MỞ ĐẦU

VoIP là công nghệ truyền thoại qua mạng IP, VoIP đã phát triển từ những năm 90 của thế kỷ trước. VoIP ra đời là một bước đột phá lớn trong lĩnh vực viễn thông, VoIP thừa hưởng những ưu điểm mà mạng IP đem lại. Công nghệ VoIP từ khi ra đời đến nay đã và đang được nghiên cứu, phát triển để ngày càng đáp ứng tốt hơn các yêu cầu về chất lượng dịch vụ, giá thành, số lượng tích hợp các dịch vụ thoại và phi thoại, an toàn bảo mật thông tin.

VoIP ra đời từ rất sớm tuy vậy cho đến nay nó vẫn còn nhiều vấn đề tồn tại và cần khắc phục. Trên thế giới cũng như ở Việt Nam VoIP vẫn đang nghiên cứu và triển khai để phát triển cùng với dịch vụ truyền thống PSTN. Hai tổ chức quốc tế là ITU-T và IETF đã đưa ra một số chuẩn cho mạng VoIP. Với mỗi chuẩn khác nhau thì thành phần thiết bị mạng cũng khác nhau, đi kèm với nó là một chồng các giao thức phục vụ cho báo hiệu.

Ở Việt Nam công nghệ VoIP đã được các nhà khai thác dịch vụ viễn thông áp dụng cho cuộc gọi đường dài trong nước và quốc tế như: Dịch vụ 171 của VNPT, 178 của Viettel, 179 của EVN. VoIP đem lại rất nhiều lợi thế vì vậy trong những năm gần đây cũng như trong những năm tới VoIP đang là một hướng phát triển hợp lý và có nhiều triển vọng của các nhà khai thác dịch vụ viễn thông ở Việt Nam. Tuy nhiên theo thống kê của hãng bảo mật Scanit vấn đề bảo mật an toàn thông tin dường như chưa được xem trọng, còn quá nhiều lỗ hổng bảo mật chưa được các nhà cung cấp dịch vụ khắc phục.

Để triển khai và khai thác tối đa những thuận lợi và khắc phục những nhược điểm, sơ hở bảo mật của VoIP thì việc nắm bắt công nghệ được xây dựng cho VoIP, làm chủ các thiết bị trong mạng VoIP để đưa ra giải pháp, mô hình mạng ứng dụng VoIP cho các cơ quan doanh nghiệp sao cho phù hợp và đặc biệt là an toàn cho thông tin quan trọng trong kinh doanh là cần thiết. Trên cơ sở thực tiễn đó em đã chọn đề tài " BẢO MẬT TRONG VOIP " là đề tài của đồ án tốt nghiệp.

Dựa vào những tài liệu của các tác giả trong nước, tác giả nước ngoài và các nhà sản xuất thiết bị như Cisco kết hợp với những khuyến nghị của các tổ chức chuẩn hóa viễn thông quốc tế, em đã tập trung nghiên cứu các mô hình mạng VoIP với các giao thức, phương thức bảo mật được sử dụng trong đó. Các vấn đề này được trình bày trong bốn chương đầu của đồ án.

- Chương 1. TỔNG QUAN VỀ VOIP
- Chương 2. MÔ HÌNH KIẾN TRÚC PHÂN TẦNG VÀ CÁC GIAO THỨC TRUYỀN TẢI TRONG MẠNG VOIP
- Chương 3. MẠNG VOIP VỚI CÁC GIAO THỨC BÁO HIỆU H.323/SIP
- Chương 4. CÁC PHƯƠNG THỨC TẤN CÔNG VÀ BẢO MẬT TRONG VOIP

Trên cơ sở nắm chắc lý thuyết em đã tiến hành các thực nghiệm trong chương 5 của đồ án.

- Chương 5. CẤU HÌNH VOIP CƠ BẢN VÀ TRIỂN KHAI TRÊN MẠNG CỤC BỘ ỨNG DỤNG CHO DOANH NGHIỆP NHỎ

  Chương này thực hiện một số vấn đề sau:

  ✧ Thiết lập mạng VoIP cơ bản trong phòng Lap dựa trên các thiết bị của Cisco. Các thiết bị chủ yếu là router 2600, access router 2500 và các PC.

  ✧ Dựa vào mô hình cơ bản tìm ra sơ hở bảo mật để đưa ra mô hình an toàn thông tin hơn ứng dụng cho doanh nhiệp.

Chương 1

TỔNG QUAN VỀ VOIP

1.1. GIỚI THIỆU

VoIP (Voice over Internet Protocol) là công nghệ truyền tải các cuộc liên lạc thoại trên giao thức Internet hay còn gọi là giao thức IP. VoIP đang trở thành một trong những công nghệ hấp dẫn nhất hiện nay không chỉ đối với các doanh nghiệp mà còn cả với những người sử dụng dịch vụ. VoIP có thể thực hiện tất cả các dịch vụ như trên PSTN (public switched telephone network) ví dụ như: truyền thoại, truyền fax, truyền dữ liệu trên cơ sở mạng dữ liệu có sẵn với tham số chất lượng dịch vụ (QoS) chấp nhận được. Điều này tạo thuận lợi cho những người sử dụng có thể tiết kiệm chi phí bao gồm chi phí cho cơ sở hạ tầng mạng và chi phí liên lạc, nhất là liên lạc đường dài. Đối với các nhà cung cấp dịch vụ, VoIP được xem như một mô hình hấp dẫn có thể mang lại lợi nhuận nhờ khả năng mở rộng và phát triển các loại hình dịch vụ với chi phí thấp.

VoIP cho phép tạo cuộc gọi đường dài qua mạng dữ liệu IP có sẵn thay vì phải được truyền qua mạng PSTN. 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.

Nguyên tắc VoIP gồm việc số hoá tín hiệu giọng nói, nén tín hiệu đã số hoá, 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.

1.2. TỔNG QUAN VỀ VOIP [2],[4]

Với sự phát triển mạnh mẽ của internet và xu hướng hội tụ công nghệ của mạng NGN (Next Generation Networks - mạng thế hệ sau). Các cuộc đàm thoại đã được truyền trên đường truyền chung với các cuộc gọi dữ liệu dựa trên cơ sở hạ tầng của mạng IP.

1.2.1. Kỹ thuật chuyển mạch gói

Trong kỹ thuật chuyển mạch gói các bản tin được chia thành nhiều gói và được đóng gói theo các chuẩn quy định, trong mỗi gói có đầy đủ các thông tin giúp cho việc định tuyến đường đi của gói tin đến đích. Trong chuyển mạch gói các bản tin tương tác với các nút mạng. Các gói tin độc lập với nhau về đường đi, các gói đến đích không theo một thứ tự quy định. Kỹ thuật chuyển mạch gói cũng như kỹ thuật chuyển mạch kênh, nó cũng có những ưu điểm và những nhược điểm.

Ưu điểm

- Tính mềm dẻo trong định tuyến, trong việc thay đổi băng thông. Chuyển mạch gói không cố định các kênh truyền thông hay các tuyến vì vậy hiệu suất sử dụng đường truyền rất cao, tận dụng tối đa hiệu năng đường truyền.
- Với một chồng các giao thức đi kèm, chuyển mạch gói có chế độ ưu tiên cho các ứng dụng khác nhau theo các mức khác nhau. Điều này cũng là cơ sở để phát triển mạng VoIP.
- Khả năng cung cấp nhiều dịch vụ thoại và phi thoại.

Nhược điểm

- Độ trễ thay đổi tùy thuộc vào từng tuyến và từng thời gian truyền thông tin.
- Chuyển mạch gói thực hiện dựa trên cơ chế cố gắng tối đa vì vậy khó thỏa mãn được chất lượng dịch vụ.
- Các gói tin đến không theo thứ tự rất dễ gây ra mất mát dữ liệu, tăng thời gian xử lý dẫn đến trễ truyền dẫn tăng lên.

1.2.2. Những ưu điểm và nhược điểm của VoIP

Những ưu điểm của VoIP

Hiện nay hầu hết các nhà cung cấp dịch vụ internet cũng như các công ty viễn thông đang đưa vào khai thác sử dụng một hệ thống mạng hội tụ IP. VoIP là một trong những dịch vụ đó và nó đem lại nhiều thuận lợi .

- Hiệu quả sự dụng băng thông cao hơn: VoIP chia sẻ băng thông giữa nhiều kênh logic. Có thể thay đổi băng thông dễ dàng tùy vào chất lượng dịch vụ cung cấp để thay đổi chất lượng cuộc gọi.
- Giảm chi phí cho cuộc gọi: Đây là ưu điểm nổi bật của VoIP so với điện thoại đường dài thông thường. Chi phí cuộc gọi đường dài chỉ bằng chi phí cho truy nhập Internet. Một giá cước chung sẽ thực hiện được với mạng Internet và do đó tiết kiệm đáng kể các dịch vụ thoại và fax. Sự chia sẻ chi phí thiết bị và thao tác giữa những người sử dụng thoại và dữ liệu cũng tăng cường hiệu quả sử dụng mạng. Đồng thời kỹ thuật nén thoại tiên tiến làm giảm tốc độ bit từ 64Kbps xuống dưới 8Kbps, tức là một kênh 64Kbps lúc này có thể phục vụ đồng thời 8 kênh thoại độc lập.

  Trong trường hợp cuộc gọi ở mạng PSTN, một kênh vật lý sẽ được thiết lập và duy trì giữa hai bên cho đến khi một trong hai bên hủy bỏ liên kết. Như vậy, trong khoảng thời gian không có tiếng nói, tín hiệu vẫn được lấy mẫu, lượng tử hoá và truyền đi. Vì vậy, hiệu suất đường truyền sẽ không cao. Với VoIP, chỉ có kết nối từ người dùng trong mạng PSTN tới Gateway của nhà cung cấp dịch vụ được duy trì. Điều này đã tiết kiệm đáng kể tài nguyên của mạng dẫn tới giảm chi phí cuộc gọi. VoIP còn có các cơ chế phát hiện khoảng lặng (khoảng thời gian không có tiếng nói) nên sẽ làm tăng hiệu suất mạng.
- Khả năng tích hợp nhiều chức năng: Do việc thiết kế cơ sở hạ tầng tích hợp nên có khả năng hỗ trợ tất cả các hình thức thông tin cho phép chuẩn hoá tốt hơn và giảm tổng số thiết bị. Các tín hiệu báo hiệu, thoại và cả số liệu đều đi trên cùng mạng IP. Tích hợp đa dịch vụ sẽ tiết kiệm chi phí đầu tư nhân lực, chi phí xây dựng cơ sở hạ tầng các mạng riêng lẻ.
- Thống nhất: Vì con người là nhân tố quan trọng nhưng cũng dễ sai lầm nhất trong một mạng viễn thông, mọi cơ hội để hợp nhất các thao tác, loại bỏ các điểm sai sót và thống nhất các điểm thanh toán sẽ rất có ích. Trong các tổ chức kinh doanh, sự quản lý trên cơ sở

SNMP (Simple Network Management Protocol) có thể được cung cấp cho cả dịch vụ thoại và dữ liệu sử dụng VoIP. Việc sử dụng thống nhất giao thức IP cho tất cả các ứng dụng hứa hẹn giảm bớt phức tạp và tăng cường tính mềm dẻo. Các ứng dụng liên quan như dịch vụ danh bạ và dịch vụ an ninh mạng có thể được chia sẻ dễ dàng hơn.

- Tính mềm dẻo trong việc sử dụng các thiết bị đầu cuối: Có rất nhiều cách lựa chọn các thiết bị đầu cuối cho VoIP. Chỉ cần một phần mềm trên máy PC cũng có thể thực hiện cuộc gọi VoIP. Có thể dùng IP phone, hay các thiết bị đầu cuối hỗ trợ VoIP khác.

Những nhược điểm của VoIP

Bên cạnh những ưu điểm vượt trội thì VoIP vẫn còn tồn tại nhiều yếu điểm cần nghiên cứu và khắc phục.

- Chất lượng dịch vụ chưa cao: Các mạng số liệu vốn dĩ không phải xây dựng với mục đích truyền thoại thời gian thực, vì vậy khi truyền thoại qua mạng số liệu cho chất lượng cuộc gọi thấp và không thể xác định trước được. Sở dĩ như vậy là vì gói tin truyền trong mạng có trễ thay đổi trong phạm vi lớn, khả năng mất mát thông tin trong mạng hoàn toàn có thể xảy ra. Một yếu tố làm giảm chất lượng thoại nữa là kỹ thuật nén để tiết kiệm đường truyền. Nếu nén xuống dung lượng càng thấp thì kỹ thuật nén càng phức tạp, cho chất lượng không cao và đặc biệt là thời gian xử lý sẽ lâu, gây trễ.
- Một yếu điểm khác của VoIP là vấn đề tiếng vọng: Nếu như trong mạng thoại, độ trễ thấp nên tiếng vọng không ảnh hưởng nhiều thì trong mạng IP, do trễ lớn nên tiếng vọng ảnh hưởng nhiều đến chất lượng thoại.
- Vấn đề bảo mật trong VoIP: Voice là một loại dữ liệu quan trọng mà lại truyền trên mạng IP có tính chất rộng khắp. Chịu sự tấn công của những kẻ phá hoại là không thể tránh khỏi, vấn đề này sẽ

được tìm hiểu rõ hơn trong chương 4. Mạng VoIP còn rất nhiều kẽ hở mà các nhà cung cấp dịch vụ mạng cần khắc phục.

1.2.3. Các ứng dụng của VoIP

Mạng điện thoại PSTN truyền thống không thể bị thay thế một cách dễ dàng, thậm chí thay đổi hoàn toàn trong tương lai. Mục đích của các nhà cung cấp dịch vụ VoIP là tạo ra một mạng điện thoại với một chi phí vận hành thấp hơn nhiều song vẫn đảm bảo chất lượng gần như PSTN và đưa ra các giải pháp kỹ thuật bổ sung cho mạng PSTN.

Mạng điện thoại này có thể được áp dụng cho gần như mọi yêu cầu của giao tiếp thoại, từ một cuộc đàm thoại đơn giản cho đến một cuộc gọi hội nghị nhiều người phức tạp. Chất lượng âm thanh được truyền cũng có thể biến đổi tùy theo ứng dụng. Ngoài ra, với khả năng của Internet, VoIP sẽ cung cấp thêm nhiều tính năng mới.

Một số các ứng dụng của VOIP sẽ được đề cập cụ thể dưới đây:

- **Thoại thông minh:** Điện thoại thông thường chỉ có một số ít chức năng, thực hiện bởi một vài phím điều khiển. Trong những năm gần đây, người ta đã cố gắng để tạo ra thoại thông minh, đầu tiên là các thoại để bàn, sau là đến các server.

  Giữa mạng máy tính và mạng điện thoại vốn tồn tại một mối liên hệ. Sự phát triển rộng khắp của Internet đã tạo ra một bước đột phá mới. Kể từ khi được phủ khắp toàn cầu, Internet góp phần tăng thêm tính thông minh cho mạng điện thoại toàn cầu. Internet cung cấp cách giám sát và điều khiển các cuộc thoại một cách tiện lợi hơn. Chúng ta có thể thấy được khả năng kiểm soát và điều khiển các cuộc thoại thông qua mạng Internet.
- **Dịch vụ điện thoại Web:** Sự ra đời của www (World Wide Web) đã tạo ra một cuộc cách mạng trong các quan hệ giao dịch thương mại, giữa khách hàng với các doanh nghiệp và ngược lại. Dịch vụ điện thoại Web hay "click to dial" cho phép các nhà doanh nghiệp có thể đưa thêm các phím bấm lên trang web để kết nối tới hệ thống điện thoại

của họ, tức là đưa thêm các kênh trực tiếp từ các trang Web vào hệ thống điện thoại.

- **Truy cập các trung tâm tư vấn:** Dịch vụ này cho phép một khách hàng có câu hỏi về một sản phẩm được chào hàng qua Internet được các nhân viên của công ty trả lời trực tuyến, việc này góp phần thúc đẩy mạnh mẽ thương mại điện tử.
- **Dịch vụ fax qua IP (FoIP - Fax over IP):** Việc sử dụng Internet không những được mở rộng cho thoại mà còn cho cả dịch vụ fax. Dịch vụ Internet faxing sẽ giúp tiết kiệm được chi phí và cả kênh thoại khi phải gửi fax với số lượng lớn, đặc biệt là gửi ra nước ngoài. Dịch vụ này sẽ chuyển trực tiếp từ PC qua kết nối Internet. Một trong những dịch vụ gửi fax nổi tiếng là comfax.
- **Tính cước cho phía bị gọi:** Để thực hiện được dịch vụ này, cần một PC kết nối Internet và chương trình phần mềm điều khiển như Quicknet's Technologies Internet Phone JACK chạy trên môi trường Windows.

1.2.4. Các yêu cầu khi phát triển VoIP

Để tồn tại và phát triển bền vững các nhà khai thác dịch vụ VoIP cần quan tâm đến một số vấn đề về chất lượng, tính bảo mật… Cụ thể như sau:

- Chất lượng thoại phải tương đương hoặc hơn mạng PSTN và các mạng điện thoại khác.
- Mạng IP cơ bản phải đáp ứng được những tiêu chí hoạt động khắt khe gồm giảm tối thiểu việc từ chối cuộc gọi, mất mát gói và mất liên lạc, ngắt quãng trong đàm thoại. Điều này đòi hỏi ngay cả trong trường hợp mạng bị nghẽn hoặc khi nhiều người sử dụng chung tài nguyên của mạng cùng một lúc.
- Tín hiệu báo hiệu phải có khả năng tương tác với các mạng khác để không gây ra sự thay đổi khi chuyển giao giữa các mạng.
- Liên kết các dịch vụ PSTN/VoIP bao gồm các Gateway giữa các môi trường mạng thoại và mạng dữ liệu.

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

Từ khi ra đời VoIP đã được triển khai thực tế kiểm nghiệm và đã có những cải tiến về công nghệ, về các chuẩn giao thức phong phú, các nhà khai thác VoIP đang dần khẳng định chất lượng dịch vụ của mình.

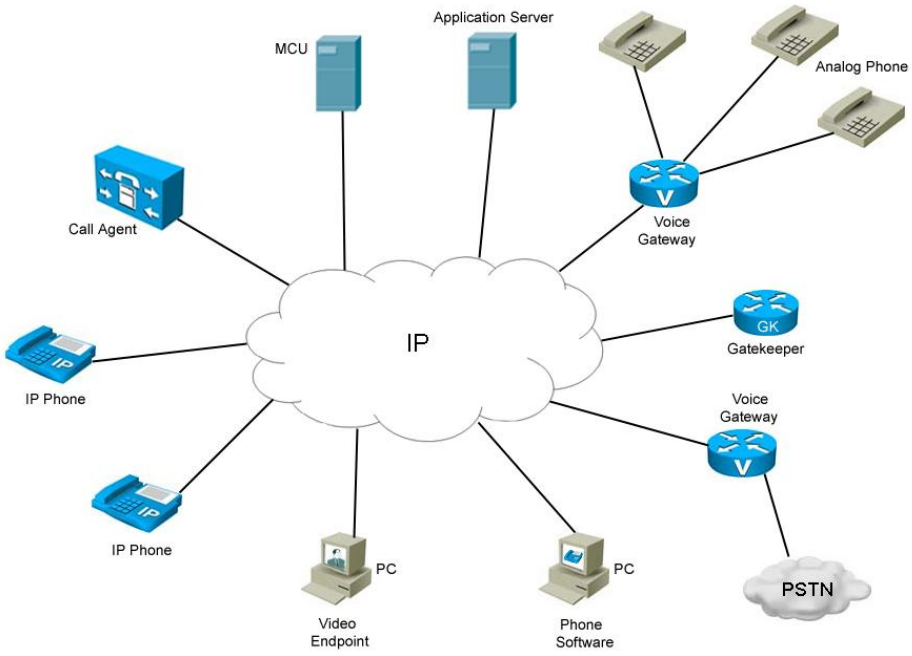
1.2.5. Mô hình mạng VoIP điển hình và các thành phần

Từ khi ra đời đến nay dịch vụ VoIP đã được nhiều tổ chức viễn thông trên thế giới quan tâm và phát triển các giao thức đi kèm. Có nhiều chuẩn mỗi chuẩn phù hợp cho một loại giao thức được định nghĩa. Nghiên cứu sâu vào từng chuẩn sẽ được trình bày trong chương sau của đồ án. Trong phần này chỉ đưa ra mô hình tổng quát nhất với mục đích giới thiệu sơ qua về mô hình mạng VoIP.

Các giao thức báo hiệu cơ bản trong VoIP gồm:

- H.323 giao thức báo hiệu được định nghĩa bởi ITU_T. H.323 định nghĩa một kiến trúc phân phối cho việc thiết lập các ứng dụng đa phương tiện bao gồm cả VoIP.
- SIP được định nghĩa trong IETF RFC 2543. SIP định nghĩa kiến trúc phân phối cho việc thiết lập các ứng dụng đa phương tiện bao gồm cả VoIP.
- MGCP được định nghĩa trong IETF RFC 2705. MGCP định nghĩa một kiến trúc tập trung hóa cho việc thiết lập các ứng dụng đa phương tiện bao gồm VoIP.
- Megaco/H248 là giao thức điều khiển gateway.

Mô hình mạng VoIP tổng quát:



Hình 1.1. Mô hình mạng VoIP tổng quát

Hình trên cho ta mô hình tổng quát với những yếu tố phổ biến nhất trong mạng VoIP, cụ thể về các thiết bị như sau:

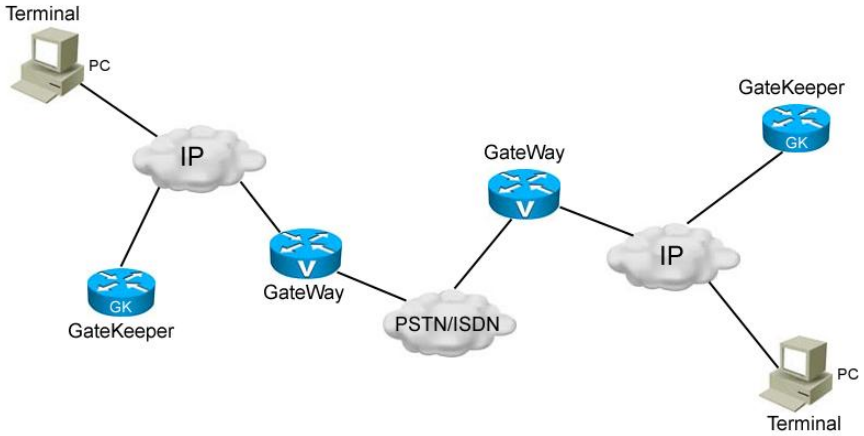
- Telephone: Telephone có thể là các điện thoại IP (IP phone), các phần mềm hỗ trợ hoạt động như một điện thoại được cài trên PC hoặc là những điện thoại truyền thống (tương tự hay ISDN).
- Gateway: Gateway liên kết mạng VoIP với mạng điện thoại truyền thống. Thường sử dụng các router hỗ trợ voice. Gateway cung cấp một số chức năng sau:

  - Trên một giao diện Gateway được cắm đường dây điện thoại. Gateway kết nối tới PSTN và thông tin với bất kỳ điện thoại nào trên thế giới.
  - Trên một giao diện khác, Gateway kết nối tới mạng IP và thông tin với bất kỳ máy tính nào trên thế giới.
  - Gateway thu tín hiệu điện thoại chuẩn, số hóa (nếu tín hiệu chưa được số hóa), nén, đóng gói sử dụng IP, và định tuyến gói tin đến đích thông qua mạng IP.
  - Gateway sắp xếp lại các gói tin đến và chuyển tiếp cho các điện thoại.

