is directly connected, FastEthernet0/0
C          172.17.128.0/17 is directly connected, FastEthernet0/1
C        192.168.1.0/24 is directly connected, Ethernet0/1/0
R2#
```

Hình 4: parent and child routes

Mạng 172.16.0.0/24 và 172.17.0.0/16 là *parent routes*, các mạng khác

172.16.1.0 – 172.16.12.0 và 172.17.1.0/24 – 172.17.128.0/24 là *child routes* vì chúng là mạng con của địa chỉ mạng chính 172.16.0.0 và 172.17.0.0

Trong phần này chúng ta chia làm 2 trường hợp

- Trường hợp 1: Tất cả các subnet của cùng một mạng chính có subnet mask bằng nhau

Parent route là địa chỉ classful có subnet mask được chỉ ra đại diện cho các mạng con của nó. Trên hình 4, 172.16.0.0/24 là *parent route* có subnet mask là 24 chỉ ra rằng hai mạng con của nó 172.16.1.0 và 172.16.12.0 để sử dụng subnet mask là 24.

- Trường hợp 2: Các subnet của cùng một mạng có subnet mask với chiều dài khác nhau

Parent route cũng là địa chỉ classful nhưng subnet mask là **classfull mask** (classfull mask của địa chỉ mạng lớp A là /8, lớp B /16, lớp C/24). Mỗi subnet đều mang thông tin riêng về subnet mask của mình. Trên hình 4, 172.17.0.0/16 được chia làm 2 mạng con có địa chỉ 172.17.1.0/24 và 172.17.128/17. Parent route 172.17.0.0/16 có classfull mask là /16 và mỗi mạng con đều có subnet mask riêng của mình.

## **II/ Quá trình router thực hiện tra bảng định tuyến:**

Khi router nhận được một gói IP nó sử dụng địa chỉ IP đích của gói tin này kết hợp với bảng định tuyến để xác định đường đi. Như vậy quá trình tra bảng định tuyến như thế nào? Làm thế nào router có thể xác định được đường đi tốt nhất? Subnet mask của mỗi mạng trong bảng định tuyến có ý nghĩa gì? . . .

### **Các bước router thực hiện tra bảng định tuyến:**

**Bước 1:** Đầu tiên router sẽ so sánh địa chỉ IP đích với tất cả *level 1 routes* trong bảng định tuyến. Nếu địa chỉ này phù hợp nhất với *level 1 ultimate route* thì nó sử dụng đường này để chuyển gói tin đi. Nếu địa chỉ này phù hợp nhất với *level 1 parent route* thì router sẽ thực hiện sang bước thứ 2.

**Bước 2:** Router sẽ so sánh địa chỉ IP đích với tất cả *level 2 child routes*. Nếu có một tuyến phù hợp nhất thì nó sẽ sử dụng tuyến này để chuyển gói tin đi. Nếu không phù hợp thì router thực hiện tiếp bước 3.

**Bước 3:** Router xét xem nó thực hiện định tuyến classfull routing behavior hay classless routing behavior

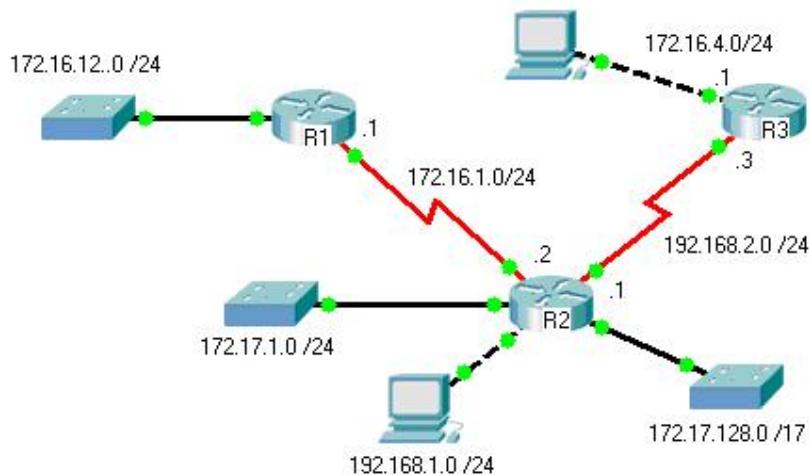
Nếu router thực hiện định tuyến classful routing behavior ( Router(config) # no ip classless) : Gói tin này sẽ bị hủy

Nếu router thực hiện định tuyến là classless routing behavior ( Router(config)# ip classless): Router sẽ quay lại tìm tiếp level 1 xem có default route hay supernet ( địa chỉ mạng có subnet mask nhỏ hơn classfull mask) được chỉ ra hay không, nếu có thì router thực hiện tiếp bước 4.

**Bước 4:** Nếu router tìm được default route hay supernet phù hợp thì nó sẽ sử dụng tuyến đường này để chuyển gói đi, nếu không tìm thấy bất kỳ sự phù hợp nào thi gói sẽ bị hủy.

*Để hiểu rõ ta xét ví dụ sau với 2 router như hình 2 kết hợp với router 3, trên router có mạng 172.16.4.0 /24. Ta tắt cấu hình định tuyến động trên mạng 192.168.2.0 (Router(config-rip)# no network 192.168.2.0) và cấu hình static route 172.0.0.0/8 tới router R3.*

### **Mô hình lab.**



### Bảng định tuyến trên router 2.

