LỜI MỞ ĐẦU

Như ta đã thấy với sự phát triển của mạng chuyển mạch gói IP cùng với sự hội nhập mạnh mẽ vào nền kinh tế của khu vực và thế giới. Và một trong những yếu tố quan trọng để có thể cạch tranh được đó là chi phí thấp. Cũng vì lý do đó mà VoIP đang trở thành một công nghệ rất phổ biến với chi phí thấp và cấu trúc mềm dẻo đáp ứng được nhu cầu của người sử dụng. Tuy nhiên, để thiết lập một hệ thống VoIP thì ngoài chất lượng dịch vụ (QoS) thì cũng cần phải tính đến bảo mật cho hệ thống VoIP. Việc tích hợp các dịch vụ thoại, dữ liệu, video,… trên cùng một hạ tầng mạng IP đã mang đến nhiều nguy cơ tiềm ẩn về bảo mật. Không chỉ do mạng IP là một mạng công cộng, nguy cơ bị tấn công rất lớn mà bản thân các giao thức VoIP cũng có những nguy cơ về bảo mật.

Xuất phát từ những ý nghĩ trên mà em quyết định chọn đề tài "*Bảo Mật Trong VoIP*". Trong giới hạn đề tài, em chỉ tìm hiểu về lý thuyết bảo mật cho hệ thống VoIP. Nội dung của đề tài bao gồm tìm hiểu về kiến trúc và các giao thức của các mạng VoIP cụ thể, từ đó phân tích những lỗ hổng trong mạng VoIP và các công nghệ để khắc phục các lỗ hổng đó. Nội dung luận văn được chia thành 3 chương:

Chương 1: Tổng Quan Trong Mạng VoIP
Chương 2: Công Nghệ Trong VoIP
Chương 3: Bảo Mật Trong VoIP

Trong quá trình nghiên cứu đề tài này, do kiến thức và kinh nghiệm của em còn hạn chế vì vậy không tránh được những thiếu sót, rất mong được sự nhận xét và góp ý của Thầy Cô cùng bạn bè.

Hải Phòng, ngày tháng năm 2010
Sinh viên
Trần Mạnh Tuyên

Chương 1:

TỔNG QUAN TRONG MẠNG VoIP

1.1 Giới thiệu chung về VoIP

VoIP (Voice over Internet Protocol) là công nghệ cho phép truyền thoại sử dụng giao thức mạng IP, trên cơ sở hạ tầng sẵn có của mạng Internet. VoIP là một trong những công nghệ viễn thông đang được quan tâm nhất hiện nay không chỉ đối với nhà khai thác, các nhà sản xuất mà còn cả với người sử dụng dịch vụ.

Hình 1.1: Mô hình truyền thoại qua IP

VoIP dựa trên sự kết hợp của mạng chuyển mạch kênh và chuyển mạch gói là mạng IP. Mỗi loại mạng có một đặc điểm khác biệt nhau. Trong mạng chuyển mạch kênh một kênh truyền dẫn dành riêng được thiết lập giữa hai thiết bị đầu cuối thông qua một hay nhiều nút chuyển mạch trung gian. Dòng thông tin truyền trên kênh này là dòng bít truyền liên tục theo thời gian. Băng thông của kênh dành riêng được đảm bảo và cố định trong quá trình liên lạc (64Kbps đối với mạng điện thoại PSTN), và độ trễ thông tin là rất nhỏ chỉ cỡ thông thời gian truyền thông tin trên kênh. Khác với mạng chuyển mạch kênh, mạng chuyển mạch gói (Packet Switching Network) sử dụng hệ thống lưu trữ

rồi truyền trên các nút mạng. Thông tin được chia thành các gói, mỗi gói được thêm các thông tin điều khiển cần thiết cho quá trình truyền như là địa chỉ nơi gửi, địa chỉ nơi nhận… Các gói thông tin đến các nút mạng được sử lý và lưu trữ trong một thời gian nhất định rồi mới được truyền đến các nút tiếp theo sao cho việc sử dụng kênh có hiệu quả nhất. Trong mạng chuyển mạch gói không có kênh dành riêng nào được thiết lập, băng thông của kênh logic giữa hai thiết bị đầu cuối thường không cố định, và độ trễ thông tin thường lớn hơn mạng chuyển mạch gói rất nhiều.

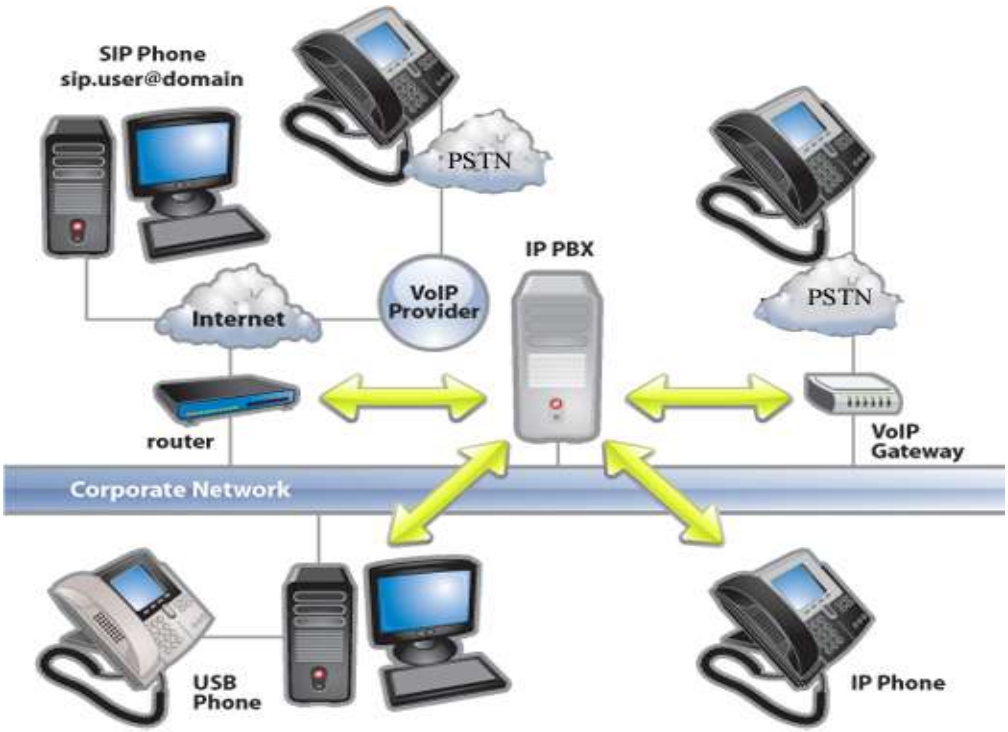
Nguyên tắc VoIP gồm việc số hóa tín hiệu giọng nói, nén tín hiệu đã số hóa, chia tín hiệu thành các gói và truyền những gói số liệu này trên nền IP. Đến nơi nhận, các gói số liệu được ghép lại, giải mã ra tín hiệu analog để phục hồi âm thanh.

VoIP cho phép thực hiện cuộc gọi dùng máy tính qua mạng dữ liệu như internet. VoIP chuyển đổi tín hiệu thoại từ điện thoại tương tự analog vào tín hiệu số digital trước khi truyền qua internet, sau đó chuyển đổi ngược lại ở đầu nhận. Khi tạo một cuộc gọi VoIP dùng điện thoại với một bộ điều hợp, chúng ta sẽ nghe âm mời gọi, quay số sẽ xảy ra sau tiến trình này. VoIP cũng thể sẽ cho phép tạo một cuộc gọi trực tiếp từ máy tính dùng loại điện thoại tương ứng hay dùng microphone.

VoIP cho phép tạo cuộc gọi đường dài qua mạng dữ liệu IP có sẵn thay vì được truyền qua mạng PSTN (public switched telephone network). Ngày nay nhiều công ty đã thực hiện giải pháp VoIP của họ để giảm chi phí cho những cuộc gọi đường dài giữa nhiều chi nhánh xa nhau.

Áp dụng VoIP có thể khai thác tính hiệu quả của mạng truyền số liệu, khai thác tính linh hoạt trong phát triển các ứng dụng mới của giao thức IP. Tuy nhiên để thực hiện và ứng dụng và bảo vệ trong VoIP là phức tạp.

Để gọi điện qua VoIP, người dùng cần có chương trình phần mềm điện thoại SIP hoặc một điện thoại VoIP dạng phần cứng. Có thể gọi điện thoại đến bất cứ đâu, cho bất kỳ ai đối với cả số điện thoại VoIP và những người dùng số điện thoại bình thường.



Hình 1.2: Mô hình chung của một kế nối VoIP

1.2 Các đặc tính của mạng VoIP

1.2.1. Ưu điểm

VoIP ra đời nhằm khai thác tính hiệu quả của các mạng truyền số liệu, khai thác tính linh hoạt trong phát triển các ứng dụng mới của giao thức IP và nó được áp dụng trên một mạng toàn cầu là mạng Internet. Các tiến bộ của công nghệ đã mang đến cho VoIP những ưu điểm sau:

- *Giảm chi phí cuộc gọi*: Ưu điểm nổi bật của điện thoại IP so với dịch vụ điện thoại hiện tại là khả năng cung cấp những cuộc gọi đường dài giá rẻ với chất lượng chấp nhận được. Nếu dịch vụ điện thoại IP được triển khai thì chi phí cho một cuộc gọi đường dài sẽ chỉ tương đương với chi phí truy nhập Internet. Nguyên nhân dẫn đến chi phí thấp như vậy là do tín hiệu thoại được truyền tải trong mạng IP có khả năng sử dụng kênh hiệu quả cao. Đồng thời, kỹ thuật nén thoại tiên tiến giảm tốc độ bít từ 64Kbps xuống thấp tới 8Kbps kết hợp với tốc độ xử lý nhanh của các bộ vi xử lý ngày nay cho phép việc truyền tiếng nói theo thời gian thực là có thể thực hiện được với lượng tài nguyên băng thông thấp hơn nhiều so với kỹ thuật cũ.

- *Khả năng mở rộng*: Nếu như các hệ tổng đài thường là những hệ thống kín, thì rất khó để thêm vào đó những tính năng thì các thiết bị trong

mạng Internet thường có khả năng thêm vào những tính năng mới. Chính tính mềm dẻo đó mang lại cho dịch vụ điện thoại IP khả năng mở rộng dễ dàng hơn so với điện thoại truyền thống.

- *Không cần thông tin điều khiển để thiết lập kênh truyền vật lý*: Gói thông tin trong mạng IP truyền đến đích mà không cần một sự thiết lập kênh nào. Gói tin chỉ cần mang địa chỉ của nơi nhận cuối cùng là thông tin đó có thể đến được đích. Do vậy, việc điều khiển cuộc gọi trong mạng IP chỉ cần tập trung vào chức năng cuộc gọi mà không cần phải tập trung vào chức năng thiết lập kênh.
- *Quản lý băng thông:* Trong điện thoại chuyển mạch kênh, tài nguyên băng thông cung cấp cho một cuộc thoại là cố định (một kênh 64Kbps), nhưng trong điện thoại IP việc phân chia tài nguyên cho các cuộc thoại linh hoạt hơn nhiều. Khi một cuộc liên lạc diễn ra, nếu lưu lượng của mạng thấp thì băng thông dành cho liên lạc sẽ cho chất lượng thoại tốt nhất có thể, nhưng khi lưu lượng của mạng cao thì mạng sẽ hạn chế băng thông của từng cuộc gọi ở mức duy trì chất lượng thoại chấp nhận được nhằm phục vụ cùng lúc được nhiều người nhất. Điểm này cũng là một yếu tố làm tăng hiệu quả sử dụng của điện thoại IP.Việc quản lý băng thông một cách tiết kiệm như vậy cho phép người ta nghĩ tới những dịch vụ cao cấp hơn như điện thoại hội nghị, điều mà với công nghệ chuyển mạch cũ thì không thực hiện vì chi phí quá cao.
- *Nhiều tính năng dịch vụ*: Tính linh hoạt của mạng IP cho phép tạo ra nhiều tính năng mới trong dịch vụ thoại như: Cho biết thông tin về người gọi tới hay một thuê bao điện thoại IP có thể có nhiều số liên lạc mà chỉ cần một thiết bị đầu cuối duy nhất.
- *Khả năng multimedia*: Trong một cuộc gọi người sử dụng có thể vừa nói chuyện vừa sử dụng các dịch vụ khác như truyền file, chia sẻ dữ liệu, hay xem hình ảnh của người nói chuyện bên kia.
- *Sử dụng hiệu quả*: Như đã biết VoIP truyền thoại qua mạng Internet và sử dụng giao thức IP, ngày nay IP là giao thức mạng được sử dụng rộng rãi nhất và có rất nhiều ứng dụng đang được khai thác trên cơ sở các giao thức của mạng IP, VoIP có thể kết hợp sử dụng các ứng dụng này để nâng cao hiệu

quả sử dụng mạng. Kỹ thuật VoIP được sử dụng chủ yếu kết hợp với các mạng máy tính do đó có thể tận dụng được sự phát triển của công nghệ thông tin để nâng cao hiệu quả sử dụng, các phần mềm sẽ hỗ trợ rất nhiều cho việc khai thác các dịch vụ của mạng VoIP. Công nghệ thông tin càng phát triển thì việc khai thác càng có hiệu quả, sẽ xuất hiện nhiều dịch vụ mới hỗ trợ người sử dụng trong mọi lĩnh vực.

1.2.2 Nhược điểm

Kỹ thuật phức tạp: Truyền tín hiệu theo thời gian thực trên mạng chuyển mạch gói là rất khó thực hiện do mất gói trong mạng là không thể tránh và độ trễ không cố định của các gói thông tin khi truyền trên mạng. Để có được một dịch vụ thoại chấp nhận được cần phải có một kỹ thuật nén tín hiệu đạt được những yêu cầu khắt khe như: Tỉ số nén lớn, có khả năng suy đoán và tạo lại thông tin của các gói bị thất lạc…Tốc độ xử lý của các bộ Codec phải đủ nhanh để không làm cuộc đàm thoại bị gián đoạn. Đồng thời cơ sở hạ tầng của mạng cũng cần được nâng cấp lên các công nghệ mới để có tốc độ cao hơn và có cơ chế thực hiện chức năng QoS (Quality of Service).

Vấn đề bảo mật: Mạng Internet là mạng có tính rộng khắp và hỗn hợp, trong đó có rất nhiều loại máy tính khác nhau, các dịch vụ khác nhau cùng sử dụng chung một cơ sở hạ tầng. Do vậy không có gì đảm bảo rằng thông tin liên quan đến cá nhân cũng như số liên lạc truy nhập sử dụng dịch vụ của người dùng được giữ bí mật. Và nguy cơ nghe lén cuộc gọi VoIP khá cao do các gói dữ liệu phải chuyển tiếp qua nhiều trạm trung gian trước khi đến người nghe hoặc vấn đề truy cập trái phép, hacker có thể lợi dụng các lỗ hổng bảo mật để xâm nhập vào hệ thống mạng.

Ngoài ra VoIP có thể gặp những vấn đề như không thể sử dụng được dịch vụ khi cúp điện, không thể kết nối đến các dịch vụ khẩn như: cấp cứu, báo cháy...

1.3 Xu hướng phát triển của dịch vụ điện thoại IP

1.3.1 Những yêu cầu khi phát triển VoIP

Chất lượng thoại phải ổn định, độ trễ chấp nhận được và phải so sánh được với chất lượng thoại của mạng PSTN và các mạng có chất lượng phục vụ khác nhau.

Mạng IP cơ bản phải đáp ứng được những tiêu chí hoạt động khắt khe

bao gồm giảm thiểu việc từ chối cuộc gọi, mất mát gói và mất liên lạc. Điều này đòi hỏi ngay cả khi mạng bị nghẽn hoặc khi người sử dụng chung tài nguyên của mạng cùng một lúc.

Tín hiệu báo hiệu phải có khả năng tương tác được với báo hiệu của mạng khác (PSTN) để không gây ra sự thay đổi khi chuyển giao giữa các mạng cũng như không ảnh hưởng đến hoạt động của mạng.

Quản lý hệ thống an toàn, địa chỉ hóa và thanh toán phải được cung cấp, tốt nhất là được hợp nhất với các hệ thống hỗ trợ hoạt động

1.3.2 Những khó khăn khi triển khai dịch vụ

Vấn đề tiêu chuẩn: Do tiêu chuẩn quốc tế cả điện thoại IP còn đang không ngừng phát triển và hoàn thiện và đặc biệt là tiêu chuẩn thông tin giữa các miền khác nhau, giữa các mạng khác nhau v.v…còn đang trong thời gian tranh luận đã ảnh hưởng trực tiếp đến sự tương thích giữa các sản phẩm điện thoại VoIP của các nhà cung cấp khác nhau. Ngoài ra vấn đề chuyển mạch của thuê bao ở các miền khác nhau, vấn đề lộ trình và vấn đề tương thích dịch vụ, vấn đề thanh toán cước phí giữa các nhà cung cấp dịch vụ khác nhau còn đang chờ đợi.

Vấn đề mạng truyền tải: Trong mạng Internet là không thể xác định trước được và luôn thay đổi, vì vậy ảnh hưởng nghiêm trọng đến chất lượng thông thoại. Căn cứ vào tình hình kỹ thuật hiện nay có thể nói Internet đối với thông tin điện thoại thời gian thực yêu cầu chất lượng cao còn tồn tại nhiều khuyết điểm.

Vấn đề dung lượng thiết bị: Các nhà sản xuất thiết bị tiếp nhận Internet và các nhà sản xuất thiết bị cổng mạng đều đang cố gắng phát triển với quy mô lớn, từ vài cửa ra E1 cho đến hơn 100 cửa ra E1. Tuy nhiên chất lượng của thiết bị hiện nay còn cách xa so với sản phẩm viễn thông.

1.3.3 Xu hướng phát triển

Hiện nay mảnh đất hứa hẹn cho VoIP là các mạng doanh nghiệp Intranet và mạng Etranet thương mại. Cở sở hạ tầng dựa trên IP cho phép điều khiển quản lý việc sử dụng các dịch vụ cho phép hay không cho phép truy cập các dịch vụ. Các sản phẩm điện thoại trên mạng Internet chưa thể đáp ứng các yêu cầu chất lượng dịch vụ như điện thoại thông thường. Bởi vậy, phát triển VoIP trên Intranet, Etranet là hướng phát triển trước mắt.

Một xu thế phát triển khác hứa hẹn là xây dựng các cổng nối giữa mạng IP và mạng thoại là các VoIP Gateway. Những Gateway này xây dựng từ nền tảng PC trở thành các hệ thống mạnh có khả năng điều khiển hàng trăm cuộc gọi đồng thời. Bởi vậy các doanh nghiệp sẽ phát triển lượng lớn các Gateway trong nỗ lực giảm chi phí liên quan đến lưu lượng thoại, fax và video hội nghị.