- Multipoint control units (MCU): Một MCU được yêu cầu cho các cuộc hội nghị nhiều bên. Tất cả các thành phần của hội nghị được gửi đến MCU. MCU xử lý, quản lý tất cả các thành phần của cuộc hội nghị này.
- Application server: Application cung cấp dịch vụ XML cơ bản tới IP phone. Những người sử dụng IP phone truy cập tới các thư mục và cơ sở dữ liệu thông qua XML application.
- Gatekeepers: Gatekeepers là rất hữu ích, những nó là thành phần tùy chọn trong mạng, có thể có hoặc có thể không. Gatekeeper cung cấp chức năng đăng ký, định tuyến và quản lý tất cả đầu cuối (terminals, gateways, và MCUs) trong một miền mạng nhất định. Gatekeeper cung cấp điều khiển thu nạp cuộc gọi (Call Admission Control - CAC). CAC chuyển đổi số điện thoại hay tên tới địa chỉ IP để giúp định tuyến trong mạng H.323.
- Call Agents: Call Agent cung cấp chức năng điều khiển cuộc gọi CAC, điều khiển băng thông, dịch vụ chuyển đổi địa chỉ tới địa chỉ IP hay giao thức điều khiển gateway đa phương tiện.
- Video endpoint: Video endpoint cung cấp các tính năng video cho người sử dụng. Cũng như thoại cuộc điện thoại video cũng cần có một trung tâm giám sát các cuộc gọi hội thoại video.

1.2.6. Các hình thức truyền thoại qua mạng VoIP

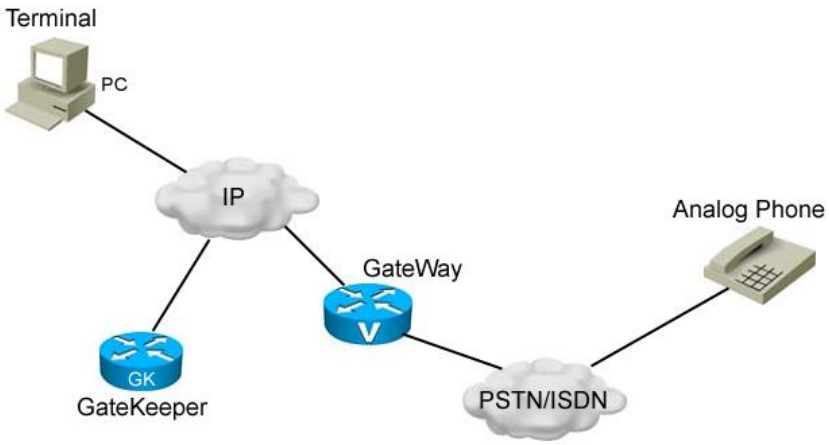
- **Cấu hình "PC to PC"**



Hình 1.2. Cấu hình "PC to PC"

Hai PC được kết nối trực tiếp với nhau trong cùng một mạng IP, hay giữa các mạng IP với nhau thông qua một mạng trung gian khác (PSTN/ISDN). Các PC được coi như các đầu cuối H.323, có thể là máy tính đa phương tiện có cài đặt phần mềm phục vụ dịch vụ thoại Internet.

- **Cấu hình "PC to Phone"**

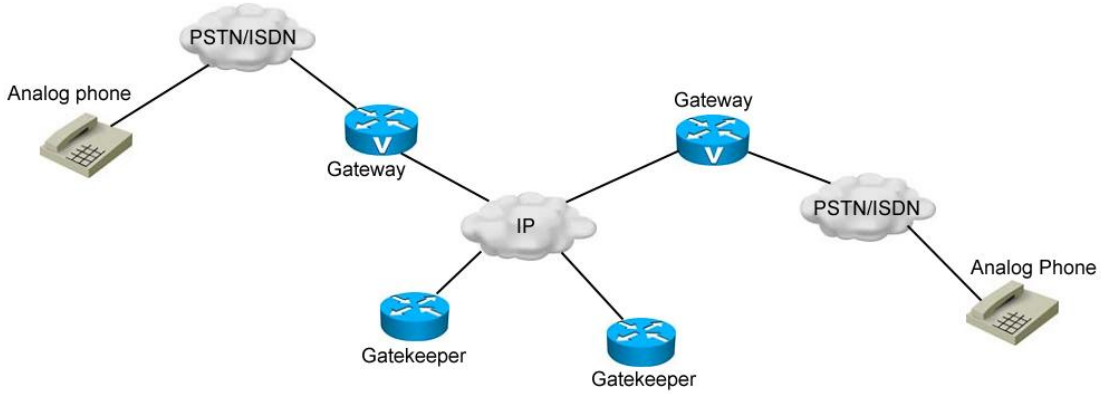


Hình 1.3. Cấu hình "PC to Phone"

Cuộc gọi được tiến hành từ máy tính đa phương tiện tới một thuê bao cố định PSTN hoặc một thuê bao di động thông thường. Tín hiệu thoại (đã được đóng trong các gói IP) được truyền qua mạng tới các Gateway. Tại đó các gói tin IP được chuyển thành tín hiệu PCM 64Kbps thông thường và truyền tới tới tổng đài nội hạt của thuê bao bị gọi và từ đó chuyển tới máy điện thoại bị gọi.

- **Cấu hình "Phone to Phone"**

Hai phía đầu cuối đều sử dụng điện thoại thông thường. Tín hiệu thoại PCM 64Kbps được chuyển thành gói tin IP và ngược lại tại các Gateway ở mỗi phía. Các gói tin IP được truyền qua mạng IP.



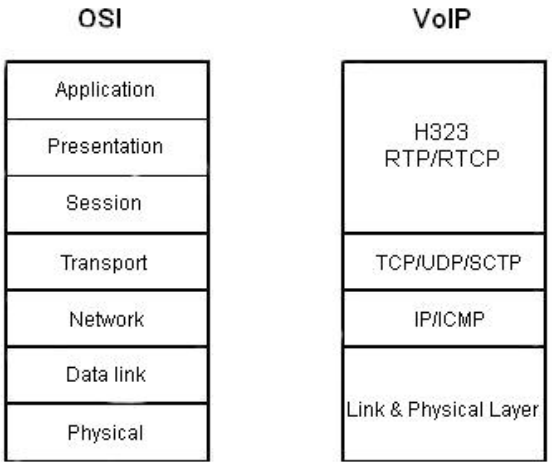
Hình 1.4. Cấu hình "Phone to Phone"

Dịch vụ này hiện nay rất phổ biến tại Việt Nam do có rất nhiều nhà cung cấp. Như VNPT với 171, Viettel với 178, EVN telecom với 179...

Chương 2

MÔ HÌNH KIẾN TRÚC PHÂN TẦNG VÀ CÁC GIAO THỨC TRUYỀN TẢI TRONG MẠNG VOIP

Mạng VoIP có mô hình kiến trúc phân tầng như sau:



Hình 2.1. Mô hình tham chiếu OSI so với mô hình mạng VoIP.

2.1. LỚP VẬT LÝ VÀ LỚP LIÊN KẾT DỮ LIỆU (LINK & PHYSICAL LAYER) [6]

Lớp vật lý tương ứng với lớp vật lý của mô hình OSI. Trong mô hình tham chiếu OSI, lớp vật lý là lớp thấp nhất chịu trách nhiệm truyền tín hiệu trên các đầu cuối mạng. Có thể điểm qua một số chức năng của lớp vật lý như sau:

- Định nghĩa các phần cứng đặc biệt. Cung cấp môi trường truyền dẫn như: truyền trên môi trường có dây, môi trường không dây, truyền qua cáp quang hay cáp đồng.
- Mã hóa tín hiệu. Lớp vật lý có chức năng mã hóa tín hiệu sao cho phù hợp với môi trường truyền.
- Truyền và thu tín hiệu tại các đầu cuối mạng.

Lớp liên kết dữ liệu (data link) là phân lớp thứ hai trong mô hình OSI. Lớp liên kết dữ liệu bảo đảm truyền dữ liệu tin cậy giữa các đầu cuối cục bộ (local). Lớp liên kết dữ liệu được chia thành hai phân lớp con là: Điều khiển liên kết logic (LLC) và điều khiển truy cập (MAC). Giao thức tầng liên kết dữ liệu định nghĩa khuôn dạng đơn vị dữ liệu cho trao đổi giữa các nút ở mỗi đầu của đường truyền. Công việc của giao thức liên kết dữ liệu khi gửi và nhận frame bao gồm: Phát hiện lỗi, truyền lại, điều khiển lưu lượng và truy cập ngẫu nhiên.

2.2. LỚP MẠNG [6],[7]

Lớp mạng tương ứng với lớp thứ ba trong mô hình tham chiếu OSI. Lớp mạng sử dụng những giao thức nhằm đảm bảo truyền dữ liệu giữa các trạm không kề nhau sao cho không có lỗi. Giao thức lớp mạng trong mô hình OSI chỉ ra cơ chế đánh địa chỉ cho gói tin nhằm đóng gói dữ liệu từ lớp transport và truyền đến đích. Cơ chế đóng gói lớp mạng cho phép nội dung của nó được truyền tới đích trong các mạng LAN hoặc mạng WAN với lượng thông tin overhead là tối thiểu.

Lớp mạng thực hiện 4 nhiệm vụ chính sau:

- Đánh địa chỉ cho gói tin, do vậy các gói có thể di chuyển được trong mạng. Tất cả các host trong mạng đều được cung cấp một địa chỉ IP duy nhất. Địa chỉ lớp mạng là địa chỉ logic, địa chỉ IPv4 hoặc IPv6. Địa chỉ IPv4 có 32bit và địa chỉ IPv6 có 128bit.
- Thực hiện phân mảng và đóng gói các segment của lớp transport rồi chuyển xuống lớp dưới.
- Định tuyến: Đây là chức năng rất quan trọng đối với lớp mạng. Định tuyến là tìm đường đi cho gói tin trên mạng để đến được đích. Định tuyến sẽ tìm đường đi tối ưu cho gói tin. Có nhiều giao thức định tuyến cho gói tin trong internet như RIP, OSPF…
- Giải đóng gói: Thực hiện khi gói tin đến đích, tại đây dữ liệu sẽ được giải đóng gói và gửi các segment lên lớp transport.

Trong mạng internet lớp mạng sử dụng giao thức IP để thực hiện chức năng của mình.

2.2.1. Giao thức IP

Giao thức mạng IP được thiết kế để liên kết các mạng máy tính sử dụng phương pháp truyền thông và nhận dữ liệu dưới dạng gói. Giao thức IP cho phép truyền các gói dữ liệu từ điểm nguồn tới điểm đích có địa chỉ cố định. Đơn vị dữ liệu được trao đổi là các gói dữ liệu. Các chức năng được thực hiện ở IP là:

- Đánh địa chỉ: tất cả các host trong mạng và trong liên mạng đều được cung cấp một địa chỉ IP duy nhất. Theo giao thức IP version 4, mỗi địa chỉ IP gồm 32bit và được chia làm 5 lớp A,B,C,D,E. Các lớp A,B,C được sử dụng để định danh các host trên các mạng. Lớp D được sử dụng cho quá trình truyền đa điểm còn lớp E để dự phòng.
- Định tuyến: giúp xác định đường đi (tuyến) cho gói tin khi được truyền trên mạng. Nó giúp lựa chọn đường đi tối ưu cho các gói dữ liệu. Nếu hai host cần liên lạc không nằm trên cùng một subnet thì bảng định tuyến sẽ được sử dụng để quyết định việc chuyển dữ liệu và các bộ định tuyến thường xuyên trao đổi và cập nhật thông tin trong bảng định tuyến tùy thuộc vào phương pháp định tuyến được sử dụng.
- Truyền đa điểm:

  Hiện nay có ba cách truyền các gói IP là:

  ✧ Truyền một điểm đích (unicast): các gói tin được truyền từ host nguồn đến host đích duy nhất.

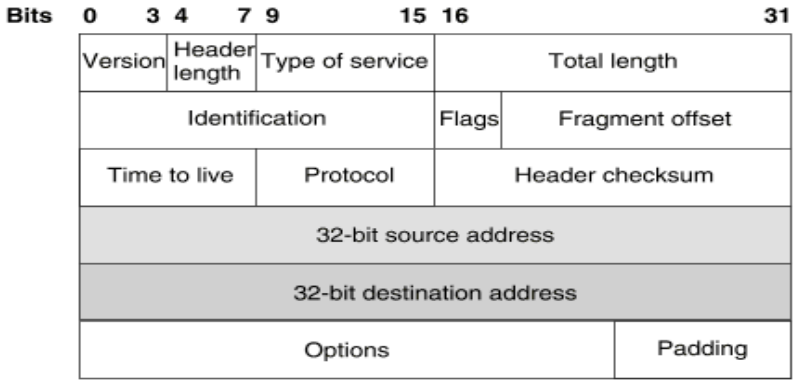
  ✧ Truyền quảng bá: gói tin được truyền đến tất cả các host trong mạng.

  ✧ Truyền đa điểm (multicast): gói tin được gửi đến một số các host nhất định trong mạng

Ngoài ra, giao thức IP còn cung cấp khả năng phân mảnh dữ liệu lớn thành các gói có kích thước nhỏ hơn để truyền qua mạng.

2.2.1.1. Giao thức IP phiên bản 4 (IPv4)

Cấu trúc của header IPv4 như sau:



Hình 2.2. Cấu trúc gói IP phiên bản 4

Ý nghĩa các trường như sau:

- Version: độ rộng 4 bit mô tả phiên bản IP
- IP Header Length(IHL): có độ rộng 4 bit, xác định độ rộng của phần tiêu đề của gói tin IP
- Type of Service: có độ rộng 8 bit, xác định các tham số chỉ dịch vụ sử dụng khi truyền gói tin qua mạng. Rất nhiều mạng cung cấp các dịch vụ về độ ưu tiên lưu thông, đặc biệt khi mạng bị quá tải. Việc lựa chọn này đảm bảo đường truyền đạt ba tiêu chuẩn là thời gian trễ, độ tin cậy, bộ thông suốt của gói tin. Được mô tả cụ thể như sau:
  - ✧ Quyền ưu tiên (3 bit)
  - ✧ Độ trễ D (1 bit)

    D=0: độ trễ bình thường

    D=1: độ trễ cao
  - ✧ Thông lượng T (1bit)

    T=0: thông lượng bình thường

    T=1: thông lượng cao
  - ✧ Độ tin cậy (1bit):

    R=0: độ tin cậy bình thường

    R=1: độ tin cậy cao
- Total Length (16bit): xác định độ dài của gói tin kể cả phần tiêu đề. Có giá trị tối đa là 65535 byte. Thông thường các host chỉ có thể xử lý gói

tin có độ dài là 576 byte gồm 512 byte dữ liệu và 64 byte tiêu đề. Các host chỉ có thể gửi các gói tin cố độ dài lớn hơn 576 byte khi biết trước là host đích có khả năng xử lý gói này.

- Indentification: cùng với trường địa chỉ nguồn, đích dùng để định danh duy nhất cho một gói tin trong khoảng thời gian nó tồn tại.
- Flag : có độ rộng 3 bit, chỉ độ phân đoạn của gói tin
  - ✧ Bit 0: luôn bằng 0
  - ✧ Bit 1 (DF):
    DF=0: có phân đoạn
    DF=1: không phân đoạn
  - ✧ Bit 2 (MF):
    MF=0: mảnh cuối cùng
    MF=1: không phải mảnh cuối cùng
- Fragment Offset: độ rộng 13 bit, chỉ rõ vị trí của phân mảnh trong gói tin tính theo đơn vị 64bit.
- Time to Live: độ rộng 8 bit, quy định thời gian tồn tại của gói tin.
- Protocol: độ rộng 8 bit, xác định giao thức tầng giao vận. Ví dụ
  - ✧ Protocol = 6: giao thức TCP
  - ✧ Protocol=17: giao thức UDP
- Header Checksum: độ rộng 16 bit, mã kiểm tra CRC-16 của phần tiêu đề cho phát hiện lỗi.
- Source Address: độ rộng 32 bit, xác định địa chỉ nguồn.
- Destination Address: độ rộng 32 bit, xác định địa chỉ đích.
- Option: có độ dài thay đổi để lưu thông tin tùy biến của người dùng.
- Padding: có độ dài thay đổi, đảm bảo độ dài của header luôn là bội 32 bit.
- Data: có độ dài tối đa là 65535 byte chứa dữ liệu lớp cao hơn.

Đánh địa chỉ trong IPv4

Hệ thống địa chỉ này được thiết kế mềm dẻo qua một sự phân lớp, có 5 lớp địa chỉ IP là: A, B, C, D, E. Sự khác nhau cơ bản giữa các lớp địa chỉ này là ở khả năng tổ chức các cấu trúc con của nó.

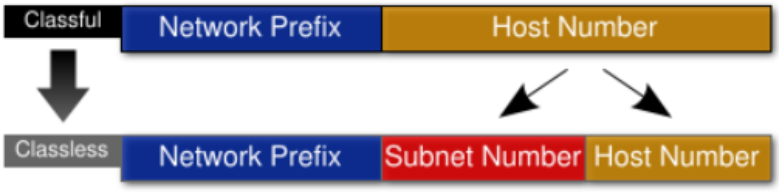
Lớp	Nhận dạng	Địa chỉ đầu	Địa chỉ cuối	Mặt nạ mạng
A	0xxx	0.0.0.0	127.255.255.255	255.0.0.0
B	10xx	128.0.0.0	191.255.255.255	255.255.0.0
C	110x	192.0.0.0	223.255.255.255	255.255.255.0
D	1110	224.0.0.0	239.255.255.255	
E	1111	240.0.0.0	255.255.255.255	

Địa chỉ lớp A: Lớp A sử dụng byte đầu tiên của 4 byte để đánh địa chỉ mạng. Như hình trên, nó được nhận ra bởi bit đầu tiên trong byte đầu tiên của địa chỉ có trị giá 0. Ba byte còn lại được sử dụng để đánh địa chỉ máy trong mạng. Có 126 địa chỉ lớp A với số máy tính trong mạng là 2^{24} – 2= 16.777.214 máy cho mỗi địa chỉ lớp A. Địa chỉ lớp A thường được cấp cho những tổ chức có số lượng máy tính lớn. Nguyên nhân chỉ có 126 network trong khi dùng 8 bit vì bit đầu tiên mang giá trị 0 dùng để định nghĩa lớp A. Do vậy còn lại 7 bit đánh từ 0 – 127, tuy nhiên người ta không sử dụng một địa chỉ chứa toàn các con số 1 hoặc 0 nên chỉ còn lại 126 mạng lớp A được sử dụng. Giá trị byte đầu tiên của lớp A sẽ luôn nằm trong khoảng từ 1 tới 126, mỗi một byte trong 3 byte còn lại sẽ có giá trị trong khoảng 1 đến 254.

Địa chỉ lớp B: Một địa chỉ lớp B được nhận ra bởi 2 bit đầu tiên của byte thứ nhất mang giá trị 10. Lớp B sử dụng 2 byte đầu tiên của 4 byte để đánh địa chỉ mạng và 2 byte cuối đánh địa chỉ máy trong mạng. Có 64*256 = 16.384 địa chỉ mạng lớp B với 2^{16} – 2= 65.534 máy cho mỗi địa chỉ lớp B.

Địa chỉ lớp C: Một số tổ chức có quy mô nhỏ có thể xin cấp phát địa chỉ lớp C. Một địa chỉ lớp C được nhận ra với 3 bit đầu mạng giá trị 110. Mạng lớp C sử dụng 3 byte đầu để đánh địa chỉ mạng và 1 byte cuối đánh địa chỉ máy trong mạng. Có 32*256*256= 2.097.152 địa chỉ mạng lớp C, mỗi địa chỉ lớp C có 256 – 2=254 máy.

Từ các lớp mạng cơ bản trên, ta có thể thực hiện chia subnet cho mạng để tạo thành các mạng con (subnet) tùy theo yêu cầu cụ thể. Phần dùng để đánh mạng con được lấy để đánh subnet được lấy từ phần dành đánh địa chỉ host.



Hình 2.3. Quy các địa chỉ IP khi chia subnet

Khi đó, để xác định địa chỉ mạng của trạm, ta cần phải biết mặt nạ mạng tương ứng với IP được chia. Ví dụ việc tính toán ra địa chỉ mạng của IP được tính như sau:

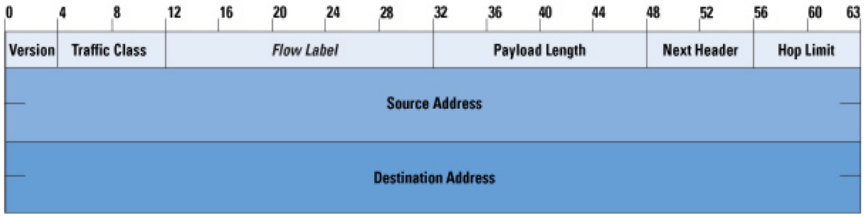
	Dạng thập phân	**Dạng nhị phân**
Địa chỉ IP của trạm	192.168.5.130	11000000.10101000.00000101.10000010
Mặt nạ mạng	255.255.255.192	11111111.11111111.11111111.11000000
Địa chỉ mạng	192.168.5.128	11000000.10101000.00000101.10000000

2.2.1.2. Giao thức IP phiên bản 6 (IPv6)

Trong IPv4 trường địa chỉ nguồn và đích có độ dài 32 bit nên không thể đáp ứng đủ nhu cầu đánh địa chỉ của mạng. Ngoài ra, do sự phát triển của Internet, bảng định tuyến của router không ngừng lớn lên và khả năng định tuyến đã bộc lộ hạn chế. Yêu cầu nâng cao chất lượng dịch vụ và bảo mật được đặt ra. IPv6 là giao thức Internet mới được kế thừa đặc điểm chính của IPv4 và có nhiều cải tiến để khắc phục những hạn chế:

- Tăng kích thước địa chỉ từ 32 bit lên 128 bit
- Phạm vi định tuyến đa điểm: giao thức này hỗ trợ phương thức truyền mới “anycasting”. Phương thức này sử dụng để gửi các gói tin đến một nhóm xác định.
- Phần tiêu đề của IPv6 được đơn giản hóa hơn IPv4. Điều đó cho phép xử lý gói tin nhanh hơn. Ngoài ra, IPv6 còn cung cấp một số tiêu đề phụ cho phép giao thức IPv6 có thể sử dụng một cách mềm dẻo hơn hẳn so với IPv4.

Cấu trúc gói tin IPv6 như sau:



Hình 2.4. Cấu trúc gói tin IP phiên bản 6

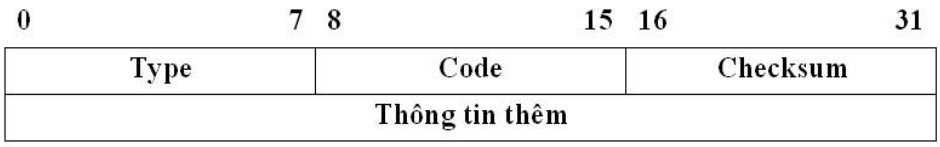
Ý nghĩa các trường như sau:

- Version: có giá trị bằng 6 với IPv6
- Traffic Class: độ dài 8 bit, xác định độ ưu tiên
- Flow Label: độ dài 20bit, xác định các gói dữ liệu được ưu tiên trên đường truyền nếu có xảy ra tranh chấp, thường được sử dụng cho các dịch vụ đòi hỏi chất lượng dịch vụ cao hay thời gian thực.
- Payload Length: độ dài 16 bit, xác định độ dài phần dữ liệu không tính phần tiêu đề.
- Hop Limit: độ dài 8 bit, giống như trường Time to Live của IPv4
- Source Address và Destination Address giống như IPv4 nhưng có độ dài 128bit.
- Data: có độ dài tối đa là 65535 byte.