```

Gateway of last resort is not set

172.0.0.0/8 is subnetted, 1 subnets
S      172.0.0.0 [1/0] via 192.168.2.3
172.16.0.0/24 is subnetted, 2 subnets
C        172.16.1.0 is directly connected, Serial0/0/0
R        172.16.12.0 [120/1] via 172.16.1.1, 00:00:08, Serial0/0/0
          172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C          172.17.1.0/24 is directly connected, FastEthernet0/0
C          172.17.128.0/17 is directly connected, FastEthernet0/1
C        192.168.1.0/24 is directly connected, Ethernet0/1/0
C        192.168.2.0/24 is directly connected, Serial0/0/1
R2#

```

*Dừng trên Router 2 ta ping tới địa chỉ IP 172.16.4.1. Router thực hiện tra bảng định tuyến như sau:*

Bước 1: Router so sánh địa chỉ IP 172.16.4.1 với level 1 routes, những level 1 ultimate route ( 192.168.1.0 /24 và 192.168.2.0 /24 ) không phù hợp chỉ có 1 level parent route 172.0.0.0 /24 phù hợp với 8 bits đầu và 1 level parent route 172.16.0.0 /24 phù hợp với 16 bits đầu. Trong đó, level 1 parent route 172.16.0.0 /24 là phù hợp nhất. Router thực hiện tiếp bước 2

Bước 2: Vì level 1 parent route 172.16.0.0 /24 là phù hợp nhất do đó router sẽ tiếp tục so sánh địa chỉ IP 172.16.4.1 với các level 2 child routes ( 172.16.1.0 và 172.16.2.0 ), 2 level child route này không phù hợp với địa chỉ 172.16.4.1 router thực hiện tiếp bước 3

Bước 3:

- Nếu router được cấu hình IP classless ( mặc định IOS từ 11.3 trở đi, các router có chức năng này) router thực hiện so sánh lại một lần nữa địa chỉ 172.16.4.1 với level 1 route và thấy level 1 parent route 172.0.0.0 /8 phù hợp với 8 bits đầu của địa chỉ do đó router sẽ chuyển gói tin tới IP next-hop 192.168.2.3
- Nếu router không cấu hình IP classless ( command: R(config) # no ip classless) thì gói tin này sẽ bị hủy cho dù router có cấu hình default route tới IP next-hop 192.168.2.3

**Chú ý: Nếu router được cấu hình “no ip classless” defaul route chỉ được sử dụng khi không có bất kì một level 1 ultimate route và level 1 parent route nào phù hợp.**

---

Bài 38:

## TỔNG QUAN VỀ IP VERSION 6

### I- GIỚI THIỆU CHUNG

#### II-

Hệ thống địa chỉ IPv4 hiện nay không có sự thay đổi về cơ bản kể từ RFC 791 phát hành 1981. Qua thời gian sử dụng cho đến nay đã phát sinh các yếu tố như:

- Sự phát triển mạnh mẽ của hệ thống Internet dẫn đến sự cạn kiệt về địa chỉ Ipv4
- Nhu cầu về phương thức cấu hình một cách đơn giản
- Nhu cầu về Security ở IP-Level
- Nhu cầu hỗ trợ về thông tin vận chuyển dữ liệu thời gian thực (Real time Delivery of Data) còn gọi là Quality of Service (QoS)
- ...

Dựa trên các nhược điểm bộc lộ trên, hệ thống IPv6 hay còn gọi là IPng (Next Generation : thế hệ kế tiếp) được xây dựng với các điểm chính như sau :

1- Định dạng phần Header của các gói tin theo dạng mới

Các gói tin sử dụng Ipv6 (Ipv6 Packet) có cấu trúc phần Header thay đổi nhằm tăng cường tính hiệu quả sử dụng thông qua việc dời các vùng (field) thông tin không cần thiết (non-essensial) và tùy chọn (Optional) vào vùng mở rộng (Extension Header Field)

2- Cung cấp không gian địa chỉ rộng lớn hơn

3- Cung cấp giải pháp định tuyến (Routing) và định vị địa chỉ (Addressing) hiệu quả hơn

-Phương thức cấu hình Host đơn giản và tự động ngay cả khi có hoặc không có DHCP Server  
(stateful / stateless Host Configuration)

4- Cung cấp sẵn thành phần Security (Built-in Security)

5- Hỗ trợ giải pháp Chuyển giao Uy tiên (Prioritized Delivery) trong Routing

6- Cung cấp Protocol mới trong việc tương tác giữa các Điểm kết nối (Nodes )

7- Có khả năng mở rộng dễ dàng thông qua việc cho phép tạo thêm Header ngay sau Ipv6 Packet Header

Chúng ta có thêm tham khảo 1 Bảng so sánh giữa IPv6 Packet và IPv4 packet sau :

#### Bảng so sánh Ipv6 / Ipv4

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length. For more information, see “IPv6 Addressing.”
IPsec support is optional.	IPsec support is required. For more information, see “IPv6 Header.”
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field. For more information, see “IPv6 Header.”
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host. For more information, see “IPv6 Header.”
Header includes a checksum.	Header does not include a checksum. For more information, see “IPv6 Header.”
Header includes options.	All optional data is moved to IPv6 extension headers. For more information, see “IPv6 Header.”
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages. For more information, see “Neighbor Discovery.”
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages. For more information, see “Multicast Listener Discovery.”
ICMP Router Discovery is used to determine the IPv4 address of the best default	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required. For

gateway and is optional.	more information, see “Neighbor Discovery.”
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used. For more information, see “Multicast IPv6 Addresses.”
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP. For more information, see “Address Autoconfiguration.”
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses. For more information, see “IPv6 and DNS.”
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names. For more information, see “IPv6 and DNS.”
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation). For more information, see “IPv6 MTU.”

## II- ĐỊA CHỈ IPv6

### 1- Không gian địa chỉ IPv6

Địa chỉ IPv6 (IPv6 Address) với 128 bits địa chỉ cung cấp khối lượng tương đương số thập phân là

$2^{128}$  hoặc **340,282,366,920,938,463,463,374,607,431,768,211,456** địa chỉ

so với IPv4 với 32 bits địa chỉ cung cấp khối lượng tương đương số thập phân là

$2^{32}$  hoặc **4,294,967,296** địa chỉ

### 2-Hình thức trình bày

IPv6 Address gồm 8 nhóm, mỗi nhóm 16 bits được biểu diễn dạng số Thập lục phân (Hexa-Decimal)

Vd-1 : 2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

(1) (2) (3) (4) (5) (6) (7) (8)

Có thể đơn giản hóa với quy tắc sau :

- Cho phép bỏ các số không (0) nằm phía trước trong mỗi nhóm
- Thay bằng 1 số 0 cho nhóm có giá trị bằng không
- Thay bằng :: cho các nhóm liên tiếp có giá trị bằng không

Như vậy địa chỉ ở Vd-1 có thể viết lại như sau :

Vd-2 : 2001:DB8:0:2F3B:2AA:FF:FE28:9C5A

Vd-3 : địa chỉ = FE80:**0:0:0:2AA:FF:FE9A:4CA2**  
Có thể viết lại = FE80::2AA:FF:FE9A:4CA2

**(\*) Lưu ý** : phần Giá trị đầu (Prefix) được xác định bởi Subnet Mask IPv6 tương tự IPv4

Vd-4 : 21DA:D3::/48      có Prefix = 21DA:D3:0 (48 bits)  
hoặc 21DA:D3:0:2F3B::/64 có Prefix = 21DA:D3:0:2F3B ( 64 bits)

### **Chú thích :**

Để không bị bỡ ngỡ, chúng ta nên lưu ý về một số khái niệm trước khi nói về địa chỉ của IPv6 Host

**a) Link-Local** : khái niệm chỉ về các Host kết nối cùng hệ thống thiết bị vật lý (tạm hiểu Hub, Switch)

**b) Site-Local** : khái niệm chỉ về các Host kết nối cùng Site

**c) Node** : điểm kết nối vào mạng (tạm hiểu là Network Adapter). Mỗi Node sẽ có nhiều IPv6 Address cần thiết (Interface Address) dùng cho các phạm vi (Scope), trạng thái (State), vận chuyển (Tunnel) khác nhau thay vì chỉ có 1 địa chỉ cần thiết như IPv4

**d) Do** vậy khi cài đặt IPv6 Protocol trên một Host, mỗi Network Adapter sẽ có nhiều IPv6 Address gán cho các Interface khác nhau

## **3-Các loại IPv6 Address**

### **a- Unicast**

Unicast Address dùng để định vị một Interface trong phạm vi các Unicast Address. Gói tin (Packet) có đích đến là Unicast Address sẽ thông qua Routing để chuyển đến 1 Interface duy nhất

### **b- Multicast**

Multicast Address dùng để định vị nhiều Interfaces. Packet có đích đến là Multicast Address sẽ thông qua Routing để chuyển đến tất cả các Interfaces có cùng Multicast Address

### **c-Anycast**

Anycast Address dùng để định vị nhiều Interfaces. Tuy vậy, Packet có đích đến là Anycast Address sẽ thông qua Routing để chuyển đến một Interfaces trong

số các Interface có cùng Anycast Address, thông thường là Interface gần nhất (khái niệm **Gần** ở đây được tính theo khoảng cách Routing)

Trong các trường hợp nêu trên, IPv6 Address được cấp cho Interface chứ không phải Node, một Node có thể được định vị bởi một trong số các Interface Address

IPv6 không có dạng Broadcast, các dạng Broadcast trong IPv4 được xem như tương đương Multicast trong Ipv6

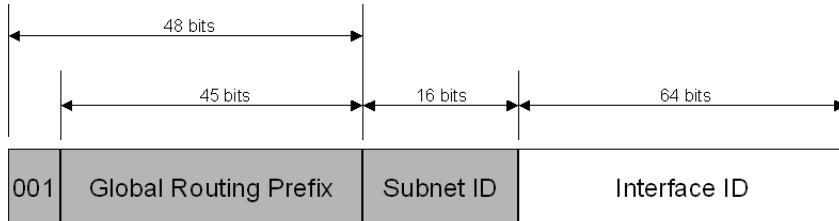
#### 4-Các loại IPv6 - Unicast Address

IPv6 Unicast Address gồm các loại :

- Global unicast addresses
- Link-local addresses
- Site-local addresses
- Unique local IPv6 unicast addresses
- Special addresses

##### a-Global unicast addresses (GUA)

GUA là địa chỉ IPv6 Internet (tương tự Public IPv4 Address). Phạm vi định vị của GUA là toàn bộ hệ thống IPv6 Internet (RFC 3587)



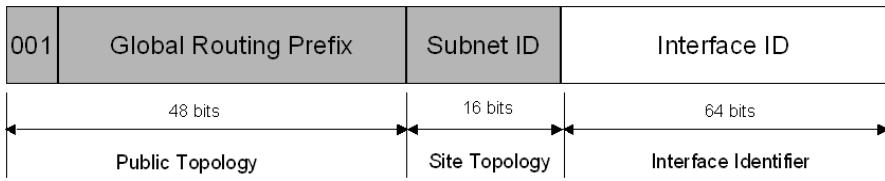
**001** : 3 bits đầu luôn có giá trị = 001 nhị phân (Binary – bin) (Prefix = 001 /3)

**Global Routing Prefix** : gồm 45 bits. Là địa chỉ được cấp cho một tổ chức, Công ty / Cơ quan ..(Organization) khi đăng ký IPv6 Internet Address (Public IP)

**Subnet ID** : gồm 16 bits. Là địa chỉ tự cấp trong tổ chức để tạo các Subnets

**Interface ID** : gồm 64 bits. Là địa chỉ của Interface trong Subnet

Có thể đơn giản hóa thành dạng như sau (Global Routing Prefix = 48 bits)



**(\*) Các địa chỉ Unicast trong nội bộ (Local Use Unicast Address)** : gồm 2 loại :

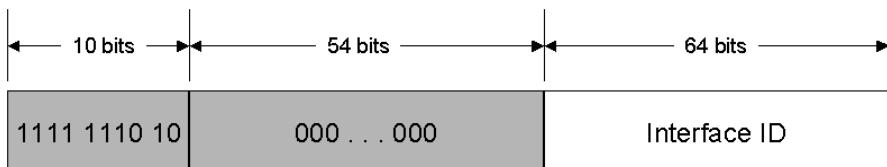
**Link-Local Addresses** : gồm các địa chỉ dùng cho các Host trong cùng Link và *Neighbor Discovery Process* (quy trình xác định các Nodes trong cùng Link)

**Site-Local Addresses** : gồm các địa chỉ dùng để các Nodes trong cùng Site liên lạc với nhau

### b-Link-local addresses (LLA)

LLA là địa chỉ IPv6 dùng cho các Nodes trong cùng Link liên lạc với nhau (tương tự các địa chỉ IPv4 = 169.254.X.X). Phạm vi sử dụng của LLA là trong cùng Link (do vậy có thể bị trùng lặp trong các Link)

Khi dùng HĐH Windows, LLA được cấp tự động với cấu trúc như sau :



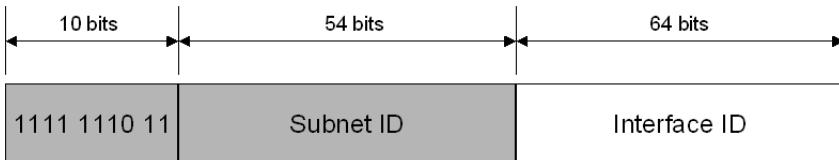
**64 bits đầu** = FE80 là giá trị cố định (Prefix = FE80 :: / 64)

**Interface ID** = gồm 64 bits . Kết hợp với Physical Address của Network Adapter (nói ở phần sau)

### c-Site-local addresses (SLA)

SLA tương tự các địa chỉ Private IPv4 (10.X.X.X, 172.16.X.X, 192.168.X.X) được sử dụng trong hệ thống nội bộ (Intranet). Phạm vi sử dụng SLA là trong cùng Site.

**(\*) Site** : là khái niệm để chỉ một phần của hệ thống mạng tại các tọa độ địa lý khác nhau



**1111 1110 11** = 10 bits đầu là giá trị cố định (Prefix = FEC0 /10)

**Subnet ID** : gồm 54 bits dùng để xác định các Subnets trong cùng Site

**Interface ID** : gồm 64 bits. Là địa chỉ của Interfaces trong Subnet

#### (\*) *Chú thích*

Với cấu trúc như trình bày ở phần trên, các Local Use Unicast Address (Link-local, Site Local) có thể bị trùng lặp (trong các Link khác, Site khác). Do vậy khi sử dụng các Local Use Unicasts có 1 thông số định vị được thêm vào (Additional Identifier) gọi là Zone\_ID với cú pháp :

Address%Zone\_ID

Vd-5 : **ping fe80::2b0:d0ff:fee9:4143%3**      Zone\_ID = %3. Trong đó :

Address = Local-Use Address (Link-Local / Site-Local)

Zone ID = giá trị nguyên, giá trị tương đương (so với Host) xác định Link hoặc Site.

Trong các Windows-Based IPv6 Host, Zone ID được xác định như sau :

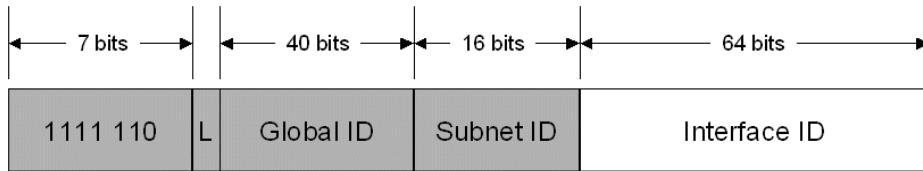
+ Đối với Link-Local Address (LLA) : Zone ID là số thứ tự của Interface (trong Host) kết nối với Link. Có thể xem bằng lệnh : **netsh interface ipv6 show interface**

+ Đối với Site-Local Address (SLA) : Zone ID là Site ID, được gán cho Site trong Organization. Đối với các Organization chỉ có 1 Site, Zone ID = Site ID = 1 và có thể xem bằng lệnh :

**netsh interface ipv6 show address level=verbose**

#### d-Unique- local addresses (ULA)

Đối với các Organization có nhiều Sites, Prefix của SLA có thể bị trùng lặp. Có thể thay thế SLA bằng ULA (RFC 4193), ULA là địa chỉ duy nhất của một Host trong hệ thống có nhiều Sites với cấu trúc:

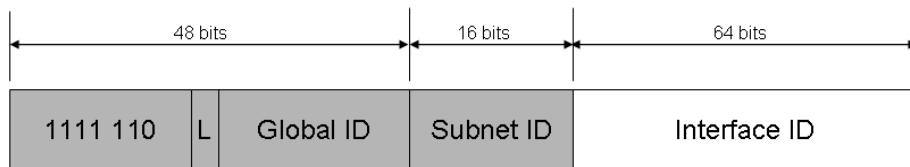
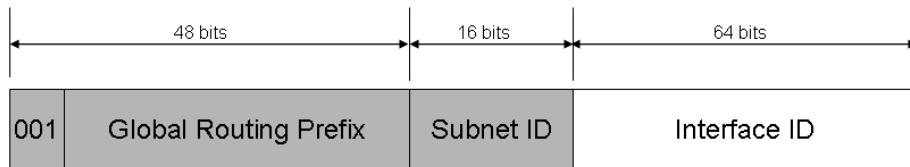


**111 110** : 7 bits đầu là giá trị cố định FC00/7. L=0 : Local → Prefix =FC00 /8

**Glocal ID** : địa chỉ Site (Site ID). Có thể gán tùy ý

**Subnet ID** : địa chỉ Subnet trong Site

Với cấu trúc này, ULA sẽ tương tự GUA và khác nhau ở phần Prefix như sau :



### e- Các địa chỉ đặc biệt (Special addresses)

Các địa chỉ đặc biệt trong IPv6 gồm :

**0:0:0:0:0:0:0:0** : địa chỉ không xác định (Unspecified address)

**0:0:0:0:0:0:0:1** : địa chỉ Loopback (tương đương IPv4 127.0.0.1)

**IPv4-Compatible Address (IPv4CA)** :

Format : **0:0:0:0:0:0:w.x.y.z** Trong đó w,x,y,z là các IPv4 Address

Vd : 0:0:0:0:0:0:192.168.1.2

IPv4CA là địa chỉ tương thích của một *IPv4/IPv6 Node*. Khi sử dụng IPv4CA như một IPv6 Destination, gói tin sẽ được đóng gói (Packet) với IPv4 Header để truyền trong môi trường IPv4

## **IPv4-mapped address (IPv4MA)**

Format : **0:0:0:0:FFFF:w.x.y.z** (::FFFF:w.x.y.z) Trong đó w,x,y,z là các IPv4 Address

Vd : 0:0:0:0:FFFF:192.168.1.2

IPv4MA là địa chỉ của một *IPv4 Only Node* đối với một IPv6 Node, IPv4MA chỉ có tác dụng thông báo và không được dùng như Resource hoặc Destination Address

## **6to4 Address**

Là địa chỉ sử dụng trong liên lạc giữa các IPv4/IPv6 nodes trong hệ thống hạ tầng IPv4 (IPv4 Routing Infrastructure). 6to4 được tạo bởi Prefix gồm 64 bits như sau :

Prefix = 2002/16 + 32 bits IPv4 Address =64 bits

6to4 Address là địa chỉ của Tunnel (Tunneling Address) định nghĩa bởi RFC 3056

## **5-Các loại IPv6 - Multicast Address**

Multicast Address của IPv6 Node có hoạt động tương tự Multicast trong IPv4. Một IPv6 Node có thể tiếp nhận tín hiệu của nhiều Multicast Address cùng lúc. IPv6 Node có thể tham gia hoặc rời khỏi một IPv6 Multicast Address bất kỳ lúc nào

Ví dụ về một số IPv6 Multicast Address được sử dụng :

FF01::1 (interface-local scope all-nodes multicast address)

FF02::1 (link-local scope all-nodes multicast address)

FF01::2 (interface-local scope all-routers multicast address)

FF02::2 (link-local scope all-routers multicast address)

FF05::2 (site-local scope all-routers multicast address)

## **Solicited-Node Address (SNA)**

Là địa chỉ sử dụng trong quy trình phân giải để cấp địa chỉ LLA (Link-Local Address) tự động cho các Node (tương tự quy trình tự cấp địa chỉ 169.254.X.X trong IPv4)

SNA có dạng : FF02:0:0:0:1:FF / 104 + 24 bits địa chỉ MAC

## 6-Các loại IPv6 - Anycast Address

Anycast Address có thể gán cho nhiều Interfaces, gói tin chuyển đến Anycast Address sẽ được vận chuyển bởi hệ thống Routing đến Interface gần nhất. Hiện nay, Anycast Address chỉ được dùng như *Destination Address* và gán cho các Router.

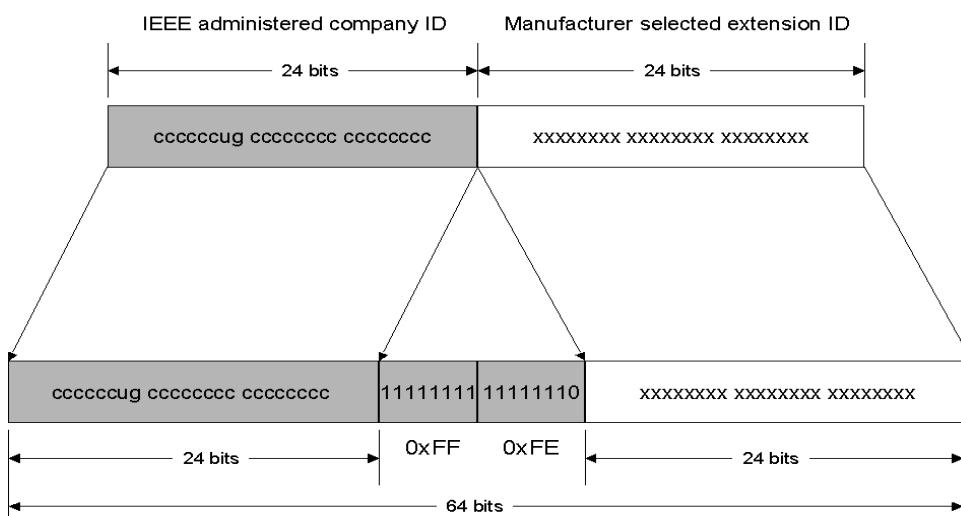
### IPv6 - Interface ID

Trong tất cả các loại địa chỉ nói trên đều có giá trị Interface ID dùng để xác định Interface. Giá trị Interface ID được xem xét và tạo nên theo các yếu tố sau :

- Xác định bởi Extended Unique Identifier (EUI)-64 Address (\*). EUI-64 Address có thể do gán hoặc kết hợp với MAC (physical) Address của Network Adapter (Window XP / Windows 2k3)
- Được gán tạm thời với giá trị ngẫu nhiên (\*\*) (RFC 3041)
- Được tạo thành bởi Link-layer address hoặc Serial Number khi cấu hình Point-to-Point Protocol (PPP)
- Tự cấp (manual address configuration)
- Là một giá trị phát sinh ngẫu nhiên và gán thường trực cho Interface (Windows Vista / LogHorn)

### Extended Unique Identifier (EUI)-64 Address (\*)

EUI-64 Address xác định phương thức tạo 64 bits Interface ID bằng cách kết hợp Mac Address của Network Adapter (48 bits) theo quy tắc như sau :



Mac Address = 6 nhóm 8 bits = 48 bits. Trong đó 24 bits là mã nhà sản xuất, 24 bits là mã số Adapter

Bước 1 : Tách đôi MAC Address làm 2 nhóm (mỗi nhóm 24 bits), chèn vào giữa 16 bits giá trị FFFE

Bước 2 : Đảo ngược giá trị bit thứ 7 của nhóm đầu

Ví dụ : Network Adapter có MAC address = 00-AA-00-3F-2A-1C

Bước 1 → 00-AA-00-**FF:FE**-3F-2A-1C

Bước 2 → 02-AA-00-FF-FE-3F-2A-1C → Interface ID =

**02AA:00FF:FE3F:2A1C** (64 bits)

#### Bảng so sánh tương đương giữa IPv4 và IPv6

IPv4 Address	IPv6 Address
Internet address classes	Not applicable in IPv6
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
Autoconfigured addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
Text representation: Dotted decimal notation	Text representation: Colon hexadecimal format with suppression of leading zeros and zero compression. IPv4-compatible addresses are expressed in dotted decimal notation.
Network bits representation: Subnet mask in dotted decimal notation or prefix length	Network bits representation: Prefix length notation only
DNS name resolution: IPv4 host address (A) resource record	DNS name resolution: IPv6 host address (AAAA) resource record
DNS reverse resolution: IN-ADDR.ARPA domain	DNS reverse resolution: IP6.ARPA domain

Bài 38:

## **OSPF, cung có kiến thức lại nào.**

Distance vector và link state

Khi ta học về giao thức distance vector thì router học đường đi nhờ neighbors [định tuyến theo tin đồn, neighbors bảo gì nghe nấy như RIP]. Giao thức distance chỉ tin cậy thông tin route của neighbor.

Học qua EIGRP thì có tiến bộ hơn tí là nó nghe tin đồn nhưng nó còn xác nhận lại để xem có đúng hay không [ở đây là xem đường nào tốt hơn]. EIGRP thì nhanh hơn nhưng chỉ hỗ trợ sản phẩm cisco.

Có một giao thức khác khá hơn 2 cái kia nhưng hơi tốn performance một chút, hỗ trợ đa chủng loại sản phẩm là OSPF. OSPF thì không nghe tin đồn như những giao thức kia mà nó lấy toàn bộ thông tin về state [trạng thái: links của router đó, interfaces, những neighbor của router đó, và trạng thái up/down, ip, subnet, ...] của thằng gốc copy vào link state database của nó rồi tự tìm ra đường đi tốt nhất cho mình bằng thuật toán shortest-path-first [hay còn gọi là Dijkstra].

**Những con biên [ABR: area border router] nằm giữa nhiều biên có bản topology cho nhiều vùng khác nhau. Nó chỉ gửi tuyến route summary từ area khác ra cho area0 [backbone].**

Nhưng trước khi trao đổi thông tin thì nó cần phải thiết lập một mối qua hệ gọi là neighbor. Quan hệ neighbor sẽ được thiết lập nhờ vào gói những gói hellos.

Khi router nhận gói hello từ neighbor thì nó kiểm tra:

- Area ID
- Authentication
- Networkmask [subnet mask phải giống nhau]
- HelloInterval, DeadInterval timer [trong môi trường broadcast là hello 10', và Nonbroadcast là 40'. DeadInterval gấp 4 lần hello]. Sau thời gian dead mà không nhận được hello thì bỏ neighbors.
- Cờ stub
- Và một số option cấu hình trên interface nhận vào gói hello.

Khi trở thành neighbor thì các router có thể trao đổi các gói update cho nhau. Nhưng nếu như vậy thì sẽ tốn một lượng băng thông rất lớn vì một con sẽ cần trao đổi với tất cả các con còn lại.

=> Có  $n(n-1)/2$  các quan hệ gần [adjacencies] với nhau.

Vì vậy cần tồn tại một quá trình để bầu chọn con chính [DR], chỉ có con chính là quan hệ được với các con khác, và một con phụ là BDR để backup con chính khi nó chết.

	Broadcast	NBMA	Point-to-multipoint	Virtual links	Point-to-point
Bầu chọn DR/BDR	Yes	Yes	No	Like Point-to-point	No
Update by	224.0.0.5: All Router 224.0.0.6:DR/BDR	All packet unicast	Unicast	Unicast over virtual-link	224.0.0.5

### Quá trình bầu chọn DR, BDR có thể xảy ra trên môi trường Broadcast và NBMA networks.

Quá trình hình thành full adjacency có thể diễn ra qua 7 quá trình cơ bản sau.  
Có 2 router A và B với Router ID tương ứng là a và b.

#### 1. Down state

Hai router mới gắn vào và cấu hình thì ở trạng thái **Down state**  
[router không nhận được thông tin từ router cận kề]

#### 2. Init State

Chỉ có 1 router gửi gói tin hello và router kia nhận được nhưng chưa biết router ID của chính nó nên chỉ là 1 chiều. [one way]

#### 3. Two-way state

1 router gửi có router ID của nó, router kia nhận được và hồi đáp lại với router ID của nó. Ở trong trạng thái này nếu ở môi trường Ethernet [hay còn gọi là multiaccess, hoặc broadcast] cũng bầu chọn luôn DR và BDR.

\*\*Router có ưu tiên lớn nhất là DR, lớn nhì là BDR.

Ưu tiên theo thứ tự sau:

- cấu hình priority [ip ospf priority]
- cấu hình router ID bằng lệnh [router ID]
- Loopback có IP cao nhất
- interface vật lý có IP cao nhất

Router có priority là 0 thì không tham gia vào quá trình bầu chọn DR/BDR.

Bài 39:

### Tại sao interface serial không nhận được IP động từ DHCP-server?

#### Câu hỏi:

Trong khi cấu hình DHCP Relay thì câu lệnh IP helper address A.B.C.D(địa chỉ của con DHCP) chỉ tác dụng trong kết nối Ethernet(FastEthernet), còn trong kết nối Serial thì không được?

Và khi cấu hình DHCP client trên Router, mình cấu hình trên cổng Ethernet thì nó support còn trong kết nối Serial thì lại không nhỉ?.

#### Trả lời:

Câu trả lời cho vấn đề này là để cấp IP cho client thì DHCP server cần biết MAC của client để nó có thể lưu trong cơ sở dữ liệu của nó. Sau này nếu client có xin IP cũng dựa vào bảng này mà cấp phát lại IP cho client.

```
DHCP#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/           Lease expiration      Type
                  Hardware address/
                  User name
192.168.20.1        0063.6973.636f.2d30.   Mar 02 2002 12:00 AM  Automatic
                   3061.612e.3030.6161.
                   2e30.3061.612d.4661.
                   302f.30
```

Nhưng **serial** là dạng point-to-point và **không có MAC**, cho nên nó không thể xin IP từ DHCP server được. Do đó không có lệnh **ip address dhcp** hỗ trợ cho nó.

Đối với interface Ethernet, ta có thể xin địa chỉ IP mới nhằm mục đích test cho các bài Lab bằng cách sau.

```
R1(config)#int f0/0
R1(config-if)#mac-address aa.aa.aa
R1(config-if)#shut
R1(config-if)#no sh
```

Sẵn tiện đây mình cũng trích một chút của CCNA về 2 dạng đóng gói phổ biến của interface serial.

Mặc định serial sẽ có dạng **HDLC**.

```
R1#sh int s1/0
Serial1/0 is up, line protocol is up
Hardware is M4T
Internet address is 1.1.1.2/8
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
```

```
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:05, output 00:00:07, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
97 packets input, 7396 bytes, 0 no buffer
Received 93 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
116 packets output, 9881 bytes, 0 underruns
0 output errors, 0 collisions, 5 interface resets
0 output buffer failures, 0 output buffers swapped out
7 carrier transitions DCD=up DSR=up DTR=up RTS=up CTS=up
```

Một dạng tiên tiến hơn so với HDLC là **PPP**. Ta có thể cấu hình interface serial thành dạng PPP bằng lệnh sau.