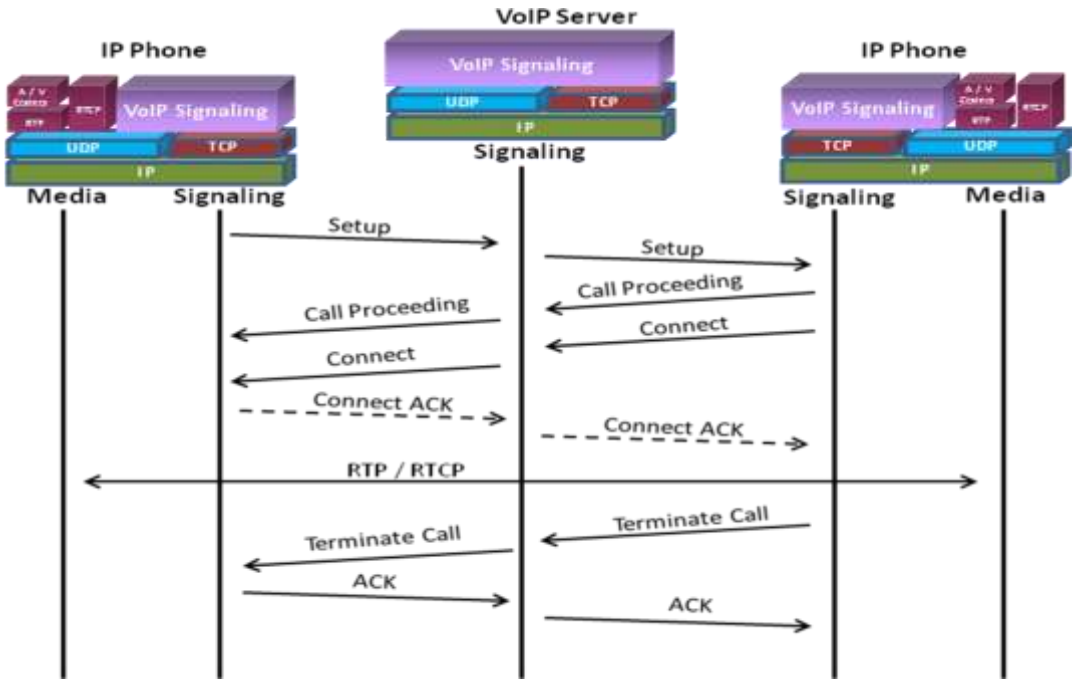
Chương 2:

CÔNG NGHỆ TRONG VoIP

Để hiểu được các nguyên tắc tấn công cũng như các giải pháp bảo vệ mạng khỏi bị tấn công, cần hiểu rõ kiến trúc cũng như hoạt động của hệ thống VoIP. Chương này sẽ tìm hiểu rõ kiến trúc quá trình xử lý tín hiệu cũng như giao thức SIP, H.323 và các giao thức vận chuyển VoIP.

2.1. Kiến trúc mạng VoIP

2.1.1 Mô hình kiến trúc mạng VoIP



Hình 2.1 Mô hình kiến trúc tổng quan của mạng VoIP

Trong mô hình này là sự có mặt của hai thành phần chính trong mạng VoIP đó là:

IP Phone (hay còn gọi là SoftPhone): Là thiết bị giao diện đầu cuối phía người dùng với mạng VoIP. Cấu tạo chính của một IP Phone gồm hai thành phần chính:

+ Thành phần báo hiệu mạng VoIP: Báo hiệu có thể là H.323 sử dụng giao thức TCP hay SIP sử dụng UDP hoặc TCP làm giao thức truyền tải của mình.

+ Thành phần truyền tải media: Sử dụng RTP để truyền luồng media với chất lượng thời gian thực và được điều khiển theo giao thức RTCP.

VoIP Server: Chức năng chính của Server trong mạng VoIP tùy thuộc vào giao thức báo hiệu được sử dụng. Nhưng về mô hình chung thì VoIP Server thực hiện các chức năng sau:

+ Định tuyến bản tin báo hiệu trong mạng VoIP.

+ Đăng kí, xác thực người sử dụng.

+ Dịch địa chỉ trong mạng.

Nói chung, VoIP Server trong mạng như là đầu não chỉ huy mọi hoạt động của mạng. Server có thể tích hợp tất cả các chức năng (SoftSwitch) hoặc nằm tách biệt trên các Server chức năng khác nhau (Location Server, Registrar Server, Proxy Server,…).

2.1.2 Phương thức hoạt động

VoIP chuyển đổi tín hiệu giọng nói thông qua môi trường mạng. Do vậy, trước hết giọng nói phải được chuyển đổi thành các dãy bit kỹ thuật số (digital bits) và được đóng gói thành các packet để sau đó truyền tải qua mạng IP network và cuối cùng được chuyển lại thành tín hiệu âm thanh đến người nghe.

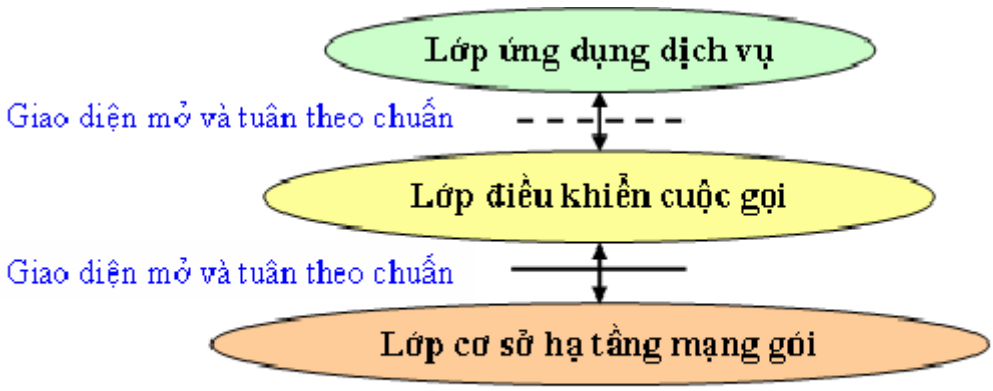
Tiến trình hoạt động của VoIP thông qua hai bước:

Call setup: trong quá trình này, người gọi phải xác định vị trí (thông qua địa chỉ của người nhận) và yêu cầu một kết nối để liên lạc với người nhận. Khi địa chỉ người nhận được xác định là tồn tại trên các proxy server giữa hai người sẽ thiết lập một cuộc kết nối cho quá trình trao đổi dữ liệu voice.

Voice data processing: tín hiệu giọng nói (analog) sẽ được chuyển đổi sang tín hiệu số (digital) rồi được nén lại nhằm tiết kiệm đường truyền (bandwidth) sau đó sẽ được mã hóa (tính năng bổ sung nhằm tránh các bộ phận tích mạng-sliffer). Các voice samples sau đó sẽ được chèn vào các gói dữ liệu để vận chuyển trên mạng. Giao thức dùng cho các gói voice này là RTP (real-time transport protocol). Một gói tin RTP có các field chứa dữ liệu cần thiết cho việc biên dịch lại các gói tin sang tín hiệu voice ở thiết bị người nghe. Các gói tin voice được truyền đi bởi giao thức UDP. Ở thiết bị cuối, tiến trình được thực hiện ngược lại.

2.1.3 Mô hình phân lớp chức năng

Về mặt chức năng, công nghệ VoIP có thể được chia làm ba lớp như sau:



Hình 2.2: Mô hình phân lớp chức năng của VoIP

2.1.3.1 Lớp cơ sở hạ tầng mạng gói

Thực hiện chức năng truyền tải lưu lượng thoại. Trong VoIP, cơ sở hạ tầng là các mạng IP. Giao thức truyền tải thời gian thực RTP kết hợp với UDP và IP giúp truyền tải thông tin thoại qua mạng IP. RTP chạy trên UDP, còn UDP hoạt động trên IP hình thành lên cơ chế truyền RTP/UDP/IP trong VoIP.

Trong các mạng IP, hiện tượng các gói IP thất lạc hoặc đến không theo thứ tự thường xuyên xảy ra. Cơ chế truyền TCP/IP khắc phục việc mất gói bằng cơ chế truyền lại không phù hợp với các ứng dụng thời gian thực vốn rất nhạy cảm với trễ. RTP với trường tem thời gian (timestamp) được dùng để bên thu nhận biết và xử lý các vấn đề như trễ, sự thay đổi độ trễ (jitter) và sự mất gói.

2.1.3.2 Lớp điều khiển cuộc gọi

Thực hiện chức năng báo hiệu, định hướng cuộc gọi trong VoIP. Sự phân tách giữa mặt phẳng báo hiệu và truyền tải đã được thực hiện ở PSTN với báo hiệu kênh chung SS7, nhưng ở đây nhấn mạnh một thực tế có nhiều chuẩn báo hiệu cho VoIP cùng tồn tại như H.323, SIP hay SGCP/MGCP. Các giao thức báo hiệu này có thể hoạt động cùng nhau, được ứng dụng để phù hợp với những nhu cầu cụ thể của mạng. Ngoài ra, lớp này còn cung cấp chức

năng truy nhập tới dịch vụ bên trên cũng như các giao diện lập trình mở để phát triển ứng dụng.

2.1.3.3 Lớp ứng dụng dịch vụ

Đảm nhiệm chức năng cung cấp dịch vụ trong mạng với cả dịch vụ cũ tương tự như trong PSTN và các dịch vụ mới thêm vào. Các giao diện mở cho phép các nhà cung cấp phần mềm độc lập phát triển ra nhiều ứng dụng mới. Đặc biệt là các ứng dụng dựa trên Web, các ứng dụng kết hợp giữa thoại và dữ liệu, các ứng dụng liên quan tới thương mại điện tử. Sự phân tách lớp dịch vụ làm cho các dịch vụ mới được triển khai nhanh chóng. Ngoài ra, các chức năng như quản lý, nhận thực cuộc gọi và chuyển đổi địa chỉ cũng được thực hiện ở lớp này.

Do các giao diện giữa các lớp là mở và tuân theo chuẩn, tạo ra nhiều sự lựa chọn khi xây dựng thiết kế mạng. Ví dụ, ứng với lớp cơ sở hạ tầng mạng ta có thể dùng các Router và Switch của hãng Cisco, điều khiển cuộc gọi thực hiện bằng các Gatekeeper của VocalTec và các dịch vụ được cung cấp bởi Server dịch vụ của Netspeak. Do đó mô hình trên không chỉ có giá trị về mặt lý thuyết.

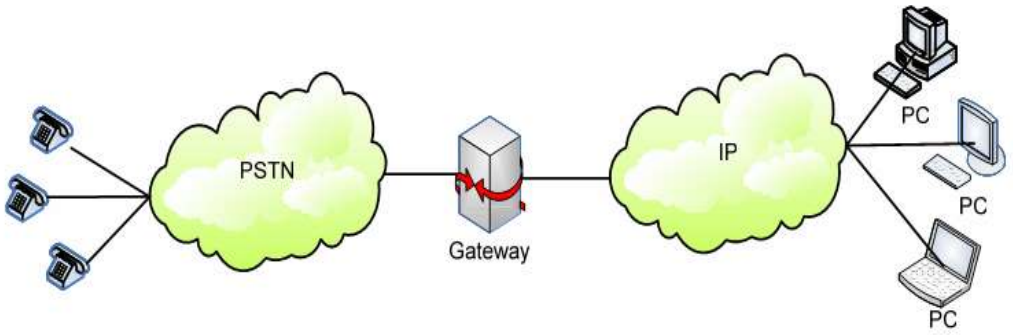
2.1.4 Các kiểu kết nối sử dụng VoIP

2.1.4.1 Computer to Computer

Hình 2.3 : Mô hình PC-PC

Với một kênh truyền internet có sẵn, là một dịch vụ miễn phí được sử dụng rộng khắp nơi trên thế giới. Chỉ cần người gọi (caller) và người nhận (receiver) sử dụng chung một VoIP service (skype, MSN, yahoo messenger…) 2 headphone + microphone, sound card. Cuộc hội thoại là không giới hạn. Và nó được áp dụng trong một tổ chức hay một công ty để thuận tiện cho việc liên lạc mà không cần nắp thêm tổng đài nội bộ.

2.1.4.2 Computer to phone



Hình 2.4: Mô hình PC to Phone

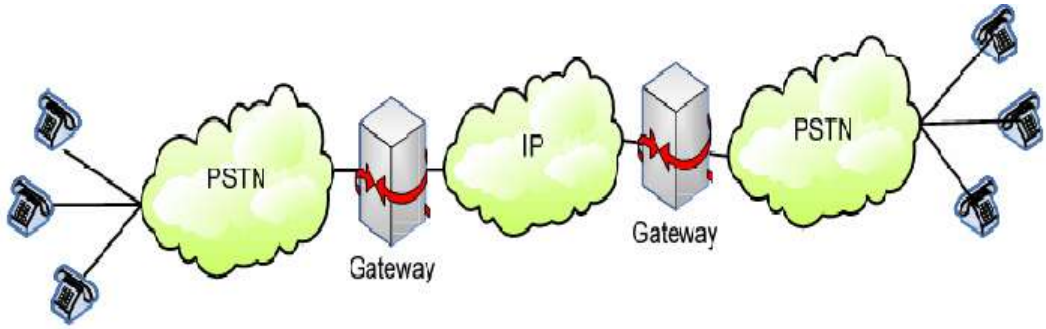
Trong mô hình này mạng Internet và mạng PSTN có thể giao tiếp với nhau nhờ một thiết bị đặc biệt đó là Gateway

Là một dịch vụ có phí. Bạn phải trả tiền để có một account + software. Với dịch vụ này một máy PC có kết nối tới một máy điện thoại thông thường ở bất cứ đâu (tùy thuộc vào phạm vi cho phép trong danh sách các quốc gia mà nhà cung cấp cho phép. Người gọi sẽ bị tính phí trên lưu lượng cuộc gọi và khấu trừ vào tài khoản hiện có.

Ưu điểm: Đối với các cuộc hội thoại quốc tế, người sử dụng sẽ tốn ít phí hơn một cuộc hội thoại thông qua hai máy điện thoại thông thường, chi phí rẻ và dễ nắp đặt.

Nhược điểm: chất lượng cuộc gọi phụ thuộc vào kết nối internet và service nhà cung cấp.

2.1.4.3 Phone to phone



Hình 2.5: Mô hình Phone to Phone

Là một dịch vụ có phí. Bạn không cần một kết nối internet mà chỉ cần một VoIP adapter kết nối với máy điện thoại. Lúc này máy điện thoại trở thành một IP phone.

Sử dụng Internet làm phương tiện liên lạc giữa các mạng PSTN. Tất cả

các mạng PSTN đều kết nối với mạng Internet thông qua các Gateway. Khi tiến hành cuộc gọi, mạng PSTN sẽ kết nối đến Gateway gần nhất, tại đây địa chỉ sẽ được chuyển đổi từ địa chỉ PSTN sang địa chỉ IP để có thể định tuyến các gói tin đến được mạng đích. Đồng thời Gateway nguồn có nhiệm vụ chuyển đổi tín hiệu thoại tương tự thành dạng số sau đó mã hóa, nén, đóng gói lại và gửi qua mạng. Mạng đích cũng được kết nối với Gateway và tại đó địa chỉ lại được chuyển đổi trở thành địa chỉ PSTN và tín hiệu được giải nén, giải mã, rồi chuyển đổi ngược lại thành tín hiệu tương tự gửi vào mạng PSTN đến đích.

2.2 Các giao thức trong VoIP

2.2.1 Giao Thức H.323

2.2.1.1 Tổng quan về giao thức H.323

H.323 là giao thức được phát triển bởi ITU-T. *H.323* ban đầu được sử dụng cho mục đích truyền các cuộc hội thoại đa phương tiện trên các mạng LAN, nhưng sau đó H.323 đã phát triển thành 1 giao thức truyền tải VoIP trên thế giới.

H.323 là một tập giao thức, gồm các giao thức chính:

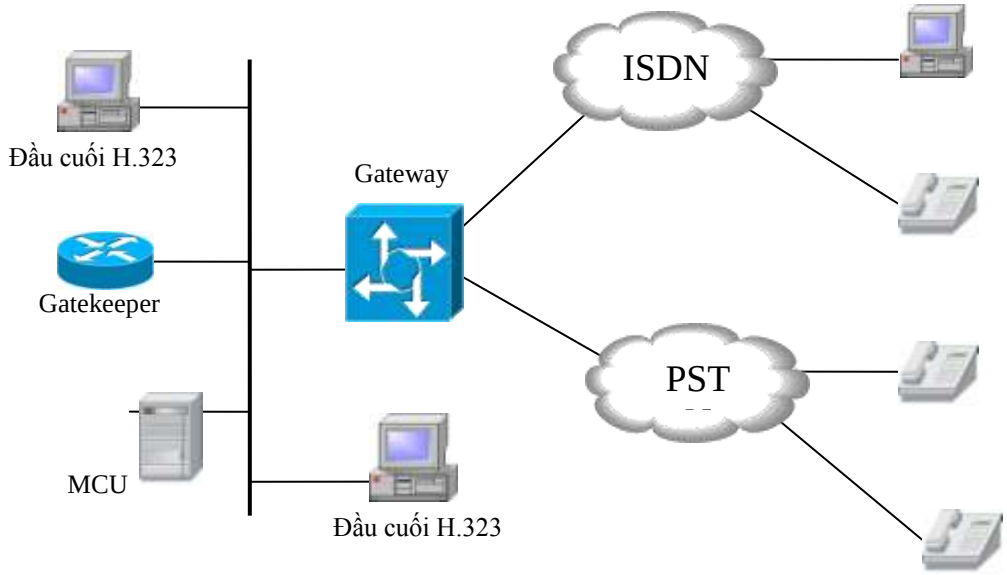
+ H.225: là giao thức báo hiệu thiết lập và giải tỏa cuộc gọi.

+ H.245: là giao thức điều khiển cho phép các đầu cuối thỏa hiệp kênh và trao đổi khả năng của chúng.

+ H.235: công cụ bảo mật hỗ trợ cho H.323.

2.2.1.2 Các thành phần chính trong mạng H.323

Tiêu chuẩn H.323 đề nghị một cấu trúc mà bao gồm **4** thành phần: *đầu cuối, Gateway, Gatekeeper, và đơn vị điều khiển đa điểm MCU (Multipoint Control Unit)*. Cấu trúc này được mô tả như trong hình sau:



Hình 2.6: Cấu trúc của H.323

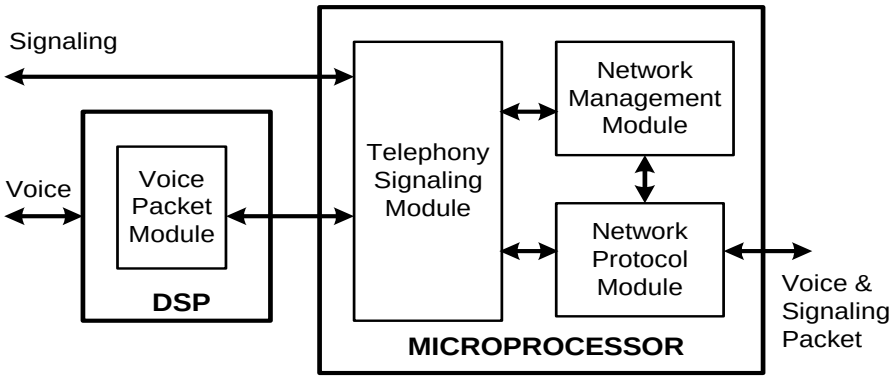
2.2.1.2.1 Đầu cuối (terminal)

Đây là một điểm cuối khác của LAN cung cấp thông tin thời gian thực, hai chiều. Tất cả các đầu cuối H.323 đều yêu cầu hỗ trợ H.245, H.225, Q.931, trạng thái công nhận đăng kí RAS (Registration Admission Status) và các giao thức truyền thời gian thực RTP (real-time transport protocol). H.245 được dùng để điều khiển việc sử dụng kênh, trong khi H.225 hoặc Q.931 được dùng cho báo hiệu cuộc gọi, thiết lập và xóa cuộc gọi.

RTP được dùng như là một giao thức truyền dẫn mang thông tin lưu thoại. RAS được sử dụng bởi điểm cuối để tương tác với gatekeeper. Một đầu cuối H.323 có thể truyền thông với một đầu cuối H.323 khác, một gateway H.323 hoặc một MCU.

2.2.1.2.2 Gateway

Là cầu nối giữa mạng H.323 với các mạng khác như SIP, PSTN,… Gateway đóng vai trò chuyển đổi các giao thức trong việc thiết lập và kết thúc các cuộc gọi, chuyển đổi các định dạng dữ liệu giữa các mạng khác nhau. Chức năng phần mềm của gateway được chia làm 4 module như hình dưới:



Hình 2.7: Kiến trúc phần mềm trong GK

- *Đóng gói thoại*(voice packet module): thực hiện chức năng nhận ra tín hiệu điện của thoại, loại bỏ tiếng vọng, loại bỏ jitter, nén thoại, đồng bộ đồng hồ và đóng gói thoại.

