**18.5 IPv6**

Giao thức Internet (IP) đã là nền tảng của Internet và hầu như tất cả các mạng internet đều riêng tư đa phương thức. Giao thức này sắp hết thời hạn sử dụng và có một giao thức mới, được gọi là IPv6 (IP phiên bản 6), đã được xác

Trước tiên, chúng tôi xem xét động lực phát triển phiên bản IP mới và sau đó kiểm tra một số chi tiết của nó.

* **IP thế hệ tiếp theo**

Động lực thúc đẩy việc áp dụng phiên bản IP mới là hạn chế được áp đặt bởi trường địa chỉ 32 bit trong IPv4. Với trường địa chỉ 32 bit, về nguyên tắc có thể gán các địa chỉ khác nhau, có thể có hơn 4 tỷ địa chỉ. . Người ta có thể nghĩ rằng số lượng địa chỉ này là quá đủ để đáp ứng các nhu cầu giải quyết trên Internet. Tuy nhiên, vào cuối những năm 1980, nó đã nhận thấy rằng sẽ có vấn đề và vấn đề này bắt đầu xuất hiện chính nó vào đầu những năm 1990. Các lý do cho sự không phù hợp của địa chỉ 32 bit bao gồm sau đây:

. Cấu trúc hai cấp của địa chỉ IP (số mạng, số máy chủ) là thuận tiện nhưng lãng phí không gian địa chỉ. Khi một số mạng là được chỉ định cho một mạng, tất cả các địa chỉ số máy chủ cho số mạng đó đều được chỉ định cho mạng đó. Không gian địa chỉ cho mạng đó có thể được sử dụng ít, nhưng đối với không gian địa chỉ IP hiệu quả, nếu một số mạng được sử dụng, thì tất cả các địa chỉ trong mạng sẽ được sử dụng.

. Mô hình địa chỉ IP thường yêu cầu một số mạng duy nhất được chỉ định cho mỗi mạng IP cho dù mạng đó có thực sự được kết nối với Internet hay không.

. Mạng đang phát triển nhanh chóng. Hầu hết các tổ chức tự hào có nhiều mạng LAN chứ không chỉ có một hệ thống mạng LAN duy nhất. Mạng không dây đã nhanh chóng đảm nhận một vai trò quan trọng. Bản thân Internet đã phát triển bùng nổ trong nhiều năm.

. Sự phát triển của việc sử dụng TCP / IP sang các lĩnh vực mới sẽ dẫn đến sự tăng trưởng nhanh chóng về nhu cầu đối với các địa chỉ IP duy nhất. Ví dụ bao gồm việc sử dụng TCP / IP để kết nối các thiết bị đầu cuối điểm bán hàng điện tử và cho máy thu truyền hình cáp.

. Thông thường, một địa chỉ IP duy nhất được chỉ định cho mỗi máy chủ lưu trữ. Một cách sắp xếp linh hoạt hơn là cho phép nhiều địa chỉ IP trên mỗi máy chủ lưu trữ. Tất nhiên, điều này làm tăng nhu cầu về địa chỉ IP.

Vì vậy, nhu cầu về không gian địa chỉ tăng lên đòi hỏi một phiên bản IP mới là cần thiết. Ngoài ra, IP là một giao thức rất cũ và các yêu cầu mới trong các lĩnh vực cấu hình địa chỉ, tính linh hoạt của định tuyến và hỗ trợ lưu lượng đã được xác định.

Để đáp ứng những nhu cầu này, Lực lượng Đặc nhiệm Kỹ thuật Internet (IETF) đã kêu gọi các đề xuất cho IP thế hệ tiếp theo (IPng) vào tháng 7 năm 1992. Một số đề xuất đã được nhận và đến năm 1994, thiết kế cuối cùng cho IPng đã xuất hiện. Một cột mốc quan trọng đã đạt được với việc xuất bản RFC 1752, “Khuyến nghị cho Giao thức IP Thế hệ Tiếp theo”, được ban hành vào tháng 1 năm 1995. RFC 1752 phác thảo các yêu cầu đối với IPng, chỉ định các định dạng PDU và làm nổi bật cách tiếp cận IPng trong các lĩnh vực địa chỉ, định tuyến và bảo mật. Một số tài liệu Internet khác đã định nghĩa chi tiết về giao thức, hiện nay chính thức được gọi là IPv6; chúng bao gồm một đặc điểm kỹ thuật tổng thể của IPv6 (RFC 2460), một RFC xử lý cấu trúc địa chỉ của IPv6 (RFC 2373) và nhiều loại khác.

**IPv6 bao gồm các cải tiến sau so với IPv4:**

**. Không gian địa chỉ được mở rộng**: IPv6 sử dụng địa chỉ 128 bit thay vì 32 bit địa chỉ của IPv4. Đây là sự gia tăng của không gian địa chỉ theo hệ số 296 . Người ta đã chỉ ra [HIND95] rằng điều này cho phép theo thứ tự 6 \* 1023  địa chỉ duy nhất trên mỗi mét vuông bề mặt trái đất. Ngay cả khi các địa chỉ được phân bổ rất kém hiệu quả, không gian địa chỉ này dường như vô tận.

**. Cơ chế tùy chọn được cải thiện**: Tùy chọn IPv6 được đặt trong các tiêu đề tùy chọn riêng biệt nằm giữa tiêu đề IPv6 và tiêu đề lớp truyền tải. Hầu hết các tiêu đề tùy chọn này không được kiểm tra hoặc xử lý bởi bất kỳ bộ định tuyến trên đường dẫn của gói. Điều này giúp đơn giản hóa và tăng tốc quá trình xử lý gói tin IPv6 của bộ định tuyến so với biểu đồ dữ liệu IPv4, đồng thời giúp dễ dàng thêm các tùy chọn bổ sung.