```
R1(config)#int serial 1/0
R1(config-if)#encapsulation ppp
```

```
R1#sh interfaces serial 1/0
Serial1/0 is up, line protocol is down
Hardware is M4T
Internet address is 1.1.1.2/8
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Listen, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:04, output 00:00:02, output hang never
Last clearing of "show interface" counters 00:01:10
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
8 packets input, 184 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort  
20 packets output, 280 bytes, 0 underruns  
0 output errors, 0 collisions, 2 interface resets  
0 output buffer failures, 0 output buffers swapped out  
2 carrier transitions DCD=up DSR=up DTR=up RTS=up CTS=up
```

HDLC chỉ chạy được IP (không hỗ trợ IPX, apple talk, ...)

PPP thêm vào trường để hỗ trợ thêm các giao thức IPX, apple talk, ...

PPP(layer 2) gồm có 2 trường chính:

+ NCP:giao tiếp để biết IP, IPX, ... để đóng gói cho chính xác.

+ LCP đóng gói khởi tạo đường link, gồm 5 phần nhỏ bên trong:

- Authentication: PAP: bắt tay 2 bước, không mã hóa /CHAP: bắt tay 3 bước và mã hóa MD5.

- Compress: nén

- Multilink: gom nhiều đường lại với nhau làm tăng bandwidth lên.

- Error detection: kiểm tra lỗi

- Callback.

---

Bài 40:

## **BẢO MẬT MẠNG WLAN**

- Mạng WLAN bản thân nó là không bảo mật, tuy nhiên, đối với mạng có dây nếu bạn không có một sự phòng ngừa hay cấu hình bảo vệ nào thì nó cũng chẳng bảo mật gì. Điểm mấu chốt để tạo ra một mạng WLAN bảo mật và giữ nó an toàn là việc đào tạo những người triển khai và quản lý mạng WLAN. Đào tạo những nhà quản trị về mức độ bảo mật cơ bản và nâng cao cho mạng WLAN là một điều cốt yếu để ngăn chặn những lỗ hổng bảo mật trong mạng WLAN.

### **I. Wired Equivalent Privacy (WEP):**

- WEP là một thuật toán mã hóa được sử dụng bởi tiến trình xác thực Shared Key Authentication để xác thực người dùng và mã hóa dữ liệu trên phân đoạn không dây của mạng LAN. Chuẩn 802.11 yêu cầu sử dụng WEP như là một phương thức bảo mật cho mạng không dây.

- WEP là một thuật toán đơn giản sử dụng bộ phát sinh số giả ngẫu nhiên (**PRNG = Pseudo-Random Number Generator**) và mã hóa dòng (*stream cipher*) RC4. Trong nhiều năm, thuật toán này được xem như là một bí mật thương mại và chi tiết về nó là không được tiết lộ, nhưng vào tháng 9 năm 1994, một người nào đó đã phát tán mã nguồn của nó trên các mailing list. RC4 thuộc sở hữu thương mại của RSADSL. Mã hóa dòng RC4 là khá nhanh để giải mã và mã hóa, vì thế nó tiết kiệm được CPU, RC4 cũng đủ đơn giản để các nhà phát triển phần mềm lập trình nó vào trong sản phẩm của mình.

- Chúng ta nói WEP là đơn giản, điều đó có nghĩa là nó khá yếu. Thuật toán

RC4 được cài đặt một cách không thích hợp vào WEP tạo nên một giải pháp bảo mật thấp hơn mức vừa đủ cho mạng 802.11. Cả 64 bit và 128 bit WEP đều có mức độ yếu kém như nhau trong việc cài đặt **24 bit IV (Initialization Vector)** và cùng sử dụng tiến trình mã hóa có nhiều lỗ hổng. Tiến trình này khởi tạo giá trị ban đầu cho IV là 0, sau đó tăng IV lên 1 khi mỗi gói được truyền. Trong một mạng thường xuyên nghẽn, những phân tích thống kê cho thấy rằng tất cả các giá trị IV có thể ( $2^{24}$ ) sẽ được sử dụng hết chỉ trong  $\frac{1}{2}$  ngày, điều đó có nghĩa là IV sẽ khởi tạo lại từ 0 ít nhất một lần trong ngày. Điều này tạo ra lỗ hổng cho các hacker. Khi WEP được sử dụng, IV sẽ được truyền đi (mà không mã hóa) cùng với mỗi gói tin (đã mã hóa). Cách làm này tạo nên những lỗ hổng bảo mật sau:

- + Tấn công chủ động để chèn traffic mới: Các trạm di động không đặc quyền (chưa được quyền, unauthorized) có thể chèn các gói tin vào mạng dựa trên chuỗi dữ liệu biết trước.
- + Tấn công chủ động để giải mã traffic: Dựa trên việc lừa gạt AP
- + Tấn công bằng cách xây dựng từ điển (*Dictionary-building*): Sau khi thu thập đầy đủ traffic thì WEP key có thể bị crack dùng các phần mềm miễn phí. Một khi WEP key đã bị crack thì việc giải mã các gói tin theo thời gian thực có thể được thực hiện bằng cách lắng nghe các gói tin được quản bá, sau đó dùng WEP key để giải mã chúng.
- + Tấn công bị động để giải mã traffic: Bằng cách sử dụng những phân tích thống kê, WEP traffic có thể bị giải mã.

### **1. Tại sao WEP được chọn:**

- Nếu như WEP không bảo mật như vậy thì tại sao nó được chọn để cài đặt trong chuẩn 802.11? Khi chuẩn 802.11 được hoàn tất và thông qua, các nhà sản xuất thiết bị WLAN bắt đầu đưa sản phẩm của họ ra thị trường. Chuẩn 802.11 xác định rằng thiết bị phải bảo đảm các tiêu chuẩn về bảo mật sau:

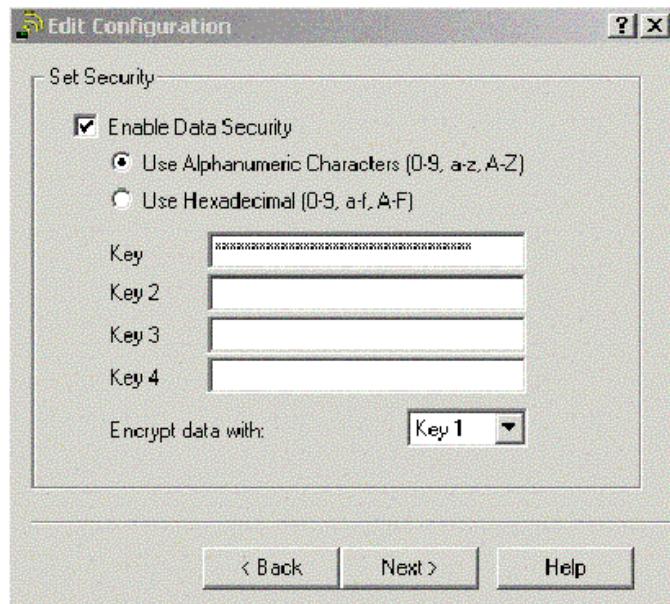
- + Có thể xuất được (exportable)
- + Khá mạnh (reasonable strong)
- + Tự đồng bộ hóa (self-synchronizing)
- + Tính toán một cách hiệu quả (computationally efficient)
- + Tùy chọn (optional)
  - Và WEP đã thỏa mãn được tất cả các yêu cầu này. Khi WEP được cài đặt, nó dự định sẽ hỗ trợ các mục tiêu bảo mật như tính tin cậy (*confidentiality*), điều khiển truy cập, và tính toàn vẹn (*integrity*) dữ liệu. Điều thật sự xảy ra là có quá nhiều nhà phê chuẩn nghĩ rằng chỉ đơn giản là cài đặt WEP và chúng ta sẽ có một giải pháp bảo mật toàn diện cho WLAN. Nhưng họ cũng nhanh chóng nhận ra rằng WEP không phải là một giải pháp toàn diện cho bảo mật WLAN. Nhưng thật may mắn cho ngành công nghiệp không dây vì các thiết bị WLAN đã rất phổ biến trước khi những vấn đề này được biết đến, điều này đã làm cho nhiều nhà sản xuất và các tổ chức thứ 3 kết hợp với nhau để tạo ra các giải pháp bảo mật cho WLAN.
  - Chuẩn 802.11 để lại việc cài đặt WEP tùy thuộc vào các nhà sản xuất. Vì thế các nhà sản xuất cài đặt WEP key có thể giống hoặc khác nhau là cho WEP có phần nào đó yếu đi. Thậm chí, chuẩn tương thích wi-fi của

WECA chỉ kiểm tra 40 bit WEP key. Một số nhà sản xuất WLAN đã tìm cách mở rộng WEP trong khi một số khác lại sử dụng các chuẩn mới như 802.1X với EAP hay VPN. Có nhiều giải pháp trên thị trường khắc phục được những yếu điểm của WEP.

## 2. WEP key:

- Chức năng chính của WEP dựa trên các key, là các yếu tố cơ bản cho thuật toán mã hóa. WEP key được cài đặt vào client và các thiết bị hạ tầng trong mạng WLAN. Một WEP key là một chuỗi ký tự và số được sử dụng theo 2 cách. Thứ nhất, WEP key có thể được sử dụng để kiểm tra định danh xác thực client. Thứ 2, WEP key có thể được dùng để mã hóa dữ liệu.
- Khi một client sử dụng WEP có gắng xác thực và kết nối với AP thì AP sẽ xác định xem client có giá trị WEP key chính xác hay không. Chính xác ở đây có nghĩa là client đã có key là một phần của hệ thống phân phát WEP key được cài đặt trong WLAN. WEP key phải khớp ở cả 2 đầu xác thực (AP và Client).
- Một nhà quản trị WLAN có thể phân phát WEP key một cách thủ công hay sử dụng các phương thức cấp cao như hệ thống phân phát WEP key. Hệ thống phân phát WEP key có thể đơn giản chỉ là việc cài đặt các key tĩnh hay cao cấp hơn như sử dụng các server mã hóa key tập trung. Rõ ràng là các giải pháp cao cấp hơn sẽ gây ra khó khăn hơn cho các hacker khi muốn đột nhập vào mạng,
- Có 2 loại WEP key là **64 bit** và **128 bit** (đôi khi bạn thường nghe nhắc đến là **40 bit** và **104 bit**). Điều này gây ra sự hiểu nhầm. Lý do cho sự hiểu nhầm này là WEP được cài đặt theo cách giống nhau cho cả 2 kích thước mã hóa kể trên. Mỗi WEP key đều sử dụng **24 bit IV** kết nối với key bí mật. Chiều dài của key bí mật là 40 hoặc 104 bit, vì thế tạo thành WEP key 64 và 128 bit.
- Việc nhập WEP key tĩnh vào client hay các thiết bị hạ tầng như Bridge hay AP là hoàn toàn đơn giản. Đôi khi, sẽ có một checkbox để chọn chiều dài WEP key sử dụng, đôi khi không có checkbox nào, vì thế admin phải biết phải nhập vào bao nhiêu ký tự khi được yêu cầu. Thông thường các phần mềm client sẽ cho phép nhập vào WEP key theo dạng ký tự số (**ASCII**) hay theo dạng thập lục phân (**HEX**)

FIGURE 10.1 Entering WEP keys on client devices



- Số ký tự nhập vào cho key bí mật tùy thuộc vào phần mềm cấu hình yêu cầu dạng ASCII hay HEX và sử dụng 64 bit hay 128 bit. Nếu card không dây của bạn hỗ trợ 128 bit, thì nó cũng hỗ trợ 64 bit. Nếu bạn nhập WEP key theo định dạng ASCII thì bạn sẽ phải nhập **5 ký tự** cho 64 bit và **13 ký tự** cho 128 bit. Nếu bạn nhập theo dạng HEX thì phải nhập **10 ký tự** cho 64 bit và **26 ký tự** cho 128 bit.

## 2.1 WEP Key tĩnh (static):

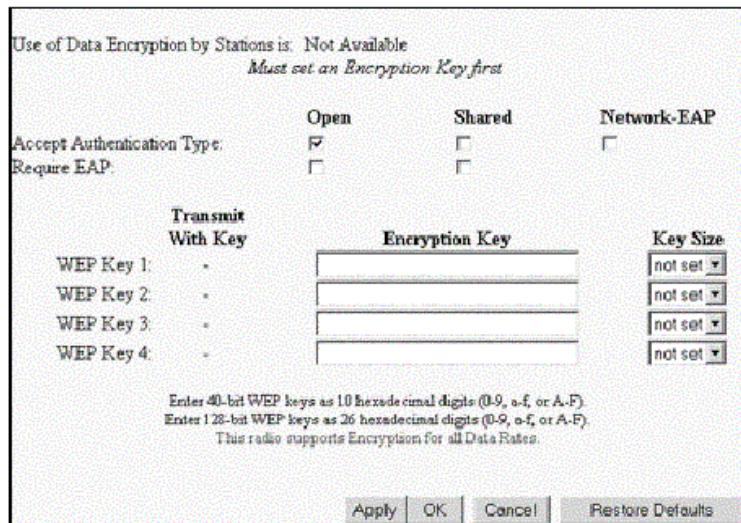
- Nếu bạn chọn cài đặt WEP key tĩnh, bạn sẽ phải gán các WEP key tĩnh này một cách thủ công cho các AP và các client. Các WEP key này sẽ không bao giờ thay đổi làm cho đoạn mạng đó dễ bị hacker tấn công. Vì lý do này mà WEP key tĩnh chỉ thích hợp sử dụng như là một phương thức bảo mật căn bản cho các mạng WLAN nhỏ, đơn giản. Nó không được khuyến khích sử dụng cho các doanh nghiệp lớn.

- Khi sử dụng WEP key tĩnh, mạng sẽ có rất nhiều sơ hở. Hãy xem xét trường hợp một nhân viên rời khỏi công ty và làm mất card mạng không dây của họ. Vì WEP key được lưu trữ trong firmware của card mạng nên card đó vẫn có thể truy cập vào mạng không dây chừng nào WEP key trên WLAN chưa thay đổi.

- Hầu hết các AP và client có khả năng lưu trữ 4 WEP key đồng thời. Một lý do hữu ích cho việc có nhiều WEP key chính là việc phân đoạn (segment) mạng. Giả sử rằng mạng có 100 client, sử dụng 4 WEP key thay vì 1 sẽ phân người dùng vào 4 nhóm khác nhau, mỗi nhóm 25 người dùng. Nếu WEP key bị crack thì điều đó có nghĩa là chỉ cần thay đổi WEP key cho 25 client và AP thay vì phải thay đổi toàn bộ mạng.

- Một lý do khác để có nhiều WEP key là trong môi trường hỗn hợp các card hỗ trợ 128 bit và các card chỉ hỗ trợ 64 bit. Trong trường hợp này, chúng ta có thể phân ra 2 nhóm người dùng.

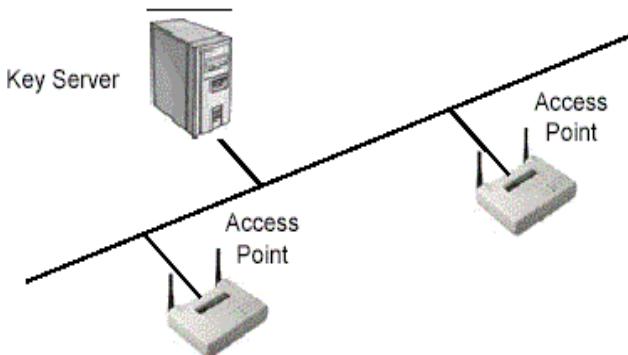
**Figure 10.2** Entering WEP keys on infrastructure devices



## 2.2 Server mã hóa key tập trung:

- Các doanh nghiệp sử dụng WEP key như là một phương thức bảo mật cơ bản cho WLAN thì nên sử dụng các server mã hóa key tập trung nếu có thể vì các lý do sau:
  - + Sinh khóa tập trung (centralized key generation)
  - + Phân phát khóa tập trung (Centralized key distribution)
  - + Tự động quay vòng khóa lúc sử dụng (ongoing key rotation)
  - + Giảm chi phí quản lý khóa
- Bất cứ một thiết bị nào cũng có thể hoạt động như là một server key tập trung. Thường thì một server như RADIUS server hay các server ứng dụng chuyên biệt sẽ đảm nhận việc phát sinh WEP key mới trong thời gian sử dụng. Bình thường, khi sử dụng WEP, key (được gán bởi admin) sẽ được nhập một cách thủ công vào client và AP. Khi sử dụng server key tập trung thì một tiến trình tự động giữa client, AP và Server sẽ thực hiện tác vụ phân phát key.

**FIGURE 10.3** Centralized Encryption Key Server



- Server mã hóa key tập trung cho phép tự động sinh key theo từng gói tin (per-packet), từng phiên làm việc (per-session) ... tùy thuộc vào cài đặt của nhà sản xuất. Việc phân phát WEP key theo per-packet sẽ sinh ra một WEP key mới

cho cả 2 đầu kết nối đối với từng gói tin được truyền đi, trong khi per-session sử dụng WEP key mới cho mỗi phiên làm việc giữa các node. Chú ý là việc sử dụng per-packet sẽ ngắn nhiều băng thông mạng hơn là per-session.

### **2.3 Sử dụng WEP:**

- Khi WEP được khởi tạo, phần dữ liệu của gói tin truyền sẽ được mã hóa, tuy nhiên, một phần header của gói tin (bao gồm MAC address) là không được mã hóa. Tất cả những thông tin lớp 3 bao gồm địa chỉ nguồn, địa chỉ đích đều được mã hóa bởi WEP. Khi một AP gửi ra một Beacon trong mạng WLAN sử dụng WEP, Beacon này cũng không được mã hóa. Hãy lưu ý là Beacon không chứa thông tin lớp 3 nào.

- Khi các gói tin được gửi sử dụng mã hóa WEP, những gói tin đó phải được giải mã mới có thể sử dụng được. Việc giải mã này làm tiêu tốn tài nguyên CPU và giảm hiệu quả băng thông trên WLAN đôi khi là rất đáng kể. Một số nhà sản xuất đã cài đặt thêm CPU vào AP của họ nhằm mục đích thực hiện mã hóa và giải mã WEP. Nhiều nhà sản xuất cài đặt mã hóa và giải mã WEP bằng phần mềm và sử dụng chung CPU cho việc quản lý AP, truyền gói tin ...

Những AP này sẽ bị ảnh hưởng lớn nếu như có sử dụng WEP. Bằng việc cài đặt WEP trong phần cứng thì có vẻ như là AP sẽ duy trì được băng thông 5 Mbps (hay nhiều hơn) khi WEP được sử dụng. Điểm bất lợi của giải pháp này là nó làm tăng chi phí cho các AP cấp cao.

- WEP có thể được triển khai như là một cơ chế bảo mật cơ bản nhưng nhà quản trị mạng cần phải biết những yếu điểm của WEP và cách khắc phục chúng. Admin cũng nên biết rằng mỗi nhà sản xuất khác nhau sẽ cài đặt WEP khác nhau làm cho việc sử dụng sản phẩm của nhiều nhà sản xuất khác nhau gặp khó khăn.

### **3. Advantage Encryption Standard (AES):**

- AES đã đạt được một sự chấp nhận như là một sự thay thế xứng đáng cho thuật toán RC4 được sử dụng trong WEP. AES sử dụng thuật toán Rijndale có chiều dài key lần lượt là 128 bit, 192 bit và 256 bit

- AES được xem như là không thể crack được bởi hầu hết các chuyên gia mật mã và National Institute of Standard and Technology (NIST) đã chọn sử dụng AES cho chuẩn xử lý thông tin liên bang (FIPS = Federal Information Processing Standard). Như là một phần của nỗ lực cải tiến chuẩn 802.11, ban làm việc 802.11i đã xem xét sử dụng AES trong phiên bản WEPv2

- AES được thông qua bởi nhóm làm việc 802.11i để sử dụng trong WEPv2 sẽ được cài đặt trong firmware và software bởi các nhà sản xuất. AP firmware và Client firmware (PCMCIA card) sẽ phải nâng cấp lên để có thể hỗ trợ AES. Các phần mềm trên client (driver và ứng dụng) sẽ hỗ trợ cấu hình AES với key bí mật.

## CÁC KIỀU TẤN CÔNG TRÊN MẠNG WLAN

- Hacker có thể tấn công mạng WLAN bằng các cách sau:
  - + Passive Attack (eavesdropping)
  - + Active Attack (kết nối, thăm dò và cấu hình mạng)
  - + Jamming Attack
  - + Man-in-the-middle Attack

- Các phương pháp tấn công trên có thể được phối hợp với nhau theo nhiều cách khác nhau

### 1. Passive Attack (eavesdropping):

- Tấn công bị động (passive) hay nghe lén (eavesdropping) có lẽ là một phương pháp tấn công WLAN đơn giản nhất nhưng vẫn rất hiệu quả. Passive attack không để lại dấu vết nào chứng tỏ đã có sự hiện diện của hacker trong mạng vì hacker không thật kết nối với AP để lắng nghe các gói tin truyền trên đoạn mạng không dây. WLAN sniffer hay các ứng dụng miễn phí có thể được sử dụng để thu thập thông tin về mạng không dây ở khoảng cách xa bằng cách sử dụng anten định hướng. Phương pháp này cho phép hacker giữ khoảng cách với mạng, không để lại dấu vết trong khi vẫn lắng nghe và thu thập được những thông tin quý giá.

- Có nhiều ứng dụng có khả năng thu thập được password từ những địa chỉ HTTP, email, instant message, phiên làm việc FTP, telnet. Nhiều kiểu kết nối trên đều truyền password theo dạng clear text (không mã hóa). Nhiều ứng dụng có thể bắt được password hash (mật mã đã được băm) truyền trên đoạn mạng không dây giữa client và server lúc client đăng nhập vào. Bất kỳ thông tin nào truyền trên đoạn mạng không dây theo kiểu này đều rất dễ bị tấn công bởi hacker. Hãy xem xét những tác động nếu như hacker có thể đăng nhập vào mạng bằng thông tin của một người dùng nào đó và gây ra những thiệt hại cho mạng. Hacker là thủ phạm nhưng những thông tin log được lại chỉ đến người dùng mà hacker đã đăng nhập vào. Điều này có thể làm cho nhân viên đó mất việc.

- Một hacker có thể ở đâu đó trong bãi đậu xe, dùng những công cụ để đột nhập vào mạng WLAN của bạn. Các công cụ có thể là một packet sniffer, hay một số phần mềm hacking miễn phí để có thể crack được WEP key và đăng nhập vào mạng.

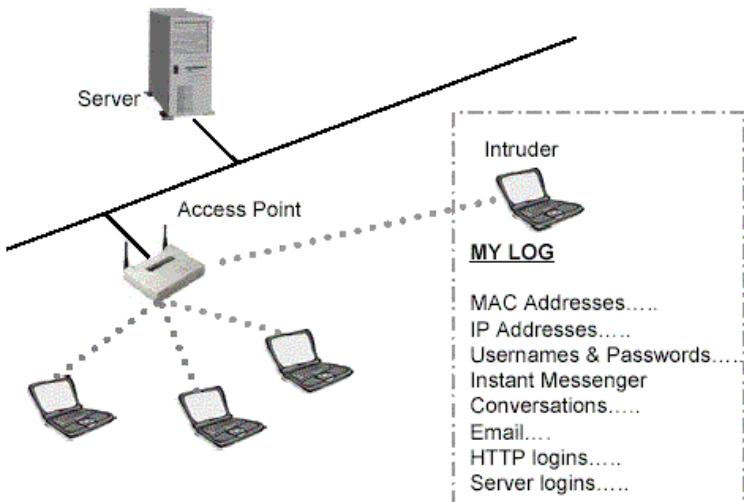
### 2. Active Attack:

- Hacker có thể tấn công chủ động (active) để thực hiện một số tác vụ trên mạng. Một cuộc tấn công chủ động có thể được sử dụng để truy cập vào server và lấy được những dữ liệu có giá trị hay sử dụng đường kết nối Internet của doanh nghiệp để thực hiện những mục đích phá hoại hay thậm chí là thay đổi cấu hình của hạ tầng mạng. Bằng cách kết nối với mạng không dây thông qua AP, hacker có thể xâm nhập sâu hơn vào mạng hoặc có thể thay đổi cấu hình

của mạng. Ví dụ, một hacker có thể sửa đổi để thêm MAC address của hacker vào danh sách cho phép của MAC filter trên AP hay vô hiệu hóa tính năng MAC filter giúp cho việc đột nhập sau này dễ dàng hơn. Admin thậm chí không biết được thay đổi này trong một thời gian dài nếu như không kiểm tra thường xuyên.

- Một số ví dụ điển hình của active attack có thể bao gồm các Spammer hay các đối thủ cạnh tranh muốn đột nhập vào cơ sở dữ liệu của công ty bạn. Một spammer (kẻ phát tán thư rác) có thể gửi một lúc nhiều mail đến mạng của gia đình hay doanh nghiệp thông qua kết nối không dây WLAN. Sau khi có được địa chỉ IP từ DHCP server, hacker có thể gửi cả ngàn bức thư sử dụng kết nối internet của bạn mà bạn không hề biết. Kiểu tấn công này có thể làm cho ISP của bạn ngắt kết nối email của bạn vì đã lạm dụng gửi nhiều mail mặc dù không phải lỗi của bạn.

**FIGURE 10.6** Passive Attack Example



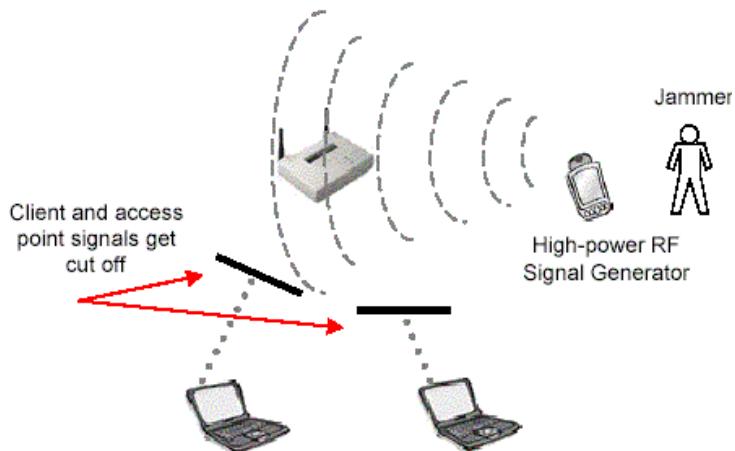
- Đối thủ cạnh tranh có thể muốn có được danh sách khách hàng của bạn cùng với những thông tin liên hệ hay thậm chí là bảng lương để có mức cạnh tranh tốt hơn hay giành lấy khách hàng của bạn. Những kiểu tấn công này xảy ra thường xuyên mà admin không hề hay biết.

- Một khi hacker đã có được kết nối không dây vào mạng của bạn, hắn có thể truy cập vào server, sử dụng kết nối WAN, Internet hay truy cập đến laptop, desktop người dùng. Cùng với một số công cụ đơn giản, hacker có thể dễ dàng thu thập được những thông tin quan trọng, giả mạo người dùng hay thậm chí gây thiệt hại cho mạng bằng cách cấu hình sai. Dò tìm server bằng cách quét công, tạo ra phiên làm việc NULL để chia sẻ hay crack password, sau đó đăng nhập vào server bằng account đã crack được là những điều mà hacker có thể làm đối với mạng của bạn.

### 3. Jamming (tấn công bằng cách gây nghẽn):

- Jamming là một kỹ thuật được sử dụng chỉ đơn giản để làm hỏng (shut down) mạng không dây của bạn. Tương tự như những kẻ phá hoại sử dụng tấn công DoS vào một web server làm nghẽn server đó thì mạng WLAN cũng có thể bị shut down bằng cách gây nghẽn tín hiệu RF. Những tín hiệu gây nghẽn này có thể là có ý hay vô ý và có thể loại bỏ được hay không loại bỏ được. Khi một hacker chủ động tấn công jamming, hacker có thể sử dụng một thiết bị WLAN đặc biệt, thiết bị này là bộ phát tín hiệu RF công suất cao hay sweep generator.
- Để loại bỏ kiểu tấn công này thì yêu cầu đầu tiên là phải xác định được nguồn tín hiệu RF. Việc này có thể làm bằng cách sử dụng một Spectrum Analyzer (máy phân tích phổ). Có nhiều loại Spectrum Analyzer trên thị trường nhưng bạn nên dùng loại cầm tay, dùng pin cho tiện sử dụng. Một cách khác là dùng các ứng dụng Spectrum Analyzer phần mềm kèm theo các sản phẩm WLAN cho client.

FIGURE 10.8 Jamming Attack Example

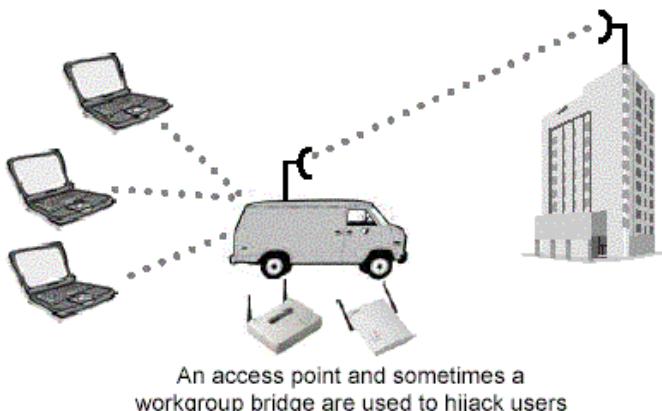


- Khi nguồn gây ra jamming là không thể di chuyển được và không gây hại như tháp truyền thông hay các hệ thống hợp pháp khác thì admin nên xem xét sử dụng dãy tần số khác cho mạng WLAN. Ví dụ, nếu admin chịu trách nhiệm thiết kế và cài đặt mạng WLAN cho môi trường rộng lớn, phức tạp thì cần phải xem xét kỹ càng. Nếu như nguồn nhiễu RF trải rộng hơn 2.4 Ghz như bộ đàm, lò vi sóng ... thì admin nên sử dụng những thiết bị theo chuẩn 802.11a hoạt động trong băng tần 5 Ghz UNII thay vì sử dụng những thiết bị 802.11b/g hoạt động trong băng tần 2.4 Ghz sẽ dễ bị nhiễu.