- *Báo hiệu điện thoại*(telephony signaling module): giao tiếp với điện thoại, chuyển các chỉ thị báo hiệu thành các thay đổi trạng thái mà giao thức mạng có thể hiểu được.

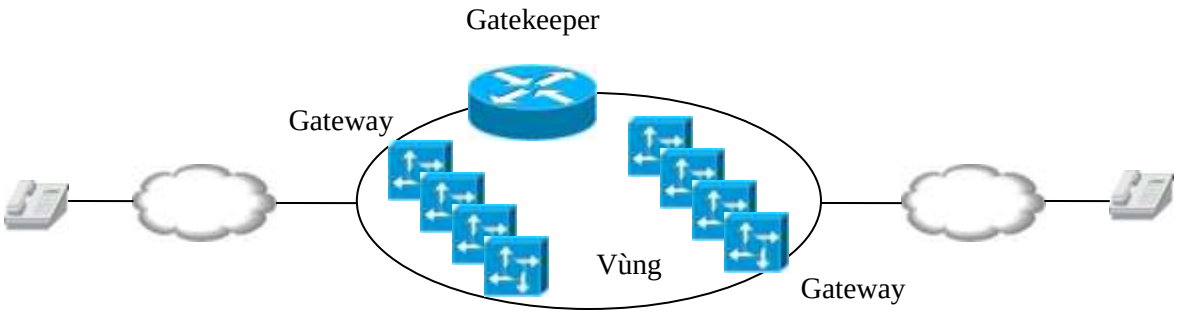
- *Giao thức mạng*(network protocol module): chuyển giao thức báo hiệu trong mạng điện thoại thành các giao thức báo hiệu trong mạng gói.

- *Quản lý mạng*(network management module): quản lý mạng bằng SNMP (Simple Network Management Protocol).

2.2.1.2.3 Gatekeeper

Đây là một thành phần quan trọng trong cấu trúc của H.323 và có chức năng quản lý. Nó là điểm chung tâm cho tất cả các cuộc gọi trong vùng của nó và cung cấp các dịch vụ tới các điểm cuối. Một vùng là sự tập hợp của gatekeeper và các điểm cuối. Nếu mạng tồn tại nhiều GK thì sẽ được thiết lập thành nhiều vùng và mỗi vùng sẽ do một GK quản lý. Việc thông tin giữa các GK sẽ được thực hiện thông qua các bản tin giao tiếp xác định vị trí đầu cuối trong quá trình thiết lập cuộc gọi. Tuy nhiên GK là một thành phần tùy chọn trong cấu trúc của H.323.

Cấu trúc vùng được quản lý bởi gatekeeper được trình bày trong hình sau:



Hình 2.8: Vùng gatekeeper

Nếu gatekeeper có mặt trong hệ thống H.323 thì nó thực hiện các nhiệm vụ sau:

Dịch địa chỉ: Cho phép dịch các quy ước, các ký hiệu, các địa chỉ "email" thành địa chỉ IP để thiết lập liên lạc IP.

Điều chỉnh công nhận (AC): sự truy cập của các đầu cuối có thể được chấp nhận hoặc từ chối dựa vào việc xác nhận địa chỉ nguồn hoặc địa chỉ đích thời gian hoặc bất kỳ biến số nào mà gatekeeper quản lý.

Quản lý cuộc gọi: Gatekeeper hoạt động như một điểm liên lạc ban đầu cho người gọi, cho hai Gateway hoặc cho hai điểm cuối báo hiệu trực tiếp cho nhau.

Quản lý băng thông: Gatekeeper có thể yêu cầu các đầu cuối và Gateway thay đổi các thông số truyền thông cuộc gọi để quản lý sử dụng băng thông.

Quản lý vùng: Gatekeeper có thể yêu cầu không quá một số lượng cuộc gọi nào đó qua kết nối có dải tần thấp để tránh giảm sút về chất lượng.

2.2.1.2.4 Đơn vị điều khiển đa điểm MCU

MCU là thiết bị hỗ trợ việc hội thoại đa điểm cho ba hoặc nhiều hơn ba đầu cuối trong mạng H.323. Một MCU gồm 2 phần: MC (Multipoint Controller) là thành phần bắt buộc và MP (Multipoint Processor) là thành phần tùy chọn.

Chức năng của MC là quyết định dung lượng chung của các kết cuối, có thể định vị đầu cuối, Gateway hoặc Gatekeeper.

MP nhận các luồng dữ liệu audio, video và phân phối chúng tới các điểm cuối tham dự vào kết nối đa điểm. MP có thể không cần đến nhưng sự vắng mặt của nó là một gánh nặng trên đầu cuối.

2.2.2 H.225

H.225 bao gồm các bản tin RAS và Q.931. Các bản tin RAS liên quan đến việc quản lý user, còn Q.931 mang phần báo hiệu cuộc gọi. Cả hai giao thức dùng kênh kết nối riêng là kênh RAS và kênh báo hiệu cuộc gọi.

2.2.2.1 Bản tin RAS(Registration, Admission, Status)

Chức năng chính của các bản tin RAS:

- EP(endpoint) phát hiện ra GK mà chúng sẽ phải đăng ký.
- EP đăng ký với GK của nó.
- EP phải yêu cầu sự cho phép của GK khi khởi tạo một cuộc gọi.
- EP yêu cầu giải phóng cuộc gọi.
- Trước khi ngắt kết nối với GK, EP phải ngắt đăng ký.

Bản tin RAS được gửi đi bằng giao thức vận chuyển UDP. EP và GK trao đổi thông tin trên kênh RAS theo dạng client-server.

Các bản tin RAS:

Bản tin RAS	Ý nghĩa
GRQ	Gatekeeper Request
GCF	Gatekeeper Confirm
GRJ	Gatekeeper Reject
RRQ	Registration Request
RCF	Registration Confirm
RRJ	Registration Reject
ARQ	Admission Request
ACF	Admission Confirm
ARJ	Admission Reject
DRQ	Disengage Request
DCF	Disengage Confirm
DRJ	Disengage Reject

Bảng 2- 1: Các bản tin RAS

2.2.2.2 Q.931

Q.931 là khuyến nghị của ITU-T cho báo hiệu cuộc gọi, làm chức năng thiết lập, duy trì và kết thúc cuộc gọi. Bản tin Q.931 được vận chuyển bằng giao thức TCP. EP sẽ thương lượng lắng nghe trên port nào. Quá trình thỏa thuận này được thực hiện bằng các bản tin RAS (trong call Admission), port 1720 thường được chọn.

Bản tin Q.931	Ý nghĩa
Setup	Bản tin đầu tiên trong quá trình khởi tạo cuộc gọi
CallProceeding	Không có thông tin thiết lập cuộc gọi nào nữa.
Alerting	Người bị gọi rung chuông
Connect	Kết thúc việc thiết lập cuộc gọi
Realease Complete	Kết thúc cuộc gọi

Bảng 2- 2: Các loại bản tin Q.931

2.2.3 H.245

H.245 là giao thức điều khiển báo hiệu cuộc gọi giữa các EP bao gồm năng lực trao đổi, xác định master-slave, quản lý kênh luận lý. Giao thức này được vận chuyển bằng TCP.

Xác định Master-slave: để tránh xung đột khi cả hai bên đều khởi tạo cùng một cuộc gọi. Đầu cuối thỏa thuận vai trò này bằng cách áp dụng theo một cách nào đó. Vai trò này sẽ giữ nguyên trong suốt cuộc gọi.

Trao đổi năng lực: mỗi đầu cuối phải biết được khả năng của nhau bao gồm khả năng truyền và nhận, nếu không nó có thể không chấp nhận cuộc gọi.

Quản lý kênh luận lý: đảm bảo cho đầu cuối có khả năng nhận và đọc được dữ liệu khi kênh luận lý mở. Bản tin *OpenLogicalChannel* sẽ mô tả loại dữ liệu sẽ truyền.

2.2.4 Các thủ tục báo hiệu trong mạng H.323

Người ta chia một cuộc gọi làm 5 giai đoạn gồm :

Giai đoạn 1: Thiết lập cuộc gọi

Giai đoạn 2: Thiết lập kênh điều khiển

Giai đoạn 3: Thiết lập kênh gọi ảo

Giai đoạn 4: Dịch vụ

Giai đoan 5: Kết thúc cuộc gọi

2.2.4.1 Thiết lập cuộc gọi

Việc thiết lập cuộc gọi sử dụng các bản tin được định nghĩa trong khuyến nghị H.225.0. Ta sẽ xem xét thủ tục thiết lập cuộc gọi trong 6 trường hợp sau:

- Cả hai thiết bị đầu cuối đều không đăng ký.
- Cả hai thuê bao đều đăng ký tới một GK.
- Chỉ có thuê bao chủ gọi có đăng ký với GK.
- Chỉ có thuê bao bị gọi có đăng ký với GK.
- Hai thuê bao đăng ký với hai GK khác nhau.
- Thiết lập cuộc gọi qua Gateway.

2.2.4.2 Thiết lập kênh điều khiển

Khi kết thúc giai đoạn 1 tức là cả chủ gọi lẫn bị gọi đã hoàn thành việc trao đổi các bản tin thiết lập cuộc gọi, thì các đầu cuối sẽ thiết lập kênh điều khiển H.245:

Bản tin đầu tiên được trao đổi giữa các đầu cuối là *terminal CapabilitySet* để các bên thông báo cho nhau khả năng làm việc của mình (chế độ mã hoá, truyền, nhận và giải mã các tín hiệu đa dịch vụ).

Kênh điều khiển này có thể do thuê bao bị gọi thiết lập sau khi nó nhận được bản tin *Set-up* hoặc do thuê bao chủ gọi thiết lập khi nó nhận được bản tin *Alerting* hoặc *Call Proceeding*. Trong trường hợp không nhận được bản tin *Connec*t hoặc một đầu cuối gởi *Release Complete*, thì kênh điều khiển H.245 sẽ được giải phóng.

2.2.4.3 Thiết lập kênh truyền thông

Sau khi trao đổi khả năng (tốc độ nhận tối đa, phương thức mã hoá…) và xác định quan hệ master-slave trong giao tiếp ở giai đoạn 2, thủ tục điều khiển kênh H.245 sẽ thực hiện việc mở kênh logic để truyền dữ liệu. Các kênh này là kênh H.225.

Sau khi mở kênh logic để truyền tín hiệu là âm thanh và hình ảnh thì mỗi đầu cuối truyền tín hiệu sẽ truyền đi một bản tin h2250 MaximumSkew Indication để xác định thông số truyền.

2.2.4.4 Dịch vụ cuộc gọi

Có một số dịch vụ cuộc gọi được thực hiện trên mạng H.323 như: thay đổi độ rộng băng tần, giám sát trạng thái hoạt động, hội nghị đặc biệt, các dịch vụ bổ sung. Dưới đây là hai loại dịch vụ điển hình: hay đổi độ rộng băng tần và giám sát trạng thái hoạt động.

2.2.4.5 Kết thúc cuộc gọi

Một thiết bị đầu cuối có thể kết thúc cuộc gọi theo các bước của thủ tục sau:

+ Dừng truyền luồng tín hiệu video khi kết thúc truyền hình ảnh, sau đó giải phóng tất cả các kênh logic phục vụ truyền video.

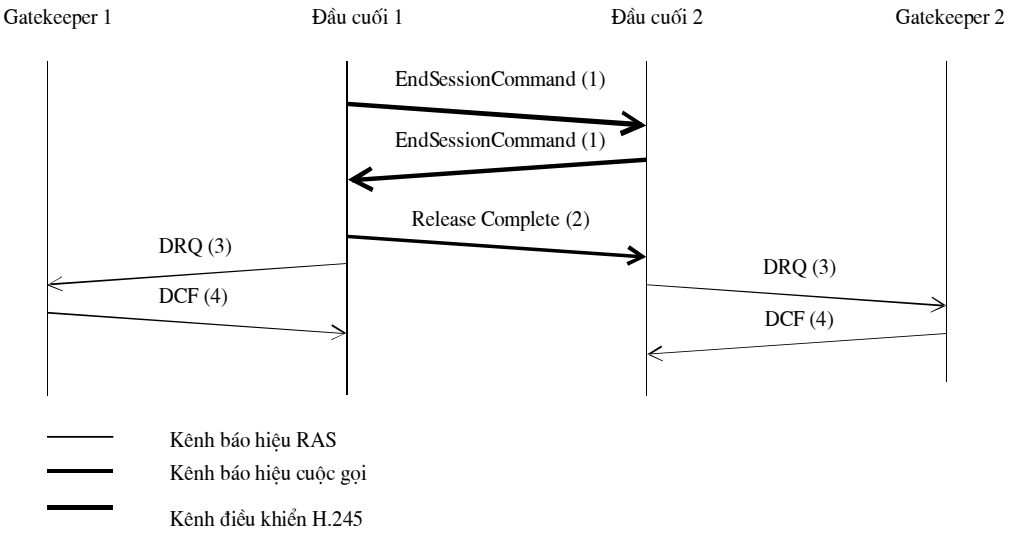
+ Dừng truyền dữ liệu và đóng tất cả các kênh logic dùng để truyền dữ liệu.

+ Dừng truyền audio sau đó đóng tất cả các kênh logic dùng để truyền audio.

Truyền bản tin H.245 *end Session Command* trên kênh điều khiển H.245 để báo cho thuê báo đầu kia biết nó muốn kết thúc cuộc gọi. Sau đó nó dừng truyền các bản tin H.245 và đóng kênh điều khiển H.245. Nó sẽ chờ nhận bản tin *end Session Command* từ thuê bao đầu kia và sẽ đóng kênh điều khiển H.245. Nếu kênh báo hiệu cuộc gọi đang mở, thì nó sẽ truyền đi bản tin ReleaseComplete sau đó đóng kênh báo hiệu.

Nó có thể kết thúc cuộc gọi theo các thủ tục sau đây: Một đầu cuối nhận bản tin *end Session Command* mà trước đó nó không truyền đi bản tin này, thì nó sẽ lần lượt thực hiện các bước từ 1 đến 6 ở trên chỉ bỏ qua bước 5.

Chú ý: Kết thúc một cuộc gọi không có nghĩa là kết thúc một hội nghị (cuộc gọi có nhiều đầu cuối tham gia). Một hội nghị sẽ chắc chắn kết thúc khi sử dụng bản tin H.245 *drop Conference*. Khi đó các đầu cuối sẽ chờ MC kết thúc cuộc gọi theo thủ tục trên.



Chú ý: Gatekeeper 1 và Gatekeeper 2 có thể là một Gatekeeper

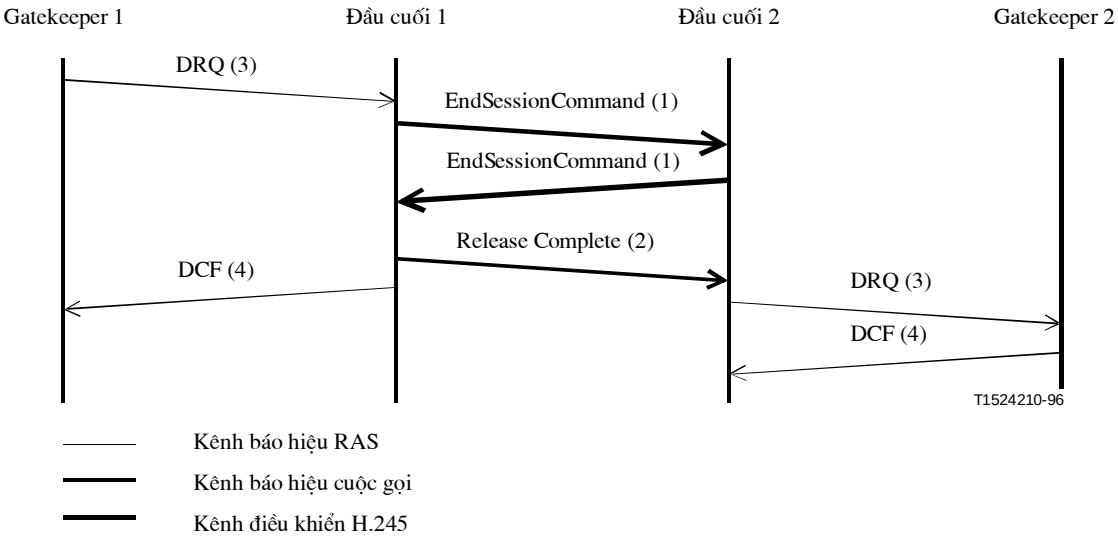
Hình 2.9: Kết thúc cuộc gọi có sự tham gia của GK

Thiết bị đầu cuối kết thúc cuộc gọi có sự tham gia của GK.

Trong một cuộc gọi không có sự tham gia của GK thì chỉ cần thực hiện các bước 1 đến 6. Trong cuộc gọi có sự tham gia của GK thì cần có hoạt động giải phóng băng tần. Vì vậy, sau khi thực hiện các bước từ 1 đến 6, mỗi đầu cuối sẽ truyền đi bản tin DRQ(3) tới GK. Sau đó, GK sẽ trả lời bằng bản tin DCF(4). Sau khi gởi DRQ, đầu cuối sẽ không gởi bản tin IRR tới GK nữa và khi đó cuộc gọi kết thúc.

Thủ tục kết thúc cuộc gọi do GK thực hiện.

Đầu tiên, GK gởi bản tin DRQ tới đầu cuối. Khi nhận được bản tin này, đầu cuối sẽ lần lượt thực hiện các bước từ 1 đến 6, sau đó trả lời GK bằng bản tin DCF. Thuê bao đầu kia khi nhận được bản tin endSessionCommand sẽ thực hiện thủ tục giải phóng cuộc gọi giống trường hợp đầu cuối chủ động kết thúc cuộc gọi. Nếu cuộc gọi là một hội nghị thì GK sẽ gởi DRQ tới tất cả các đầu cuối tham gia hội nghị.



Chú ý: Gatekeeper 1 và Gatekeeper 2 có thể là một Gatekeeper

Hình 2.10: Kết thúc cuộc gọi bắt đầu từ GK

2.2.5 Giao thức SIP

2.2.5.1 Tổng Quan

Giao thức SIP (Session Initiation Protocol) là một giao thức điều khiển và được tiêu chuẩn hóa bởi IETF. Nhiệm vụ của nó là thiết lập, hiệu chỉnh và xóa các phiên làm việc giữa các người dùng. Các phiên làm việc cũng có thể là hội nghị đa phương tiện, cuộc gọi điện thoại điểm-điểm SIP được sử dụng kết hợp với các chuẩn giao thức IETF khác như SAP, SDP và MGCP để cung cấp một lĩnh vực rộng hơn cho các dịch vụ VoIP. Cấu trúc của SIP cũng tương tự như cấu trúc của HTTP (giao thức client-server). Nó bao gồm các yêu cầu được gửi đến từ người sử dụng SIP client đến SIP server. Server sử lý các yêu cầu và đáp ứng đến các client. Một thông điệp yêu cầu cùng với thông điệp đáp ứng tạo nên sự thực thi SIP.

SIP là một công cụ hỗ trợ hấp dẫn đối với điện thoại IP với các lí do sau:

+ Nó có thể hoạt động vô trạng thái hoặc có trạng thái. Vì vậy sự hoạt động vô trạng thái cung cấp sự mở rộng tốt do các server không phải duy trì thông tin về trạng thái cuộc gọi một khi sự thực hiện đã được xử lý.

+ Nó có thể sử dụng nhiều dạng hoặc cú pháp giao thức chuyển siêu văn bản HTTP. Vì vậy, nó cung cấp một cách thuận lợi để hoạt động trên các trình duyệt.