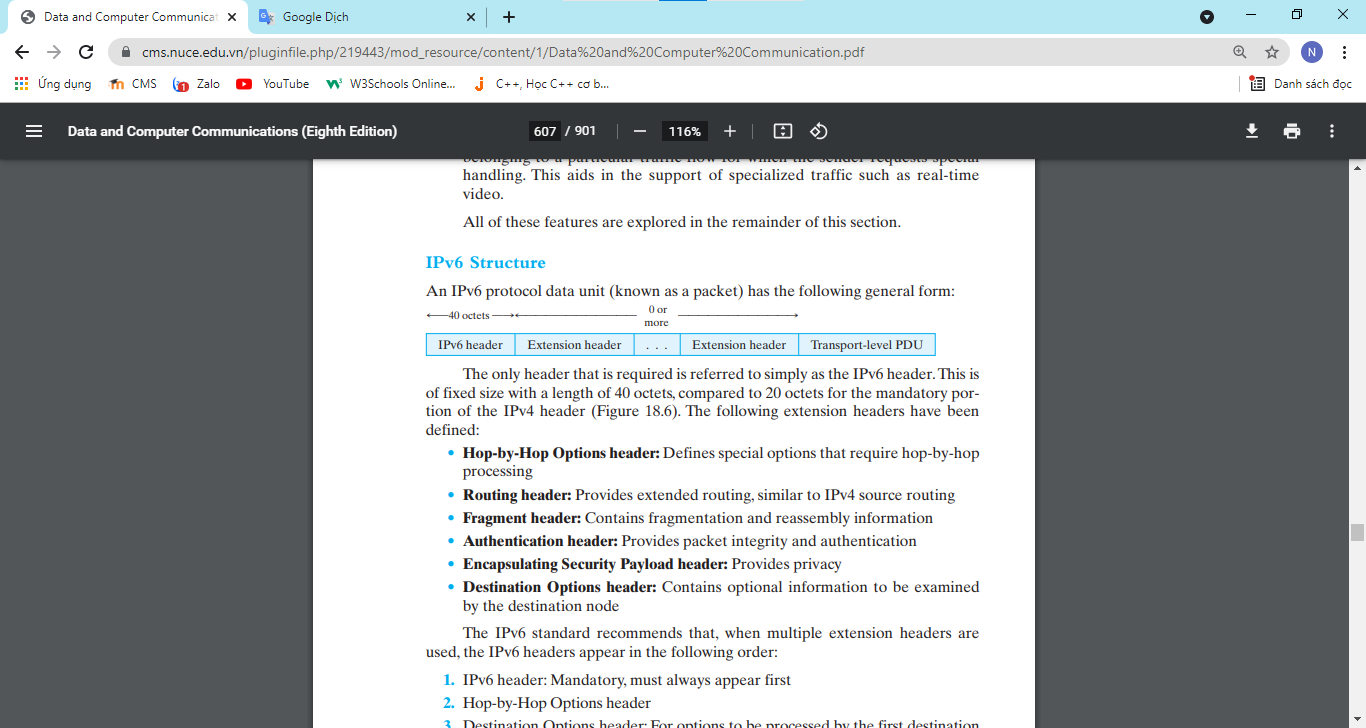
**. Tự động định cấu hình địa chỉ**: Khả năng này cung cấp khả năng gán động các địa chỉ IPv6.

. Tăng tính linh hoạt của việc định địa chỉ: IPv6 bao gồm khái niệm về địa chỉ anycast, nơi một gói được phân phối tới chỉ một trong số các nút. Khả năng mở rộng của định tuyến đa hướng được cải thiện bằng cách thêm trường phạm vi vào đa hướng các địa chỉ.

**. Hỗ trợ phân bổ tài nguyên**: IPv6 cho phép ghi nhãn các gói thuộc một luồng lưu lượng cụ thể mà người gửi yêu cầu xử lý đặc biệt. Điều này hỗ trợ hỗ trợ lưu lượng truy cập chuyên biệt như video thời gian thực.

Tất cả các tính năng này được khám phá trong phần còn lại của phần này.

* **Cấu trúc IPv6**

**Đơn vị dữ liệu giao thức IPv6 (được gọi là gói) có dạng chung sau:** 

Tiêu đề duy nhất được yêu cầu được gọi đơn giản là tiêu đề IPv6, có kích thước cố định với độ dài 40 octet, so với 20 octet cho phần bắt buộc của tiêu đề IPv4 (như hình trên). Các tiêu đề tiện ích mở rộng sau đây đã được xác định:

**. Tiêu đề lựa chọn Hop-by-Hop**: Xác định các tùy chọn đặc biệt yêu cầu xử lý hop-by-hop.

**. Tiêu đề định tuyến**: Cung cấp định tuyến mở rộng, tương tự như định tuyến nguồn IPv4.

**. Tiêu đề phân mảnh**: Chứa thông tin phân mảnh và tập hợp lại.

**. Tiêu đề xác thực**: Cung cấp tính toàn vẹn của gói và xác thực.

**. Đóng gói tiêu đề Tải trọng bảo mật**: Cung cấp quyền riêng tư.

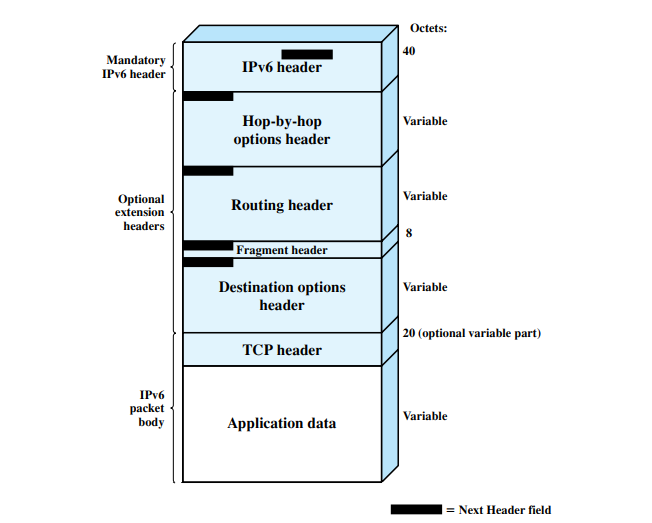
**. Tiêu đề Tùy chọn Đích**: Chứa thông tin tùy chọn được nút đích kiểm tra.

