**BỘ GIÁO DỤC VÀ ĐÀO TẠO**
**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**----------o0o----------**

# LUẬN VĂN THẠC SĨ KHOA HỌC

# SỬ DỤNG IP CHO MẠNG DI ĐỘNG THẾ HỆ MỚI

NGÀNH: XỬ LÝ THÔNG TIN VÀ TRUYỀN THÔNG

MÃ SỐ:

PHẠM THỊ THANH HUYỀN

Người hướng dẫn khoa học: TS. PHẠM HUY HOÀNG

HÀ NỘI 2006

# DANH MỤC CÁC CHỮ VIẾT TẮT

| STT | Chữ viết tắt | Tiếng Anh |
|---|---|---|
| 1 | 3GPP | 3rd Generation Partnership Project |
| 2 | ATM | Asynchronous Transfer Mode |
| 3 | CDMA | Code division multiple access |
| 4 | CN | Correspondant Node |
| 5 | COA | Care-Of-Address |
| 6 | DHCP | Dynamic Host Configuration Protocol |
| 7 | EDGE | Enhanced Data rates for GSM Evolution |
| 8 | FA | Foreign Agent |
| 9 | FA | Foreign Agent |
| 10 | FDMA | Frequency Division Multiple Access |
| 11 | FN | Foreign Network |
| 12 | FN | Foreign network |
| 13 | GGSN | Gateway GPRS Support Node |
| 14 | GPRS | General Packet Radio Service |
| 15 | GRU | Globally Routable Unicast |
| 16 | GSM | Global System for Mobile Communications |
| 17 | HA | Home Agent |
| 18 | HN | Home network |
| 19 | HN | Home network |
| 20 | HSCSD | High-Speed Circuit-Switched Data |
| 21 | ICMP | Internet Control Message Protocol |
| 22 | ICMP | Internet Control Message Protocol |
| 23 | IETF | Internet Engineering Task Force |

| | | |
|---|---|---|
| 24 | IETF | Internet Engineering Task Force |
| 25 | IMT-2000 | International Mobile Telecommunications-2000 |
| 26 | IP | Internet Protocol |
| 27 | MIP | Mobile Internet Protocol |
| 28 | MN | Mobile Node |
| 29 | MN | Mobile Node |
| 30 | MTU | Maximum Transfer Unit |
| 31 | NGN | Next Generation Network |
| 32 | NLA | Next level gregator |
| 33 | PSDN | Packet Data Serving Node |
| 34 | TDMA | Time Division Multiple Access |
| 35 | TTL | Time to Live |
| 36 | UMTS | Universal Mobile Telecommunications |
| 37 | UTRAN | UMTS Terrestrial Radio Access |

# DANH MỤC CÁC BẢNG



# DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

# MỞ ĐẦU

Từ những thời gian đầu vào những năm 70 và 80 của Internet và cho đến ngày nay, Internet đã tạo lập cho mình một vị trí thống trị trong truyền thông toàn cầu cho phép tạo ra một số lượng rất đa dạng các ứng dụng máy tính. Các ứng dụng Internet hiển nhiên là hết sức cần thiết xét từ góc độ Internet, nhưng tất cả các dự báo đều cho thấy các ứng dụng này cũng trở nên cần thiết với hầu hết các mạng vô tuyến trong tương lai. Ngành công nghiệp này cũng đã nhận thức được rất rõ các hạn chế của giao thức IPv4, các nhà cung cấp mạng di động thế hệ sau cũng như các nhà cung cấp thiết bị cho biết họ cần số lượng địa chỉ IP cho hàng triệu thiết bị. Một trong những tiêu chí chính của các nhà khai thác mạng di động tương lai là khả năng luôn luôn kết nối với mạng của người sử dụng. Điều này đòi hỏi một số lượng lớn địa chỉ IP. IPv6 cung cấp thêm nhiều khả năng trong đó đáng chú ý nhất là sự mở rộng về không gian địa chỉ, IPv6 có không gian địa chỉ là 128 bit trong khi IPv4 chỉ sử dụng 32 bit.

Việc tổ hợp IPv6 và các hệ thống di động (như GSM/GPRS và UMTS) sẽ giảm thiểu được các vấn đề hiện tại về sự thiếu hụt của cả hai bên IP và mạng di động: thiếu địa chỉ IP, chất lượng dịch vụ và bảo mật trong IP và sự thiếu hụt phổ tần trong mạng di động. Bằng cách tổ hợp hai công nghệ này, có thể đảm bảo cung cấp lợi ích tốt nhất cho người sử dụng di động đầu cuối.

Trong luận văn này trình bày các vấn đề cần thiết khi đưa IPv6 vào mạng di động tương lai. Chương 1 trình bày tổng quan về mạng 3G, chương 2 giới thiệu về mobile IP, chương 3 trình bày về IPv6 và chương 4 đưa ra các giải pháp thực hiện IPv6 trên nền IPv4.

# CHƯƠNG 1. TỔNG QUAN VỀ MẠNG 3G

## 1.1. Lịch sử phát triển.

Những hệ thống thông tin di động đầu tiên, nay được gọi là thế hệ thứ nhất (1G), sử dụng công nghệ analog gọi là đa truy nhập phân chia theo tần số (FDMA) để truyền kênh thoại trên sóng vô tuyến đến thuê bao điện thoại di động. Nhược điểm của các hệ thống này là chất lượng thấp, vùng phủ sóng hẹp và dung lượng nhỏ. Vào cuối thập niên 1980, các hệ thống thế hệ thứ hai (2G) được đưa vào khai thác sử dụng công nghệ số đa truy nhập phân chia theo thời gian (TDMA). Đến đầu thập niên 1990, công nghệ TDMA được dùng cho hệ thống thông tin di động toàn cầu GSM ở Châu Âu. Đến giữa thập kỷ 1990, đa truy nhập phân chia theo mã (CDMA) trở thành loại hệ thống 2G thứ hai khi người Mỹ đưa ra Tiêu chuẩn nội địa - 95 (IS-95), nay gọi là cdmaOne.

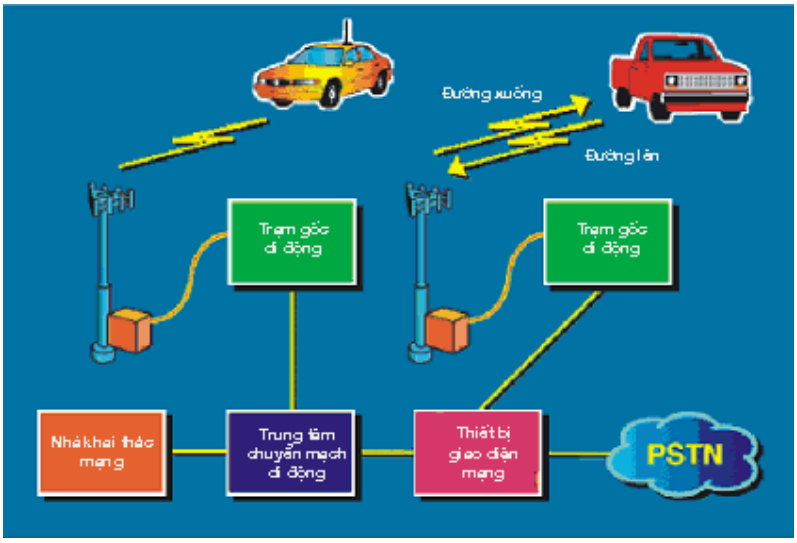
Tất cả các hệ thống 2G đều có khả năng cung cấp chất lượng và dung lượng cao hơn. Chuyển vùng trở thành một phần của dịch vụ và vùng phủ sóng cũng ngày một rộng hơn, nhưng vẫn phải đối mặt với các vấn đề hạn chế về dung lượng trên nhiều thị trường. Thông tin di động ngày nay đang tiến tới một hệ thống thế hệ thứ ba hứa hẹn dung lượng thoại lớn hơn, kết nối dữ liệu di động tốc độ cao hơn và sử dụng các ứng dụng đa phương tiện. Các hệ thống vô tuyến thế hệ thứ 3 (3G) cần cung cấp dịch vụ thoại với chất lượng tương đương các hệ thống hữu tuyến và dịch vụ truyền số liệu có tốc độ từ 144kbit/s đến 2 Mbit/s.

Hiện đang có 2 hệ thống tiêu chuẩn hoá: một chuẩn dựa trên hệ thống CDMA băng hẹp IS-95, được gọi là cdma2000. Chuẩn kia là sự kết hợp của các tiêu chuẩn Nhật Bản và Châu Âu do Dự án Hợp tác Thế hệ thứ 3 (3GPP) tổ chức. 3GPP đang xem xét tiêu chuẩn vô tuyến tên là truy nhập vô tuyến

mặt đất (UTRA-UMTS Terrestrial Radio Access) UMTS. Tiêu chuẩn này có 2 sơ đồ truy nhập vô tuyến. Một trong số đó sắp xếp các cặp dải tần thông qua ghép song công phân chia theo tần số (FDD)-thường gọi là CDMA băng thông rộng (WCDMA).

### 1.1.1. Các kỹ thuật đa truy nhập (FDMA, TDMA VÀ CDMA).

Trước khi xem xét tương lai 3G, cũng cần khảo sát hoạt động của từng giao diện nói trên. Thứ nhất, các kênh này được ghép cặp sao cho một kênh đi từ trạm di động đến trạm gốc và kênh kia đi từ trạm gốc đến trạm di động, tạo điều kiện cho liên lạc song công. Hình 1.1 minh hoạ giao diện không gian với đường lên và đường xuống. Thứ hai, có một tập các kênh điều khiển 2 chiều dùng để điều khiển các kênh thoại. Cuối cùng, giao diện không gian cần một quy trình mà ở đó, các kênh thoại được phân bổ cho nhiều người dùng đồng thời. FDMA, TDMA và CDMA là các phương thức phân bổ kênh của giao diện không gian.




Hình 1.1. Tổng quan về hệ thống vô tuyến

- FDMA là phương thức phân bổ đầu tiên và ra đời sớm nhất. Một thuê bao muốn tạo một cuộc gọi sẽ phải nhập số điện thoại cần gọi và nhấn phím gửi.

Nếu còn dung lượng thoại cho tế bào, một cặp kênh sẽ được phân bổ cho trạm di động để phục vụ đàm thoại - mỗi kênh cho một chiều thoại. Xét trên một sơ đồ phân bổ tế bào điển hình, số chiều thoại tối đa của một tế bào bất kỳ là khoảng 60. Rõ ràng là không thể phục vụ hàng triệu người dùng với một dung lượng hạn chế như thế.

- Các hệ thống TDMA khắc phục vấn đề dung lượng kênh bằng cách chia kênh vô tuyến đơn thành các khe thời gian và phân bổ 1 khe thời gian cho mỗi thuê bao. Ví dụ, hệ thống TDMA của Hoa Kỳ có 3 khe thời gian trên mỗi kênh trong khi hệ thống GSM có 8 khe thời gian trên mỗi kênh. Để sử dụng các khe thời gian, tín hiệu thoại tương tự cần được chuyển sang dạng số. Một bộ mã hoá thoại, được gọi là vocoder, thực hiện công việc này. Dung lượng có được ban đầu hơi nhỏ song với việc dùng các vocoder tốc độ bít thấp, số kênh thoại trên mỗi kênh vô tuyến có thể được tăng lên đáng kể.... Công nghệ này đòi hỏi vốn đầu tư ban đầu ít tốn kém hơn CDMA.

- Còn công nghệ đa truy nhập phân chia theo mã CDMA là công nghệ trải phổ cho phép nhiều tần số được sử dụng đồng thời; mã hóa từng gói tín hiệu số bằng một mã khóa duy nhất trước khi đưa lên kênh vật lý và gửi đi. Quá trình này còn được gọi là điều chế tạp âm vì tín hiệu đầu ra của nó giống như tạp âm nền. Bộ nhận CDMA chỉ biết nhận và giải mã. Công nghệ này có tính bảo mật tín hiệu cao hơn TDMA. Theo các chuyên gia CNTT Việt Nam, xét ở góc độ bảo mật thông tin, CDMA có tính năng ưu việt hơn.

Nhờ hệ thống kích hoạt thoại, hiệu suất tái sử dụng tần số trải phổ cao và điều khiển năng lượng, nên nó cho phép quản lý số lượng thuê bao cao gấp 5 - 20 lần so với công nghệ GSM. Áp dụng kỹ thuật mã hóa thoại mới, CDMA nâng chất lượng thoại lên ngang bằng với hệ thống điện thoại hữu tuyến. Đối với điện thoại di động, để đảm bảo tính di động, các trạm phát phải được đặt rải rác khắp nơi. Mỗi trạm sẽ phủ sóng một vùng nhất định và chịu trách

nhiệm với các thuê bao trong vùng đó. Với CDMA, ở vùng chuyển giao, thuê bao có thể liên lạc với 2 hoặc 3 trạm thu phát cùng một lúc, do đó cuộc gọi không bị ngắt quãng, làm giảm đáng kể xác suất rớt cuộc gọi.

Một ưu điểm khác nữa của CDMA là nhờ sử dụng các thuật toán điều khiển nhanh và chính xác, thuê bao chỉ phát ở mức công suất vừa đủ để đảm bảo chất lượng tín hiệu, giúp tăng tuổi thọ của pin, thời gian chờ và đàm thoại. Máy điện thoại di động CDMA cũng có thể sử dụng pin nhỏ hơn, nên trọng lượng máy nhẹ, kích thước gọn và dễ sử dụng.

Trong thông tin di động, thuê bao di động di chuyển khắp nơi với nhiều tốc độ khác nhau, vì thế tín hiệu phát ra có thể bị sụt giảm một cách ngẫu nhiên. Để bù cho sự sụt giảm này, hệ thống phải điều khiển cho thuê bao tăng mức công suất phát. Các hệ thống analog và GSM hiện nay có khả năng điều khiển chậm và đơn giản, thuê bao không thể thay đổi mức công suất đủ nhanh, do đó phải luôn luôn phát ở công suất cao hơn vài dB so với mức cần thiết. Tuy nhiên, để sử dụng mạng điện thoại di động CDMA, người dùng phải trang bị thiết bị đầu cuối phù hợp với công nghệ của mạng. Trong vấn đề bảo mật, CDMA cung cấp chế độ bảo mật cao nhờ sử dụng tín hiệu trải băng phổ rộng. Các tín hiệu băng rộng khó bị rò ra vì nó xuất hiện ở mức nhiễu, những người có ý định nghe trộm sẽ chỉ nghe được những tín hiệu vô nghĩa. Ngoài ra, với tốc độ truyền nhanh hơn các công nghệ hiện có, nhà cung cấp dịch vụ có thể triển khai nhiều tùy chọn dịch vụ như thoại, thoại và dữ liệu, fax, Internet...

Không chỉ ứng dụng trong hệ thống thông tin di động, CDMA còn thích hợp sử dụng trong việc cung cấp dịch vụ điện thoại vô tuyến cố định với chất lượng ngang bằng với hệ thống hữu tuyến, nhờ áp dụng kỹ thuật mã hóa mới. Đặc biệt các hệ thống này có thể triển khai và mở rộng nhanh và chi phí hiện thấp hơn hầu hết các mạng hữu tuyến khác, vì đòi hỏi ít trạm thu phát.

Tuy nhiên, những máy điện thoại di động đang sử dụng chuẩn GSM hiện nay không thể sử dụng chuẩn CDMA. Nếu tiếp tục phát triển GSM, hệ thống thông tin di động này sẽ phải phát triển lên WTDMA mới đáp ứng được nhu cầu truy cập di động các loại thông tin từ mạng Internet với tốc độ cao, thay vì với tốc độ 9.600 bit/giây như hiện nay, và so với tốc độ 144.000 bit/giây của CDMA

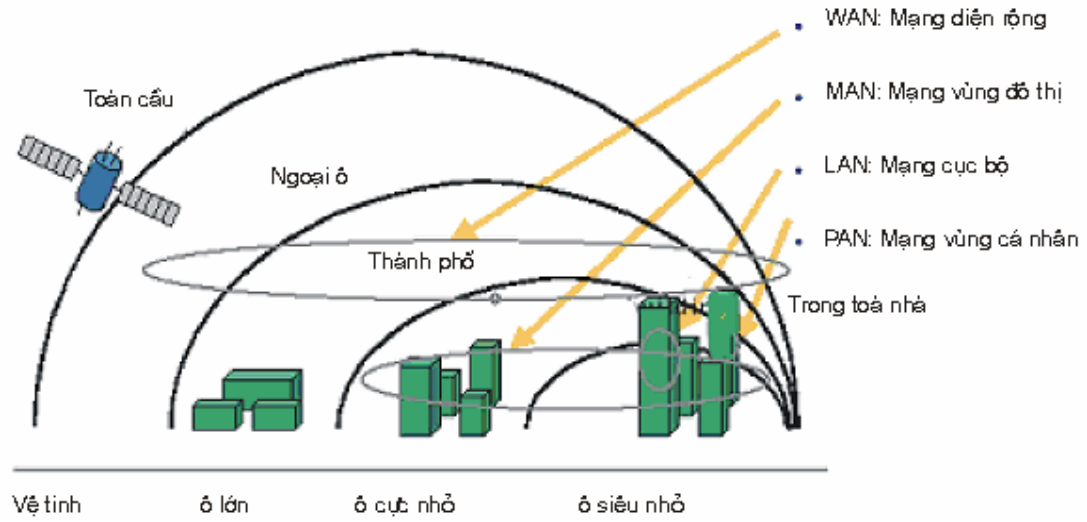
Trong hơn một tỷ thuê bao điện thoại di động trên thế giới, khoảng 863,6 triệu thuê bao sử dụng công nghệ GSM, 120 triệu dùng CDMA và 290 triệu còn lại dùng FDMA hoặc TDMA. Khi tiến tới 3G, các hệ thống GSM và CDMA sẽ tiếp tục phát triển trong khi TDMA và FDMA sẽ chìm dần vào quên lãng. Con đường GSM sẽ tới là CDMA băng thông rộng (WCDMA) trong khi CDMA sẽ là cdma2000.

### 1.1.2. Mạng di động 3G

Từ thập niên 1990, Liên minh Viễn thông Quốc tế đã bắt tay vào việc phát triển một nền tảng chung cho các hệ thống viễn thông di động. Kết quả là một sản phẩm được gọi là Thông tin di động toàn cầu 2000 (IMT-2000). Con số 2000 có nghĩa là sản phẩm này sẽ có mặt vào khoảng năm 2000, nhưng thực tế là chậm đến 2, 3 năm. IMT-2000 không chỉ là một bộ dịch vụ, nó đáp ứng ước mơ liên lạc từ bất cứ nơi đâu và vào bất cứ lúc nào. Để được như vậy, IMT-2000 tạo điều kiện tích hợp các mạng mặt đất và (hoặc) vệ tinh. Hơn thế nữa, IMT-2000 cũng đề cập đến Internet không dây, hội tụ các mạng cố định và di động, quản lý di động (chuyển vùng), các tính năng đa phương tiện di động, hoạt động xuyên mạng và liên mạng.

Như đã nói, các hệ thống 3G cần phải hoạt động trên một dải phổ đủ rộng và cung cấp được các dịch vụ thoại, dữ liệu, đa phương tiện. Đối với một thuê bao hoạt động trên một ô siêu nhỏ (picrocell), tốc độ dữ liệu có thể đến 2,048 Mbit/s. Với một thuê bao di động với tốc độ chậm hoạt động trên một ô cực

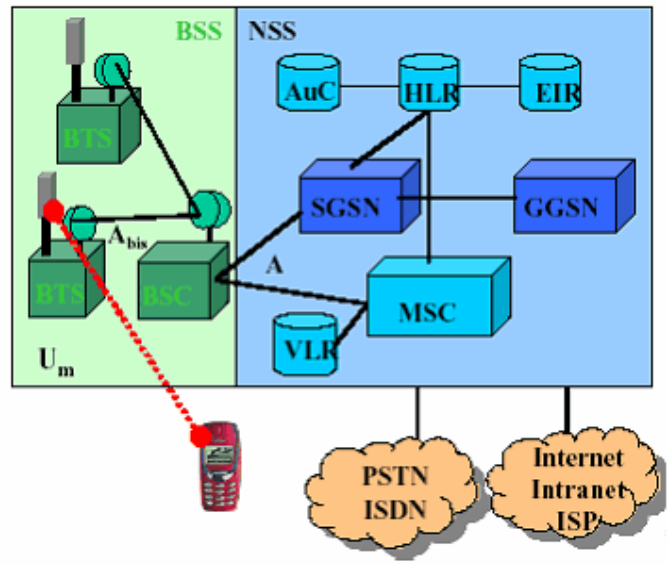
nhỏ (microcell), tốc độ dữ liệu có thể đạt tới 348 kbit/s. Với một người dùng di động trên phương tiện giao thông hoạt động trên một ô lớn (macrocell), tốc độ dữ liệu có thể đạt tới 144 kbit/s. Hình 1.2 minh hoạ mối quan hệ giữa các khu vực dịch vụ khác nhau của IMT-2000. Một phần quan trọng của hệ thống này là dịch vụ chuyển mạch gói dữ liệu. Con đường tiến lên 3G từ 2G bắt đầu từ sự ra đời của các dịch vụ dữ liệu bùng nổ và theo gói.




Hình 1.2. Các khu vực dịch vụ của IMT-2000

Con đường tiến tới 3G duy nhất của GSM là CDMA băng thông rộng. Trên thị trường châu Âu, WCDMA được gọi là Hệ thống viễn thông di động toàn cầu (UMTS). Trong cấu trúc dịch vụ 3G, cần có băng thông rất lớn và như thế cần nhiều phổ tần hơn. Các nhà cung cấp dịch vụ châu Âu dùng hơn 100 tỷ USD để mua phổ tần cho các dịch vụ 3G, các nhà cung cấp dịch vụ khác trên thế giới cũng đã phân bổ phổ 3G. Ở Hoa Kỳ, FCC chưa thể nhanh chóng phân bổ bất cứ phổ nào cho các dịch vụ 3G. Hoa Kỳ có khoảng 190MHz phổ tần phân bổ cho các dịch vụ vô tuyến di động trong khi phần còn lại của thế giới chỉ được phân bổ 400 MHz. Vì thế có thể tin rằng sự phát triển lên 3G ở Hoa Kỳ sẽ rất khác với phần còn lại của thế giới.

Để đến 3G có lẽ cần phải đi qua giai đoạn 2,5G. Nói chung, 2,5G bao gồm một hoặc tất cả các công nghệ sau: Dữ liệu chuyển mạch gói tốc độ cao (HSCSD), Dịch vụ vô tuyến gói chung (GPRS), Tốc độ dữ liệu nâng cao cho sự phát triển GSM hay toàn cầu (EDGE).




Hình 1.3. Cấu trúc hệ thống GPRS.

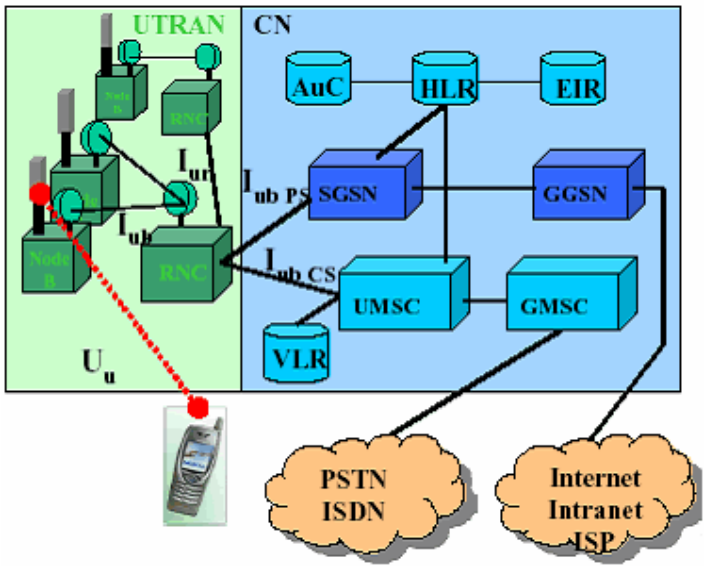
- HSCSD là phương thức đơn giản nhất để nâng cao tốc độ. Thay vì một khe thời gian, một trạm di động có thể sử dụng một số khe thời gian để kết nối dữ liệu. Trong các ứng dụng thương mại hiện nay, thông thường sử dụng tối đa 4 khe thời gian, một khe thời gian có thể sử dụng hoặc tốc độ 9,6kbit/s hoặc 14,4kbit/s. Đây là cách không tốn kém nhằm tăng dung lượng dữ liệu chỉ bằng cách nâng cấp phần mềm của mạng (dĩ nhiên là cả các máy tương thích HSCSD). Nhưng nhược điểm lớn nhất của nó là cách sử dụng tài nguyên vô tuyến. Bởi đây là hình thức chuyển mạch kênh, HSCSD chỉ định việc sử dụng các khe thời gian một cách liên tục, thậm chí ngay cả khi không có tín hiệu trên đường truyền.

- Giải pháp tiếp theo là GPRS và dường như là giải pháp được nhiều nhà cung cấp lựa chọn. Tốc độ dữ liệu của nó có thể lên tới 115,2kbit/s bằng việc dùng 8 khe thời gian. Nó được quan tâm vì là hệ thống chuyển mạch gói, do đó nó không sử dụng tài nguyên vô tuyến một cách liên tục mà chỉ thực hiện khi có một cái gì đó để gửi đi. GPRS đặc biệt thích hợp với các ứng dụng phi thời gian thực như email, lướt Web. Triển khai hệ thống GPRS thì tốn kém hơn hệ thống HSCSD. Mạng này cần các thành phần mới, cũng như cần sửa đổi các thành phần hiện có nhưng nó được xem là bước đi cần thiết để tiến tới tăng dung lượng, dịch vụ. Một mạng GSM mà không có khả năng GPRS sẽ không tồn tại lâu trong tương lai.

Bước tiếp theo là cải tiến GSM thành tốc độ dữ liệu nâng cao cho sự phát triển GSM hay toàn cầu (EDGE), tăng tốc độ dữ liệu lên tới 384kbit/s với 8 khe thời gian. Thay vì 14,4kbit/s cho mỗi khe thời gian, EDGE đạt tới 48kbit/s cho một khe thời gian. Ý tưởng của EDGE là sử dụng một phương pháp điều chế mới được gọi là 8PSK. EDGE là một phương thức nâng cấp hấp dẫn đối với các mạng GSM vì nó chỉ yêu cầu một phần mềm nâng cấp trạm gốc. Nó không thay thế hay nói đúng hơn cùng tồn tại với phương pháp điều chế khóa dịch tối thiểu Gaussian (GMSK), được sử dụng trong GSM, nên các thuê bao có thể tiếp tục sử dụng máy di động cũ của mình nếu không cần được cung cấp chất lượng dịch vụ tốt hơn. Xét trên khía cạnh kỹ thuật, cũng cần giữ lại GMSK cũ vì 8PSK chỉ có hiệu quả ở vùng hẹp, với vùng rộng vẫn cần GMSK. Nếu EDGE được sử dụng cùng với GPRS thì sự kết hợp này được gọi là GPRS nâng cấp (EGPRS), còn sự kết hợp của EDGE và HSCSD được gọi là ECSD.

WCDMA thực sự là một dịch vụ vô tuyến băng thông rộng sử dụng băng tần 5MHz để đạt được tốc độ dữ liệu lên tới 2Mbit/s. Hiện tại cả châu Âu và

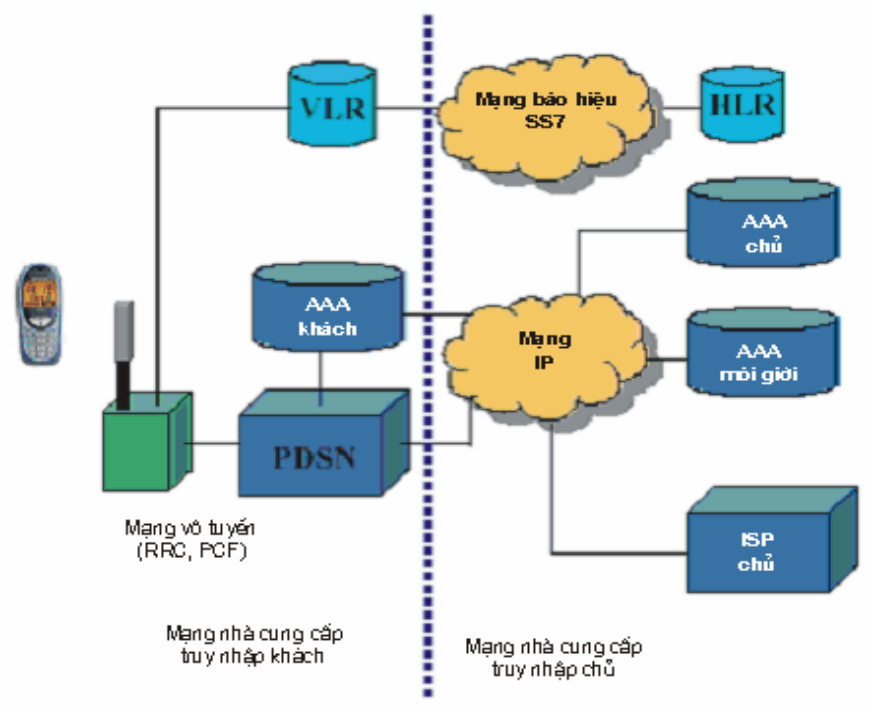
Nhật Bản đều đang thử nghiệm/triển khai WCDMA và công nghệ này đang tiến triển nhanh trên con đường thương mại hoá.