+ Bản tin SIP thì không rõ ràng, nó có thể là bất cứ cú pháp nào. Vì vậy, nó có thể được mô tả theo nhiều cách. Chẳng hạn, nó có thể được mô tả với sự mở rộng thư internet đa mục đính MIME (Multipurpose Internet Mail Extension) hoặc ngôn ngữ đánh dấu mở rộng XML (Extensible Markup Language).

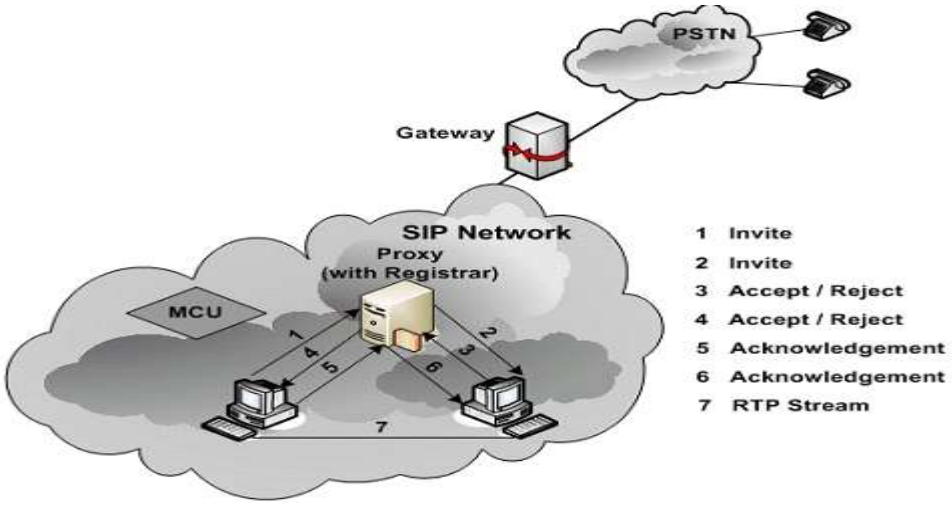
+ Nó nhận dạng một người dùng với bộ định vị tài nguyên đồng nhất URL(Uniform Resource Locator), vì vậy nó cung cấp cho người dùng khả năng khởi tạo cuộc gọi bằng cách nhập vào một liên kết trên trang web.

Nói chung, SIP hỗ trợ các hoạt động chính sau:

- Định vị trí của người dùng.
- Định media cho phiên làm việc.
- Định sự sẵn sàng của người dùng để tham gia vào một phiên làm việc.
- Thiết lập cuộc gọi, chuyển cuộc gọi và kết thúc.

2.2.5.2 Cấu trúc của giao thức SIP

Một khía cạch khác biệt của SIP đối với các giao thức xử lý cuộc gọi IP khác là nó không sử dụng bộ điều khiển Gateway. Nó không dùng khái niệm Gatway/bộ điều khiển Gateway nhưng nó dựa vào mô hình khách chủ(client/server).



Hình 2.11: Kiến trúc báo hiệu SIP và thủ tục báo hiệu

Server: Là một chương trình ứng dụng chấp nhận các bản tin yêu cầu để phục vụ các yêu cầu này và gửi trả các đáp ứng cho các yêu cầu đó. Server là Proxy, Redirect, UA hoặc Registrar.

Proxy server: là một chương trình trung gian, hoạt động như là một server và một client cho mục đính tạo các yêu cầu thay mặt cho các client khác. Các yêu cầu được phục vụ bên trong hoặc truyền chúng đến server khác. Một proxy có thể dịch và nếu cần thiết, có thể tạo lại bản tin yêu cầu SIP trước khi chuyển chúng đến server khác hoặc một UA

Redirect server: là một server chấp nhận một yêu cầu SIP, ánh xạ địa chỉ trong yêu cầu thành một địa chỉ mới và trả lại địa chỉ này về client. Không giống như proxy server, nó không khởi tạo một yêu cầu SIP và không chuyển các yêu cầu đến các server khác. Không giống như server đại diện người dùng USA, nó không chấp nhận cuộc gọi.

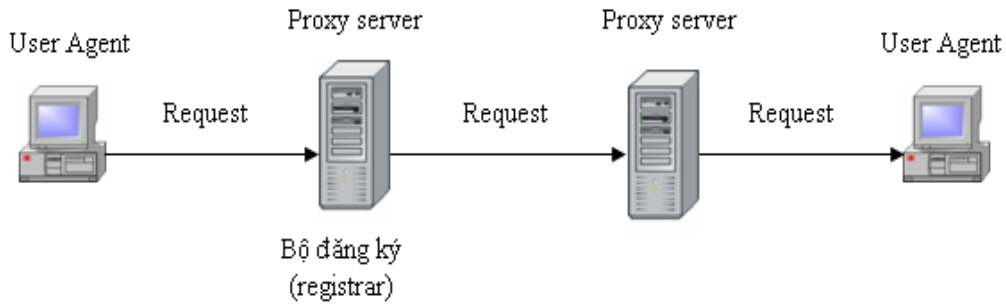
Registrar: là một server chấp nhận yêu cầu register. Một Registrar được xếp đặt với một Proxy hoặc một server gửi lại và có thể đưa ra các dịch vụ định vị. Registrar được dùng đằng kí các đối tượng SIP trong miền SIP và cập nhật vị trí hiện tại của chúng. Một miền SIP thì tương tự với một vùng H.323.

UA (User Agent): là một ứng dụng chứa cả UAC (user agent client) và UAS (user agent server).

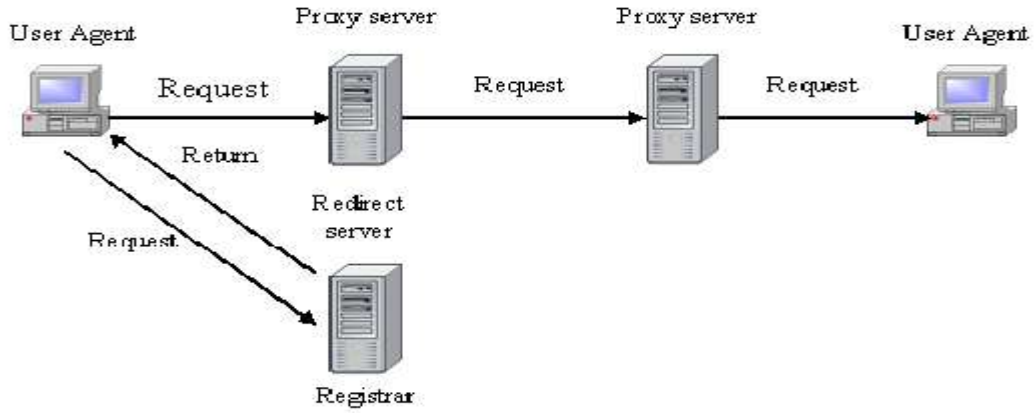
- UAC: là phần người sử dụng được dùng để khởi tạo một yêu cầu SIP tới Server SIP hoặc tới UAS.

- UAS: là một ứng dụng server gio tiếp với người dùng khi yêu cầu SIP được nhận và trả lại một đáp ứng đại diện cho người dùng.

Server SIP có hai loại: *Proxy server* và *Redirect server*. Proxy server nhận một yêu cầu từ client và quyết định server kế tiếp mà yêu cầu sẽ đi đến. Proxy này có thể gửi yêu cầu đến một server khác một Redirect hoặc UAS. Đáp ứng sẽ được truyền cùng đường với yêu cầu nhưng theo chiều ngược lại. Proxy server hoạt động như là một client và server. Redirect sẽ không chuyển yêu cầu nhưng sẽ chỉ định client tiếp xúc trực tiếp với server kế tiếp, đáp ứng gửi lại client chứa chỉ định của server kế tiếp. Nó không hoạt động được như là một client, nó không chấp nhận cuộc gọi.



Hình 1-11(a). Proxy Server



Hình 1-11(b). Redirect Server

2.2.5.3 SDP (Session Description Protocol)

Là giao thức cho phép client chia sẻ thông tin về phiên kết nối cho các client khác. Nó đóng một vai trò quan trọng trong VoIP.

Mô tả SDP:

SDP không phải là một giao thức lớp vận chuyển, nó không thực sự vận chuyển dữ liệu giữa các client mà nó chỉ thiết lập cấu trúc thông tin về các thuộc tính của luồng dữ liệu, dữ liệu thực sự được truyền đi bởi các giao thức SIP, RTSP hay HTTP.

Thông tin trong gói SDP ở dạng ASCII gồm nhiều dòng, mỗi dòng là 1 trường. Ví dụ bản tin SDP:

```
v=0
o=bsmith 2208988800 2208988800 IN IP4 68.33.152.147
s=
e=bsmith@foo.com
c=IN IP4 20.1.25.50
```

t=0 0

a=recvonly

m=audio 0 RTP/AVP 0 1 101

a=rtpmap:0 PCMU/8000

Trường	Ý nghĩa
V	*Phiên bản của giao thức*
O	*Chủ của phiên kết nối, nhận dạng, phiên bản phiên kết nối, Loại mạng, Loại địa chỉ, IP của chủ.*
S	*Tên phiên kết nối*
I	*Miêu tả kết nối*
U	*URI*
E	*E-mail của người cần liên lạc*
P	*Số điện thoại của người cần liên lạc*
C	*Thông tin kết nối:: IP version and CIDR IP address*
k	*Khóa mã hóa như clear text,base64, uri*
m	*Loại mạng, port kết nối,phương thức vận chuyển,danh sách định dạng*
t	*Thời điểm bắt đầu và kết thúc kết nối*
a	*Thuộc tính.*

Bảng 2-3: Ý nghĩa của các trường

Hoạt động của SDP:

Client gửi SIP request, thiết bị sẽ tạo một gói SDP gửi trả lại. Gói SDP này mang thông tin về phiên kết nối. Sau đây là một ví dụ:

v=0

o=alice 2890844526 2890844526 IN IP4 host.atlanta.example.com

s=

c=IN IP4 host.atlanta.example.com

t=0 0

m=audio 49170 RTP/AVP 0 8 97

a=rtpmap:0 PCMU/8000

a=rtpmap:8 PCMA/8000

a=rtpmap:97 iLBC/8000
m=video 51372 RTP/AVP 31 32
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000

Trong ví dụ trên, người gửi là Alice, lắng nghe kết nối từ host. atlanta. Example .com. Gói được gửi tới bất kỳ ai muốn tham gia phiên kết nối. Kết nối của Alice hỗ trợ ba loại kết nối cho audio là PCMU, PCMIA và iLBC, hai loại kết nối video H.261 và MPV. Nếu Bob muốn tham gia kết nối thì gửi lại bản tin SDP:

v=0
o=bob 2808844564 2808844564 IN IP4 host.biloxi.example.com
s=
c=IN IP4 host.biloxi.example.com
t=0 0
m=audio 49174 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=video 49170 RTP/AVP 32
a=rtpmap:32 MPV/90000

Bảo mật cho SDP:

Bản tin SDP mang thông tin về phiên kết nối như nhận dạng phiên kết nối, IP người gửi, người nhận,… Nếu kẻ tấn công bắt được những gói SDP này nó có thể thay đổi giá trị trong các trường rồi gửi đi. Nhưng điều này hoàn toàn có thể khắc phục bằng phương pháp chứng thực user của SIP.

2.2.5.4 Các bản tin của SIP

Có hai loại bản tin SIP: bản tin yêu cầu được khởi tạo từ client và bản tin đáp ứng được trả lại từ server. Mỗi bản tin chứa một tiêu đề mô tả chi tiết về sự truyền thông.

Một bản tin cơ bản gồm: dòng bắt đầu (start-line), một hoặc nhiều trường tiêu đề, một dòng trống (CRLF) dùng để kết thúc các trường tiêu đề và một nội dung bản tin tùy chọn.

Bản tin chung = Dòng bắt đầu
Tiêu đề bản tin
CRLF
[Nội dung bản tin]

2.2.5.4.1 Tiêu đề bản tin

Dùng để chỉ ra người gọi, người bi gọi, đường định tuyến và loại bản tin của cuộc gọi. Có bốn nhóm bản tin như sau:

Tiêu đề chung: áp dụng cho các yêu cầu và các đáp ứng.

Tiêu đề thực thể: định nghĩa thông tin về loại bản tin và chiều dài.

Tiêu đề yêu cầu: cho phép client thêm vào các thông tin yêu cầu.

Tiêu đề đáp ứng: cho phép server thêm vào các thông tin đáp ứng.

Các tiêu đề này được liệt kê trong bảng dưới đây:

Tiêu đề chung	**Tiêu đề thực thể**	**Tiêu đề yêu cầu**	**Tiêu đề đáp ứng**
Accept	Content-Encoding	Authorization	Allow
Accept-Encoding	Content-Length	Contact	Proxy-Authenticate
Accept-Language	Content-Type	Hide	Retry-After
Call-ID		Max-Forwards	Server
Contact		Organization	Unsupported
CSeq		Priority	Warning
Date		Proxy-Authorization	www-Authenticate
Encryption		Proxy-Require	
Expires		Route	
From		Require	
Record-Route		Response-Key	
Timestamp		Subject	
To		User-Agent	
Via			

Bảng 2-4: Tiêu đề của SIP

Giải thích một số tiêu đề chính của SIP theo bảng dưới:

Tiêu đề	Giải thích
Call-ID	So khớp các yêu cầu với các đáp ứng tương ứng, nhận dạng duy nhất lời mời hoặc sự đăng ký của client.
Cseq	Trong một cuộc gọi, Cseq tăng lên khi một yêu cầu mới được gửi đi và bắt đầu ở một giá trị ngẫu nhiên. Tuy nhiên, đối với yêu cầu ACK và Cancel thì Cseq không tăng.
To	Có mặt trong tất cả các yêu cầu và đáp ứng để chỉ ra nơi nhận yêu cầu.
From	Có mặt trong tất cả các yêu cầu và đáp ứng chứa tên và địa chỉ của nơi khởi tạo yêu cầu.
Via	Ghi lại đường đi của yêu cầu để cho phép các server SIP trung gian chuyển các câu trả lời trở lại cùng đường đi.
Encryption	Chỉ định nội dung và một số tiêu đề bản tin đã được mã hóa như thế nào.
Content-Length	Chỉ ra kích thước của nội dung bản tin (tính bằng octet).
Content-Type	Chỉ ra loại media của nội dung bản tin (văn bản/html, …).
Expires	Nhận dạng ngày và thời gian khi bản tin hết hạn.
Accept	Chỉ ra loại media nào được chấp nhận trong bản tin đáp ứng.
Subject	Cho thông tin về bản chất của cuộc gọi.

Bảng 2: Giải thích một số tiêu đề chính của SIP.

2.2.5.4.2 Bản tin yêu cầu.

Các yêu cầu cũng có thể được xem như các phương pháp (method) cho phép User agent và server mạng định vị, mời và quản lí các cuộc gọi. Bản tin yêu cầu SIP có dạng sau:

Yêu cầu = Dòng yêu cầu (Request-line)
Tiêu đề chung/tiêu đề yêu cầu/tiêu đề thực thể.
CRLF
[Nội dung bản tin]

Dòng yêu cầu bắt đầu bằng mã phương pháp, bộ nhận dạng tài nguyên đồng nhất yêu cầu, phiên bản giao thức SIP và kết thúc với CRLF. Các thành phần được phân các bởi ký tự SP.

Có 6 loại bản tin yêu cầu SIP: *INVITE, ACK, OPTIONS, BYE, CANCEL và REGISTER.*

INVITE: Bản tin *INVITE* chỉ ra người dùng hoặc dịch vụ đang được mời tham dự một phiên làm việc. Nội dung bản tin chứa sự mô tả phiên mà người bị gọi được mời. Đối với cuộc gọi hai người, người gọi chỉ ra loại media mà nó có thể nhận. Một đáp ứng thành công phải chứa trong nội dung bản tin của nó loại media nào mà người bị gọi mong muốn nhận. Với bản tin này, người dùng có thể nhận biết được khả năng của người dùng khác và mở ra một phiên hội thoại với số bản tin giới hạn.

ACK: Bản tin ACK xác nhận client đã nhận được đáp ứng sau cùng đối với bản tin INVITE (ACK chỉ được sử dụng với bản tin INVITE).

Nội dung bản tin ACK chứa sự mô tả phiên sau cùng được sử dụng bởi người bị gọi. Nếu nội dung bản tin ACK bị rỗng thì người bị gọi sử dụng sự mô tả phiên trong bản tin INVITE.

OPTIONS: Bản tin này cho phép truy vấn và thu thập User Agent và các khả năng của Server mạng. Tuy nhiên, bản tin này không được sử dụng để thiết lập phiên.

BYE: User Agent Client sử dụng bản tin BYE báo cho Server biết nó muốn giải phóng cuộc gọi. Bản tin BYE được chuyển giống như là bản tin INVITE và có thể được phát đi từ người gọi hoặc người bị gọi. Khi một đối tác nhận bản tin BYE thì nó phải ngừng việc truyền các luồng dữ liệu về hướng đối tác phát đi bản tin BYE.

CANCEL: Bản tin CANCEL cho phép User Agent và server mạng hủy bỏ bất cứ yêu cầu nào đang trong quá trình xử lý, nó không ảnh hưởng đến các yêu cầu đã hoàn thành mà các đáp ứng sau cùng đã nhận được.

RIGISTER: Bản tin này được sử dụng bởi client để đăng ký thông tin vị trí của nó với server SIP.

2.2.5.4.3 Đáp ứng bản tin

Các bản tin đáp ứng có dạng như sau:

Đáp ứng = Dòng trạng thái
Tiêu đề chung/tiêu đề đáp ứng/tiêu đề thực thể
CRLF
[Nội dung bản tin]

Dòng trạng thái bao gồm phiên bản của giao thức, mã trạng thái (số), lý do và CRLF. Các thành phần được cách nhau bằng hai ký tự SP.

Dòng trạng thái = SIP-version SP status-code SP Reason-Phrase CRLF

Mã trạng thái có 3 chứ số chỉ ra kết quả của việc đáp ứng yêu cầu. Lý do là sự mô tả ngắn gọn về mã trạng thái.

Chữ số đầu tiên của mã trạng thái định nghĩa lớp đáp ứng. SIP phiên bản 2.0 định nghĩa 6 giá trị cho lớp đáp ứng.

1xx: thông tin-các yêu cầu được nhận, xử lý các yêu cầu

2xx: thành công-hoạt động được nhận thành công và được chấp nhận.

3xx: đổi hướng (redirection) cần thêm một số hoạt động để hoàn thành yêu cầu.

4xx: lỗi client – yêu cầu bị sai lỗi cú pháp hoặc không thỏa mãn ở server.

5xx: lỗi server – server không thỏa mãn một yêu cầu đúng.

6xx: lỗi toàn cầu – yêu cầu không thể thỏa mãn ở bất kì server nào.