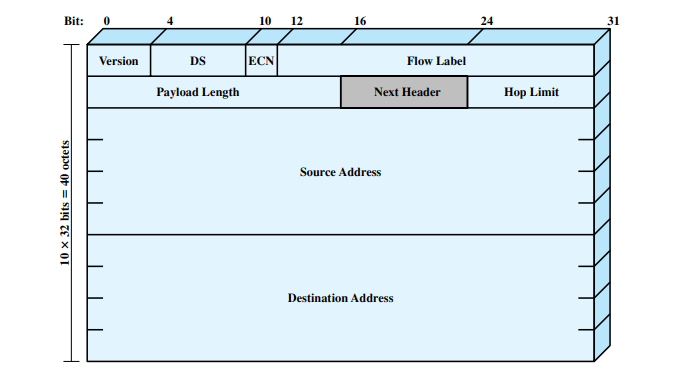
Tiêu chuẩn IPv6 khuyến nghị rằng, khi nhiều tiêu đề mở rộng được sử dụng, các tiêu đề IPv6 xuất hiện theo thứ tự sau:

1. Tiêu đề IPv6: Bắt buộc, phải luôn xuất hiện đầu tiên
2. Tiêu đề tùy chọn Hop-by-Hop
3. Tiêu đề tùy chọn Đích: Dành cho các tùy chọn được xử lý bởi đích đầu tiên xuất hiện trong trường địa chỉ Đích IPv6 cộng với các điểm đến tiếp theođược liệt kê trong tiêu đề Định tuyến
4. Tiêu đề định tuyến
5. Tiêu đề phân mảnh
6. Tiêu đề xác thực
7. Đóng gói tiêu đề Tải trọng bảo mật
8. Tiêu đề Tùy chọn Đích: Dành cho các tùy chọn chỉ được xử lý bởi đích cuối cùng của gói

( Hình sơ đồ bên dưới )cho thấy một ví dụ về một gói IPv6 bao gồm một thể hiện của mỗi tiêu đề, ngoại trừ những tiêu đề liên quan đến bảo mật. Lưu ý rằng tiêu đề IPv6 và mỗi tiêu đề tiện ích mở rộng bao gồm trường Tiêu đề tiếp theo. Trường này xác định loại tiêu đề ngay sau. Nếu tiêu đề tiếp theo là tiêu đề tiện ích mở rộng, thì trường này chứa mã định danh loại của tiêu đề đó. Nếu không, trường này chứa mã nhận dạng giao thức của giao thức lớp trên sử dụng IPv6 (thường là giao thức mức truyền tải), sử dụng các giá trị giống như trường Giao thức IPv4. Trong hình sơ đồ bên dưới, giao thức lớp trên là TCP; do đó, dữ liệu lớp trên do gói IPv6 mang theo bao gồm một tiêu đề TCP theo sau là một khối dữ liệu ứng dụng.

Đầu tiên chúng ta xem xét tiêu đề IPv6 chính và sau đó lần lượt xem xét từng phần mở rộng.





**\*Tiêu đề IPv6**

Tiêu đề IPv6 có độ dài cố định là 40 octet, bao gồm các trường sau:

**. Phiên bản (4 bit)**: Số phiên bản giao thức Internet; giá trị là 6.

**. DS / ECN (8 bit)**: Có sẵn để sử dụng bởi các nút gốc và / hoặc bộ định tuyến chuyển tiếp cho các dịch vụ và chức năng tắc nghẽn khác nhau, như được mô tả cho trường IPv4 DS / ECN.

**. Nhãn luồng (20 bit)**: Máy chủ lưu trữ có thể sử dụng để gắn nhãn các gói mà nó đang yêu cầu xử lý đặc biệt bởi các bộ định tuyến trong mạng; thảo luận sau đó.

**. Độ dài tải trọng (16 bit)**: Độ dài phần còn lại của gói IPv6 theo sau tiêu đề, tính bằng octet. Nói cách khác, đây là tổng chiều dài của tất cả các tiêu đề mở rộng cộng với PDU cấp độ truyền tải.

**. Tiêu đề tiếp theo (8 bit)**: Xác định loại tiêu đề ngay sau tiêu đề IPv6; đây sẽ là tiêu đề mở rộng IPv6 hoặc tiêu đề lớp cao hơn, chẳng hạn như TCP hoặc UDP.

**. Giới hạn hop (8 bit)**: Số bước nhảy còn lại cho phép đối với gói tin này. Giới hạn bước nhảy được nguồn đặt thành một số giá trị tối đa mong muốn và giảm đi 1 bởi mỗi nút chuyển tiếp gói tin. Gói tin bị loại bỏ nếu Hop Limit giảm xuống 0. Đây là sự đơn giản hóa quá trình xử lý cần thiết cho trường Thời gian tồn tại của IPv4. Sự đồng thuận là nỗ lực bổ sung trong việc tính toán các khoảng thời gian trong IPv4 không tạo thêm giá trị đáng kể nào cho giao thức. Trên thực tế, các bộ định tuyến IPv4, theo nguyên tắc chung, coi trường Thời gian tồn tại như một trường giới hạn bước nhảy.

**. Địa chỉ nguồn (128 bit)**: Địa chỉ của người khởi tạo gói tin.

**. Địa chỉ đích (128 bit)**: Địa chỉ của người nhận gói tin. Trên thực tế, đây có thể không phải là đích cuối cùng dự định nếu có tiêu đề Định tuyến, như đã giải thích sau đó.

Mặc dù tiêu đề IPv6 dài hơn phần bắt buộc của tiêu đề IPv4 (40 octet so với 20 octet), nó chứa ít trường hơn (8 so với 12). Do đó, các bộ định tuyến có ít xử lý hơn để thực hiện trên mỗi tiêu đề, điều này sẽ tăng tốc độ định tuyến.