Hình 1.4. Cấu trúc hệ thống UMTS

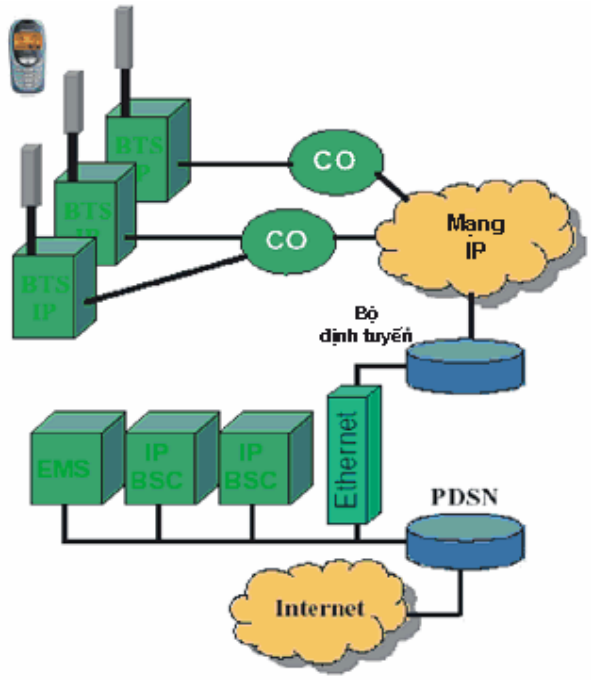
CDMA không chuyển ngay sang 3G do thiếu phổ tần trên thị trường Hoa Kỳ. Thị trường Hàn Quốc đã thử nghiệm cdma2000 trên phổ tần 3G của mình. Cũng như đối với GSM, Hoa Kỳ và phần còn lại của thế giới có những con đường rất khác nhau để đi đến 3G.Cdma2000 được cấu trúc theo cách để cho phép nhiều mức dịch vụ 3G trên kênh IS-95 1,25MHz truyền thống. Các dịch vụ này là cdma2000 1xRTT (một thời được gọi là công nghệ truyền dẫn vô tuyến kích thước kênh IS-95). Với công suất 3G tối đa, cdma2000 sử dụng một kênh 3,75 MHz, lớn gấp 3 lần kênh truyền thống, gọi là 3xRTT.

Hệ thống 1xRTT sử dụng một sơ đồ điều chế hiệu quả hơn để tăng gấp đôi số lượng thuê bao thoại và tạo ra các kênh dữ liệu lên tới 144kbit/s. Tốc độ này đã cho phép một số nhà cung cấp dịch vụ cho rằng mình đang thực hiện 3G. Trong thực tế, tốc độ người dùng sẽ ở trong khoảng 50-60kbit/s. Dữ liệu theo sơ đồ 1xRTT sẽ được chuyển mạch gói để đảm bảo sử dụng kênh hiệu quả.

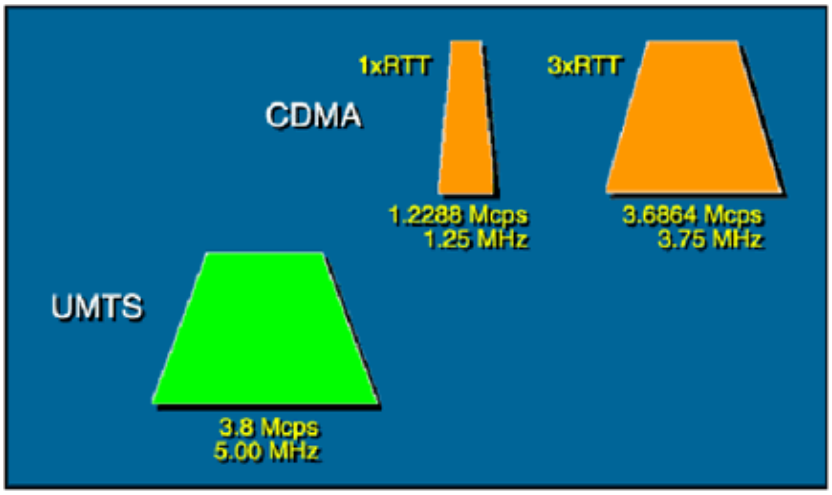



Hình 1.5. Cấu trúc hệ thống cdma 2000 1X

Tốc độ lên tới 2,4Mbit/s có thể đạt được bằng cách triển khai 1xEV-DO tức là dịch vụ chỉ có dữ liệu - không có thoại trên kênh này. Khi 1xEV-DV được triển khai thì ta sẽ có kênh đa phương tiện thực sự.




Hình 1.6. Cấu trúc hệ thống cdma 2000 1x EV DO




Hình 1.7. Băng thông và tốc độ chip của UMTS và cdma 1x, 3xRTT

Xa hơn 1xEV-DV, 3xRTT là một kênh 3,75MHz trên phổ 5MHz - 1,25 MHz còn lại được dùng cho dải tần bảo vệ trên và dưới. Có một số kịch bản hoạt động cho phổ 10MHz, 15MHz, và 20 MHz. CDMA2000 3xRTT còn có tên là `3x,` `MC-3x,` và `IMT-CDMA MultiCarrier 3x`. Hình 1.7 so sánh kích thước kênh và tốc độ chip của UMTS và CDMA 1x và 3x..

Như vậy  là sẽ có không chỉ một con được đi tới các hệ thống vô tuyến di động 3G. Và cũng rõ ràng là IMT-2000 đã được đông đảo chấp nhận. Tuy nhiên, tính không tương thích của các công nghệ 3G, việc thiếu phổ tần, thiếu các ứng dụng và thiết bị 3G đặt ra một số vấn đề cần giải quyết. Từ quan điểm công nghệ, cả WCDMA và cdma2000 đều sử dụng các kỹ thuật trải phổ rộng. Tuy nhiên, chúng có cấu trúc kênh, mã chip, tốc độ chip và thủ tục đồng bộ hoá khác nhau. Cần có thời gian để hài hoà các trở ngại công nghệ này. Để giải quyết được vấn đề phổ trên toàn cầu sẽ tốn kém và mất nhiều thời gian. Cuối cùng, cần có nhiều dịch vụ hơn nữa để thu hút khách hàng. Chúng ta đã thấy sự phổ biến của email và tin nhắn đối với PDA và

điện thoại di động. Giờ đây chúng ta cần một loạt các ứng dụng đa phương tiện đòi hỏi phải có tốc độ dữ liệu của 3G

## 1.2. Các nhà cung cấp dịch vụ 3G trên thế giới.

Bốn nhà cung cấp dịch vụ lớn dưới đây đang cho triển khai các dịch vụ khả dụng trên mạng 3G, tuy nhiên kế hoạch và thời điểm triển khai có khác nhau đôi chút. Bốn nhà cung cấp dịch vụ 3G bao gồm: Cingular/AT&T Wireless (Cingular sát nhập với AT&T Wireless), T-Mobile, Verzon và Sprint Nextel.

### 1.2.1. Cingular/AT&T Wireless

Mạng hiện tại: GSM/GPRS/EDGE

Mạng 3G dự kiến: UMTS/HSPDA

Kế hoạch 3G: Cingular/AT&T WirelessThe đã ký kết hợp tác với Ericsson và Lucent Technologies để triển khai dịch vụ UMTS/HSDPA, dự kiến sẽ bắt đầu vào nửa đầu năm nay (2005).

Các thiết bị di động hỗ trợ: Nokia 6651, Motorola A845

### 1.2.2. Sprint/Nextel

Mạng hiện tại: CDMA/1xRTT

Mạng 3G dự kiến: 1xEV-DO, tương lai sẽ nâng cấp lên 1xEV-DV

Kế hoạch 3G: Sprint vừa ký kết một hợp đồng trị giá 3 tỷ USD với Lucent, Motorola, và Nortel để nghiên cứu và thực hiện chiến lược 3G.

### 1.2.3. T-Mobile

Mạng hiện tại: GSM/GPRS

Mạng 3G dự kiến: UMTS/HSPDA

Kế hoạch 3G: T-Mobile đang đối mặt với nhiều thách thức và cạnh tranh khi triển khai mạng 3G. Theo đại diện của hãng này, dải tần cho mạng di động

3G của T-Mobile hiện không còn đủ, và chỉ có thể khắc phục được vào năm 2007.

### 1.2.4. Verizon

Mạng hiện tại: CDMA/1xRTT

Mạng 3G dự kiến: 1xEV-DO

Kế hoạch 3G: Verizon đã cho triển khai mạng 3G từ khá sớm với dịch vụ 1xEV-DO tại San Diego và Washington D.C. từ tháng 10/2003.

Các thiết bị di động hỗ trợ: LG VX8000, Samsung SCH-A890, UTStarcom CDM-8940

## 1.3. Tổng quan về mạng NGN.

NGN là mạng hội tụ cả thoại, video và dữ liệu trên cùng một cơ sở hạ tầng dựa trên nền tảng IP, làm việc trên cả hai phương tiện truyền thông vô tuyến và hữu tuyến. NGN là sự tích hợp cấu trúc mạng hiện tại với cấu trúc mạng đa dịch vụ dựa trên cơ sở hạ tầng có sẵn, với sự hợp nhất các hệ thống quản lý và điều khiển. Các ứng dụng cơ bản bao gồm thoại, hội nghị truyền hình và nhắn tin hợp nhất (unified messaging) như voice mail, email và fax mail, cùng nhiều dịch vụ tiềm năng khác.

### 1.3.1. Các đặc điểm của NGN:

- Sử dụng công nghệ chuyển mạch mềm (SW-SoftSwitch) thay thế các thiết bị tổng đài chuyển mạch phần cứng (hardware) cồng kềnh. Các mạng của từng dịch vụ riêng rẽ được kết nối với nhau thông qua sự điều khiển của một thiết bị tổng đài duy nhất, thiết bị tổng đài này dựa trên công nghệ SW được ví như là 'trái tim' của NGN.
- Mạng hội tụ thoại và dữ liệu, cố định và di động. Các loại tín hiệu được truyền tải theo kỹ thuật chuyển mạch gói, xu hướng sắp tới đang tiến dần lên sử dụng mạng IP với kỹ thuật QoS như MPLS.

- Mạng băng thông rộng cung cấp đa dịch vụ: Mạng truyền dẫn quang với công nghệ WDM (Wavelength Division Multiplexing) hay DWDM (dense WDM).

### 1.3.2. Cấu trúc mạng NGN.

Cấu trúc mạng NGN bao gồm 5 lớp chức năng: lớp truy nhập dịch vụ (service access layer), lớp chuyển tải dịch vụ (service transport/core layer), lớp điều khiển (control layer), lớp ứng dụng/dịch vụ (application/service layer) và lớp quản lý (management layer). Hình 1 thể hiện cấu trúc của NGN.

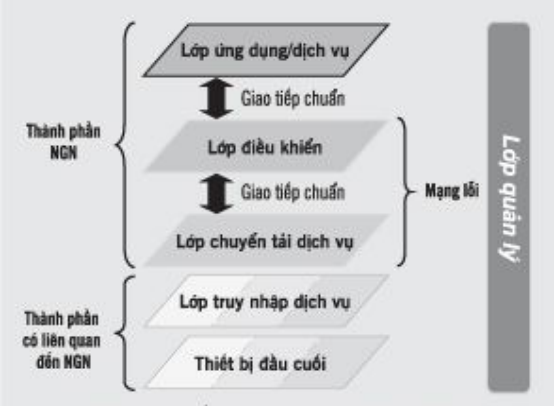
#### *1.3.2.1. Lớp ứng dụng/dịch vụ*

Lớp ứng dụng và dịch vụ cung cấp các ứng dụng và dịch vụ như dịch vụ mạng thông minh IN (Intelligent network), trả tiền trước, dịch vụ giá trị gia tăng Internet cho khách hàng thông qua lớp điều khiển... Hệ thống ứng dụng và dịch vụ mạng này liên kết với lớp điều khiển thông qua các giao diện mở API. Nhờ giao diện mở này mà nhà cung cấp dịch vụ có thể phát triển các ứng dụng và triển khai nhanh chóng các dịch vụ trên mạng. Trong môi trường phát triển cạnh tranh sẽ có rất nhiều thành phần tham gia kinh doanh trong lớp này.

#### *1.3.2.2. Lớp điều khiển.*

Lớp điều khiển bao gồm các hệ thống điều khiển kết nối cuộc gọi giữa các thuê bao thông qua việc điều khiển các thiết bị chuyển mạch (ATM+IP) của lớp chuyển tải và các thiết bị truy nhập của lớp truy nhập. Lớp điều khiển có chức năng kết nối cuộc gọi thuê bao với lớp ứng

dụng/dịch vụ. Các chức năng như quản lý, chăm sóc khách hàng, tính cước cũng được tích hợp trong lớp điều khiển.




Hình 1.8 Cấu trúc mạng NGN

***1.3.2.3. Lớp chuyển tải dịch vụ***

Bao gồm các nút chuyển mạch (ATM+IP) và các hệ thống truyền dẫn (SDH, WDM), thực hiện chức năng chuyển mạch, định tuyến các cuộc gọi giữa các thuê bao của lớp truy nhập dưới sự điều khiển của thiết bị điều khiển cuộc gọi thuộc lớp điều khiển. Hiện nay đang còn nhiều tranh cãi khi sử dụng ATM hay MPLS cho lớp chuyển tải này.

***1.3.2.4. Lớp truy nhập dịch vụ***

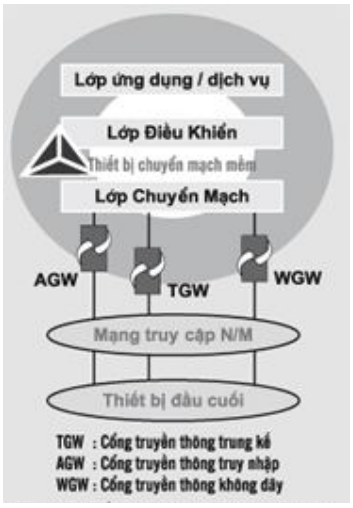
Bao gồm các thiết bị truy nhập cung cấp các cổng kết nối với thiết bị đầu cuối thuê bao qua hệ thống mạng ngoại vi cáp đồng, hoặc cáp quang, hoặc thông qua môi trường vô tuyến (thông tin di động, vệ tinh, truy nhập vô tuyến cố định...)

***1.3.2.5. Lớp quản lý***

Đây là lớp đặc biệt xuyên suốt các lớp trên. Các chức năng quản lý được chú trọng là: quản lý mạng, quản lý dịch vụ, quản lý kinh doanh.

**1.3.3. Các thành phần của mạng NGN.**

Mối tương quan giữa cấu trúc phân lớp chức năng và các thành phần chính của mạng NGN được mô tả trong hình 1.9.



Hình 1.9 Cấu trúc lớp và các thành phần chính trong mạng NGN

Theo hình 2 ta nhận thấy, các loại thiết bị đầu cuối kết nối đến mạng truy nhập (Access Network), sau đó kết nối đến các cổng truyền thông (Media Gateway) nằm ở biên của mạng trục. Thiết bị quan trọng nhất của NGN là SW nằm ở tâm của mạng trục (còn hay gọi là mạng lõi). SW điều khiển các chức năng chuyển mạch và định tuyến qua các giao thức. Các giao thức n phần sau. Hình 3 liệt kê chi tiết các thành phần trong mạng NGN cùng với các đặc điểm kết nối của nó đến các mạng công cộng (PSTN).

### *1.3.3.1. Thiết bị SW*

Thiết bị SW là thiết bị đầu não trong mạng NGN. Nó làm nhiệm vụ điều khiển cuộc gọi, báo hiệu và các tính năng để tạo một cuộc gọi trong mạng NGN hoặc xuyên qua nhiều mạng khác (ví dụ PSTN, ISDN). SW còn được gọi là Call Agent (vì chức năng điều khiển cuộc gọi của nó) hoặc Media Gateway Controller - MGC (vì chức năng điều khiển cổng truyền thông - Media Gateway).

Thiết bị SW có khả năng tương tác với mạng PSTN thông qua các cổng báo hiệu (Signalling Gateway) và cổng truyền thông (Media Gateway). SW điều khiển cuộc gọi thông qua các báo hiệu, có hai loại chính:

- Ngang hàng (peer-to-peer): giao tiếp giữa SW và SW, giao thức sử dụng là BICC hay SIP.

- Điều khiển truyền thông: giao tiếp giữa SW và Gateway, giao thức sử dụng là MGCP hay Megaco/H.248.

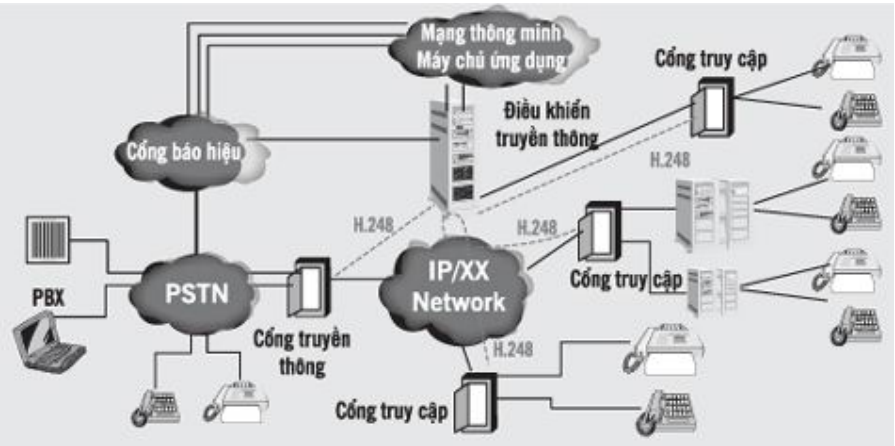
#### *1.3.3.2. Cổng truyền thông*

Nhiệm vụ chủ yếu của cổng truyền thông (MG - Media Gateway) là chuyển đổi việc truyền thông từ một định dạng truyền dẫn này sang một định dạng khác, thông thường là từ dạng mạch (circuit) sang dạng gói (packet), hoặc từ dạng mạch analog/ISDN sang dạng gói. Việc chuyển đổi này được điều khiển bằng SW. MG thực hiện việc mã hóa, giải mã và nén dữ liệu thoại.

Ngoài ra, MG còn hỗ trợ các giao tiếp với mạng điện thoại truyền thống (PSTN) và các giao thức khác như CAS (Channel Associated Signalling) và ISDN. Tóm lại, MG cung cấp một phương tiện truyền thông để truyền tải thoại, dữ liệu, fax và hình ảnh giữa mạng truyền thống PSTN và mạng gói IP.

#### *1.3.3.3. Cổng truy nhập*

Cổng truy nhập (AG - Access Gateway) là một dạng của MG. Nó có khả năng giao tiếp với máy PC, thuê bao của mạng PSTN, xDSL và giao tiếp với mạng gói IP qua giao tiếp STM. Ở mạng hiện nay, lưu lượng thoại từ thuê bao được kết nối đến tổng đài chuyển mạch PSTN khác bằng giao tiếp V5.2 thông qua cổng truy nhập. Tuy nhiên, trong mạng NGN, cổng truy nhập được điều khiển từ SW qua giao thức MGCP hay Megaco/H.248. Lúc này, lưu lượng thoại từ các thuê bao sẽ được đóng gói và kết nối vào mạng trục IP.




Hình 1.10: Các thành phần chính trong NGN

### *1.3.3.4. Cổng báo hiệu*

Cổng báo hiệu (SG - Signalling Gateway) đóng vai trò như một cổng giao tiếp giữa mạng báo hiệu số 7 (SS7 - Signalling System 7, giao thức được dùng trong PSTN) và các điểm được quản lý bởi thiết bị SW trong mạng IP. Cổng SG đòi hỏi một đường kết nối vật lý đến mạng SS7 và phải sử dụng các giao thức phù hợp. SG tạo ra một cầu nối giữa mạng SS7 và mạng IP, dưới sự điều khiển của SW. SG làm cho SW giống như một điểm nút bình thường trong mạng SS7. Lưu ý rằng SG chỉ điều khiển SS7; còn MG điều khiển các mạch thoại thiết lập bởi cơ chế SS7.

### *1.3.3.5. Mạng trục IPv6*

Mạng trục được thể hiện là mạng IP kết hợp công nghệ ATM hoặc MPLS. Vấn đề sử dụng ATM hay MPLS còn đang tách thành 2 xu hướng. Các dịch vụ và ứng dụng trên mạng NGN được quản lý và cung cấp bởi các máy chủ dịch vụ (server). Các máy chủ này hoạt động trên mạng thông minh (IN - Intelligent Network) và giao tiếp với mạng PSTN thông qua SS7.

# CHƯƠNG 2. MOBILE IP

## 2.1. Giao thức Mobile IP .

IP di động do tổ công tác IETF (Internet Engineering Task Force) đề xuất. Đó là một bộ khuyến nghị và cơ chế của IP, giải quyết tính di động của điểm nút Internet, dựa vào các giao thức theo lớp OSI. IP di động tạo cho các đầu cuối có khả năng di động tại các vị trí, đảm bảo cho đầu cuối tiến hành thông tin không phải khởi động lại hoặc sắp đặt lại các tham số IP.

Mạng triển khai IP đã được thành lập trên 20 năm. Phương pháp đánh số mạng ban đầu dựa theo IPv4 (giao thức Internet phiên bản 4). Mạng IP hiện nay triển khai một phần nào áp dụng IPv4, IETF đã đưa ra giao thức IPv6 có nhiều đặc điểm ưu việt hơn IPv4.

Giao thức Mobile IP được nghiên cứu dựa trên nền tảng của giao thức TCP/ IP kế thừa các ưu điểm và khắc phục các nhược điểm cho phù hợp với tình hình phát triển hiện tại là giao thức cho phép các đầu cuối (Node) di chuyển trên mạng mà không phải thay đổi địa chỉ IP của Node. Nói cách khác là các Node này có khả năng kết nối vào Internet tại bất cứ địa điểm nào trên thế giới.

Nhưng cả IPv4 và IPv6 vẫn nhận định địa chỉ IP của Node xác định điểm kết nối vật lý duy nhất của Node với Internet. Do vậy khi các máy tính chuyển vùng làm việc như từ Việt Nam sang Châu Âu thì bắt buộc những máy tính đó phải mang một địa chỉ IP mới và toàn bộ các liên hệ về dữ liệu hiện có sẽ bị hủy bỏ. Do vậy một yêu cầu vô cùng cần thiết được đặt ra là phải nghiên cứu khả năng sao cho các máy tính phải có thể di chuyển, làm việc từ xa mà toàn bộ các mối liên hệ hiện có vẫn tồn tại hay là IP có khả năng di động, đó chính là nguyên nhân ra đời của giao thức Mobile IP (hay là IP có khả năng di động).

Một trạm làm việc hoặc bộ định tuyến có khả năng thay đổi điểm liên kết từ một Net hoặc Subnet với Net hoặc Subnet khác, có thể thay đổi vị trí của nó mà không thay đổi địa chỉ IP, nó có thể tiếp tục giao tiếp với các Node Internet khác ở bất cứ điểm này với địa chỉ IP (bất biến) của nó được gọi là Mobile Node. Một Mobile Node phải có khả năng giao tiếp với các Node khác. Khi nó ở mạng gốc thì những Node này hoạt động không cần đến các chức năng di động. Khi Node làm việc ngoài mạng gốc thì các Node cần phải được cung cấp các chức năng di động.

## 2.2. Truyền số liệu trong mạng Mobile IP.

### 2.2.1. Kiến trúc mạng Mobile IP.

Hình 2.1 mô tả kiến trúc mạng Mobile IP đơn giản, trong đó:

- Nút di động (Mobile Node - MN): Là đầu cuối di động IP, có thể thay đổi vị trí truy nhập mạng, nó duy trì liên tục địa chỉ IP và kết nối trên Internet.

- Nút tương ứng (Correspondant Node - CN): Có thể là đầu cuối di động hoặc cố định sẽ kết nối với MN.

- Mạng gốc (Home network - HN): Là mạng quản lý trực tiếp địa chỉ IP của MN, tính di động của MN không có ý nghĩa trong mạng này.

- Mạng ngoài (Foreign Network - FN): Là mạng MN di chuyển tới và không quản lý trực tiếp MN.

- Địa chỉ quản lý (Care-Of-Address - CoA): Là một địa chỉ IP của FA, nó định nghĩa vị trí hiện tại của MN. Các gói IP không được chuyển trực tiếp tới địa chỉ IP của MN mà phải chuyển tiếp qua FA .

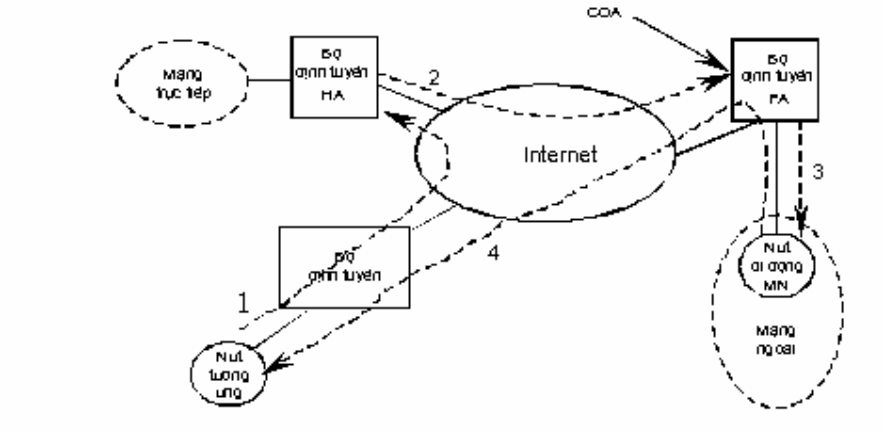
- Trạm ngoài (Foreign Agent - FA): Thuộc mạng FN, cung cấp các dịch vụ cho MN khi nó chuyển vùng tới. FA có thể là bộ định tuyến cho MN và có CoA nên nó hoạt động như là điểm cuối và chuyển tiếp các gói số liệu tới MN.

- Trạm gốc (Home Agent - HA): Thuộc mạng HN có thể được tích hợp vào Router, là hệ thống để MN đăng ký sử dụng dịch vụ. Tất cả các gói số liệu truyền tới MN đều xuất phát từ đây. HA biết vị trí hiện tại của MN thông qua CoA, nó duy trì số liệu đăng ký chuyển vùng cho các MN.

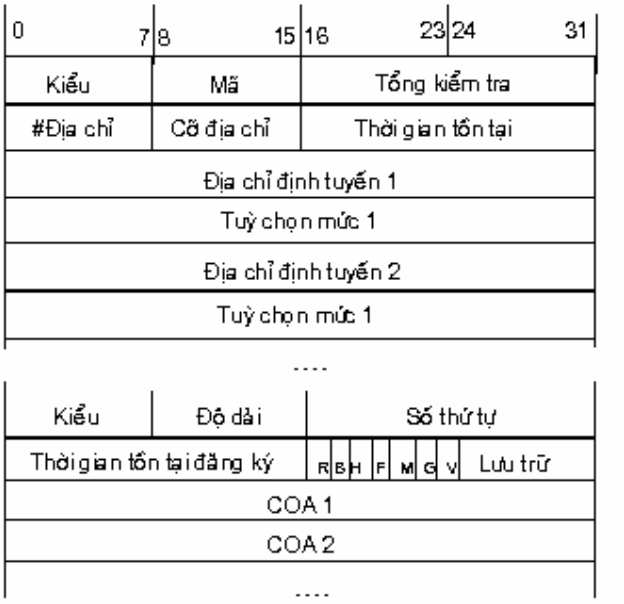
Theo hình 2.1 MN đang ở mạng FN và trao đổi số liệu IP với Node CN. Do yêu cầu che dấu tính di động của đầu cuối ở Mobile IP, nên CN không cần biết vị trí hiện tại của MN mà chỉ việc gửi số liệu tới địa chỉ IP của nó (1).

Vì không biết MN đang ở đâu, nên Internet định tuyến gói số liệu tới Router tương ứng ở mạng gốc (HN) của MN.

Vì biết MN không ở HN (MN thông báo vị trí của mình cho HA), nên HA chặn gói số liệu CN gửi tới lại, vì thế số liệu không được chuyển vào mạng như thường lệ mà được mã hoá lại (thêm tiêu đề IP mới với CoA là địa chỉ đích và HA là nguồn) lên trước tiêu đề cũ rồi chuyển tới CoA (2). Khi nhận được gói số liệu FA sẽ sửa lại bằng cách loại bỏ phần tiêu đề do HA thêm vào và chuyển tới MN (3). Việc gửi số liệu từ MN tới CN đơn giản hơn, bình thu N giống như đối




Hình 2.1. Kiến trúc mạng Mobile IPv6.




Hình 2.2. Minh họa cấu trúc bản tin thông báo.

Vấn đề nẩy sinh khi MN di chuyển khỏi mạng HN là làm thế nào để xác định được trạm FA mà MN chuyển tới và cách thức MN lấy thông tin sau khi nó chuyển vùng. Để giải quyết vấn đề này các trạm điều khiển (FA, Router và HA) phải đều đặn quảng bá lên mạng các thông tin về sự hiện diện của mình thông qua các bản tin thông báo đặc biệt (theo giao thức ICMP). Hình 2.2 minh họa cấu trúc bản tin thông báo. Phần trên là mô tả bản tin ICMP còn phần mở rộng bên dưới mô tả các thông tin về tính di động, ở đây không mô tả chi tiết các trường.

MN có thể nhận được các bản tin thông báo từ FA hoặc HA, nhờ đó mà nó xác định được vị trí hiện tại của mình. Nếu không nhận được bản tin thông báo của các trạm điều khiển trên mạng, thì MN phải gửi yêu cầu cho HA đề nghị cung cấp thông tin trạm điều khiển trên mạng. Về nguyên tắc MN có thể liên tục gửi các bản tin yêu cầu để tìm trạm điều khiển, nên phải đề phòng việc có quá nhiều bản tin như thế phát ra gây nên tình trạng nghẽn mạng. Ngoài ra, MN có thể tìm kiếm trạm điều khiển mới vào mọi thời điểm, kể cả khi đang bận, nghĩa là nó vẫn có thể vừa tìm kiếm kết nối mới tốt hơn mà vẫn

trao đổi thông tin trên kết nối hiện tại. Trường hợp này xảy ra khi MN đang di chuyển qua nhiều cell của các mạng di động khác nhau. Sau khi các trạm điều khiển thông báo lên mạng thông tin của chúng và MN thu nhận được các thông tin này, thì nó có thể xác định được vị trí của mình (đang ở HN hoặc FN) và năng lực của trạm điều khiển. Nếu lúc này MN đang ở FN thì nó phải đăng ký với HA như trình bày ở dưới đây.

Một vấn đề cần quan tâm là việc sử dụng tiêu chuẩn như RFC 1256 cho mục đích khác với ban đầu (thông báo trạm điều khiển) là nguyên nhân làm nẩy sinh một số vấn đề. Cụ thể, khoảng thời gian bé nhất 3s giữa hai thông báo chỉ có thể phù hợp đối với mạng cố định vì sự biến động mạng không cao, còn ở mạng không dây có các MN đang di chuyển và đặc biệt là các ứng dụng yêu cầu dòng số liệu liên tục, thì khoảng thời gian 3s này là quá dài. MN phải đợi ít nhất 3s để thông báo tình trạng không thể tìm được trạm điều khiển.