Mã số mã trạng thái được định nghĩa trong SIP phiên bản 2.0 được định nghĩa trong bảng dưới đây:

Lớp đáp ứng	Mã trạng thái	Giải thích
Thông tin	100	Đang cố gắng
	180	Rung chuông
	181	Cuộc gọi được chuyển
	182	Được xếp hàng đợi
Thành công	200	OK
Đổi hướng	300	Nhiều chọn lựa
	301	Được di chuyển thường xuyên
	302	Được di chuyển tạm thời
	380	Dịch vụ thay đổi
Lỗi client	400	Yêu cầu lỗi

	401	Không nhận thực được
	402	Yêu cầu trả tiền (payment required)
	403	Cấm
	404	Không tìm thấy
	405	Bản tin không cho phép
	406	Không chấp nhận
	407	Yêu cầu nhận thức proxy
	408	Yêu cầu timeout
	409	Xung đột
	410	Tiếp tục (gone)
	411	Yêu cầu chiều dài
	413	Thực thể yêu cầu quá lớn
	414	URL yêu cầu quá lớn
	415	Không hỗ trợ loại media
	420	Mở rộng sai
	480	Không sẵn có
	481	Cuộc gọi hoặc sự trao đổi không tồn tại
	482	Vòng lặp được phát hiện
	483	Quá nhiều hop
	484	Địa chỉ không hoàn thành
	485	Mơ hồ
	486	Đang bận
Lỗi Server	500	Lỗi server bên trong
	501	Không thực thi
	502	Gateway lỗi
	503	Dịch vụ không có sẵn
	504	Gateway timeout
	505	Phiên bản SIP không hỗ trợ
Lỗi toàn cầu	600	Bận ở mọi nơi
	603	Từ chối
	604	Không tồn tại ở mọi nơi
	606	Không chấp nhận

Bảng 2-5: Các đáp ứng của SIP

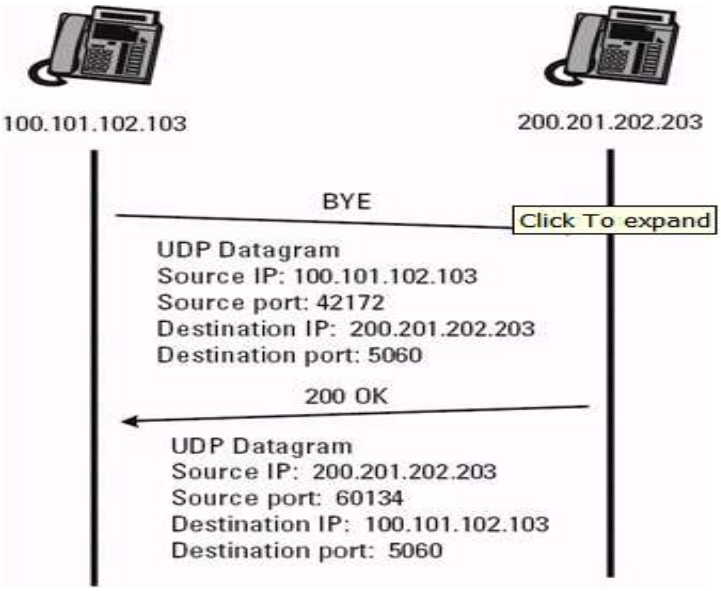
2.2.6 Các giao thức vận chuyển trong SIP.

SIP có thể sử dụng UDP và TCP. Khi được gửi trên UDP hoặc TCP, nhiều sự giao dịch SIP có thể được mang trên một kết nối TCP đơn lẻ hoặc gói dữ liệu UDP. Gói dữ liệu UDP (bao gồm tất cả các tiêu đề) thì không vượt quá đơn vị truyền dẫn lớn nhất MTU (Maximum Transmission Unit) nếu

MTU được định nghĩa hoặc không vượt quá 1500 byte nếu MTU không được định nghĩa.

2.2.6.1 UDP

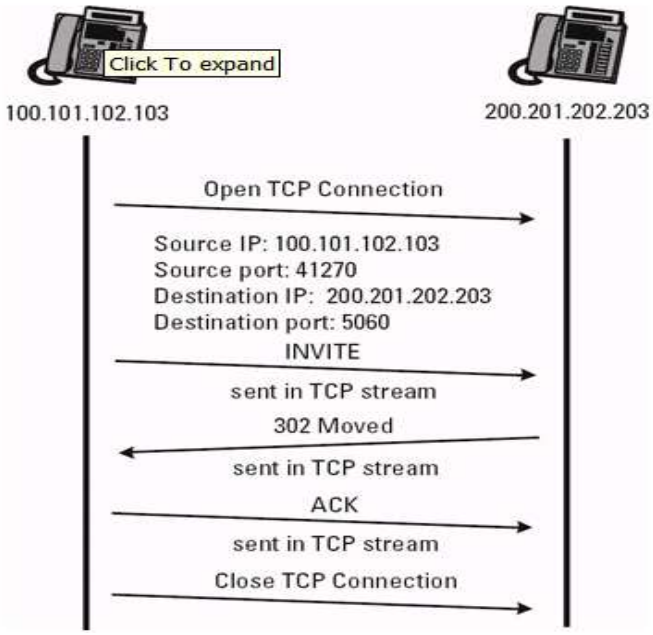
UDP là giao thức tầng vận chuyển không có điều khiển tắc nghẽn. Nó được dùng để vận chuyển bản tin SIP vì đơn giản và thích hợp với các ứng dụng thời gian thực. Các bản tin SIP thường có kích thước nhỏ hơn MTU (Message Transport Unit). Nếu bản tin lớn thì phải dùng TCP, vì lý do này mà SIP không có chức năng chia nhỏ gói.



Hình 2.12 (a): Trao đổi bản tin SIP bằng UDP

2.2.6.2 TCP

TCP là giao thức ở tầng vận chuyển đáng tin cậy do có điều khiển tắc nghẽn, hơn nữa nó có thể vận chuyển gói tin có kích thước bất kỳ. Nhược điểm của nó là tăng độ trễ.



Hình 2.12(b): Vận chuyển bản tin SIP bằng TCP

Để tăng cường tính bảo mật thì còn có những giao thức bổ sung để vận chuyển bản tin SIP như TLS, SRTP.

2.2.7 So sánh H.323 và SIP

SIP và H.323 được phát triển với những mục đích khác nhau bởi các tổ chức khác nhau. H.323 được phát triển bởi ITU-T từ theo PSTN, dùng mã hóa nhị phân và dùng lại một phần báo hiệu ISDN. SIP được IETF phát triển dựa trên mạng Internet, dùng một số giao thức và chức năng của mạng Internet.

Hệ thống mã hóa: SIP là giao thức text-based (text dạng ASCII) giống như HTTP trong khi đó H.323 dùng các bản tin mã hóa nhị phân. Mã hóa nhị phân giúp giảm kích thước bản tin nhưng nó phức tạp hơn dạng text bình thường. Ngược lại các bản tin text dễ dàng tạo ra, lưu lại, kiểm tra và không cần bất cứ một tool nào để biên dịch nó, điều này làm cho SIP thân thiện với môi trường Internet và các nhà phát triển web. Bản tin SIP có cấu trúc ABNF, (Augmented Backus-Naur Form) còn bản tin H.323 ASN.1 không có cấu trúc.

H.323 chỉ có chức năng báo hiệu, SIP có thêm khả năng thông tin về trạng thái của user (presense and Instant message) vì SIP sử dụng địa chỉ URI. Điều này là thế mạnh của SIP và hầu hết các dịch vụ ngày nay dùng SIP nhiều hơn so với H.323. SIP được hỗ trợ bởi thiết bị của các nhà cung cấp dich vụ và đang dần thay thế H.323. SIP cũng được các hãng di động sử dụng như giao thức báo hiệu cuộc gọi.

Tính cước: SIP muốn có thông tin tính cước phải ở trong quá trình báo hiệu cuộc gọi để phát hiện ra thời điểm kết thúc cuộc gọi. Còn với H.323, tại thời điểm khởi tạo và kết thúc cuộc gọi, các thông tin tính cước nằm trong các bản tin ARQ/DRQ. Với trường hợp cuộc gọi báo hiệu trực tiếp, EP thông báo cho GK thời điểm bắt đầu và kết thúc cuộc gọi bằng bản tin RAS.

Về mức độ bảo mật: SIP có nhiều hỗ trợ bảo mật đảm bảo mã hóa, chứng thực dùng certificate, toàn vẹn bản tin end-to-end. Bản thân SIP không phát triển những hỗ trợ này mà nó thừa hưởng từ các giao thức hỗ trợ bảo mật của Internet như TLS và S/MIME. Còn H.323 thì xây dựng H.235 cho chứng thực và mã hóa.

Các thiết bị SIP còn hạn chế về việc trao đổi khả năng. Còn các thiết bị trong mạng H.323 có khả năng trao đổi khả năng và thương lượng mở kênh nào (audio, thoại, video hay dữ liệu).

H.323 và SIP cùng tồn tại và có chức năng tương tự như nhau. SIP được hỗ trợ DNS và URL ngay từ đầu còn H.323 thì không. Tương tự như vậy H.323 hỗ trợ hội nghị truyền hình với khái niệm MCU ngay từ đầu thì với SIP tính năng đó được phát triển sau gọi là "focus".

SIP ban đầu dùng UDP, sau đó dùng TCP. Còn với H.323 thì ban đầu không dùng UDP nhưng bây giờ đã có hỗ trợ thêm UDP.

*Ưu điểm của từng giao thức**:***

H.323 dùng thay thế một phần trong hệ thống PSTN và chiếm lĩnh thị trường hội nghị truyền hình. Đối với những bộ phận chỉ dùng tính năng báo hiệu (thiết lập và kết thúc) cuộc gọi, không dùng hết những ưu điểm nổi trội của SIP thì không cần thay thế H.323 bằng SIP.

SIP hiện tại vẫn chưa hỗ trợ hội nghị truyền hình. Điểm mạnh của nó hiện tại vẫn là một giao thức đơn giản, dựa trên kiến trúc Internet.

2.2.8 Giao thức vận chuyển trong VoIP

Giao thức thời gian thực Real-time Protocol (RTP) được ra đời do tổ chức IETF đề xuất, nó đảm bảo cơ chế vận chuyển và giám sát phương thức truyền thông thời gian thực trên mạng IP. RTP có hai thành phần:

- Bản thân RTP mang chức năng vận chuyển, cung cấp các thông tin về các gói tin thoại.

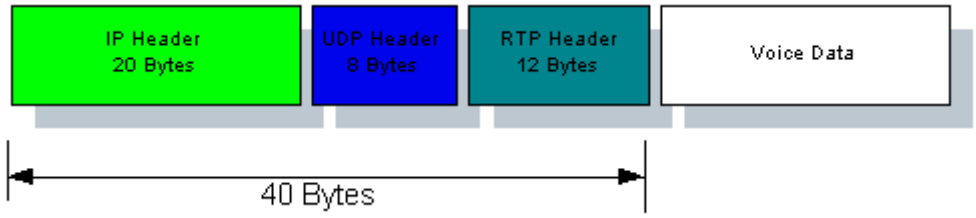
- Giao thức điều khiển thời gian thực RTCP (Real-time Control Protocol) mang chức năng giám sát và đánh giá chất lượng truyền tin.

2.2.8.1 RTP

Một cuộc thoại thông thường được chia thành các phiên báo hiệu cuộc gọi, điều khiển cuộc gọi, thỏa thuận phương thức truyền thông và phiên hội thoại. Vị trí của RTP nằm trong phiên hội thoại.

Cách thức truyền tiếng nói qua mạng IP: Qua phiên thoả thuận phương thức truyền thông, các bên tham gia hội thoại tiến hành mở hai cổng UDP kề nhau, cổng chẵn cho truyền tiếng nói (RTP), cổng lẻ cho truyền các thông tin trạng thái để giám sát (RTCP). Thông thường, hai cổng được chọn mặc định là 5004 và 5005.

Tại phía phát, tiếng nói được điều chế thành dạng số hoá, qua bộ CODEC được nén thành các gói tin để truyền đi. Khi đi xuống tầng UDP/IP, mỗi gói tin được gắn với một header tương ứng. Header này có kích thước 40 byte, cho biết địa chỉ IP nguồn, địa chỉ IP đích, cổng tương ứng, header RTP và các thông tin khác:



Hình 2.13: Gói RTP

Chẳng hạn như ta sử dụng G.723.1 thì mỗi payload có kích thước 24 byte, như vậy phần dữ liệu cho mỗi gói tin chỉ chiếm 37,5%.

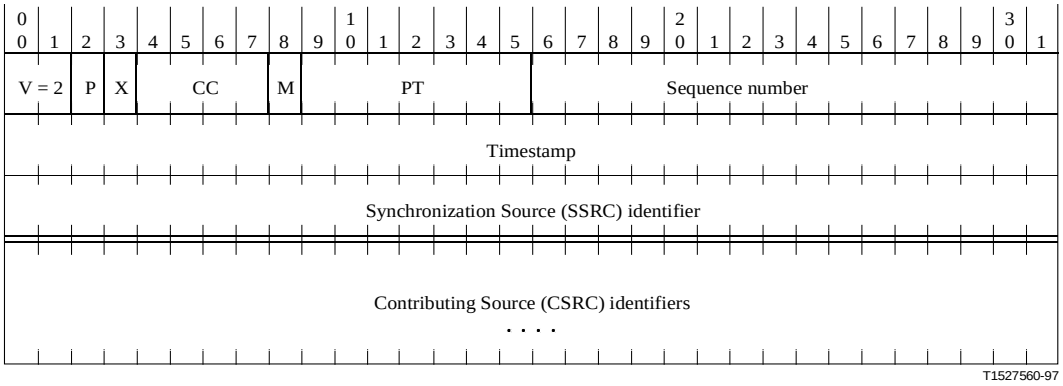
Header RTP cho biết phương thức mã hóa được sử dụng cho gói tin này, chỉ mục gói, nhãn thời gian của nó và các thông tin quan trọng khác. Từ các thông tin này ta có thể xác định ràng buộc giữa gói tin với thời gian.

Header RTP gồm 2 phần :

Phần cố định dài 12 byte.

Phần mở rộng để người sử dụng có thể đưa thêm các thông tin khác.

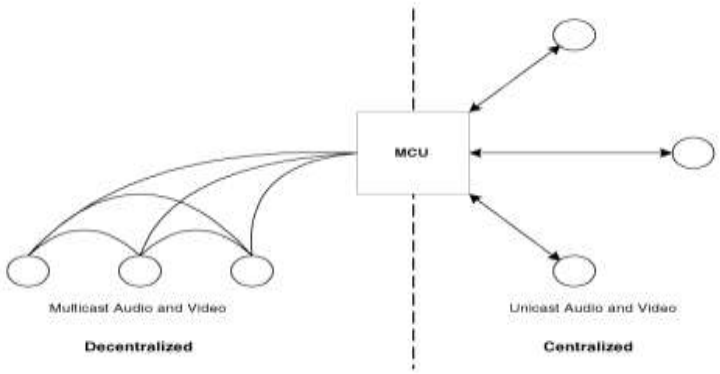
Header RTP cho mỗi gói tin có dạng :



Hình 2.14: Cấu trúc header của RTP

Các gói được sắp xếp lại theo đúng thứ tự thời gian thực ở bên nhận rồi được giải mã và phát lại.

RTP hỗ trợ hình thức hội thoại đa điểm một cách rất linh hoạt. Điều này hết sức quan trọng, đặc biệt trong trường hợp số thành viên tham gia hội thoại là nhỏ để tiết kiệm tài nguyên mạng. Đa phần hội thoại diễn ra dưới hình thức phát đa điểm. Nếu có yêu cầu phúc đáp giữa hai thành viên thì ta lựa chọn cách thức hội thoại đơn phát đáp.



Hình 2.15: Hội thoại đa điểm

RTP cho phép sử dụng các bộ trộn và bộ chuyển đổi. Bộ trộn là thiết bị nhận các luồng thông tin từ vài nguồn có tốc độ truyền khác nhau, trộn chúng lại với nhau và chuyển tiếp theo một tốc độ xác định ở đầu ra. Bộ chuyển đổi nhận một luồng thông tin ở đầu vào, chuyển đổi nó thành một khuôn dạng khác ở đầu ra. Các bộ chuyển đổi có ích cho sự thu nhỏ băng thông theo yêu cầu của dòng số liệu trước khi gửi vào kết nối băng thông hẹp hơn mà không cần yêu cầu nguồn phát RTP thu nhỏ tốc độ truyền tin của nó. Điều này cho phép các bên kết nối theo một liên kết nhanh mà vẫn đảm bảo truyền thông

chất lượng cao. Các bộ trộn cho phép giới hạn băng thông theo yêu cầu hội thoại.

2.2.8.2 RTCP

Từ các thông tin cung cấp trong RTP cho mỗi gói tin, ta có thể giám sát chất lượng truyền tiếng nói trong quá trình diễn ra hội thoại. RTCP phân tích và xử lý các thông tin này để tổng hợp thành các thông tin trạng thái rồi đưa ra các bản tin phản hồi đến tất cả các thành viên. Ta có thể để điều chỉnh tốc độ truyền số liệu nếu cần, trong khi các bên nhận khác có thể xác định xem vấn đề chất lượng dịch vụ là cục bộ hay toàn mạng. Đồng thời, nhà quản lý mạng có thể sử dụng các thông tin tổng hợp cho việc đánh giá và quản lý chất lượng dịch vụ trong mạng đó.

Ngoài ra, các bên tham gia có thể trao đổi các mục mô tả thành viên như tên, e-mail, số điện thoại và các thông tin khác.

Giao thức điều khiển thời gian thực Real-time Control Protocol (RTCP) có nhiệm vụ giám sát và đánh giá quá trình truyền tin dựa trên việc truyền một cách định kỳ các gói tin điều khiển tới các thành viên tham gia hội thoại với cùng cơ chế truyền dữ liệu. RTCP thi hành 4 chức năng chính :

Cung cấp cơ chế phản hồi chất lượng truyền dữ liệu. Bên gửi thống kê quá trình gửi dữ liệu qua bản tin người gửi cho các thành viên. Bên nhận cũng tiến hành gửi lại bản thống kê các thông tin nhận được qua bản tin người nhận. Từ việc giám sát quá trình gửi và nhận giữa các bên, ta có thể điều chỉnh lại các thông số cần thiết để tăng chất lượng cho cuộc gọi. Đây là chức năng quan trọng nhất của RTCP.

Mỗi nguồn cung cấp gói tin RTP được định danh bởi một tên CNAME (Canonical end-point identifer SDES item). RTCP có nhiệm vụ cho các thành viên biết tên này. Khi có thành viên mới tham gia hội thoại thì anh ta phải được gán với một trường CNAME trong gói tin SDES.

Quan sát số thành viên tham gia hội thoại thông qua sự thống kê ở các bản tin.

Mang các thông tin thiết lập cuộc gọi, các thông tin về người dùng. Đây là chức năng tùy chọn. Nó đặc biệt hữu ích với việc điều khiển các phiên lỏng, cho phép dễ dàng thêm bớt số thành viên tham gia hội thoại mà không cần có ràng buộc nào.

RTCP định nghĩa 5 loại gói tin như bảng dưới:

SR	Sender Report, bản tin người gửi
RR	Receiver Report, bản tin người nhận
SDES	Source Description items, các mục mô tả nguồn
BYE	Thông báo kết thúc hội thoại
APP	Cung cấp các chức năng riêng biệt của từng ứng dụng

Các thông tin được cung cấp gói tin RTCP cho phép mỗi thành viên tham gia hội thoại giám sát được chất lượng truyền tin, số gói tin đã gửi đi, số gói tin nhận được, tỷ lệ gói tin bị mất, trễ là bao nhiêu…Vì vậy, các thông tin này thường được cập nhật một cách định kỳ và chiếm không quá 5% giải thông cuộc gọi.

Như vậy không những RTP đáp ứng được yêu cầu thời gian thực cho việc truyền tiếng nói qua mạng IP mà còn cho phép ta giám sát và đánh giá chất lượng truyền tin cho VoIP. Có rất nhiều yếu tố ảnh hưởng tới chất lượng dịch vụ (Quality of Service-

QoS) cho VoIP nhưng chủ yếu là do 3 nguyên nhân trễ, tỷ lệ gói tin mất và Jitter. Tại mỗi thời điểm diễn ra hội thoại ta đều có thể quan sát và đánh giá các tham số này.

Tuy nhiên, bản thân RTP hoạt động trên tầng IP mà bản chất mạng IP là chuyển mạch gói, do vậy RTP không can thiệp được tới các nguyên nhân trên. Ta không thể điều khiển được chất lượng dịch vụ qua thoại trên IP mà chỉ giám sát và đánh giá qua việc sử dụng RTP. Biện pháp khắc phục hiện nay là sử dụng giao thức giữ trước tài nguyên Resource Reservation Protocol (RSVP) cho VoIP.