2.2.2. Giao thức ICMP

Bên cạnh IP còn có các giao thức khác hỗ trợ chức năng điều khiển và định tuyến. Giao thức ICMP là một trong số đó. ICMP gửi các thông điệp về các vấn đề, tình trạng xảy ra trong môi trường mạng.

Khuôn dạng bản tin ICMP



Các bản tin ICMP được xác định nhờ vào trường code. Có các loại bản tin ICMP sau:

- Bản tin vọng và bản tin đáp ứng vọng.
- Bản tin Time Stamp và trả lời Time Stamp.

- Bản tin không gặp đích.
- Bản tin quench source.
- Bản tin định hướng lại.
- Bản tin báo tham số có lỗi.

2.3. TẦNG GIAO VẬN [6],[7]

Tầng giao vận nằm trên lớp thứ 3 trong mô hình mạng VoIP tương ứng với lớp 4 của mô hình tham chiếu OSI. Cung cấp dịch vụ truyền thông giữa các chương trình ứng dụng chạy trên các máy tính khác nhau. Tầng giao vận có 2 giao thức quan trọng TCP và UDP. Ngoài ra để phù hợp với các dịch vụ truyền thời gian thực trong lớp giao vận còn có giao thức SCTP.

Lớp transport có một số nhiệm vụ như:

- Cho phép nhiều ứng dụng truyền thông qua mạng tại cùng một thời điểm, trên cùng một thiết bị.
- Đảm bảo dữ liệu được nhận tin cậy khi sử dụng giao thức TCP, sắp xếp đúng gói tin cho từng loại ứng dụng khác nhau.
- Cung cấp cơ chế truyền lại trong trường hợp gói tin bị mất hoặc lỗi trong quá trình truyền từ nguồn tới đích.

Chức năng của lớp transport:

- Đảm bảo duy trì các kết nối riêng biệt giữa các ứng dụng khác nhau trên host nguồn và đích.
- Thực hiện phân mảnh tại nguồn và có cơ chế quản lý gói tin này.
- Ghép các mảnh dữ liệu tại đích để tạo thành luồng dữ liệu ứng dụng trước khi đẩy lên lớp ứng dụng.
- Có khả năng nhận diện các ứng dụng khác nhau. Điều này giúp cho lớp transport có thể khởi tạo, duy trì, bảo dưỡng và kết thúc nhiều ứng dụng khác nhau trên cùng một thiết bị.

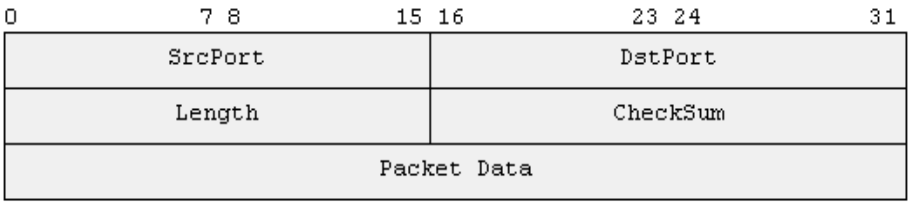
2.3.1. Giao thức UDP

UDP là giao thức lớp giao vận đơn giản, không hướng kết nối, được mô tả trong RFC768. Ứng dụng gửi bản tin tới socket UDP, sau đó được đóng gói

thành một UDP paragram và được truyền xuống lớp IP để gửi tới đích. Gói tin UDP được truyền mà không đảm bảo rằng nó có thể tới đích, giữ đúng thứ tự và đến đích một lần.

Nếu datagram tới đích nhưng trường kiểm tra tổng (checksum) có lỗi hay gói tin bị drop ở trên mạng thì nó sẽ được truyền lại. Nếu muốn xác định được rằng gói tin đã tới đích thì cần rất nhiều tính năng trong ứng dụng: ACK từ đầu cuối khác, điều khiển việc truyền lại,..Mỗi một UDP datagram có chiều dài và được truyền lên cùng với dữ liệu cho lớp ứng dụng. Điều này khác với TCP là giao thức luồng byte (byte-stream protocol).

Chúng ta cũng có thể nói: UDP cung cấp dịch vụ không hướng kết nối. Ví dụ, client UDP có thể tạo một socket và gửi datagram tới server này và sau đó gửi một datagram khác cũng tới server khác. Cũng giống như server UDP có thể nhận nhiều datagram trên một socket UDP từ các client khác nhau.



Hình 2.5. Cấu trúc đơn vị dữ liệu UDP

2.3.2. Giao thức TCP

TCP là giao thức hướng kết nối và tin cậy. TCP thực hiện phân mảnh gói tin tại nguồn và trước khi gửi gói tin xuống lớp network nó chèn thêm một số thông tin điều khiển gọi là TCP header. Mỗi segment của TCP có 20byte header.

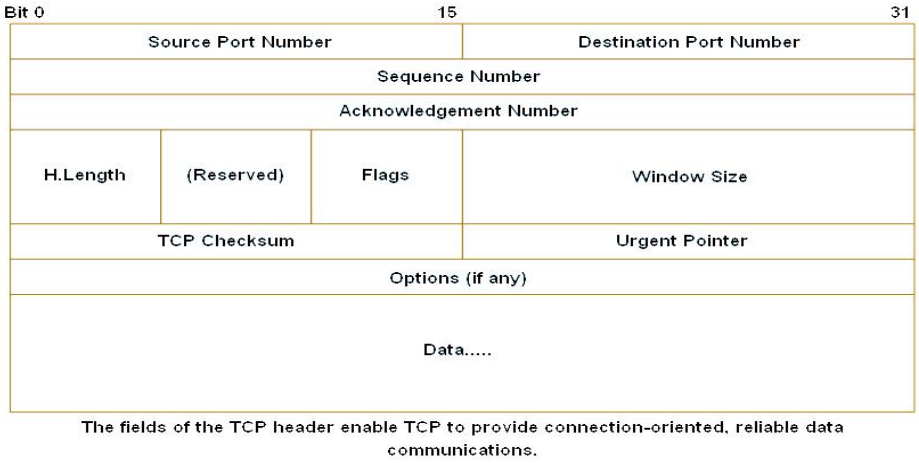
TCP cung cấp các chức năng:

- Truyền tin cậy với cơ chế ARQ, mỗi bản tin có số trình tự phát và trình tự thu riêng.
- Cung cấp thứ tự chính xác của các segment với cơ chế sắp xếp lại segments tại đích. Có cơ chế loại bỏ các bản tin kép.
- Cung cấp điều khiển luồng để kiểm soát tắc nghẽn bằng phương pháp sử dụng cửa sổ trượt.

Trong mạng giao thức TCP thích hợp cho các ứng dụng cần đảm bảo sự tin cậy và không yêu cầu thời gian thực như: web, mail, truyền file.

Trong mạng VoIP, TCP được sử dụng để truyền các bản tin báo hiệu như: H.225, H.245 vì các bản tin báo hiệu cần độ chính xác cao.

Header và ý nghĩa của các trường trong phần header TCP:



Hình 2.6. Trường TCP segment header

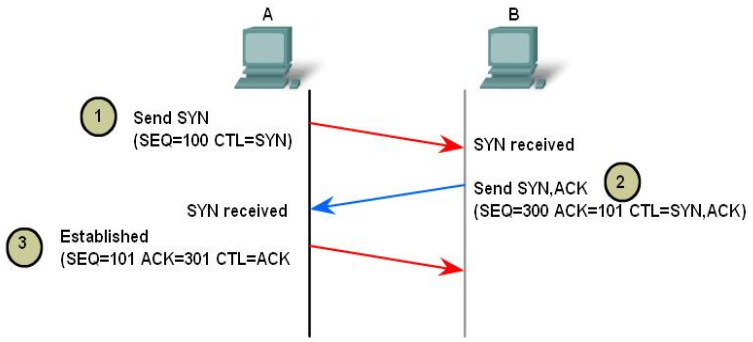
Ý nghĩa các trường như sau:

- Source Port & Destination Port: Chỉ số cổng nguồn và chỉ số cổng đích của mỗi ứng dụng. Mỗi ứng dụng sẽ có chỉ số cổng nguồn chỉ và số cổng đích khác nhau. Cổng nguồn và đích đều có 16bit do vậy có thể tạo được 65535 cổng khác nhau.
- Sequence Number: độ dài 32 bit. Được sử dụng đồng bộ dữ liệu truyền giữa nguồn và đích và sắp xếp chính xác dữ liệu tại đích.
- Acknowledgement Number (ACK): độ dài 32 bit, chỉ số này được gửi đến host nguồn. Thông báo cho host nguồn biết là đã nhận tốt byte thứ n và mong muốn nhân được byte thứ n+1 trong lần truyền tiếp theo.
- Window size: Dài 16bit dùng điều khiển luồng. Đích nhận gói tin căn cứ vào tài nguyên của mình có thể gửi thông tin về của sổ trượt (slidding windows) cho nguồn, yêu cầu nguồn gửi dữ liệu kích thước phù hợp.
- H.length: Dài 4 bit. Cho biết chiều dài phần header của bản tin TCP.
- Reserved: Dài 6bit. Là bít dự trữ chưa được sử dụng, được gán giá trị bằng 0.

- Flags:
    - URG: vùng Urgent Pointer có hiệu lực
    - ACK: vùng ACK có hiệu lực
    - PSH: chức năng Push
    - RST: khởi động lại liên kết
    - SYN: đồng bộ hóa các số hiệu tuần tự
    - FIN: không còn số liệu từ trạm cuối
- Checksum: Dài 16bit. Dùng để kiểm tra lỗi, sử dụng mã CRC16.
- Urgent Pointer: Dài 16bit. Là con trỏ trỏ tới số hiệu tuần tự của byte đi sau dữ liệu chuẩn, cho bên nhận biết được độ dài của dữ liệu.
- Option: có độ dài thay đổi, khai báo các lựa chọn của người dùng.
- TCP data: Là phần dữ liệu lớp trên có giá trị tối đa là 536 byte. Giá trị này có thể thay đổi nhờ khai báo trong phần Option.

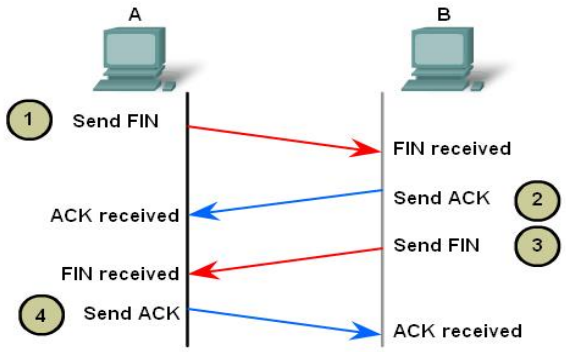
Trong một phiên TCP sử dụng: (TCP 3-way handshake SYN) bắt tay 3 bước để khởi tạo kết nối, truyền tin và hủy kết nối.

- Khởi tạo kết nối:
    1. Nguồn gửi bản tin SYN kèm theo sequence number đến đích để thiết lập kết nối.
    2. Đích gửi bản tin SYN chứa tham số ACK để khẳng định quá trình nhận dữ liệu tốt tới nguồn. bản tin này cũng chứa chỉ số sequence number và chỉ số này được sinh ra ngẫu nhiên.
    3. Khi nguồn nhận được bản tin SYN kèm theo ACK nó sẽ gửi bản tin thiết lập tới đích.



Hình 2.7. Khởi tạo phiên TCP

- Truyền tin: Sau khi thiết lập thông qua 3 bước trên, nguồn và đích thực hiện truyền dữ liệu kèm theo các thông tin điều khiển chứa trong header của TCP.
- Kết thúc phiên truyền: Khi không còn nhu cầu truyền dữ liệu nữa host sẽ gửi cờ FIN để kết thúc phiên truyền dữ liệu giữa hai host. Sau khi kết thúc phiên truyền dữ liệu, kết nối end-to-end giữa nguồn và đích sẽ được giải phóng.



Hình 2.8. Kết thúc phiên truyền dữ liệu

2.3.3. Giao thức SCTP

SCTP cũng như TCP và UDP là một giao thức tầng giao vận. SCTP được thiết kế thay cho TCP/UDP khi truyền báo hiệu SS7 qua mạng internet. Ban đầu SCTP chỉ được thiết kế với mục đích trên nhưng ngày nay SCTP đã được sử dụng rộng rãi và nó được xem như một thế hệ tiếp theo của giao thức TCP. SCTP là giao thức hướng kết nối và tin cậy đồng thời SCTP còn đảm bảo tính thời gian thực cho dữ liệu không giống như TCP. SCTP cung cấp các chức năng sau:

- Hỗ trợ đa luồng: Các bản tin độc lập với nhau trên một liên kết SCTP. Mỗi bản tin được gán cho một luồng riêng. Tất cả các bản tin trong một luồng được nhận theo đúng thứ tự bên gửi đã đánh dấu. Mỗi dữ liệu của luồng sẽ được nhận chính xác mà không bị lẫn lộn với các luồng khác. Với hỗ trợ đa luồng SCTP hỗ trợ các ứng dụng liên quan đến hợp kênh dữ liệu như: Thoại, video trên mỗi đường liên kết giữa hai đầu cuối.
- Liên kết đa điểm: Giữa hai đầu cuối trong quá trình thiết lập liên kết có thể xác định liên kết đa điểm. Có nhiều giao diện sẽ cho phép dữ liệu

gửi theo địa chỉ khác khi xảy ra lỗi. Giao thức TCP không thể thực hiện việc này.

- Hướng bản tin: Trong TCP, dữ liệu được gửi giữa hai đầu cuối là luồng các byte. Nếu cần thiết các ứng dụng phải làm chức năng định dạng khung cho bản tin. SCTP bản tin được giữ nguyên định dạng, bản tin không bị thay đổi ở hai đầu cuối. UDP cũng cung cấp hướng bản tin nhưng không tin cậy.
- Nhận bản tin không theo thứ tự: Giao thức TCP, tất cả các bản tin được nhận theo đúng thứ tự bên gửi. Đối với SCTP, cung cấp cơ chế nhận bản tin không theo thứ tự (giữa các luồng song song với nhau).
- Quy định thời gian sống của bản tin: SCTP có một tùy chọn cho phép xác định thời gian sống của bản tin. Nó cho phép ứng dụng truyền tin xác định khoảng thời gian mà bản tin còn có ích. Nếu thời gian sống của bản tin không còn, SCTP có thể hủy bỏ bản tin hoặc dừng việc cố gắng gửi nó vào mạng. Việc này giúp tiết kiệm băng thông tránh tắc nghẽ đường truyền.
- Syn cookie: SCTP khởi tạo liên kết bằng thủ tục bắt tay bốn bước với việc sử dụng cookie có dấu hiệu định trước.
- Khả năng kiểm soát lỗi mạnh: Với TCP và UDP trường checksum chỉ có 16bit còn SCTP trường này lên tới 32bit.

So sánh tính năng dịch vụ của SCTP,TCP, UDP

Services/Features	SCTP	TCP	UDP
Hướng liên kết	Có	Có	Không
Song công	Có	Có	Có
Tin cậy	Có	Có	Không
Tin cậy cục bộ	optional	Không	Không
Nhận dữ liệu có thứ tự	Có	Có	Không
Nhận dữ liệu không có thứ tự	Có	Không	Có
Điều khiển luồng	Có	Có	Không
Điều khiển tắc nghẽn	Có	Có	Không
Cơ chế ECN	Có	Có	Không
Selective ACKs	Có	Tùy chọn	Không
Hướng bản tin	Có	Không	Có
Tìm lại đường MTU	Có	Có	Không
Phân mảnh PDU tầng ứng dụng	Có	Có	Không

Bọc các PDU tầng ứng dụng	Có	Có	Không
Đa luồng	Có	Không	Không
Chống tấn công tràn SYN	Có	Không	Không
Kết nối half-closed	Không	Có	Không
Kiểm tra dữ liệu tới đích	Có	Có	Không

2.4. LỚP ỨNG DỤNG [6]

Lớp ứng dụng trong mạng VoIP là tầng liên quan trực tiếp đến người dùng. Tầng ứng dụng chứa một loạt các giao thức phục vụ cho ứng dụng voice.

- Các giao thức báo hiệu: H.323, SIP, MGCP, Megaco/H.248.
- Các giao thức truyền tin thời gian thực: RTP, RTCP, RSVP.
- Các chuẩn nén thoại, video: G.711, G.722, G.723.1, G.728, G.729, H.261, H.263.

Các giao thức báo hiệu sẽ được trình bày cụ thể trong chương sau. Trong chương này chỉ trình bày chi tiết về các giao thức hỗ trợ truyền tin thời gian thực.

2.4.1. Giao thức RTP

RTP (Real Time Transport Protocol-*Giao thức Vận chuyển Thời gian Thực*) là một giao thức dựa trên giao thức IP tạo ra các hỗ trợ để truyền tải các dữ liệu yêu cầu thời gian thực với các yêu cầu:

- Liên tục: Các gói tin phải được sắp xếp theo đúng thứ tự khi chúng đến bên nhận, các gói đến có thể không theo thứ tự và nếu gói tin bị mất thì bên nhận phải dò tìm hay bù lại sự mất các gói tin này.
- Sự đồng bộ trong các phương thức truyền thông: Các khoảng lặng trong tiếng nói được triệt tiêu hoặc nén lại để giảm thiểu băng thông cần thiết, tuy nhiên khi đến bên nhận, thời gian giữa các khoảng lặng này phải được khôi phục một cách chính xác.
- Sự đồng bộ giữa các phương thức truyền thông: Có thể tín hiệu thoại sử dụng một phương thức truyền thông trong khi tín hiệu video lại sử dụng một phương thức truyền thông khác, các tín hiệu tiếng và hình phải được đồng bộ một cách chính xác, gọi là sự đồng bộ tiếng - hình.

- Sự nhận diện phương thức truyền tải: Trong Internet, thông thường cần thay đổi sự mã hoá cho phương thức truyền tải (payload) trên hành trình truyền để hiệu chỉnh thay đổi độ rộng băng thông sẵn sàng hoặc đủ khả năng cho người dùng mới kết nối vào nhóm. Một vài cơ chế cần được sử dụng để nhận diện sự mã hoá cho mỗi gói đến.

Các dịch vụ cung cấp bởi RTP bao gồm:

- Đa phát đáp thân thiện: (multicast – friendly): RTP và RTCP là kỹ thuật cho đa phát đáp, cung cấp khả năng mở rộng cuộc hội thoại nhiều bên. Trên thực tế, chúng được thiết kế để có thể hoạt động trong cả các nhóm đa phát đáp nhỏ, phù hợp cho các cuộc điện đàm ba bên. Đối với các nhóm lớn, chúng sử dụng đa phát đáp quảng bá (broadcast).
- Độc lập thiết bị: RTP cung cấp các dịch vụ cần thiết chung cho phương thức truyền thông thời gian thực nói chung như thoại, video hay bất kì một bộ mã hoá, giải mã cụ thể nào có sự định nghĩa các phương thức mã hoá và giải mã riêng bằng các thông tin tiêu đề và định nghĩa.
- Các bộ trộn và chuyển đổi: Các bộ trộn là thiết bị nắm giữ phương thức truyền thông từ một vài người sử dụng riêng lẻ, để trộn hoặc nối chúng vào các dòng phương thức truyền thông chung, chuyển đổi chúng vào khuôn dạng khác và gửi nó ra. Các bộ chuyển đổi có ích cho sự thu nhỏ băng thông yêu cầu của dòng số liệu từ dòng số liệu chung trước khi gửi vào từng kết nối băng thông hẹp hơn mà không yêu cầu nguồn phát RTP thu nhỏ tốc độ bit của nó. Điều này cho phép các bên nhận kết nối theo một liên kết nhanh để vẫn nhận được truyền thông chất lượng cao. RTP hỗ trợ cả các bộ trộn và cả các bộ chuyển đổi.
- Mã hoá thành mật mã: Các dòng phương thức truyền thông RTP có thể mã hoá thành mật mã dùng các khoá, việc mã hoá đảm bảo cho việc thông tin trên mạng được an toàn hơn.

Các gói tin truyền trên mạng Internet có trễ. Nhưng các ứng dụng đa phương tiện yêu cầu một thời gian thích hợp khi truyền các dữ liệu và phát lại. RTP cung cấp các cơ chế bảo đảm thời gian, số thứ tự và các cơ chế khác liên quan đến thời gian. Bằng các cơ chế này RTP cung cấp sự truyền tải dữ liệu thời gian thực giữa các đầu cuối qua mạng.

Bản thân RTP không cung cấp một cơ chế nào cho việc bảo đảm phân phối kịp thời các dữ liệu tới các trạm mà nó dựa trên các dịch vụ của tầng thấp hơn để thực hiện điều này. RTP cũng không đảm bảo việc truyền các gói theo đúng thứ tự. Tuy nhiên, số thứ tự trong RTP header cho phép bên thu xây dựng lại đúng thứ tự các gói của bên phát.

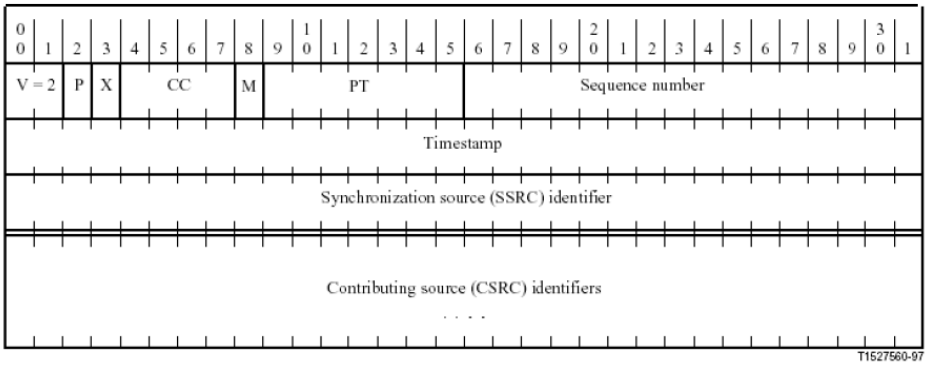
Hoạt động của RTP được hỗ trợ bởi một giao thức khác là RTCP để nhận các thông tin phản hồi về chất lượng truyền dẫn và các thông tin về thành phần tham dự các phiên hiện thời. Không giống như các giao thức khác là sử dụng các trường trong header để thực hiện các chức năng điều khiển, RTP sử dụng một cơ chế điều khiển độc lập trong định dạng của gói tin RTCP để thực hiện các chức năng này.

Khuôn dạng bản tin RTP:

RTP header bao gồm một phần cố định có ở mọi gói RTP và một phần mở rộng phục vụ cho các mục đích nhất định.

Phần cố định:

Có độ dài không đổi.



Hình 2.9. Phần cố định của đơn vị dữ liệu RTP

- Version (2 bits): Chỉ ra version của RTP, hiện nay là version 2.
- Padding (1 bit): Nếu bit này được đặt, sẽ có thêm một vài octets thêm vào cuối gói dữ liệu. Các octets này không phải là thông tin, chúng được thêm vào để nhằm mục đích:
  - ✧ Phục vụ cho một vài thuật toán mã hoá thông tin cần kích thước của gói cố định.

- ✧ Dùng để cách ly các gói RTP trong trường hợp có nhiều gói thông tin được mang trong cùng một đơn vị dữ liệu của giao thức ở tầng dưới.