### 2.2.3. Đăng ký

Sau khi nhận được CoA, MN phải đăng ký với và thông báo cho HA biết vị trí hiện tại của mình để HA chuyển tiếp số liệu. Việc đăng ký có thể được thực hiện theo hai cách, tuỳ thuộc vào vị trí hiện tại của CoA, đó là:

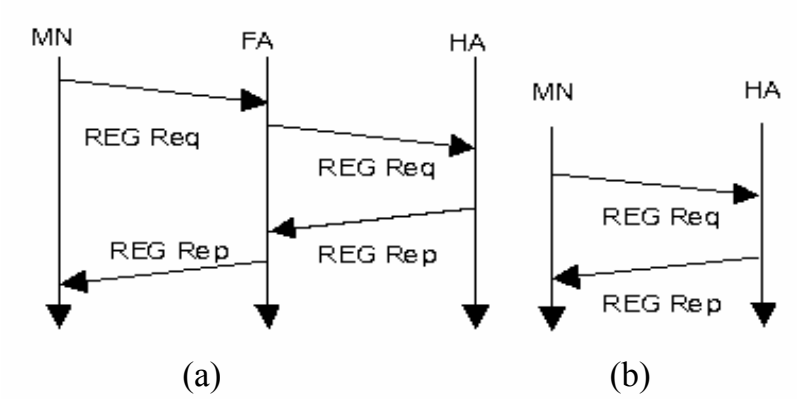
- CoA thuộc FA: thủ tục đăng ký được minh hoạ như hình 2.3a. MN gửi yêu cầu đăng ký của nó tới FA để chuyển tiếp cho HA. Lúc này HA thiết lập mối liên kết di động gồm địa chỉ IP gốc của MN và CoA hiện tại. Ngoài ra mối liên kết di động chứa cả khoảng thời gian đăng ký đã thoả thuận. Việc đăng ký sẽ tự động hết hiệu lực và bị huỷ bỏ sau khoảng thời gian cho phép này, vì vậy MN cần đăng ký trước khi hết thời gian cho phép. Cơ chế này cần

thiết để tránh mối liên kết di động không sử dụng nữa. Sau khi thiết lập mối liên kết di động, HA gửi bản tin trả lời tới FA đã yêu cầu.

- CoA đồng vị trí (CoA co-located): Việc đăng ký đơn giản hơn như hình 2.3b. MN gửi yêu cầu đăng ký trực tiếp tới HA và HA sẽ gửi lại bản tin trả lời.

Khi sử dụng giao thức UDP để đăng ký, thì địa chỉ nguồn IP gói số liệu được đặt tới địa chỉ giao tiếp của MN, địa chỉ đích IP đặt tới địa chỉ giao tiếp của FA hoặc HA (tuỳ thuộc vào vị trí của CoA). Cổng UDP đích là 434.

Trong môi trường di động, hiệu suất mạng khi sử dụng UDP cao hơn so với TCP, nên UDP thường được sử dụng.




Hình 2.3. Minh hoạ thủ tục đăng ký

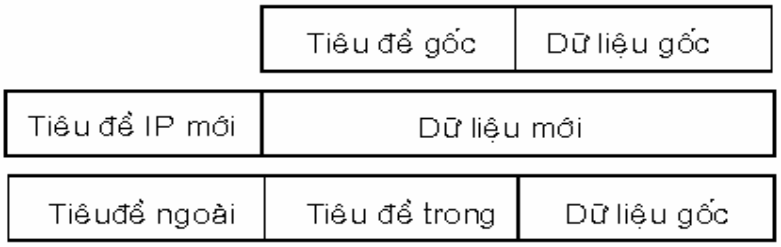
### 2.2.4. Kênh số liệu và mã hoá

Khi sử dụng kênh số liệu để truyền tin, các gói số liệu sẽ được mã hoá ở đầu vào và giải mã ở đầu ra, nội dung gói số liệu không bị thay đổi khi đi qua kênh số liệu này.

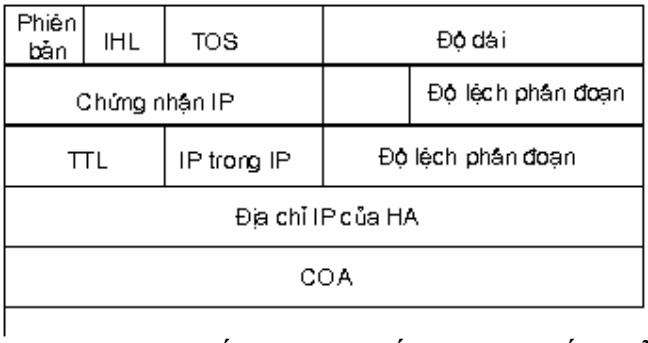
Mã hoá là việc lấy phần tiêu đề và nội dung của gói số liệu đặt vào phần số liệu của gói mới. Ngược với mã hoá, quá trình giải mã sẽ tách phần tiêu đề và nội dung đã ghép vào ra. Mã hoá và giải mã thường được sử dụng khi trao đổi

số liệu giữa các lớp với nhau, tuy nhiên ở Mobile IP, các quá trình này lại được thực hiện trong việc vận chuyển số liệu trên cùng một lớp.

Hình 2.4 minh họa các xử lý của HA tại đầu vào kênh số liệu. HA lấy gói số liệu gốc với MN là đích nhận, chèn vào phần dữ liệu của gói mới và đặt tiêu đề IP mới. Bằng cách này gói số liệu sẽ được định tuyến tới CoA. Tiêu đề mới gọi là tiêu đề Ngoài. Ngoài ra còn có tiêu đề trong để nhận dạng tiêu đề gốc. Có một số cách mã hoá cần cho việc vận chuyển số liệu trong kênh số liệu giữa HA và CoA là IP-in-IP, cực tiểu, định tuyến chung,...




Hình 2.4. Các xử lý của HA tại đầu vào kênh số liệu




Hình 2.5. Minh hoạ cấu trúc gói số liệu trong ống dẫn

- Mã hoá IP-in-IP : ở giao thức Mobile IP áp dụng phương thức mã hoá IP-in-IP. Hình 2.5 minh hoạ cấu trúc gói số liệu trong ống dẫn (đã mã hoá). Nói chung các trường đều tuân theo tiêu chuẩn giao thức IP định nghĩa ở RFC 791, chỉ có các trường sau có ý nghĩa đặc biệt cho Mobile IP, đó là trường

Ver - Version của giao thức, IHL biểu thị tiêu đề Ngoài, TOS là copy của tiêu đề Trong, IP-in-IP kiểu của giao thức, các trường khác chứa địa chỉ IP của HA và CoA. Nếu không có các lựa chọn tiếp theo tiêu đề Ngoài, thì tiêu đề Trong bắt đầu với các trường giống như mô tả ở trên. Các phần còn lại của tiêu đề này đều không thay đổi trong suốt quá trình mã hoá.

- Mã hoá định tuyến chung (GRE): Trong khi mã hoá IP-in-IP và cực tiểu chỉ áp dụng cho Mobile IP thì mã hoá chung có thể áp dụng cho cả các giao thức lớp mạng khác. GRE cho phép mã hoá gói số liệu của một giao thức thành gói số liệu của giao thức khác.

Hình 2.6 mô tả quá trình mã hoá định tuyến chung. Phần tiêu đề và dữ liệu gói số liệu của một giao thức được lấy ra và đặt vào phần dữ liệu gói mới của giao thức khác, phần tiêu đề của gói mới cấu tạo bởi tiêu đề ngoài và GRE.


Hình 2.6. Mô tả quá trình mã hoá định tuyến

### 2.2.5. Tối ưu

Như trình bày ở trên, việc trao đổi số liệu giữa hai Node di động đăng ký ở các vùng khác nhau phải đi qua HA và CoA tương ứng. Trường hợp hai Node này di chuyển đến cùng một vùng và liên lạc với nhau thì với các thủ tục trao đổi số liệu như trên là không hiệu quả, chưa tối ưu (Hai Node gần nhau nhưng số liệu vẫn phải chuyển đi từ vùng này sang vùng kia). Theo nguyên tắc của giao thức Mobile IP, tất cả các gói số liệu chuyển tới MN đều phải chuyển

tiếp qua HA, đây là một trong những nguyên nhân làm tăng lưu lượng mạng giữa CN, HA và CoA.

Phương pháp tối ưu việc định tuyến là HA thông báo cho CN biết vùng hiện tại của MN, qua đó CN lưu vùng này vào bảng định tuyến nội bộ của mình. Để thực hiện được điều này, phải bổ xung cho giao thức Mobile IP các bản tin như sau:

- Yêu cầu liên kết (Binding request) - Khi một Node nào đó muốn biết vị trí hiện tại của MN, nó chỉ việc gửi yêu cầu liên kết tới HA. HA kiểm tra xem MN có cho phép thông báo vị trí của nó hay không, nếu được phép HA sẽ gửi bản tin cập nhật liên kết cho Node yêu cầu.

- Cập nhật liên kết (Binding update) - Bản tin này thông báo vị trí hiện tại của MN, bao gồm địa chỉ IP cố định của MN và CoA, và có thể cả yêu cầu xác nhận.

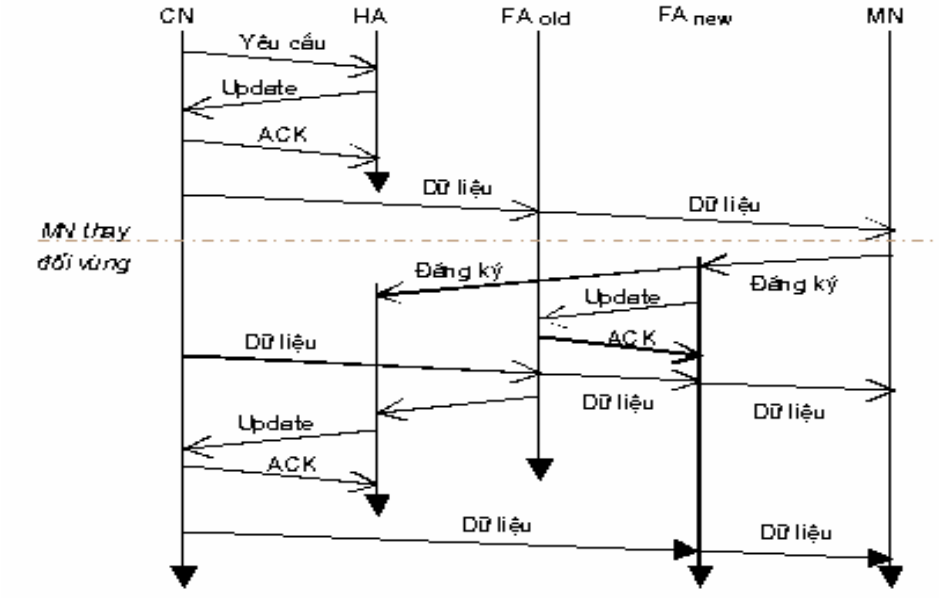
- Xác nhận liên kết (Binding acknowledgement) - Nếu có yêu cầu, Node yêu cầu liên kết phải gửi bản tin xác nhận này cho HA sau khi nhận được bản tin cập nhật liên kết.

- Cảnh báo liên kết (Binding warning) - Trong khi giải mã gói số liệu đối với MN mà Node yêu cầu không biết FA hiện tại của MN, thì nó gửi bản tin cảnh báo này tới HA của MN. Bản tin này gồm có địa chỉ IP của MN và địa chỉ IP của Node đang gửi số liệu tới MN. Lúc này HA cần gửi bản tin cập nhật liên kết tới Node này.

Hình 2.7 minh họa 4 bản tin này cùng với trường hợp MN thay đổi FA. Đầu tiên CN yêu cầu HA thông báo vị trí hiện tại của MN, nếu được phép HA sẽ thông báo địa chỉ IP cố định của MN và CoA thông qua bản tin cập nhật. CN xác nhận cập nhật liên kết và lưu các thông tin nhận được vào bảng định tuyến của nó. Bây giờ CN có thể mã hoá dữ liệu và truyền trực tiếp tới FA

hiện tại của MN để nó chuyển tiếp cho MN. Lúc này nếu MN di chuyển sang vùng khác thì nó phải cập nhật lại FA mới bằng bản tin đăng ký FA (bao gồm cả địa chỉ FA cũ) đồng thời thông báo để HA cập nhật lại cơ sở dữ liệu. Ngoài ra FA mới thông báo cho FA cũ về việc MN đăng ký lại FA. Ngoài thông tin này ra FA cũ không biết vùng mới của MN và vì vậy CN sẽ chuyển số liệu cho MN thông qua FA cũ để nó chuyển tiếp cho FA mới. Quá trình chuyển tiếp số liệu này là hình thức tối ưu hoá khác của Mobile IP nhằm cung cấp tính năng chuyển vùng mềm (smooth handovers). Nếu không có tính năng này thì số liệu có thể bị mất khi MN chuyển vùng. Cuối cùng, FA cũ gửi bản tin cảnh báo tới HA yêu cầu thông báo cho CN về vùng mới của nó. Sau khi gửi bản tin xác nhận CN có thể gửi số liệu trực tiếp tới FA mới.

Thoáng nhìn chiều truyền số liệu từ MN tới CN ở hình 2.1 có vẻ đơn giản, MN có thể gửi số liệu trực tiếp tới CN bình thường như quy định trong giao thức IP tiêu chuẩn. Tuy nhiên thực tế có một số vấn đề liên quan như sau:




Hình 2.7. Minh họa 4 bản tin: Yêu cầu, cập nhật , xác nhận , cảnh báo liên

- Tường lửa (Firewalls) - Hầu hết các công ty, tổ chức bảo vệ mạng nội bộ của mình từ Internet nhờ hệ thống Firewall. Nhờ có Firewall, Quản trị mạng có thể thiết lập loại bỏ sự truy nhập từ một số địa chỉ nào đó, nghĩa là Firewall chỉ cho phép số liệu từ các địa chỉ hợp lệ đi qua. Tuy nhiên MN vẫn gửi số liệu với địa chỉ IP cố định mà mạng FN không quản lý. Hơn nữa Firewall đôi khi phải loại bỏ số liệu có chứa địa chỉ nguồn của các máy tính trên Internet nhằm ngăn ngừa khả năng chúng có thể sử dụng địa chỉ nội bộ để trở thành thành viên trong mạng. Điều này dẫn đến MN không thể gửi số liệu tới máy tính trong cùng mạng HN của nó.

- Truyền số liệu tới nhóm xác định (Multicast) - kênh số liệu (tunnel) theo chiều ngược lại từ MN tới CN cần thiết để MN tham gia vào nhóm Multicast. Trong khi các Node trong mạng HN có thể tham gia nhóm Multicast, nhưng các node MN ở mạng FN không thể truyền số liệu Multicast giống như chúng phát ra từ mạng HN.

- TTL (Time To Live) - MN gửi số liệu với TTL nào đó trong khi vẫn ở mạng HN. TTL có thể đủ thấp để không gói số liệu nào có thể truyền được ra ngoài vùng nào đó. Nếu lúc này MN di chuyển sang mạng FN thì TTL này có thể cũng thấp để các gói số liệu không truyền được ra ngoài mạng FN.

RFC 2344 định nghĩa kênh số liệu ngược là phần mở rộng của giao thức Mobile IP để khắc phục những vấn đề nêu trên. Kênh số liệu ngược tạo ra định tuyến nhập nhằng ở hướng ngược lại. RFC 2344 chưa đưa ra được giải pháp để khắc phục vấn đề định tuyến nhập nhằng này, bởi vì nó không biết liệu CN có thể giải mã được các gói số liệu hay không. Hơn nữa Mobile IP không hoạt động cùng với các Node có giao thức khác.

Kênh số liệu ngược làm nẩy sinh một số vấn đề an toàn mà cho đến nay chưa có giải pháp xử lý. Ví dụ, các kênh số liệu bắt đầu từ mạng của một công ty ra Internet có thể bị Hacker chặn lại và lợi dụng để gửi số liệu qua

Firewall. Như vậy liệu các công ty có cho phép thiết lập kênh số liệu mà không có sự kiểm soát của Firewall hay không? Nếu cho phép thì các công ty này vô hình dung đã thiết lập mạng riêng đặc biệt cho phép các thuê bao di động xâm nhập mạng của mình mà không có sự kiểm soát của Firewall.

Tóm lại, Mobile IP là giao thức hỗ trợ tính di động trong mạng IP, nó định nghĩa thêm hai phần tử mạng là HA và FA. HA quản lý các địa chỉ IP cố định của các MN còn FA liên kết tới địa chỉ IP gọi là CoA. Các gói số liệu được HA chặn lại, mã hoá và gửi tới FA thông qua địa chỉ CoA. FA giải mã số liệu rồi chuyển tiếp cho MN. Như vậy FA là thực thể IP có liên quan chặt chẽ với MN nhất. ở mạng di động đó là các trạm gốc BSC hoặc các router tích hợp trong BSC như IWF ở mạng CDMA. Khi di chuyển giữa các mạng, MN phải đăng ký với HA và FA của nó để các thiết bị này có thể xác định được địa chỉ IP mới của MN. Mỗi MN sẽ có hai địa chỉ IP, một để định vị và một để nhận dạng.

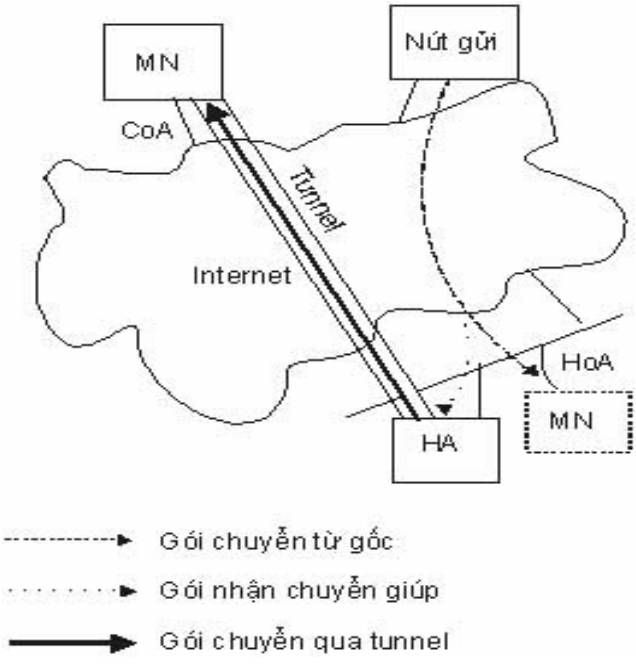
Ngày nay tất cả các đầu cuối dựa trên các công nghệ có dây và không dây đều có thể liên lạc được với nhau, đó là nhờ có giao thức Mobile IP. Nó cung cấp khả năng di động trên mạng Internet mà không phải thay đổi các hệ thống cố định hiện tại. Tuy nhiên giao thức này vẫn để lại một số vấn đề chưa giải quyết được, đó là vấn đề an toàn, hiệu suất mạng, chất lượng dịch vụ,...

## 2.3. Mobile IPv6 (MIPv6)

MIPv6 là một phiên bản nâng cấp và hoàn thiện so với MIPv4. Muốn hiểu được đặc điểm của MIPv6 (IP di động phiên bản 6) ta cần biết mục đích thiết kế của MIPv6 hướng tới đó là thông báo kịp thời những sự khác biệt giữa các nút một cách chân thực và không làm giảm sút sự an toàn. Trong Mobile IPv6, không còn khái niệm FA. MN luôn được gán địa chỉ CoA duy nhất trên mạng khách (đúng hơn là duy nhất trên mạng Internet toàn cầu). MN sử dụng

địa chỉ CoA làm địa chỉ nguồn trong phần tiêu đề của gói tin gửi đi. Các gói tin gửi đến MN bằng cách sử dụng tiêu đề định tuyến, trong gói tin IPv6, thay vì sử dụng cách đóng gói vào một gói tin IP khác như trước đây.

MIPv6 nhằm giải quyết đồng thời hai vấn đề. Thứ nhất, nó cho phép chuyển giao liên tục mặc dù MN chuyển động và thay đổi địa chỉ IP. Thứ hai, nó cho phép gói tin tìm đến một nút thông qua địa chỉ IP tĩnh tại, địa chỉ trạm gốc (HA). Nói một cách khác, MIPv6 chú trọng tới bản chất nhận dạng của các địa chỉ IP. Ta có thể nhắc lại ý tưởng của MIP (cả MIPv4 và MIPv6) là cho phép HA làm việc với nút di động MN tực như đang tĩnh tại. Bất cứ lúc nào MN đi khỏi mạng gốc thì HA nhận gói tin gửi đến nút này và chuyển tiếp gói này tới địa chỉ quản lý CoA. Lớp vận chuyển sử dụng địa chỉ trạm gốc HA như nhận dạng "tĩnh" của nút di động MN. Hình 2.8 phác họa cơ chế hoạt động của ý tưởng cơ bản này.

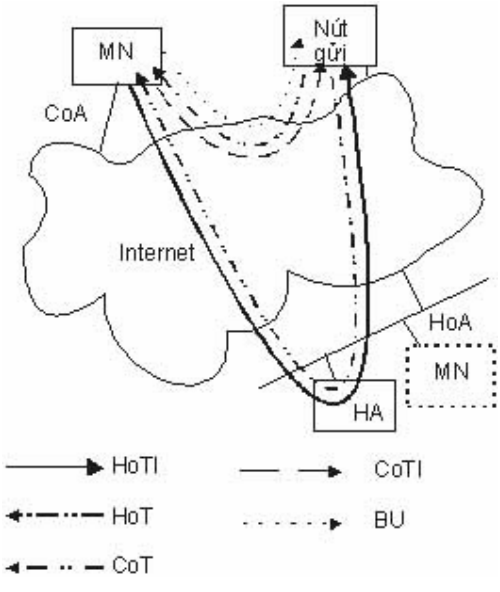



Hình 2.8. Phác họa cơ chế hoạt động của MIPv6.

Theo sơ đồ này thì gói tin chuyển theo đường tunnel thông qua HA, nên đường truyền dài hơn và dẫn tới chất lượng giảm. Để khắc phục nhược điểm này MIPv6 đưa ra việc tối ưu hoá định tuyến RO (Route Optimization) khi dùng đường truyền tối ưu, nút di động gửi các địa chỉ quản lý CoA của nó (đang ở) đến nút gửi bằng các tin báo cập nhật liên quan tới việc định tuyến BU (Binding Update).

Khi MIPv6 dùng tối ưu hoá định tuyến RO, nút gửi thực hiện hai nhiệm vụ: thứ nhất nó là nguồn của gói tin gửi; thứ hai, nó hoạt động như bộ router đầu tiên cho các gói thông báo định tuyến. Các gói này rời khỏi nút gửi là nguồn được định tuyến đến các địa chỉ quản lý CoA. Mỗi gói bao gồm một mào đầu định tuyến (routing header), chứa địa chỉ gốc HoA của các nút di động . Theo lý thuyết, gói tin được định tuyến đến CoA và tiếp theo qua kênh ảo, gói tin được chuyển từ CoA đến HoA. Mối nguy hiểm nhất trong MIPv6 là địa chỉ bị "mất cắp", nghĩa là hacker dóng giả là một nút nào đó tại một địa chỉ đã cho rồi "lấy cắp" các lưượng tin gửi đến địa chỉ đó.

MIPv6 thực hiện bảo mật và tối ưu hoá định tuyến để ngăn ngừa hoặc giảm nhẹ số vụ mất cắp. Độ an toàn của MIPv6 không chỉ dựa vào giao thức mật mà truyền thông mà còn dựa vào hạ tầng cấu trúc định tuyến để MN được tiếp cận thông qua địa chỉ trạm gốc HoA và cả địa chỉ quản lý CoA. Độ đảm bảo an toàn và tối ưu hoá định tuyến, cơ chế hoạt động của MIPv6 dựa theo cách định tuyến có phản hồi RR (Return




Hình 2.9. Luồng vận chuyển của gói tin.

Routability). Luồng vận chuyển của gói tin như trên hình 2.9. Nó gồm có hai lựa chọn: lựa chọn địa chỉ trạm gốc HoA và lựa chọn địa chỉ quản lý CoA.

Việc lựa chọn định tuyến RR thực hiện bằng hai cặp tin báo (thử địa chỉ, cập nhật tin địa chỉ ) và (thử địa chỉ quản lý, cập nhật tin địa chỉ). Các gói thử khởi tạo địa chỉ gốc HoT và thử khởi tạo địa chỉ quản lý CoT chỉ cần dùng để kích thích các gói thử. Gói cập nhật địa chỉ BU trả lời cho cả hai phép thử. Quá trình thử địa chỉ HoA như sau:

Việc lựa chọn địa chỉ gồm có thử địa chỉ gốc HoT và cập nhật BU. HoT được chuyển qua tunnel từ trạm gốc HA đến nút di động MN. Nội dung của HoT là một hàm số gồm địa chỉ gốc của HoT có kèm theo khoá bảo mật Kcn (chỉ có nút gửi biết mật khoá Kcn). Gói HoT được gửi theo hai đường của Internet. Đường thứ nhất, từ điểm gửi đến trạm gốc HA, trên đường này, gói không được bảo vệ, bất kỳ hacker nào cũng biết nội dung. Tiếp theo HA gửi tiếp gói đến MN, trên đường gói được truyền trong tunnel có bảo vệ để không ai biết được nội dung gói.

Quá trình thử địa chỉ quản lý CoA cũng tương tự. Chỉ khác là gói được gửi trực tiếp từ địa chỉ CoA của nút di động MN. Nội dung của CoT là một hàm số có kèm theo hệ số bảo mật Kcn. Gói CoT chuyển trực tiếp từ nút gửi đến nút di động MN. Trên đường gói không được bảo vệ dễ bị các hacker ở gần điểm gửi, trên đường truyền hoặcc gần điểm MN tấn công.

Khi Mn nhận được cả hai tin HoT và CoT, nó tạo r4a khoá ràng buộc Kbm. Khoá Kbm được dùng để bảo vệ tin cập nhật BU, cho đến khi Mn di động và cần có một CoA mới. Khi nhận được tin BU đầu tiên, nút gửi đi qua một quá trình phức tạp. Đó là đảm bảo cho MN đã vừa nhận được HoT và CoT đó là do HoA và CoA yêu cầu

Giả thiết có một hacker có thể ăn cắp tin HoT tại thời điểm nào đó và tiếp theo. Nếu HoT kéo dài mãi thì hacker có thể tiếp tục lấy cắp. Để hạn chế nguy cơ này ta truyền HoT trong thời gian ngắn. Sau chu kỳ vài phút, cặp tin báo HoT lại thay đổi.

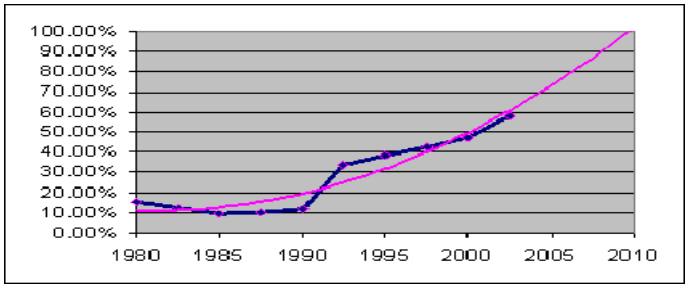
Tóm lại, ta thấy MIPv6 đã có nhiều đặc điểm cải tiến so với MIPv4 về cấu hình, độ an toàn quản lý và tính di động. MIPv6 được coi là một chiến lược dài hạn cho các nhà quản lý mạng và các nhà cung cấp dịch vụ di động.

# CHƯƠNG 3. IPv6

## 3.1. Giới thiệu về cấu trúc của IPv6

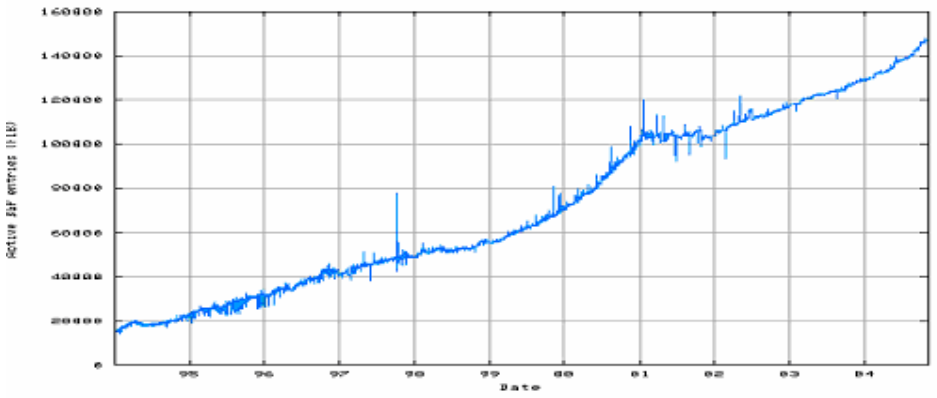
### 3.1.1.Lợi ích của IPv6.

Một trong những lý do chính để phát triển một phiên bản mới của IP đó là việc địa chỉ IPv4 lớp B đang hết dần. Hình 3.1 mô tả tình hình hiện nay của IPv4, và tầm địa chỉ hiện có của IPv4, qua đó ta thấy dự đoán có thể hết địa chỉ vào khoảng năm 2010 hay sớm hơn.




Hình 3.1: Tầm địa chỉ IPv4

Bên cạnh đó, do sự phát triển ngày một lớn của bảng định tuyến ở backbone. Hình 3.2 mô tả kích thước của bảng định tuyến được tăng dần ra



Hình 3.2. Kích thước bảng định tuyến.

theo các năm.

Các ích lợi của IPv6 gồm: Tăng kích thước của tầm địa chỉ IP; tăng sự phân cấp địa chỉ; đơn giản hoá địa chỉ host (địa chỉ được thống nhất là: toàn cục, site và cục bộ) ; đơn giản hoá việc tự cấu hình địa chỉ (gồm DHCPv6 và neighboor discovery thay cho ARP broadcast); tăng độ linh hoạt cho định tuyến multicast; có thêm địa chỉ anycast; header được sắp xếp hợp lý; tăng độ bảo mật (vì có thêm các header mở rộng về bảo mật giúp bảo đảm sự toàn vẹn dữ liệu); có tính di động tốt hơn (home agent; care-of-address; và header định tuyến mở rộng); hiệu suất tốt hơn (việc tóm tắt địa chỉ; giảm ARP broadcast; giảm sự phân mảnh gói tin; không có header checksum; QoS được tích hợp sẵn...).

#### *3.1.1.1. Tăng kích thước của tầm địa chỉ.*

IPv6 sử dụng 128 bit địa chỉ trong khi IPv4 chỉ sử dụng 32 bit; nghĩa là IPv6 có tới 2128 địa chỉ khác nhau; 3 bit đầu luôn là 001 được giành cho các địa chỉ khả định tuyến toàn cầu (Globally Routable Unicast –GRU). Nghĩa là còn lại 2125 địa chỉ, nghĩa là có khoảng 4,25.1037 địa chỉ, trong khi IPv4 chỉ có tối đa 3,7.109 địa chỉ, nghĩa là IPv6 sẽ chứa 1028 tầm địa chỉ IPv4.