Nhãn luồng RFC 3967 định nghĩa luồng là một chuỗi các gói được gửi từ một nguồn cụ thể đến một đích cụ thể (unicast, anycast hoặc multicast) mà nguồn mong muốn xử lý đặc biệt bởi các bộ định tuyến can thiệp. Luồng được xác định duy nhất bằng sự kết hợp của địa chỉ nguồn, địa chỉ đích và một số khác Nhãn luồng 20 bit. Do đó, tất cả các gói là một phần của cùng một luồng sẽ được nguồn gán cùng một nhãn luồng.

Theo quan điểm của nguồn, một luồng thường sẽ là một chuỗi các gói được tạo từ một phiên bản ứng dụng duy nhất tại nguồn và có cùng một yêu cầu về dịch vụ chuyển nhượng. Một luồng có thể bao gồm một kết nối TCP duy nhất hoặc thậm chí nhiều kết nối TCP; một ví dụ về sau là một ứng dụng truyền tệp, có thể có một kết nối điều khiển và nhiều kết nối dữ liệu. Một ứng dụng có thể tạo ra một luồng duy nhất hoặc nhiều luồng. Một ví dụ về cái sau là hội nghị đa phương tiện, có thể có một luồng dành cho âm thanh và một luồng dành cho các cửa sổ đồ họa, mỗi cửa sổ có các yêu cầu truyền khác nhau về tốc độ dữ liệu, độ trễ và độ trễ thay đổi.

Theo quan điểm của bộ định tuyến, luồng là một chuỗi các gói chia sẻ các thuộc tính ảnh hưởng đến cách bộ định tuyến xử lý các gói này. Chúng bao gồm đường dẫn, phân bổ tài nguyên, các yêu cầu loại bỏ, tính toán và các thuộc tính bảo mật. Bộ định tuyến có thể xử lý các gói từ các luồng khác nhau theo một số cách khác nhau, bao gồm phân bổ các kích thước bộ đệm khác nhau, ưu tiên khác nhau về chuyển tiếp và yêu cầu chất lượng dịch vụ khác nhau từ các mạng.

Không có ý nghĩa đặc biệt đối với bất kỳ nhãn dòng cụ thể nào. Thay vào đó, việc xử lý đặc biệt được cung cấp cho một luồng gói phải được khai báo theo một số cách khác. Ví dụ, một nguồn có thể thương lượng hoặc yêu cầu xử lý đặc biệt trước thời hạn từ bộ định tuyến bằng giao thức điều khiển hoặc tại thời điểm truyền thông tin trong một trong các tiêu đề mở rộng trong gói, chẳng hạn như tiêu đề Tùy chọn Hop-by-Hop. Ví dụ về xử lý đặc biệt có thể được yêu cầu bao gồm một số loại chất lượng dịch vụ không mặc định và một số dạng dịch vụ thời gian thực.

Về nguyên tắc, tất cả các yêu cầu của người dùng đối với một luồng cụ thể có thể được xác định trong tiêu đề mở rộng và được bao gồm trong mỗi gói. Nếu chúng ta muốn để ý niệm về luồng mở để bao gồm nhiều yêu cầu khác nhau, thì cách tiếp cận thiết kế này có thể dẫn đến các tiêu đề gói rất lớn. Giải pháp thay thế, được chấp nhận cho IPv6, là nhãn luồng, trong đó các yêu cầu về luồng được xác định trước khi bắt đầu luồng và một nhãn luồng duy nhất được gán cho luồng. Trong trường hợp này, bộ định tuyến phải lưu thông tin yêu cầu luồng về mỗi luồng.

Các quy tắc sau áp dụng cho nhãn luồng:

1. Máy chủ hoặc bộ định tuyến không hỗ trợ trường Nhãn dòng phải đặt trường này thành 0 khi khởi tạo gói, chuyển trường không thay đổi khi chuyển tiếp gói và bỏ qua trường khi nhận gói.
2. Tất cả các gói bắt nguồn từ một nguồn nhất định có cùng một Nhãn dòng khác phải có cùng Địa chỉ đích, Địa chỉ nguồn, nội dung tiêu đề tùy chọn Hop-by-Hop (nếu có tiêu đề này) và nội dung tiêu đề Định tuyến (nếu có tiêu đề này) . Mục đích là một bộ định tuyến có thể quyết định cách định tuyến và xử lý gói bằng cách chỉ cần tra cứu nhãn luồng trong bảng và không cần kiểm tra phần còn lại của tiêu đề
3. Nguồn gán nhãn luồng cho luồng. Các nhãn luồng mới phải được chọn ngẫu nhiên và thống nhất trong phạm vi 1 để tuân theo hạn chế là nguồn không được sử dụng lại nhãn luồng cho luồng mới trong thời gian tồn tại của luồng hiện có. Nhãn luồng 0 được dành riêng để chỉ ra rằng không có nhãn luồng nào đang được sử dụng.

Điểm cuối cùng này đòi hỏi một số công phu. Bộ định tuyến phải duy trì thông tin về các đặc điểm của từng luồng hoạt động có thể đi qua nó, có lẽ là trong một số loại bảng. Để chuyển tiếp các gói một cách hiệu quả và nhanh chóng, việc tra cứu bảng phải hiệu quả. Một giải pháp thay thế là có một bảng với (khoảng 1 triệu) mục nhập, một mục cho mỗi nhãn luồng có thể có; điều này tạo ra gánh nặng bộ nhớ không cần thiết cho bộ định tuyến. Một giải pháp thay thế khác là có một mục nhập trong bảng cho mỗi luồng hoạt động, bao gồm nhãn luồng với mỗi mục nhập và yêu cầu bộ định tuyến tìm kiếm toàn bộ bảng mỗi khi gặp gói. Điều này đặt ra gánh nặng xử lý không cần thiết đối với bộ định tuyến. Thay vào đó, hầu hết các thiết kế bộ định tuyến có khả năng sử dụng một số loại phương pháp tiếp cận bảng băm. Với cách tiếp cận này, một bảng có kích thước vừa phải được sử dụng và mỗi mục nhập luồng là ánh xạ vào bảng bằng cách sử dụng hàm băm trên nhãn luồng. Hàm băm có thể chỉ đơn giản là một vài bit bậc thấp (ví dụ 8 hoặc 10) của nhãn luồng hoặc một số tính toán đơn giản trên 20 bit của nhãn luồng. Trong mọi trường hợp, hiệu quả của phương pháp băm thường phụ thuộc vào các nhãn luồng được phân phối đồng đều trong phạm vi có thể của chúng. Do đó yêu cầu số 3 trong danh sách trước.