- Jamming do vô ý xuất hiện thường xuyên do nhiều thiết bị khác nhau chia sẻ chung băng tần 2.4 ISM với mạng WLAN. Jamming một cách chủ động thường không phổ biến lắm, lý do là bởi vì để thực hiện được jamming thì rất tốn kém, giá của thiết bị rất mắc tiền, kết quả đạt được chỉ là tạm thời shut down mạng trong thời gian ngắn.

#### 4. Man-in-the-middle Attack:

- Tấn công theo kiểu Man-in-the-middle là trường hợp trong đó hacker sử dụng một AP để đánh cắp các node di động bằng cách gửi tín hiệu RF mạnh hơn AP hợp pháp đến các node đó. Các node di động nhận thấy có AP phát tín hiệu RF tốt hơn nên sẽ kết nối đến AP giả mạo này, truyền dữ liệu có thể là những dữ liệu nhạy cảm đến AP giả mạo và hacker có toàn quyền xử lý.
- Để làm cho client kết nối lại đến AP giả mạo thì công suất phát của AP giả mạo phải cao hơn nhiều so với AP hợp pháp trong vùng phủ sóng của nó. Việc kết nối lại với AP giả mạo được xem như là một phần của roaming nên người dùng sẽ không hề biết được. Việc đưa nguồn nhiễu toàn kênh (all-band interference - chẳng hạn như bluetooth) vào vùng phủ sóng của AP hợp pháp sẽ buộc client phải roaming.
- Hacker muốn tấn công theo kiểu Man-in-the-middle này trước tiên phải biết được giá trị SSID là các client đang sử dụng (giá trị này rất dễ dàng có được). Sau đó, hacker phải biết được giá trị WEP key nếu mạng có sử dụng WEP. Kết nối upstream (với mạng trực có dây) từ AP giả mạo được điều khiển thông qua một thiết bị client như PC card hay Workgroup Bridge. Nhiều khi, tấn công Man-in-the-middle được thực hiện chỉ với một laptop và 2 PCMCIA card. Phần mềm AP chạy trên máy laptop nơi PC card được sử dụng như là một AP và một PC card thứ 2 được sử dụng để kết nối laptop đến AP hợp pháp gần đó. Trong cấu hình này, laptop chính là man-in-the-middle (người ở giữa), hoạt động giữa client và AP hợp pháp. Từ đó hacker có thể lấy được những thông tin giá trị bằng cách sử dụng các sniffer trên máy laptop.

FIGURE 10.9 Man-in-the-middle attack



- Điểm yếu trong kiểu tấn công này là người dùng không thể nhận biết được. Vì thế, số lượng thông tin mà hacker có thể thu được chỉ phụ thuộc vào thời gian mà hacker có thể duy trì trạng thái này trước khi bị phát hiện. Bảo mật vật lý (Physical security) là phương pháp tốt nhất để chống lại kiểu tấn công này.

Bài 42:  
**CÁC KHUYẾN CÁO VỀ BẢO MẬT WLAN**

**1. WEP:**

- Không nên chỉ dựa vào WEP cho dù bạn đã cài đặt một giải pháp bảo mật tốt đến thế nào đi nữa. Một môi trường không dây chỉ được bảo vệ bởi WEP là một môi trường hoàn toàn không an toàn. Khi sử dụng WEP, không nên sử dụng WEP key có liên quan đến SSID hay công ty. Hãy tạo ra một WEP key khó nhớ và khó nhận biết được. Trong nhiều trường hợp, WEP key có thể đoán ra mà chỉ cần nhìn vào SSID hay tên của công ty. WEP chỉ nên được sử dụng để giảm những nguy cơ như nghe trộm tình cờ chứ không nên là một giải pháp bảo mật duy nhất.

**2. Kích thước Cell:**

- Để giảm nguy cơ bị nghe lén, admin nên đảm bảo rằng kích thước cell của AP là hợp lý. Phần lớn các hacker thường tìm những vị trí có sóng RF và ít được bảo vệ nhất như vỉa hè, bãi đậu xe để đột nhập vào mạng không dây. Vì thế, các AP không nên phát tín hiệu mạnh đến bãi đậu xe (hay các vị trí khác) trừ khi thật sự cần thiết. Các AP dành cho doanh nghiệp cho phép cấu hình công suất phát, rất hiệu quả để điều khiển kích thước của cell xung quanh AP. Nếu kẻ nghe lén ở trong bãi đậu xe của công ty không bắt được sóng RF của AP thì sẽ không có cách nào xâm nhập được mạng nên mạng sẽ được bảo vệ khỏi kiểu tấn công này.

- Thường thì các admin bị hấp dẫn bởi việc thiết lập mức công suất phát tối đa trên tất cả các thiết bị WLAN nhằm đạt được throughput cũng như vùng bao phủ tối đa, nhưng cách cấu hình mù quáng như vậy sẽ trả giá rất đắt cho an toàn của mạng WLAN. Kích thước cell thích hợp của một AP trong một vùng nào đó nên được document cẩn thận lại lúc cấu hình AP. Trong một số trường hợp có thể cài đặt 2 AP (ở cùng một vị trí) với kích thước cell nhỏ hơn để giảm nguy cơ bị tấn công.

- Hãy cố đặt AP ở trung tâm của tòa nhà, điều này sẽ làm giảm nguy cơ rò rỉ tín hiệu ra bên ngoài vùng bao phủ mong muốn. Nếu bạn đang sử dụng một anten lắp ngoài thì nên chọn kiểu anten thích hợp để giảm thiểu kích thước phủ sóng vừa đủ. Hãy tắt AP khi không còn sử dụng, điều này sẽ giúp giảm nguy cơ tấn công cũng như bị sét đánh.

**3. Xác thực người dùng:**

- Bởi vì xác thực người dùng chính là điểm yếu nhất trong mạng WLAN và chuẩn 802.11 không chỉ định một phương thức nào để xác thực người dùng nên điều cần thiết đối với admin là cài đặt một phương thức xác thực dựa trên người dùng (user-based) càng sớm càng tốt khi cài đặt hạ tầng mạng WLAN. Xác thực người dùng nên dựa trên những cơ chế không phụ thuộc thiết bị như username, password, sinh trắc học, smart card, hệ thống token-based, hay các phương thức xác thực khác định danh người dùng (chứ không phải là thiết bị). Giải pháp bạn triển khai nên hỗ trợ xác thực 2 chiều giữa Server xác thực (RADIUS) và các client không dây.

- RADIUS là một chuẩn thực tế trong các hệ thống xác thực người dùng được sử dụng phổ biến trên thị trường công nghệ thông tin. AP sẽ gửi một yêu cầu xác thực người dùng đến RADIUS server (user authentication request), RADIUS server này có thể có cơ sở dữ liệu người dùng tích hợp hay có thể chuyển authentication request đến một domain controller, một NDS server, một Active Directory server hay thậm chí là một hệ thống tương thích LDAP. Một số nhà cung cấp RADIUS còn hỗ trợ các giao thức xác thực mới nhất như EAP.
- Việc quản lý một RADIUS server có thể là rất đơn giản hoặc rất phức tạp tùy thuộc vào việc cài đặt. Bởi vì các giải pháp bảo mật không dây là rất nhạy cảm nên cần cẩn thận khi chọn một giải pháp RADIUS server để đảm bảo các admin có thể quản trị.

#### **4. Sự cần thiết của bảo mật:**

- Hãy chọn lựa một giải pháp bảo mật thích hợp với nhu cầu và ngân sách của công ty cho cả hiện tại lẫn tương lai. Mạng WLAN có được sự phổ biến nhanh như vậy là do tính dễ cài đặt của chúng. Giả sử một mạng WLAN bắt đầu với một AP và 5 người dùng có thể phát triển nhanh chóng lên 15 AP và 300 người dùng trên toàn bộ campus của công ty. Vì thế, cơ chế bảo mật đã sử dụng cho 1 AP không còn thích hợp nữa khi số lượng người dùng tăng lên đến 300 người. Công ty có thể lảng phí tiền bạc vào các giải pháp bảo mật mà có thể nhanh chóng bị lỗi thời khi WLAN phát triển. Trong nhiều trường hợp, các công ty đã có sẵn IDS (Intrusion Detection System), firewall hay RADIUS server, khi quyết định lựa chọn giải pháp bảo mật không dây thì hãy tận dụng những thiết bị có sẵn để giảm chi phí xuống thấp nhất có thể.

#### **5. Sử dụng các công cụ bảo mật khác:**

- Tận dụng những công nghệ sẵn có như VPN, Firewall, Hệ thống phát hiện xâm nhập (IDS = Intrusion Detection System), các giao thức và chuẩn như 802.1X, EAP, xác thực người dùng với RADIUS ... sẽ giúp cho mạng không dây được an toàn hơn nhiều so với yêu cầu của chuẩn 802.11. Chi phí và thời gian để cài đặt những giải pháp này tùy thuộc vào độ lớn của doanh nghiệp.

#### **6. Giám sát những phần cứng giả mạo:**

- Để phát hiện được những AP giả mạo thì bạn nên thường xuyên kiểm tra các AP hiện có của mình nhưng không nên thông báo rộng rãi điều này. Chủ động phát hiện và loại bỏ những AP giả sẽ giúp chống lại hacker và cho phép admin duy trì và điều khiển mạng một cách an toàn. Thường xuyên kiểm tra bảo mật để xác định những AP có cấu hình sai có thể gây nguy hiểm cho mạng. Cấu hình hiện tại nên được so sánh với những cấu hình đã lưu trước đó để biết được liệu người dùng hay hacker đã thay đổi cấu hình của AP hay chưa. Bạn cũng có thể cài đặt và giám sát việc truy nhập của người dùng nhằm mục đích phát hiện những truy nhập trái phép trên phân đoạn mạng không dây. Kiểu giám sát này có thể giúp tìm lại những thiết bị không dây đã bị mất.

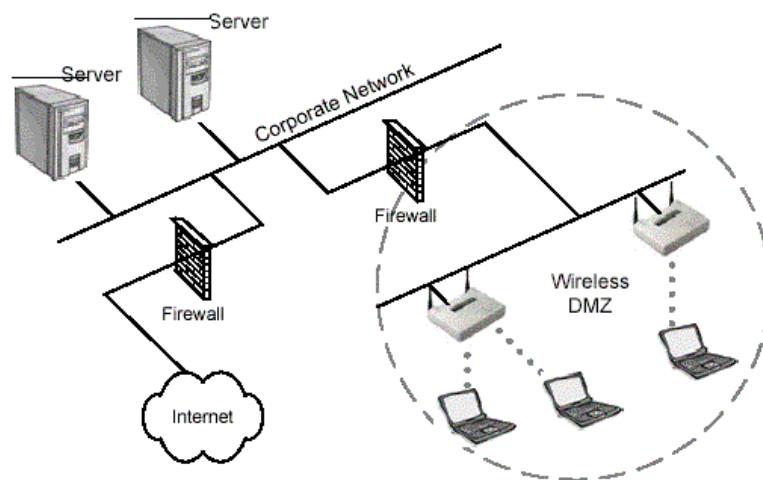
## 7. Switch, not Hub:

- Một chính sách khác nên được tuân thủ là luôn luôn kết nối AP với Switch thay vì Hub. Hub là một thiết bị broadcast, vì thế, mọi gói tin mà Hub nhận được sẽ được phát ra trên tất cả các port của Hub. Nếu AP được kết nối với Hub thì mọi gói tin truyền trong mạng có dây sẽ được broadcast ra mạng có dây. Điều này sẽ giúp hacker thu thập thêm được những thông tin giá trị như password hay IP address.

## 8. Wireless DMZ:

Một ý tưởng khác trong bảo mật mạng WLAN là tạo ra một vùng phi quân sự không dây (WDMZ = Wireless Demilitarized Zone). Việc tạo ra những WDMZ này sử dụng Firewall hay Router có thể tốn kém tùy thuộc vào mức độ của việc cài đặt. WDMZ thường được cài đặt ở những môi trường WLAN trung bình và lớn. Vì AP là một thiết bị không an toàn và không đáng tin vì thế, chúng nên được cách ly khỏi những đoạn mạng khác bằng một Firewall.

FIGURE 10.13 Wireless DMZ



## 9. Cập nhật Firmware và Software:

- Bạn nên thường xuyên cập nhật firmware và driver cho AP và card mạng. Việc sử dụng firmware và driver phiên bản mới nhất sẽ giúp tránh được những lỗ hổng bảo mật đã biết, vì chúng được các nhà sản xuất và những lỗ hổng này cũng như thêm vào các tính năng mới.

Bài 43:

## LỖ HỒNG SSID TRONG MẠNG WIRELESS

### 1. Tính năng quảng bá SSID:

- Các wireless network admin thường hay tắt tính năng quảng bá Service Set Identifier (SSID) trên Access Point (AP) hay router nhằm mục đích bảo mật. Thậm chí một người khi đã biết nơi có thể truy nhập mạng không dây thì họ vẫn không thể kết nối được nếu họ không biết SSID.
- Vì vậy, việc làm ẩn SSID bằng cách tắt tính năng quảng bá SSID có thể ngăn chặn việc truy nhập trái phép vào mạng. Tuy nhiên, đừng để điều này đánh lừa nhận thức về bảo mật của bạn. Một người với thiết bị cần thiết vẫn có thể dễ dàng lấy được SSID của mạng.
- Theo cấu hình mặc định, các beacon được gửi bởi AP hay router sẽ chứa các SSID để thông báo cho các client trong vùng của mình. Các SSID này được hiển thị trong Windows XP như là các mạng sẵn có. Tuy nhiên, khi tắt tính năng quảng bá SSID thì beacon sẽ không chứa SSID nữa, điều này sẽ ngăn chặn việc hiển thị mạng trong Windows XP. Nếu nó được sử dụng với các phương thức mã hóa khác thì có thể giúp bảo vệ mạng của bạn.

### 2. Phát hiện SSID khi nó không được quảng bá:

- Tuy nhiên, việc tắt tính năng quảng bá SSID trên AP hay router sẽ không thể ngăn chặn được các hacker hay war driver phát hiện ra mạng không dây và thậm chí là cả SSID nữa. Các hacker có thể sử dụng phần mềm hợp lệ như AirMagnet là có thể dễ dàng phát hiện ra SSID cho dù nó có được quảng bá trong beacon hay không.
- AirMagnet sẽ chụp lấy SSID từ các gói tin được gửi trong mạng giữa các client. SSID được chứa trong các association request, và trong một số trường hợp cả probe request và probe response đều chứa nó mặc dù bạn đã tắt tính năng quảng bá SSID rồi. Ví dụ, SSID của mạng có thể bị chụp lấy bởi AirMagnet khi một client trong mạng boot up thực hiện việc kết nối vào mạng không dây, lúc đó client sẽ gửi gói tin association request đến AP để có thể kết nối vào mạng không dây.
- Hacker và war driver có thể sử dụng các công cụ khác như AirJack cũng có hiệu quả tương tự. Các công cụ này làm việc bằng cách gửi một gói tin de-association giả đến một client nào đó. Điều này sẽ làm cho client thực hiện việc re-authentication và re-association với AP. Các công cụ này sẽ nhanh chóng chụp lấy SSID của mạng từ các gói tin association request.

### 3. Các điều cần nhớ:

- Việc bỏ tính năng quảng bá SSID chỉ có thể giúp bảo vệ mạng của bạn bằng cách ẩn nó trước những người dùng bình thường.
- Sử dụng tính năng ẩn SSID không có nghĩa là bạn không còn cần đến WAP hay WPA để bảo mật mạng.
- Các công cụ để phát hiện và phân tích luôn sẵn có bất cứ khi nào, cho dù bạn có sử dụng phương pháp bảo mật nào đi nữa.

Bài 44:

## CHÍNH SÁCH BẢO MẬT CHO DOANH NGHIỆP SỬ DỤNG WLAN

- Mỗi công ty sử dụng WLAN nên có một chính sách bảo mật trong đó đưa ra các mối nguy hiểm mà mạng WLAN có thể gặp phải. Ví dụ, nếu kích thước cell không thích hợp thì sẽ cho phép các hacker có thể kết nối vào mạng từ ngoài đường hay bãi đậu xe, vì thế bạn nên đưa chi tiết này vào trong chính sách bảo mật. Các chi tiết khác có thể có trong chính sách bảo mật bao gồm mật mã, WEP key, sử dụng các giải pháp bảo mật cao cấp, thường xuyên kiểm kê phần cứng WLAN ... Ngoài ra còn có nhiều yếu tố khác tùy thuộc vào nhu cầu bảo mật của công ty cũng như mức độ rộng lớn của mạng WLAN.

- Lợi thế của việc có, cài đặt và duy trì một chính sách bảo mật vững chắc là rất nhiều. Ngăn chặn việc mất trộm dữ liệu, ngăn chặn những kẻ phá hoại hay gián điệp, bảo vệ bí mật kinh doanh ...

- Khởi đầu của một chính sách bảo mật chính là quản lý. Nhận diện được những nhu cầu về bảo mật và ủy thác nhiệm vụ phải tạo ra được một tài liệu thích hợp bao gồm chính sách bảo mật cho WLAN là một ưu tiên hàng đầu. Trước tiên, người chịu trách nhiệm bảo mật WLAN phải được đào tạo về mặt công nghệ. Tiếp theo, những chuyên gia đã được đào tạo đó phải làm việc với cấp trên để thống nhất về một chính sách bảo mật cho công ty. Đội ngũ các cá nhân đã được đào tạo này sau đó có thể xây dựng nên một danh sách các yêu cầu mà nếu tuân thủ theo sẽ đảm bảo cho mạng không dây được bảo vệ giống như mạng có dây.

### 1. Giữ những thông tin nhạy cảm được bí mật:

- Một số điều mà chỉ có admin mới nên biết bao gồm:

+ Username và password của AP hay Bridge

+ SNMP strings

+ WEP key

+ MAC address list

- Việc giữ những thông tin này trong tay những người đáng tin cậy, những cá nhân tài năng như admin là điều rất quan trọng bởi vì những kẻ phá hoại hay hacker có thể dễ dàng sử dụng những thông tin này để truy cập vào mạng và các thiết bị mạng. Những thông tin này có thể được lưu trữ theo nhiều cách an toàn khác nhau. Trên thị trường hiện nay có các ứng dụng sử dụng mã hóa rất mạnh dành cho mục đích lưu trữ những thông tin nhạy cảm.

### 2. Physical Security:

- Mặc dù physical security là rất quan trọng đối với mạng có dây truyền thông nhưng nó lại càng quan trọng hơn đối với những công ty có sử dụng công nghệ WLAN. Vì hacker có thể không cần phải ở trong tòa nhà mới có thể kết nối vào mạng được mà chỉ cần ở ngoài đường hay bãi đậu xe là đủ. Thậm chí những phần mềm phát hiện xâm nhập là không đủ để ngăn chặn các hacker đánh cắp những thông tin nhạy cảm. Tấn công bị động không hề để lại dấu vết nào trên mạng bởi vì hacker không thật sự kết nối vào mạng mà chỉ lắng nghe. Hiện nay có những ứng dụng có thể làm cho card mạng hoạt động trong chế độ hỗn hợp

(promiscuous mode) cho phép truy cập dữ liệu mà không cần phải thiết lập kết nối.

- Khi WEP là giải pháp bảo mật duy nhất trong mạng WLAN thì bạn nên kiểm soát chặt chẽ những user đang sử dụng thiết bị không dây thuộc sở hữu của công ty, chẳng hạn như không cho phép họ mang những thiết bị đó ra khỏi công ty. Vì WEP key được lưu trữ trong firmware của thiết bị, vì thế thiết bị đi đến đâu thì điểm yếu nhất của mạng nằm ở đó. Admin nên biết ai, ở đâu và khi nào các PC card bị đem ra khỏi công ty.

- Admin nên biết một điều là WEP bản thân nó không phải là một giải pháp bảo mật an toàn. Thậm chí với việc kiểm soát chặt chẽ như trên nhưng khi card bị đánh rơi hay làm mất thì người sử dụng phải có trách nhiệm báo cáo sự mất mát đó ngay lập tức cho admin để admin có thể đưa ra một số biện pháp ngăn ngừa cần thiết. Ở đây, admin có thể thiết lập lại MAC filter hay thay đổi WEP key ...

- Việc thường xuyên tìm kiếm quanh công ty để phát hiện những hành động khả nghi là một cách hiệu quả để giảm những nguy cơ tiềm ẩn. Nhân viên bảo vệ nên được huấn luyện để nhận biết được những phần cứng 802.11 lạ và cảnh báo cho công ty để tìm kiếm những kẻ phá hoại đang ẩn nấp đâu đó trong tòa nhà.

### **3. Kiểm kê thiết bị WLAN và mức độ bảo mật:**

- Như là một phần bổ sung cho chính sách bảo mật vật lý, tất cả các thiết bị WLAN nên thường xuyên được kiểm kê để thống kê các truy nhập hợp pháp cũng như ngăn chặn việc sử dụng các thiết bị không dây một cách trái phép. Nếu như mạng quá lớn và có quá nhiều thiết bị không dây thì việc thường xuyên kiểm kê thiết bị là không thực tế. Trong trường hợp này, chúng ta nên cài đặt một giải pháp bảo mật không dựa trên phần cứng mà dựa trên username và password hay các giải pháp khác. Đối với mạng vừa và nhỏ thì việc kiểm kê hàng tháng hay hàng quý sẽ giúp biết được những mất mát về thiết bị.

- Thường xuyên scan mạng bằng sniffer để tìm kiếm những thiết bị giả mạo là một bước quan trọng để giúp bảo mật mạng. Hãy xem xét trường hợp một mạng không dây phức tạp (và mắc tiền) đã được cài đặt với chính sách bảo mật hợp lý. Nhưng nếu một người dùng tự ý cài đặt thêm một AP trong mạng thì điều này có thể sẽ tạo ra những lỗ hổng cho hacker lợi dụng và nó cũng phá vỡ các chính sách bảo mật tốt (và mắc tiền) đã được cài đặt.

- Kiểm kê về phần cứng cũng như mức độ bảo mật nên được document lại trong chính sách bảo mật của công ty. Các bước đã thực hiện, các công cụ đã được sử dụng và các báo cáo nên được rõ ràng trong chính sách bảo mật và công việc nhầm chán này không nên làm một cách sơ sài. Các nhà quản lý nên thường xuyên nhận được những báo cáo kiểu này từ các admin.

### **4. Sử dụng các giải pháp bảo mật cao cấp:**

- Các công ty có sử dụng mạng WLAN nên tận dụng những ưu điểm của các cơ chế bảo mật hiện có trên thị trường. Một yêu cầu với chính sách bảo mật là bất kỳ một sự cài đặt nào của các cơ chế bảo mật đều phải được document lại một cách rõ ràng. Bởi vì những công nghệ này khá mới, độc quyền và thường được

sử dụng kết hợp với các giao thức hay công nghệ bảo mật khác nên chúng phải được document lại để lúc có những lỗ hổng xuất hiện thì admin có thể xác định ở đâu và làm thế nào mà lỗ hổng lại xuất hiện.

- Bởi vì có ít người trong nghành công nghiệp công nghệ thông tin được đào tạo bài bản về công nghệ không dây nên những sơ xuất của người sử dụng có thể làm hỏng mạng hay để lại những lỗ hổng cho hacker. Những sai lầm này của các nhân viên là một lý do rất quan trọng cho việc phải document một cách rõ ràng tính năng bảo mật đã cài đặt.

## 5. Mạng không dây công cộng:

- Một điều không thể tránh khỏi là các nhân viên với thông tin nhạy cảm trên máy laptop của họ sẽ kết nối với mạng không dây công cộng. Một yêu cầu nên có trong chính sách bảo mật là buộc tất cả các nhân viên chạy các phần mềm tường lửa (firewall) cá nhân và các phần mềm antivirus trên máy tính laptop của họ. Hầu hết các mạng không dây công cộng có rất ít hoạt động không có một cơ chế bảo mật nào nhằm làm tăng tính đơn giản cho người sử dụng lúc kết nối đồng thời cũng làm giảm những yêu cầu về hỗ trợ kỹ thuật từ người sử dụng.

- Thậm chí những upstream server trên đoạn mạng có dây đã được bảo vệ thì người dùng không dây vẫn có nguy cơ bị tấn công. Hãy xem xét tình huống trong đó hacker ngồi ở sân bay sử dụng các điểm nóng wi-fi (wi-fi hot spot). Hacker này có thể sniff (lắng nghe, điều tra ...) mạng WLAN để lấy được username, password, đăng nhập vào hệ thống đợi cho người dùng cũng đăng nhập vào. Sau đó hacker có thể dùng ping để scan qua toàn bộ subnet tìm kiếm những người dùng khác và bắt đầu hack vào laptop của họ.

## 6. Giới hạn và theo dõi truy cập:

- Hầu hết mạng LAN của doanh nghiệp đều có một số phương pháp nào đó để giới hạn và theo dõi sự truy cập của nhân viên trong mạng LAN. Thông thường thì hệ thống sẽ được triển khai dịch vụ AAA (Authentication, Authorization, Accounting). Dịch vụ này cũng nên được document lại và cài đặt như là một phần của bảo mật mạng WLAN. Dịch vụ AAA sẽ cho phép doanh nghiệp gán quyền truy cập đến một lớp người dùng nào đó. Ví dụ, khách hàng chỉ được cho phép sử dụng internet trong khi nhân viên sẽ được truy cập đến server nội bộ và internet.