Chương 3:

BẢO MẬT TRONG VoIP

3.1 Vấn đề bảo mật trong VoIP

Chính vì VoIP dựa trên kết nối internet nên có thể có những điểm yếu đối với bất kì mối đe doạ và các vấn đề gì mà máy tính của bạn có thể đối mặt. Công nghệ này cũng là một công nghệ mới nên cũng có nhiều tranh cãi về những tấn công có thể xảy ra, VoIP cũng có thể bị tấn công bởi virut và mã nguy hiểm khác, các kẻ tấn công có thể chặn việc truyền thông, nghe trộm và thực hiện các tấn công giả mạo bằng việc thao túng ID và làm hỏng dịch vụ của bạn. Các hành động tiêu tốn lượng lớn các tài nguyên mạng như tải file, chơi trò chơi trực tuyến…cũng ảnh hưởng đến dịch vụ VoIP.

VoIP cũng chịu chung với các vấn đề bảo mật vốn có của mạng data. Những bộ giao thức mới dành riêng của VoIP ra đời cũng mang theo nhiều vấn đề khác về tính bảo mật.

Nghe nén cuộc gọi: nghe nén qua công nghệ VoIP càng có nguy cơ cao do có nhiều node chung gian trên đường truyền giữa hai người nghe và người nhận. Kẻ tấn công có thể nghe nén được cuộc gọi bằng cách tóm lấy các gói IP đang lưu thông qua các node trung gian. Có khá nhiều công cụ miễn phí và có phí kết hợp với các card mạng hỗ trợ chế độ pha tạp giúp thực hiện được các điều này.

Truy cập trái phép(unauthorized access attack): kẻ tấn công có thể xâm phạm các tài nguyên trên mạng do nguyên nhân chủ quan của các admin. Nếu các mật khẩu mặc định của các gateway và switch không được đổi thì kẻ tấn công có thể lợi dụng để xâm nhập. Các switch cũ vẫn còn dùng telnet để truy cập từ xa, và clear-text protocol có thể bị khai thác một khi kẻ tấn công có thể sniff được các gói tin. Với các gateway hay switch sử dụng giao diện web server cho việc điều khiển từ xa thì kẻ tấn công có thể tóm các dụng cụ kỹ thuật ARP để tóm lấy các gói tin đang lưu chuyển trong một mạng nội bộ.

Caller ID spoofing: caller ID là một dịch vụ cho phép uer có thể biết được số của người gọi đến. Caller ID spoofing là kỹ thuật mạo danh cho phép

thay đổi số ID của người gọi bằng những con số do uer đặt ra. So với mạng điện thoại truyền thông, thì việc giả mạo số điện thoại VoIP dễ hơn nhiều, bởi có khá nhiều công cụ và website cho phép thực hiện điều này.

Đặc điểm	Đặc tả
Cấu trúc IP	Điểm yếu này liên quan đến các hệ thống sử dụng mạng chuyển mạch gói, nó làm ảnh hướng đến cấu trúc hoạt động của VoIP
Hệ điều hành	Các thiết bị VoIP kế thừa các điểm yếu của hệ điều hành và các firmware mà chúng chạy trên đó (windows và linux)
Cấu hình	Cấu hình mặc định của thiết bị VoIP luôn có những dịch vụ dư thừa. và các port của các dịch vụ dư thừa này trở thành điểm yếu cho các tấn công Dos, tràn bộ đệm hoặc tránh sự xác thực
Mức ứng dụng	Các công nghệ mới còn non yếu có thể bị tấn công bẻ gãy hoặc mất điều khiển đối với các dịch vụ.

Bảng 3: Mô tả các cấp độ mà cấu trúc VoIP có thể bị tấn công

Ngoài những vấn đề trên, VoIP còn kế thừa những vấn đề chính trong việc định tuyến trên kết nối băng thông rộng. Không giống như các hệ thống điện thoại truyền thông bạn có thể gọi cả khi mất điện. Trong hệ thống VoIP, nếu mất nguồn điện thì VoIP cũng không thể thực hiện được cuộc gọi . Ở đây cũng có vài vấn đề liên quan đó là các hệ thống bảo mật ở nhà hoặc số khẩn cấp có thể không làm việc theo như mong muốn.

3.2 Nhu cầu bảo mật

Trước khi đi vào chi tiết về những công nghệ khác nhau để bảo vệ cho mạng VoIP. Bạn cần phải hiểu những vấn đề và tập hợp những nhu cầu mà bạn đã được thấy. Phần này sẽ phác thảo những nhu cầu bảo mật tiêu biểu. Không phải là một danh sách toàn diện. Những dịch vụ VoIP đặc biệt có thể cần những nhu cầu phụ:

Tính toàn vẹn : Người nhận nên nhận những gói dữ liệu của người khởi tạo gửi với nội dung không có sự thay đổi. Một bên thứ ba cần phải không có khả năng chỉnh sửa gói trong quá trình vận chuyển. Định nghĩa này được áp dụng một cách chính xác trong trường hợp của tín hiệu VoIP. Tuy nhiên,

trong trường hợp của phương tiện truyền thông, sự mất mát gói thông thường có thể tha thứ được.

Tính bí mật: Một hãng thứ ba không nên có khả năng để đọc dữ liệu mà được dự định cho người nhận.

Tính xác thực: Bên gửi và bên nhận tín hiệu VoIP hay thông điệp truyền thông nên chắc chắn rằng chúng đang liên lạc ngang hàng nhau.

Tính sẵn sàng: Sự bảo vệ từ việc tấn công DoS(từ chối dịch vụ) đối với thiết bị VoIP nên sẵn có đối với những người sử dụng liên tục. Những người sử dụng/những thiết bị có ác tâm hoặc có cư xử không đúng đắn không được cấp quyền để phá vỡ dịch vụ. Để làm dịu các cuộc tấn công DoS đòi hỏi cách xử lý lây nhiễm để bảo vệ tài nguyên VoIP và bảo vệ mạng IP bên dưới.

3.3 Một số cách tấn công chặn cuộc gọi

3.3.1 Tấn công Replay

Tấn công replay là tấn công chủ động hướng về nghi thức. Đặc trưng của người tấn công này giành được gói dữ liệu gởi hoặc nhận đến host. Anh ta sửa đổi chúng và sử dụng lại để truy cập vào một số dịch vụ nào đó. Một ví dụ tương ứng với loại thoại IP là người tấn công đạt được trong tay các gói dữ liệu gởi từ một user có quyền để thiết lập cuộc gọi và gởi lại chúng sau khi đã sửa đổi địa chỉ nguồn và IP. Nó có thể bị ngăn chặn bằng cách thực thi hai dịch vụ bảo mật nhận thực thực thể ngang hàng (peer entity authencation) và tính toàn vẹn dữ liệu (data intergrity).

3.3.2 Tấn công tràn bộ đệm

Đây là phương thức tấn công phổ biến. Đây là kết quả chính của việc phát triển phần mềm không đúng lúc. Kỹ thuật này lợi dụng trên thực tế là có một vài lệnh không kiểm tra đầu vào dữ liệu. Chúng được ứng dụng đặc biệt để xâu chuỗi xử lý các lệnh. Quá trình gia nhập với nhiều đầu vào, các lệnh hay là các chương trình có khả năng làm cho bộ nhớ hệ thống bị viết đè lên. Nội dung của bộ nhớ này có thể bắt đầu hoặc quay trở lại địa chỉ của các chương trình subroutine. Trường hợp xấu nhất người tấn công có thể thêm vào đoạn code hiểm để cung cấp cho anh ta các quyền quản lí của hệ thống. Biện pháp đối phó là huỷ tất cả các code "yếu", chính các lỗ hổng nhận thức được chứa trong các hệ thống hoạt động và các chương trình ngôn ngữ.

3.3.3 Tấn công man in the middle

Trong tấn công man in the middle người tấn công quản lý để cắt đứt kết nối giữa hai bên gọi. Cả hai bên tham gia kết nối này đều nghĩ rằng chúng truyền thông với nhau. Thực tế, tất cả các dữ liệu được định tuyến qua người tấn công. Hacker đã hoàn thành việc truy cập để thay thế các dữ liệu bên trong. Hacker có thể đọc chúng, thay đổi chúng hoặc và gửi chúng như là dữ liệu của anh ta. Thực tế hacker được xác định ở vị trí ở giữa của hai bên truyền thông mang lại cho người tấn công tên của hai bên truyền thông. Một ví dụ cho tấn công này là thiết lập của việc bảo đảm kết nối được sử dụng bởi bảo mật lớp dữ liệu. Điểm yếu của TLS là nguyên nhân của việc thiết lập phiên này. Ở đây hai bên truyền thông có thể trao đổi hai khóa. Khóa này được đổi có khả năng làm cho người tấn công có thể ở giữa hai bên truyền thông.

3.3.4 Chặn và đánh cắp cuộc gọi

Nghe trộm và đánh chặn cuộc gọi là vấn đề liên quan đến mạng VoIP, định nghĩa nghe lén có nghĩa là một người tấn công có thể giám sát toàn bộ báo hiệu hoặc dòng dữ liệu giữa hai hoặc nhiều đầu cuối VoIP, nhưng không thể biến đổi dữ liệu. Đánh cắp cuộc gọi thành công tương tự như việc nghe trộm trên dây nối, cuộc gọi của hai bên có thể bị đánh cắp, ghi lại, và nghe lại mà hai bên không hề biết. Rõ ràng người tấn công mà có thể đánh chặn và chứa dữ liệu này có thể sử dụng dữ liệu này cho mục đích khác phục vụ cho mục đích của anh ta.

3.3.5 Đầu độc DNS

Một hồ sơ DNS (Domain Name System) A được sử dụng cho việc chứa các domain hay hostname ánh xạ thành địa chỉ IP. SIP tạo ra việc sử dụng rộng rãi hồ sơ SRV để xác định các dịch vụ SIP như là SIP uỷ quyền và đăng nhập. Các hồ sơ SRV thường bắt đầu với gạch dưới (_sip.tcpserver.udp.domain.com) và chứa thông tin về miêu tả dịch vụ, vận chuyển, host, và thông tin khác. Các hồ sơ SRV cho phép người quản lý sử dụng một vài user cho một domain, để di chuyển dịch vụ từ host đến host với một ít quan trọng hoá, và để bổ nhiệm một vài host như là các server chính cho các dịch vụ.

Một người có mục đích tấn công, sẽ cố gắng đầu độc DNS hay tấn công giả mạo, sẽ thay thế giá trị lưu trữ hồ sơ DNS A, SSRV, hay NS với các bản tin mà chỉ đến các server của người tấn công. Điều này có thể được hoàn thành bằng cách bắt đầu bằng cách dời vùng từ DNS server của người tấn công đến DNS server nạn nhân, bằng cách yêu cầu server DNS nạn nhân phân tích thiết bị mạng trong domain của người tấn công. Server DNS nạn nhân không những chấp nhận yêu cầu hồ sơ mà còn chấp nhận và chứa các hồ sơ mà server tấn công có.

Vì vậy việc thêm vào hồ sơ A cho www.Attacker.com, server DNS nạn nhân có thể nhận được hồ sơ giả là www.yourbank.com. Nạn nhận vô tội sẽ bị hướng đến chuyển hướng lại đến attacker.com. Trang web mà bất mà bất kỳ thời điểm nào muốn truy cập là yourbank.com. Trang web mà hồ sơ giả được lưu trữ. SIP URL thay thế cho địa chỉ website, và vấn đề tương tự cũng gặp phải trong môi trường VoIP.

Các loại đe doạ này dựa vào sự vắng mặt của bảo đảm nhận thực của người tạo ra yêu cầu. Các tấn công trong loại này cố gắng tìm kiếm để phá hoại tính toàn vẹn của dữ liệu đàm thoại.Các thảm hoạ này chỉ ra rằng việc cần thiết phải bảo mật dịch vụ để có khả năng nhận thực thể tạo ra yêu cầu và để kiểm tra nội dung của thông điệp và điều khiển các luồng không bị biến đổi khi phát.

3.3.6 Đánh lừa (ARP Spoofing)

ARP là giao thức cơ sở Ethernet. Có lẽ do nguyên nhân này, thao tác vào các gói ARP là kỹ thuật tấn công thường thấy trong mạng VoIP. Một vài kỹ thuật hay công cụ hiện tại cho phép bất kỳ user nào có thể tìm ra lưu lượng mạng trên mạng bởi vì ARP không có điều khoản cho câu hỏi nhận thực và câu hỏi trả lời. Thêm vào đó, bởi vì ARP là một giao thức stateless, hầu hết các hệ thống hoạt động cập nhật cache của nó khi mà nhận một lời đáp ARP, bất chấp nó được gởi đi từ một yêu cầu thực tế hay không.

Trong số những tấn công này, chuyển hướng ARP, đánh lừa ARP, đánh cắp ARP và đầu độc cache ARP là các phương pháp để phá hoại quá trình ARP bình thường. Các dạng này thường xuyên được xen kẽ hoặc xáo trộn nhau. Dành cho mục đích của chương này, có thể xem đầu độc cache ARP và đánh lừa ARP như là cùng một quá trình. Sử dụng các công cụ tuỳ thích có

thể như là ettercap, Cain, và dsnif, và các thiết bị IP có hại có thể đánh lừa thiết bị IP thông thường bằng cách gởi một đáp ứng ARP không yêu cầu đến host mục tiêu. Một đáp ứng ARP giả chứa địa chỉ phần cứng của thiết bị bình thường và địa chỉ IP của thiết bị có ý đồ xấu. Ned là máy tính tấn công. Khi SAM broadcast một câu hỏi ARP cho địa chỉ IP của Sally, NED, người tấn công, đáp ứng câu hỏi để chỉ ra rằng địa chỉ IP (10.1.1.2) liên quan đến địa chỉ MAC của Ned, BA:AD:BA:AD. Các gói giả sử gửi từ SAM đến Sally sẽ được thay thế gởi đến Ned. Sam sẽ hiểu lầm rằng địa chỉ MAC của Ned tương ứng với địa chỉ IP của Sally. Thực tế, Ned có thể đầu độc cache ARP của Sam mà không cần đợi một yêu cầu ARP từ hệ thống Windows (9x/NT/2k), các mục ARP tĩnh được viết đè lên khi một trả lời câu hỏi được nhận bất chấp có hay không câu hỏi được phát. Mục này sẽ được giữ cho đến khi chúng hết hạn hoặc mục mới thay thế.

Chuyển hướng ARP có thể hoạt động hai chiều và thiết bị đánh lừa có thể đưa vào ở giữa của cuộc đàm thoại giữa hai thiết bị IP trên mạng chuyển mạch. Bằng cách định tuyến các gói trên các thiết bị được nhận các gói, việc gài vào này (được biết như là Man/Monkey/Moron trong việc tấn công ở giữa) có thể vẫn không được nhận ra cho một vài lần. Người tấn công có thể định tuyến các gói như mong muốn, dẫn đến như tấn công DoS.

Vì tất cả lưu lượng IP giữa người gởi thực và người nhận thực bây giờ đều đi qua thiết bị của người tấn công, thật bình thường để cho người tấn công tìm ra lưu lượng sử dụng các công cụ tuỳ thích như là Ethereal hay tcpdump. Bất kỳ thông tin nào không được mã hoá (bao gồm email, username và password, và lưu lượng web) có thể bị chặn đứng và bị xem.

Sự chặn đứng này có khả năng tác động mạnh đến lưu lượng VoIP. Các công cụ miễn phí như là vomit hay rtpsnif, cũng như là các công cụ công cộng như là VoIPCrack, cho phép chặn đứng và mã hoá lưu lượng VoIP. Các nội dụng chiếm được có thể bao gồm thoại, báo hiệu và thông tin tính cước, đa phương tiện, số PIN. Đàm thoại qua nội mạng IP có thể bị chặn và ghi âm lại sử dụng kỹ thuật này.

Ở đây cũng có một số biến thể của kỹ thuật kể trên. Thay cho việc phỏng theo các host, người tấn công có thể phỏng theo gateway. Điều này làm cho người tấn công có thể chặn đứng nhiều luồng gói. Tuy nhiên, hầu hết kỹ

thuật chuyển hướng dựa vào việc lén lút. Người tấn công trong các trường hợp này đều hy vọng việc không nhận ra của các user mà chúng mạo nhận. Mạo nhận gateway có thể có kết quả trong các user đề phòng sự có mặt của người tấn công xâm phạm bất ngờ trong mạng.

Trong các thủ tục giới hạn lỗi do thao tác ARP, người quản lí phải thực thi các công cụ phần mềm để giám sát việc ánh xạ địa chỉ IP thành địa chỉ MAC. Ở lớp mạng, ánh xạ địa chỉ MAC/IP có thể được mật mã tĩnh trên switch, tuy nhiên nó thường xuyên không được quản lý tốt.

Các rủi ro của việc mã hoá lưu lượng VoIP có thể được giới hạn bởi thực thi mật mã. Sử dụng việc mật mã hoá media, các cuộc đàm thoại giữa hai đầu cuối IP phải được sử dụng cùng một dạng mật mã hoá. Trong môi trường bảo mật cao thì các tổ chức cần phải đảm bảo cùng một phương thức mật mã trong bộ codec IP.

Tiếp theo là một vài ví dụ thêm vào của các đánh chặn hay ăn cắp cuộc gọi hay tín hiệu. Các đe doạ của lớp này khó thực hiện hoàn thành hơn là DoS, kết quả của nó có thể là dữ liệu bị mất hay bị thay đổi. Các tấn công DoS, là do nguyên nhân của các phương pháp hoạt động hay sơ xuất, nó làm ảnh hưởng đến chất lượng dịch vụ và thường gây sự không hài lòng đối với user và người quản trị mạng. Các tấn công đánh chặn và ăn cắp, thường là các tấn công chủ động với việc đánh cắp dịch vụ, thông tin, hoặc tiền như là mục tiêu tấn công. Cần chú ý rằng danh sách này không khái quát hết khía cạnh nhưng cũng bao gồm một vài tấn công cốt lõi.

3.3.7 Tấn công đánh lừa đầu cuối VoIP (Roque VoIP Endpoint Attack)

Giả mạo đầu cuối EP giao tiếp với các dịch vụ VoIP bằng cách dựa trên các đánh cắp hay ước đoán các nhận dạng, các uỷ nhiệm hoặc các truy cập mạng. Ví dụ, một đánh lừa đầu cuối EP có thể sử dụng các jack không được bảo vệ hay tự động đăng ký thoại VoIP để có thể vào mạng. Ước chừng mật mã có thể được sử dụng để giả dạng như là một đầu cuối hợp pháp. Việc quản lí các tài khoản không chặt chẽ có thể gia tăng nguy cơ của việc lợi dụng này

3.3.8 Cướp đăng ký (Registration Hijacking)

Cướp đăng ký xảy ra khi một người tấn công mạo nhận là một UA có giá trị để giữ và thay thế đăng ký với địa chỉ của mình. Các tấn công này là nguyên nhân của việc tất cả các cuộc gọi đến được gởi đến người tấn công.

3.3.9 Giả mạo ủy nhiệm

Giả mạo uỷ nhiệm xảy ra khi một người tấn công đánh lừa một uỷ nhiệm (proxy) trong việc truyền thông với một proxy giả.. Nếu một người tấn công thành công trong việc giả mạo uỷ nhiệm, anh ta có thể truy cập vào tất cả các thông điệp SIP.

3.3.10 Lừa tính phí

Giả mạo đầu cuối VoIP sử dụng server VoIP để đặt việc tính phí bất hợp pháp của cuộc gọi qua PSTN. Ví dụ, các điều khiển truy cập không đầy đủ có thể cho phép các thiết bị giả đặt phí của các cuộc gọi bằng cách gởi yêu cầu VoIP đến các ứng dụng tiến hành cuộc gọi. Các server VoIP có thể bị hack trong các thủ tục để tiến hành cuộc gọi miễn phí đến đích bên ngoài.