**\*Địa chỉ IPv6**

Địa chỉ IPv6 có độ dài 128 bit, các địa chỉ được gán cho các giao diện riêng lẻ trên các nút chứ không phải cho chính các nút đó. Một giao diện duy nhất có thể có nhiều địa chỉ unicast duy nhất. Bất kỳ địa chỉ unicast nào được liên kết với giao diện của một nút đều có thể được sử dụng để xác định duy nhất nút đó.

Sự kết hợp của các địa chỉ dài và nhiều địa chỉ trên mỗi giao diện cho phép cải thiện hiệu quả định tuyến qua IPv4. Trong IPv4, các địa chỉ thường không có cấu trúc hỗ trợ định tuyến và do đó một bộ định tuyến có thể cần duy trì một bảng lớn các đường dẫn định tuyến. Địa chỉ internet dài hơn cho phép tổng hợp địa chỉ theo phân cấp của mạng, nhà cung cấp truy cập, địa lý, công ty, v.v. Việc tổng hợp như vậy sẽ tạo ra các bảng định tuyến nhỏ hơn và bảng nhanh hơn tra cứu. Việc cho phép nhiều địa chỉ trên mỗi giao diện sẽ cho phép người đăng ký sử dụng nhiều nhà cung cấp quyền truy cập trên cùng một giao diện có các địa chỉ riêng biệt được tổng hợp trong không gian địa chỉ của mỗi nhà cung cấp.giao diện của nút đều có thể được sử dụng để xác định duy nhất nút đó.

IPv6 cho phép ba loại địa chỉ:

**. Unicast**: Một mã định danh cho một giao diện duy nhất. Một gói được gửi đến một địa chỉ unicast được gửi đến giao diện được xác định bởi địa chỉ đó.

**. Anycast**: Một định danh cho một tập hợp các giao diện (thường thuộc về các nút khác nhau). Một gói được gửi đến một địa chỉ anycast sẽ được gửi đến một trong những giao diện được xác định bởi địa chỉ đó (giao diện “gần nhất”, theo thước đo khoảng cách của các giao thức định tuyến).

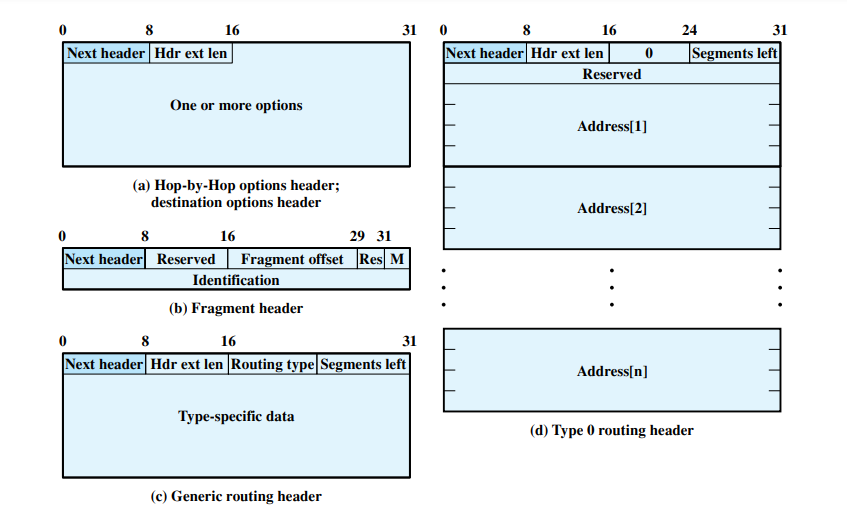
**. Multicast**: Một định danh cho một tập hợp các giao diện (thường thuộc về các nút khác nhau). Một gói được gửi đến một địa chỉ multicast sẽ được gửi đến tất cả các giao diện được xác định bởi địa chỉ đó.

**\*Tiêu đề tùy chọn Hop-by-Hop**

Tiêu đề Tùy chọn Hop-by-Hop mang thông tin tùy chọn, nếu có, phải được kiểm tra bởi mọi bộ định tuyến dọc theo đường dẫn. Tiêu đề này bao gồm ( hình bên dưới ):

**. Tiêu đề tiếp theo (8 bit)**: Xác định loại tiêu đề ngay sau tiêu đề này.

**. Chiều dài phần mở rộng tiêu đề (8 bit)**: Chiều dài của tiêu đề này theo đơn vị 64 bit, không bao gồm 64 bit đầu tiên.

**. Tùy chọn**: Một trường có độ dài thay đổi bao gồm một hoặc nhiều định nghĩa tùy chọn. Mỗi định nghĩa ở dạng ba trường con: Loại tùy chọn (8 bit), xác định tùy chọn; Độ dài (8 bit), chỉ định độ dài của trường Dữ liệu tùy chọn tính bằng octet; và Dữ liệu tùy chọn, là một thông số kỹ thuật có độ dài thay đổi của tùy chọn.

Nó thực sự là năm bit bậc thấp nhất của trường Loại tùy chọn được sử dụng để chỉ định một tùy chọn cụ thể. Hai bit bậc cao chỉ ra rằng hành động sẽ được thực hiện bởi một nút không nhận ra loại tùy chọn này, như sau:

. 00 — Bỏ qua tùy chọn này và tiếp tục xử lý tiêu đề

. 01 — Bỏ gói tin.

. 10 — Hủy gói và gửi thông báo Sự cố tham số ICMP tới Địa chỉ nguồn của gói, trỏ đến Loại tùy chọn không được công nhận.

. 11 — Loại bỏ gói và chỉ khi Địa chỉ đích của gói không phải là địa chỉ phát đa hướng, hãy gửi thông báo Sự cố tham số ICMP đến Địa chỉ nguồn của gói, trỏ đến Loại tùy chọn không được nhận dạng.