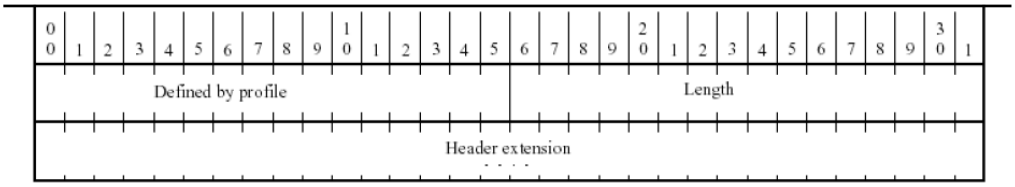
- Extension (1 bit): Nếu bit này được đặt, thì theo sau phần header cố định sẽ là một header mở rộng.
- Contributing Sources Count (4 bits): số lượng các thành phần nhận dạng nguồn CSRC nằm trong phần header gói tin. Số này lớn hơn 1 nếu các gói tin RTP đến từ nhiều nguồn.
- Marker (1 bit): Mang ý nghĩa khác nhau, tuỳ theo từng trường hợp cụ thể, được chỉ ra trong hiện trạng (profile) đi kèm.
- Payload Type (7 bits): Chỉ ra loại tải trọng mang trong gói. Các mã sử dụng trong trường này ứng với các loại tải trọng được quy định trong một profile đi kèm.
- Sequence Number (16 bits): mang số thứ tự của gói RTP. Số này được tăng thêm 1 sau mỗi gói RTP được gửi đi. Có thể được sử dụng để phát hiện được sự mất gói và khôi phục mất gói tại đầu thu. Giá trị khởi đầu của trường này là ngẫu nhiên.
- Time stamp (tem thời gian, 32 bits): Phản ánh thời điểm lấy mẫu của octet đầu tiên trong gói RTP. Thời điểm này được lấy từ một đồng hồ tăng đều đặn và tuyến tính theo thời gian để cho phép việc đồng bộ và tính toán độ jitter. Tần số đồng hồ này không cố định, tuỳ thuộc vào loại tải trọng. Giá trị khởi đầu được chọn ngẫu nhiên. Một vài gói RTP có thể mang cùng một giá trị "Tem thời gian" nếu như chúng được phát đi cùng lúc về mặt logic. Nếu gói dữ liệu được phát ra đều đặn thì "tem thời gian" được tăng một cách đều đặn. Trong trường hợp khác thì giá trị "tem thời gian" tăng không đều. "Tem thời gian" là thành phần thông tin quan trọng nhất trong các ứng dụng thời gian thực. Người gửi thiết lập các "tem thời gian" ngay thời điểm octet đầu tiên của gói được lấy mẫu. "Tem thời gian" tăng dần theo thời gian đối với mọi gói. Sau khi nhận được gói dữ liệu, bên thu sử dụng các "tem thời gian" này nhằm khôi phục thời gian gốc để chạy các dữ liệu này với tốc độ thích hợp. Ngoài ra, nó còn được sử dụng để đồng bộ các dòng dữ liệu khác

nhau (chẳng hạn như giữa hình và tiếng). Tuy nhiên RTP không thực hiện đồng bộ mà các ứng dụng phía trên sẽ thực hiện sự đồng bộ này.

- Synchronization Source Identifier (SSRC, 32 bits): chỉ ra nguồn đồng bộ của gói RTP, số này được chọn ngẫu nhiên. Trong 1 phiên RTP có thể có nhiều hơn một nguồn đồng bộ. Mỗi một nguồn phát ra một luồng RTP. Bên thu nhóm các gói của cùng một nguồn đồng bộ lại với nhau để phát lại tín hiệu thời gian thực.
- Contributing Source Identifier (CSRC, từ 0-15 mục, mỗi mục 32 bits): chỉ ra những nguồn đóng góp thông tin vào phần tải trọng của gói. Giúp bên thu nhận biết được gói tin này mang thông tin của những nguồn nào.

Phần mở rộng:

Có độ dài thay đổi. Sự tồn tại phụ thuộc vào bit Extension của phần cố định.



Hình 2.10. Phần mở rộng cấu trúc dữ liệu RTP

- 16 bit đầu tiên được sử dụng với mục đích riêng cho từng ứng dụng được định nghĩa bởi profile. Thường được dùng để phân biệt các loại header mở rộng.
- Length (16 bits): giá trị chiều dài phần header mở rộng tính theo đơn vị 32 bit, không bao gồm 32 bit đầu tiên của phần header mở rộng.

Thực tế RTP được thực hiện chủ yếu trong các ứng dụng mà tại các mức ứng dụng này có các cơ chế khôi phục lại gói bị mất, điều khiển tắc nghẽn.

Mạng Internet hiện nay vẫn chưa thể đáp ứng được đầy đủ các yêu cầu của các dịch vụ thời gian thực. Các dịch vụ RTP yêu cầu băng thông cao có thể làm giảm chất lượng các dịch vụ khác trong mạng đến mức nghiêm trọng. Trong quá trình triển khai phải chú ý đến giới hạn băng thông sử dụng của các ứng dụng trong mạng.

2.4.2. Giao thức RTCP

Giao thức RTCP (Real-time Transport Control Protocol) là giao thức hỗ trợ cho RTP có chức năng điều khiển, kiểm soát bản tin RTP. Giao thức RTCP dựa vào việc truyền đều đặn các gói điều khiển tới tất cả các người tham gia vào phiên truyền. Các dịch vụ mà RTCP cung cấp là:

- Giám sát chất lượng và điều khiển tắc nghẽn: Đây là chức năng cơ bản của RTCP. Nó cung cấp thông tin phản hồi tới một ứng dụng về chất lượng phân phối dữ liệu. Thông tin điều khiển này rất hữu ích cho các bộ phát, bộ thu và giám sát. Bộ phát có thể điều chỉnh cách thức truyền dữ liệu dựa trên các thông báo phản hồi của bộ thu. Bộ thu có thể xác định được tắc nghẽn là cục bộ, từng phần hay toàn bộ. Người quản lý mạng có thể đánh giá được hiệu suất mạng.
- Xác định nguồn: Trong các gói RTP, các nguồn được xác định bởi các số ngẫu nhiên có độ dài 32 bít, các số này không thuận tiện đối với người sử dụng. RTCP cung cấp thông tin nhận dạng nguồn cụ thể hơn ở dạng văn bản. Nó có thể bao gồm tên người sử dụng, số điện thoại, địa chỉ e-mail và các thông tin khác.
- Đồng bộ môi trường: Các thông báo của bộ phát RTCP chứa thông tin để xác định thời gian và nhãn thời gian RTP tương ứng. Chúng có thể được sử dụng để đồng bộ giữa âm thanh với hình ảnh.
- Điều chỉnh thông tin điều khiển: Các gói RTCP được gửi theo chu kỳ giữa những người tham dự. Khi số lượng người tham dự tăng lên, cần phải cân bằng giữa việc nhận thông tin điều khiển mới nhất và hạn chế lưu lượng điều khiển. Để hỗ trợ một nhóm người sử dụng lớn, RTCP phải cấm lưu lượng điều khiển rất lớn đến từ các tài nguyên khác của mạng. RTP chỉ cho phép tối đa 5% lưu lượng cho điều khiển toàn bộ lưu lượng của phiên làm việc. Điều này được thực hiện bằng cách điều chỉnh tốc độ phát của RTCP theo số lượng người tham dự. Mỗi người tham gia một phiên truyền RTP phải gửi định kỳ các gói RTCP đến tất cả những người khác cũng tham gia phiên truyền. Nhờ vậy mà có thể theo dõi được số người tham gia.

Gói RTCP góp phần làm tăng nghẽn mạng. Băng thông yêu cầu bởi RTCP là 5% tổng số băng thông phân bổ cho phiên. Khoảng thời gian trung bình giữa các gói RTCP được đặt tối thiểu là 5s.

Các loại thông báo điều khiển chính được RTCP cung cấp là:

- SR (Sender Report): chứa các thông tin thống kê liên quan tới kết quả truyền như tỷ lệ tổn hao, số gói dữ liệu bị mất, khoảng trễ. Các thông báo này phát ra từ phía phát trong 1 phiên truyền thông.
- RR (Receiver Report): Chứa các thông tin thống kê liên quan tới kết quả nhận, được phát từ phía thu trong 1 phiên truyền thông.
- SDES (Source Description): thông số mô tả nguồn (tên, vị trí…)
- APP (Application): cho phép truyền các dữ liệu ứng dụng
- BYE: chỉ thị sự kết thúc tham gia vào phiên truyền.

Chương 3

MẠNG VOIP VỚI CÁC GIAO THỨC BÁO HIỆU H.323/SIP

Trong chương một của đồ án đã đề cập đến một mô hình tổng quan về mạng VoIP. Trên thực tế, từ khi dịch vụ mạng VoIP hình thành và phát triển các tổ chức quốc tế và các nhà khai thác dịch vụ mạng luôn tìm kiếm các công cụ khai thác hiệu quả nhất. Dựa trên các bộ giao thức khác nhau, mô hình mạng VoIP cũng thay đổi theo với các chuẩn phù hợp với các giao thức đó. Trong chương này của đồ án sẽ trình bày chi tiết về mô hình mạng với chuẩn được ứng dụng.

3.1. MẠNG VOIP VỚI CHUẨN H.323 [1],[4]

Khi đề cập đến thoại IP, tiêu chuẩn quốc tế thường được đề cập đến là H.323. Giao thức H.323 được phát triển bởi ITU-T, H.323 cung cấp nền tảng kỹ thuật cho truyền thông đa phương tiện như: Audio thời gian thực, video và thông tin dữ liệu qua mạng chuyển mạch gói.

H.323 phiên bản đầu tiên được ITU-T đưa ra vào năm 1996. Trong quá trình phát triển H.323 đã được nâng cấp và sửa đổi để ngày càng hoàn thiện. Các phiên bản muộn hơn của H.323 được đưa ra vào các năm: H.323 v1 năm 1998, H.323 v2 năm 1999, H.323 v3 năm 2000, H.323 v4 năm 2003, H.323 v5 năm 2005, H.323 v6 năm 2006.

Đi kèm theo chuẩn H.323 là một chồng các giao thức bao gồm chức năng thiết lập, điều khiển, quản lý thông tin đa phương tiện và quản lý băng thông, ngoài ra còn cung cấp các giao diện giữa LAN và các mạng khác.

3.1.1. Thành phần mạng VoIP với chuẩn H.323

3.1.1.1.Thiết bị đầu cuối H.323 (H.323 Endpoint)

- Các thiết bị nằm ngoài phạm vi khuyến nghị H.323
  - Thiết bị vào ra Video.
  - Thiết bị vào ra Audio.
  - Thiết bị vào ra số liệu.

- Giao diện mạng LAN.
- Giao diện người sử dụng.

❖ Các phần tử nằm trong phạm vi khuyến nghị H.323

- Bộ mã hoá và giải mã Video.
- Bộ mã hoá và giải mã Audio.
- Bộ đệm nhận dữ liệu.
- Khối điều khiển hệ thống.

❖ Khối điều khiển theo chuẩn H.245

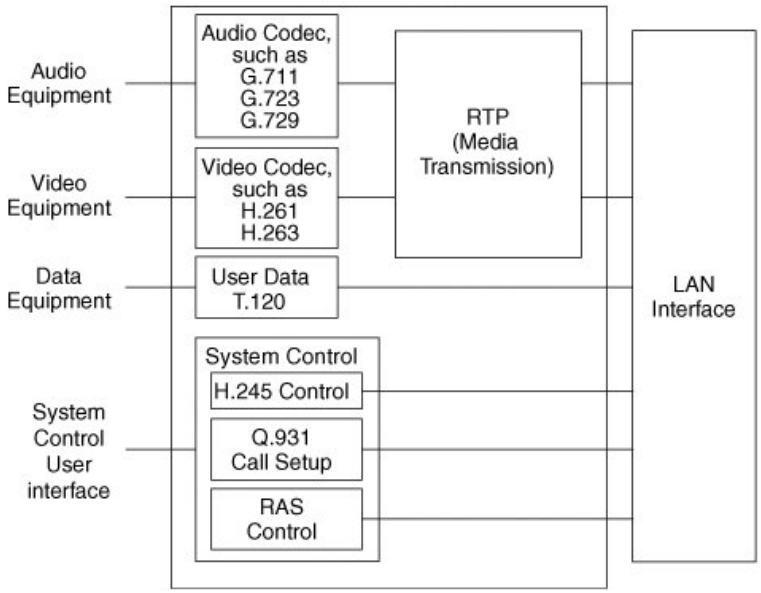
Sử dụng kênh điều khiển H.245 để mang các bản tin điều khiển điểm - điểm điều khiển hoạt động của thực thể H.323 đó bao gồm : khả năng trao đổi, mở và đóng các kênh logic, các yêu cầu chế độ hoạt động thích hợp, điều khiển luồng bản tin, phát các lệnh và các chỉ thị.

❖ Điều khiển báo hiệu cuộc gọi

Sử dụng báo hiệu cuộc gọi theo khuyến nghị H.225 để thiết lập một kết nối giữa hai đầu cuối H.323. Kênh báo hiệu cuộc gọi độc lập với kênh RAS và kênh điều khiển H.245. Trong hệ thống không có Gatekeeper thì kênh báo hiệu cuộc gọi được thiết lập giữa hai đầu cuối H.323 tham gia cuộc gọi. Còn trong hệ thống có Gatekeeper thì kênh báo hiệu cuộc gọi được thiết lập giữa các đầu cuối và Gatekeeper hoặc giữa hai đầu cuối với nhau, việc lựa chọn phương án thiết lập kênh báo hiệu cuộc gọi như thế nào là do Gatekeeper quyết định.

❖ Chức năng báo hiệu RAS

Sử dụng các bản tin H.225 để thực hiện: đăng ký, cho phép dịch vụ, thay đổi băng thông, trạng thái, các thủ tục tách rời giữa các đầu cuối và Gatekeeper.



Hình 3.1.Sơ đồ khối thiết bị đầu cuối H.323

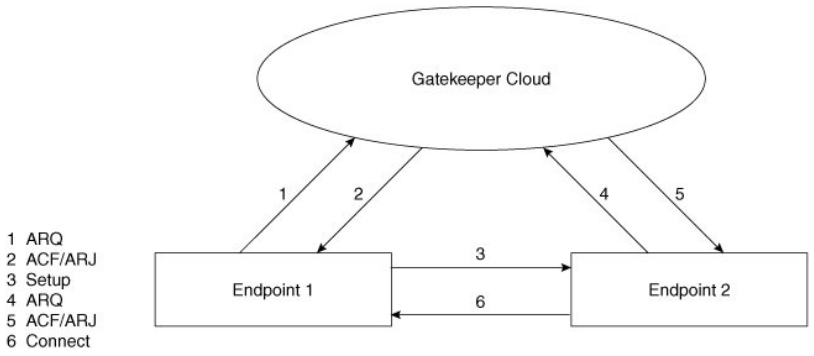
3.1.1.2. Gatekeeper

Một miền H.323 trên cơ sở mạng IP là tập hợp tất cả các đầu cuối được gán với một bí danh. Mỗi miền được quản trị bởi một Gatekeeper duy nhất, là trung tâm đầu não, đóng vai trò giám sát mọi hoạt động trong miền đó. Đây là thành phần tuỳ chọn trong hệ thống VoIP theo chuẩn H.323. Tuy nhiên nếu có mặt Gatekeeper trong mạng thì các đầu cuối H.323 và các Gateway phải hoạt động theo các dịch vụ của Gatekeeper đó. Mọi thông tin trao đổi của Gatekeeper đều được định nghĩa trong RAS. Mỗi người dùng tại đầu cuối được Gatekeeper gán cho một mức ưu tiên duy nhất. Mức ưu tiên này rất cần thiết cho cơ chế báo hiệu cuộc gọi mà cùng một lúc nhiều người sử dụng. H.323 định nghĩa cả những tính chất bắt buộc tối thiểu phải có cho Gatekeeper và những đặc tính tuỳ chọn:

- Các chức năng bắt buộc tối thiểu của một Gatekeeper gồm : Phiên dịch địa chỉ, điều khiển cho phép truy nhập, điều khiển dải thông, quản lý miền dịch vụ.
- Các chức năng tuỳ chọn của Gatekeeper gồm có : Báo hiệu điều khiển cuộc gọi, cấp phép cho cuộc gọi, quản lý cuộc gọi.

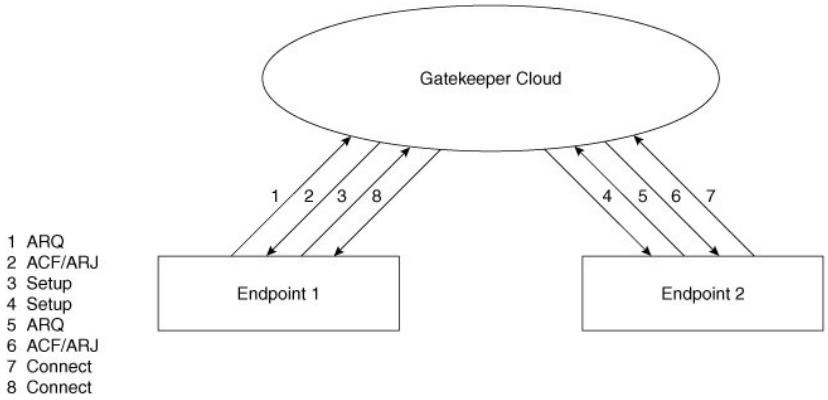
Gatekeeper hoạt động ở hai chế độ :

- Chế độ trực tiếp: Gatekeeper chỉ có nhiệm vụ cung cấp địa chỉ đích mà không tham gia vào các việc định tuyến các bản tin báo hiệu.



Hình 3.2. Phương thức định tuyến trực tiếp

- Chế độ định tuyến qua Gatekeeper : Gatekeeper là thành phần trung gian, định tuyến mọi bản tin báo hiệu trong mạng H.323.



Hình 3.3. Phương thức định tuyến qua Gatekeeper

Các chức năng cụ thể của Gatekeeper được mô tả như sau:

- Chức năng dịch địa chỉ: Gatekeeper sẽ thực hiện chuyển đổi địa chỉ URI (dạng tên gọi hay địa chỉ hộp thư) của một đầu cuối hay Gateway sang địa chỉ truyền dẫn (địa chỉ IP). Việc chuyển đổi được thực hiện bằng cách sử dụng bản đối chiếu địa chỉ được cập nhật thường xuyên bởi các bản tin đăng ký. Cũng có thể là việc chuyển đổi từ quy cách đánh số E.164 sang dạng URI.
- Điều khiển truy cập: Gatekeeper cho phép một truy cập mạng LAN bằng cách sử dụng các bản tin H.225 là ARQ/ACF/ARJ. Việc điều

khiển này dựa trên sự cho phép cuộc gọi, băng thông, hoặc một vài thông số khác do nhà sản xuất quy định. Nó có thể là chức năng rỗng có nghĩa là chấp nhận mọi yêu cầu truy nhập của đầu cuối.

- Điều khiển độ rộng băng thông: Gatekeeper hỗ trợ các bản tin BRQ/BRJ/BCF cho việc quản lý băng thông. Nó có thể là chức năng rỗng nghĩa là chấp nhận mọi yêu cầu thay đổi băng thông. Gatekeeper có thể hạn chế một số các đầu cuối H.323 cùng một lúc sử dụng mạng. Thông qua việc sử dụng kênh báo hiệu H.225, Gatekeeper có thể loại bỏ các các cuộc gọi từ một đầu cuối do sự hạn chế băng thông. Điều đó có thể xảy ra nếu Gatekeeper thấy rằng không đủ băng thông sẵn có trên mạng để trợ giúp cho cuộc gọi. Việc từ chối cũng có thể xảy ra khi một đầu đang tham gia một cuộc gọi yêu cầu thêm băng thông. Nó có thể là một chức năng rỗng nghĩa là mọi yêu cầu truy nhập đều được đồng ý.
- Quản lý miền dịch vụ: ở đây miền dịch vụ (domain) nghĩa là tập hợp tất cả các phần tử H.323 gồm thiết bị đầu cuối. Gateway, MCU có đăng ký hoạt động với Gatekeeper để thực hiện liên lạc giữa các phần tử trong miền dịch vụ hay từ dịch vụ này sang dịch vụ khác.
- Điều khiển báo hiệu cuộc gọi: Gatekeeper có thể lựa chọn hai phương thức điều khiển báo hiệu cuộc gọi là: hoàn thành báo hiệu cuộc gọi với các đầu cuối và xử lý báo hiệu cuộc gọi chính bản thân nó, hoặc Gatekeeper có thể ra lệnh cho các đầu cuối kết nối một kênh báo hiệu cuộc gọi hướng tới nhau. Theo phương thức này thì Gatekeeper không phải giám sát báo hiệu trên kênh H.225.
- Quản lý cuộc gọi: Một ví dụ cụ thể về chức năng này là Gatekeeper có thể lập một danh sách tất cả các cuộc gọi H.323 hướng đi đang thực hiện để chỉ thị rằng một đầu cuối bị gọi đang bận và cung cấp thông tin cho chức năng quản lý băng thông.

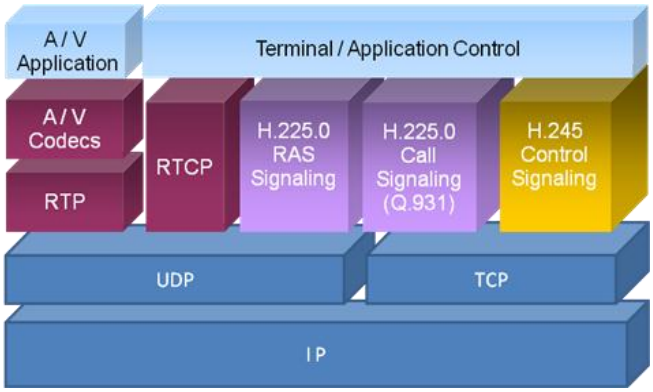
3.1.1.3.Khối điều khiển đa điểm

Khối điều khiển đa điểm (MCU) được sử dụng khi một cuộc gọi hay hội nghị cần giữ nhiều kết nối hoạt động. Do có một số hữu hạn các kết nối đồng thời, nên các MCU giám sát sự thoả thuận giữa các đầu cuối và sự kiểm tra mọi đầu cuối về tính năng mà chúng có thể cung cấp cho hội nghị hoặc

cuộc gọi. Các MCU gồm hai phần: Bộ điều khiển đa điểm (MC) và Bộ xử lý đa điểm (MP).

Bộ điều khiển đa điểm có trách nhiệm trong việc thoả thuận và quyết định khả năng của các đầu cuối. Trong khi đó bộ xử lý đa điểm được sử dụng để xử lý multimedia, các luồng trong suốt quá trình của một hội nghị hoặc một cuộc gọi đa điểm.

3.1.2.Giao thức H.323



Hình 3.4. Giao thức báo hiệu H.323

Giao thức H.323được chia làm 3 phần chính:

- Báo hiệu H.225 RAS (Registration, Admissions, and Status): báo hiệu giữa thiết bị đầu cuối với H.323 gatekeeper trước khi thiết lập cuộc gọi.
- Báo hiệu H.225 Q.931 sử dụng để kết nối, duy trì và hủy kết nối giữa hai đầu cuối.
- Báo hiệu H.245 sử dụng để thiết lập phiên truyền media sử dụng giao thức RTP.

3.1.2.1. Báo hiệu RAS

Báo hiệu RAS cung cấp điều khiển tiền cuộc gọi trong mạng H.323 có tồn tại gatekeeper và một vùng dịch vụ (do gatekeeper đó quản lý). Kênh RAS được thiết lập giữa các thiết bị đầu cuối và gatekeeper qua mạng IP. Kênh RAS được mở trước khi các kênh khác được thiết lập và độc lập với các

kênh điều khiển cuộc gọi và media khác. Báo hiệu này được truyền trên UDP cho phép đăng kí, chấp nhận, thay đổi băng thông, trạng thái và hủy.