#### *3.1.1.2.Tăng sự phân cấp địa chỉ.*

IPv6 chia địa chỉ thành một tập hợp các tầm xác định hay boundary: Ba bit đầu cho phép biết được địa chỉ có thuộc địa chỉ khả định tuyến toàn cầu (GRU) hay không, giúp các thiết bị định tuyến có thể xử lý nhanh hơn. Top level ggregation (TLA) ID được sử dụng vì 2 mục đích:

- Thứ nhất, nó được sử dụng để chỉ định một khối địa chỉ lớn mà từ đó các khối địa chỉ nhỏ hơn được tạo ra để cung cấp sự kết nối cho những địa chỉ nào muốn truy cập vào Internet.

- Thứ hai, nó được sử dụng để phân biệt một đường (route) đến từ đâu. Nếu các khối địa chỉ lớn được cấp phát cho các nhà cung cấp dịch vụ và sau đó được cấp phát cho khách hàng thì sẽ dễ dàng nhận ra các mạng chuyển tiếp mà đường đó đã đi qua cũng như mạng mà từ đó route xuất phát.

Với IPv6, việc tìm ra nguồn của một router sẽ rất dễ dàng Next level gregator (NLA) là một khối địa chỉ được gán bên cạnh khối TLA, những địa chỉ này được tóm tắt lại thành những khối TLA lớn hơn. Khi chúng được trao đổi giữa các nhà cung cấp dịch vụ trong lõi internet, ích lợi của loại cấu trúc địa chỉ này là: sự ổn định về định tuyến, nếu chúng ta có 1 NLA và muốn cung cấp dịch vụ cho các khách hàng, ta sẽ cố cung cấp dịch vụ đầy đủ nhất, tốt nhất và cho phép các khách hàng nhận được đầy đủ bảng định tuyến nếu họ muốn để tạo việc định tuyến theo chính sách; cân bằng tải... để thực hiện việc này chúng ta phải mang tất cả các đường trong backbone để có thể chuyển cho họ.

#### *3.1.1.3.Đơn giản hoá việc đặt địa chỉ host:*

IPv6 sử dụng 64 bit sau cho địa chỉ host,và trong 64 bit đó thì có cả 48 bit là địa chỉ MAC của máy, do đó phải đệm vào đó một số bit đã được định nghĩa trước mà các thiết bị định tuyến sẽ biết được những bit này trên subnet, ngày nay, ta sử dụng chuỗi 0xFF và 0xFE (:FF:FE: trong IPv6) để đệm vào địa chỉ MAC. Bằng cách này, mọi host sẽ có một host ID duy nhất trong mạng. Sau này nếu đã sử dụng hết 48 bit MAC thì có thể sẽ sử dụng luôn 64 bit mà không cần đệm.

#### *3.1.1.4.Việc tự cấu hình địa chỉ đơn giản hơn.*

Một địa chỉ multicast có thể được gán cho nhiều máy, địa chỉ anycast là các gói anycast sẽ gửi cho đích gần nhất (một trong những máy có cùng địa chỉ) trong khi multicast packet được gửi cho tất cả máy có chung địa chỉ (trong một nhóm multicast).

Kết hợp host ID với multicast ta có thể sử dụng việc tự cấu hình như sau: khi một máy được bật lên, nó sẽ thấy rằng nó đang được kết nối và nó sẽ gửi một gói multicast vào LAN, gói tin này sẽ có địa chỉ là một địa chỉ multicast có tầm cục bộ (Solicited Node Multicast address). Khi một router thấy gói tin này, nó sẽ trả lời một địa chỉ mạng mà máy nguồn có thể tự đặt địa chỉ, khi máy nguồn nhận được gói tin trả lời này, nó sẽ đọc địa chỉ mạng mà router gửi. Sau đó, nó sẽ tự gán cho nó một địa chỉ IPv6 bằng cách thêm host ID (được lấy từ địa chỉ MAC của interface kết nối với subnet đó) với địa chỉ mạng. Do đó, tiết kiệm được công sức gán địa chỉ IP.

***3.1.1.5.Tăng độ linh hoạt cho định tuyến multicast.***

Đặt trường hợp: giám đốc muốn gửi một hội nghị truyền hình đến các nhân viên trong công ty mà không muốn gửi tất cả mọi người trong internet (chỉ gửi những người cần xem). Khi đó, IPv6 có một khái niệm về tầm vực multicast. Với IPv6, có thể thiết kế một luồng multicast xác định chỉ được gửi trong một khu vực nhất định và không bao giờ cho phép các packet ra khỏi


Hình 3.3. Cấu trúc của gói tin multicast.

khu vực đó. 8 bit đầu luôn được thiết lập là 1 giúp các thiết bị định tuyến biết được gói tin này là một gói tin multicast. 4 bit sau là flag (hiện tại, 3 bit đầu không được định nghĩa và luôn là 0, bit thứ tư là T bit được sử dụng để quyết

định xem địa chỉ multicast này là địa chỉ được gán lâu dài (được gọi là well-known) hay tạm thời (transient). 4 bit tiếp theo là scope, xác định gói tin multicast có thể đi bao xa, trong khu vực nào thì gói tin được định tuyến; scope có thể có các giá trị sau: 1(có tầm trong nội bộ node); 2 (có tầm trong nội bộ liên kết); 5 (có tầm trong nội bộ site); 8 (có tầm trong nội bộ tổ chức); E (có tầm toàn cục).

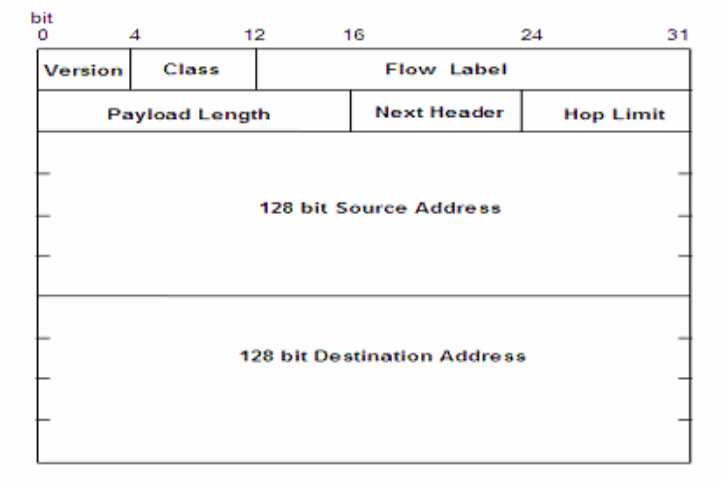
Tuỳ vào cách gán địa chỉ multicast, chúng ta có thể kiểm soát các gói tin multicast được đi bao xa, và các thông tin định tuyến kết hợp với các nhóm multicast được quảng bá bao xa. Ví dụ: nếu chúng ta muốn quảng bá một multicast trong văn phòng của ta, và muốn toàn thế giới thấy nó, ta sẽ gán tầm cho nó là E (110), tuy nhiên, nếu bạn muốn tạo một nhóm multicast cho một hội nghị truyền hình bạn có thể gán tầm là 5 hay 2.

#### *3.1.1.6. Địa chỉ Anycast.*

IPv6 định nghĩa một loại địa chỉ mới: anycast. Một địa chỉ anycast là một địa chỉ IPv6 được gán cho một nhóm các máy có chung chức năng, mục đích. Khi packet được gửi cho một địa chỉ anycast, việc định tuyến sẽ xác định thành viên nào của nhóm sẽ nhận được packet qua việc xác định máy gần nguồn nhất. Việc sử dụng anycast có hai lợi ích: một là, nếu bạn đang đến một máy gần nhất trong một nhóm, bạn sẽ tiết kiệm được thời gian bằng cách giao tiếp với máy gần nhất; thứ hai là việc giao tiếp với máy gần nhất giúp tiết kiệm được băng thông. Địa chỉ anycast không có các tầm địa chỉ được định nghĩa riêng như multicast, mà nó giống như một địa chỉ unicast, chỉ có khác là có thể có nhiều máy khác cũng được đánh số với cùng scope trong cùng một khu vực xác định. Anycast được sử dụng trong các ứng dụng như DNS...

#### *3.1.1.7.Header hợp lý.*

Header của IPv6 đơn giản và hợp lý hơn IPv4. IPv6 chỉ có 6 trường và 2 địa chỉ, trong khi IPv4 chứa 10 trường và 2 địa chỉ. IPv6 header có dạng như hình 3.4.




Hình 3.4. IPv6 header.

IPv6 cung cấp các đơn giản hoá sau:

· Định dạng được đơn giản hoá: IPv6 header có kích thước cố định 40 octet với ít trường hơn IPv4, nên giảm được overhead, tăng độ linh hoạt.

· Không có header checksum: trường checksum của IPv4 được bỏ đi vì các liên kết ngày nay nhanh hơn và có độ tin cậy cao hơn vì vậy chỉ cần các host tính checksum còn router thì khỏi cần.

· Không có sự phân mảnh theo từng hop: trong IPv4, khi các packet quá lớn thì router có thể phân mảnh nó, tuy nhiên việc này sẽ làm tăng thêm overhead cho packet. Trong IPv6 thì chỉ có host nguồn mới có thể phân mảnh một packet theo các giá trị thích hợp dựa vào một MTU path mà nó tìm được, do đó, để hỗ trợ host thì IPv6 chứa một hàm giúp tìm ra MTU từ nguồn đến đích.

***3.1.1.8.Bảo mật:***

IPv6 tích hợp tính bảo mật vào trong kiến trúc của mình bằng cách giới thiệu 2 header mở rộng tùy chọn: Authentication header(AH) và Encrypted Security Payload (ESP) header. Hai header này có thể được sử dụng chung hay riêng để hỗ trợ nhiều chức năng bảo mật.

·AH: quan trọng nhất trong header này là trường Integriry Check Value (ICU). ICU được tính bởi nguồn và được tính lại bởi đích để xác minh.

Quá trình này cung cấp việc xác minh tín toàn vẹn và xác minh nguồn gốc của dữ liệu. AH cũng chứa cả một số thứ tự để nhận ra một tấn công bằng các packet replay giúp ngăn các gói tin được nhân bản.

· ESP header: ESP header chứa một trường : security parameter index (SPI) giúp đích của gói tin biết payload được mã hoá như thế nào. ESP header có thể được sử dụng khi tunneling, khi tunnelling thì cả header và payload gốc sẽ được mã hoá và bỏ vào một ESP header bọc ngoài, khi đến gần đích thì các gateway bảo mật sẽ bỏ header bọc ngoài ra và giải mã để tìm ra header và payload gốc.

***3.1.1.9.Tính di động:***

IPv6 hỗ trợ tốt các MNnhư laptop. IPv6 giới thiệu 4 khái niệm giúp hỗ trợ tính toán di động gồm: Home address; care-of address; binding; home agent.

Trong IPv6 thì các MNđược xác định bởi một địa chỉ home address mà không cần biết hiện tại nó được gắn vào đâu. Khi một MNthay đổi từ 1 subnet này sang subnet khác; nó phải có một CoAqua một quá trình tự cấu hình. Sự kết hợp giữa home address và CoAđược gọi là một binding. Khi một MNnhận được 1 care-of address, nó sẽ báo ho HAcủa nó bằng gói tin được gọi là binding update để HAcó thể cập nhật lại binding cache của HAvề CoAcủa MNvừa gửi. HA sẽ duy trì một ánh xạ giữa các home address và care-address

và bỏ nó vào binding cache. Một MNcó thể được truy cập bằng cách gửi một packet đến các home address của nó.

Nếu MNkhông được kết nối trên subnet của HA thì HA sẽ gửi packet đó cho MN qua CoA của máy đó trong binding cache của HA (Lúc này, HA được xem như máy trung gian để máy nguồn có thể đến được máy di động). MN sau đó sẽ gửi một gói tin binding update cho máy nguồn của gói tin. Máy nguồn sau đó sẽ cập nhật binding cache của nó, thì sau này máy nguồn muốn gửi đến máy di động, chỉ cần gửi trực tiếp đến cho MNqua CoA chứa trong binding cache của nó mà không cần phải gửi qua home address. Do đó chỉ có gói tin đầu tiên là qua HA.

#### *3.1.1.10. Hiệu suất:*

IPv6 cung cấp các lợi ích sau:

· Giảm được overhead vì chuyện dịch địa chỉ: vì trong IPv4 có sử dụng private address để tránh hết địa chỉ, do đó xuất hiện kỹ thuật NAT để dịch địa chỉ, nên tăng overhead cho gói tin. Trong IPv6 do không thiếu địa chỉ nên không cần private address, nên không cần dịch địa chỉ.

· Giảm được overhead do định tuyến: nhiều khối địa chỉ IPv4 được phân phát cho các user nhưng lại không tóm tắt được, nên phải cần các entry trong bảng định tuyến làm tăng kích thước của bảng định tuyến và thêm overhead cho quá trình định tuyến, ngược lại, các địa chỉ IPv6 được phân phát qua các ISP theo một kiểu phân cấp địa chỉ giúp giảm được overhead.

· Tăng độ ổn định cho các đường: trong IPv4, hiện tượng route flapping thường xảy ra, trong IPv6, một ISP có thể tóm tắt các router của nhiều mạng thành một mạng đơn và chỉ quản lý mạng đơn đó và cho phép hiện tượng flapping chỉ ảnh hưởng đến nội bộ của mạng bị flapping.

· Giảm broadcast: trong IPv4 sử dụng nhiều broadcast như ARP, trong khi IPv6 sử dụng neighbor discovery để thực hiện chức năng tương tự trong quá trình tự cấu hình mà không cần sử dụng broadcast.

· Multicast có giới hạn: trong IPv6, một địa chỉ multicast có chứa một trường scope có thể hạn chế các gói tin multicast trong các node, trong các link, hay trong một tổ chức.

· Không có checksum.

### 3.1.2. Cấu trúc của địa chỉ.

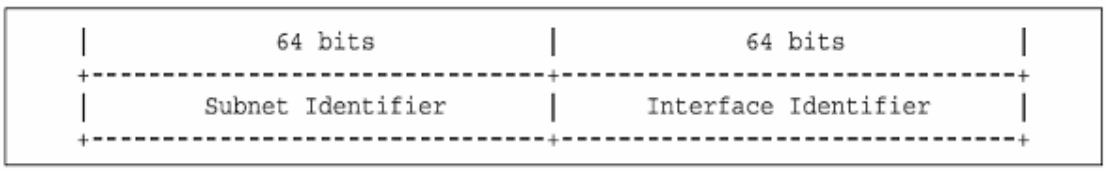
IPV4 định nghĩa ba dạng địa chỉ: unicast, broadcast, và multicast. Thế hệ địa chỉ IPV6 có các dạng địa chỉ như sau: unicast, multicast và anycast.

Khái niệm địa chỉ broadcast không tồn tại nữa. Chức năng broadcast được đảm nhiệm bởi địa chỉ multicast trong IPV6.

Địa chỉ unicast được cấu hình cho mỗi giao diện mạng của một node. Địa chỉ multicast, mặt khác, được phân bổ cho một nhóm các node. Một địa chỉ anycast được gắn cho mỗi chức năng nhất định, và địa chỉ anycast được sử dụng để thực hiện một chức năng nhất định.

Địa chỉ unicast IPv6 có chiều dài 128 bit và được chia làm 2 phần: một subnet prefix và interface ID. Với các địa chỉ khả định tuyến toàn cục AGU, thì cả prefix và interface ID đều có chiều dài là 64 bit. Subnet prefix là địa chỉ mạng được gán cho liên kết. Trong khi interface ID là địa chỉ MAC của node.

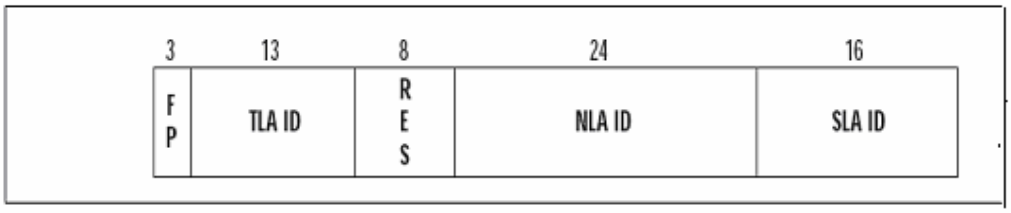
Trong quá trình tự cấu hình của IPv6, host sẽ cung cấp interface ID của nó từ ROM và yêu cầu router cục bộ hay sử dụng DHCPv6 server để xác định subnet prefix.




Hình 3.5. Định dạng địa chỉ IPv6.

· Do địa chỉ MAC chỉ có 48 bit nên 16 bit trong interface ID sẽ được để giành. IEEE có yêu cầu một địa chỉ MAC dài 64 bit được gọi là EUI-64.

· Quản lý địa chỉ: một địa chỉ khả định tuyến toàn cục sẽ có subnet prefix là 64 bit và subnet prefix này sẽ được chia nhỏ thành 5 trường:




Hình 3.6. Các trường của subnet prefic.

Trường đầu tiên là trường format prefix(FP), giúp xác định một địa chỉ khả định tuyến toàn cục (AGU) với giá trị nhị phân là 001. Trường thứ 3 chưa được dùng đến và được để giành cho tương lai. Hai trường: TLA ID và NLA ID là quan trọng nhất. TLA ID là top level aggregation identifier. Các địa chỉ toàn cục IPv6 sẽ được gán cho các ISP hay các tổ chức dạng TLA. Các tổ chức TLA sẽ tiếp tục phân phát các tầm địa chỉ này cho các tổ chức Next level aggregation (NLA). Phương pháp phân phối địa chỉ theo thứ bậc này cho phép việc tóm tắt địa chỉ để giảm kích thước của bảng định tuyến ở core. Còn với các nhà quản trị mạng thì trường quan trọng nhất là site-level aggregation (SLA) ID. Không giống với 2 trường kia, SLA ID thường sẽ không được gán sẵn giá trị khi cung cấp cho các tổ chức. SLA ID cho phép 1 tổ chức định nghĩa các phân cấp địa chỉ trong cơ quan của họ. 16 bit SLA ID có thể hỗ trợ lên đến 65535 subnet.

### 3.1.3. Khảo sát cấu trúc mạng của IPv6

Sau đây sẽ khảo sát cách các thiết bị giao tiếp với nhau trong một mạng và cách IPv6 tham gia vào đó cũng như khảo sát việc giao tiếp giữa 2 host/subnet, host với router...

### *3.1.3.1. Các giao tiếp trong một subnet:*

IPv6 được thiết kế theo kiểu "plug and play".

Có hỗ trợ việc tự cấu hình. Để hiểu các giao tiếp trong một subnet, ta có các khái niệm sau: tự cấu hình phi trạng thái (stateless); địa chỉ liên kết cục bộ (link-local); link-local prefix; Interface ID; Neighbor solicitation message; neighbor advertisement message; neighbor cache.

· Nếu một mạng không có router, không có kết nối với internet, và không có cả các server để hỗ trợ cho quá trình tự cấu hình thì các host trong mạng đó phải cấu hình địa chỉ IPv6 của nó bằng một quá trình gọi là stateless autoconfiguration.

· Khi một máy kết nối với 1 port trên 1 subnet, máy sẽ tự cấu hình một địa chỉ thử (tentative address) được gọi là địa chỉ liên kết cục bộ (link-local address). Địa chỉ này có kích thước 128 bit gồm 1 prefix liên kết cục bộ và địa chỉ MAC của máy; prefix liên kết cục bộ là một định danh toàn số 0 và theo dạng hex là FE8. Một địa chỉ liên kết cục bộ có dạng sau: FE80:0:0:0:xxxx:xxxx:xxxx:xxxx Để đảm bảo địa chỉ đó là duy nhất thì máy sẽ gửi một gói tin đặc biệt là: neighbor solicitation đến địa chỉ vừa cấu hình và đợi reply trong một giây. Nếu không thấy thì máy sẽ xem địa chỉ đó là duy nhất trong mạng, nếu có một gói tin neighbor advertisement message thì địa chỉ đó không duy nhất. Sau khi xác định địa chỉ liên kết cục bộ là duy nhất, quá trình tiếp theo là query các router lân cận trong mạng.

· Để giao tiếp với host đích trên mạng, máy phải tìm ra interface ID của máy đích. Do đó, máy sẽ sử dụng chức năng được gọi là IPv6 Neighbor Discovery protocol. Máy sẽ gửi một gói tin neighbor solicitation cho đích và interface ID sẽ được gửi trả lại trong gói tin Neighbor advertisement. Interface ID sẽ được bỏ vào header của IPv6 và truyền trên mạng. Máy sau đó

sẽ thêm một entry vào neighbor cache của nó. Entry đó sẽ chứa địa chỉ IPv6 của đích, interface ID của nó , một con trỏ vào packet sắp truyền, và một flag để xác định đích có phải là một router hay không. Cache này sẽ được sử dụng cho những lần gửi sau mà không cần gửi lại gói tin solicitation.

· Địa chỉ liên kết cục bộ không thể được sử dụng để giao tiếp ra khỏi một subnet. Với những giao tiếp liên subnet thì cần các địa chỉ site-local và global address để nối các router.

### *3.1.3.2. Các giao tiếp liên subnet.*

Khi một máy phát hiện thấy có một router tồn tại trên subnet, thì quá trình tự cấu hình có sự khác biệt và có các khái niệm sau: site-local address; subnet ID; router solicitation message; router advertisement message; default router list cache; destination cache; prefix list cache; redirect message; path MTU discovery.

· Trong và sau quá trình tự cấu hình thì PC đều phụ thuộc rất nhiều vào quá trình IPv6 neighbor discovery protocol, để tìm các node trong cùng subnet và tìm các router cho các đích đến các subnet khác.

· Trong quá trình tự cấu hình, sau khi P4C sinh ra một địa chỉ liên kết cục bộ duy nhất thì nó sẽ query một router. PC sẽ gửi một gói tin được gọi là router solicitation và một router sẽ phản hồi lại với một gói itn gọi là router advertisement.

Việc hiện diện của router nghĩa là có thể có các subnet khác kết nối với router. Mỗi subnet phải có một subnet ID của nó vì việc định tuyến là dựa trên subnet ID. Địa chỉ của PC bây giờ phải có một subnet ID duy nhất vì địa chỉ liên kết cục bộ không còn đủ để sử dụng nữa. Để hỗ trợ quá trình stateless autoconfig thì router advertisement sẽ chứa một subnet ID. Router advertisement của mỗi interface sẽ chứa một subnet ID khác nhau. ID này sẽ

được kết hợp với interface ID để tạo địa chỉ IPv6. PC sẽ bỏ địa chỉ liên kết cục bộ của nó và cấu hình một địa chỉ mới được gọi là site-local address, gồm 16 bit subnet ID có dạng: FEC0:0:0:<subnet ID>:xxxx:xxxx:xxxx:xxxx

· PC sẽ sử dụng thông tin từ router advertisement để cập nhật các cache của nó. Subnet ID sẽ được thêm vào prefix list cache của PC. Cache này được sử dụng để xem một địa chỉ có cùng subnet hay không với PC. Thông tin của router sẽ được thêm vào neighbor cache và destination cache. Nếu router có thể được sử dụng là một router mặc định thì một entry sẽ được thêm vào default router list cache.

· Khi PC đã sẵn sàng gửi packet cho đích, nó sẽ query prefix list để xem địa chỉ đích có chung subnet với nó hay không. Nếu không thì packet sẽ được gửi cho router trong default router list. PC sau đó sẽ cập nhật destination cache của nó với một entry cho host đích và next hop của nó. Nếu default router được chọn không phải là next hop tối ưu đến đích thì router sẽ gửi một Redirect message cho PC nguồn với một next hop router tốt hơn đến đích. PC sau đó sẽ cập nhật destination cache của nó với next hop mới cho đích đó. Các cache được duy trì bởi bởi mỗi IPv6 host và được query trước khi các solicitation message được truyền, các cache sẽ giúp giảm được số message và các cache này sẽ được cập nhật định kỳ.

· Để hỗ trợ các giao tiếp liên subnet thì IPv6 cung cấp một dích vụ hữu ích khác là Path MTU discovery. IPv6 không cho phép các router phân mảnh các packet quá lớn được truyền qua các liên kết của next hop, chỉ có các node nguồn mới được phép phân mảnh packet. Sử dụng IPv6 Path MTU discovery, một node nguồn có thể quyết định packet lớn nhất có thể được gửi đến đích. Với thông tin về các MTU của các liên kết có trên những hop trung gian, node nguồn có thể định lại kích thước cho các packet của nó một cách phù hợp để truyền.

### *3.1.3.3. Giao tiếp giữa các mạng:*

Trong quá trình tự cấu hình stateless, mỗi node có trách nhiệm cấu hình địa chỉ của chính nó và cache lại interface ID của nó và thông tin được cung cấp bởi giao thức neighbor discovery. Trong một mạng nhỏ, quá trình này có ích lợi là đơn giản và dễ dùng. Bất lợi của nó là quá dựa vào kỹ thuật multicast, sử dụng không hiệu quả tầm địa chỉ và thiếu bảo mật, thiếu sự kiểm soát chính sách và việc đăng nhập.

· Để hỗ trợ các giao tiếp giữa các mạng lớn hơn và phức tạp hơn thì ta phải sử dụng quá trình tự cấu hình stateful. Để hiểu rõ hơn quá trình này, ta phải hiểu rõ các khái niệm sau: stateful autodiscovery; DHCPv6; DHCPv6 client, relay, agent, server.

· Stateful autoconfig dựa trên các server để cung cấp các thông tin cấu hình, những server này được gọi là các DHCPv6 server. Tuy nhiên, với các nhà quản trị thì stateful phức tạp hơn stateless vì nó yêu cầu các thông tin cấu hình phải được thêm vào cơ sở dữ liệu của DHCPv6 server. Do đó, stateful có khả năng mở rộng tốt hơn cho những mạng lớn.

· Stateful có thể được sử dụng đồng thời với stateless. Ví dụ: một node có thể theo các quá trình stateless trong quá trình khởi động để lấy địa chỉ liên kết cục bộ. Sau đó, nó có thể sử dụng stateful để lấy thêm các thông tin từ DHCPv6 server.

· Để lấy thông tin cấu hình thì PC phải xác định một DHCPv6 server bằng cách gửi ra một DHCP solicit message hay bằng cách lắng nghe một DHCP advertisement. PC sau đó sẽ gửi một unicast DHCPv6 Request. Nếu DHCPv6 server không ở chung subnet với PC thì một DHCP relay hay agent sẽ forward yêu cầu cho một server khác. Server sẽ hồi âm bằng một DHCPv6 Reply chứa thông tin cấu hình cho PC.

· Việc sử dụng DHCPv6 có nhiều ích lợi như:

+ Kiểm soát: DHCPv6 kiểm soát việc phân phối và gán các địa chỉ từ một điểm kiểm soát tập trung.

+ Tóm tắt: do việc phân phối có thứ bậc nên có thể tóm tắt.

+ Renumbering: khi một ISP mới được chọn để thay thế cái cũ thì các địa chỉ mới có thể dễ dàng được phân phối hơn với dịch vụ DHCPv6.

+ Bảo mật: một hệ thống đăng ký host có thể được sử dụng trong một dịch vụ DHCPv6. Hệ thống đăng ký này có thể cung cấp một cách có chọn lựa các dịch vụ mạng cho các host đăng ký và từ chối truy cập cho các host không đăng ký.

## 3.2. Cách đặt địa chỉ trong IPv6

### 3.2.1.Cấu trúc địa chỉ IPv6.

Địa chỉ IPv6 dài 128 bit gồm 8 phần ở dạng thập lục phân được phân cách bởi các dấu hai chấm (:). Mỗi phần của nó sẽ dài 16 bit. IPv6 sử dụng dang thập lục phân, đây là thay đổi cơ bản so với IPv4 sử dụng dạng chấm (dot). Nguyên nhân là do tầm địa chỉ IPv6 quá lớn nên không thể sử dụng dạng dot vì sẽ rất dài (gấp 4 chiều dài của IPv4 hiện tại).

Một dạng chuẩn của một địa chỉ IPv6 sẽ có dạng:

2001:0010:3456:6EFD:00AC:0DEC:DDEE:EEDD

IPv6 cung cấp 2 phương pháp để rút gọn việc ghi địa chỉ. Thứ nhất là việc bỏ các số 0 đứng đầu và thứ hai là việc thay thế nhiều nhóm số 0 thành một dấu :

Ví dụ: địa chỉ sau đây trước khi được rút gọn có dạng:

ADBF:0:0:0:0:000A:00AB:0ACD

Sau khi rút gọn theo cách 1:

ADBF:0:0:0:0:A:AB:ACD

Sau khi rút gọn theo cách 2:

ADBF::A:AB:ACD

Chú ý: Dấu :: chỉ xuất hiện duy nhất một lần trong địa chỉ.

Để biểu diễn một địa chỉ IPv4 theo dạng IPv6, ta gán 6 phần đầu của địa chỉ IPv6 bằng 0, 2 phần còn lại dài 32 bit được ghi theo kiểu IPv4. Ví dụ: IPv4 sẽ có dạng: 0:0:0:0:0:0.A.B.C.D hay ::A.B.C.D

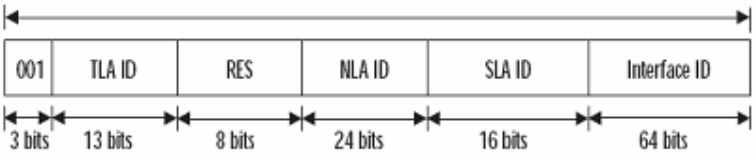
Ví dụ: ::192.168.1.1

### 3.2.2. Các loại địa chỉ.

IPv6 có các loại địa chỉ sau: unicast, multicast và anycast.

- Unicast: một địa chỉ unicast đại diện cho một host. Các địa chỉ unicast được chia nhỏ thành những dạng sau: địa chỉ unicast khả tóm tắt toàn cục (AGU); địa chỉ loopback; địa chỉ không xác định; interface ID; địa chỉ unicast cục bộ; NSAP; IPX.

· AGU (Global Unicast Address): là một cấu trúc giúp gán và phân phối các địa chỉ IPv6. Cấu trúc này chia tầm địa chỉ ra làm 5 phần gồm: FP(Format




Hình 3.7. Cấu trúc địa chỉ AGU.

prefix); Top level aggregation identifier (TLA ID); next level aggregation identifier (NLA ID); site level aggregation identifier (SLA ID); và interface ID.