Bit bậc cao thứ ba chỉ định liệu trường Dữ liệu tùy chọn không thay đổi (0) hoặc có thể thay đổi (1) trên đường từ nguồn đến đích. Dữ liệu có thể thay đổi phải được loại trừ khỏi các tính toán xác thực, như đã thảo luận trong Chương 21.

Các quy ước này cho trường Loại tùy chọn cũng áp dụng cho tiêu đề Tùy chọn đích.

Bốn tùy chọn hop-by-hop đã được chỉ định cho đến nay:

**. Pad1**: Được sử dụng để chèn một byte đệm vào vùng Tùy chọn của tiêu đề.

**. PadN**: Được sử dụng để chèn N byte đệm vào vùng Tùy chọn của tiêu đề. Hai tùy chọn đệm đảm bảo rằng tiêu đề có độ dài là bội số của 8 byte.

**. Jumbo payload**: Được sử dụng để gửi các gói IPv6 có trọng tải dài hơn 65.535 octet. Trường Dữ liệu tùy chọn của tùy chọn này dài 32 bit và cung cấp độ dài của gói tính bằng octet, không bao gồm tiêu đề IPv6. Đối với các gói như vậy, trường Độ dài tải trọng trong tiêu đề IPv6 phải được đặt thành 0 và không được có tiêu đề Phân mảnh. Với tùy chọn này, IPv6 hỗ trợ kích thước gói lên đến hơn 4 tỷ octet. Điều này tạo điều kiện cho việc truyền các gói video lớn và cho phép IPv6 tận dụng tối đa dung lượng khả dụng trên bất kỳ phương tiện truyền dẫn nào.

**. Cảnh báo bộ định tuyến**: Thông báo cho bộ định tuyến rằng nội dung của gói này được bộ định tuyến quan tâm và xử lý bất kỳ dữ liệu điều khiển nào cho phù hợp. do đó có thể được định tuyến một cách an toàn mà không cần phân tích gói thêm nữa. Các gói IPv6 có nguồn gốc từ máy chủ được yêu cầu bao gồm tùy chọn này trong một số trường hợp nhất định. Mục đích của tùy chọn này là cung cấp hỗ trợ hiệu quả cho các giao thức như RSVP (Chương 19) tạo ra các gói cần được kiểm tra bởi các bộ định tuyến trung gian cho các mục đích điều khiển lưu lượng. Thay vì yêu cầu các bộ định tuyến trung gian xem xét chi tiết các tiêu đề mở rộng của gói tin, tùy chọn này cảnh báo bộ định tuyến khi cần chú ý như vậy.

**\*Tiêu đề phân mảnh**

Trong IPv6, phân mảnh chỉ có thể được thực hiện bởi các nút nguồn chứ không phải bởi các bộ định tuyến dọc theo đường phân phối gói. Để tận dụng tối đa môi trường làm việc trên internet, một nút phải thực hiện một thuật toán khám phá đường dẫn cho phép nó học đơn vị truyền tối đa nhỏ nhất (MTU) được hỗ trợ bởi bất kỳ mạng nào trên đường dẫn. Với kiến thức này, nút nguồn sẽ phân mảnh, theo yêu cầu, cho mỗi địa chỉ đích nhất định. Nếu không, nguồn phải giới hạn tất cả các gói ở 1280 octet, đây là MTU tối thiểu phải được hỗ trợ bởi mỗi mạng.

Tiêu đề phân mảnh bao gồm như sau ( như hình dưới ):

**. Tiêu đề tiếp theo (8 bit)**: Xác định loại tiêu đề ngay sau tiêu đề này.

**. Dành riêng (8 bit)**: Để sử dụng trong tương lai

**. Fragment Offset (13 bit**): Cho biết vị trí trong gói ban đầu, trọng tải của đoạn này thuộc về, được đo bằng đơn vị 64 bit. Điều này ngụ ý rằng các đoạn (không phải đoạn cuối) phải chứa trường dữ liệu là bội số của 64 bit Dài.

**. Res (2 bit)**: Được dự trữ để sử dụng trong tương lai.

**.Cờ M ( 1 bit )**: 1=more fragments; 0 = last fragment.

**. Nhận dạng (32 bit)**: Nhằm mục đích nhận dạng duy nhất gói tin gốc. Số nhận dạng phải là duy nhất cho địa chỉ nguồn và đích của gói địa chỉ cho thời gian mà gói tin sẽ vẫn còn trên internet. Tất cả các đoạn có cùng mã định danh, địa chỉ nguồn và địa chỉ đích được tập hợp lại để tạo thành gói ban đầu.

Thuật toán phân mảnh giống như được mô tả trong Phần 18.3.

**\*Tiêu đề định tuyến**

Tiêu đề Định tuyến chứa danh sách một hoặc nhiều nút trung gian sẽ được truy cập trên đường đến đích của gói. Tất cả các tiêu đề định tuyến bắt đầu bằng một khối 32 bit bao gồm bốn trường 8 bit, tiếp theo là dữ liệu định tuyến dành riêng cho một kiểu định tuyến nhất định. Bốn trường 8 bit như sau:

**. Tiêu đề tiếp theo**: Xác định loại tiêu đề ngay sau tiêu đề này.

**. Chiều dài phần mở rộng tiêu đề**: Chiều dài của tiêu đề này tính bằng đơn vị 64 bit, không bao gồm 64 bit đầu tiên.

**. Loại định tuyến**: Xác định một biến thể tiêu đề định tuyến cụ thể. Nếu một bộ định tuyến không nhận ra giá trị Loại định tuyến, nó phải loại bỏ gói tin.

**. Phân đoạn còn lại**: Số đoạn tuyến đường còn lại; nghĩa là, số lượng các nút trung gian được liệt kê rõ ràng vẫn phải được truy cập trước khi đến đích cuối cùng.