Báo hiệu RAS chia làm các loại sau:

- Tìm kiếm Gatekeeper: việc này có thể được thực hiện thủ công hoặc tự động cho phép xác định gatekeeper mà thiết bị đầu cuối đăng kí; bao gồm:
  - Gatekeeper Request (GRQ): bản tin multicast gửi bởi thiết bị đầu cuối để tìm gatekeeper.
  - Gatekeeper Confirm (GCF): bản tin thông báo địa chỉ kênh RAS của gatekeeper cho thiết bị đầu cuối.
  - Gatekeeper Reject (GRJ): báo cho thiết bị đầu cuối biết rằng đã gatekeeper từ chối.
- Đăng kí: cho phép gateway, thiết bị đầu cuối và MCU tham gia vào một vùng dịch vụ do gatekeeper quản lý và thống báo cho gatekeeper về địa chỉ và bí danh của nó; bao gồm:
  - Registration Request (RRQ): được gửi từ thiết bị đầu cuối tới địa chỉ kênh RAS của gatekeeper.
  - Registration Confirm (RCF): được gửi bởi gatekeeper để xác nhận cho phép việc đăng kí bởi bản tin RRQ.
  - Registration Reject (RRJ): không chấp nhận đăng kí của thiết bị
  - Unregister Request (URQ): được gửi bởi thiết bị đầu cuối để hủy đăng kí với gatekeeper trước đó và được trả lời bằng Unregister Confirm (UCF) và Unregister Reject (URJ) (tương tự như trên).
- Xác định vị trí thiết bị đầu cuối: Thiết bị đầu cuối và gatekeeper sử dụng bản tin này để lấy thêm thông tin khi chỉ có thông tin ví danh được chỉ ra. Bản tin này được gửi thông qua địa chỉ kênh RAS của gatekeeper hoặc multicast. Loại bản tin này bao gồm:
  - Location Request (LRQ): được gửi để yêu cầu thông tin về thiết bị đầu cuối, gatekeeper, hay địa chỉ E.164.

- Location Confirm (LCF): được gửi bởi gatekeeper chức các kênh báo hiệu cuộc gọi hay địa chỉ kênh RAS của nó hay thiết bị đầu cuối đã yêu cầu.
- Location Reject (LRJ): được gửi bởi gatekeeper thông báo LRQ trước đó không hợp lệ.

❖ Admissions: bản tin giữa các thiết bị đầu cuối và gatekeeper cung cấp cơ sở cho việc thiết lập cuộc gọi và điều khiển băng thông sau này. Bản tin này bao gồm cả các yêu cầu về băng thông(có thể được thay đổi bởi gatekeeper). Loại bản tin này gồm:

- Admission Request (ARQ): Gửi bởi thiết bị đầu cuối để thiết lập cuộc gọi
- Admission Confirm (ACF): Cho phép thiết lập cuộc gọi. Bản tin này có chứa địa chỉ IP của thiết bị được gọi hay gatekeeper và cho phép gateway nguồn thiết lập cuộc gọi.
- Admission Reject (ARJ): không cho phép thiết bị đầu cuối thiết lập cuộc gọi.

❖ Thông tin trạng thái: dùng để lấy thông tin trạng thái của một thiết bị đầu cuối. Ta có thể sử dụng bản tin này để theo dõi trạng thái online hay offline của thiết bị đầu cuối trong tình trạng mạng bị lỗi. Thông thường bản tin này sẽ được gửi 10 giây một lần. Trong quá trình cuộc gọi, gatekeeper có thể yêu cầu thiết bị đầu cuối gửi theo chu kì các bản tin trạng thái. Loại bản tin này bao gồm:

- Information Request (IRQ): gửi từ gatekeeper tới thiết bị đầu cuối yêu cầu thông tin trạng thái.
- Information Request Response (IRR): được gửi từ thiết bị đầu cuối tới gatekeeper trả lời cho bản tin IRQ. Bản tin này cũng được gửi từ thiết bị đầu cuối tới gatekeeper theo chu kì.
- Status Enquiry Sent : Thiết bị đầu cuối hay gatekeeper có thể gửi bản tin này tới thiết bị đầu cuối khác để xác thực về trạng thái cuộc gọi.

❖ Điều khiển băng thông: Dùng để thay đổi băng thông cho cuộc gọi với các bản tin như sau:

- Bandwidth Request (BRQ): gửi bởi thiết bị đầu cuối để yêu cầu tăng hoặc giảm băng thông cuộc gọi
- Bandwidth Confirm (BCF): chấp nhận thay đổi yêu cầu bởi thiết bị đầu cuối.
- Bandwidth Reject (BRJ): không chấp nhận thay đổi yêu cầu bởi thiết bị đầu cuối.

❖ Hủy kết nối: Khi muốn kết thúc cuộc gọi thì trước hết thiết bị đầu cuối dừng hết mọi kết nối và đóng hết các kênh logic lại. Sau đó, nó sẽ ngắt phiên H.245 và gửi tín hiệu RLC trên kênh báo hiệu cuộc gọi. Ở bước này, nếu không có gatekeeper thì cuộc gọi sẽ được hủy còn nếu không thì các bản tin sau sẽ được gửi trên kênh RAS để kết thúc cuộc gọi:

- Disengage Request (DRQ): Gửi bởi thiết bị đầu cuối hay gatekeeper để kết thúc cuộc gọi.
- Disengage Confirm (DCF): Gửi bởi thiết bị đầu cuối hay gatekeeper để chấp nhận bản tin DRQ trước đó.
- Disengage Reject (DRJ): Được gửi bởi thiết bị đầu cuối hoặc gatekeeper thông báo không chấp nhận yêu cầu DRQ.

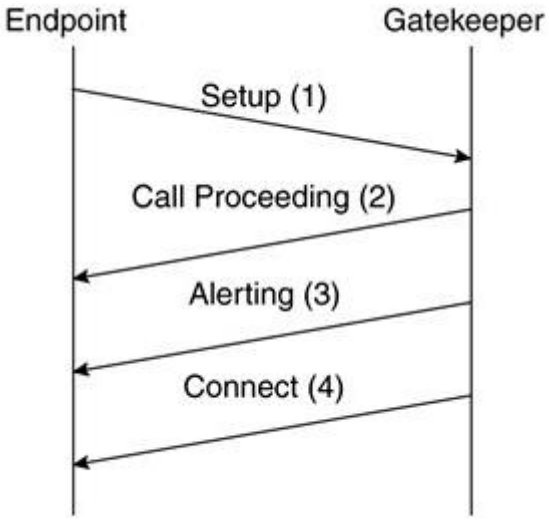
3.1.2.2. Giao thức điều khiển báo hiệu cuộc gọi H.225

Giao thức H.225 dùng để thiết lập liên kết giữa các điểm cuối H.323, thông qua liên kết dữ liệu thời gian thực sẽ được truyền đi. Quá trình báo hiệu cuộc gọi được bắt đầu bởi bản tin Setup được gửi đi trên kênh báo hiệu H.225, tiếp theo là một chuỗi các bản tin phục vụ cho quá trình thiết lập cuộc gọi. H.225 sử dụng các bản tin báo hiệu Q.931. Một kênh điều khiển báo hiệu được thiết lập dựa trên giao thức TCP/IP tại cổng 1720.

Các bản tin Q.931 và Q.932 thường được sử dụng trong báo hiệu cuộc gọi VoIP:

- Setup: Được gửi từ thực thể H.323 chủ gọi để cố gắng thiết lập kết nối tới thực thể H.323 bị gọi qua cổng 1720 TCP.
- Call Proceeding: thực thể bị gọi gửi bản tin này tới thực thể chủ gọi để chỉ thị rằng thủ tục thiết lập cuộc gọi đã được khởi tạo.
- Alerting: Được gửi từ thực thể bị gọi tới thực thể chủ gọi để chỉ thị rằng chuông bên đích bắt đầu rung.
- Connect: Được gửi từ thực thể bị gọi để thông báo rằng bên bị gọi đã trả lời cuộc gọi. Bản tin Connnect có thể mang địa chỉ truyền vận UDP/IP.
- Release Complete: Được gửi bởi một đầu cuối khởi tạo ngắt kết nối, nó chỉ thị rằng cuộc gọi đang bị giải phóng. Bản tin này chỉ có thể được gửi đi nếu kênh báo hiệu cuộc gọi được mở hoặc đang hoạt động.
- Facility: Đây là một bản tin Q.932 dùng để yêu cầu hoặc phúc đáp các dịch vụ bổ sung. Nó cũng được dùng để cảnh báo rằng một cuộc gọi sẽ được định tuyến trực tiếp hay thông qua GK.

Các bản tin trong quá trình thiết lập cuộc gọi như sau:



Hình 3.5. Q.931 trong thiết lập cuộc gọi

1. Thiết bị đầu cuối H.323 gửi bản tin Setup yêu cầu thiết lập cuộc gọi. Giả sử ở đây bản tin được gửi tới Gatekeeper (thiết lập cuộc gọi thông qua Gatekeeper).
2. Gatekeeper sẻ gửi trả lại bản tin Call Proceeding nhằm thông báo cho phía gọi rằng: Thiết bị này đang thực hiện thiết lập cuộc gọi.
3. Khi đầu cuối bị gọi rung chuông, Gatekeeper sẽ gửi bản tin Alerting về đầu cuối gọi thông báo về trạng thái này.
4. Khi người được gọi nhấc máy, bản tin Connect sẽ được gửi tới đầu cuối gọi thông báo cuộc gọi đã được thiết lập.
5. Cuộc gọi được thực hiện

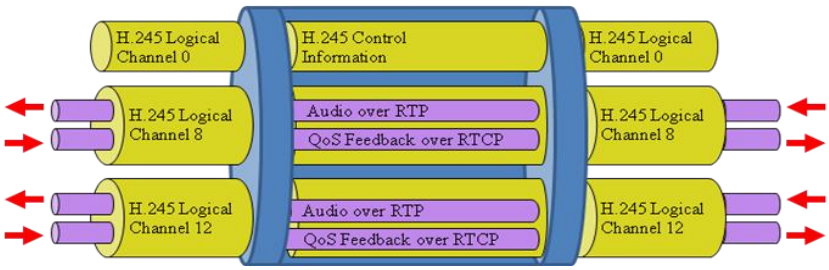
3.1.2.3. Giao thức H.245

Chức năng H.245 là thiết lập các kênh logic để truyền audio, video, data và các thông tin kênh điều khiển. Giữa hai thiết bị đầu cuối được thiết lập một kênh H.245 cho một cuộc gọi. Kênh điều khiển này được tạo dựa trên TCP gán động port. Chức năng điều khiển của kênh H.245 là thương lượng về một số thông số sau:

- Bộ mã hóa tiếng nói sẽ được sử dụng ở hai phía. Lấy ví dụ, chuẩn mã hóa tiếng nói và tốc độ bit tương ứng như sau: G.729 - 8 kbps, G.728 - 16 kbps, G.711 - 64 kbps, G.723 - 5.3 hay 6.3 kbps, G.722 - 48, 56, và 64 kbps…
- Thương lượng về Chủ/tớ giữa hai thiết bị đầu cuối: xác lập vai trò của các thiết bị trong khi thực hiện cuộc gọi tránh hiện tượng xung đột.
- Round-Trip Delay: xác định độ trễ giữa phía phát và phía thu. Dựa vào thông số này để xác định kết nối vẫn hoạt động.
- Báo hiệu trên kênh logic để thực hiện việc mở và đóng các kênh logic. Các kênh này được thiết lập trước khi thông tin được truyền đên đó. Báo hiệu này có thể thiết lập kênh đơn hướng hoặc song hướng. Sau khi kênh logic đã được thiết lập, cổng UDP cho kênh media RTP được truyền từ phía nhận tới phía phát. Khi sử dụng một hình định tuyến qua

Gatekeeper thì Gatekeeper sẽ chuyển hướng luồng RTP bằng cách cung cấp địa chỉ UDP/IP thực của thiết bị đầu cuối. Luồng RTP sẽ truyền trực tiếp giữa hai thiết bị đầu cuối với nhau.

Mỗi kênh media sử dụng RTP để truyền thời gian thực sẽ có một kênh phản hồi về chất lượng dịch vụ QoS theo chiều ngược lại giúp phía phát kiểm soát được luồng media truyền đi và có những điều chỉnh phù hợp.

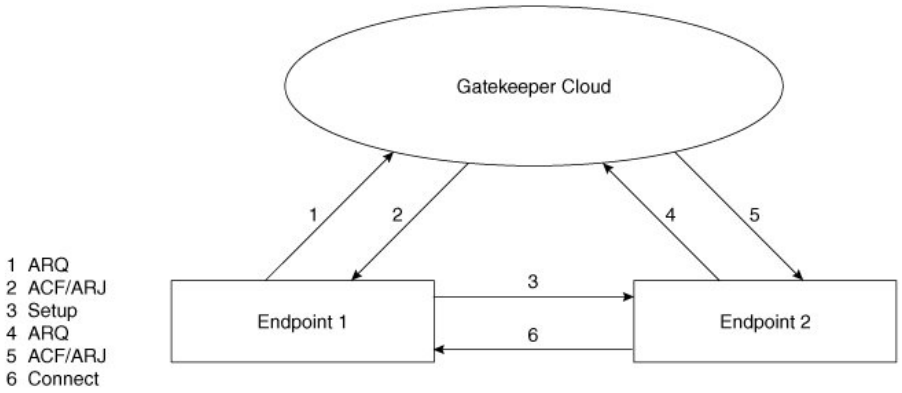


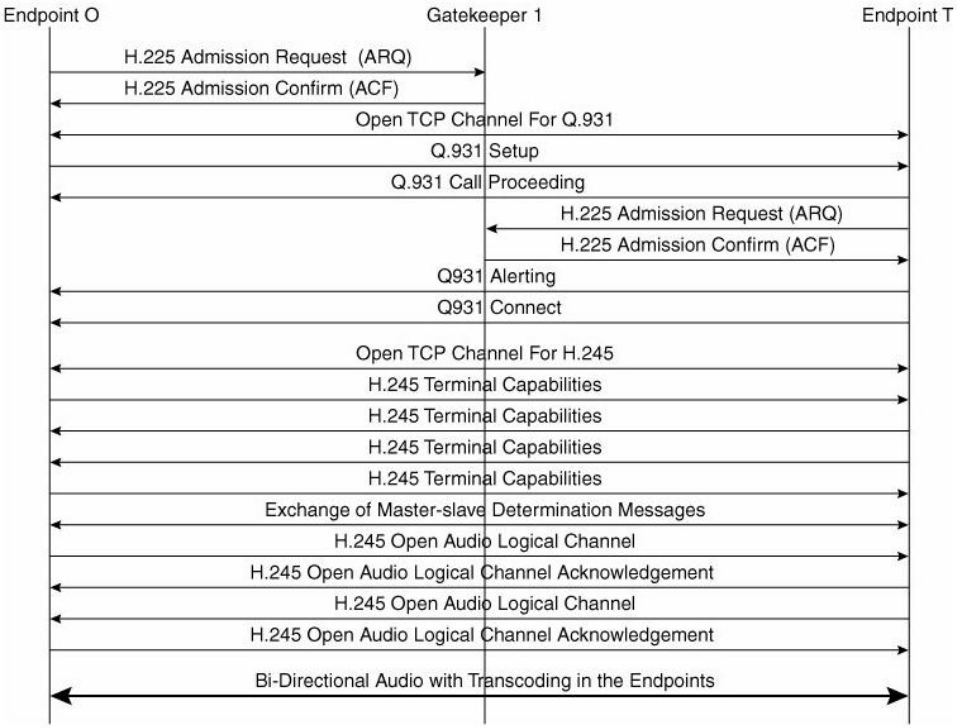
Hình 3.6. Cấu trúc luồng media giữa các đầu cuối

3.1.3. Thiết lập cuộc gọi VoIP sử dụng giao thức H.323

3.1.3.1. Báo hiệu trực tiếp giữa các thiết bị đầu cuối

Trong mô hình này, có chú ý là các thiết bị đầu cuối (Endpoint) chỉ xin phép Gatekeeper thực hiện cuộc gọi thông qua báo hiệu RAS còn các bước báo hiệu giữa các thiết bị này được thực hiện trực tiếp không thông qua Gatekeeper.





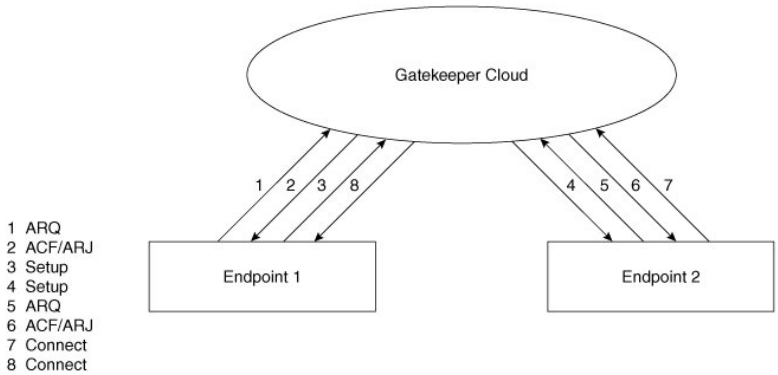
Hình 3.7. Thiết lập báo hiệu H.323 trực tiếp giữa các đầu cuối

- *Bước 1*: Endpoint O đăng kí với Gatekeeper yêu cầu cho phép thực hiện một cuộc gọi tới Endpoint T. Các bước thực hiện xác thực thuê bao gọi sẽ được thực hiện ở bước này. Gatekeeper trả lời cho phép Endpoint O thực hiện cuộc gọi và địa chỉ của chính xác của Endpoint T. Trong trường hợp này, hai Endpoint thực hiện cuộc gọi trực tiếp với nhau.
- *Bước 2*: Endpoint O và Endpoint T thiết lập một kết nối TCP cho báo hiệu H.225 để truyền các bản tin Q.931 cho phép thiết lập cuộc gọi. Endpoint O gửi bản tin Setup tới Endpoint T yêu cầu thiết lập cuộc gọi. Endpoint T trả lời bằng bản tin Call Proceeding thông báo cuộc gọi đang được thực hiện.
- *Bước 3*: Endpoint T xin phép Gatekeeper cho phép thực hiện cuộc gọi với Endpoint O. Gatekeeper trả lời đồng ý cho Endpoint T chấp nhận cuộc gọi. Endpoint T thực hiện rung chuông và báo cho Endpoint O biết là đang rung chuông người bị gọi.

- *Bước 4*: Người bị gọi nhấc ống nghe. Endpoint T gửi bản tin Conect tới Endpoint O thông báo kênh cuộc gọi đã được thiết lập. Lúc này, giữa hai Endpoint mở một kết nối TCP nữa cho kênh báo hiệu H.245 để thương lượng, thiết lập và duy trì kênh media.
- *Bước 5*: Khi đã thương lượng xong (các thông số được mô tả trong phần báo hiệu H.245), mỗi Endpoint yêu cầu mở một kết nối audio để truyền thoại. Như vậy sẽ tồn tại hai kênh cho phép thực hiện cuộc gọi hai chiều giữa hai thuê bao. Quá trình thoại được thực hiện hiện dựa trên giao thức RTP với sự kiểm soát của RTCP.

3.1.3.2. Báo hiệu được định tuyến thông qua Gatekeeper

Trong hình thức báo hiệu này thì mọi bản tin báo hiệu để được gửi qua Gatekeeper. Gatekeeper sẽ xử lý và chuyển tiếp bảo tin tới phía bị gọi. Khi đó, phía gọi không nhất thiết phải biết chính xác địa chỉ của phía bị gọi nhưng quá trình này sẽ bị trễ nhiều hơn.



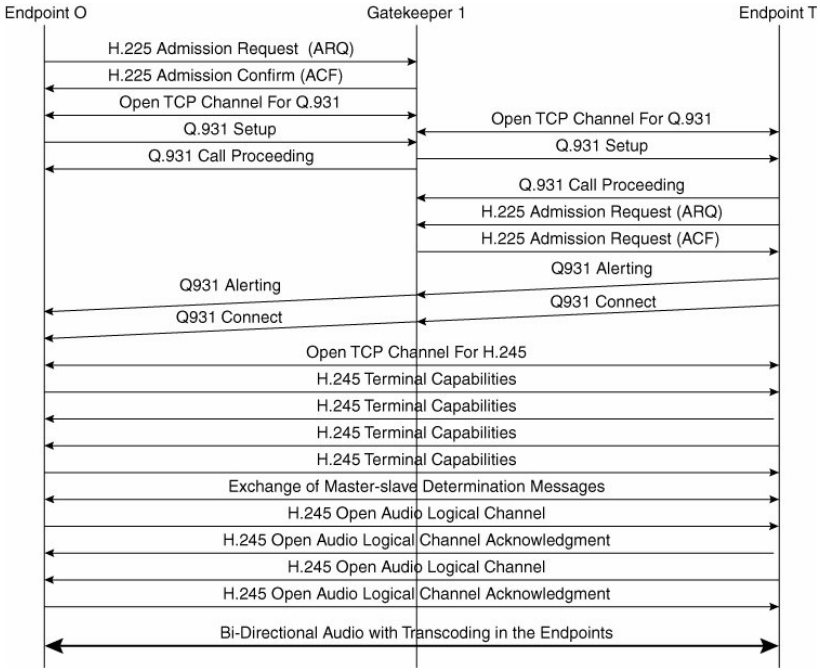
Các bản tin báo hiệu trong mô hình này gần như giống với trường hợp báo hiệu trực tiếp giữa hai thiết bị đầu cuối nhưng có một số chú ý như sau:

❖ Gatekeeper ở đây sẽ gồm có hai giao diện: giao diện với Endpoint O và Endpoint T. Việc phân biệt như vậy sử giúp chúng ta rõ rằng hơn trong việc gửi nhận các bản tin vì hai giao diện này hoạt động có sự độc lập nhất định với nhau.

- Kênh báo hiệu H.225 được thiết lập giữa các Endpoint và Gatekeeper

- Khi nhận được bản tin Setup từ Endpoint O gửi tới, Gatekeeper sẽ gửi bản tin này tới Endpoint T và gửi ngay bản tin Call Proceeding về cho Endpoint O báo rằng cuộc gọi đang trong quá trình thiết lập.

❖ Sau khi nhận được bản tin Connect từ Endpoint T, Endpoint O và Endpoint T sẽ thực hiện báo hiệu trực tiếp với nhau để mở kênh truyền media.