+ FP: luôn là 001 để xác định địa chỉ này ở dạng địa chỉ khả định tuyến toàn cục. Với mỗi loại địa chỉ IPv6 sẽ có một Format Prefix duy nhất để giúp các thiết bị định tuyến dễ dàng xử lý địa chỉ hơn.

+ TLA-ID: cung cấp 8192 TLA, nghĩa là có thể có 8192 nhà cung cấp ở cấp này. Các TLA ở cấp cao nhất của bảng phân cấp định tuyến. Các TLA sẽ được gán một trong 8192 TLA ID và sẽ có trách nhiệm phân phát các địa chỉ của mình quản lý xuống cho các khách hàng.

+ NLA-ID: là các ID cho các nhà cung cấp cấp 2, một NLA có thể là một tổ chức có một kết nối với một TLA hay là một ISP. NLA sẽ được nhận một NLA-ID từ TLA, và đến lượt nó, nó phải cung cấp địa chỉ của nó cho các khách hàng.

+ SLA-ID: SLA là mạng của khách hàng.

· Nhà cung cấp cao nhất cho các tầm địa chỉ IPv6 là Internet Assigned Number Authority (IANA). IANA sẽ phân phối các tầm địa chỉ cho các Internet Registry (IR) ở từng khu vực. Có 3 IR là: ARIN; RIPE Network Cordination Centre (NCC); và APNIC. ARIN thuộc khu vực châu Mỹ, Caribê, và một phần châu Phi; RIPE NCC quản lý châu Âu, Trung Đông, và phần còn lại của châu Phi; APNIC quản lý khu vực châu Á Thái Bình Dương. Các IR sẽ chia tầm TLA thành những tầm TLA con, giúp phân phối địa chỉ theo quy luật sau:

+ IR sẽ gán các địa chỉ cho các TLA con (TLA ISP).

+ TLA ISP sẽ gán các địa chỉ NLA cho các NLA ISP.

+ NLA ISP sẽ gán các SLA cho khách hàng.

· Địa chỉ loopback: không phải là một địa chỉ, có dạng: 0:0:0:0:0:0:0:1 hay ::1. Được sử dụng để kiểm tra.

· Interface ID: để tạo các địa chỉ EUI-64 từ địa chỉ MAC, ta thực hiện các bước sau:+ Thêm FF-FE vào giữa các byte 3 và 4 của địa chỉ MAC.

+ Lấy bù bit "Universal/Local"(U/L), là bit thứ 7 kể từ trái sang của địa chỉ MAC.

Ví dụ: Ta có địa chỉ MAC: 0008:749B:3CF4

Bước 1: Thêm FF-FE vào giữa byte thứ 3,4 của địa chỉ MAC:

Là thêm vào giữa 74 và 9B:

0008:74FF:FE9B:3CF4

Bước 2: Lấy bù bit U/L của byte đầu tiên:

Byte đầu tiên là 00:

00000000=00000010=02h

Vậy ta có EUI-64 từ MAC trên là:

0208:74FF:FE9B:3CF4

· Địa chỉ sử dụng cục bộ: gồm 2 loại: địa chỉ liên kết cục bộ (được sử dụng trên 1 liên kết) và địa chỉ site cục bộ (được sử dụng trong một site).

+ Địa chỉ liên kết cục bộ: chỉ có tác dụng trên một liên kết của router. Chỉ những host và interface của router được kết nối vào cùng một subnet mới có được địa chỉ liên kết cục bộ của segment đó. Router sẽ không quảng bá địa chỉ này.

Có dạng sau:

1111111010 0.....0 Interface I

10bit 54bit 64 bit

hay :FE80::/64

+ Site-local address: là địa chỉ chỉ có thể định tuyến được trong một site. Nghĩa là các host được cấu hình với địa chỉ này có thể giao tiếp với các host

khác trong cùng một múi mạng nhưng không được định tuyến ra ngoài. Site-local giống như địa chỉ private trong IPv4. Có dạng:

1111111011 0.....0 subnet ID Interface

10 bit 38bit 16bit 64 bit

Hay: FEC0::/10

- Subnet trong IPv6. IPv6 được chia nhỏ thành các prefix là TLA, subTLA, NLA và SLA. Các ARIN, RIPE, APNIC phân phối các sub TLA cho các nhà cung cấp TLA. Những nhà cung cấp này lại phân phối các tầm địa chỉ NLA cho các nhà cung cấp nhỏ hơn...

Các tầm địa chỉ sau sẽ được phân phối cho các IR:

2001:0400::/23 cho ARIN

2001:0200::/23 cho APNIC

2001:0600::/23 cho RIPE

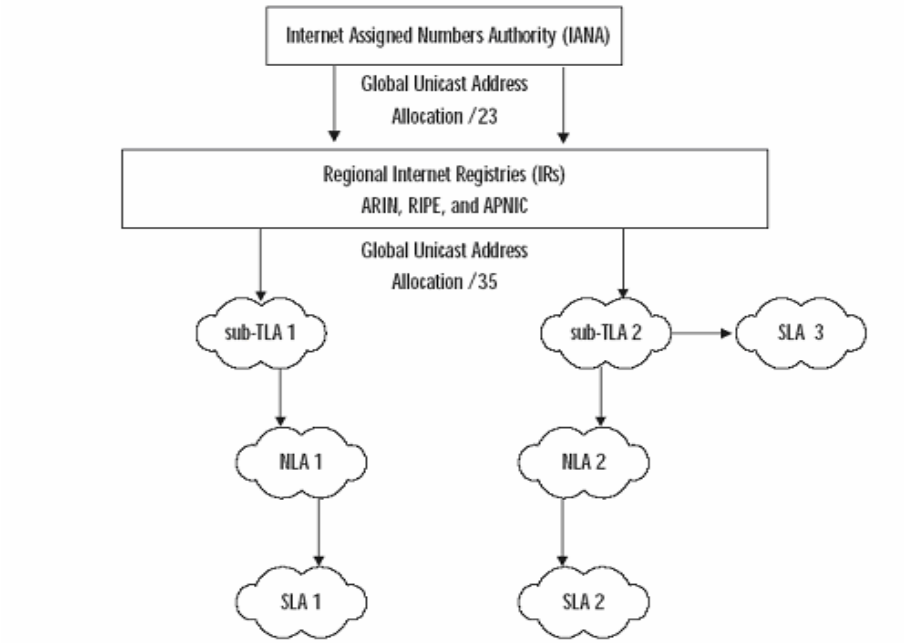
Ví dụ sử dụng ARIN, quy luật phân phối như sau:

- ARIN sẽ phân phối các địa chỉ /35 cho các subTLA.

- TLA sẽ phân phối các tầm địa chỉ cho các NLA, các NLA sẽ phân phối một tầm địa chỉ /48 cho các SLA.

- Phân phối /64 cho các SLA chỉ có một subnet.

- Phân phối /128 cho các SLA với chỉ 1 subscriber.




Hình 3.8. Phân phối địa chỉ AGU.

Ví dụ: ARIN có được tầm địa chỉ 2001:0420::/23, sẽ phân phối xuống cho các subTLA: subTLA1 có tầm 2001:0420::/35; subTLA2 có tầm 2001:0428::/35. Việc phân phối này cho phép các subTLA subnet tầm địa chỉ được phân để phân phối xuống cho các NLA:

· SubTLA1 sẽ cung cấp các prefix cho các NLA:

2001:0420:0001::/48

2001:0420:0002::/48

· SubTLA2 sẽ cung cấp cho các NLA:

2001:0428:0001::/48

2001:0428:0002::/48

· Mỗi NLA lại subnet và phân phối cho các SLA; với NLA có tầm địa chỉ 2001:0420:0001::/48 có thể phân phối các địa chỉ sau:

2001:0420:0001:1::/48

2001:0420:0001:2::/48

Sử dụng cách phân phối này, ta chỉ cần quản l tầm địa chỉ ở mỗi cấp, vì vậy giảm được kích thước bảng định tuyến.

- Địa chỉ multicast.

Địa chỉ multicast có cấu trúc như sau:

11111111 flag scope groupID

8bit 4bit 4bit 112bit

· Flag: là trường 4 bit, trong đó chỉ sử dụng bit thứ tư (ba bit đầu không sử dụng) để xác định xem đây là địa chỉ thường được sử dụng (permanent) hay không. Nếu bit đó bằng 0 thì nghĩa là permanent và 1 nghĩa là non-permanent. Các địa chỉ permanent là do một tổ chức quốc tế gán.

· Trường scope: được sử dụng để xác định phạm vi của group, gồm các giá trị sau:

1- Node-local scope

2- Linl-local scope

5-site-local scope

8-organization-local scope

E-global scope

GroupID: xác định ID của group.

Các địa chỉ thường dùng:

- Node-local scope: FF01:0:0:0:0:0:0:1(địa chỉ cho tất cả các node);

FF01:0:0:0:0:0:0:2(tất cả router).

- Link-local scope:

FF02::1-tất cả các node

FF02::2-tất cả router

FF02::4-DVMRP router

FF02::5-tất cả OSPF IGP router

FF02::6-tất cả OSPF IGP DR

FF02::7-ST router

FF02::8-ST host

FF02::9-RIP router

FF02::A-EIGRP router

FF02::B-mobile agent

FF02::D-PIM router

FF02::1:2-DHCP agent

FF02::1:FFxx:xxx-solicited node address

- Site-local scope:

FF05::2-tất cả router

FF05::1:3-tất cả DHCP server

- Địa chỉ anycast: bất cứ địa chỉ nào được gán cho nhiều hơn 1 interface thì được xem là địa chỉ anycast. Các packet được gửi đến một địa chỉ anycast sẽ được định tuyến đến interface gần nhất có địa chỉ đó. Anycast không khác unicast. Do đó, router phải được cấu hình để xử l những gói tin anycast. Địa chỉ này có dạng:

Subnet prefix 0….0

n bit 128-n bit

Có 2 loại địa chỉ anycast được giành sẵn. Định dạng của những địa chỉ này phụ thuộc vào loại địa chỉ IPv6 được cấu hình. Định dạng này được quyết định bằng cách xét định dạng prefix. Quy luật là nếu các bit đầu tiên của 1 địa chỉ là 000 thì interface ID có thể có chiều dài không cố định, còn nếu các bit đầu không phải là 000 thì interface ID phải là 64 bit.

Ví dụ: Loại địa chỉ anycast có 64 bit interface ID có dạng:

Subnet Prefix 111…111 Anyast ID

n bit 121-n 7 bit

Interface ID của loại này tùy thuộc vào chiều dài của subnet ID.

· Các địa chỉ anycast này không được sử dụng để gán cho các interface. Hiện nay chỉ có 3 Anycast ID là: 7E (làm địa chỉ của home-agent trong mibile IPv6); 7F, và 00.

· Ví dụ: Nếu ta viết interface ID của IPv6 home agent, ta sẽ viết:

1111110111111111 111….111 1…10=111111011…111 1111110

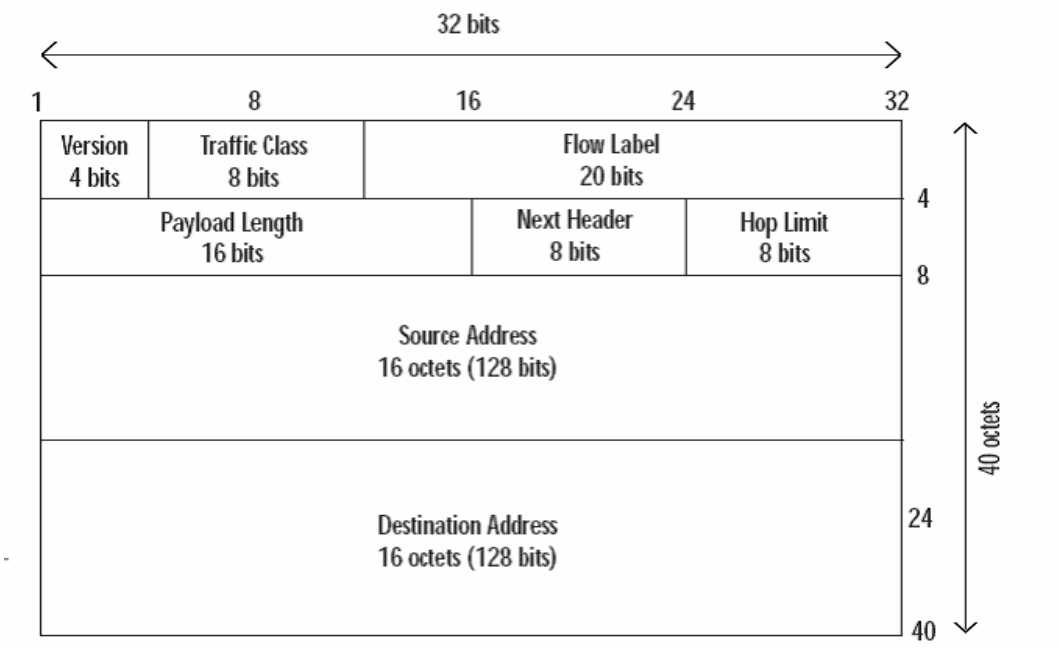
57bit 7bit=FE

## 3.3. IPv6 Header

### 3.3.1. Phân tích:

IPv6 header có kích thước cố định. Trong khi IPv4 header có kích thước thay đổi. Với kích thước cố định thì một router có thể xử lý gói tin một cách hiệu quả.

IPv6 header lưu các thông tin cần thiết để định tuyến và phân phát gói tin đến đích. Các header sẽ được xử lý bởi mỗi node trên đường đến đích. Bốn bit đầu tiên là version được sử dụng để xác định version của giao thức IP đang được sử dụng và nó có giá trị là 6 với IPv6. Trường này rất quan trọng vì nó cho phép cả hai giao thức cùng tồn tại trên một segment mà không xảy ra đụng độ.




Hình 3.9. IPv6 header.

Hai trường tiếp theo là traffic class và flow label được sử dụng để cung cấp các kiểu chất lượng dịch vụ (QoS) dạng diffServe và cung cấp sự hỗ trợ các ứng dụng có yêu cầu xử lý đặc biệt theo từng luồng dữ liệu. Trường traffic class có tác dụng như trường Type of Service (ToS) của IPv4, được sử dụng để ưu tiên traffic. Trường flow label kết hợp với địa chỉ nguồn và đích giúp xác định luồng traffic có yêu cầu được xử lý đặc biệt bởi các router trên đường. Khi một router xác định dòng traffic lần đầu, nó sẽ nhớ dòng traffic đó, cũng như các xử lý đặc biệt ứng với traffic này, và khi các traffic khác thuộc dòng này đến, nó sẽ xử lý nhanh hơn là xử lý từng packet.

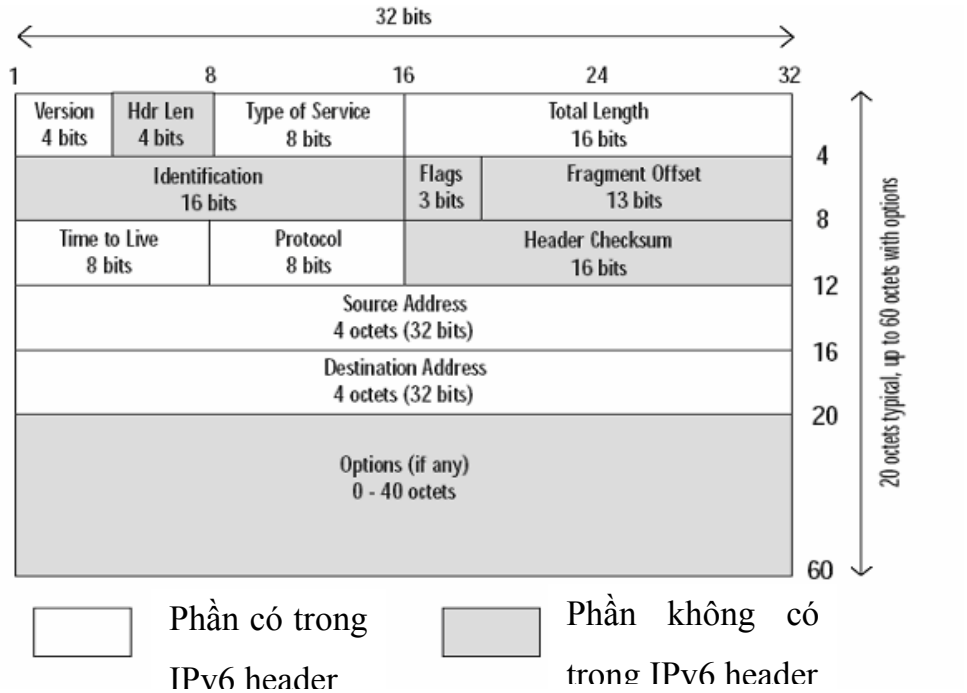
Trường payload tương tự như trường total length của IPv4, xác định tổng kích thước của gói tin IPv6 (không chứa header).

Trường next header được sử dụng để xác định header tiếp theo sau IPv6 header. Mục đích của trường nay giống với trường protocol bên IPv4.

Trường hop limit được sử dụng để giới hạn số hop mà packet đi qua, được sử dụng để tránh cho packet được định tuyến vòng vòng trong mạng. Trường này giống như trường TTL (Time-To-Live) bên IPv4.

### 3.3.2. So sánh IPv6 và IPv4 header.

IPv6 header có một vài điểm chung so với IPv4, chúng ta sẽ phân tích lại IPv4 header để xem xét sự giống và khác nhau giữa chúng cũng như thấy được sự cải tiến trong nội dung header của IPv6.




Hình 3.10. IPv4 header.

- Version: giống ở IPv6

- Header length: xác định kích thước header tùy thuộc vào trường Option. Trường này không có ở IPv6 vì IPv6 header có kích thước cố định.

- Type of service (ToS): tương tự như traffic class bên IPv6.

- Total length: giống với payload length bên IPv6.

- Identification, flags, fragment offset: được sử dụng để xử lý việc phân mảnh và kết hợp các gói tin. Ở IPv4, một hop trung gian có thể phân mảnh một packet khi kích thước lớn hơn MTU của hop đó. Không giống với IPv4, việc xử lý phân mảnh trong IPv6 xảy ra chỉ trên node nguồn bằng việc sử dụng kỹ thuật gọi là path MTU. Do đó, thông tin liên quan đến việc phân mảnh sẽ được mã hoá trong header "fragmentation" (là một header mở rộng của gói tin IPv6).
- TTL: giống như hop limit bên IPv6.
- Protocol: tương tự như next header bên IPv6.
- Header checksum: được sử dụng để đảm bảo sự toàn vẹn của IPv6 header.

Tuy nhiên, ở lớp trên lại tính lại checksum cho toàn packet nên việc tính header checksum là dư thừa, nên trong IPv6 header không có trường này.

- Options: trường này được được mã hoá trong các header mở rộng bên IPv6.

### 3.3.3. Header mở rộng của IPv6.

Các header mở rộng được đặt giữa IPv6 header và header của các giao thức lớp trên, được sử dụng để mang các thông tin tuỳ chọn ở lớp Internet trong packet. Một IPv6 packet có thể chứa một hay nhiều header mở rộng. Mỗi header mở rộng sẽ có giá trị đại diện cho nó. Ví dụ: TCP (6); UDP (7); Routing header (43); Fragment header (44); ESP (50); AH (51); ICMP (58)...

IPv6 có thể được thực thi đầy đủ với các header mở rộng sau: hop-by-hop option; routing; fragment; destination option; authentication và ESP. Khi có nhiều header cùng tồn tại trong một packet thì chúng nên theo thứ tự sau:

- IPv6 header
- Hop-by-hop option (0)

- Destination option header (60) (được xử lý bởi mọi node có xuất hiện trong Routing header)
- Routing header (43)
- Fragment header (44)
- Authentication header (51)
- Encapsulating security payload (ESP) header (50)
- Destination option header (60) (chỉ được xử lý bởi đích của gói tin)
- Upper layer header.

Trừ destination option header ra, các header khác đều xuất hiện một lần trong packet. Destination option header chứa thông tin được xử lý bởi đích cuối. Khi packet có chứa routing header, thì có thể sẽ có thêm một Destination option header nữa được sử dụng để xác định rằng packet này nên được xử lý bởi tất cả các node trung gian được liệt kê trong routing header.

Khi IPv4 có chứa trường Option thì tất cả các hop trung gian đều phải xử lý gói tin nên làm tăng độ trễ truyền cho gói tin. Chỉ trừ header Hop-by-hop option, còn các header còn lại chỉ được xử lý bởi node đích của packet. Hop-by-hop option header chứa các thông tin tuỳ chọn mà cần được xử lý bởi tất cả các node trung gian. Giá trị của trường next header xác định hành động kế tiếp được xử lý, do đó các header mở rộng phải được xử lý theo thứ tự mà chúng xuất hiện trong các packet. Khi một node nhận được một giá trị next header mà nó không biết, nó sẽ bỏ gói tin và gửi một gói tin được gọi là ICMP parameter problem cho nguồn của gói tin. Hiện tại, hop-by-hop option header và destination option header sẽ chứa một số các tùy chọn được mã hoá ở dạng Type-Length-Value (TLV). Loại tùy chọn được mã hoá sao cho 2 bit cao nhất sẽ xác định hành động mà node sẽ làm nếu nó không nhận ra loại tuỳ chọn và bit thứ 3 sẽ xác định dữ liệu tuỳ chọn có thể thay đổi đường đi để đến

đích cuối của packet hay không. Ví dụ: khi một node xác định một giá trị kiểu tuỳ chọn là 130 (10000010), 2 bit cao nhất là 10 (nghĩa là bỏ packet và gửi một ICMP parameter problem cho nguồn của gói tin). Các giá trị 2 bit đầu như sau:

00-bỏ qua option này và tiếp tục xử lý header

01-bỏ qua packet

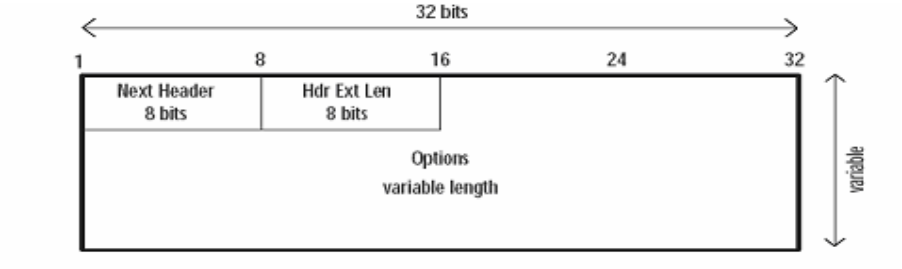
10-bỏ qua packet và gửi ICMP parameter problem

11-bỏ qua packet và nếu đích của packet không phải là multicast thì mới gửi ICMP parameter problem.

Bit thứ 3 bằng 0 là không cho phép dữ liệu tuỳ chọn thay đổi đường đến đích và bằng 1 là cho phép thay đổi.

***3.3.3.1.Hop-by-hop option header.***

Hop-by-hop option header header chứa thông tin tùy chọn được xử lý bởi

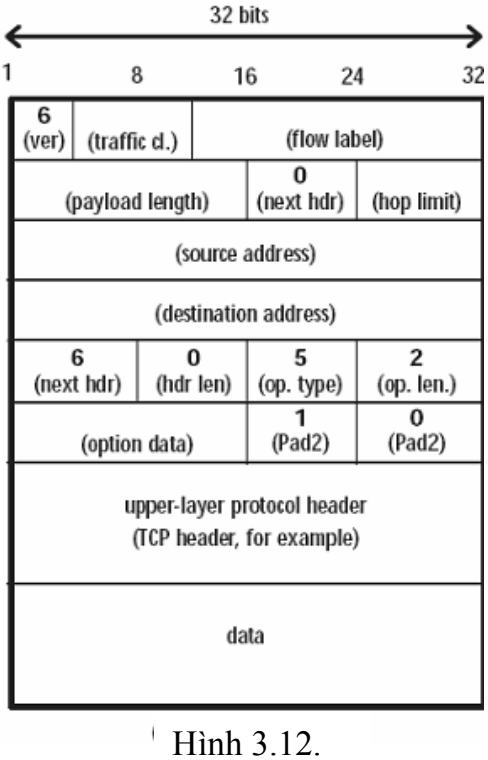



Hình 3.11. Hop-by-hop option header

tất cả các node trung gian. Nó có dạng:

Loại tuỳ chọn của tùy chọn cảnh báo router (Router Alert option) là 5 (00000101) xác định rằng các node nếu không nhận ra tùy chọn này có thể bỏ qua nó và tiếp tục xử lý header, và dữ liệu tuỳ chọn không được thay đổi đường đi. Kích thước của tùy chọn là 2. Ví dụ: hình 3.12 sẽ mô tả một packet

gồm một router alert hop-by-hop option

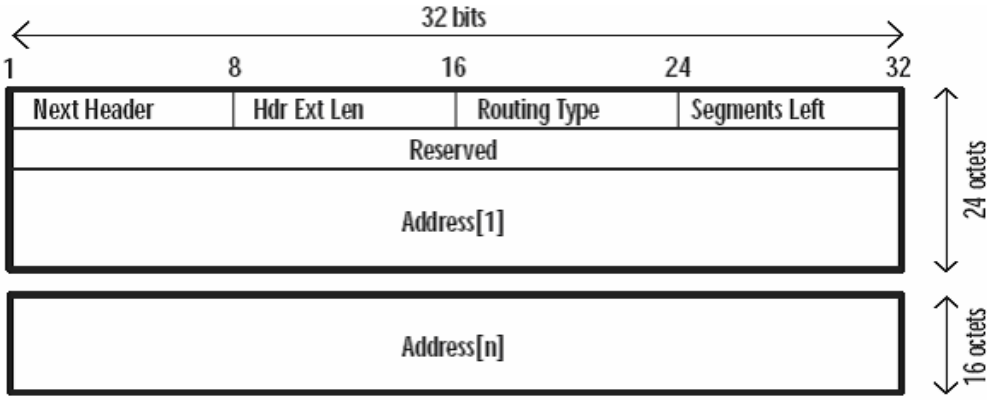



Hình 3.12.

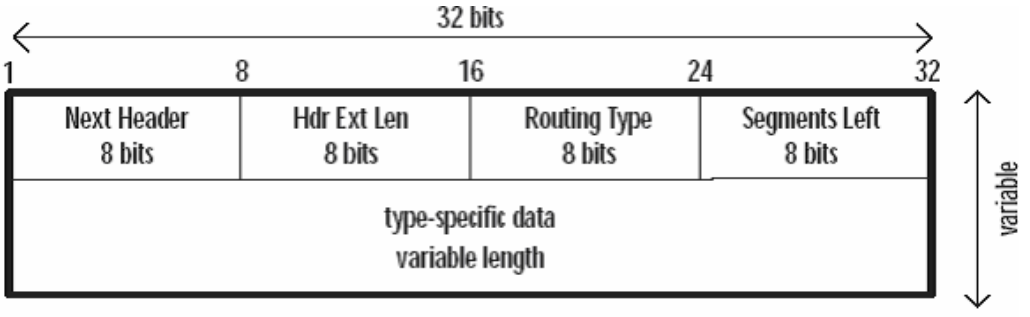
### *3.3.3.2. Routing header.*

Routing header là header cho phép nguồn quyết định những đường để đến đích bằng cách liệt kê một hay nhiều các node mà nó sẽ đi qua. Nó có dạng:

Khi một node xác định kiểu định tuyến mà nó không biết và giá trị của segment left bằng 0, nó sẽ bỏ qua routing header và tiếp tục xử lý header. Tuy nhiên nếu segment left khác




Hình 3.14. Routing header có kiểu định tuyến bằng 0.



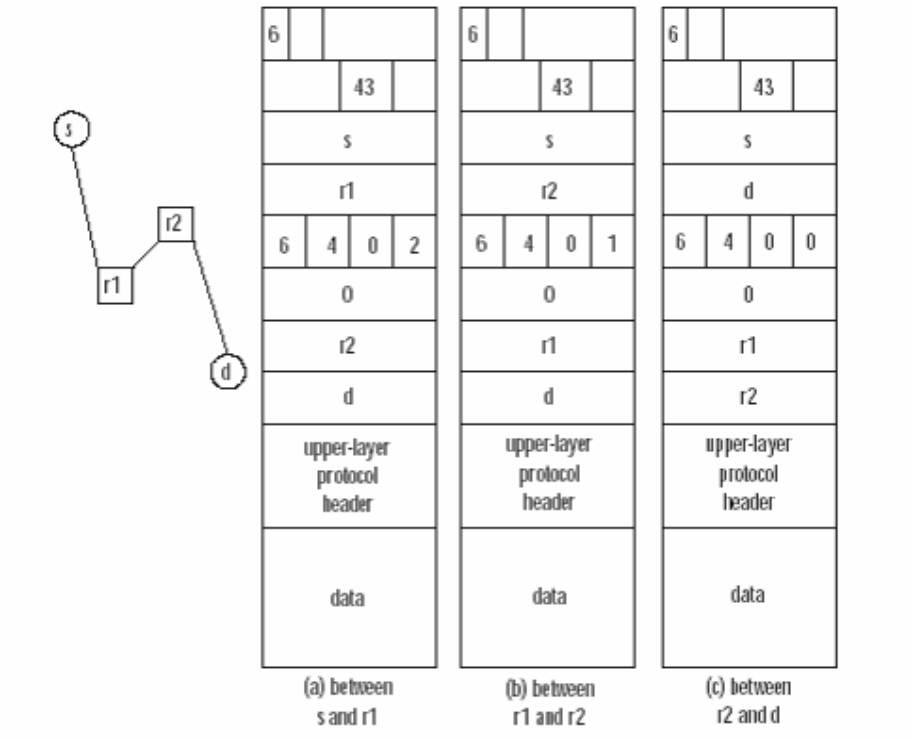

Hình 3.13. Routing header

0 thì node sẽ bỏ gói tin và gửi ICMP parameter problem đến nguồn. Hiện nay, chỉ có kiểu định tuyến bằng 0 mới được định nghĩa và nó có dạng:

Tác dụng khác của routing header là để giao tiếp với một node di động ở xa home network của nó mà không cần định tuyến tam giác. Nếu không cần tối ưu đường thì packet có thể được gửi đến home network của node di động và sau đó sẽ được HAtruyền đi, tạo nên định tuyến tam giác. Do đó, nguồn của kết nối có thể xác định đường đi bằng cách sử dụng routing header loại 0 và cho phép nguồn xác định đường mà không cần định tuyến tam giác.

Ví dụ: Với kết nối giữa node nguồn s và node đích d qua 2 router trung gian r1, r2 thì s có thể tạo IPv6 packet với routing header như hình 3.15.