Định dạng tiêu đề định tuyến cụ thể duy nhất được xác định trong RFC 2460 là tiêu đề Định tuyến Loại 0. Khi sử dụng tiêu đề Định tuyến Loại 0, nút nguồn không đặt địa chỉ đích cuối cùng trong tiêu đề IPv6. Thay vào đó, địa chỉ đó là địa chỉ cuối cùng được liệt kê trong tiêu đề Định tuyến (Địa chỉ [n] trong hình trên) và tiêu đề IPv6 chứa địa chỉ đích của bộ định tuyến mong muốn đầu tiên trên đường dẫn. Tiêu đề định tuyến sẽ không được kiểm tra cho đến khi gói đến nút được xác định trong tiêu đề IPv6. Tại thời điểm đó, nội dung tiêu đề IPv6 và Định tuyến được cập nhật và gói được chuyển tiếp. Cập nhật bao gồm việc đặt địa chỉ tiếp theo sẽ được truy cập trong tiêu đề IPv6 và giảm trường Phân đoạn còn lại trong tiêu đề Định tuyến.

**\*Tiêu đề Tùy chọn Đích**

Tiêu đề Tùy chọn Đích mang thông tin tùy chọn, nếu có, chỉ được kiểm tra bởi nút đích của gói. Định dạng của tiêu đề này giống với định dạng của tiêu đề Tùy chọn Hop-by-Hop.

**18.6 MẠNG RIÊNG TƯ RIÊNG VÀ BẢO MẬT IP**

Trong môi trường máy tính phân tán ngày nay, mạng riêng ảo (VPN) cung cấp một giải pháp hấp dẫn cho các nhà quản lý mạng. Về bản chất, VPN bao gồm một tập hợp các máy tính kết nối với nhau bằng một mạng tương đối không an toàn và sử dụng mã hóa và các giao thức đặc biệt để cung cấp bảo mật. Tại mỗi trang web của công ty, các máy trạm, máy chủ và cơ sở dữ liệu được liên kết bởi một hoặc nhiều mạng cục bộ (LAN). Các mạng LAN nằm dưới sự kiểm soát của người quản lý mạng và có thể được định cấu hình và điều chỉnh để đạt hiệu quả về chi phí. giao nhiệm vụ quản lý mạng diện rộng cho nhà cung cấp mạng công cộng. Cũng chính mạng công cộng đó cung cấp một đường dẫn truy cập cho các nhà viễn thông và các nhân viên di động khác đăng nhập vào các hệ thống của công ty từ các trang web từ xa.

Nhưng người quản lý phải đối mặt với một yêu cầu cơ bản: bảo mật. Việc sử dụng mạng công cộng khiến lưu lượng truy cập của công ty bị nghe trộm và cung cấp một điểm vào cho người dùng trái phép. Để giải quyết vấn đề này, người quản lý có thể chọn từ nhiều gói và sản phẩm mã hóa và xác thực khác nhau. Các giải pháp độc quyền làm nảy sinh một số vấn đề. Đầu tiên, giải pháp an toàn như thế nào? Nếu độc quyền các chương trình mã hóa hoặc xác thực được sử dụng, có thể có ít sự đảm bảo trong tài liệu kỹ thuật về mức độ bảo mật được cung cấp. Thứ hai là câu hỏi về tính tương thích. Không người quản lý nào muốn bị giới hạn trong việc lựa chọn máy trạm, máy chủ, bộ định tuyến, tường lửa, v.v. bởi nhu cầu tương thích với bảo mật cơ sở. Đây là động lực cho bộ tiêu chuẩn Internet Bảo mật IP (IPSec).

**\*IPSec**

Năm 1994, Hội đồng Kiến trúc Internet (IAB) đã đưa ra một báo cáo có tiêu đề “Bảo mật trong Kiến trúc Internet” (RFC 1636). Trong số này có nhu cầu bảo mật cơ sở hạ tầng mạng khỏi sự giám sát và kiểm soát trái phép lưu lượng mạng và nhu cầu bảo mật lưu lượng người dùng cuối đến người dùng cuối bằng cách sử dụng các cơ chế xác thực và mã hóa.

Để cung cấp bảo mật, IAB đã bao gồm xác thực và mã hóa làm các tính năng bảo mật cần thiết trong IP thế hệ tiếp theo, đã được cấp dưới dạng IPv6. May mắn thay, các khả năng bảo mật này được thiết kế để có thể sử dụng được cả với IPv4 và IPv6 trong tương lai. Điều này có nghĩa là các nhà cung cấp có thể bắt đầu cung cấp các tính năng này ngay bây giờ và nhiều nhà cung cấp hiện đã có một số khả năng IPSec trong các sản phẩm của họ. Đặc tả IPSec hiện tồn tại như một tập hợp các tiêu chuẩn Internet.

**\*Các ứng dụng của IPSec**

IPSec cung cấp khả năng bảo mật thông tin liên lạc qua mạng LAN, qua mạng riêng tư và các mạng WAN công cộng và trên Internet. Ví dụ về việc sử dụng nó bao gồm:

**. Kết nối văn phòng chi nhánh an toàn qua Internet**: Một công ty có thể xây dựng một mạng riêng ảo an toàn qua Internet hoặc qua mạng WAN công cộng. Cái này cho phép một doanh nghiệp phụ thuộc nhiều vào Internet và giảm nhu cầu về mạng riêng, tiết kiệm chi phí và chi phí quản lý mạng.

**. Truy cập từ xa an toàn qua Internet**: Người dùng cuối có hệ thống được trang bị các giao thức bảo mật IP có thể thực hiện cuộc gọi nội hạt tới nhà cung cấp dịch vụ Internet (ISP) và có được quyền truy cập an toàn vào mạng công ty. Điều này làm giảm chi phí của phí cho nhân viên đi lại và viễn thông.

**. Thiết lập kết nối extranet và mạng nội bộ với các đối tác**: IPSec có thể được sử dụng để bảo mật thông tin liên lạc với các tổ chức khác, đảm bảo xác thực và bảo mật và cung cấp cơ chế trao đổi chính.