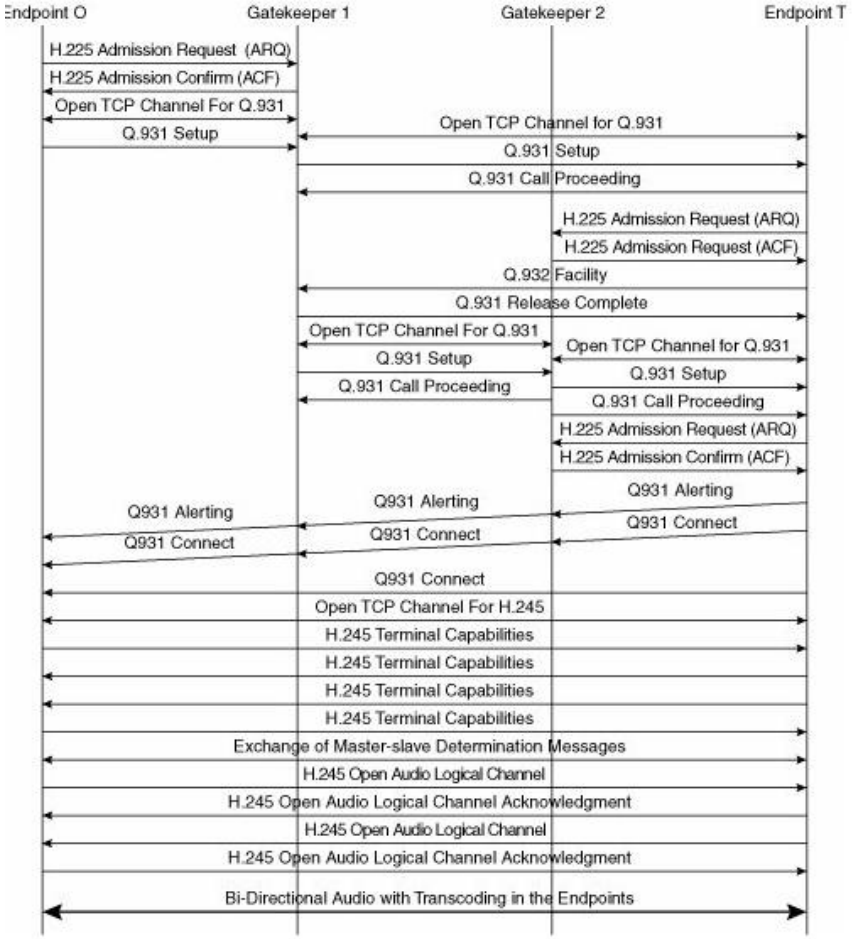
Hình 3.8. Thiết lập báo hiệu H.323 định tuyến qua Gatekeeper

3.1.3.3. Thiết lập cuộc gọi giữa hai thiết bị đầu cuối ở hai vùng dịch vụ

Trong mô hình này là việc thực hiện cuộc gọi giữa hai thiết bị đầu cuối ở hai vùng dịch vụ khác nhau cho nhau. Đây là mô hình báo hiệu dựa trên việc định tuyến của các Gatekeeper.

Sau khi nhận được yêu cầu của Endpoint O muốn thiết lập cuộc gọi với Endpoint T, Gatekeeper 1 gửi tới Endpoint T yêu cầu thiết lập cuộc gọi. Vì Endpoint T nằm trong vùng dịch vụ do Gatekeeper 2 quản lý nên nó phải xin sự cho phép để có thể thực hiện cuộc gọi (giống như các trường hợp trước). Ở trong trường hợp này, Gatekeeper 2 cũng gửi trả lời bản tin ARQ của Endpoint T bằng bản tin ACF cho phép thiết lập cuộc gọi nhưng phải thông

qua nó (không cho thực hiện cuộc gọi trực tiếp tới Endpoint T). Do vậy, Endpoint T gửi bản tin Facility tới Gatekeeper 1 thông báo là cuộc gọi được chấp nhận nhưng phải được định tuyến lại thông qua Gatekeeper 2. Chính vì vậy, kênh báo hiệu H.245 cũ được hủy và thay bằng các kênh báo hiệu biểu diễn như trong hình vẽ.



Hình 3.9. Thiết lập kết nối giữa hai vùng dịch vụ

3.2. GIAO THỨC SIP [1],[4]

SIP (Session Initiation Protocol) là giao thức báo hiệu điều khiển lớp ứng dụng được dùng để thiết lập, duy trì, kết thúc các phiên truyền thông đa phương tiện (multimedia). Các phiên multimedia bao gồm thoại Internet, hội nghị, và các ứng dụng tương tự có liên quan đến các phương tiện truyền đạt (media) như âm thanh, hình ảnh, và dữ liệu. SIP sử dụng các bản tin mời (invite) để thiết lập các phiên và để mang các thông tin mô tả phiên truyền

dẫn. SIP hỗ trợ các phiên đơn quảng bá (unicast) và đa quảng bá (multicast) tương ứng các cuộc gọi điểm tới điểm và cuộc gọi đa điểm. Có thể sử dụng năm chức năng của SIP để thiết lập và kết thúc truyền dẫn là định vị thuê bao, khả năng thuê bao, độ sẵn sàng của thuê bao, thiết lập cuộc gọi và xử lý cuộc gọi. SIP được IETF đưa ra trong RFC 2543. Nó là một giao thức dựa trên ý tưởng và cấu trúc của HTTP (HyperText Transfer Protocol) giao thức trao đổi thông tin của World Wide Web và là một phần trong kiến trúc multimedia của IETF. Các giao thức có liên quan đến SIP bao gồm giao thức đặt trước tài nguyên RSVP (Resource Reservation Protocol), giao thức truyền vận thời gian thực RTP (Realtime Transport Protocol), giao thức cảnh báo phiên SAP (Session Announcement Protocol), giao thức miêu tả phiên SDP (Session Description Protocol). Các chức năng của SIP độc lập, nên chúng không phụ thuộc vào bất kỳ giao thức nào thuộc các giao thức trên.

Mặt khác, SIP có thể hoạt động kết hợp với các giao thức báo hiệu khác như H.323. SIP là một giao thức theo thiết kế mở do đó nó có thể được mở rộng để phát triển thêm các chức năng mới. Sự linh hoạt của các bản tin SIP cũng cho phép đáp ứng các dịch vụ thoại tiên tiến bao gồm cả các dịch vụ di động.

3.2.1.Các thành phần trong mạng SIP

3.2.1.1. Giới thiệu chung về các thành phần trong mạng SIP

- SIP Client: là thiết bị hỗ trợ giao thức SIP như SIP phone, chương trình chat,… Đây chính là giao diện và dịch vụ của mạng SIP cho người dùng.
- SIP Server: là thiết bị trong mạng xử lý các bản tin SIP với các chức năng cụ thể như sau:
    1) Proxy Server: là thực thể trong mạng SIP làm nhiệm vụ chuyển tiếp các SIP request tới thực thể khác trong mạng. Như vậy, chức năng chính của nó trong mạng là định tuyến cho các bản tin đến đích. Proxy server cũng cung cấp các chức năng xác thực trước khi cho khai thác dịch vụ. Một proxy có thể lưu (stateful) hoặc

không lưu trạng thái (stateless) của bản tin trước đó. Thông thường, proxy có lưu trạng thái, chúng duy trì trạng thái trong suốt thời gian thực hiện (khoảng 32 giây).

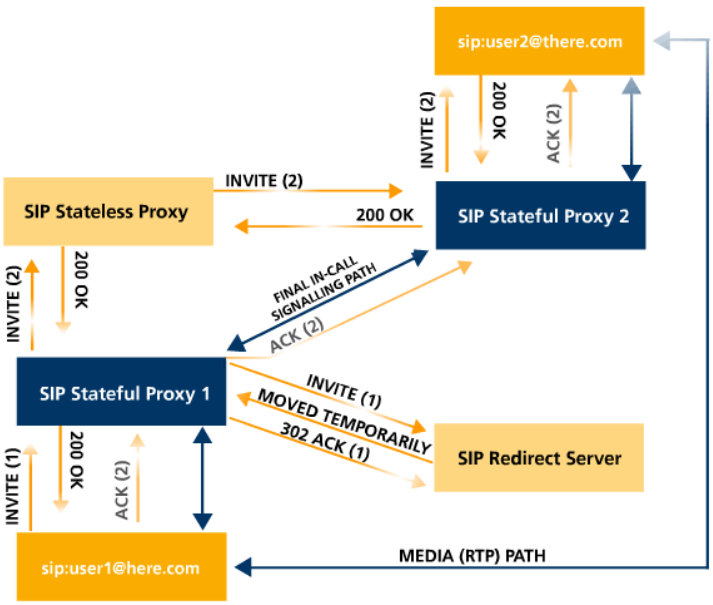
2) Redirect Server: chấp nhận một SIP request và gửi một redirect response trở lại client chứa địa chỉ của server kế tiếp. Redirect server có thể không chấp nhận cuộc gọi, không xử lý các cuộc gọi hay chuyển hướng các SIP request.

3) Registrar server: là server nhận bản tin SIP REGISTER yêu cầu và cập nhật thông tin từ bản tin request vào "location database" nằm trong Location Server.

4) Location Server: lưu thông tin trạng thái hiện tại của người dùng trong mạng SIP.

3.2.1.2. Mối liên hệ giữa các thành phần trong mạng SIP

Trong ví dụ hình 3.10, cho thấy cái nhìn khái quát về chức năng của Proxy Server, Redirect Server, SIP Phone trong mạng. Giả sử thuê bao có tên user1 trong miền dịch vụ here.com muốn thực hiện một cuộc gọi thoại tới thuê bao có thể là user2 (thuộc there.com).



Hình 3.10. Chức năng của Proxy, Redirect Server trong mạng SIP

1. Khi User 1 muốn gọi tới User 2, trước hết nó sẽ gửi bản tin đề nghị INVITE 1 đến Proxy Server 1. Proxy Server 1 chuyển tiếp bản tin tới Redirect Server.
2. Redirect Server này xử lý và trả về mã 3xx thông báo cho Proxy Server tự thực hiện kết nối.
3. Proxy Server 1 gửi bản tin INVITE 2 tới đích trả về bởi Redirect Server (chính là Stateless Proxy Server 1). Vì đây là Stateful Proxy nên thực chất bản tin INVITE được gửi bởi Stateful Proxy là khác so với bản tin nhận được từ User1(ban đầu).
4. Stateless Proxy Server chuyển tiếp bản tin INVITE tới SIP Statefull Proxy 2. Do là Stateless Proxy nên công việc của nó đơn giản là chuyển tiếp bản tin.
5. SIP Statefull Proxy 2 chuyển tiếp bản tin INVITE tới user2.
6. Khi user2 nhấc máy thì nó sẽ gửi bản tin 200 OK theo chiều ngược lại.
7. Sau khi nhận được bản tin 200 OK, user1 sẽ gửi xác nhận ACK tới user2.
8. Luồng RTP trực tiếp giữa hai thuê bao được thiết lập. Và cuộc gọi được thực hiện.

Khi một SIP Phone được kết nối với mạng. Nó liên tục gửi bản tin REGISTER tới Registrar Server để thông báo vị trí hiện tại của nó. Giả sử trong miền dịch vụ có tên chicago.com thì quá trình REGISTER (đăng kí) được tiến hành như sau:

1. Thuê bao có tên Carol gửi bản tin REGISTER tới Registrar Server. Server này tiến hành xác thực. Nếu hợp lệ thì các thông tin đó được lưu trong Location Server.
2. Khi một thuê bao khác (có tên là Bob) gửi bản tin INVITE tới Proxy Server để xin kết nối tới thuê bao Carol. Proxy Server sẽ truy vấn các thông tin về thuê bao bị gọi thông qua Location Server.
3. Proxy Server gửi bản tin INVITE tới thuê bao Carol để thiết lập cuộc gọi.

3.2.2. Bản tin SIP

3.2.2.1. Các loại bản tin SIP

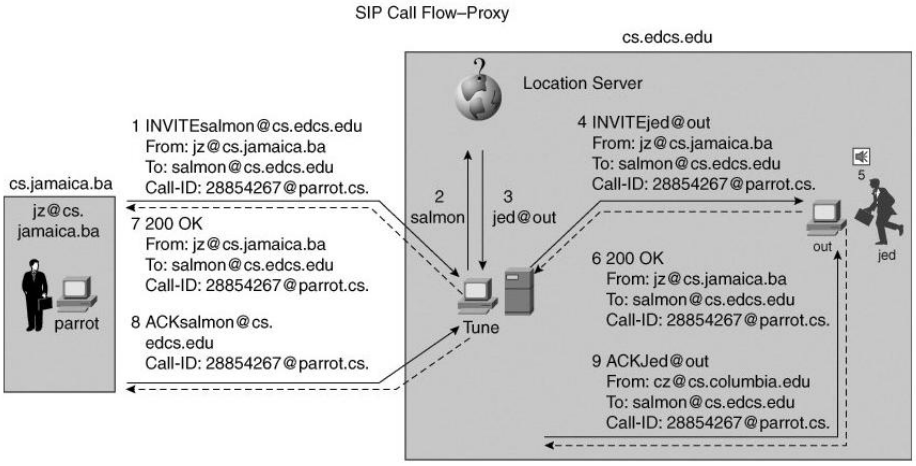
- Bản tin yêu cầu (Request): được gửi từ client tới server. RFC 3261 định nghĩa 6 kiểu bản tin request cho phép UA và proxy có thẻ xác định người dùng, khởi tạo, sửa đổi, hủy một phiên.
  - Bản tin INVITE: yêu cầu thiết lập một phiên hoặc để thay đổi các đặc tính của phiên trước đó.Trong bản tin này có sử dụng SDP để định nghĩa về các thông số media của phiên. Một response thành công có giá trị 200 được trả lại các thông số mà người được gọi chấp nhận trong phiên media.
  - Bản tin ACK xác nhận rằng client đã nhận được response cuối cùng của bản tin INVITE. ACK chỉ được sử dụng kèm với bản tin INVITE. ACK được gửi từ đầu cuối đến đầu cuối cho response 200 OK. ACK cũng có thể chứa phần thân bản tin với mô tả phiên cuối cùng nếu bản tin INVITE không chứa.
  - Bản tin OPTIONS: UA sử dụng request này để truy vấn tới server về khả năng của nó.
  - Bản tin BYE: UA sử dụng bản tin này để yêu cầu hủy một phiên đã được thiết lập trước đó.
  - Bản tin CANCEL: cho phép client và server hủy một request, ví dụ như INVITE. Nó không ảnh hưởng tới request đã hoàn thành trước đó mà server đã gửi response.
  - Bản tin REGISTER: Một client sử sụng REGISTER để yêu cầu đang kí vị trí của nó tới AOR (address of record) của người dùng với SIP server.
- Bản tin đáp ứng (Response): server gửi bản tin SIP đáp ứng (SIP response) tới client để báo về trạng thái của SIP request mà client gửi trước đó. Các SIP response được đánh số từ 100 đến 699, được chia thành các lớp nghĩa khác nhau.

Các lớp Response	Mã trả về	Mô tả
Thông tin	100	Đang thực hiện kết nối
	180	Đang đổ chuông
	181	Cuộc gọi đang được chuyển tiếp
	182	Được đặt vào hàng đợi
	183	Phiên đang được xử lý
Thành công	200	Thành công
Chuyển hướng	300	Nhiều lựa chọn
	301	Chuyển vĩnh viễn
	302	Chuyển tạm thời
	305	Sử dụng proxy
	380	Dịch vụ khác
Lỗi Client	400	Yêu cầu không hợp lệ
	401	Không nhận dạng được
	402	Yêu cầu thành toán
	403	Bị cấm
	404	Không tìm thấy
	405	Phướng thức không được phép
	406	Không chấp nhận
	407	Yêu cầu xác thực Proxy
	408	Request timeout
	410	Đã dời đi
	413	Yêu cầu quá dài
	414	URL được yêu cầu quá lớn
	415	Không hỗ trợ kiểu media
	416	Không hỗ trợ URI
	420	Phần mở rộng lỗi
	421	Yêu cầu phần mở rộng
	423	Khoảng thời gian giữa hai sự kiện quá ngắn

Các lớp Response	Mã trả về	Mô tả
	480	Tạm thời chưa sẵn sàng
	481	Transaction không tồn tại
	482	Phát hiện thấy "loop" (chu trình)
	483	Quá nhiều "hop"
	484	Địa chỉ không đủ
	485	Mật mở không rõ ràng
	486	Đang bận
	487	Yêu cầu bị hủy
	488	Không thể chấp nhận tại đây
	491	Yêu cầu chưa được giải quyết
	493	Không giải mã được
Lỗi Server	500	Lỗi nội tại trong server
	501	Chưa được thực hiện đầu đủ
	502	Gateway lỗi
	503	Dịch vị không tồn tại
	504	Server timeout
	505	Phiên bản SIP không được hỗ trợ
	513	Bản tin quá lớn
Lỗi toàn cục	600	Bận ở khắp mọi nơi
	603	Suy sụp
	604	Không tồn tại
	606	Không thể chấp nhận

3.2.3. Mô tả cuộc gọi SIP

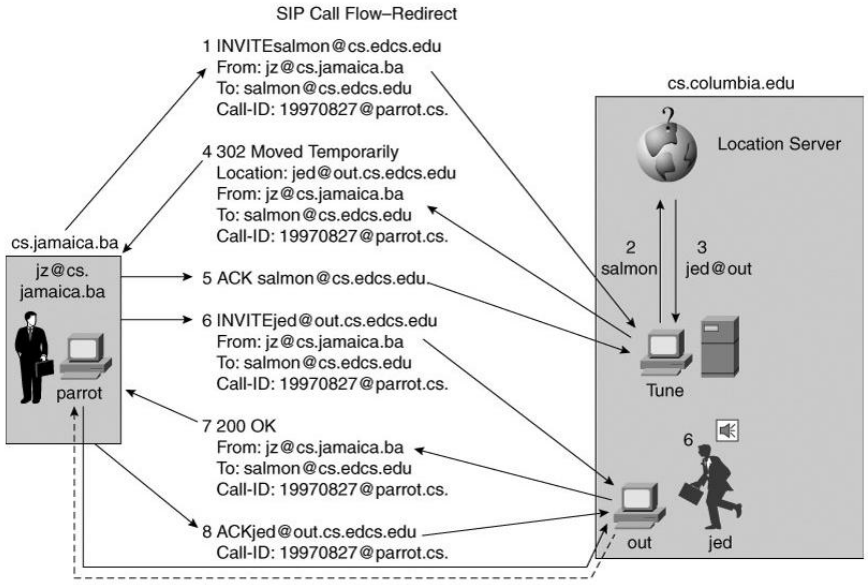
3.2.3.1. Cuộc gọi được định tuyến qua Proxy Server



Hình 3.12. Thiết lập cuộc gọi SIP với Proxy Server

1. Proxy server nhận được bản tin INVITE từ client.
2. Proxy server liên lạc với Location server để xác định địa chỉ của người bị gọi.
3. Location server xác định vị trí của người được gọi và cung cấp địa chỉ server đích.
4. Bản tin INVITE được chuyển tiếp tới địa chỉ mà Location server trả về. Proxy server sẽ thêm tiêu đề Record-Route vào bản tin INVITE để chắc rằng tất cả các bản tin tuần tự sau đó được định tuyến qua proxy. Điều này cần thiết cho quá trình tính cước hoặc các ứng dụng khác cần thiết để kiểm soát các bản tin cho dialog này.
5. Phía được gọi rung chuông. Người được gọi nhấc máy.
6. Phía được gọi gửi bản tin 200 OK thông báo cuộc gọi bắt đầu.
7. Bản tin 200 OK được chuyển tiếp qua proxy server tới phía gọi.
8. Phía gọi trả lời bản tin 200 OK nhận được bằng bản tin ACK tới proxy-server (khi proxy chèn tiêu đề Record-Route vào trong bản tin INVITE) hoặc gửi trực tiếp tới phía người được gọi.
9. Proxy chuyển tiếp ACK tới người được gọi.
10. Cuộc gọi thoại được thiết lập.

3.2.3.2. Báo hiệu trực tiếp giữa các thiết bị đầu cuối



Hình 3.13. Thiết lập cuộc gọi với Redirect Server

1. Redirect server nhận được bản tin INVITE từ phía UA gọi.
2. Redirect server liên lạc với Location server để lấy thông tin địa chỉ của UA được gọi.
3. Location server trả lại địa chỉ của UA được gọi.
4. Redirect server trả địa chỉ trực tiếp về UA gọi với bản tin 3xx với trường Contact đã được cập nhật. Không giống như Proxy server, Redirect server không chuyển tiếp bản tin INVITE.
5. UA gọi gửi bản tin ACK tới Redirect server để xác nhận về bản tin 3xx.
6. UAC gọi gửi trực tiếp bản tin INVITE với trường Contact: là địa chỉ trả về bởi Redirect server tới UA được gọi.
7. UA được gọi rung chuông và người dùng nhấc máy. UA được gọi gửi bản tin 200 OK tới UA gọi.
8. UAC gọi gửi bản tin ACK xác nhận.

3.3. SO SÁNH GIỮA GIAO THỨC H.323 VÀ SIP

Giữa H.323 và SIP có nhiều điểm tương đồng. Cả hai đều cho phép điều khiển, thiết lập và huỷ cuộc gọi. Cả H.323 và SIP đều hỗ trợ tất cả các dịch vụ cần thiết, tuy nhiên có một số điểm khác biệt giữa hai chuẩn này.

- ❖ H.323 hỗ trợ hội nghị đa phương tiện rất phức tạp. Hội nghị H.323 về nguyên tắc có thể cho phép các thành viên sử dụng những dịch vụ như bảng thông báo, trao đổi dữ liệu, hoặc hội nghị video.
- ❖ SIP hỗ trợ SIP-CGI (SIP-Common Gateway Interface) và CPL (Call Processing Language).
- ❖ SIP hỗ trợ điều khiển cuộc gọi từ một đầu cuối thứ 3. Hiện nay H.323 đang được nâng cấp để hỗ trợ chức năng này.

	SIP	**H.323**
Nguồn gốc	IETF	ITU-T
Quan hệ mạng	Ngang cấp	Ngang cấp
Khởi điểm	Kế thừa cấu trúc HTTP.	Kế thừa Q.931, Q.SIG
Đầu cuối	SIP	H.323
Server	• Proxy Server • Redirect Server • Location Server • Registrar Servers.	H.323 Gatekeeper
Khuôn dạng	Text, UTF-8	Nhị phân
Trễ thiết lập cuộc gọi	1.5 RTT	6-7 RTT hoặc hơn
Giám sát trạng thái cuộc gọi	Có 2 lựa chọn: • Trong thời gian thiết lập cuộc gọi • Suốt thời gian cuộc gọi	Phiên bản 1 và 2: máy chủ phải giám sát trong suốt thời gian cuộc gọi và phải giữ trạng thái kết nối TCP. Điều này hạn chế khả năng mở rộng và giảm độ tin cậy

Báo hiệu quảng bá	Có hỗ trợ	Không
Chất lượng dịch vụ	Sử dụng các giao thức khác như RSVP, OPS, OSP để đảm bảo chất lượng dịch vụ	Gatekeeper điều khiển băng thông. H.323 khuyến nghị dùng RSVP để lưu dữ tài nguyên mạng.
Bảo mật	Đăng ký tại Registrar server, có xác nhận đầu cuối và mã hoá	Chỉ đăng ký khi trong mạng có Gatekeeper, xác nhận và mã hóa theo chuẩn H.235.
Định vị đầu cuối và định tuyến cuộc gọi	Dùng SIP URL để đánh địa chỉ. Định tuyến nhờ sử dụng Redirect và Location server	Định vị đầu cuối sử dụng E.164 hoặc tên ảo H.323 và phương pháp ánh xạ địa chỉ nếu trong mạng có Gatekeeper. Chức năng định tuyến do Gatekeeper đảm nhiệm.
Tính năng thoại	Hỗ trợ các tính năng của cuộc gọi cơ bản	Được thiết kế nhằm hỗ trợ rất nhiều tính năng hội nghị, kể cả thoại, hình ảnh và dữ liệu, quản lý tập trung nên có thể gây tắc nghẽn ở Gatekeeper
Tạo tính năng và dịch vụ mới	Dễ dàng, sử dụng SIP-CGI và CPL	H.450.1
Khả năng mở rộng	Dễ dàng	Hạn chế

Chương 4

CÁC PHƯƠNG THỨC TẤN CÔNG VÀ BẢO MẬT TRONG VOIP

Việc thoại và dữ liệu hội tụ trên cùng một dây với bất kỳ giao thức nào được sử dụng là một vấn đề đối với các kỹ sư bảo mật và các nhà quản trị. Hệ quả của vấn đề hội tụ này là các mạng chính có thể bị tấn công, kiến trúc viễn thông thông tin của các tổ chức sẽ có thể gặp phải rủi ro nguy hiểm.