Ta thấy, ở hình (a) trường đích là r1 mà không phải là node d, nguyên nhân là do, vì chỉ trừ hop-by-hop option header là được xử l bởi tất cả các node trung gian trên đường đi tới đích, các header còn lại chỉ được xử l bởi duy nhất node đích của packet, do đó, đích của gói tin phải là router r1, sau khi xem xét IPv6 header, nó sẽ tiếp tục xử lý header mở rộng, lúc đó, r1 sẽ xử lý routing header mà node s gửi cho nó: địa chỉ đầu của routing header là router tiếp theo trên đường đi (r2) theo sau là node đến cuối cùng. Router r1 sẽ giảm trường segment left và hóan đổi các giá trị của trường destination trong IPv6 header với trường first address trong routing header, và gửi cho r2. Hình b miêu tả packet mà r1 gửi cho r2. Tương tự như vậy, sau khi xem xét IPv6 header, r2 sẽ tiếp tục xử lý routing header (vì trường đích là r2 nên r2 được phép mở routing header), r2 sẽ giảm segment left và hóan đổi trường destination với địa chỉ thứ 2 trong routing header. Khi xử lý routing header, index của địa chỉ để có thể hoán chuyển với trường đích được tính như sau:




Hình 3.15. Các gói với routing header.

(Header extension length%2)-(Segment left -1)

Header Extension header=2*(số địa chỉ có trong routing header)

Do đó, Hdr Ext length không được lẻ, nếu l3 thì node đang xử lý sẽ gửi gói tin ICMP parameter problem về node nguồn.

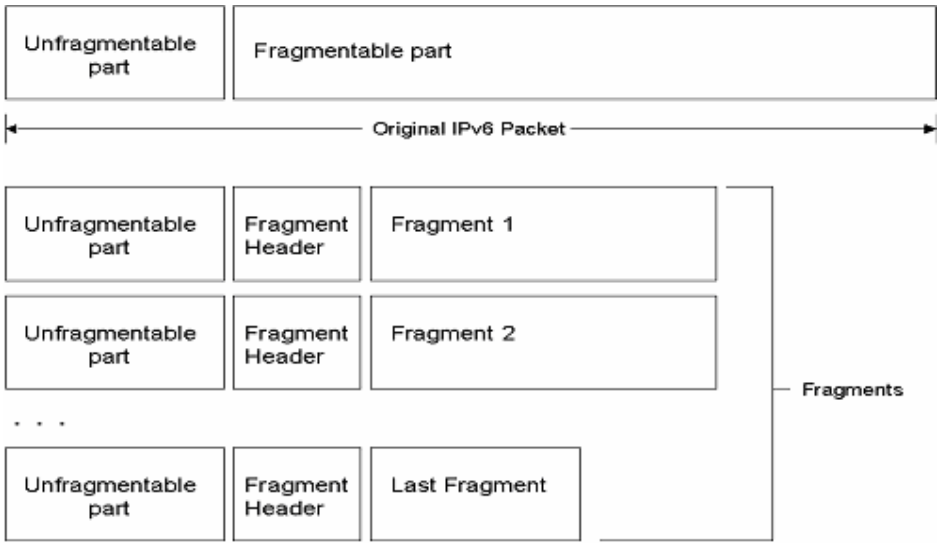
Khi segment left giảm tới 0 thì node đang xử l routing header sẽ được xem như node đích của gói tin và nó sẽ tiếp tục xử lý các header khác trong packet mà không gửi gói tin đi nữa.

#### *3.3.3.3. Fragment header.*

Ở IPv4 thì trường total length trong header sẽ giới hạn kích thước tối đa của 1 packet là 64 kB. Tuy nhiên, phụ thuộc vào kỹ thuật được sử dụng mà kích thước thật của packet có thể được giới hạn lại. Do đó, nếu packet quá lớn thì IP có nhiệm vụ phân mảnh packet để đảm bảo kích thước packet không

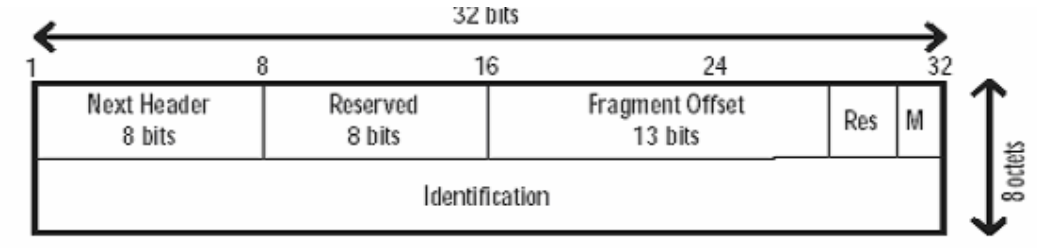
vượt quá MTU. Do đó, dữ liệu của người dùng được gửi trong một packet từ một nguồn có thể đến đích trong nhiều packet nếu có 1 liên kết có MTU nhỏ hơn MTU của node nguồn. Tuy nhiên việc phân mảnh này sẽ không tối ưu.

Ví dụ: giả sử, ta gửi 1 ứng dụng 3000 byte từ nguồn có MTU là 3000 byte, khi gửi đến liên kết tiếp theo có MTU=1500 byte, do đó, packet phải bị chia đôi, sau đó lại gửi đến liên kết tiếp theo nữa có MTU là 1000 byte thì gói tin lại phải chia làm 4 phân: 2 phần 1000 và 2 phần 500. Do đó, không tối ưu. Nếu nguồn biết được MTU thì nó có thể chỉ cần chia gói tin ra làm 3 phần, mỗi phần 1000byte ngay từ đầu. Ở IPv6 thì node nguồn sẽ tìm ra MTU nhỏ nhất trên đường đi và thực hiện việc phân mảnh tối ưu. Trước khi phân mảnh thì gói tin gốc sẽ gồm 2 phần: phần có thể phân mảnh và phần không thể phân mảnh. Trong đó, IPv6 header và các header mở rộng (được xử l bởi node đích) là có thể phân mảnh. Hình 3.16 sẽ mô tả quá trình phân mảnh trong IPv6.




Hình 3.16. Quá trình phân mảnh trong IPv6

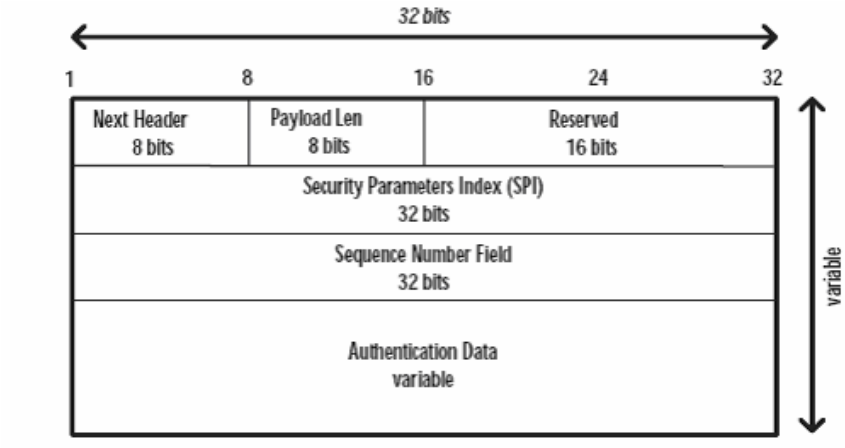
Fragment header có dạng:




Hình 3.17. Fragment header

### *3.3.3.4.Authentication header.*

Trong một mạng IP, cả trong IPv4 và IPv6 thì header này được sử dụng để cung cấp sự toàn vẹn dữ liệu và xác minh nguồn gốc của dữ liệu. Trong




Hình 3.18. Định dạng của AH.

mạng IPv6, AH cung cấp sự xác thực cho IPv6 header, các header của các giao thức lớp trên và dữ liệu người dùng, cũng như các header mở rộng không được phép thay đổi trên đường đi. Định dạng của AH được mô tả trong hình 3.18.

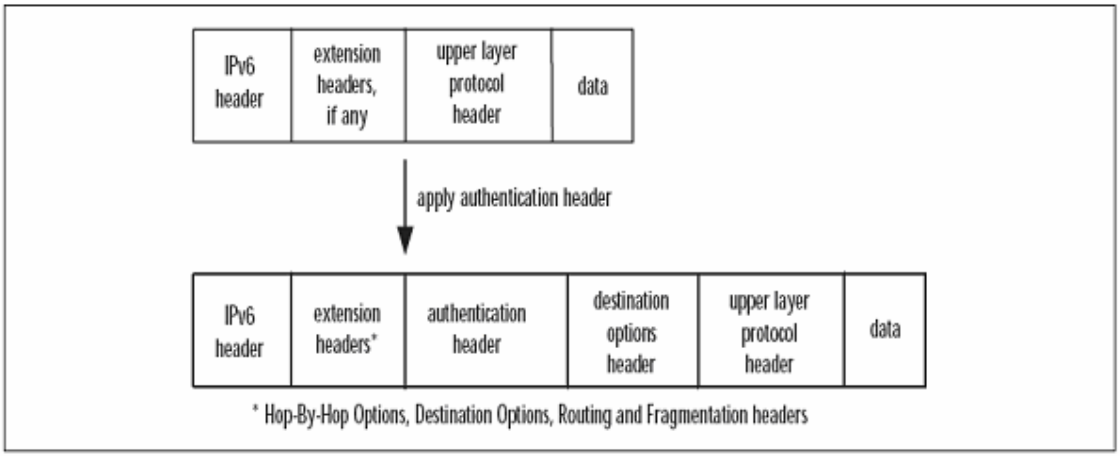
Trường sequence number được sử dụng để cung cấp sự bảo vệ chống lại sự nghe lén dữ liệu. Khi một Security Association (SA) được thiết lập giữa nguồn và đích thì các bộ đếm ở bên gửi và bên nhận sẽ được thiết lập là 0. Do

đó, bắt buộc bên gửi phải tăng trường này qua mỗi lần truyền, tuy nhiên, bên nhận có thể không xử lý việc truyền này. Dịch vụ này chỉ hiệu quả nếu bên nhận xử lý trường này.

Trường xác thực dữ liệu chứa Integrity Check Value(ICV) cho packet. Giải thuật xác minh (được lựa chọn khi SA được thiết lập giữa bên gửi và bên nhận) sẽ xác định kích thước của ICV, các quy tắc so sánh, và các bước xử lý cần thiết. Giá trị này được tính trên gói tin bởi node nguồn và được xác minh bởi node đích (bằng cách so sánh giá trị trong packet nhận được với cái mà nó tính ra).

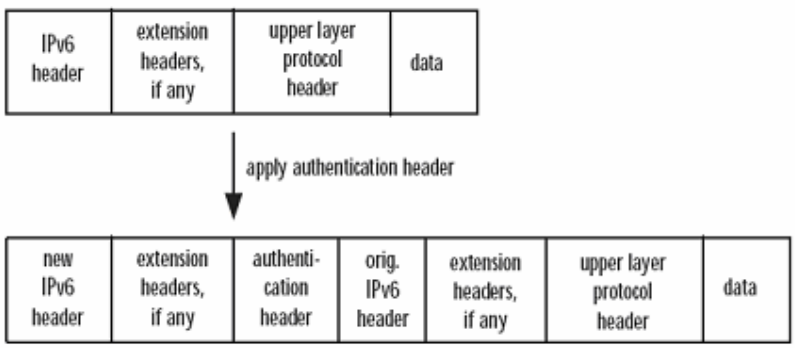
AH có thể được sử dụng ở trạng thái transport hay tunnel. AH ở transport mode được thực thi ở các host, cung cấp sự bảo vệ cho các header ở lớp trên và các trường trong IPv6 header. Còn AH ở tunnel mode được áp vào gói tin IPv6 gốc, bao đóng gói tin gốc bằng cách xây dựng một gói tin IPv6 mới sử dụng các địa chỉ IPv6 riêng, như một gateway bảo mật.

Ở transport mode, AH được xem như một end-to-end payload và được đặt sau IPv6 header và các header mở rộng trừ destination option header.




Hình 3.19. AH hoạt động ở transport mode.

Trong tunnel mode, AH được áp vào gói tin IPv6 ban đầu sử dụng các địa chỉ IPv6 khác như những điểm giao tiếp và một IPv6 header mới được xây




Hình 3.20. Thứ tự của các header khi áp AH vào tunnel mode.

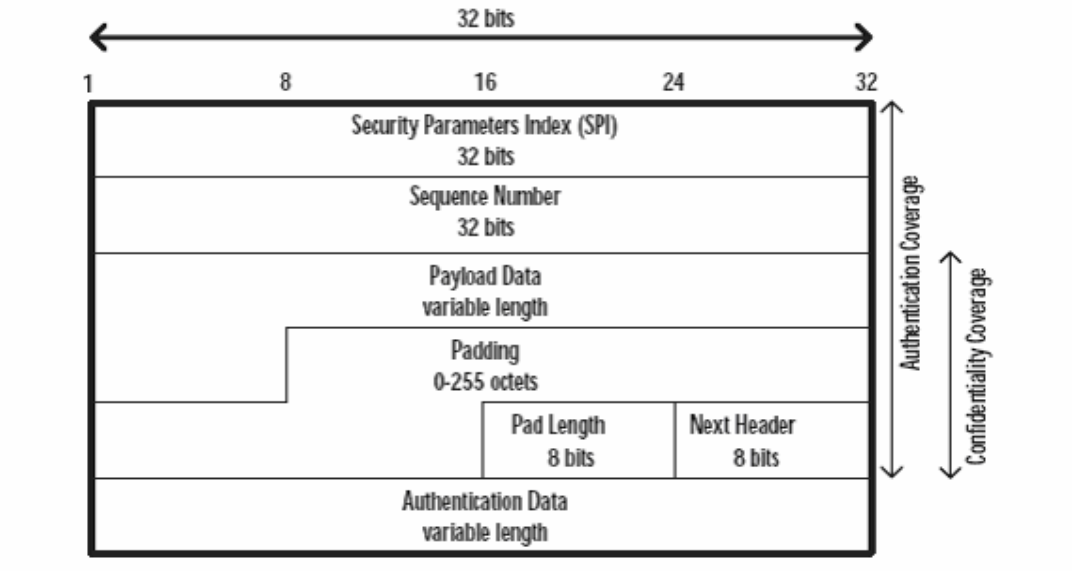
dựng sử dụng các địa chỉ của các gateway bảo mật cho các địa chỉ nguồn và đích. Quá trình xử lý phân mảnh có thể được áp vào AH.

***3.3.3.5 .Encapsulating security payload:***

ESP header được sử dụng ở transport mode hay tunnel mode cũng cung cấp các dịch vụ bảo mật trong các mạng IPv4 và IPv6. Các dịch vụ bảo mật qua ESP gồm xác thực nguồn gốc dữ liệu, dịch vụ anti-replay...Sự thực thi và các tuỳ chọn được chọn ở thời điểm thiết lập SA sẽ quyết định các dịch vụ bảo mật được sử dụng.

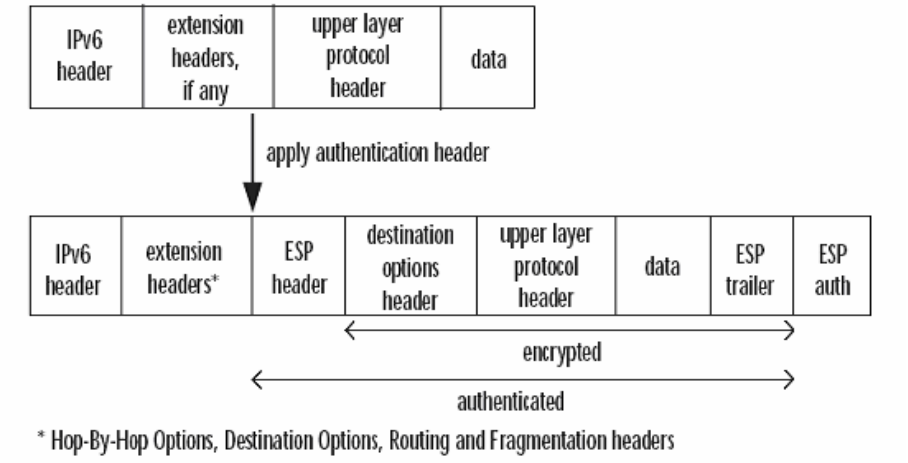
Trong trường hợp của AH khi cung cấp dịch vụ anti-replay, nguồn sẽ tăng sequence number tuy nhiên node đích phải kiểm tra trường nay để bật dịch vụ anti-replay. Để cung cấp dịch vụ xác thực nguồn traffic thì thông tin về nguồn và đích thực phải được che đi. Do đó, dịch vụ này yêu cầu ESP header được sử dụng trong tunnel mode. Hình 3.21 sẽ mô tả định dạng của ESP header. Giá trị next header của header trước nếu bằng 50 nghĩa là header tiếp theo được xử lý chính là ESP header. Trường payload data chứa dữ liệu đã được

mã hoá được mô tả bởi trường next header. Giải thuật mã hoá được sử dụng xác định kích thước và vị trí của cấu trúc dữ liệu trong trường payload data.



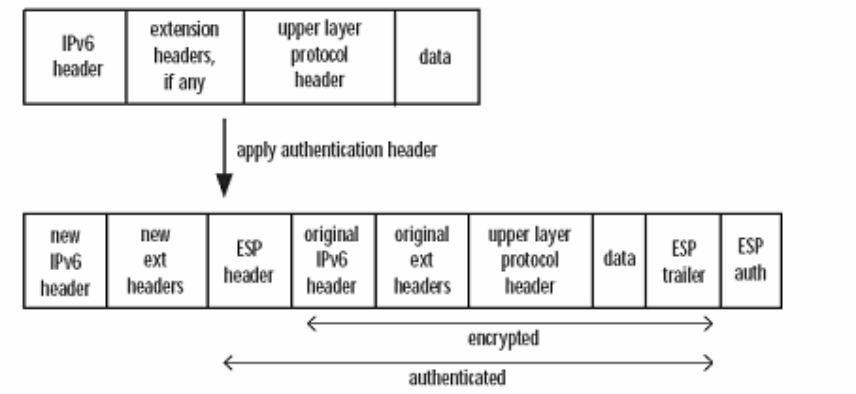

Hình 3.21. Định dạng của ESP header

thì thứ tự của các header trong IPv6 packet sẽ như sau:




Hình 3.23. Thứ tự của các header trong IPv6 khi hoạt động ở transport mode.

Và ở tunnel mode sẽ có thứ tự như sau:




Hình 3.24. Thứ tự của các header trong IPv6 khi hoạt động ở tunnel mode.

# CHƯƠNG 4. GIẢI PHÁP THỰC HIỆN IPv6 TRÊN NỀN IPv4

## 4.1. Các vấn đề chung.

IPv6 là một giao thức Internet mới được thiết kế nhằm đáp ứng các yêu cầu về phát triển các dịch vụ mới và mở rộng không gian địa chỉ trên mạng Internet, đồng thời khắc phục những hạn chế khác của IPv4 hiện nay không hỗ trợ tính "mở" của giao thức, dịch vụ QoS, các chức năng bảo mật… Tuy nhiên hai giao thức IPv4 và IPv6 không thật sự tương thích với nhau. Mặt khác, hệ thống IPv4 đã phát triển mạnh mẽ và hiện nay đã hình thành một mạng Internet toàn cầu có quy mô hết sức rộng lớn cả về kiến trúc mạng và dịch vụ trên mạng. Do vậy trong một tương lai gần không thể chuyển đổi mạng toàn bộ hệ thống mạng IPv4 hiện nay sang hệ thống mạng IPv6. Để triển khai mạng IPv6 hiệu quả và thiết thực, các nhà thiết kế IPv6 đã đưa ra các giải pháp sau:

- Xây dựng các cơ chế chuyển đổi cho phép kết nối các host/router IPv6 trên nền cơ sở hạ tầng của mạng IPv4 hiện nay.
- Song song là triển khai kết nối các mạng IPv6 lại với nhau hình thành một mạng IPv6 toàn cầu (kết nối vào mạng thử nghiệm 6Bone).

Thách thức mà IPv6 phải đối mặt là khả năng chuyển đổi "trọn vẹn" các gói tin IPv6 từ định dạng theo giao thức IPv6 sang IPv4 để từ đó có thể vận chuyển trên nền hạ tầng là mạng IPv4, vì hầu hết các thiết bị kết nối mạng Internet hiện nay đều được thiết kế cho IPv4.

Để thực hiện yêu cầu này, quá trình triển khai IPv6 phải đảm bảo tính linh động một cách tối đa, nhưng điều này mâu thuẫn với quy mô rộng lớn của mạng Internet. Do vậy, đây cũng thể coi là một điểm chính trong quá

trình thiết kế IPv6, đảm bảo sự thành công của mạng IPv6. Không đảm bảo được yêu cầu trên sẽ không có sự thành công của mạng IP6. Ví dụ : trước đây đã có một vài giao thức được thiết kế để thử thay thế TCP/IPv6, như XTP nhưng đã không thể thành công là do không có khả năng chạy song song (dual stack), hay không có tính tương thích lẫn nhau giữa các họ giao thức cũ và mới. IPv6 cũng vậy, nếu với các đặc tính ưu việt của nó so với IPv4 cũng chưa đủ để thuyết phục người dùng bỏ mạng IPv4 hiện nay để xây dựng mạng IPv6, do vậy cần phải đảm bảo tính tương thích trên cơ sở các chức năng của IPv4 trong quá trình chuyển đổi sang IPv6.

Để triển khai mạng IPv6 có các phương thức diễn ra đồng thời là xây dựng mạng IPv6 trên nền hạ tầng là mạng IPv4 hiện nay, sau đó thay thế dần mạng IPv4 hiện nay.

Mục đích của các cơ chế chuyển đổi là đảm bảo một số chức năng chính như sau:

- Đảm bảo thực hiện các đặc tính ưu việt của mạng IPv6 so với mạng IPv4.
- Tận dụng hạ tầng sẵn có của mạng Ipv4 trong giai đoạn chuyển tiếp sang một mạng thuần IPv6.
- Tăng cường khả năng nâng cấp và triển khai. Việc chuyển đổi đối với các host/router không bị phụ thuộc vào nhau.
- Tối thiểu hoá sự phụ thuộc trong các quá trình nâng cấp. Một trong những điều kiện bắt buộc để nâng cấp host tới IPv6 là hệ thống DNS server hỗ trợ IPv6. Các điều kiện đối với các router như hỗ trợ các giao thức định tuyến BGP4+, hỗ trợ IPv6 … chưa phải là bắt buộc.
- Gán và cấp phát các loại địa chỉ thuận tiện. Khi các hệ thống IPv4 được cài đặt được gán các địa chỉ IPv4, mặt khác địa chỉ IPv4 là một tập con của địa chỉ IPv6, do vậy có thể tiếp tục sử dụng với các địa chỉ IPv4 sẵn có.

Chỉ gán các địa chỉ IPv6 thật sự cần thiết cho các kết nối tới 6Bone và tuân theo các kế hoạch phân bổ địa chỉ của tổ chức đó.

- Giá thành khởi điểm thấp. Vì không cần chuẩn bị cần thiết để nâng cấp các hệ thống từ IPv4 sang IPv6 khi triển khai một hệ thống IPv6 mới. Cơ chế này được thực hiện hoàn toàn trên nền IPv4 đã có.

Cơ chế chuyển đổi của IPv6 là có thể kết hợp các trạm IPv6 cùng làm việc với các trạm IPv4 ở bất kỳ nơi nào trên Internet cho đến khi địa chỉ IPv4 không còn tồn tại, và cho phép các trạm IPv6 và IPv4 trong một không gian giới hạn để cùng làm việc sau đó. Các cơ chế này bảo đảm khoản đầu tư to lớn của người dùng trong việc xây dựng hệ thống mạng IPv4 đồng thời triển khai được mạng IPv6.

Hiện nay số lượng các mạng IPv4 là rất lớn, hầu hết các dịch vụ và các giao dịch trên mạng đều dựa trên hạ tầng mạng IPv4. Do vậy xuất hiện nhiều cơ chế chuyển đổi cho phép kết nối các host IPv6 qua mạng IPv4.

Việc xây dựng lại các giao thức của tầng Internet trong mô hình TCP/IP đã dẫn đến nhiều thay đổi. Trong đó vấn đề thay đổi lớn nhất của IPv6 với IPv4 là việc thay đổi cấu trúc địa chỉ. Sự thay đổi này ảnh hưởng đến các vấn đề sau:

- Ảnh hưởng tới hoạt động của các giao thức ở tầng trên (tầng giao vận và tầng ứng dụng).
- Ảnh hưởng tới các phương thức định tuyến.

Mặt khác, một yêu cầu quan trọng trong việc triển khai IPv6 là phải thực hiện được mục tiêu ban đầu đề ra khi thiết kế giao thức IPv6 đó là: IPv6 phải làm việc được trong môi trường sử dụng giao thức IPv4. Sẽ có hiện tượng chỉ có những host dùng duy nhất IPv6 và đồng thời cũng tồn tại những host chỉ duy nhất có IPv4. Đồng thời những host “thuần” IPv6 đó phải giao tiếp được

với những host IPv4 trong khi đó vẫn đảm bảo địa chỉ IPv4 là có tính thống nhất toàn cầu. Do vậy, để đảm bảo thực hiện các sự tương thích giữa IPv4 và IPv6, các nhà thiết kế IPv6 đã xây dựng một số cơ chế chuyển đổi khác nhau.

Các cơ chế chuyển đổi này có những đặc điểm chung như sau:

- Đảm bảo các host/router cài đặt IPv6 có thể làm việc được với nhau trên nền IPv4.
- Hỗ trợ các khả năng triển khai các host và router hoạt động trên nền IPv6 với mục tiêu thay thế dần các host đang hoạt động IPv4.
- Có một phương thức chuyển đổi dễ dàng, thực hiện được ở các cấp độ khác nhau từ phía người dùng cuối tới người quản trị hệ thống, các nhà quản lý mạng và cung cấp dịch vụ.

Các cơ chế này là một tập các giao thức thực hiện đối với các host và các router, kèm theo là các phương thức như gán địa chỉ và triển khai, thiết kế để làm quá trình chuyển đổi sang IPv6 làm việc với ít rủi ro nhất có thể được.

Hiện nay các nhà thiết kế IPv6 đã đưa ra 3 cơ chế chuyển đổi chính cho phép kết nối IPv6 trên nền IPv4 như sau:

- Dual IPv6 layer: Cơ chế này đảm bảo một host/router được cài đặt cả 2 stack IPv4 và IPv6 ở tầng Internet Layer trong kiến trúc TCP/IPv6 của nó.
- IPv6 tunnel qua IPv4: Cơ chế này thực hiện đóng gói một tin IPv6 theo chuẩn giao thức IPv4 để có thể mang gói tin đó trên nền kiến trúc IPv4. Có 2 loại tunneling là cài đặt sẵn (configured) và tự động (automatic).
- 6to4: Cơ chế này hoạt động dựa trên các host IPv4 đã sẵn có các địa chỉ IPv4 từ đó xây dựng một địa chỉ IPv6 có cấu trúc đặc biệt, các host sử dụng cơ chế này không cần phải thông qua một ISP có hỗ trợ IPv6.

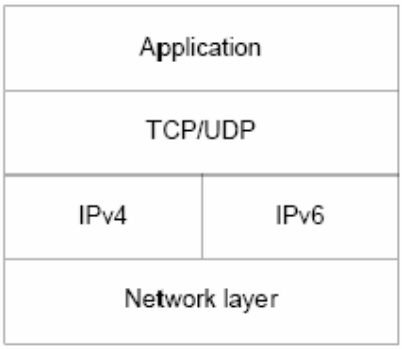
## 4.2. Cơ chế Dual-Layer.

### 4.2.1. Mô tả.

Dual IP layer: cơ chế này đảm bảo mỗi host/router được cài đặt cả hai giao thức IPv4 và IPv6. Với cơ chế "đôi" này, hoạt động của các host/router hoàn toàn tương thích với IPv4 và IPv6.

Theo cơ chế này, IPv6 sẽ cùng tồn tại với IPv4 và nó sẽ dùng cơ sở hạ tầng của IPv4. Sự lựa chọn để sử dụng stack (lựa chọn giao thức nào trong tầng Internet) sẽ dựa vào thông tin được cung cấp bởi dịch vụ named qua DNS server.

Hình 4.1 minh họa cơ chế này. Đây là cơ chế được coi là "thẳng hướng" nhất để đảm bảo một nodes IPv6 hoàn toàn tương thích với những nodes IPv4 khác. Những node vừa hỗ trợ IPv6 vừa hỗ trợ IPv4 như vậy, gọi là IPv4/IPv6. Những node này có khả năng vừa nhận vừa gửi cả những gói tin IPv4 và IPv6.




Hình 4.1. Cơ chế dual IP layer.

Chúng có thể làm việc trực tiếp IPv4 sử dụng giao thức IPv4 đồng thời vừa có thể trực tiếp làm việc với với các host "thuần" IPv6 qua giao thức IPv6. Hạn chế của mô hình Dual-Stack là phải gán thêm một địa chỉ IPv4 đối với mỗi node IPv6 mới.

Đối với mỗi host sử dụng kỹ thuật dual IP layer, có kết hợp với cơ chế chuyển đổi IPv6-over-IPv4 tunneling (cơ chế này sẽ trình bày dưới đây). Đối với những node này, có thể sử dụng kết hợp với các cơ chế tunneling tự động hoặc tunneling cài sẵn, hoặc cả hai kỹ thuật tunneling này. Do đó có thể có 3 cơ chế chuyển đổi đối với mỗi node IPv4/IPv6 là:

- Node IPv4/IPv6 không kết hợp sử dụng kỹ thuật tunneling.
- Node IPv4/IPv6 sử dụng kết hợp tunneling cài sẵn.

- Node IPv4/IPv6 sử dụng kết hợp cả tunneling cài sẵn và tunneling tự động.

Để triển khai trong mạng LAN, người ta thường vận dụng mô hình Dual-Stack "hạn chế". Mô hình Dual-Stack "hạn chế" được mô tả như sau: Một site khi thiết kế theo mô hình Dual-Stack chỉ có những node làm "server" là các node "Dual-Stack". Những node đóng vai trò Client chỉ là những node "thuần" IPv6. Node server đóng vai trò là điểm cung cấp các dịch vụ như DNS, Web, file sharing…Với phương thức này, chỉ có 1 địa chỉ IPv4 được gán cho server; giảm thiểu các địa chỉ IPv4 gán cho các node trong site.