- Việc lưu giữ những thông tin về quyền truy cập của user cũng nhu những thao tác họ đã thực hiện sẽ là một bằng chứng quan trọng để biết được ai đã làm gì trên mạng. Chẳng hạn, nếu nhân viên đang nghỉ phép và trong suốt kỳ nghỉ phép đó account của họ được sử dụng liên tục thì có thể biết được account đó đã bị hacker biết được password. Có được những thông tin về các thao tác đã làm sẽ giúp cho admin biết được điều gì đã thật sự xảy ra với mạng để có biện pháp đối phó thích hợp

## Bài 45:

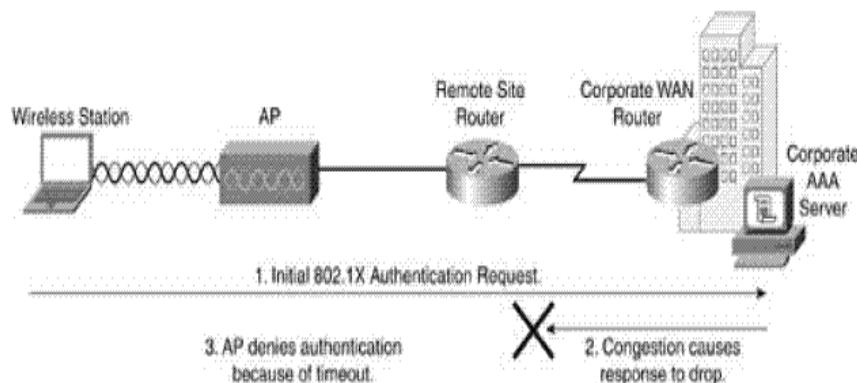
### CÁC VẤN ĐỀ CẦN XEM XÉT KHI TRIỂN KHAI WLAN

Sau khi bạn đã kết thúc site survey và có được bản đồ triển khai vật lý, bạn có thể chuyển sang bước tiếp theo của quá trình triển khai. Một mạng WLAN bảo mật đòi hỏi phải có AAA Server như RADIUS để cho phép xác thực theo người dùng. Hơn nữa, bạn nên triển khai 1 cơ chế để quản lý WLAN.

#### 1. Các vấn đề cần xem xét khi triển khai 802.1X:

- Giải pháp 802.1X yêu cầu phải có AAA server để cung cấp xác thực theo người dùng. AAA server thường được đặt ở trung tâm dữ liệu (data center) đã được bảo vệ. Vì nó nằm ở layer 3 và có tốc độ chuyển mạch của đường dây (wire-speed) nên bạn có thể đo đạc được độ trễ của mạng giữa biên mạng (network edge) và data center vào khoảng vài milisecond hay thậm chí microsecond.
- Việc triển khai 802.1X trở nên phức tạp hơn khi phải triển khai qua kết nối WAN. Kết nối WAN thường có băng thông (bandwidth) thấp hơn so với kết nối LAN và kết quả là nghẽn có thể xuất hiện trên những kết nối này. Nghẽn có thể có những ảnh hưởng đáng kể lên xác thực 802.1X vì nó có thể drop (hủy bỏ) những gói tin RADIUS làm cho việc xác thực của trạm client bị time out như được minh họa trong hình dưới.

**Figure 8-7. WAN Link Congestion Impacting 802.1x Authentication in Remote Sites**



- Bạn có thể hạn chế ảnh hưởng bằng 2 cách sau:

- + Sử dụng QoS để ưu tiên các gói tin 802.1X RADIUS được truyền qua kết nối WAN
- + Cài đặt AAA server cục bộ ở chi nhánh

#### Ưu tiên gói tin 802.1X RADIUS sử dụng IP QoS:

- Phương pháp này cung cấp độ ưu tiên cho các gói tin 802.1X khi kết nối WAN xảy ra nghẽn. Đối với các mạng đã triển khai QoS để hỗ trợ các ứng dụng VoIP thì hầu như chúng ta không cần cầu hình gì thêm.
- VoIP thường có giá trị IP Precedence bằng 5 và giá trị DSCP (Differentiated

Service Code Point) là EF (Expedited Forwarding). Video có IP Precedence bằng 4 và DSCP là AF41 đến AF43. Các giao thức điều khiển cuộc gọi VoIP (MGCP hay H.323) có IP Precedence bằng 3 và DSCP là AF31 đến AF33. Các gói tin 802.1X RADIUS có thể được xem như là control traffic nên có thể xếp vào IP Precedence bằng 3 và DSCP là AF31 đến AF33. Bảng dưới đây tóm tắt các giá trị này.

**Table 8-1. IP QoS Summary**

Function	IP Precedence Value	DSCP Value
Voice (VoIP)	5	EF
Video	4	AF41-AF43
Signaling (VoIP call control, 802.1x)	3	AF31-AF33
Normal data	0	0

- Việc sử dụng QoS để ưu tiên traffic của 802.1X RADIUS không giải quyết được hết mọi vấn đề liên quan đến việc xác thực từ xa. Các vấn đề sau vẫn luôn tồn tại:

- + Không có dịch vụ WAN (WAN outage)
- + Độ trễ của WAN

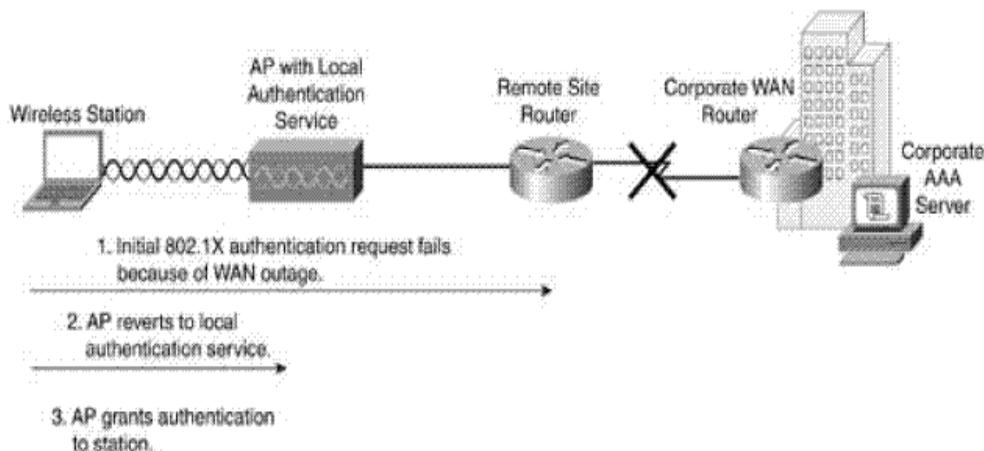
- Nếu kết nối WAN bị đứt thì trạm client không thể truy cập vào WLAN cũng như tài nguyên cục bộ. Với kết nối WAN có độ trễ rất cao như vệ tinh cũng có những ảnh hưởng xấu đến quá trình xác thực vì nó có thể làm cho việc xác thực bị time out làm cho hiệu năng hoạt động của station bị giảm sút nghiêm trọng.

#### Xác thực cục bộ ở chi nhánh:

- Xác thực cục bộ ở chi nhánh thường như là một giải pháp tốt để giải quyết vấn đề, nhưng nó cũng không phải là một công cụ chưa được bách bệnh. Việc triển khai AAA server ở chi nhánh có những vấn đề sau:

- + Chi phí – Đối với những công ty có nhiều chi nhánh thì cần ít nhất 1 server ở mỗi chi nhánh
- + Khả năng quản lý
- Số lượng authentication server có thể lên đến hàng ngàn tùy thuộc vào sự triển khai
- Việc phải tái tạo lại cơ sở dữ liệu người dùng cho một lượng lớn các chi nhánh có thể là một vấn đề khó thực hiện
- Việc truy cập của admin có thể là một vấn đề nếu như các admin ở chi nhánh cần thường xuyên truy cập vào server trung tâm
- Một số nhà sản xuất như Cisco đã tích hợp authentication server vào trong AP để giúp người dùng tiết kiệm chi phí và những rắc rối liên quan đến việc quản lý AAA server cục bộ như được minh họa trong hình dưới

**Figure 8-8. Local Authentication Service on the AP**



## 2. Quản lý WLAN:

- Quản lý mạng nói chung và quản lý WLAN nói riêng là một chủ đề lớn và cần phải có một sách khác nói về chúng. Phần này chỉ đưa ra một số khái niệm quan trọng nổi bật nhất cần phải xem xét trong suốt quá trình triển khai.
- Trong bất kỳ kiểu mạng nào, bạn không thể quản lý những gì mà bạn không thể đo đạc được
  - Trong các mạng lớn, có thể lên đến hàng ngàn thiết bị cần được quản lý. Trong các triển khai mạng WLAN cho một doanh nghiệp lớn không hiếm khi ta thấy số lượng AP nhiều gấp 3 lần bình thường. WLAN có thể sẽ ảnh hưởng chính đến việc bạn sẽ quản lý mạng như thế nào. Để có được một mạng WLAN hoạt động đáng tin cậy như mạng LAN và giảm thiểu những phức tạp trong việc quản lý thì bạn cần phải có một giải pháp quản lý trong đó bao gồm việc quản lý WLAN.
  - Những nhà phê chuẩn WLAN đầu tiên đã gặp những khó khăn về gánh nặng quản lý trong WLAN. Hầu hết các gói quản lý giá rẻ rất khó mở rộng đến hàng ngàn thiết bị mà không phải sử dụng nhiều trạm quản lý, và không có một giải pháp nào đưa ra những chức năng quản lý sóng vô tuyến (RF). Những thiếu sót này làm cho việc triển khai WLAN có hiệu năng hoạt động nghèo nàn và buộc admin phải tự phát triển những công cụ riêng của họ để quản lý WLAN một cách hiệu quả.
  - Nhiều giải pháp quản lý WLAN cung cấp các dịch vụ quản lý giống với mạng có dây như: SNMP, giám sát lỗi, thu thập các bẫy lỗi (trap), phân phối cấu hình, phân phối firmware ... Tuy nhiên, không có giải pháp nào cho admin có cái nhìn sâu hơn về bản thân mạng vô tuyến. Hiệu năng của WLAN khác nhau rất lớn trong các cài đặt khác nhau. Vật liệu của tường và vị trí của nhiều bên ngoài như lò vi sóng có thể ảnh hưởng đến hiệu năng của WLAN. Ngoài ra thì các thiết bị Bluetooth, ad-hoc client và mạng WLAN của hàng xóm sẽ làm suy giảm hiệu năng của WLAN đến mức độ không thể sử dụng được.
  - Việc quản lý được sóng vô tuyến sẽ cho phép admin nhìn thấy được các vấn

đề như vậy và tùy thuộc vào các giải pháp cài đặt mà nó có thể tự động điều khiển các tham số của radio (sóng vô tuyến) như lựa chọn kênh/tần số và công suất truyền của client/AP để thích nghi với môi trường RF.

### **Kết luận:**

- Quyết định của bạn khi triển khai mạng WLAN là điều quan trọng để tối ưu mạng WLAN:
  - + Kiểu người dùng nào sẽ sử dụng WLAN? (có tính di động cao hay chỉ thỉnh thoảng)
  - + Kiểu ứng dụng nào mà những người dùng này sẽ sử dụng trong WLAN?
  - Mặc dù 2 câu hỏi này là rất cơ bản và hầu như bản thân nó đã tự giải thích nhưng chúng vẫn thường bị bỏ quên trong lúc triển khai. Chúng là nền tảng cho việc tiết kiệm chi phí trong suốt quá trình triển khai, chính là trong việc lựa chọn kiểu triển khai coverage-oriented hay capacity-oriented.
  - Một khi bạn đã chọn được kiểu triển khai thì việc biết được các công cụ để thực hiện site survey cũng như các trường hợp site survey thực tế có thể giúp bạn tiết kiệm thời gian và tiền bạc cho một công việc nhảm chán và tốn thời gian. Ngày nay, site survey là một công việc thủ công có nghĩa là người khảo sát sẽ phải thực hiện tất cả các đo đạc cũng như tính toán. Cùng với sự phát triển của WLAN thì các công cụ quản lý cũng giúp tự động một số tiến trình này.

---

Bài 46:

## **CÁC CÔNG NGHỆ CẠNH TRANH VỚI WLAN**

Có nhiều công nghệ cạnh tranh với các chuẩn 802.11. Khi nhu cầu kinh doanh thay đổi và công nghệ đã được cải tiến thì vẫn liên tục có nhiều chuẩn mới được tạo ra để hỗ trợ cho thị trường. Ở đây chúng ta xét những công nghệ sau:

- + HomeRF
- + Bluetooth
- + Infrared
- + OpenAir

### **1. HomeRF**

- HomeRF hoạt động trong băng tần 2.4 Ghz và sử dụng công nghệ nhảy tần (frequency hopping). Các thiết bị HomeRF nhảy khoảng 50 hop trong một giây – khoảng 5 đến 20 lần nhanh hơn các thiết bị 802.11 FHSS. Phiên bản mới là HomeRF 2.0 sử dụng quy tắc nhảy tần băng rộng (wide band) mới đã được phê chuẩn bởi FCC. Hãy nhớ lại các quy tắc sau được áp dụng sau ngày 31/8/2000:
  - + Tần số sóng mang rộng lớn nhất là 5 Mhz
  - + Ít nhất là 15 hop trong một chuỗi nhảy (hop sequence)
  - + Công suất phát tối đa là 125 mW.
- Bởi vì HomeRF cho phép tăng tần số sóng mang và rất linh hoạt trong việc cài đặt nên có người nghĩ rằng nhảy tần băng rộng sẽ phổ biến. Tuy

nhiên, điều này đã không xảy ra. Mặc dù có thuận lợi về mặt tốc độ (10 Mbps) nhưng vẫn không bù được những bất lợi về giới hạn công suất phát 125 mW. Điều này gây ra giới hạn việc nhảy tần băng rộng chỉ trong phạm vi 150 feet. Những giới hạn này đã làm cho các thiết bị nhảy tần băng rộng chỉ được sử dụng chủ yếu trong môi trường SOHO.

- HomeRF sử dụng giao thức SWAP, là một sự kết hợp giữa CSMA và TDMA. SWAP là một sự lai tại giữa 802.11 và chuẩn DECT và đã được phát triển bởi nhóm làm việc HomeRF. Các thiết bị HomeRF là các thiết bị duy nhất trên thị trường hiện tại vẫn còn sử dụng các quy tắc nhảy tần băng rộng. Các thiết bị HomeRF được xem là bảo mật hơn 802.11 trong việc sử dụng WEP bởi vì HomeRF sử dụng 32 bit IV thay vì chỉ 24 bit như trong 802.11. Hơn nữa, HomeRF chỉ định các IV được chọn như thế nào trong quá trình mã hóa. 802.11 không có quá trình này nên nó rất dễ bị tấn công.

## 2. Bluetooth

- Bluetooth là một công nghệ nhảy tần khác hoạt động trong băng tần 2.4 Ghz ISM. Tỷ lệ nhảy của các thiết bị Bluetooth khoảng 1600 hop trong một giây (có dwell time khoảng 625 uS) vì thế chúng có chi phí nhiều hơn đáng kể so với hệ thống nhảy tần trong 802.11. Tỷ lệ nhảy cao cũng giúp cho công nghệ kháng cự tốt hơn với nhiễu băng hẹp. Các hệ thống Bluetooth không được thiết kế để có throughput cao nhưng lại rất đơn giản trong sử dụng, có công suất thấp và khoảng cách ngắn (WPAN). Chuẩn IEEE 802.15 bao gồm các đặc tả cho Bluetooth.

- Một điểm bất lợi lớn nhất trong việc sử dụng công nghệ Bluetooth là chúng thường như phá hủy hoàn toàn các mạng 2.4 Ghz khác. Tốc độ nhảy cao của Bluetooth trong toàn bộ băng tần 2.4 sử dụng được làm cho tín hiệu Bluetooth xuất hiện trong các hệ thống khác như là nhiễu all-band (all-band interference). Bluetooth cũng ảnh hưởng đến các hệ thống FHSS khác. Nhiều all-band có nghĩa là làm hỏng tín hiệu trong toàn bộ dãy tần số có thể sử dụng được. Nhưng lạ thay, nhiễu ngược (counter-interference) (nhiễu của mạng WLAN gây ra cho Bluetooth) không ảnh hưởng đến các thiết bị bluetooth một cách nghiêm trọng như là nhiễu của Bluetooth gây ra cho các thiết bị WLAN.

- Các thiết bị Bluetooth hoạt động trong 3 lớp công suất: 1 mW, 2.5 mW và 100 mW. Hiện tại thì rất ít thiết bị bluetooth sử dụng lớp 3 (100 mW). Các thiết bị bluetooth lớp 2 (2.5 mW) có phạm vi hoạt động tối đa là 10 mét (33 feet). Nếu bạn muốn mở rộng vùng hoạt động thì bạn nên sử dụng anten định hướng.

## 3. Infrared Data Association (IrDA)

IrDA không phải là một chuẩn như Bluetooth, HomeRF hay 802.11 mà là một tổ chức. Được thành lập vào tháng 6 năm 1993, IrDA là một tổ chức có nhiệm vụ tạo ra các chuẩn có thể tương tác với nhau, chi phí thấp, công suất thấp, half-duplex, serial data interconnection hỗ trợ cho các người dùng di động trong mô hình point-to-point và có thể gắn vào các phần cứng máy tính khác nhau. Truyền thông được sử dụng chủ yếu trong các máy tính toán (calculator), máy in, các liên kết building-to-building và các máy tính cầm tay.

### **Infrared (IR):**

- Infrared là một công nghệ truyền thông dựa trên ánh sáng chứ không phải là một công nghệ trai phỏ. Các thiết bị IR có thể đạt được tốc độ tối đa là 4 Mbps ở khoảng cách gần nhưng vì nó là một công nghệ dựa vào ánh sáng nên các nguồn ánh sáng IR khác có thể gây nhiễu đến việc truyền thông IR. Tốc độ thường thấy của một thiết bị IR là khoảng 115 Kbps là đủ cho việc trao đổi dữ liệu giữa các thiết bị cầm tay. Một lợi thế quan trọng của mạng IR là nó không gây nhiễu với mạng trai phỏ RF nên chúng có thể được sử dụng cùng với nhau.

### **Security:**

- Tính bảo mật của bản thân các thiết bị IR là rất tuyệt vời do 2 nguyên nhân chính. Thứ nhất, IR không thể truyền xuyên tường ở mức công suất thấp như thế (2 mW). Thứ 2, một hacker hay một kẻ nghe lén phải can thiệp trực tiếp vào các beam để có thể truy cập vào các thông tin được truyền. Với PDA và Laptop, IR được sử dụng cho các kết nối point-to-point ở một khoảng cách rất ngắn vì thế, tính bảo mật là không cần thiết trong trường hợp này.

### **Stability (tính ổn định):**

IR không thể truyền xuyên tường mà nó sẽ phản xạ lại khỏi tường và trần nhà. Infrared không bị phá hủy bởi tín hiệu điện từ, điều này làm tăng tính ổn định của hệ thống IR. Các thiết bị IR quảng bá (broadcast) có thể được treo trên trần nhà. Thiết bị IR quảng bá (tương tự như anten RF) sẽ truyền sóng mang IR và các thông tin theo tất cả mọi hướng. Vì lý do tiêu thụ điện năng nên Broadcast IR thường được sử dụng trong nhà. Truyền thông IR point-to-point có thể được sử dụng outdoor và có phạm vi hoạt động tối đa lên đến 1 Km (khoảng 3280 feet) nhưng khoảng cách này có thể bị làm ngắn lại bởi ánh sáng mặt trời. Ánh sáng mặt trời xấp xỉ 60% ánh sáng infrared và có thể làm suy yếu tín hiệu broadcast IR một cách nghiêm trọng.

## **4. Wireless LAN Interoperability Forum (WLIF)**

- Chuẩn OpenAir là chuẩn được tạo ra bởi WLIF (hiện tại thì diễn đàn này không còn hoạt động nữa) như là một hệ thống WLAN thay thế cho 802.11. OpenAir có 2 tốc độ hoạt động là 800 Kbps và 1.6 Mbps. Các hệ thống OpenAir và 802.11 không tương thích với nhau và không thể tương tác được với nhau. Hiện nay thì chuẩn này rất ít được sử dụng. OpenAir tập trung chủ yếu vào các thiết bị FHSS và chỉ hoạt động ở 2 tốc độ.

Bài 47:

## CÁC BẢNG ĐƯỢC SỬ DỤNG TRONG CHUYỂN MẠCH

- Các Catalyst switch chứa một vài kiểu bảng để sử dụng cho quá trình chuyển mạch. Các bảng này được thay đổi đối với chuyển mạch lớp 2 hoặc đa lớp, và được giữ trong một bộ nhớ nhanh để nhiều trường bên trong một frame hoặc gói được so sánh song song.

### 1. Bộ nhớ nội dung địa chỉ CAM (Content Addressable Memory):

- Tất cả Catalyst switch đều sử dụng một bảng CAM cho chuyển mạch lớp 2. Vì frame đến các port của switch, nên địa chỉ MAC nguồn được học và ghi lại trong bảng CAM. Cả port đến và VLAN đều được ghi lại, cùng với một đánh dấu thời gian (timestamp). Nếu một địa chỉ MAC học trên một port chuyển sang port khác, thì địa chỉ MAC và timestamp được ghi lại cho hầu hết các port đến trước đó. Sau đó, các mục trước sẽ được xoán. Nếu tìm thấy một địa chỉ MAC được đã tồn tại trong bảng cho port đến chính xác, thì timestamp sẽ được cập nhật.
- Các switch thường có bảng CAM lớn để truy tìm nhiều địa chỉ cho việc chuyển tiếp frame. Tuy nhiên, không gian bảng không đủ để giữ mỗi địa chỉ có thể trên một mạng lớn. Để quản lý không gian bảng CAM, các mục cũ (địa chỉ không được dùng trong khoảng thời gian nào đó) sẽ bị xóa. Khoảng thời gian mặc định là 300s. Ta cũng có thể cấu hình switch để thay đổi giá trị mặc định này.
- Điều gì sẽ xảy ra khi địa chỉ MAC của host được học trên một port của switch, và sau đó chuyển sang port khác. Thông thường mục bảng CAM gốc của host có thời hạn là 300s, trong khi địa chỉ của nó được học trên một port mới. Để tránh việc trùng lắp các mục trong bảng CAM, thì switch sẽ làm sạch mục đã tồn tại đối với địa chỉ MAC được học trên port khác. Đây là điều chấp nhận được vì địa chỉ MAC là duy nhất và một host không bao giờ được thấy trên nhiều hơn một port trừ khi mạng có vấn đề. Nếu switch chú ý rằng, địa chỉ MAC đang được học trên các port qua lại, nó sẽ phát ra một thông điệp báo lỗi địa chỉ MAC "flapping" giữa hai interface.

### 2. Bộ nhớ nội dung địa chỉ bậc ba TCAM (Ternary Content Addressable Memory):

- Trong cách định tuyến truyền thống, các ACL có thể so khớp, lọc, hoặc điều khiển lưu lượng đặc biệt. Danh sách truy cập được cấu thành từ một hoặc nhiều mục truy cập (ACE - Access Control Entry), hoặc so khớp câu lệnh được ước lượng (Evaluating) trong lệnh theo sau. Việc ước lượng (Evaluating) một danh sách truy cập có thể bổ sung thời gian vào các gói chuyển tiếp.
- Tuy nhiên trong chuyển mạch đa lớp, tất cả quá trình so khớp mà các ACL cung cấp được thực hiện ở phần cứng. TCAM cho phép một gói được ước lượng dựa vào toàn bộ danh sách truy cập trong bảng tra cứu. Hầu hết switch có nhiều bảng TCAM để bảo mật cả trong và ngoài, và các QoS ACL được ước lượng đồng thời, hoặc hoàn toàn trong quyết định song song chuyển tiếp lớp 2 hoặc lớp 3.

- Phần mềm IOS của Catalyst có hai thành phần để thực thi hoạt động của TCAM:

- **Quản lý tính năng FM (Feature Manager):** sau khi một danh sách truy cập được tạo hoặc cấu hình, phần mềm quản lý tính năng sẽ biên dịch, và các ACE sẽ được hợp nhất vào trong toàn bộ bảng TCAM. Sau đó TCAM được tra cứu với tốc độ chuyển tiếp frame.
- **Quản lý cơ sở dữ liệu chuyển mạch SDM (Switching Database Manager):** ta có thể chia TCAM trên các Catalyst switch thành các vùng có chức năng khác nhau. Phần mềm SDM cấu hình hoặc các phần chia TCAM này nếu cần.

### **Cấu trúc bảng TCAM:**

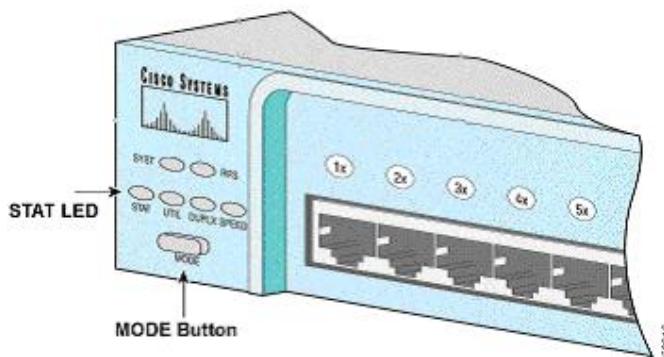
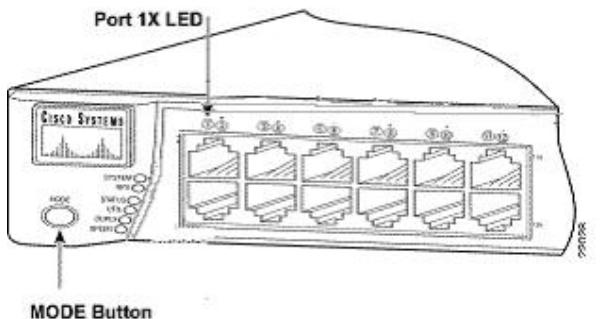
- TCAM là một bảng mở rộng của bảng CAM, nên nó cũng thực hiện truy tìm dựa trên thuật toán so trùng gồm có hai giá trị vào là bit 0 và 1, cho kết quả nhanh nhưng hoạt động của trùu tượng hơn. Ví dụ giá trị nhị phân (0 và 1) là từ khóa trong bảng, nhưng giá trị mặt nạ cũng được sử dụng để quyết định bit nào có liên quan thực sự. Như vậy từ khóa của bảng TCAM có ba giá trị đó là 0,1 và X.

- Toàn bộ TCAM được so sánh kết hợp cả ba giá trị, mặt nạ và kết quả (Value, Mask, và Result). Các trường có được từ header của frame hoặc packet và sẽ được dưa vào TCAM. Việc ánh xạ được thực hiện như sau:

- Value: là một chuỗi 134 bit, gồm có địa chỉ nguồn và đích, và các thông tin giao thức liên quan, tất cả đều được so trùng. Thông tin móc nối đến Value liên quan đến kiểu danh sách truy cập được biểu diễn trong bảng 1. Value trong bảng TCAM lấy trực tiếp từ địa chỉ, port và thông tin giao thức trong ACE.
- Mask: cũng là một chuỗi 134 bit trong cùng frame. Mask chỉ chọn các bit Value, và bit mask sẽ được thiết lập để so trùng bit Value chính xác. Mask sử dụng bảng TCAM xuất phát từ địa chỉ hoặc bit mask trong các ACE.
- Result: là giá trị bằng số cho biết hành động sau khi so trùng xảy ra ở bảng TCAM. Ví dụ Result có thể là một quyết định cho phép hoặc không, hoặc giá trị QoS, hoặc con trỏ đến bảng định tuyến kết tiếp...

## Bài 48: Recovery Password Switch !

Việc crack password switch cực kỳ đơn giản trong các dòng switch sau: 2900XL, 3500XL, 2940, 2950, 2960, 2970, 3550, 3560, and 3750 series switches



Nhấn và giữ nút "mode" , bên trái của switch, cho đến khi thấy switch hiện các câu thông báo "... password recovery mechanism is enable.."

Và đợi switch khởi động lại, Lúc này ta được cấu hình rỗng. Ta đã vào được mode privileged . Để copy file cấu hình cũ lên lại, mục đích sửa, xoá password, ta dùng lệnh :

Quote:

```
Switch#copy flash:config.text.rename running-config
```

CCNA#

Sau khi sửa password đã quên, ta lưu cấu hình lại bình thường .

Tuy nhiên, với dòng Switch 2955 series, chúng ta không thể sử dụng nút "mode" để recovery password. Mà ta tiến hành các bước sau :

Gỡ cáp nguồn switch, và gắn lại, cũng tương tự router, ta nhấn CTRL + Break để nhất tiến trình boot. ( Lưu ý : tuỳ vào hệ điều hành mà ta có tổ hợp phím ngắt khác nhau )

Quote:

```
C2955 Boot Loader (C2955-HBOOT-M) Version 12.1(0.0.514), CISCO
```

```
DEVELOPMENT TEST  
VERSION  
Compiled Fri 13-Dec-02 17:38 by madison  
WS-C2955T-12 starting...  
Base ethernet MAC Address: 00:0b:be:b6:ee:00  
Xmodem file system is available.  
Initializing Flash...  
flashfs[0]: 19 files, 2 directories  
flashfs[0]: 0 orphaned files, 0 orphaned directories  
flashfs[0]: Total bytes: 7741440  
flashfs[0]: Bytes used: 4510720  
flashfs[0]: Bytes available: 3230720  
flashfs[0]: flashfs fsck took 7 seconds.  
...done initializing flash.
```

Chờ đợi thấy màn hình hiện ra :

Quote:

```
The system has been interrupted prior to initializing the flash file system to  
finish  
loading the operating system software:
```

```
flash_init  
load_helper  
boot
```

Nhấn CTRL + Break

Quote:

```
switch:
```

Gõ command :

Quote:

```
switch: flash_init  
Initializing Flash...  
flashfs[0]: 143 files, 4 directories  
flashfs[0]: 0 orphaned files, 0 orphaned directories  
flashfs[0]: Total bytes: 3612672  
flashfs[0]: Bytes used: 2729472  
flashfs[0]: Bytes available: 883200  
flashfs[0]: flashfs fsck took 86 seconds  
....done Initializing Flash.
```

Boot Sector Filesystem (bs😊 installed, fsid: 3

Parameter Block Filesystem (pb😊 installed, fsid: 4

Gõ command

Quote:

```
switch: load_helper  
switch:
```

Tiếp tục ta gõ dir flash để xem IOS trên switch

(Lưu ý, có dấu : sau chữ flash)

Quote:

```
switch: dir flash:  
Directory of flash:/  
-rwx 1803357 <date> c3500xl-c3h2s-mz.120-5.WC7.bin  
-rwx 1131 <date> config.text ( file lưu cấu hình )-rwx 109 <date> info  
-rwx 389 <date> env_vars  
drwx 640 <date> html  
-rwx 109 <date> info.ver  
403968 bytes available (3208704 bytes used)  
switch:
```

Ta sửa file cấu hình đã lưu password

Quote:

```
switch: rename flash:config.text flash:config.old
```

Enter boot command

Quote:

```
switch: boot  
Loading "flash:c3500xl-c3h2s-mz.120-  
5.WC7.bin"...#####  
#####  
#####  
#####  
#####  
File "flash:c3500xl-c3h2s-mz.120-5.WC7.bin" uncompressed and installed,  
entry po  
int: 0x3000  
executing...
```

Sau khi khởi động lên :

Quote:

```
--- System Configuration Dialog ---  
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '[]'.  
Continue with configuration dialog? [yes/no]: n
```

Press RETURN to get started.

Switch>

```
Switch>en  
Switch#
```

Sửa file config lại thành file config.text như lúc đầu :

Quote:

```
Switch#rename flash:config.old flash:config.text  
Destination filename [config.text]
```

Copy file password cũ lên để xoá, sửa :

Quote:

```
Switch#copy flash:config.text system:running-config  
Swpass#
```

Ta sửa password xong, lưu lại , kết thúc quá trình recovery password :

Quote:

```
Sw1#write memory  
Building configuration...  
[OK]
```

---

Bài 49:

## CÁC THIẾT BỊ HẠ TẦNG MẠNG KHÔNG DÂY

### 2.1. CÁC THIẾT BỊ HẠ TẦNG MẠNG KHÔNG DÂY (WLAN)

#### 2.1.1. Điểm truy cập: AP(access point)

Cung cấp cho các máy khách(client) một điểm truy cập vào mạng. AP là một thiết bị song công(Full duplex) có mức độ thông minh tương đương với một chuyển mạch Ethernet phức tạp(Switch).



**Hình 2-1: Access Point**



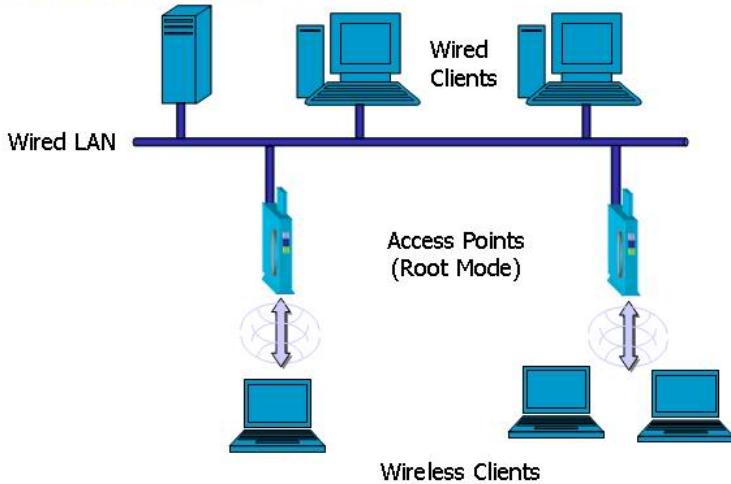
**Hình 2-2: Kết nối giữa Access Point và máy tính có hỗ trợ card mạng không dây**

### 2.1.1. Các chế độ hoạt động của AP:

AP có thể giao tiếp với các máy không dây, với mạng có dây truyền thông và với các AP khác. Có 3 Mode hoạt động chính của AP:

- Chế độ gốc (Root mode): Root mode được sử dụng khi AP được kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP sẽ hỗ trợ các mode khác ngoài root mode, tuy nhiên root mode là cấu hình mặc định. Khi một AP được kết nối với phân đoạn có dây thông qua cổng Ethernet của nó, nó sẽ được cấu hình để hoạt động trong root mode. Khi ở trong root mode, các AP được kết nối với cùng một hệ thống phân phối có dây có thể nói chuyện được với nhau thông qua phân đoạn có dây. Các client không dây có thể giao tiếp với các client không dây khác nằm trong những cell (ô tế bào, hay vùng phủ sóng của AP) khác nhau thông qua AP tương ứng mà chúng kết nối vào, sau đó các AP này sẽ giao tiếp với nhau thông qua phân đoạn có dây như ví dụ trong hình 2-3.

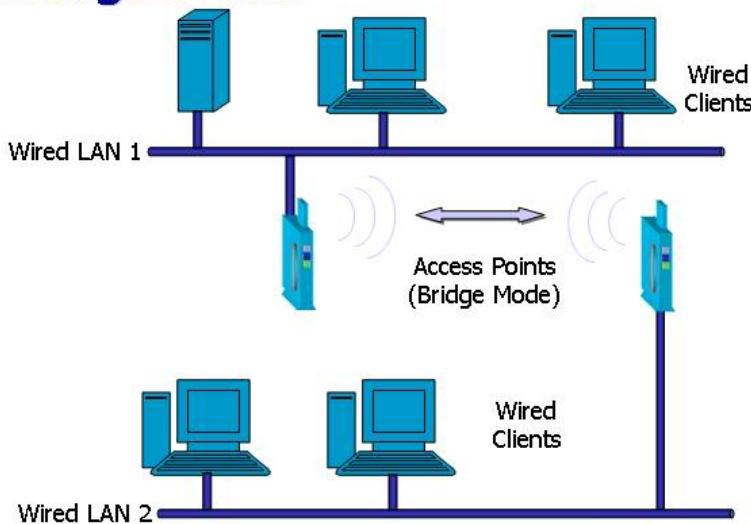
## Root Mode



Hình 2-3: Mô hình hình Root Mode

Chế độ cầu nối(Bridge Mode): Trong Bridge mode, AP hoạt động hoàn toàn giống với một cầu nối không dây. AP sẽ trở thành một cầu nối không dây khi được cấu hình theo cách này. Chỉ một số ít các AP trên thị trường có hỗ trợ chức năng Bridge, điều này sẽ làm cho thiết bị có giá cao hơn đáng kể. Chúng ta sẽ giải thích một cách ngắn gọn cầu nối không dây hoạt động như thế nào, từ hình 2-3 Client không kết nối với cầu nối, nhưng thay vào đó, cầu nối được sử dụng để kết nối 2 hoặc nhiều đoạn mạng có dây lại với nhau bằng kết nối không dây.

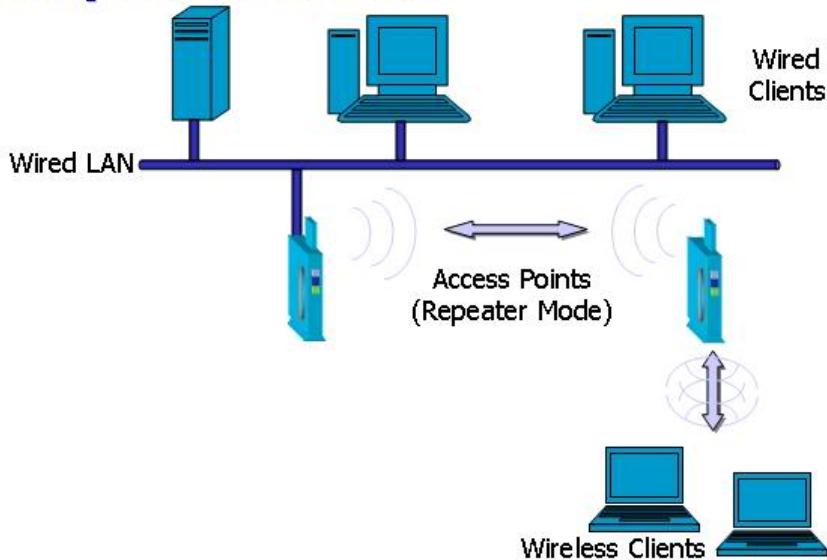
## Bridge Mode



Hình 2-4: Mô hình bridge mode

Chế độ lặp(repeater mode): AP có khả năng cung cấp một đường kết nối không dây upstream vào mạng có dây thay vì một kết nối có dây bình thường. Một AP hoạt động như là một root AP và AP còn lại hoạt động như là một Repeater không dây. AP trong repeater mode kết nối với các client như là một AP và kết nối với upstream AP như là một client.

## Repeater Mode



Hình 2-5: Mô hình Repeater mode

### 2.1.1. Các thiết bị máy khách trong WLAN:

Là những thiết bị WLAN được các máy khách sử dụng để kết nối vào WLAN.

#### 2.1.1.a. Card PCI Wireless:

Là thành phần phổ biến nhất trong WLAN. Dùng để kết nối các máy khách vào hệ thống mạng không dây. Được cắm vào khe PCI trên máy tính. Loại này được sử dụng phổ biến cho các máy tính để bàn(desktop) kết nối vào mạng không dây.



Hình 2-6: Card mạng không dây chuẩn PCI

### **2.1.1.a. Card PCMCIA Wireless:**

Trước đây được sử dụng trong các máy tính xách tay(laptop) và các thiết bị hỗ trợ cá nhân số PDA(Personal Digital Association). Hiện nay nhờ sự phát triển của công nghệ nên PCMCIA wireless ít được sử dụng vì máy tính xách tay và PDA,... đều được tích hợp sẵn Card Wireless bên trong thiết bị.



**Hình 2-7: Card mạng không dây chuẩn PCMCIA**

### **2.1.1.a. Card USB Wireless:**

Loại rất được ưu chuộng hiện nay dành cho các thiết bị kết nối vào mạng không dây vì tính năng di động và nhỏ gọn. Có chức năng tương tự như Card PCI Wireless, nhưng hỗ trợ chuẩn cắm là USB (Universal Serial Bus). Có thể tháo lắp nhanh chóng (không cần phải cắm cố định như Card PCI Wireless) và hỗ trợ cắm khi máy tính đang hoạt động.



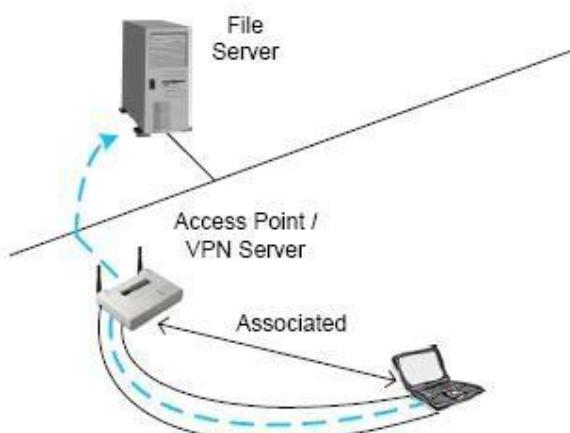
**Hình 2-8: Card mạng không dây chuẩn USB**

Bài 50:

## Một số giải pháp bảo mật trong mạng không dây

### 50.1. WLAN VPN:

Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu, và dùng các thuật toán khác để xác thực gói dữ liệu. IPSec cũng sử dụng thẻ xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, cổng kết nối của VPN đảm nhận việc xác thực, đóng gói và mã hóa.



Truy cập đến mạng LAN bên trong  
qua đường hầm VPN

Hình 50.1: WLAN VPN

### 50.2. TKIP(Temporal Key Integrity Protocol):

Là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm(hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC(message integrity check ) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

### 50.3. AES(Advanced Encryption Standard):

Là một chức năng mã hóa được phê chuẩn bởi NIST(Nation Institute of Standard and Technology). IEEE đã thiết kế một chế độ cho AES để đáp ứng nhu cầu của mạng WLAN. Chế độ này được gọi là CBC-CTR(Cipher Block Chaining Counter Mode) với CBC-MAC(Cipher Block Chaining Message Authenticity Check). Tổ hợp của chúng được gọi là AES-CCM . Chế độ CCM là sự kết hợp của mã hóa CBC-CTR và thuật toán xác thực thông điệp CBC-MAC. Sự kết hợp này cung cấp cả việc mã hóa cũng như kiểm tra tính toàn vẹn của dữ liệu gửi.

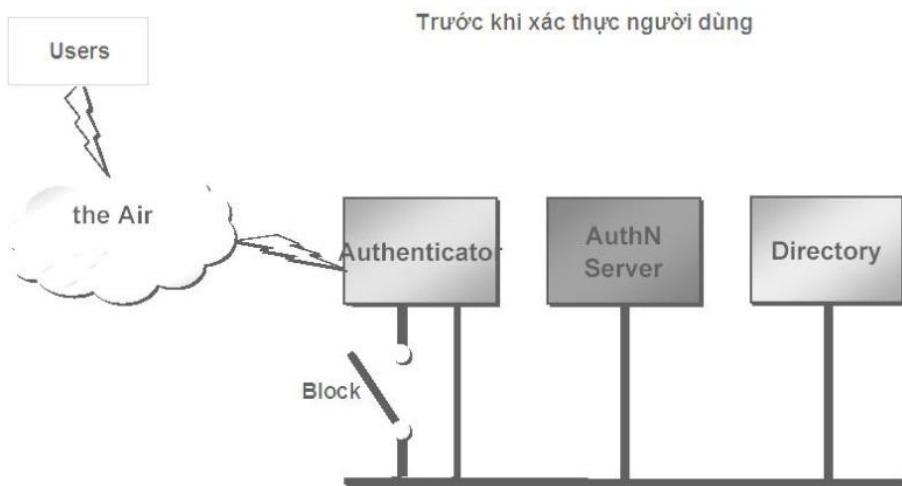
Mã hóa CBC-CTR sử dụng một biến đếm để bổ sung cho chuỗi khóa. Biến đếm sẽ tăng lên 1 sao khi mã hóa cho mỗi khối(block). Tiến trình này đảm bảo chỉ có duy nhất một khóa cho mỗi khối. Chuỗi ký tự chưa được mã hóa sẽ được phân mảnh ra thành các khối 16 byte.

CBC-MAC hoạt động bằng cách sử dụng kết quả của mã hóa CBC cùng với chiều dài frame, địa chỉ nguồn, địa chỉ đích và dữ liệu. Kết quả sẽ cho ra giá trị 128 bit và được cắt thành 64 bit để sử dụng lúc truyền thông.

AES-CCM yêu cầu chi phí khá lớn cho cả quá trình mã hóa và kiểm tra tính toàn vẹn của dữ liệu gửi nên tiêu tốn rất nhiều năng lực xử lý của CPU khá lớn.

### 50.4. 802.1x và EAP:

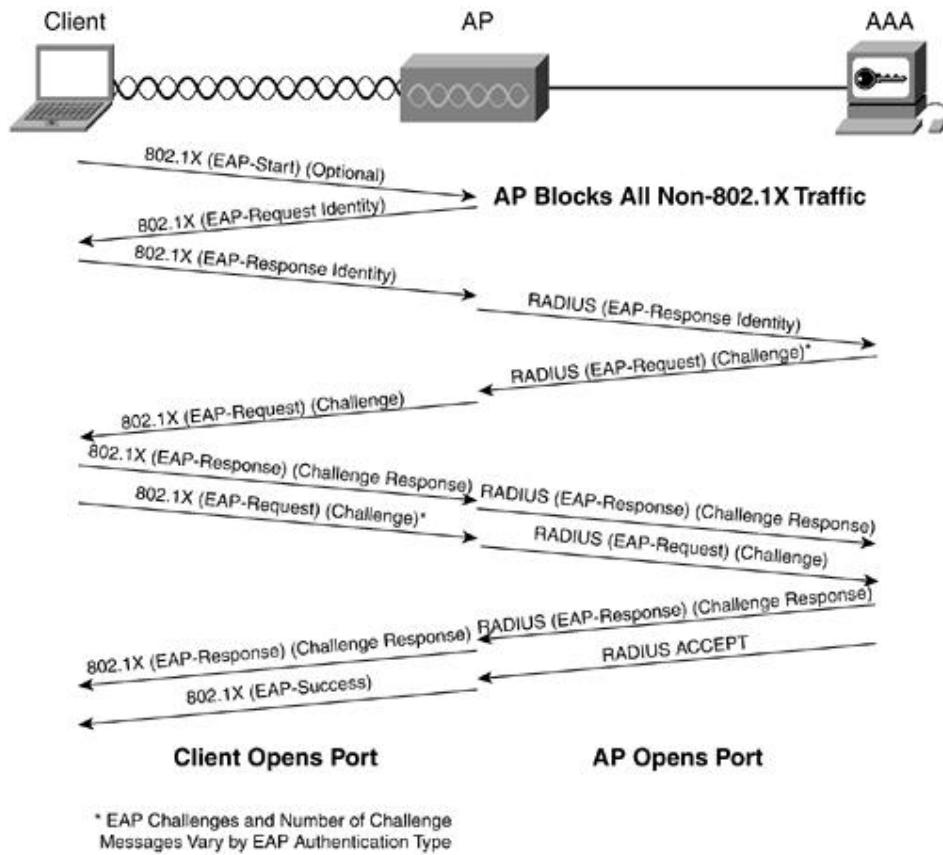
802.1x là chuẩn đặc tả cho việc truy cập dựa trên cổng(port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy cập được thực hiện bằng cách: Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn(blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.



Hình 50.2: Mô hình hoạt động xác thực của 802.1x

EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng(password, certificate,...), giao thức được sử dụng(MD5, TLS\_Transport Layer Security, OTP\_One Time Password,...) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

Mô hình xác thực 802.1X-EAP cho Client dien ra nhu sau:



The 802.1X Message Exchange

Hình 50.3: Quá trình trao đổi thông tin xác thực của 802.1x

### 50.5. WPA (Wi-Fi Protected Access)

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm.

Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lỗ hổng ở công nghệ này. Do đó, công nghệ mới có tên gọi WPA (Wi-Fi Protected Access) ra đời, khắc phục được nhiều nhược điểm của WEP.

Trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol). WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu. Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message

Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm.

Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.

Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán (đừng sử dụng những từ như "PASSWORD" để làm mật khẩu).

Điều này cũng có nghĩa rằng kỹ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu "mật" hay các thông tin nhạy cảm... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

### 50.6. WPA 2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã đổi xứng này. Và chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm. Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard). Để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít người sử dụng mạng không dây quan tâm tới vấn đề này. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

### 50.7. Lọc (Filtering)

Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP. Lọc hoạt động giống như Access list trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể được sử dụng trong wireless lan:

- + Lọc SSID
- + Lọc địa chỉ MAC
- + Lọc giao thức

### 50.7.a. Lọc SSID

Lọc SSID là một phương thức cơ bản của lọc và chỉ nên được sử dụng cho việc điều khiển truy cập cơ bản. SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với tập dịch vụ. SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ bị phát hiện bằng cách sử dụng các phần mềm. Một số sai lầm mà người sử dụng WLAN mắc phải trong việc quản lý SSID gồm:

Sử dụng giá trị SSID mặc định tạo điều kiện cho hacker dò tìm địa chỉ MAC của AP.

Sử dụng SSID có liên quan đến công ty.

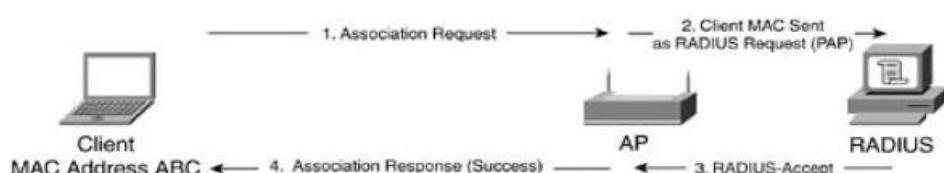
Sử dụng SSID như là phương thức bảo mật của công ty.

Quảng bá SSID một cách không cần thiết.

### 50.7.b. Lọc địa chỉ MAC

Hầu hết các AP đều có chức năng lọc địa chỉ MAC. Người quản trị có thể xây dựng danh sách các địa chỉ MAC được cho phép. Nếu client có địa chỉ MAC không nằm trong danh sách lọc địa chỉ MAC của AP thì AP sẽ ngăn chặn không cho phép client đó kết nối vào mạng. Nếu công ty có nhiều client thì có thể xây dựng máy chủ RADIUS có chức năng lọc địa chỉ MAC thay vì AP.

Cấu hình lọc địa chỉ MAC là giải pháp bảo mật có tính mở rộng cao.

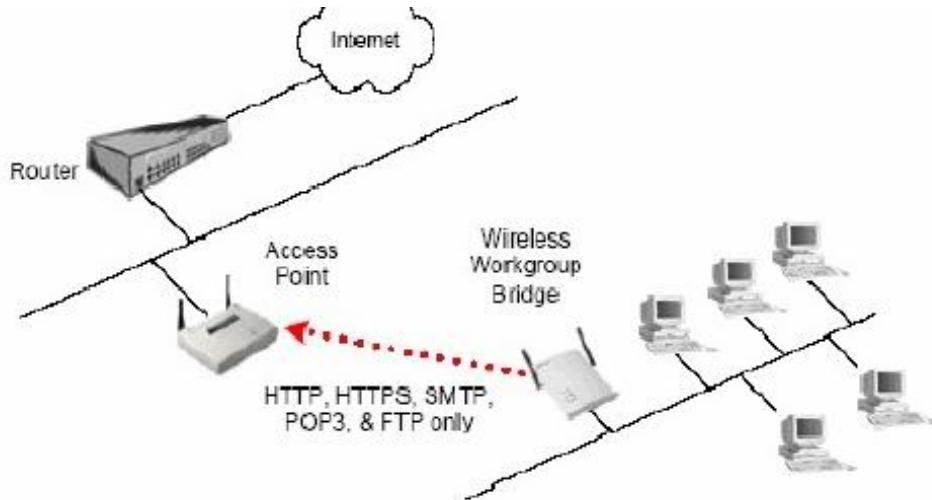


Hình 50.4: Tiến trình xác thực MAC

### 50.7.c. Lọc giao thức

Mạng Lan không dây có thể lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7. Trong nhiều trường hợp người quản trị nên cài đặt lọc giao thức trong môi trường dùng chung, ví dụ trong trường hợp sau:

Có một nhóm cầu nối không dây được đặt trên một Remote building trong một mạng WLAN của một trường đại học mà kết nối lại với AP của tòa nhà kỹ thuật trung tâm. Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5Mbs giữa những tòa nhà này, nên một số lượng đáng kể các điều khiển trên các sử dụng này phải được thực hiện. Nếu các kết nối này được cài đặt với mục đích đặc biệt của sự truy nhập internet của người sử dụng, thì bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ HTTP, SMTP, HTTPS, FTP...



**Hình 50.5: Lọc giao thức**

### Bài 51:

## CÁC KIẾU TẤN CÔNG TRONG MẠNG WLAN

Một số hình thức tấn công xâm nhập mạng không dây phổ biến:

### 51.1. ROGUE ACCESS POINT

#### 51.1.a. Định nghĩa

Access Point giả mạo được dùng để mô tả những Access Point được tạo ra một cách vô tình hay cố ý làm ảnh hưởng đến hệ thống mạng hiện có. Nó được dùng để chỉ các thiết bị hoạt động không dây trái phép mà không quan tâm đến mục đích thực của chúng.

#### 51.b. Phân loại

##### a) Access Point được cấu hình không hoàn chỉnh

Một Access Point có thể bất ngờ trở thành 1 thiết bị giả mạo do sai sót trong việc cấu hình. Sự thay đổi trong Service Set Identifier(SSID), thiết lập xác thực, thiết lập mã hóa,... điều nghiêm trọng nhất là chúng sẽ không thể chứng thực các kết nối nếu bị cấu hình sai. Ví dụ: trong trạng thái xác thực mở (open mode authentication) các người dùng không dây ở trạng thái 1(chưa xác thực và chưa kết nối) có thể gửi các yêu cầu xác thực đến một Access Point và được

xác thực thành công sẽ chuyển sang trạng thái 2 (được xác thực nhưng chưa kết nối). Nếu 1 Access Point không xác nhận sự hợp lệ của một máy khách do lỗi trong cấu hình, kẻ tấn công có thể gửi một số lượng lớn yêu cầu xác thực, làm tràn băng yêu cầu kết nối của các máy khách ở Access Point, làm cho Access Point từ chối truy cập của các người dùng khác bao gồm cả người dùng được phép truy cập.

**b) Access Point giả mạo từ các mạng WLAN lân cận**

Các máy khách theo chuẩn 802.11 tự động chọn Access Point có sóng mạnh nhất mà nó phát hiện được để kết nối. ví dụ: Windows XP tự động kết nối đến kết nối tốt nhất có thể xung quanh đó. Vì vậy, những người dùng được xác thực của một tổ chức có thể kết nối đến các Access Point của các tổ chức khác lân cận. Mặc dù các Access Point lân cận không cố ý thu hút kết nối từ các người dùng, những kết nối đó vô tình để lộ những dữ liệu nhạy cảm.

**c) Access Point giả mạo do kẻ tấn công tạo ra**

Giả mạo AP là kiểu tấn công “man in the middle” cổ điển. Đây là kiểu tấn công mà tin tức đứng ở giữa và trộm lưu lượng truyền giữa 2 nút. Kiểu tấn công này rất mạnh vì tin tức có thể trộm tất cả lưu lượng đi qua mạng. Rất khó khăn để tạo một cuộc tấn công “man in the middle” trong mạng có dây bởi vì kiểu tấn công này yêu cầu truy cập thực sự đến đường truyền. Trong mạng không dây thì lại rất dễ bị tấn công kiểu này. Tin tức cần phải tạo ra một AP thu hút nhiều sự lựa chọn hơn AP chính thống. AP giả này có thể được thiết lập bằng cách sao chép tất cả các cấu hình của AP chính thống đó là: SSID, địa chỉ MAC v.v.. Bước tiếp theo là làm cho nạn nhân thực hiện kết nối tới AP giả.

- Cách thứ nhất là đợi cho người dùng tự kết nối.
- Cách thứ hai là gây ra một cuộc tấn công từ chối dịch vụ DoS trong AP chính thống do vậy người dùng sẽ phải kết nối lại với AP giả.

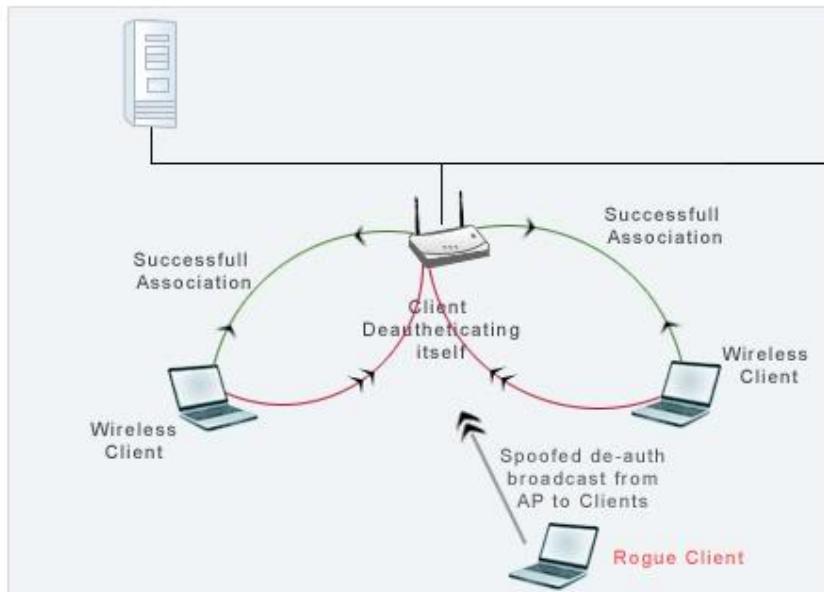
Trong mạng 802.11 sự lựa chọn AP được thực hiện bởi cường độ của tín hiệu nhận. Điều duy nhất tin tức phải thực hiện là chắc chắn rằng AP của mình có cường độ tín hiệu mạnh hơn cả. Để có được điều đó tin tức phải đặt AP của mình gần người bị lừa hơn là AP chính thống hoặc sử dụng kỹ thuật anten định hướng. Sau khi nạn nhân kết nối tới AP giả, nạn nhân vẫn hoạt động như bình thường do vậy nếu nạn nhân kết nối đến một AP chính thống khác thì dữ liệu của nạn nhân đều đi qua AP giả. Tin tức sẽ sử dụng các tiện ích để ghi lại mật khẩu của nạn nhân khi trao đổi với Web Server. Như vậy tin tức sẽ có được tất cả những gì anh ta muốn để đăng nhập vào mạng chính thống. Kiểu tấn công này tồn tại là do trong 802.11 không yêu cầu chứng thực 2 hướng giữa AP và nút. AP phát quảng bá ra toàn mạng. Điều này rất dễ bị tin tức nghe trộm và do vậy tin tức có thể lấy được tất cả các thông tin mà chúng cần. Các nút trong mạng sử dụng WEP để chứng thực chúng với AP nhưng WEP cũng có những lỗ hổng có thể khai thác. Một tin tức có thể nghe trộm thông tin và sử dụng bộ phân tích mã hoá để trộm mật khẩu của người dùng

**d) Access Point giả mạo được thiết lập bởi chính nhân viên của công ty**

Vì sự tiện lợi của mạng không dây một số nhân viên của công ty đã tự trang bị Access Point và kết nối chúng vào mạng có dây của công ty. Do không hiểu rõ và nắm vững về bảo mật trong mạng không dây họ vô tình tạo ra một lỗ hổng lớn về bảo mật. Những người lạ vào công ty và hacker bên ngoài có thể kết nối

đến Access Point không được xác thực để đánh cắp băng thông, đánh cắp thông tin nhạy cảm của công ty, sử dụng hệ thống mạng của công ty tấn công người khác,...

### 51.2. De-authentication Flood Attack (tấn công yêu cầu xác thực lại )

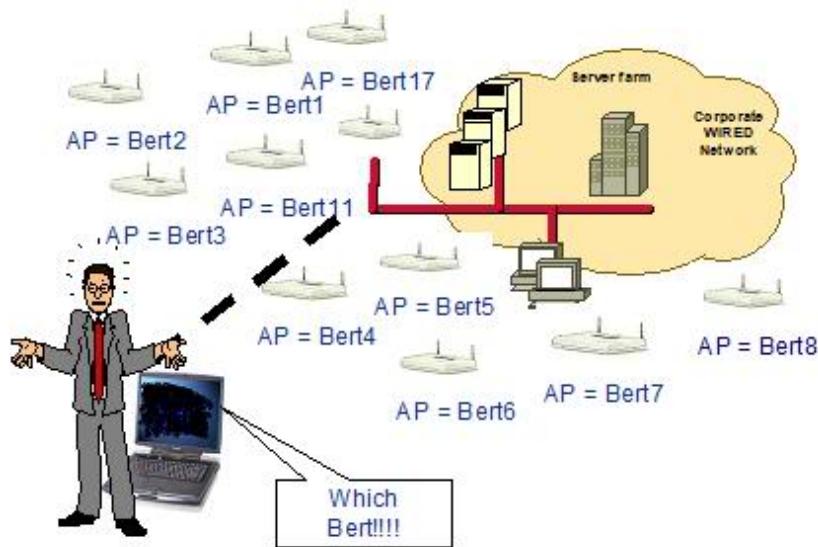


Hình 51.1: Mô tả tấn công de-authentication flood

- Kẻ tấn công xác định mục tiêu tấn công là các người dùng trong mạng wireless và các kết nối của họ(Access Point đến các kết nối của nó).
- Chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng.
- Người dùng wireless khi nhận được frame yêu cầu xác thực lại thì nghĩ rằng chúng do Access Point gửi đến.
- Sau khi ngắt được một người dùng ra khỏi dịch vụ không dây, kẻ tấn công tiếp tục thực hiện tương tự đối với các người dùng còn lại.
- Thông thường người dùng sẽ kết nối lại để phục hồi dịch vụ, nhưng kẻ tấn công đã nhanh chóng tiếp tục gửi các gói yêu cầu xác thực lại cho người dùng.

### 51.3. Fake Access Point

Kẻ tấn công sử dụng công cụ có khả năng gửi các gói beacon với địa chỉ vật lý(MAC) giả mạo và SSID giả để tạo ra vô số Access Point giả lập. Điều này làm xáo trộn tất cả các phần mềm điều khiển card mạng không dây của người dùng.

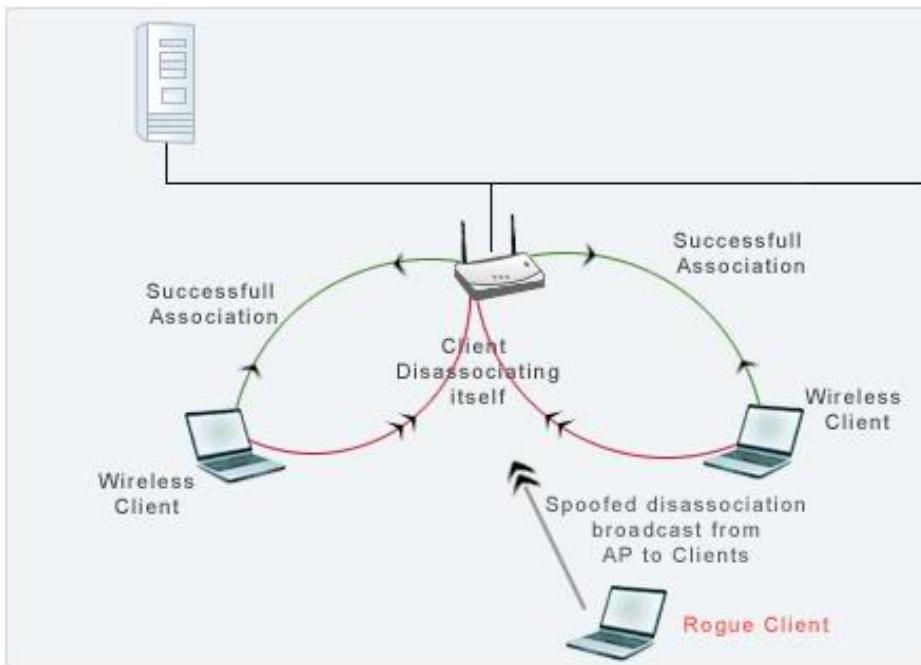


**Hình 51.2: Tấn công Fake AP**

#### 51.4. Tấn công dựa trên sự cảm nhận sóng mang lớp vật lý

Tần số là một nhược điểm bảo mật trong mạng không dây. Mức độ nguy hiểm thay đổi phụ thuộc vào giao diện của lớp vật lý. Có một vài tham số quyết định sự chịu đựng của mạng là: năng lượng máy phát, độ nhạy của máy thu, tần số RF, băng thông và sự định hướng của anten. Trong 802.11 sử dụng thuật toán đa truy cập cảm nhận sóng mang (CSMA) để tránh va chạm. CSMA là một thành phần của lớp MAC. CSMA được sử dụng để chắc chắn rằng sẽ không có va chạm dữ liệu trên đường truyền. Kiểu tấn công này không sử dụng tạp âm để tạo ra lỗi cho mạng nhưng nó sẽ lợi dụng chính chuẩn đó. Có nhiều cách để khai thác giao thức cảm nhận sóng mang vật lý. Cách đơn giản là làm cho các nút trong mạng đều tin tưởng rằng có một nút đang truyền tin tại thời điểm hiện tại. Cách dễ nhất đạt được điều này là tạo ra một nút giả mạo để truyền tin một cách liên tục. Một cách khác là sử dụng bộ tạo tín hiệu RF. Một cách tấn công tinh vi hơn là làm cho card mạng chuyển vào chế độ kiểm tra mà ở đó nó truyền đi liên tiếp một mẫu kiểm tra. Tất cả các nút trong phạm vi của một nút giả là rất nhạy với sóng mang và trong khi có một nút đang truyền thì sẽ không có nút nào được truyền.

### 51.5. Tấn công ngắt kết nối (Disassociation flood attack)



Hình 51.3: Mô tả tấn công disassociation flood

- Kẻ tấn công xác định mục tiêu ( wireless clients ) và mối liên kết giữa AP với các clients
- Kẻ tấn công gửi disassociation frame bằng cách giả mạo Source và Destination MAC đến AP và các client tương ứng
- Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Đồng thời kẻ tấn công cũng gửi disassociation frame đến AP.
- Sau khi đã ngắt kết nối của một client, kẻ tấn công tiếp tục thực hiện tương tự với các client còn lại làm cho các client tự động ngắt kết nối với AP.
- Khi các clients bị ngắt kết nối sẽ thực hiện kết nối lại với AP ngay lập tức. Kẻ tấn công tiếp tục gửi disassociation frame đến AP và client.