Bảng 4.1. Mô tả các cấp độ mà cấu trúc VoIP có thể bị tấn công:

Điểm yếu	Đặc tả
Cấu trúc IP	Điểm yếu này liên quan đến các hệ thống sử dụng mạng chuyển mạch gói, nó làm ảnh hưởng đến cấu trúc hoạt động VoIP.
Hệ điều hành	Các thiết bị VoIP kế thừa điểm yếu của hệ điều hành và các firmware mà chúng chạy trên đó (windows và linux).
Cấu hình	Cấu hình mặc định của các thiết bị VoIP luôn có những dịch vụ dư thừa. Và các port của các dịch vụ 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.

4.1. CÁC PHƯƠNG THỨC TẤN CÔNG [3]

4.1.1. Tấn công từ chối dịch vụ (DoS) hoặc phá vỡ dịch vụ VoIP

Dịch vụ internet là một chương trình chạy trên một host máy tính chờ đợi một kết nối từ khách hàng. Tấn công DoS (Denial of Service) ngăn chặn

không cho tiếp cận dịch vụ. Đây là loại tấn công trực tiếp và chủ động. Người tấn công không có ý định ăn cắp một cái gì cả. Anh ta chỉ muốn đơn giản là đặt dịch vụ ra khỏi khách hàng. Nhưng không phải lúc nào dịch vụ không được tiếp cận là nguyên nhân của tấn công DoS. Nó có thể là nguyên nhân của cấu hình sai cũng như là nguyên nhân của việc sử dụng sai.

Phụ thuộc vào các tính chất của các hành động trên mang lại mà các dịch vụ này có thể gặp phần nào một số hậu quả khó khăn, ví dụ như một shop trực tuyến.

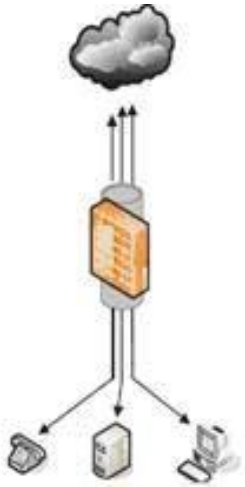
Một tấn công DoS có thể là một trong ba loại sau đây:

+ Đe doạ vật lý hoặc hay thay đổi các thành phần mạng
+ Đe doạ hay thay đổi cấu hình thông tin.
+ Giới hạn hay không thể khôi phục nguồn tài nguyên.

Các sửa đổi một phần kiến trúc phần cứng của hệ thống được xem như là truy cập đến vùng của nó. Một người tấn công chỉ có thể cố gắng phá hủy các phần cứng vật lý thông qua làm đổi hướng phần mềm. Một tấn công DoS trên internet có thể chỉ là loại thứ hai hay thứ ba. Sự thay đổi cấu hình thông tin cần phải truy cập đến host máy tính. Điều này ám chỉ rằng người tấn công được tiếp cận, quản lí hệ thống khi xâm phạm hệ thống. Cách thức tấn công dễ nhất của DoS là giới hạn nguồn tài nguyên, chẳng hạn như băng thông dành cho dịch vụ internet. Biến thể của tấn công DoS được gọi là tấn công từ chối phân bổ của dịch vụ DoS (DDoS).

Tấn công DoS có thể ảnh hưởng đến tất cả các dịch vụ trong mạng IP. Hậu quả của tấn công DoS có thể làm giảm chất lượng dịch vụ hoặc nặng hơn có thể làm mất dịch vụ. Ta có các loại tấn công như sau:

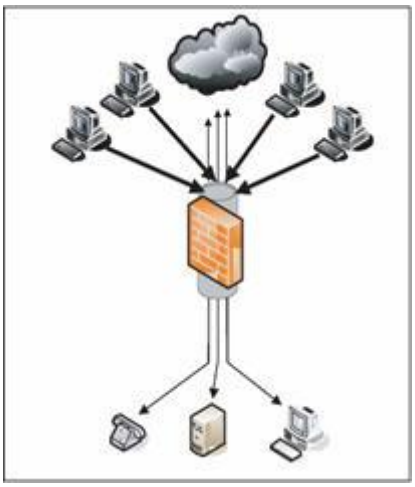
- DDoS (Distributed denial-of-service): đây là kiểu tấn công mà các gói tin làm tràn ngập mạng đích từ nhiều nguồn khác nhau bên ngoài, được mô tả trong hình 4.2 và 4.3.



Hình 4.2. Mô hình truy cập internet tiêu biểu

Các luồng traffic trao đổi bình thường giữa các host và server bên trong và ngoài mạng.

Hình 4.3 cho thấy sự tấn công luồng traffic IP trực tiếp từ interface của firewall.

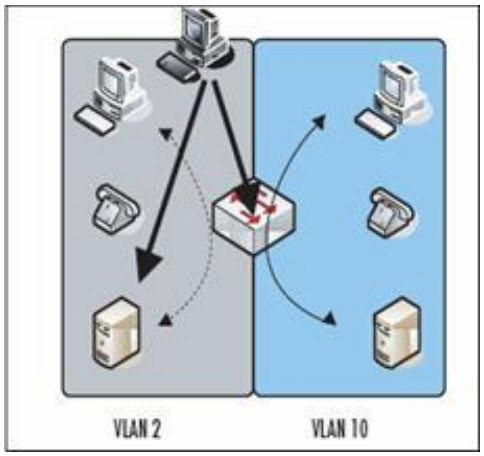


Hình 4.3. Tấn công DoS phân tán.

Ví dụ trong năm 2004, các trang web của Yahoo, Google và Microsoft đã biến mất trên internet trong vài giờ khi các server của họ bị làm tràn với hàng trăm ngàn yêu cầu từ các trang web khác. Điều này làm suy giảm băng thông và các server CPU không thể xử lý nổi.

- DoS (Denial of Service): điều kiện tấn công DoS xảy ra khi thiết bị ở trong mạng nội bộ là cái đích của việc làm tràn ngập các gói, dẫn đến

mất liên lạc giữa các phần trong cấu trúc mạng liên quan đến thiết bị đó. Cũng giống như DDoS ở trên, các dịch vụ cũng bị bẻ gãy và làm giảm băng thông và tài nguyên CPU. Ví dụ: một vài điện thoại IP sẽ ngừng hoạt động nếu chúng nhận các gói tin UDP lớn hơn 65534 bytes ở port 5060.



Hình 4.4. Tấn công DoS trong mạng nội bộ

Việc kiểm tra tính toàn vẹn và kể cả việc mã hóa cũng không thể ngăn chặn những tấn công này. Đặc tính của tấn công DoS và DDoS rất đơn giản bằng cách gửi một lượng lớn các gói tin đến máy nạn nhân. Mặc dù các gói tin này có được đăng ký với server hay không, địa chỉ IP nguồn là thật hay giả, hoặc được mã hóa với một key không có thật đi nữa thì việc tấn công vẫn có thể xảy ra.

Tấn công DoS thật khó để chống lại bởi vì VoIP cũng chỉ là một trong những dịch vụ trên mạng IP, nó cũng dễ bị tấn công như các dịch vụ trên mạng IP khác. Hơn nữa tấn công DoS có ảnh hưởng đặc biệt tới các dịch vụ như VoIP và các dịch vụ thời gian thực khác, bởi vì các dịch vụ này rất "nhạy cảm" với trạng thái mạng. Virus và worm nằm trong danh sách gây nên tấn công DoS hay DDoS dựa trên việc tăng lưu lượng mạng mà chúng tạo ra bằng cách tái tạo và nhân bản.

4.1.2. Một số cách tấn công chặn và cướp cuộc gọi

4.1.2.1. 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 gửi 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 gửi từ một user có quyền để thiết lập cuộc gọi và gửi lại chúng sau khi đã sửa đổi địa chỉ IP nguồn. Nó có thể bị ngăn chặn bằng cách thực thi hai dịch vụ bảo mật nhận thực thể ngang hàng (peer entity authencation) và tính toàn vẹn dữ liệu (data intergrity).

4.1.2.2. Tấn công tràn bộ đệm

Đây là phương thức tấn công phổ biến, 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 xâm 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 con.

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 hỗng nhận thức được chứa trong các hệ thống hoạt động và các chương trình ngôn ngữ.

4.1.2.3. 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 đã được định tuyến qua người tấn công. Người tấn công đã hoàn thành việc truy cập để thay thế các dữ liệu bên trong. Người tấn công có thể đọc chúng, thay đổi chúng hoặc và gửi chúng như là dữ liệu của anh ta. 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. 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.

4.1.2.4. Chặn và đánh cắp cuộc gọi

Nghe trộm và 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 phục vụ cho mục đích khác của anh ta.

4.1.2.5. 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, và để bổ nhiệm một vài host như là các server chính cho các dịch vụ.

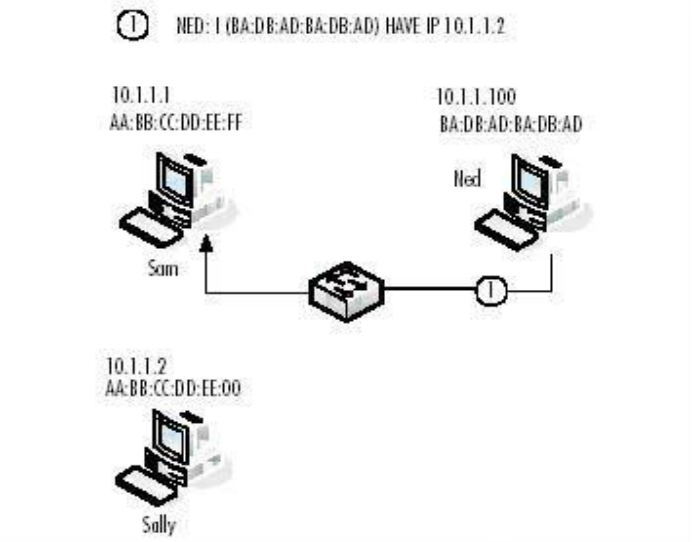
Một người có mục đích tấn công, sẽ cố gắng đầu độc DNS hay tấn công giả mạo, sẽ thay thế giá trị lưu trữ hồ sơ DNS A, SRV với các bản tin mà trỏ đến các server của người tấn công. Điều này có thể được hoàn thành bằng cách bắt đầu dời vùng từ DNS server của người tấn công đến DNS server nạn nhân, bằng 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.

Ví dụ như 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 hướng đến yourbank.com sẽ bị chuyển hướng lại đến attacker.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 biết 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.

4.1.2.6. Đánh lừa ARP (ARP Spoofing):

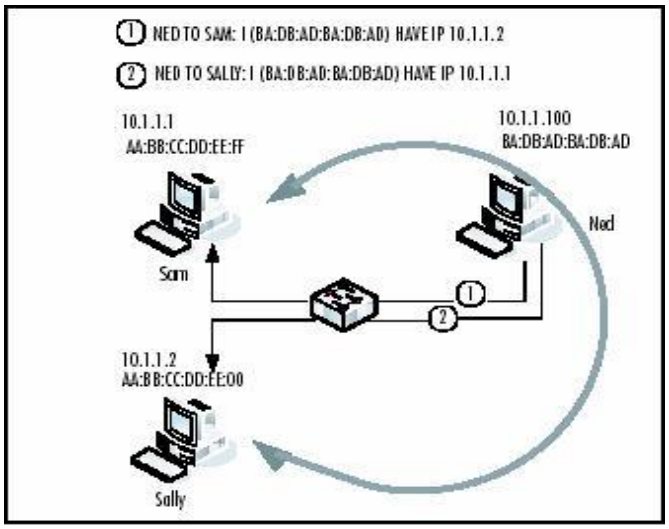
ARP (Address Resolution Protocol) là giao thức cơ sở Ethernet. Có lẽ do nguyên nhân này, thao tác vào các gói ARP là kỹ thuật tấn công thường thấy trong mạng VoIP. Một vài kỹ thuật hay công cụ hiện tại cho phép bất kỳ user nào có thể tìm ra lưu lượng mạng trên mạng bởi vì ARP không có điều khoản cho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



Hình 4.5. Đánh lừa ARP (đầu độc cache)

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 gửi 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. Trong hình 4.5, 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:DB:AD:BA:DB: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.



Hình 4.6. Tấn công chuyển hướng ARP

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 (xem hình 4.6).

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 bằng 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.

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.

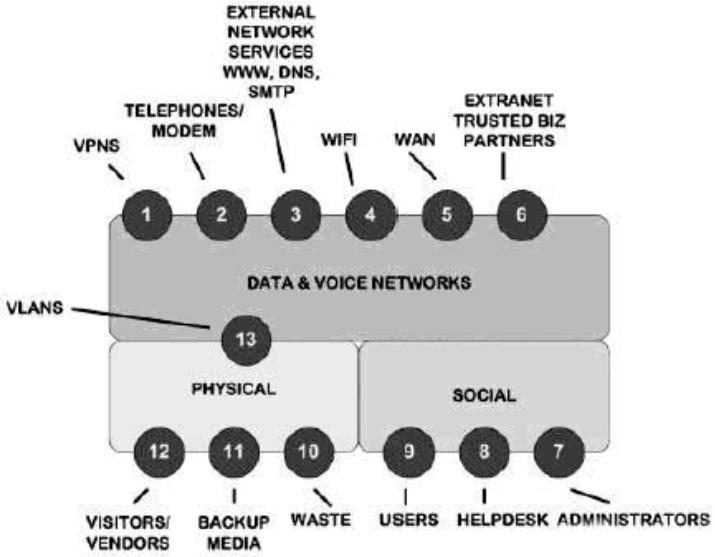
Các rủi ro của việc mã hoá lưu lượng VoIP có thể được giới hạn bởi thực thi mật mã. Sử dụng việc mật mã hoá media, các cuộc đàm thoại giữa hai đầu cuối IP phải được sử dụng cùng một dạng mật mã hoá. Trong môi trường bảo mật cao thì các tổ chức cần phải đảm bảo cùng một phương thức mật mã trong bộ codec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

4.2. CÁC PHƯƠNG THỨC BẢO MẬT [3]

4.2.1. Cơ sở của cấu trúc bảo mật hiện hành

Nghiên cứu quá trình bảo mật cấu trúc VoIP bắt đầu bằng cách xem lại các cấu trúc bảo mật hiện hành. Việc các thành phần VoIP hoạt động với dữ liệu mạng là một cơ hội tốt để xem lại và bổ sung các chính sách bảo mật hiện có, cũng như cấu trúc và quá trình xử lý của chúng.

Hình bên dưới mô tả các thành phần cấu trúc bảo mật



Hình 4.7. Các thành phần cấu trúc bảo mật

Interface giữa dữ liệu và thoại với mạng bên ngoài được mô tả bằng những vòng tròn từ 1 đến 6. Thêm vào đó, dữ liệu và thoại chia sẻ interface với giao diện vật lý và Social. Interface từ data mạng bao gồm VPN (Virtual Private Network), điện thoại và modem, các loại web và dịch vụ mail điện tử, các kết nối từ các công ty con bên ngoài thông qua đường WAN. Các kỹ thuật bảo mật như là Firewall, IDS và ACLs hữu dụng cho những Interface này. Interface từ 7 đến 9 mô tả ứng với admin, user và các tổ chức kết nối mạng Interface 10 đến 12 là những interface giữa phần vật lý với dữ liệu và thoại. Gần đây, một số vấn đề xảy ra trong khu vực này, kết quả là làm mất dữ liệu quan trọng. Cuối cùng interface 13 miêu tả VLAN (Virtual LAN) interface.

Việc liệt kê các danh sách này thực ra cũng không cần thiết, nhưng nó cũng cho biết nơi mà việc thực hiện bảo mật đạt hiệu quả nhất. Mục đích của phần này là giúp chúng ta củng cố lại các khái niệm với nhiều thành phần mà bạn được yêu cầu đảm bảo trên mạng VoIP/data.

4.2.1.1. Phương pháp và chính sách bảo mật

Từ lợi ích của thông tin liên lạc, yêu cầu đảm bảo hệ thống mạng và bao gồm cả cơ sở kiến trúc thông tin liên lạc.

Quá trình bảo mật hội tụ mạng VoIP/Data bắt đầu bằng sự đưa ra, sự bổ sung, sự liên lạc hiệu quả của các chính sách bảo mật. Một chính sách khi được viết ra, thì cũng cần thêm một khoảng thời gian để đưa ra thảo luận. Một

chính sách có những ưu điểm thuận lợi được xây dựng dựa trên hệ thống báo cáo của một tổ chức nào đó cần phải đảm bảo các tiêu chuẩn về chất lượng, tính tin cậy, tính toàn diện. Khi đạt được điều này, việc bảo mật thông tin trở nên dễ dàng đối với người quản trị cũng như gánh nặng về kỹ thuật, và thêm nhiều thuận lợi khác nữa.

Việc đề ra chính sách là một bước quan trọng tiến đến việc chuẩn hóa các hoạt động tổ chức kinh doanh. Chính sách của tổ chức là phương tiện truyền tải quản lý đảm bảo các vấn đề bảo mật IT, đồng thời cũng làm sáng rõ đối với các bên cộng tác, liên quan hoặc những người có trách nhiệm. Những chính sách đề ra phải thiết lập các chuẩn cho việc bảo vệ tài nguyên thông tin bằng cách đưa ra các chương trình quản lý, những nguyên tắc cơ bản, những định nghĩa, những hướng dẫn cho mọi người bên trong tổ chức. Mục tiêu chính của chính sách bảo mật là ngăn chặn những hành vi có thể dẫn tới nguy hiểm.

Bảo mật trong môi trường điện thoại IP bao gồm tất cả các đặc tính an toàn truyền thống cộng thêm các đặc tính an toàn dữ liệu mạng. Thoại IP biến đổi thoại thành dữ liệu, và đặt các gói dữ liệu này vào trong các gói IP. Hoạt động của các hệ thống bên dưới như là IP-PBXs, gateway dễ bị ảnh hưởng bởi những tấn công mà điều đó sẽ làm ảnh hưởng đến những server khác.

- **Sự an toàn về mặt vật lý:** Thiết bị IP-PBX phải được khóa trong phòng kín và hạn chế sự truy cập. Loại truy cập này được xác nhận bởi hệ thống xác thực user với một khóa card. Việc truy cập bằng bàn phím là không được phép. Tất cả các phương pháp vào phòng phải cung cấp danh sách user truy nhập vào phòng cùng với tem ngày tháng/thời gian.
- **VLANs:** Việc tách thoại và luồng dữ liệu qua VLAN được yêu cầu để ngăn chặn đụng độ broadcast trong VoIP, và bảo vệ dữ liệu mạng khỏi các luồng thoại.
- **Softphones:** Softphone trong một môi trường an toàn chứa đựng bất kỳ phần mềm quảng cáo nào đều phải bị cấm. Việc cài đặt softphone cần được kiểm tra trước khi thực thi. Và những phần mềm mà không mã hóa thư người gửi thì không nên sử dụng. Bởi vì softphone là một ứng dụng

chạy trên một hệ điều hành, việc bảo mật phụ thuộc nhiều vào tình trạng của hệ điều hành đó, cũng như phụ thuộc vào các chương trình truyền thông khác như email, duyệt web, IM.

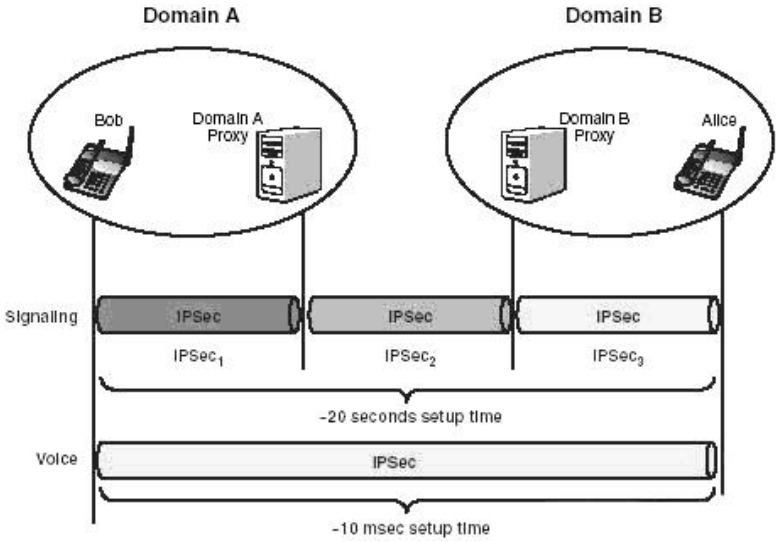
- **Mã hóa (Encryption):** Tất cả các hệ thống VoIP nên sử dụng một hình thức mã hóa Media Encryption (RTP channel). Các thông tin giữa các thành phần mạng cần phải được mã hóa. Khuyến cáo nên hoàn thành việc mã hóa thoại IP từ đầu cuối đến đầu cuối (end-to-end) để hạn chế mối đe dọa nghe trộm thoại. Đồng thời, tất cả các truy cập đến server cũng như các thành phần mạng phải được mã hóa bằng các giao thức như SSL, SSH.
- **Điều khiển truy cập lớp 2 (layer 2 access control):** Giải pháp toàn diện nhất yêu cầu tất cả thiết bị xác thực trên lớp 2 dùng 802.1X trước khi thiết lập cấu hình tại lớp 3 IP. Thêm vào đó, nên xem xét việc cho phép các port an toàn cũng như việc lọc địa chỉ MAC trên switch. Các đặc tính port security trên các thiết bị cung cấp khả năng hạn chế sử dụng port đến một địa chỉ MAC đặc biệt hoặc thiết lập một địa chỉ MAC. Nhìn chung nó khó có thể thực hiện, nhưng với kế hoạch đúng đắn, port security không phải là không làm được.

4.2.2. Các công nghệ bảo mật hiện hành

Có rất nhiều phương pháp bảo mật đang được sử dụng, trong phần này của đồ án chỉ tìm hiểu một số phương pháp tiêu biểu nhất.

4.2.2.1. IP Sec

IP sec là một giao thức bảo mật đã được chứng tỏ và triển khai rộng rãi, và cung cấp bảo vệ các ứng dụng mà sử dụng UDP hay TCP như là một giao thức vận chuyển, IP sec có thể được sử dụng trong chế độ vận chuyển hay đường hầm để bảo vệ các payload (hàng vận chuyển). IP sec có thể cung cấp sự bí mật, tính toàn vẹn và chứng thực cho các thông điệp báo hiệu và media bằng cách tạo các đường hầm đảm bảo giữa các đầu cuối. Hình 4.8 chỉ cách sử dụng của IP sec trong môi trường SIP.



Hình 4.8. SIP với IPsec

Trong ví dụ này, Bob cố gắng thiết lập cuộc gọi đến Alice. Để bảo vệ báo hiệu SIP sử dụng IPsec, điện thoại của Bob thiết lập một đường hầm IPsec với proxy tương ứng của nó (domain A). Khi mà đường hầm được thiết lập, các proxy SIP phân tích các thông điệp và chuyển tiếp chúng đến đích thích hợp. Trước khi nó gửi các thông điệp, nó phải thiết lập đường hầm IPsec khác với proxy SIP tương ứng (miền B). Khi đường hầm này được thiết lập, proxy SIP của Alice kiểm tra các thông điệp và chuyển tiếp nó đến điện thoại của Alice. Việc tạo ba đường hầm riêng biệt này có thể mất trung bình khoảng 2.7 giây cho mỗi IP sec liên kết được thiết lập (xấp xỉ 5-6 giây cho toàn bộ đường hầm IPsec. Có thể phải mất 20 giây cho việc thiết lập cuộc gọi (từ Bob đến Alice và ngược lại) khi IP sec end to end được sử dụng. Điều này là khó chấp nhận bởi vì các tổ chức kinh doanh chỉ cho phép thời gian thiết lập cuộc gọi không nên quá 25 ms.