Đối với một host/router khi hỗ trợ cả dual-Stack IP song song cần phải điều khiển hai bộ địa chỉ khác nhau. Nhưng các giao thức Automatic Neighbour Discovery của IPv4 làm cho Stack này là trong suốt đối với nhà quản lý.

Việc nâng cấp router để hỗ trợ IPv6 phức tạp hơn. Các router phải được trang bị mã để forward các gói IPv6, trang bị các giao thức định tuyến IPv6 và giao thức quản lý IPv6.

Cơ chế Dual-Stack dựa vào dịch vụ name service. Các máy chủ Dual-Stack sẽ có các bản ghi địa chỉ khai báo trong DNS server, do vậy DNS server này phải hỗ trợ IPv6. Một bản ghi A tương đương một địa chỉ IPv4 và một bản ghi AAA tương đương địa chỉ IPv6. Một giao diện (lập trình) GHN hiện tại, cho phép các ứng dụng nhận được địa chỉ IPv4 tương ứng với một domainame, sẽ được thay thế bởi một giao diện mới HNA. GHN được gọi với chỉ một lệnh là tên của đích.

HNA được gọi với hai lệnh là địa chỉ đích và quan hệ địa chỉ, hoặc là AF-INET cho địa chỉ IPv4, hoặc là AF-INT6 cho địa chỉ IPv6.

Nếu AF-INET thì thủ tục sẽ chuyển một địa chỉ của bản ghi A có trong đích của DNS. Nếu AF-INT6 thì thủ tục trước hết sẽ query DNS cho bản ghi AAA. Nếu query được thì thủ tục lại quay lại từ đầu. Nếu không tìm thấy thủ tục sẽ query DNS một lần nữa, lần này là hỏi cho địa chỉ đích IPv4. Nó sẽ dùng CIA này như một địa chỉ IPv6 được map bởi IPv4.

Các máy chủ Dual-Stack sẽ sử dụng các giao thức lookup ngược mới. Chúng sẽ nhặt ra các địa chỉ tốt nhất ngoài danh sách được trả về và sử dụng các địa chỉ này trong yêu cầu kết nối TCP hoặc coi như là các địa chỉ đích cho các datagram UDP. Các giao thức vận chuyển Dual-Stack sẽ quyết định hoặc là sử dụng IPv6 nếu như các địa chỉ IPv6 và chuyển đổi vào DNS. Sự chuyển tiếp (IPv4 sang IPv6) sẽ xảy ra một cách ngạc nhiên, ngày càng nhiều connecsion sử dụng IPv6. Sẽ không có bất kỳ một ngày nào mà việc thay thế này trở nên rõ nét tuy nhiên cuối cùng việc thay thế này sẽ bao phủ toàn bộ.

Các thủ tục DNS là trong suốt đối với nội dung của bản ghi. Chỉ những server và giao diện nào mà cần cung cấp hoặc truy nhập tới địa chỉ IPv6 mới phải được nâng cấp.

Việc trang bị cho cac server này sẽ là một phần của việc trang bị IPv6 cho các tổ chức mạng này. Nhưng chúng ta phải đảm bảo rằng các version mới phải hoạt động được, để có thể kết nối được IPv6. Các ứng dụng được nâng cấp sẽ tìm các địa chỉ trong DNS sẽ cố gắng để thiết lập kết nối TCP tới các địa chỉ này. Các kết nối này sẽ bắt đầu được cung cấp cấu trúc overlay trên internet và được xây dựng trên các đường ngầm kết nối giữa các ốc đảo.

### 4.2.2. Phương pháp thực hiện.

Qua phần phân tích trên ta thấy các thông số chính để thực hiên cơ chế Dual - stack được mô tả trong bảng 4.1.

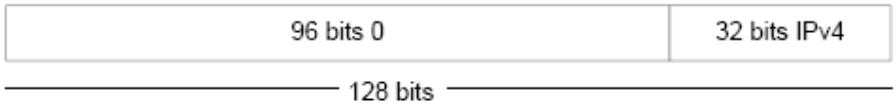
Bảng 4.1. Các tham số của cơ chế Dual-Stack

| Thông số | Giá trị |
|---|---|
| Phạm vi áp dụng | Site |
| Địa chỉ IPv4 cần gán | Một địa chỉ đối với 1 host, nhiều địa chỉ đối với router |
| Địa chỉ IPv4 yêu cầu | Một địa chỉ IPv6 đối với 1 host, nhiều địa chỉ đối với router |
| Yêu cầu đối với host | Cài đặt cả IPv4/IPv6 |
| Yêu cầu đối với router | Cài đặt cả IPv4/IPv6, các giao thức định tuyến phải hỗ trợ IPv6 |

### 4.2.3. Yêu cầu về gán địa chỉ :

Vì các host này sử dụng cả 2 giao thức ở tầng IP là IPv4 và IPv6, do vậy cần gán cả 2 loại địa chỉ IPv4 và IPv6 ở mỗi host này. Không nhất thiết phải có sự quan hệ giữa hai địa chỉ này. Do vậy, những host IPv4 /IPv6 có thể gán những địa chỉ IPv4 và IPv6 không có quan hệ với nhau.

Đối với những nodes có cơ chế chuyển đổi này kết hợp với kỹ thuật tunneling tự động cần phải gán một địa chỉ IPv6 được tạo bởi địa chỉ IPv4 gán đối với host đó. (Địa chỉ IPv6 này gọi là IPv4 – compatible IPv6). Cấu trúc của địa chỉ này như sau :




Hình 4.2. Cấu trúc địa chỉ IPv4-compatible IPv6.

Đối với những nodes IPv4 /IPv6, có thể có được địa chỉ IPv4 theo bất kỳ một giao thức cấu hình địa chỉ IPv4 nào hợp lệ. Ví dụ sử dụng qua các giao thức cấp địa chỉ động như DHCP, BOOTP, RARP; hoặc gán trực tiếp các địa chỉ IPv4 tĩnh.

Đối với địa chỉ loopback: Theo cấu hình địa chỉ IPv4, địa chỉ loopblack có dạng 127.0.0.1; địa chỉ này chuyển sang dạng địa chỉ IPv6 tương thích với IPv4 sẽ có dạng :: 127.0.0.1; đây được coi là dạng địa chỉ IPv6 tương thích với IPv6. Những packet có địa chỉ loopblack sẽ tồn tại trong node đó mà không chuyển ra mạng.

**4.2.4. Khai báo DNS :**

Trong một hệ thống có cài đặt các node hỗ trợ cơ chế dual – stack thì điều kiện tối thiểu cần thiết là dịch vụ DNS của hệ thống đó phải hỗ trợ IPv6 (Hiện nay đã có một số phần mềm như BIND 8.2 hỗ trợ IPv6 ).

Đối với các nodes IPv4 /IPv6 cần phải khai báo cả 2 loại bản ghi trong DNS server. Hay nói cách khác là cần phải cấu hình DNS đối với cả 2 loại địa chỉ mà host đó được gán. Đối với mỗi địa chỉ IPv6, cấu trúc bản ghi DNS có dạng AAAA (Đặc tả về cấu trúc các loại bản ghi hỗ trợ IPv6 đối với dịch vụ DNS được mô tả trong RFC 1886). Đối với mỗi địa chỉ IPv4, cấu trúc bản ghi DNS có dạng A.

Khi dùng địa chỉ IPv4 – compatible IPv6 được gán với các host IPv4/IPv6 ( những host này sử dụng kỹ thuật automatic tunneling ), cả 2 loại bản ghi A và AAAA phải được cấu hình trong DNS. Bản ghi AAAA phải khai báo dạng đầy đủ địa chỉ IPv4 –compatible IPv6, trong khi đó bản ghi A sẽ sử dụng 32 bits thấp trong địa chỉ này.

Khi thực hiện lookup đối với các host IPv6 /IPv4 có thể tìm thấy 2 loại bản ghi A và AAAA. Mỗi bản ghi này có thể trỏ đến mỗi địa chỉ IPv4 hoặc

IPv6. Trong trường hợp kết quả tìm thấy là một bản ghi AAAA trỏ đến một địa chỉ IPv4 –compatible IPv6, và một bản ghi A trỏ đến địa chỉ IPv4 tương ứng thì kết quả trả về có thể có các giá trị sau:

- Trả lại duy nhất địa chỉ IPv6
- Trả lại duy nhất địa chỉ IPv4
- Trả lại cả 2 địa chỉ IPv4 và IPv6

Lựa chọn loại địa chỉ nào được trả về phụ thuộc vào tuỳ từng trường hợp;trong trường hợp cả 2 loại địa chỉ được trả về thì trật tự sắp xếp các loại địa chỉ liên quan đến luồng IP đối với host đó. Nếu một địa chỉ IPv6 được trả về, node đó giao tiếp với node đích trong đó các gói tinh được đóng gói theo chuẩn IPv6. Nếu địa chỉ IPv4 được trả về thì node đó giao tiếp với một host IPv4.

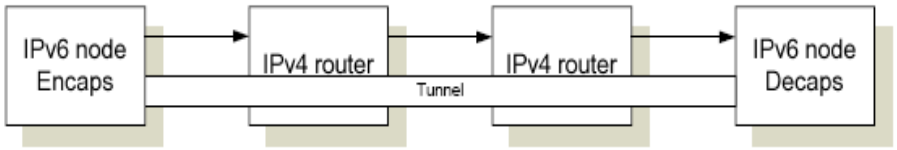
## 4.3. Cơ chế Tunneling

### 4.3.1. Đặc điểm chung.

Cơ sở hạ tâng mạng Internet hoạt động trên nền IPv4 hoạt động khá ổn định và có quy mô rộng lớn. Tận dụng khả năng này, các nhà thiết kế IPv6 đã đưa ra giải pháp là thực hiện cơ chế tunneling (đường hầm) trên nền IPv4. Có 2 loại tunneling là Automatic Tunneling và Configured Tunneling. Trước khi trình bày về đặc điểm của các cơ chế tunneling, sau đây sẽ mô tả một số khái niệm liên quan đến quá trình tunneling.

- IPv4 –only node: là một host hay router hoạt động trên nền IPv4, những host hoặc router này không hiểu IPv6, các host này chiếm phần lớn các thiết bị trên mạng Internet hiện nay, gọi là các node thuần IPv4.
- IPv6/IPv4 node: là các node có khả năng thực hiện trên nền IPv4 hoặc IPv6 và gọi đó là các node đôi.

- IPv6 –only node: là các node chỉ có khả năng hoạt động trên nền IPv6, không có khả năng thực hiện trên nền IPv4 và gọi đó là các node thuần IPv6.
- IPv6 node: node thuần IPv6 và node đôi IPv6/IPv4.
- IPv4 node: node thuần IPv4 và node đôi IPv6/IPv4
- IPv4- compatible IPv6 address: là một địa chỉ IPv6, được gán cho các node đôi IPv6/IPv4 và gọi địa chỉ IPv6 loại này là địa chỉ IPv6 tương thích IPv4. Địa chỉ loại này được sử dụng trong cơ chế tunnel IPv6 trên nền IPv4.
- IPv6-only address: là những địa chỉ IPv6 còn lại.
- IPv6-over-IPv4 tunnelling: kỹ thuật này thực hiện việc đóng gói các datagram theo cấu trúc IPv6 vào phần dữ liệu của datagram IPv4 để có thể mang các gói tin IPv6 qua mạng IPv4, gọi cơ chế này là tunnel IPv6 trên nền IPv4.
- Automatic Tunneling: theo phương thức này, địa chỉ cuối cùng có tunnel là địa chỉ IPv6 tương thích với địa chỉ IPv4.
- Configured Tunneling: theo phương thức này, địa chỉ cuối cùng có tunnel được xác định nhờ thông tin cấu hình tại node đóng gói.




Hình 4.3. Cơ chế tunneling.

Hình 4.3 minh hoạ cơ chế Tunneling. Cơ chế Tunneling được mô tả như sau: các node IPv6/IPv4 sẽ thực hiện đóng gói các datagram IPv6 vào thành phần dữ liệu trong datagram IPv4 (phần tải trọng của gói tin IPv4

truyền trên mạng là gói tin IPv6) và do đó, gói tin này sẽ có thể truyền trên nền IPv4.

Các kết nối có thể áp dụng cơ chế tunneling là:

- Router-to-router: các router IPv6/IPv4 kết nối với nhau bởi cơ sở hạ tầng IPv4, do đó có thể thực hiện chuyển các datagram IPv6 qua cơ chế tunnel. Trong trường hợp này, cơ chế tunnel trải rộng từ điểm bắt đầu tới điểm kết thúc của một gói tin IPv6.
- Host-to-router: một host đôi IPv6/IPv4 có thể thực hiện tunnel IPv6 trên nền IPv4 để chuyển các gói tin tới các router trung gian cũng được cấu hình là các node đôi IPv6/IPv4. Trong trường hợp này, cơ chế tunnel trải rộng trong phạm vi từ host tới router đó.
- Host-to-host: hai host đôi IPv6/IPv4 có thể truyền các datagram theo định dạng IPv6 trên nền IPv4. Trong trường hợp này, cơ chế tunnel trải rộng từ điểm đầu đến điểm cuối.

Kỹ thuật tunnel được phân loại  dựa trên nguyên tắc sử dụng phương thức nào để quyết định địa chỉ của node cuối cùng được cấu hình tunnel. Trong hai phương thức tunnel là Router-to-router và Host-to-router gói tin IPv6 được tunnel đến địa chỉ cuối cùng là tại router. Do đó, điểm cuối cùng của quá trình tunnel này là các router trung gian, tại các router này phải có nhiệm vụ "mở gói tin" được tunnel và chuyển nó tới đích cuối cùng. Địa chỉ trong gói tin IPv6 được tunnel, không hỗ trợ địa chỉ IPv4 của điểm cuối cùng tunnel, thay vào đó, địa chỉ điểm cuối cùng tunnel phải được quyết định từ các thông tin cấu hình trên node thực hiện đóng gói. Theo cơ chế xác định địa chỉ cuối như vậy, ta gọi là "Configured Tunneling", có nghĩa là địa chỉ điểm cuối của quá trình tunnel đã được khai báo trước.

Theo hai phương thức host-to-host và host-to-router, gói tin IPv6 được tunnel trên tất cả hành trình của chúng, cho tới khi đến được đích. Theo cơ chế này, node cuối cùng được xác định tunnel là địa chỉ đích của gói tin IPv6. Vì vậy, điểm cuối cùng của tunnel có thể được quyết định từ địa chỉ đích của gói tin IPv6. Nếu địa chỉ này là một địa chỉ tương đương với địa chỉ IPv4 thì theo cấu trúc của địa chỉ này 32 bit thấp sẽ được lấy làm địa chỉ của node đích và được sử dụng làm địa chỉ đích của node cuối cùng được tunnel. Kỹ thuật này tránh được việc phải khai báo trước địa chỉ đích của node cuối cùng tunnel, gọi là "automatic tunneling".

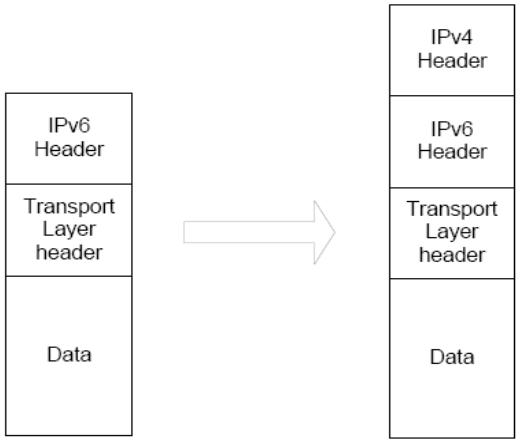
Cả hai kỹ thuật automatic tunneling và configured tunneling có khác nhau cơ bản nhất là việc quyết định địa chỉ cuối của quá trình tunnel, còn lại về cơ bản hoạt động của hai cơ chế này giống nhau. Cụ thể như sau:

- Điểm khởi tạo tunnel (điểm đóng gói tin) tạo một header IPv4 đóng gói và truyền gói tin đã được đóng gói.
- Node kết thúc của quá trình tunnel (điểm mở gói tin) nhận được gói tin đóng gói, xoá bỏ phần header IPv4, sửa đổi một số trường của header IPv6 và xử lý phần dữ liệu này như một gói tin IPv6.
- Node đóng gói cần duy trì các thông tin về trạng thái của mỗi quá trình tunnel, ví dụ các tham số MTU để xử lý các gói tin IPv6 bắt đầu thực hiện tunnel. Vì số lượng các tiến trình tunnel có thể tăng lên một số lượng khá lớn, trong khi đó các thông tin này thường lặp lại và do đó có thể sử dụng kỹ thuật cache và được loại bỏ khi cần thiết.

### 4.3.2. Cơ chế đóng gói thực hiện tunneling.

Hình 4.4 minh hoạ cơ chế đóng gói thực hiện tunnel.

Cấu trúc của phần header packet IPv4 khi thực hiện tunneling (đóng gói IPv6 packet trong một datagram IPv4) được trình bày ở bảng 4.2.




Hình 4.4. Cơ chế đóng gói thực hiện tunnel.

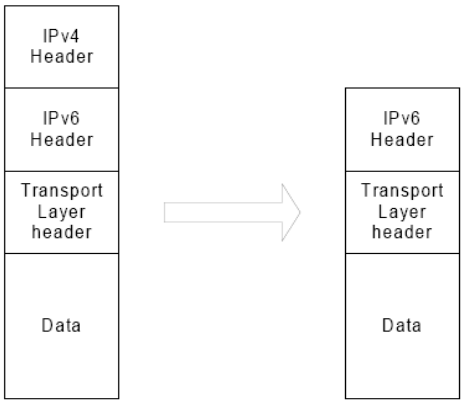
Bảng 4.2. Cấu trúc của phần header IPv4 khi thực hiện tunneling.

| Tham số | Giá trị (bit) | Ý nghĩa |
|---|---|---|
| Version | 4 | Giao thức sử dụng là IPv4 |
| IP header length | 5 | Chiều dài tối đa của trường này là 32 bit. Đối với các gói tin IPv4 đóng gói không thiết lập giá trị cho phần option trong header. |
| Type of service | 0 | |
| Total Length | 60 bytes | Xác định độ lớn gồm chiều dài phần header IPv6 + chiều dài của IPv6 + chiều dài IPv4 header. |
| Identification | | Giá trị được xác định thống nhất cho bất kỳ gói tin IPv4 được truyền bởi hệ thống. |
| Flags | DF hoặc MF | |

| | | |
|---|---|---|
| Time to live | | |
| Protocol | 41 | Gán tương ứng với loại payload trong gói tin IPv6 đóng gói |
| Header Checksum | | Giá trị tổng các byte của phần header IPv4 để kiểm tra tính toàn vẹn dữ liệu khi nhận ở địa chỉ đích. |
| Source Address | IPv4 address | Địa chỉ IPv4 của trạm nguồn |
| Destination Address | IPv4 address | Địa chỉ IPv4 của trạm đích |

### 4.3.3. Cơ chế mở gói khi thực hiện tunnel IPv6-over-IPv4.

Khi một host hay một router nhận được một datagram IPv4 có kiểu giao thức là 41 nó sẽ bỏ phần header IPv4 trong gói tin và giữ lại phần data, đó chính là gói tin IPv6. Hình 4.5 minh họa cơ chế mở gói.




Hình 4.5. Cơ chế mở gói IPv4 khi thực hiện tunnel.

Chú ý là khi thực hiện mở gói tin IPv6 (IPv6–in-IPv4), phần header của IPv6 không bị biến đổi. Nếu đó là gói tin đến đích cuối cùng, giá trị trong

trường hop-limit sẽ bị giảm xuống một giá trị. Phần header IPv4 đóng gói bị loại bỏ. Các node thực hiện mở gói sẽ thực hiện việc tái hợp các datagram IPv4 trước khi nó thực hiện mở gói IPv6. Do vậy, tất cả các giá trị option IPv6 vẫn được giữ nguyên như trước khi đóng gói.

Sau khi thực hiện việc mở gói, mọi quá trình xử lý giống với việc nhận một datagram IPv6 thông thường khác.

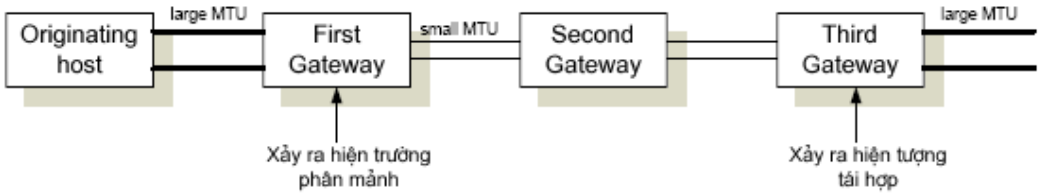
Để đảm bảo tính tương thích giữa IPv6 và IPv4, cần phải có cơ chế chuyển đổi đối với những thay đổi của IPv6 so với IPv4 mà cụ thể là phần header của các datagram và phần thay đổi địa chỉ của IPv6. Các phương thức chuyển đổi địa chỉ đảm bảo thực hiện được các nhiệm vụ chính như sau:

- Đảm bảo các host hoạt động trên nền IPv4 và IPv6 hoàn toàn làm việc được với nhau.
- Hỗ trợ các khả năng triển khai các host và router hoạt động trên nền IPv6 với mục tiêu thay thế dần các host đang hoạt động IPv4.
- Có một phương thức chuyển đổi dễ dàng, thực hiện được ở các cấp độ khác nhau từ phía người dùng cuối tới nhà quản trị hệ thống, các nhà quản lý mạng và cung cấp dịch vụ.
- IPv6 tunnel qua IPv4: cơ chế này đóng gói một gói tin IPv6 vào trong phần header của IPv4 để có thể mang gói tin đó trên nền kiến trúc IPv4. Có hai loại tunnel: cấu hình sẵn và tự động.

### 4.3.4. Lựa chọn giá trị MTU và phân mảnh.

Giá trị giới hạn kích thước gói tin trong tầng Datalink của giao thức TCP/IPv6 gọi là MTU (Maximum Transfer Unit). Đối với mỗi giao thức trên tầng Datalink khác nhau có một giá trị MTU khác nhau. Ví dụ giá trị MTU của Ethernet là 1518 octet. Do có nhiều phương thức khác nhau đối với các

luồng traffic trong mạng Internet nên sẽ xảy ra hiện tượng các giá trị MTU tại các điểm gateway nhỏ hơn giá trị MTU của các




Hình 4.6. Phân mảnh và tái hợp gói tin.

mạng trong. Do vậy sẽ xảy ra hiện tượng phân mảnh tại các điểm gateway. Sau đó sẽ xảy ra hiện tượng tái hợp ở các điểm đích. Hình 4.6 minh họa cơ chế này.

Đối với giao thức IPv4 giá trị MTU chỉ là 576 bytes, giá trị này có thể nhỏ hơn giá trị của một gói tin IPv6. Như vậy ở các node entry-point khi thực hiện đóng gói các gói tin IPv6 sẽ phải kiểm tra gói tin IPv6 mà nó đóng gói có vượt qua giá trị MTU cho phép hay không. Nếu vượt quá thì phải thực hiện phân mảnh gói tin IPv6. Việc phân mảnh này dẫn đến các hiện tượng sau:

- Ở phía nhận sẽ nhận được rất nhiều các mảnh nhỏ được tách ra từ gói lớn. Nó sẽ phải mất nhiều thời gian và bộ nhớ để tái hợp các gói tin phân mảnh trước khi mở gói.
- Trong trường hợp một gói tin phân mảnh bị mất, các gói tin còn lại sẽ chiếm mất không gian bộ đệm cho đến khi vượt quá giá trị TTL mới bị huỷ. Toàn bộ IPv6 lúc này bị mất và phải truyền lại. Tóm lại, việc tách gói sẽ chỉ là có hại cho tunnel giữa các máy chủ.

Như vậy việc thực hiện phân mảnh gói tin là không hiệu quả. Để xác định giá trị MTU hợp lý người ta đã xây dựng giao thức MTU Discovery Protocol. Có thể mô tả tóm tắt thuật toán chọn lựa giá trị MTU này như sau:

- Nếu gói tin IPv6 cần đóng gói có kích thước lớn hơn 576 bytes thì ở node entry-point trả về một thông báo ICMPtheo chuẩn IPv6 và node nguồn của gói tin IPv6 đó. Thông báo ICMP có nội dung cảnh báo là kích cỡ gói tin lớn hơn mức cho phép (packet too big). Giá trị MTU hợp lệ là 576 bytes và ở điểm entry tunnel sẽ huỷ gói tin yêu cầu tunneling.
- Nếu gói tin IPv6 cần đóng gói có kích cỡ nhỏ hơn 576 bytes sẽ thực hiện đóng gói và giá trị của trường flag fragmention trong phần header IPv4 được thiết lập bằng không (không phân mảnh).

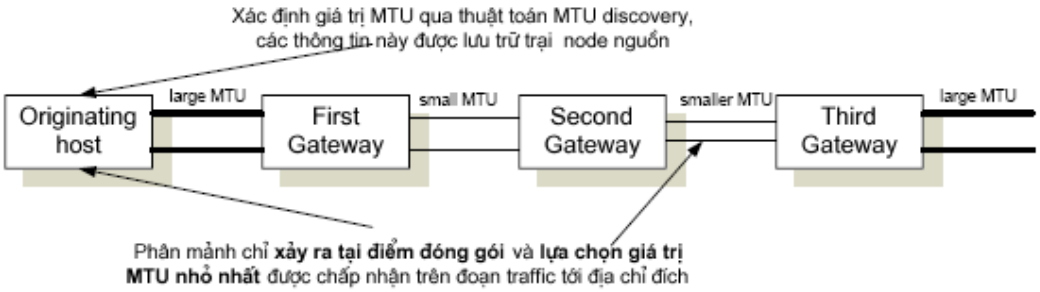
Để giảm được việc phải phân nhỏ gói tới mức nhỏ nhất, router ở hai đầu tunnel thực hiện tìm kiếm giá trị MTU được coi là hợp lý nhất. Chúng sẽ bắt đầu từ MTU của tunnel tới MTU của giao diện cục bộ của chúng. Nếu như các message ICMP trở lại để chỉ rằng gói là quá lớn, chúng sẽ chuyển tới một MTU thấp hơn. Trong vài trường hợp chúng có thể gửi một message thử để khám phá khả năng tăng trong MTU. Khi MTU của tunnel vẫn còn lớn hơn kích thước gói nhỏ nhất mà IPv6 hỗ trợ (5760 octet) thì việc phân nhỏ gói IPv4 sẽ được tắt đi trong IPv4 header. Nếu như gói IPv6 lớn hơn MTU của tunnel có trong giao diện thì nó sẽ bị loại bỏ và message ICMP “IPv6 packet too big” sẽ được gửi lại cho khách hàng.

Nhưng kích thước nhỏ nhất của gói IPv4 chỉ là 48 octet chứ không phải là 576. MTU của tunnel có thể ít khi nhỏ hơn 576 octet, điều mà buộc các router IPv6 sử dụng việc phân nhỏ gói IPv4.

Nếu MTU của tunnel IPv4 nhỏ hơn 576 octet. Các gói IPv6 lớn hơn 576 octet sẽ bị loại bỏ và message “packet too big” sẽ được gửi trở lại cho người gửi IPv6. Gói này sẽ chỉ ra một MTU IPv6 cực đại của 576 octet.

Nếu một gói IPv6 lớn hơn MTU của tunnel nhưng lại nhỏ hơn 576 thì việc phân nhỏ gói sẽ không thể được dùng.

Hình 4.7 minh họa giao thức MTU discovery được hỗ trợ trong IPv6.




Hình 4.7. Giao thức MTU discovery.

### 4.3.5. Các giao thức tunnel và routing.

Khi tunnel được cấu hình, chúng sẽ được đối xử như nhiều loại đường link khác trong toàn bộ cơ sở hạ tầng IPv6. Nếu như tunnel được sử dụng cho đường nối giữa các domain định tuyến tách biệt nhau, nó sẽ sử dụng cho việc trao đổi giữa các router, sử dụng IDRP. Nếu như tunnel bị đưa vào định tuyến, nó sẽ được xem xét như là một đường link serial thuần tuý bằng các giao thức routing như là RIP hoặc OSPF.

Nhưng các tunnel đều không phải thuần là các link. Trong trường hợp của RIP, toàn bộ số liệu là số lượng host. Ngầm định giá của tunnel đặt là 1, như là một đường kết nối trực tiếp giữa 2 router mặc dù là các gói qua tunnel trong thực tế được chuyển tiếp qua vài lần bởi các lớp IPv4. Đó có thể là do kết quả của các lựa chọn khác, giống như các lựa chọn cho việc định tuyến thông qua một tunnel dài thay vì chuyển tiếp qua một số lượng nhỏ các kết nối IPv6 trực tiếp.

### 4.3.6. Thời gian sống trong tunnel.

Do việc định tuyến IPv4 là động, thời gian sử dụng cho các gói trong tunnel là thay đổi. Các gói nên gửi qua tunnel với 1 TTL IPv4 vừa đủ để đảm bảo rằng chúng không bị timeout. Khi định tuyến các đặc tính hiện tái của cơ

chế chuyển tiếp đã được lược bớt trong điểm này. Do đó, TTL được lựa chọn trong kiểu hoạt động phụ thuộc, với giá trị ngầm định được đề xuất trong RFC 1700.

Thực tế người ta thiết lập TTL này một cách động, giống như chương trình traceroute thực hiện. Việc giám sát TTL của tunnel có thể có ích nếu như người ta muốn khám phá nhanh chóng sự thay đổi trong việc định tuyến IPv4 và cập nhật metric của tunnel.

### 4.3.7. Điều khiển việc chia sẻ tunnel.

Một điểm hạn chế của định tuyến theo lớp là làm hỗn độn việc điều khiển tài nguyên. Các gói được qua tunnel sẽ hoàn thành việc truyền tài nguyên với các gói thuần IPv4. Vấn đề có thể gây ra lỗi trong trường hợp các router IPv4 được sử dụng bởi vì tunnel sẽ chỉ nhận được một phần chia sẻ của tài nguyên của khách hàng đó, mặc dù nó thông tin có trong toàn bộ gói tin IPv6.

Các giải pháp tương tự sẽ được sử dụng cho IPv6 tunnel, nó có một số lợi ích sau:

- Người quản lý có thể điều khiển việc chia sẻ mạng mà được định vị trong IPv6.
- Dải thông tunnel có thể được sử dụng để ấn định metric hiện thực tới tunnel.

Cũng có một số bất lợi tiềm ẩn. Theo định nghĩa, việc ép buộc mã giới hạn tốc độ cho IPv6 tunnel nghĩa là các gói IPv6 sẽ không sử dụng chung được các tài nguyên đang không sử dụng đến như là các gói thuần IPv4. Cũng vì vậy nếu như dải thông tương ứng không được dành riêng có hiệu quả ở mức IPv4 thì chính sách ở mức IPv6 sẽ không được đảm bảo rằng các gói có mức ưu tiên cao nhất là không bị loại bỏ trong tunnel.