3.3.11 Xáo trộn thông điệp

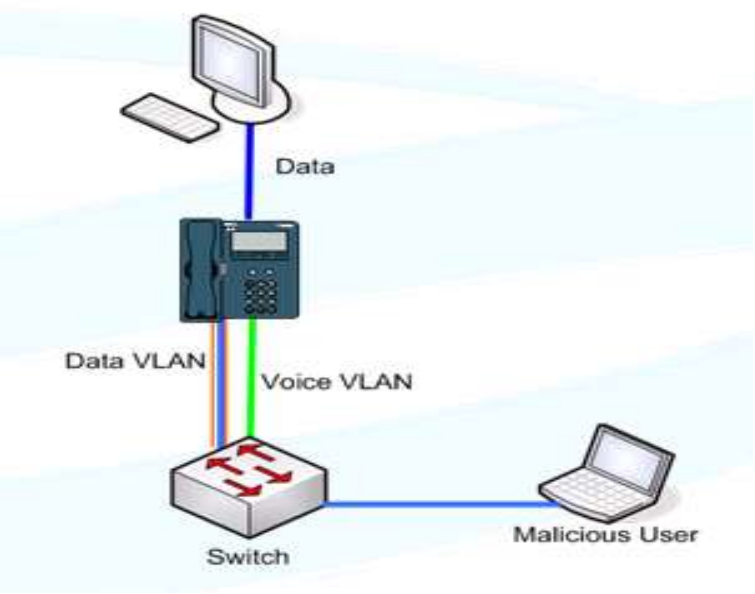
Bắt giữ, sửa đổi, và sắp đặt để không xác thực các gói VoIP đến đầu cuối. Các tấn công này có thể xảy ra qua việc đánh cắp đăng nhập, giả mạo uỷ nhiệm, hay tấn công trên bất kỳ một thành phần VoIP thực nào mà tiến hành các thông điệp SIP hay H.323, như là server proxy, registration, media gateway, hay các bức tường lửa.

3.4 Các công nghệ bảo mật

Khi đưa ra những nhu cầu bảo mật cho những thiết bị VoIP, phần này mô tả một vài công nghệ có sẵn để đảm bảo tính toàn vẹn,tính bí mật, và tính chứng thực. Các công nghệ này không phải là những giải pháp tối ưu nhưng nó góp phần giải quyết những vấn đề trong mạng VoIP:

3.4.1 VLAN

Sự tích hợp thoại, dữ liệu và video trên cùng một mạng làm cho sự bảo mật của hệ thống VoIP cũng bị ảnh hưởng bởi các dịch vụ khác. Để có thể giải quyết được vấn đề này ta tách biệt về luận lý giữa các dịch vụ bằng VLAN



Hình 3- 1: VLAN

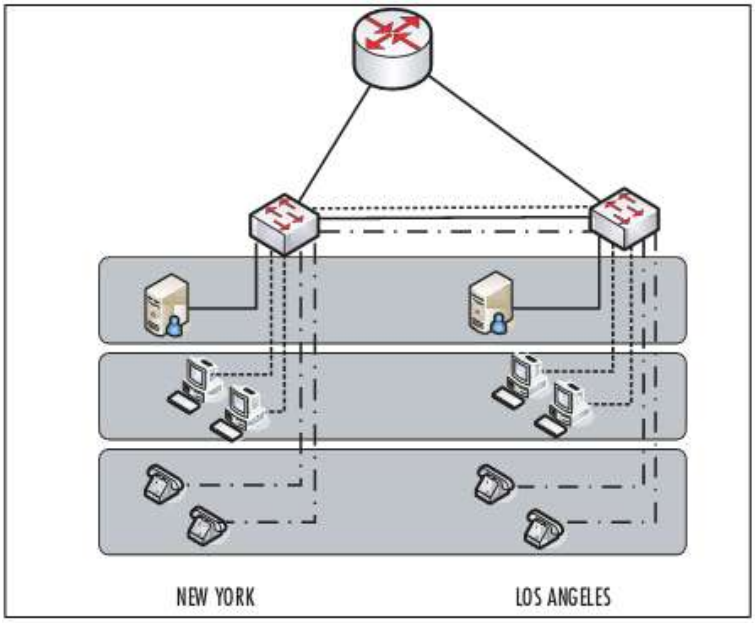
Lợi ích của VLAN:

- Giảm lưu lượng broadcast và multicast vì chỉ có các máy trong cùng một VLAN mới có thể thông tin được với nhau. VLAN được cấu hình trên switch.

- VLAN dễ dàng quản lý, giúp quản lý thiết bị một cách tập trung. VLAN có thể sắp xếp và quản lý các PC hay softphone dựa vào chức năng, lớp dịch vụ, tốc độ kết nối hoặc những tiêu chuẩn khác.

- Giảm delay và jitter, do đó cải thiện QoS.

Hệ thống VoIP có thể bị ảnh hưởng bởi sự thiếu bảo mật của các dịch vụ khác của mạng dữ liệu.



Hình 3- 2: VLAN phân theo chức năng

VLAN góp phần trong bảo mật hệ thống VoIP. Lưu lượng giữa các VLAN được đảm bảo (trừ khi sử dụng router). Nó làm giảm các broadcast lưu lượng trên mạng mà điện thoại phải nhận.

Quản lý lưu lượng bằng VLAN giúp cho lưu lượng SNMP và syslog không bị nhiễu với dữ liệu, dễ dàng hơn trong việc quản lý mạng.

VLAN còn làm giảm nguy cơ DoS. Do muốn liên lạc giữa các VLAN thì phải đi qua lớp mạng, các lưu lượng này sẽ bị lọc bởi các ACL trên lớp mạng.

Để bảo đảm an toàn cho lưu lượng tại lớp 2 thì cần hạn chế quyền truy cập bằng cổng console của Switch bằng cách sử dụng những phương pháp chứng thực mạng như RADIUS hay AAA.

3.4.2 VPN

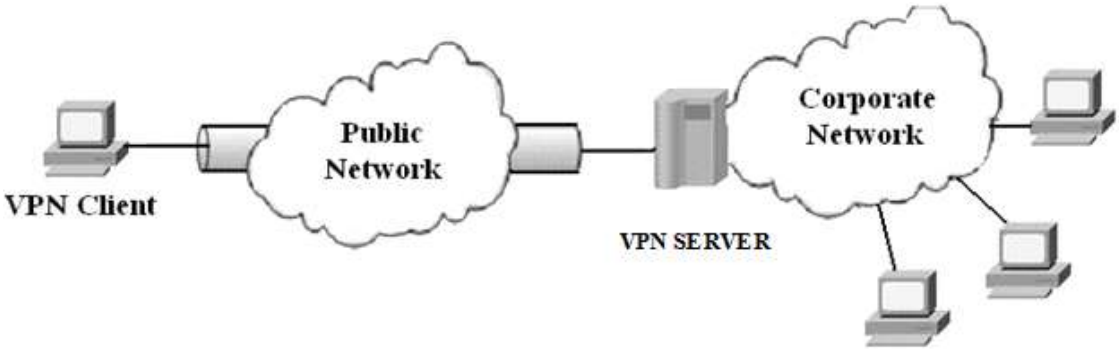
Công nghệ VPN cung cấp một phương thức giao tiếp an toàn giữa các mạng riêng dựa trên hạ tầng mạng công cộng (Internet). VPN thường được dùng để kết nối các văn phòng, chi nhánh với nhau, các người dùng từ xa về văn phòng chính. Công nghệ này có thể triển khai dùng các giải pháp sau: Frame Relay, ATM hay Leased line.

Các giao thức và thuật toán được dùng trong VPN bao gồm DES (Data Encryption Standard), Triple Des (3DES), IP Security (IPSec) và Internet key Exchange (IKE).

Có hai loại kết nốit VPN:

+ Client – to – LAN

+ LAN – to – LAN



Hình 3- 3: Client-to-LAN VPN

Công nghệ VPN dựa trên kỹ thuật đường hầm (tunneling). Kỹ thuật này bao gồm đóng gói, truyền đi, giải mã, định tuyến. VPN có ba loại: Point – to – Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), IPsec.

3.4.2.1 Point – to – Point Tunneling Protocol

Đây là một giao thức phát triển bởi Microsoft, làm việc ở lớp 2 trong mô hình OSI. PPTP đóng gói frame PPP vào gói IP bằng cách sử dụng GRE (General Routing Encapsulation).Các hình thức đảm bảo sự bảo mật gồm: chứng thực, mã hóa dữ liệu, lọc gói PPTP.

PPTP dùng các giao thức chứng thực PPP gồm: EAP, MS-CHAP (ver 1 và ver 2), PAP, trong đó MS-CHAP ver2 và EAP-TLS được xem là bảo mật nhất vì cả VPN server và VPN client đều *chứng thực lẫn nhau.* Tải trong PPP frame được mã hóa bằng RSA (Rivest, Shamir and Adleman), RC4 (Rivest Cipher 4).

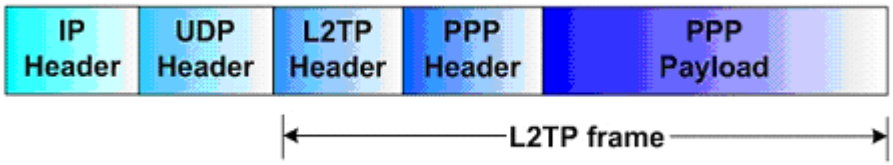
Trong MS-CHAP ver1 giá trị băm của LAN và của Windows NT được sinh ra dựa trên cùng một password và được gửi song song từ client đến server. Vì giá trị LAN manager hash được bảo mật kém nên các chương trình bẻ password có thể tấn công được, khi đã biết được giá trị băm của LAN, có thể dùng nó để tìm ra giá trị của Windows NT. MS-CHAP ver 2 khắc phục được lỗi trên nhờ dùng cơ chế mã hóa.

RSA và RC4 cũng có các điểm yếu do khóa mã hóa dựa trên password của user và cả client và server đều dùng chung khóa mã hóa.

3.4.2.2 Layer 2 Tunneling Protocol

L2TP là giao thức chuẩn của IETF (RFC 2661). Khác với PPTP, L2TP có thể chạy trên nhiều chuyển mạch khác nhau như X.25, Frame Relay, ATM, nhưng thường thì L2TP đóng gói PPP frame trong L2TP frame và dùng UDP để truyền đi (không dùng GRE). Dùng UDP tốt hơn cho các dịch vụ thời gian thực.

Bản thân L2TP không đảm bảo bảo mật, nó cần các giao thức vận chuyển bên dưới làm điều này. Điều này được thực hiện qua việc bảo mật trong PPP hoặc dùng IPsec.



Hình 3- 4: Cấu trúc L2PT

3.4.2.3 IP Security

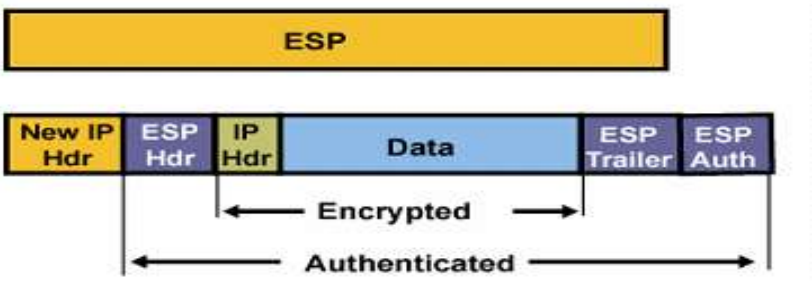
Với đặc điểm là dễ bị bắt gói trong mạng IP nên yêu cầu mã hóa là cần thiết cho hệ thống VoIP. IPsec có thể bảo mật thông tin của EP và luồng dữ liệu. IPsec là tập giao thức phát triển bởi IETF, bảo mật ở lớp IP.

IPSec bao gồm 4 thành phần: thành phần mã hóa (Encryption), trao đổi khóa (Security Association), đảm bảo toàn vẹn dữ liệu (Data Integrity) và kiểm tra nguồn gốc dữ liệu (Origin Authentication).

IPsec gồm hai giao thức: Authenticaion Header (AH) và Encapsulating Security Payload (ESP).

- AH: chứng thực data và chống replay, dùng giao thức IP số 51
- ESP: dùng giao thức IP số 50

ESP chỉ mã hóa và chứng thực trên gói ban đầu (không có header), còn AH thì chứng thực toàn bộ gói (có header) và không mã hóa.

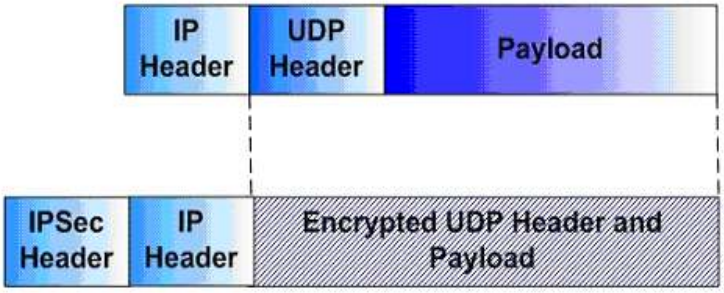


Hình 3- 5: Chứng thực và mã hóa của AH và ASP

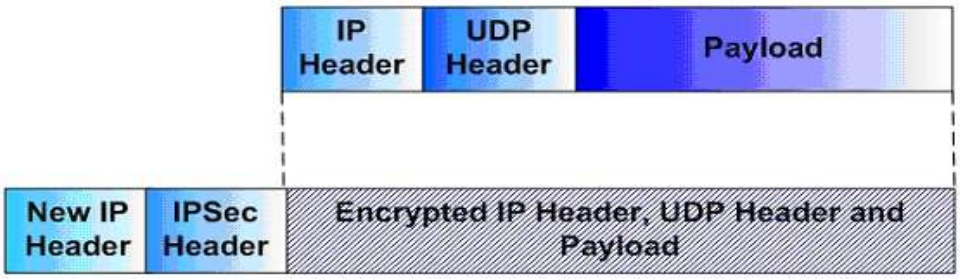
- *IPsec gồm 2 mode:*

+ *Tunnel mode*: tạo thêm một IP header mới gồm một địa chỉ nguồn và một địa chỉ đích (có thể khác với địa chỉ nguồn và địa chỉ đích trong gói IP). ESP chứng thực và mã hóa trên gói IP, còn AH chứng thực thêm một phần của header mới.

+ *Transport mode*: ESP mã hóa và chứng thực gói IP (không có phần header), AH thì có chứng thực thêm một phần header mới.



Hình 3- 6: Cấu trúc gói IPsec ở transport mode



Hình 3- 7: Cấu trúc gói IPsec ở tunnel mode

Trong quá trình thiết lập kết nối, VPN client và VPN server sẽ thương lượng thuật toán mã hóa được sử dụng trong số các thuật toán sau: DES, MD5, SHA, DH

Security Association (SA) thường được quản lý bởi IKE. SA thường có thể dùng pre-shared key, mã hóa RSA hoặc chữ ký số. IPsec chứng thực bằng shared secret và certificate, bảo mật hơn so với PPTP chứng thực bằng password của user.

3.4.3 *Firewalls*

Đóng vai trò rất quan trọng trong việc bảo mật mạng dữ liệu khỏi những tấn công từ bên ngoài. Một số loại firewall cơ bản sau có thể bảo vệ dữ liệu ở các lớp khác nhau trong mô hình OSI:

Packet filtering firewall

Circiut level gateway firewall

Personal firewall

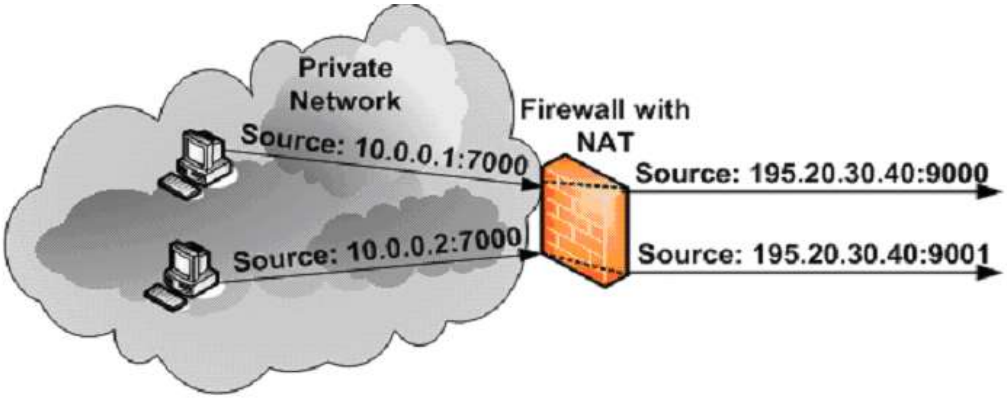
Chức năng cơ bản của firewall được thiết kế không phải dành cho các ứng dụng thời gian thực như VoIP nên việc thiết lập firewall cho hệ thống VoIP sẽ làm cho hệ thống phức tạp hơn ở một số quá trình: port động trunking, thủ tục thiết lập cuộc gọi.

Ngoài ra, firewall còn có nhiệm vụ điều khiển luồng thoại và dữ liệu. Nếu không cài đặt firewall thì tất cả các lưu lượng đến và đi từ IP phone đều phải được cho phép vì RTP dùng port UDP động, và như vậy thì tất cả các port UDP đều phải mở, thiếu bảo mật. Vì vậy, IP phone thường đặt sau firewall để tất cả các lưu lượng đều được kiểm soát mà không cần phải mở tất cả các port UDP → firewall được sử dụng để cách ly về mặt luận lý giữa thoại và dữ liệu.

3.4.4 *NAT (Network Address Translation).*

Là kỹ thuật mà địa chỉ nguồn hay địa chỉ đích thay đổi khi đi qua thiết bị có chức năng NAT, cho phép nhiều host trong mạng nội bộ dùng chung một địa chỉ IP để đi ra mạng bên ngoài.

Ngoài one-to-one mapping thì còn có many-to-one mapping hay còn gọi là NAPT (Network Address Port Translation).



Hình 3- 8: Quá trình thay đổi địa chỉ trong NAT

NAT có 4 chính sách:

- *Full*: tất cả các yêu cầu từ cùng các host bên trong (địa chỉ IP và port) được ánh xạ tới cùng một IP hay port đại diện bên ngoài, vì vậy bất kỳ một host bên ngoài có thể gửi gói tới 1 host bên trong nếu biết địa chỉ được ánh xạ đó.

- *Restricted*: chỉ cho phép 1 host bên ngoài với IP X gửi gói cho host mạng bên trong nếu host của mạng bên trong đã gửi tới IP X một gói trước đó.

- *Port restricted*: Giống Restricted one nhưng có thêm port. Chính sách này được sử dụng để có thể dùng chung một địa chỉ IP đại diện bên ngoài.

- *Symmetric*: tất cả các request từ cùng 1 IP hay port đến 1 đích nào đó được ánh xạ đi bằng 1 IP đại diện, nếu đi tới 1 đích khác thì nó sẽ đi bằng IP đại diện khác → Chỉ có những host bên ngoài nhận được gói thì mới gửi gói ngược trở lại các host bên trong được.

Lợi ích của NAT:

Giảm bớt số IP cần dùng bằng cách sử dụng chung 1 IP đại diện để đi ra bên ngoài. Với việc sử dụng chung 1 IP đại diện để đi ra bên ngoài như vậy thì mọi lưu lượng muốn truy nhập vào mạng bên trong thì phải qua NAT, bảo mật hơn.

3.4.5 *Một số chú ý khi sử dụng NAT và firewall trong hệ thống VoIP.*

Ảnh hưởng đến QoS:

Việc thiết lập firewall và NAT gây ra trễvà jitter, làm giảm QoS. Về bản chất, muốn cải thiện QoS thì quá trình xử lý gói khi qua firewall phải nhanh, mà khả năng xử lý gói của firewall lại phụ thuộc vào năng lực của

CPU. CPU xử lý gói chậm là do: header của gói thoại phức tạp hơn gói IP bình thường nên thời gian xử lý lâu hơn; số lượng gói RTP quá lớn có thể làm firewall CPU bị qua tải.