**. Tăng cường bảo mật thương mại điện tử**: Mặc dù một số ứng dụng web và thương mại điện tử có các giao thức bảo mật tích hợp, việc sử dụng IPSec sẽ tăng cường bảo mật đó. IPSec đảm bảo rằng tất cả lưu lượng do người quản trị mạng chỉ định đều được mã hóa và xác thực, thêm một lớp bảo mật bổ sung cho bất cứ thứ gì được cung cấp ở lớp ứng dụng.

Tính năng chính của IPSec cho phép nó hỗ trợ các ứng dụng đa dạng này là nó có thể mã hóa và / hoặc xác thực tất cả lưu lượng ở cấp IP. Do đó, tất cả các ứng dụng phân tán, bao gồm đăng nhập từ xa, máy khách / máy chủ, e-mail, truyền tệp, Truy cập web, v.v., có thể được bảo mật.

Hình bên dưới là một kịch bản điển hình của việc sử dụng IPSec. Một tổ chức duy trì mạng LAN tại các địa điểm phân tán. Lưu lượng IP không an toàn được thực hiện trên mỗi mạng LAN. Đối với lưu lượng ngoại vi, thông qua một số loại WAN riêng hoặc công cộng, các giao thức IPSec được sử dụng giao thức hoạt động trong các thiết bị mạng, chẳng hạn như bộ định tuyến hoặc tường lửa, kết nối mỗi mạng LAN với thế giới bên ngoài. Thiết bị mạng IPSec thường sẽ mã hóa và nén tất cả lưu lượng đi vào WAN, đồng thời giải mã và giải nén lưu lượng đến từ WAN; các hoạt động này là minh bạch đối với các máy trạm và máy chủ trên Mạng LAN. Cũng có thể truyền an toàn với những người dùng cá nhân quay số vào mạng WAN. Các máy trạm người dùng như vậy phải triển khai các giao thức IPSec để cung cấp bảo mật.

**\*Lợi ích của IPSec**

Một số lợi ích của IPSec như sau:

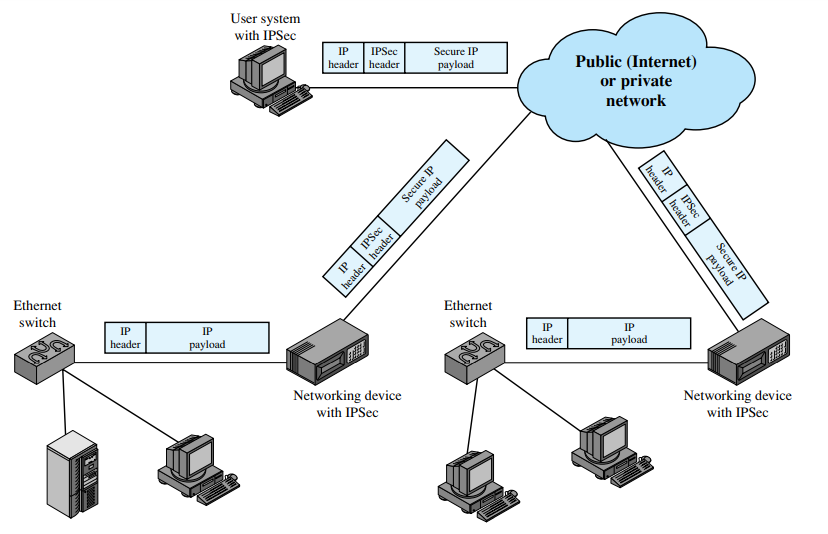
. Khi IPSec được triển khai trong tường lửa hoặc bộ định tuyến, nó cung cấp khả năng bảo mật mạnh mẽ có thể được áp dụng cho tất cả các lưu lượng đi qua ngoại vi. Lưu lượng truy cập trong một công ty hoặc nhóm làm việc không phải chịu chi phí xử lý liên quan đến bảo mật.

. IPSec trong tường lửa có khả năng chống bỏ qua nếu tất cả lưu lượng truy cập từ bên ngoài phải sử dụng IP và tường lửa là phương tiện duy nhất để truy cập từ Internet vào tổ chức.

. IPSec nằm bên dưới lớp truyền tải (TCP, UDP) và do đó, trong suốt đối với các ứng dụng. Không cần thay đổi phần mềm trên hệ thống người dùng hoặc máy chủ khi IPSec được thực hiện trong tường lửa hoặc bộ định tuyến. Ngay cả khi IPSec được triển khai trong các hệ thống đầu cuối, phần mềm lớp trên, bao gồm các ứng dụng, vẫn không bị ảnh hưởng.

. • IPSec có thể minh bạch đối với người dùng cuối. Không cần phải đào tạo người dùng về cơ chế bảo mật, phát hành tài liệu khóa trên cơ sở mỗi người dùng hoặc thu hồi khóa tài liệu khi người dùng rời khỏi tổ chức.

. IPSec có thể cung cấp bảo mật cho người dùng cá nhân nếu cần. Điều này hữu ích cho những người làm việc bên ngoài và để thiết lập một mạng con ảo an toàn trong một tổ chức cho các ứng dụng nhạy cảm.



**\*Chức năng IPSec**

IPSec cung cấp ba cơ sở chính: một chức năng chỉ xác thực được gọi là Tiêu đề xác thực (AH), một chức năng xác thực / mã hóa kết hợp được gọi là Đóng gói Tải trọng Bảo mật (ESP) và một chức năng trao đổi khóa. Đối với VPN, cả xác thực và mã hóa nói chung đều được mong muốn, bởi vì nó quan trọng là (1) đảm bảo rằng người dùng trái phép không xâm nhập vào mạng riêng ảo và (2) đảm bảo rằng những kẻ nghe trộm trên Internet không thể đọc các tin nhắn được gửi qua mạng riêng ảo. Bởi vì cả hai tính năng nói chung là mong muốn, hầu hết các triển khai có khả năng sử dụng ESP hơn là AH. Chức năng trao đổi chìa khóa cho phép trao đổi chìa khóa thủ công cũng như kiểm tra tự động.

IPSec được khám phá trong Chương 21.