Đây là một điều khá rõ ràng. Người ta có thể tưởng tượng ra một giao thức điều khiển tunnel động giám sát dải thông có sẵn cho tunnel trong các luồng IPv6 thời gian thực. Nhưng đó cũng là một vấn đề nguy hiểm bởi vì có nhiều sự tương tác rất phức tạp giữa các phần điều khiển, tốc độ gửi của các gói trong tunnel và khả năng của tunnel. Việc thiết lập một dải thông được định nghĩa trước và buộc nó sử dụng tại mức IPv4 là khá dễ dàng và có thể vững chắc hơn. Việc triển khai nhanh các khả năng nguyên thuỷ của IPv6 có thể sẽ là tốt hơn bởi vì chúng sẽ thoát ra được khỏi tunnel.

### 4.3.8. TTL cho các tunnel tự động.

Các tunnel đã từng nhận các gói tới và từ các host độc lập đã không được cấu hình một cách tường minh. Vì vậy, người ta phải chọn các thông số IPv4 như là TTL hoặc MTU. Trong trường hợp của TTL, các host sẽ dùng các giá trị được khuyến nghị 64 cho RFC1700. Trường hợp của MTU thì phức tạp hơn, thực tế có ba trường hợp:

- Các host độc lập quản lý một tunnel đơn tới một router IPv6 gần nhất.
- Các host qual điều khiển các tunnel tới các partnel độc lập của chúng.
- Các router dual xuyên các gói tới các host độc lập mà thay mặt cho các host thuần IPv6.

Các host độc lập chỉ điều khiển một tunnel. Chúng có thể có giao thức phát hiện MTU. Các host chạy dual cũng nên có khả năng chạy giao thức phát hiện MTU cho tất cả các tunnel hiện tại đang kích hoạt, mặc dù các máy chủ phổ thông không phải trả lời nhiều cho khách hàng tìm ra nó cũng khá khó khăn. Các router dual sẽ sớm đối mặt với rất nhiều các tunnel đang kích hoạt, phải có khả năng tính toán một cách hiệu quả thông số MTU cho mỗi router. Chúng sẽ luôn luôn có lợi khi sử dụng tối thiểu ngầm định của MTU là 576 byte và quản lý được việc phân mảnh IPv4 các router mà thực hiện việc

tunneling có thể nhận được các báo hiệu lỗi khác thường là ICMP. Để tránh các vấn đề này, chúng thường cố gắng chuyển các báo hiệu này trong IPv6 ICMP quay trở lại nguồn IPv6.

Các message ICMP bao gồm byte thứ nhất của gói IPv4, 40 byte tiếp theo sẽ là header IPv6 nguyên thuỷ. Nếu chúng xuất hiện thì router sẽ sử dụng chúng sẽ hồi phục lại địa chỉ nguồn IPv6 nguyên thuỷ nhằm xây dựng một message báo lỗi ICMP IPv6.

## 4. 4. Cơ chế Configure tunneling.

### 4.4.1. Mô tả.

Với phương thức tunnel này, địa chỉ mở gói được quyết định bởi các thông tin được cấu hình ở node đóng gói (entry-point encapsulations). Đối với mỗi tunnel dạng này, các node phải lưu địa chỉ của trạm cuối (trạm mở gói-end point). Khi các gói IPv6 được chuyển qua tunnel này, địa chỉ của các end point được cấu hình sao cho giống với địa chỉ đích trong phần header của gói tin IPv4 đóng gói. Các thông số yêu cầu đối với cơ chế Configure tunneling như sau:

- Khả năng ứng dụng: site.
- Yêu cầu giao thức IPv4: kết nối giữa các site sử dụng IPv4.
- Địa chỉ IPv4: tối thiểu có một địa chỉ IPv4 trong một site.
- Yêu cầu giao thức IPv6: không cần thiết.
- Yêu cầu địa chỉ IPv6: không cần thiết.
- Yêu cầu host: IPv6 stack hoặc IPv4/IPv6 stack.
- Yêu cầu đối với router: IPv4/IPv6 router.

### 4.4.2. Phương pháp thực hiện.

Để quyết định đường đi của các tunneling, hay nói cách khác để có được các thông tin về node cuối cùng cần phải dựa vào bảng định tuyến vì hướng đi của các gói phải dựa vào địa chỉ đích của chúng sử dụng các kỹ thuật netmask.

Default Configured tunneling: giống như ý nghĩa của giá trị Default router trong bảng định tuyến, đối với một tunnel khi thực hiện phương thức Configurđ tunneling nếu nó không tìm thấy địa chỉ đích trong bảng định tuyến, nó sẽ sử dụng một giá trị Default khai trên router đó làm địa chỉ đích trong gói tin đóng gói.

## 4.5. Cơ chế Automatic tunneling.

### 4.5.1. Mô tả.

Với phương thức tunneling này, địa chỉ đích trong gói tin đóng gói IPv4 được xác định là địa chỉ đích của gói tin IPv6. Do vậy địa chỉ đích của gói tin IPv6 được đóng gói phải có dạng địa chỉ IPv4 tương thích với IPv6 (IPv4-compability IPv6). Đối với những gói tin IPv6 mà địa chỉ đích là dạng địa chỉ không có dạng IPv4-compability thì sẽ không thể thực hiện Automatic tunneling.

Cơ chế Automatic tunneling thường được sử dụng khi cần thực hiện những kết nối với các host hoặc với các mạng IPv6 trong một thời gian ngắn, hoặc trong những tình huống ngẫu nhiên.

Các thông số liên quan đến Automatic tunneling:

- Khả năng ứng dụng: đối với các host.
- Yêu cầu giao thức IPv4: yêu cầu có các kết nối IPv4 giữa các site.
- Yêu cầu địa chỉ IPv4: tối thiểu có một địa chỉ IPv4.
- Yêu cầu giao thức IPv6: không cần thiết.
- Yêu cầu địa chỉ IPv6: địa chỉ dạng IPv4-compability

- Yêu cầu host: cài đặt Dual-Stack IPv4/IPv6
- Yêu cầu đối với router: không cần thiết

### 4.5.2. Phương pháp thực hiện.

Đối với những node IPv4/IPv6 có một phương thức để quyết định liệu các gói tin IPv6 có được Automatic tunneling hay không đó là dựa vào các thông số trong bảng định tuyến tĩnh. Đối với các host có địa chỉ đích dạng ::0/96 sẽ được thực hiện tự động định tuyến (vì những host này thoả mãn điều kiện là có địa chỉ đích dạng IPv4-compability).

## 4.6. Cơ chế 6to4.

### 4.6.1. Yêu cầu.

Hiện nay, để triển khai mạng IPv6 tổ chức IGTRANs (IPng Transition Working Group- một nhóm thuộc IETF) đã đưa ra một giải pháp thứ ba để triển khai mạng IPv6 trên nền IPv4 là cơ chế 6to4. Một trong những hạn chế lớn nhất của hai cơ chế trên (cơ chế Dual-Stack và cơ chế tunneling) là với mỗi khách hàng cuối (end-user site) để kết nối với mạng IPv6 (ví dụ 6Bone) đều cần phải lựa chọn một ISP có hỗ trợ dịch vụ IPv6 để giải quyết các vấn đề liên quan đến cấp phát địa chỉ và tunneling…Mặt khác phương thức này cũng hạn chế được những khó khăn của cơ chế tunneling như các hoạt động tạo, quản lý, duy trì các cấu hình tunneling của phương pháp tunneling. Yêu cầu của cơ chế 6to4:

- Một host phải có địa chỉ IPv4.
- Để đảm bảo hoạt động chính xác của 6to4 trong một topo mạng phức tạp, tất cả các host IPv6 phải đảm bảo thuật toán sau đây là có giá trị: đó là thuật toán liên quan đến lựa chọn địa chỉ khi thực hiện gửi gói tin IPv6. Vì một node có thể gán nhiều dạng địa chỉ IPv6 khác nhau. do đó, trong dịch vụ tên miền DNS có thể khai nhiều bản ghi tương ứng với các địa chỉ IPv6

khác nhau của host đó. Thuật toán lựa chọn địa chỉ đảm bảo trong một tập các địa chỉ IPv6 trả về khi host thực hiện query DNS server sẽ lựa chọn một địa chỉ có dạng tiền tố 2002::/16 trong tập các địa chỉ trả về để gửi gói tin IPv6 trong các kết nối của host đó.

**4.6.2. Mô tả.**

Theo cấu trúc của dạng địa chỉ Global Unicast, phần định danh tiền tố TLA được gán bởi tổ chức IANA. Ví dụ tiền tố 3FFE::/16 được gán cho mạng thử nghiệm 6Bone, hay 2001::/16 được phân bổ theo cơ chế production.

Hiện nay tổ chức này cũng gán một tiền tố đặc biệt là 2002::/16 để hỗ trợ cơ chế 6to4. Theo đó cấu trúc địa chỉ IPv6 của một node thực hiện 6to4 có dạng như sau:

| 3 | 13 | 32 | 16 | 64 |
|---|---|---|---|---|
| 001 | 0x0002 | V4ADDR | SLA ID | Interface ID |

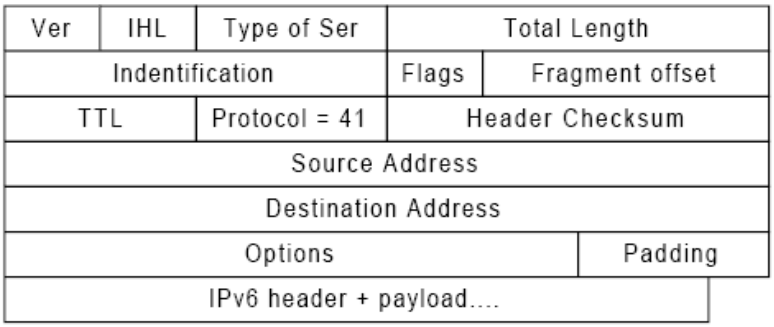
trong đó:

- Phần TLA ID được gán giá trị 0002::/16
- Phần NLA gán 32 bit còn lại là địa chỉ IPv4 của node đó.

Như vậy một node muốn thực hiện cơ chế 6to4 phải có một địa chỉ IPv4 thực (địa chỉ IPv4 này phải có giá trị trên mạng Internet, không phải là địa chỉ của mạng riêng). Cấu trúc dạng địa chỉ này đảm bảo hoàn toàn giống với các định dạng địa chỉ IPv6 Global Unicast thông thường khác.

Gói tin IPv6 trong các site cấu hình 6to4 được đóng gói theo dạng IPv4 (giống cơ chế tunneling-6over4) khi các gói tin này cần chuyển ra mạng ngoài. Sau khi gói tin đóng gói dạng IPv4 sẽ được chuyển trong mạng IPv4 như hoạt động của mạng Internet hiện nay.

Phần header của gói tin IPv4 có địa chỉ đích và địa chỉ nguồn dạng IPv4. Các địa chỉ này có được là dựa vào cơ chế lựa chọn địa chỉ, sau đó thực hiện lấy 32 bit địa chỉ V4ADDR trong cấu trúc địa chỉ IPv6 có tiền tố 2002::/16. Cấu trúc của dạng gói tin IPv4 được mô tả trên hình 4.8.




Hình 4.8. Cấu trúc gói tin IPv4 đóng gói theo cơ chế 6to4.

Trường hợp triển khai đơn giản nhất của cơ chế 6to4 là sử dụng cơ chế này để kết nối các site IPv6 với nhau, các site này kết nối với nhau dựa trên mạng IPv4. Không yêu cầu các site này có các kết nối với cùng một ISP. Chỉ có một yêu cầu là các site được cài đặt IPv6 hỗ trợ cơ chế 6to4 để thiết lập giá trị Protocol=41 trong các gói IPv4.

Để cơ chế này hoạt động, mỗi site còn cần phải gán một địa chỉ IPv6 theo cấu trúc địa chỉ đã mô tả ở trên. Đồng thời tạo một bản ghi DNS tương ứng với địa chỉ này.

Ví dụ: Một site A có địa chỉ IPv4 là 203.162.0.10 sẽ tạo một bản ghi trên DNS với tiền tố IPv6 có dạng: {FP=001, TLA=0x0002, NLA=CBA2:000A}/48.

Một site B có địa chỉ IPv4 là 9.254.253.252 sẽ tạo một bản ghi trên DNS với tiền tố IPv6 có dạng: {FP=001, TLA=0x0002, NLA=09FE:FDFC}/48.

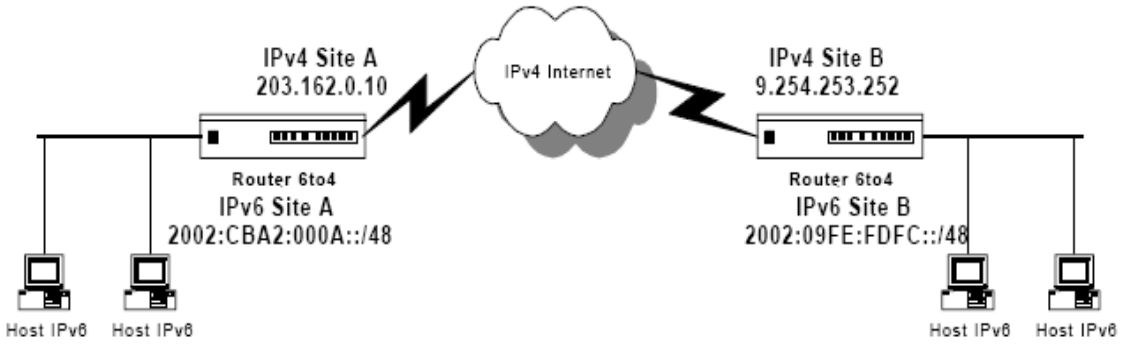
Khi một host IPv6 trên site B cần kết nối với một host IPv6 trên site A, các bước thực hiện như sau:

- Nó thực hiện query tới DNS server để tìm địa chỉ IPv6 của host trên site A. Giả sử địa chỉ mạng trả về là {FP=001, TLA=0x0002, NLA=CBA2:000A}/48. Địa chỉ một host trong site A có dạng tiền tố như trên và một giá trị SLA và Interface ID có dạng bất kỳ.
- Gói tin IPv6 được hình thành và được truyền thông thường bên trong hai site này (từ các host IPv6 đến các router 6to4 được truyền các gói tin thuần IPv6 – không có bất kỳ cơ chế chuyển đổi nào xảy ra ở trong nội bộ một site- các router 6to4 được coi là các router "cận biên").
- Khi các router này nhận thấy địa chỉ đích có phần tiền tố 2002::/16 nó sẽ thực hiện cơ chế gửi như sau:

Đóng gói gói tin IPv6 theo dạng IPv4 với cấu trúc gói tin IPv4, trong đó địa chỉ đích của gói tin IPv4 này được lấy từ 32 bit của trường V4ADDR trong địa chỉ đích IPv6 của gói tin IPv4. Sau đó chuyển gói tin như giao thức IPv4 thông thường qua các giao thức định tuyến của IPv4.

Đối với các router bên site A, sau khi nhận các gói tin IPv4 sẽ thực hiện cơ chế mở gói như sau:

Thực hiện kiểm tra giá trị của trường Protocol trong phần header của gói




Hình 4.9. Cơ chế đóng mở gói.

tin có bằng 41 hay không? Nếu giá trị này bằng 41 sẽ thực hiện bỏ phần header của gói tin IPv4 và lấy phần data của gói tin IPv4 này là một gói tin IPv6. Sau đó chuyển trong local site bằng các giao thức IPv6. Hình 4.9 mô tả hoạt động của quá trình này.

## 4.7. Phương thức lựa chọn các cơ chế.

Đối với những node IPv4/IPv6 phải có phương thức lựa chọn khi nào gửi gói tin IPv4, khi nào gửi gói tin IPv6 và khi nào thực hiện automatic hoặc configured tunneling sử dụng kết hợp với nhau. Các trường hợp có thể xảy ra như sau:

- Gửi gói tin IPv4 tới tất cả các địa chỉ đích IPv4.
- Gửi gói tin IPv6 tới tất cả các địa chỉ đích IPv6 trên cùng một link.
- Sử dụng automatic tunneling: Gửi các gói tin IPv4 đóng gói IPv6 có địa chỉ đích là dạng địa chỉ IPv4-compatible.
- Gửi các gói tin IPv6 ra mạng ngoài mà router trong mạng đó có hỗ trợ IPv6.
- Gửi các gói tin IPv6 ra mạng ngoài sử dụng default tunneling khi không có router hỗ trợ IPv6.

Các thuật toán tương ứng với các trường hợp này như sau:

### 4.7.1. Nếu địa chỉ của node cuối là một địa chỉ IPv4.

Nếu địa chỉ đích được locate trên một attached link thì sẽ gửi gói tin IPv4 tới node cuối.

Nếu địa chỉ đích của node cuối không locate trên link với node nguồn thì hoặc:

- Nếu có một router IPv4 trên link, node nguồn sẽ gửi gói tin dạng IPv4, địa chỉ đích là một dạng địa chỉ IPv4.

- Nếu không, địa chỉ đích sẽ là "unreachable" vì nó không nằm trên link host nguồn và cũng không nằm link với router.

### 4.7.2. Nếu địa chỉ của node cuối là một dạng địa chỉ IPv4-compatible IPv6.

Có các tình huống xảy ra như sau:

Nếu địa chỉ đích được locate trên một attached link, khi đó host nguồn sẽ gửi gói tin dạng IPv6 (không đóng gói). Địa chỉ đích của gói tin IPv6 là địa chỉ Global Unicast của trạm đích.

Nếu trạm đích không locate trên link (phải thông qua router), có các tình huống sau xảy ra:

- Nếu đó là một router IPv4 thì một gói tin IPv6 được đóng gói dạng IPv4 để tunnel qua router. Địa chỉ đích IPv6 là địa chỉ IPv6 của node cuối. Đối với gói tin IPv4 địa chỉ đích là 32 bit thấp của địa chỉ dạng IPv4-compatible IPv6. Địa chỉ datalink là địa chỉ datalink của router IPv4.
- Nếu là một router IPv6 nằm trên đường link, thì gói tin được gửi từ trạm nguồn có dạng gói tin IPv6. Địa chỉ nguồn là một địa chỉ IPv6 của node nhận gói tin. Địa chỉ datalink là địa chỉ IPv6 của router.
- Nếu không, không thể kết nối với trạm đích (unreachable).

### 4.7.3. Nếu node nhận là một node thuần IPv6

Có các tình huống xảy ra như sau:

Nếu node nhận nằm trên link với node gửi, sẽ gửi gói tin dạng IPv6. Địa chỉ đích là địa chỉ IPv6 của node cuối. Địa chỉ datalink là địa chỉ của node cuối.

Nếu node cuối không nằm trên link, có các tình huống sau:

- Nếu có một router IPv6, thì gói tin gửi được định dạng IPv6. Địa chỉ đích IPv6 là địa chỉ của node cuối. Địa chỉ datalink là địa chỉ IPv6 của router.

- Nếu địa chỉ đích có thể có được qua configured tunneling và có một router IPv4 để kết nối ra ngoài thì gói tin gửi sẽ được đóng gói theo IPv4. Địa chỉ đích IPv6 là địa chỉ của node cuối. Địa chỉ đích của gói tin IPv4 là địa chỉ IPv4 của node mở gói. Địa chỉ datalink là địa chỉ IPv4 của router IPv4.
- Nếu không địa chỉ đích không thể kết nối tới (unreachable).

Bảng 4.3. Tóm tắt phương thức lựa chọn cơ chế chuyển đổi.

| Dạng địa chỉ của node đích | Node đích trên link? | Router IPv4 trên link | Router IPv6 trên link | Định dạng gói tin để gửi | Dạng địa chỉ đích IPv6 | Dạng địa chỉ đích IPv4 | Dạng địa chỉ đích datalink |
|---|---|---|---|---|---|---|---|
| IPv4 | Yes | N/A | N/A | IPv4 | N/A | E4 | EL |
| IPv4 | No | Yes | N/A | IPv4 | N/A | E4 | RL |
| IPv4 | No | No | N/A | UNRCH | N/A | N/A | N/A |
| IPv4-compatible | Yes | N/A | N/A | IPv6 | E6 | N/A | EL |
| IPv4-compatible | No | Yes | N/A | IPv6/4 | E6 | E4 | RL |
| IPv4-compatible | No | No | Yes | IPv6 | E6 | N/A | RL |
| IPv4-compatible | No | No | No | UNRCH | N/A | N/A | N/A |
| IPv6-only | Yes | N/A | N/A | IPv6 | E6 | N/A | Electron |
| IPv6 -only | No | N/A | Yes | IPv6 | E6 | N/A | RL |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IPv6 -only | No | Yes | No | IPv6/4 | E6 | T4 | RL |
| IPv6 -only | No | No | No | UNRCH | N/A | N/A | N/A |

Chú thích:

N/A: không có trong thực tế.

E6: Địa chỉ IPv6 của node cuối.

E4: Địa chỉ IPv4 của node cuối.

EL: Địa chỉ datalink của node cuối.

T4: Địa chỉ IPv4 của điểm mở gói trong tunnel.

R6: Địa chỉ IPv6 của router.

R4: Địa chỉ IPv4 của router.

RL: Dạng địa chỉ datalink của router.

IPv4: Định dạng gói tin IPv4.

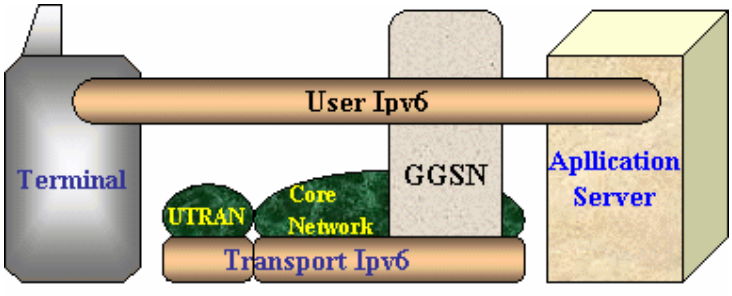
IPv6: Định dạng gói tin IPv6.

IPv6/IPv4: Gói tin IPv6 được đóng gói dưới dạng IPv4.

UNRCH: Gói tin không được gửi (Destination is unreachable)

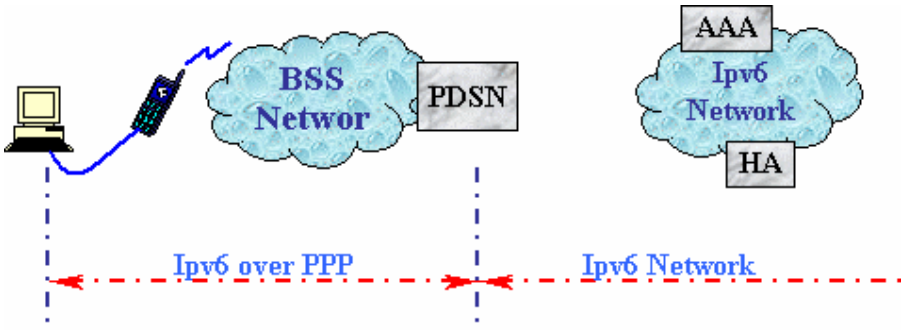
## 4.8. IPv6 và 3G.

Hình 4.10 mô tả IPv6 được ứng dụng trong UMTS như thế nào. Mức truyền tải và mức người sử dụng hoàn toàn độc lập, mạng UTRAN và mạng lõi cũng là hai mạng độc lập, vì vậy việc sử dụng IPv6 có nghĩa bao gồm người sử dụng IPv6, mạng UTRAN IPv6 và mạng lõi IPv6. Các gói IP đến/đi từ thiết bị đầu cuối xuyên qua mạng UMTS, chúng không được định hướng trực tiếp tại mức IP.




Hình 4.10. IPv6 tại các hệ thống viễn thông di động toàn cầu.

Hình 4.11 mô tả cấu hình mạng WCDMA2000 liên kết với mạng IPv6 qua PDSN hỗ trợ IPv6. Kết nối PPP giữa MS và PDSN sẽ vận chuyển gói tin

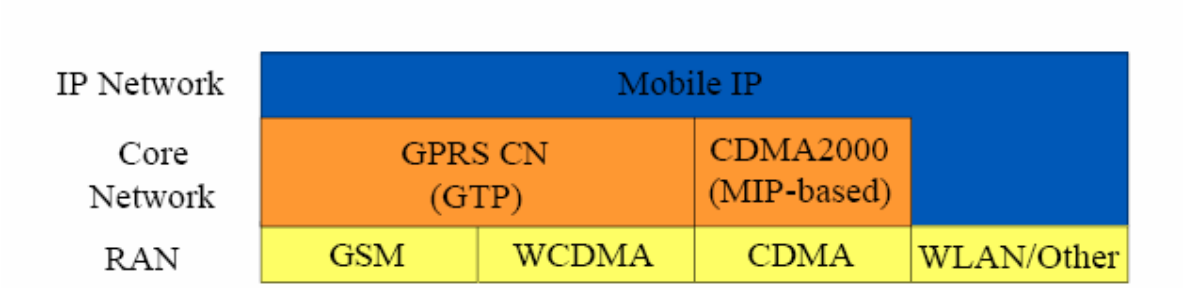



Hình 4.11. Các dịch vụ hỗ trợ IPv6 cho mạng WCDMA2000.

IPv6. Mạng truy nhập vô tuyến (RAN), bao gồm giao diện R-P, sẽ độc lập với phiên bản các gói IP được truyền tải trong các phiên PPP.

Hiện tại, mobile IP (MIP) là giải pháp được chấp nhận cho IP di động. Hiện nay các tiêu chuẩn 3GPP hỗ trợ MIPv4 bằng cách gộp chức năng FA trong GGSN. Do trong IPv6 không có FA, nên MIPv6 không có thêm yêu cầu gì đối với kiến trúc mạng 3GPP. GTP (GPRS Tunneling Protocol) được sử dụng trong mạng 3GPP cho phép di động trong cùng một miền và giữa các công nghệ truy cập khác nhau.

Các đầu cuối 3G hi vọng có khả năng thực hiện một số các giao diện để sử dụng với các mạng truy nhập khác nhau. Ví dụ, ngoài khả năng hỗ trợ các giao diện di động tổ ong, các đầu cuối có thể hỗ trợ các công nghệ vo tuyến khác như Bluetooth, Infra Red…Giả thiết các công nghệ truy nhập này kết nối với các router truy nhập khác nhau, khi đó một địa chỉ IPv6 đầu cuối có thể thay đôi khi di chuyển giữa các môi trường này. Do đó để đảm bảo tính di động liền mạch và duy trì được các kết nối đang diễn ra, có thể sử dụng MIPv6. MIPv6 cũng có thể được sử dụng khi chuyển vùng giữa các mạng




Hình 4.12. Quản lý di động trong các hệ thống vô tuyến IPv6.

3GPP khác nhau, do đó cho phép có thể liên lạc tới một thiết bị theo tuyến tối ưu nhất. Hình 4.12 mô tả việc kết hợp các giao thức quản lý di động khác nhau cho các hệ thống vô tuyến IPv6.

# KẾT LUẬN VÀ KIẾN NGHỊ

Tương lai của Internet di động đòi hỏi giao thức Internet lựa chọn phải cho phép khả năng mở rộng cao và hiệu suất quản lý cao. IPv6 cùng một số tính năng nổi trội làm cho nó trở thành ứng cử viên chính cho môi trường này. Các tính năng này đã dẫn tới quyết định của 3GPP sử dụng IPv6 cho các dịch vụ mới với các phiên bản về sau của UMTS.

Để các nhà khai thác di động động có thể tận dụng được các ưu điểm của IPv6, cần phải xem xét một cách tỉ mỉ khi thực hiện các quyết định như về vấn đề địa chỉ, bảo mật, quản lý di động trong mạng của mình. Để có thể tận dụng được giao diện vô tuyến một cách hiệu quả, các nhà khai thác và thiết kế mạng phải đảm bảo rằng mạng của mình hỗ trợ các cơ chế được xác định trong các cơ quan tiêu chuẩn để phục vụ cho mục đích này. Tại Việt Nam phương pháp phù hợp để chuyển sang IPv6 là nên chọn phương cách một hệ thống dùng song song cả IPv4 và IPv6 thì hợp lý hơn là phải đầu tư cho hai hệ thống một lúc. Về mặt kỹ thuật, việc chuyển sang IPv6 tại Việt Nam không phải là điều khó khăn. Internet ở nước ta mới phát triển và các hệ thống máy móc hầu hết đều được đầu tư mới, mà đa phần những hệ thống thiết bị mới đều có thể hỗ trợ IPv6. Tất cả thiết bị mạng nói chung của các nhà cung cấp dịch vụ Internet tại Việt Nam đều có khả năng hỗ trợ IPv6. Ngay cả các hệ thống đầu cuối như Windows XP của Microsoft cũng có khả năng này.

# TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[1]. Chu Ngọc Anh, Nguyễn Phi Hùng, Phạm Vĩnh Hòa (2003), "IPv6 cho mạng thông tin di động thế hệ mới", *Tài liệu hội nghị khoa học lần thứ năm,* tr.167-176.

[2]. TS.Nguyễn Quý Minh Hiển, TS.Đỗ Kim Bằng (2002), *Mạng viễn thông thế hệ sau*, NXB Bưu điện

**Tiếng Anh**

[3]. B. Carpenter e K. Moore (2001), *Connection of IPv6 Domains via IPv4 Clouds*, RFC3056.

[4] G.De Marco, P.Asprino, A.Fresa, M.Longo (2003), *Developing new generation network services*, IEEE Communication magazine 2003

[5]. J. Bound, L. Toutain, F. Dupont, H. Afifi e A. Durand (2001), *Dual Stack Transition Mechanism (DSTM),* Gen.

[6]. JJYH-CHENG CHEN, TAO ZHANG (2004), *IP-Based Next-Generation Wireless Networks*, John Wiley & Sons, Inc.

[7]. Juha Korhonen (2001), *Introduction to 3G Mobile Communications*, Artech House, Boston.London

[8]. Karim El Malki (2003), *IPv6 in Mobile Networks*, Ericsson.

[9]**.** K.H.Lee, K.O.Lee, K.C.Park (2003), *Ar-chitecture to be deployed on strategies of Next Generation Networks*, IEEE Communication magazine 2003

[10]. Ramjee Prasad, Werner Mohr & Walter Konhouser (2000), *Third Generation Mobile Communication Systems*, Artech House, Boston.London.