Cuộc gọi tới:

Khi một có một cuộc gọi tới thì các lưu lượng báo hiệu tới đi qua firewall, cần phải mở một số port, điều này có thể gây nguy hiểm.

Với NAT điều này càng khó khăn vì NAT dùng port động, mà một host bên ngoài chỉ có thể gọi cho 1 host nằm sau NAT nếu biết chính xác địa chỉ IP và port của nó.

Voice Stream:

RTP dùng port động (1024-65534), còn RTPC quản lý luồng thoại bằng một port ngẫu nhiên, khó mà đồng bộ port của RTP và RTPC. Nếu cả hai host đều nằm sau NAT thì càng khó khăn.

NAT chỉ ánh xạ địa chỉ bên trong và địa chỉ đại diện đi ra bên ngoài trong 1 khoảng thời gian t(s). Nếu kết nối bị đứt hay không có lưu lượng đi qua NAT trong t(s) thì ánh xạ này sẽ biến mất.

Nếu dùng TCP thì khi kết nối TCP kết thúc thì cuộc gọi cũng kết thúc. Nếu dùng UDP thì không nhận biết được vì UDP là phi kết nối. Nếu sử dụng VAD thì có khả năng thông tin kết nối bị xóa trước khi cuộc gọi thật sự kết thúc.

Mã hóa:

Việc mã hóa giúp đảm bảo tính toàn vẹn dữ liệu nhưng ta cũng gặp một số vấn đề với nó khi sử dụng NAT và firewall:

+ Firewall sẽ chặn các gói có header được mã hóa.

+ NAT dấu đi IP bên trong với mạng bên ngoài nên phương pháp chứng thực ESP và AH của Ipsec là không hợp lệ.

3.4.6 Share-key (khoá dùng chung)

Những cách tiếp cận Chìa khóa- Dùng chung:

Một cách tiếp cận tới sự chứng thực là một hệ thống mà trong đó người gửi và người nhận chia sẻ một mật khẩu bí mật (đôi khi tham chiếu tới như một chìa khóa- dùng chung) mà không được biết đối với một bên thứ ba.

Người gửi tính toán một hash nội dung thông điệp và nối vào giá trị hash đó với một thông điệp. Bên phía nhận được thông điệp, người nhận cũng

tính toán hash thông điệp với một mật khẩu dùng chung. Sau đó nó so sánh hash đã được tính toán với giá trị hash mà được bổ sung vào thông điệp. Nếu chúng phù hợp, sự toàn vẹn của thông điệp được bảo đảm như là tính xác thực của người gửi.

Bạn có thể sử dụng mật khẩu dùng chung để mã hóa nội dung thông điệp và truyền dữ liệu đã mã hóa tới người nhận. Trong trường hợp này, yêu cầu riêng tư được đề cập không vì bên thứ ba có thể đánh hơi dữ liệu đang vận chuyển và có thể nhìn nội dung thông báo của văn bản gốc. Người nhận chạy giải thuật giải mã (sự mở khóa) với mật khẩu dùng chung như một trong những đầu vào và tạo ra lại thông báo văn bản gốc.

Một hệ thống mà có nhiều nguồn dữ liệu có thể gặp phải yêu cầu xác thực bằng việc bảo đảm rằng mỗi người gửi sử dụng một chìa khóa duy nhất cho dữ liệu được gửi.

Trong một cách tiếp cận chìa khóa- dùng chung, người quản trị phải có sự chuẩn bị đối với mật khẩu bí mật dùng chung. Trong một hệ thống mà có nhiều cặp người gửi/ nhận, việc đương đầu với sự chuẩn bị có thể rất cao.

Ngoài ra, nếu một chìa khóa- dùng chung được thỏa hiệp (stolen/ lost), Mọi thiết bị sử dụng chìa khóa dùng chung cần được chuẩn bị với chìa khóa dùng chung mới.

3.4.7 Public-Key Cryptography (Mật mã chìa khoá-công cộng):

Để làm giảm bớt sự đau đầu cho người quản trị với những cách tiếp cận chìa khóa- dùng chung, bạn có thể sử dụng mật mã chìa khóa- công cộng. Những khái niệm cơ bản trong mật mã chìa khóa chung là những chìa khóa và những chữ ký số hóa không cân đối, được mô tả trong những mục sau đây:

Những chìa khóa không cân đối:

Những cặp chìa khóa không cân đối từng cặp là những chìa khóa (thông thường của độ dài cố định) được tham chiếu tới như chìa khóa công cộng và chìa khóa riêng tư mà có liên quan toán học đến lẫn nhau. Chúng thông thường được đại diện trong hệ mười sáu và có những đặc trưng sau đây:

- Chỉ có chìa khoá công cộng tương ứng mới có thể giải mã giữ liệu mà được mã hoá với một chìa khoá riêng tư.

- Chỉ có cặp chìa khoá riêng tư tương ứng mới có thể giải mã dữ liệu mà được mã hoá với một chìa khoá công cộng.

- Có mối quan hệ một-một giữa những chìa khoá.

- Chìa khoá riêng tư được giữ bí mật, còn chìa khoá công cộng thì được chia sẻ với mọi người.

Đối với sự chứng thực, một người gửi có thể sử dụng chìa khóa riêng tư của riêng mình để mã hóa thông điệp. Thông điệp chỉ có thể được giải mã với chìa khóa công cộng tương ứng. Người nhận có thể giải mã thông điệp miễn là anh ta có sự truy nhập tới chìa khóa công cộng của người gửi. Vì chỉ có người gửi mới biết chìa khóa riêng tư nên anh ta buộc phải mã hóa thông điệp.

Đối với truyền thông an toàn, một người gửi có thể mã hóa nội dung thông báo bằng cách sử dụng kỹ thuật mật mã chìa khóa- công cộng. Anh ta làm điều này bằng cách sử dụng chìa khóa công cộng của người nhận. Người nhận sau đó có thể giải mã thông điệp với chìa khóa riêng tư tương ứng. Bởi vì người nhận đã dự định có chìa khóa riêng tư nên anh ta có thể giải mã hông điệp. Không có bên thứ ba nào khác có thể giải mã thông báo này, bởi vì không ai khác biết chìa khóa riêng tư của người nhận.

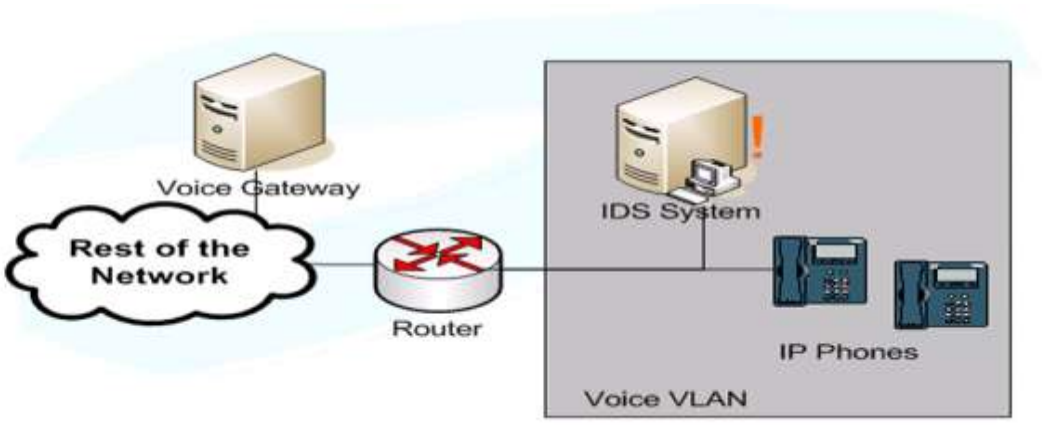
Chú ý rằng người gửi phải sử dụng chìa khóa riêng tư để mã hóa thông điệp cho những mục đích chứng thực, trong khi mà người nhận phải sử dụng chìa khóa công cộng để mã hóa thông điệp cho sự truyền thông an toàn.

Trong thế giới thực, pha chứng thực đến đầu tiên. Sau khi người gửi và người nhận xác nhận lẫn nhau thì họ chuyển tới pha truyền thông an toàn.

Sự mã hóa sử dụng những chìa khóa không cân đối là một tiến trình cường độ cao của CPU. Bởi vậy, khi mà bao gồm rất nhiều dữ liệu, những người quản lý nói chung sử dụng mật mã chìa khóa công cộng để đàm phán một bí mật dùng chung duy nhất trên phiên họp. Họ dùng những ký số chìa khóa cân đối bằng cách sử dụng bí mật dùng chung này cho phần còn lại của phiên họp.

3.4.8 IDS (Intrusion Detection)

IDS là hệ thống giám sát tất cả các lưu lượng trong mạng. IDS là thiết bị thụ động, lưu lượng không đi qua nó, mà nó chỉ lấy tất cả các gói trên mạng để phân tích. Nếu có lưu lượng không bình thường bản thân nó sẽ phát cảnh báo cho người quản trị mạng biết.



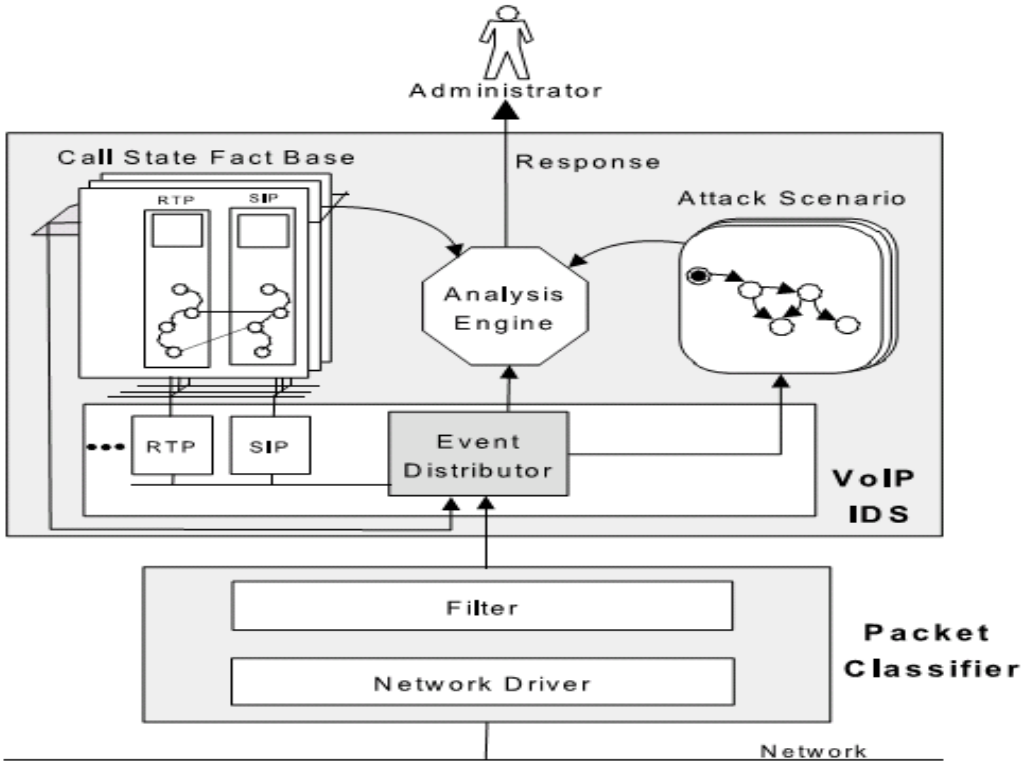
Hình 3- 9: Vị trí của IDS trong hệ thống

Hoạt động của IDS:

- IDS theo dõi tất cả những trạng thái bình thường của hệ thống và do đó phát hiện ra những tấn công bất thường vào hệ thống. Kiến trúc của nó gồm *Call State Fact Base*, chứa các trạng thái điều khiển và các biến trạng thái, cho phép theo dõi tiến trình của cuộc gọi. Thông tin trạng thái được cập nhật từ *Event Distributor*. *Attack Scenarino* chứa những kiểu tấn công đã biết.

- IDS quản lý sự thay đổi trạng thái của các gói được phân tích bằng chức năng Call basis. Tất cả gói của một cuộc gọi được phân thành một nhóm, rồi lại chia thành các nhóm nhỏ dựa trên loại giao thức, rồi đưa vào các bộ máy phân tích khác nhau, các bộ máy này được đồng bộ bằng các tham số chung và các sự kiện nội bộ. *Event Destributor* cũng phân loại các gói nhận được cho *Attack Scenarino*.

Các gói từ *Event Destributor* và thông tin trạng thái từ *Attack Scenarino/ Call State Fact Base* được đưa đến *Analysis Engine*. Khi có sự bất thường nào về giao thức hay trùng với một kiểu tấn công biết trước thì IDS sẽ bật cờ cảnh báo cho người quản trị phân tích thêm.



Hình 3- 10: Cấu trúc bên trong của thiết bị IDS

3.5 Bảo vệ các thiết bị VoIP

Để có được tính sẵn sàng của thiết bị VoIP, bạn cần phải bảo vệ những thiết bị mà lưu lượng âm thanh nguồn hay thiết bị đầu cuối của thiết bị đó phải có khả năng chống lại các cuộc tấn công, như được mô tả chi tiết ở phần dưới đây:

Vô hiệu hoá những cổng và những dịch vụ không thường sử dụng:

Điển hình là những cổng hoặc những dịch vụ không thường sử dụng mà được mở trên các thiết bị thoại làm cho chúng có thể công kích được tới sự khai thác của hacker. Luyện tập được khuyến cáo là vô hiệu hoá những cổng hoặc thiết bị của VoIP hoặc thiết bị hạ tầng IP (ví dụ như bộ switch, routers,…) sau đây là một vài điều mà bạn nên làm:

Vô hiệu hoá Telnet,TFTP, và những thiết bị tương tự nếu chúng không được sử dụng.

Nếu bạn chỉ đang sử dụng quản lý mạng đơn giản (SNMP) trên một thiết bị để thu nhặt dữ liệu, thì nên đặt SNMP ở chế độ chỉ đọc (read-only).

Nếu bạn đang sử dụng sự quản trị trên nền mạng, thì luôn luôn sử dụng sự truy nhập an toàn với những giao thức như SSL.

Vô hiệu hoá bất kỳ cửa nào không thường sử dụng trên Layer 2 switches.

+ Sử dụng hệ thống bảo vệ sự xâm nhập dựa vào Host (HIPS):

Bạn có thể sử dụng HIPS để bảo mật cho những thiết bị thoại như là những nhân tố xử lý cuộc gọi. HIPS là phần mềm điển hình mà tập hợp thông tin về những cách dùng đa dạng rộng rãi của tài nguyên thiết bị như CPU, login attemp, số lượng ngắn,…Thông tin này được so sánh chống lại một tập hợp các quy tắc để xác định phải chăng một sự xâm phạm bảo mật đã xảy ra. Bằng việc phụ thuộc vào cách định hình những tham số, những hệ thống này có thể lấy những hoạt động phòng ngừa, ví dụ như kết thúc ứng dụng offending, nhịp độ dữ liệu giới hạn từ những người sử dụng địa chỉ IP…

THUẬT NGỮ VIẾT TẮT

Kí hiệu viết tắt	Viết đầy đủ	Ý nghĩa
ADPM	Adaptive Differential Pulse Code Modulation	Điều chế xung mã vi sai thích nghi
CPU	Central Processing Unit	Đơn vị xử lý trung tâm
DNS	Domain Name System	Hệ thống phân giải tên miền
DSP	Digita Signalling Proccessor	Bộ xử lý tín hiệu số
GSM	Global System for Mobie	Hệ thống toàn cầu cho điện thoại di động
HTTP	Hypertext Tranfer Protocol	Giao thức chuyển siêu văn bản
IETF	Internet Engineering Task Force	Tổ chức viễn thông quốc tế - Lực lượng chuyên phụ trách kỹ thuật kết nối mạng
IP	Internet Protocol	Giao thức Internet
IPv4	IP version 4	Giao thức Internet phiên bản 4
IPv6	IP version 6	Giao thức Internet phiên bản 6
ISDN	Integrated Service Digital Network	Mạng dịch vụ tích hợp số
ISUP	ISDN User Part	Phần người dùng ISDN
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	Hiệp hội viễn thông quốc tế - Tổ chức chuẩn hóa các kỹ thuật viễn thông
IUA	ISDN User Adapter	Bộ chuyển đổi người dùng ISDN
LAN	Local Area Network	Mạng vùng cục bộ
LLC	Logic Link Control	Điều khiển liên kết logic
MAC	Media Access Control	Điều khiển truy nhập môi trường
MC	Multipoint Controller	Bộ phận điều khiển đa điểm
MCU	Multipoint Control Unit	Đơn vị điều khiển đa điểm
MGCP	Media Gateway	Giao thức điều khiển Media Getway

	Control Protocol	
MIPS	Millions of Instruction per second	Đơn vị thời gian (triệu/giây)
MP	Multipoint Processor	Bộ xử lý đa điểm
MTP	Message Tranfer Part	Phần truyền bản tin
M2UA	MTP2 User Adapter	Bộ chuyển đổi người dùng MTP2
M2PA	MTP L2 Peer-to-Peer Adapter	Bộ chuyển đổi bản tin lớp 2 ngang hàng
M3UA	MTP3 User Adapter	Bộ chuyển đổi người dùng MTP3
OSI	Open System Interference	Mô hình tham chiếu mạng
PAM	Pulse Amplitude Modulation	Điều biên dạng xung
PBX	Private Branche Xchange	Tổng đài chi nhánh riêng
PC	Personnal Computer	Máy tính cá nhân
PCM	Pulse-Code Modulation	Bộ mã hóa mã xung
PSTN	Public Switch Telephone Network	Mạng điện thoại công cộng
QoS	Quality of Service	Chất lượng dịch vụ
RAS	Register Admission Status	Báo hiệu đăng kí, cấp phép, thông tin trạng thái
RSVP	Reservation Protocol	Giao thức định trước nguồn tài nguyên
RTP	Real-Time Transport Protocol	Giao thức truyền thời gian thực
RTCP	Real-Time Transport Control Protocol	Giao thức điều khiển truyền thời gian thực
SAP	Session Announcement Protocol	Giao thức thông báo phiên
SCN	Switching Network	Mạng chuyển mạch kênh
SCP	Signal Control Point	Điểm điều khiển báo hiệu
SCCP	Signaling Connection Control Part	Phần điều khiển kết nối báo hiệu
SCTP	Stream Control	Giao thức truyền điều khiển luồng

	Transmission Protocol	
SDP	Session Description Protocol	Giao thức mô tả phiên
SIP	Session Initiation Protocol	Giao thức thiết lập phiên
SS7	Signaling System No.7	Hệ thống báo hiệu số 7
SSP	Switch Service Point	Điểm dịch vụ chuyển mạch
Sigtran	Signalling Transport	Giao thức truyền báo hiệu SS7 trên mạng IP
STP	Signal Tranfer Point	Điểm truyền báo hiệu
SUA	SCCP User Adapter	Bộ chuyển đổi người dùng SCCP
TCAP	Transaction Capabilities Application Part	Phần ứng dụng cung cấp giao dịch
TCP	Transmission Control Protocol	Giao thức điều khiển truyền thông tin
TUP	Telephone User Part	Phần người dùng điện thoại
UA	User Agent	Đại diện người sử dụng
UAC	User Agent Client	Đại diện người sử dụng khách hàng
UAS	User Agent Server	Đại diện người sử dụng máy chủ
UDP	User Datagram Protocol	Giao thức Datagram người dùng
VoIP	Voice over Internet Protocol	Công nghệ truyền thoại trên mạng IP
VPN	Virtual Private Network	Mạng riêng ảo
WAN	Wide Area Network	Mạng băng rộng