Trên một khía cạnh khác, đường dẫn media (RTP) được thiết lập trực tiếp giữa hai đầu cuối, và mất trung bình khoảng 10ms là không đáng kể. Điều này chỉ ra rằng không cần thiết sử dụng IP sec cho các phiên được cấp động, bởi vì thời gian phải mất cho các thông điệp báo hiệu là để đi qua các bước nhảy ở xa là lớn hơn thời gian người dùng có thể chờ cho việc thiết lập cuộc gọi. Nếu các liên kết IPsec đã sẵn sàng được thiết lập, thì hầu như sẽ

không có trễ liên kết với các định tuyến thông điệp báo hiệu, ví dụ như VoIP qua các mạng VPN là khả thi.

Trong một vài trường hợp các đường hầm IPsec cần được thiết lập lại bởi vì lỗi mạng, phần mềm hay phần cứng hỏng, hoạt động kém,…

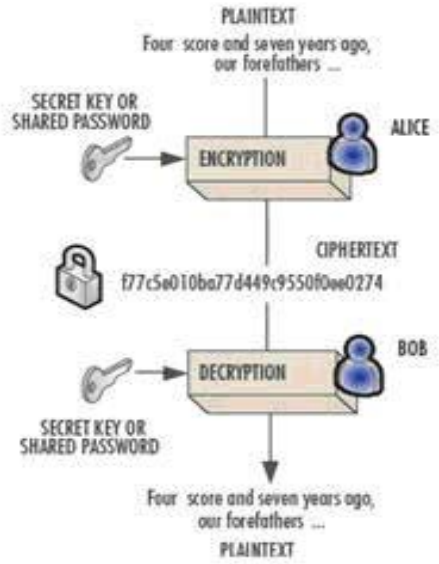
Tổng quát, IPsec có thể thích hợp bảo vệ lưu lượng VoIP giữa các mạng nếu khi mà các đường hầm VoIP được thiết lập trước. Đặc biệt IP sec giữa các site cách biệt vẫn ổn định bởi vì luôn có lưu lượng đi qua và các đường hầm không mất hiệu lực bởi khả năng hoạt động kém. Điều này là không đúng cho điện thoại VoIP mà có thể sử dụng IP sec để bảo vệ các thông điệp báo hiệu và media. Để giải quyết vấn đề này, các thực thi gửi các thông điệp đăng nhập thường xuyên đến các registrar local (đăng ký cục bộ) để duy trì đường hầm IP sec.

Có 3 phương pháp dùng trong IPsec, nhưng phương pháp được ứng dụng nhất là PKI.

- Cấu trúc khóa dùng chung PKI (Public Key Infrastructure)

PKI là bộ khung của các chính sách, dịch vụ và phần mềm mã hóa, đáp ứng nhu cầu bảo mật của người sử dụng khi gửi những thông tin quan trọng qua Internet hay các mạng khác.

Ở hình dưới, khái niệm khóa bí mật được trình bày, Alice và Bob là 2 bên của phiên truyền thông. Trong trường hợp này cả hai đều có cùng một khóa bí mật. Alice mã hóa văn bản muốn gửi đến Bod bằng khóa bí mật của mình. Khi Bod nhận được văn bản đã mã hóa và giải mã nó với cùng một khóa tương tự. Phương pháp này còn được gọi là Pre-shared key hoặc phương pháp mã hóa đối xứng.

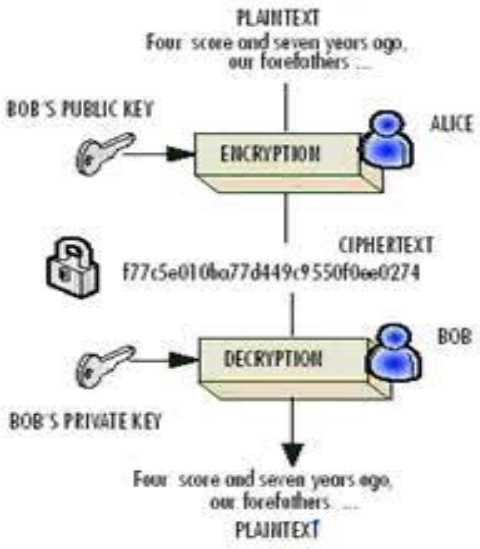


Hình 4.9. Phương pháp mã hóa khóa đối xứng

Ở phương pháp này tính bảo mật chưa cao do hai người cùng sử dụng một key.

- Chìa khóa mật mã dùng chung (Public Key Criptography): đảm bảo độ tin cậy đối với các thông tin hoặc các thông điệp bằng cách sử dụng những thuật toán. Hay nói rõ hơn là nó sẽ dùng một chìa khóa để mã hóa dữ liệu và một chìa khóa để giải mã chúng. Trong dịch vụ khóa dùng chung, người sử dụng nhận được phần mềm mã hóa đặc biệt và một cặp chìa khóa, trong đó một khóa là khóa dùng chung (Public key), và một khóa dành riêng (Private key) người sử dụng phải giữ bí mật.

Hai chìa khóa có liên hệ mật thiết với nhau sao cho khi khi mã hóa dữ liệu với khóa dùng chung thì ta có thể giải mã lại được bằng khóa dành riêng. Một người sử dụng, ví dụ Alice mã hóa một thông điệp gửi đi bằng chìa khóa công cộng của người nhận là Bob. Khi nhận được thông điệp này Bob sẽ giải mã nó bằng chìa khóa dành riêng cho mình. Với cách đó, vấn đề bảo mật sẽ được nâng cao do mỗi người tự quản lý khóa dành riêng cho mình.



Hình 4.10. Phương pháp khóa bất đối xứng

4.2.2.2. Chữ ký số

Chữ ký số phục vụ mục đích tương tự như một chữ ký trong thế giới thực để xác nhận một thông điệp hay một mẫu dữ liệu nào đó.

Việc sử dụng chữ ký số mang lại một số lợi điểm sau:

Khả năng nhận thực:

Các hệ thống mật mã hóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có người chủ của khóa biết. Để sử dụng chữ ký số thì văn bản không cần phải được mã hóa mà chỉ cần mã hóa hàm băm nhỏ của văn bản đó (thường có độ dài cố định và ngắn hơn văn bản). Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận được. Nếu 2 giá trị này khớp nhau thì bên nhận có thể tin tưởng rằng văn bản xuất phát từ người sở hữu khóa bí mật.

- *Tính toàn vẹn*

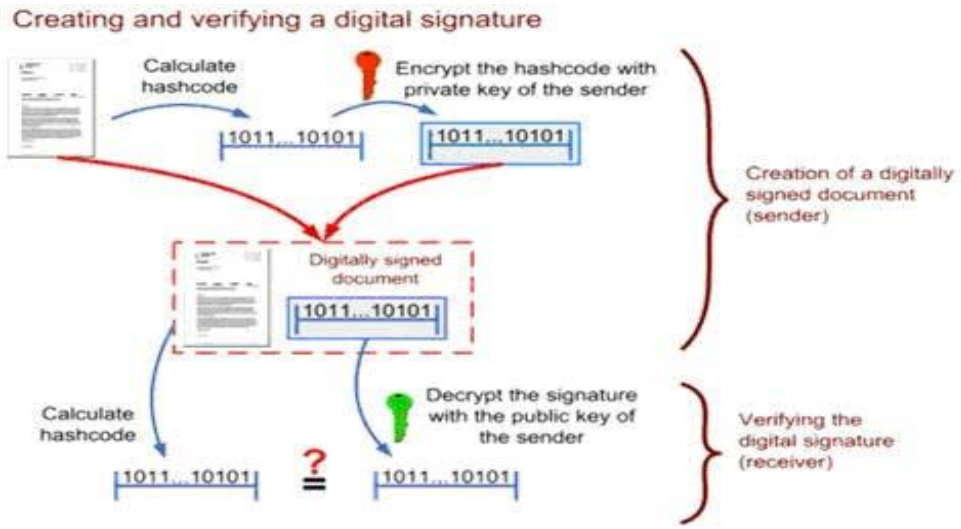
Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhưng không ngăn cản được việc thay đổi nội dung của nó.

- *Tính không thể phủ nhận*

Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này như một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt được hoàn toàn.

- *Thực hiện chữ ký số khóa công khai*

Chữ ký số khóa công khai dựa trên nền tảng mật mã khóa công khai. Để có thể trao đổi thông tin trong môi trường này, mỗi người sử dụng có một cặp khóa: một công khai và một bí mật. Khóa công khai được công bố rộng rãi còn khóa bí mật phải được giữ kín và không thể tìm được khóa bí mật nếu chỉ biết khóa công khai.



Sơ đồ tạo và kiểm tra chữ ký số

Toàn bộ quá trình gồm 3 thuật toán:

- ✧ Thuật toán tạo khóa.
- ✧ Thuật toán tạo chữ ký số.
- ✧ Thuật toán kiểm tra chữ ký số.

Xét ví dụ sau: Bob muốn gửi thông tin cho Alice và muốn Alice biết thông tin đó thực sự do chính Bob gửi. Bob gửi cho Alice bản tin kèm với chữ ký số. Chữ ký này được tạo ra với khóa bí mật của Bob. Khi nhận được bản tin, Alice kiểm tra sự thống nhất giữa bản tin và chữ ký bằng thuật toán kiểm tra sử dụng khóa công cộng của Bob. Bản chất của thuật toán tạo chữ ký đảm bảo nếu chỉ cho trước bản tin, rất khó (gần như không thể) tạo ra được chữ ký của Bob nếu không biết khóa bí mật của Bob. Nếu phép thử cho kết quả đúng thì Alice có thể tin tưởng rằng bản tin thực sự do Bob gửi. Thông thường, Bob không mật mã hóa toàn bộ bản tin với khóa bí mật mà chỉ thực hiện với giá trị băm của bản tin đó. Điều này khiến việc ký trở nên đơn giản hơn và chữ ký ngắn hơn. Tuy nhiên nó cũng làm nảy sinh vấn đề khi 2 bản tin khác nhau lại cho ra cùng một giá trị băm. Đây là điều có thể xảy ra mặc dù xác suất rất thấp.

4.2.2.3. Hệ thống phát hiện xâm nhập mạng (Network Intrusion Detection System)

Sử sụng hệ thống phát hiện xâm nhập mạng (NIDS) được thiết kế để cảnh báo cho nhà quản trị khi có những luồng traffic độc hại hay không hợp pháp được phát hiện. Luồng độc hai có thể là virus worm hay các đoạn mã xấu, còn những luồng traffic không hợp pháp khi nó sai lệch với chính sách bảo mật đã đặt ra. NIDS có thể dò tìm trong mạng rộng lớn chỉ với vài nút hoặc vài thiết bị và áp đặt lên trên mạng đó. NIDS được tìm thấy trong hầu hết các thiết bị môi trường mạng hiện nay. Trong môi trường VoIP, NIDS cung cấp thêm một lớp phòng thủ.

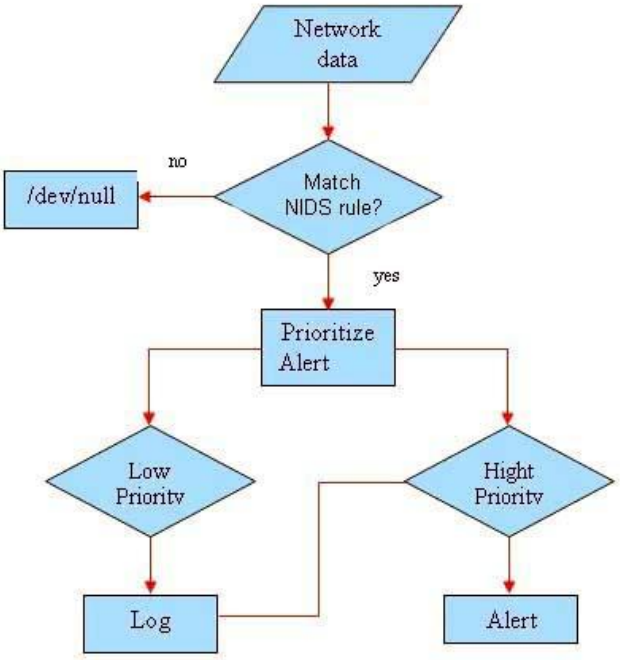
NIDS phát hiện các hành động đáng ngờ bằng ba cách.

- Thứ nhất, cộng đồng bảo mật chứa một cơ sở dữ liệu vô cùng lớn về cách tấn công chữ ký riêng biệt. Những chữ ký này được lập trình trên bộ cảm biến NIDS, mà được cập nhật một cách thường xuyên căn bản.
- Thứ hai, bộ cảm biến NIDS chứa đựng một bộ tiền xử lý mà có thể theo dõi các hành vi bất thường trên mạng. Mặc dù nó không như kiểu tấn công chữ ký, những bất thường này cũng ảnh hưởng

lớn đến sự phát hiện của port scan, sự thăm dò phân phối mạng, hình thức tràn bộ đệm mới, tấn công DoS.

- Thứ ba, tất cả các trang thiết bị NIDS có thể ứng dụng và phát hiện sự sai lệch với các chính sách bảo mật. Sự sai lệch chính sách này bao gồm sự dò tìm dịch vụ mạng không hợp pháp, những ứng dụng chạy trên những port khác thường, như hoạt động của virus Trojan.

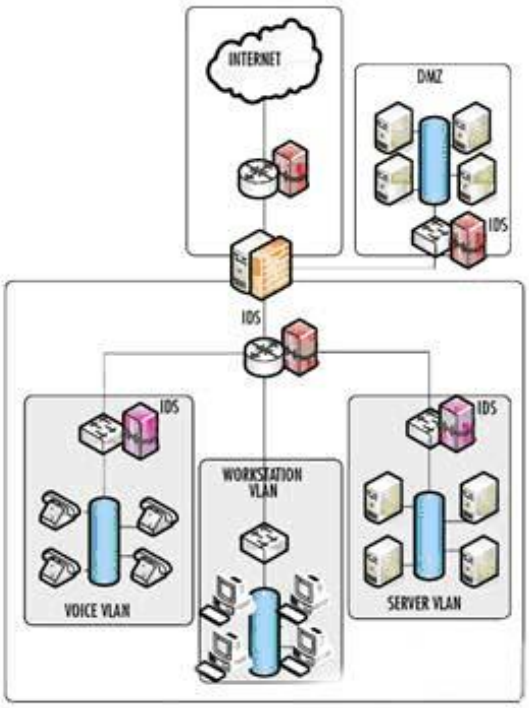
Đa số các NIDS cấu hình client-to-server. Nhiều thiết bị cảm biến thông thường sẽ báo cáo đến một hay vài bộ điều khiển quản lý. Bộ cảm biến có thể chỉ định các thiết bị, có thể chạy ứng dụng trên host đang chạy ứng dụng khác, hoặc có thể chạy độc lập trong hệ thống riêng ảo.



Hình 4.11. Minh họa nguyên lý cơ bản được dùng trong trạm quản lý NIDS

Yêu cầu phần cứng của bộ điều khiển quản lý phải chính xác hơn các bộ cảm biến, bởi vì bộ điều khiển quản lý (Manage Control) chịu trách nhiệm về tương quan dữ liệu từ nhiều cảm biến như là lưu trữ, báo động và trực quan hóa. Thường Manage Control bao gồm một bộ cảm biến tổng hợp.

NIDS được đặt ở những nơi có thể theo dõi hiệu quả nhất lưu lượng mạng. Điều này không có nghĩa là phải đặt NIDS tại nơi có thể theo dõi hết tất cả các lưu lượng mạng. Bên dưới là ví dụ về mô hình mạng. Mạng này gồm một kết nối Internet, một DMZ (Delimitarized zone- vùng ranh giới) và 3 VLAN nội bộ, cấu hình cho thoại user, workstation,và server.



Hình 4.12. Định vị NIDS

Trong hình trên, một NIDS được đặt bên ngoài bên cạnh firewall để theo dõi các lưu lượng Internet vào ra. NIDS còn được chỉ định đặt tại switch vùng Voice VLAN và Server VLAN. Ngoài ra còn có một NIDS bổ sung đặt tại vùng DMZ.

4.2.2.4. Hệ thống phát hiện xâm nhập Host (Host-based Intrusion Detection System)

Hệ thống phát hiện xâm nhập Host (HIDS) là một ứng dụng hoạt động dựa trên thông tin được tập hợp từ những máy tính riêng lẻ. Điểm lợi thế này cho phép HIDS phân tích các hoạt động trên các host để theo dõi với mức độ chi tiết cao hơn. Nó có thể xác định quá trình hoặc user nào liên quan đến các hoạt động phá hoại. Hơn nữa, không giống như NIDS, HIDS có thể phát hiện

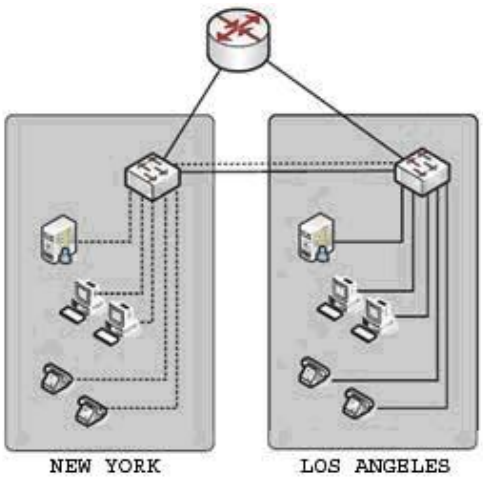
ra tấn công trên một máy bởi vì chúng có thể truy cập trực tiếp hoặc theo dõi các file dữ liệu và quá trình hệ thống. Cách khác, HIDS có thể dùng những nguồn thông tin theo hai kiểu, kiểm soát vận hành hệ thống và nhật ký hệ thống. Việc kiểm soát hệ điều hành hình thành ở mức trong cùng của hệ điều hành (nhân), bởi vậy nhật ký hệ thống bảo vệ tốt hơn và chi tiết hơn.

Hầu hết các phần mềm HIDS, thiết lập một file "kiểm kê số" và những thuộc tính của chúng. Và việc sử dụng những kiểm kê này như một đường mốc cho việc theo dõi sự thay đổi của hệ thống. "Kiểm kê" thông thường là một file chứa đựng các file kiểm tra cá nhân và các thư mục riêng được mã hóa bằng thuật toán MD5.

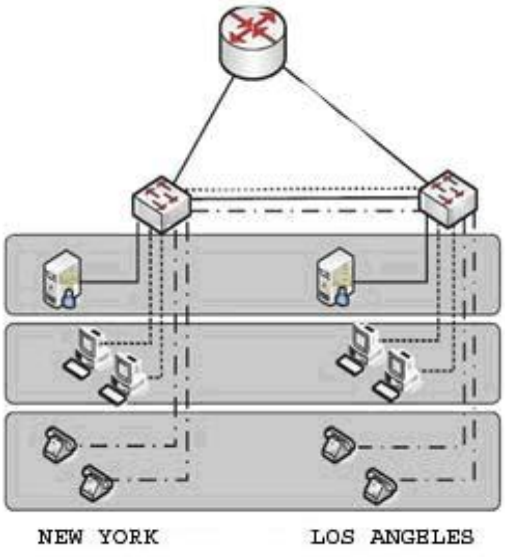
Sự giám sát HIDS đặc biệt quan trọng đối với phương tiện truyền thông VoIP, proxy, registration server và nên xem xét các phần khởi đầu của việc thiết lập gói. Thật vậy, những nhà cung cấp như Cisco thậm chí đang làm cài đặt mặc định cho phần này vào các thiết bị của họ. Tuy nhiên HIDS không thể ngăn chặn tấn công DoS cũng như không thể phát hiện các cuộc dò quét mạng và HIDS cần tài nguyên trên host để hoạt động.

4.2.2.5. VLAN

Việc tách thoại và các luồng dữ liệu đi qua VLAN được khuyến cáo để ngăn chặn dữ liệu mạng ảnh hưởng đến các luồng thoại và ngược lại Ở hình bên dưới, những đường chấm chấm đại diện cho VLAN 2, những đường nét đậm đại diện cho VLAN 1. Server và các trạm làm việc được cô lập dựa trên sự định vị vật lý của họ.



Tuy nhiên ta có thể chia VLAN theo cách sau:



Hình trên, đường dấu chấm thể hiện cho VLAN 2, đường nét đậm thể hiện cho VLAN 1, đường nét chấm gạch thể hiện cho VLAN 3.

VLAN cung cấp một sự an toàn nào đó và nó tạo ra các miền broadcast nhỏ bởi việc phân chia các mạng con. Hậu quả của tấn công DoS có thể được giảm nhẹ bởi việc phân chia hợp lý thoại và dữ liệu chia cắt trong những VLAN riêng biệt. Sự tách riêng lưu lượng mạng yêu cầu các luồng IP phải chuyển qua thiết bị lớp 3, do đó sẽ được kiểm tra tại các mức ACL (Access List).

Việc bảo mật softphone trong môi trường VoIP là một thách thức lớn, đặc biệt nếu VLAN được sử dụng như một điều khiển an toàn chính. Nhiều softphone chứa đựng phần mềm quảng cáo làm ảnh hưởng đến thông tin cá nhân người sử dụng. HIDS hay Firewall được sử dụng để hạn chế trong tình huống này bởi vì softphone yêu cầu Firewall mở một số port UDP. Nguyên lý quan trọng nhất trong việc đảm bảo các softphone là nâng cấp hệ điều hành.

4.2.2.6. Firewall

Firewall (tường lửa) là một bộ phận không thể thiếu trong bất kỳ cấu trúc bảo mật mạng nào. Firewall phân ranh giới bên trong và bên ngoài, từ mạng tin cậy đến không tin cậy. Và chúng dùng để chia dữ liệu VoIP trong

mạng nội bộ. Hai vấn đề quan trọng ảnh hưởng đến thực hiện tường lửa liên quan đến VoIP.

- Thứ nhất, ranh giới giữa bên trong và bên ngoài, hoặc những mạng tin cậy và những mạng không tin cậy dần dần trở nên khó phân biệt hơn.
- Thứ hai là đa số tường lửa không đáp ứng đầy đủ những gói và những phiên VoIP, đặc biệt nếu phiên hoặc gói đó được mã hóa.

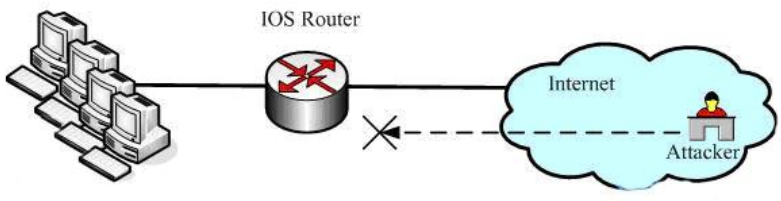
Một tường lửa thực thi kiểm tra các tiêu chuẩn được cấu hình và chỉ cho phép lưu lượng được thừa nhận đi qua. Ví dụ nó có thể kiểm tra tính hợp lệ của địa chỉ IP, header (lớp đầu) của các gói cũng như định dạng của các giao thức. Một vài dịch vụ được thừa nhận đến các well-known port (cổng cho ứng dụng) và sử dụng chúng, được biết như là các giao thức. Một ví dụ là giao thức HTTP, các loại server HTTP điển hình sử dụng port 80 cho hoạt động của chúng. Một khách hàng yêu cầu kết nối đến dịch vụ này phải có những nghi thức đi theo để việc kết nối được chấp nhận.

Với tầm quan trọng của tường lửa có thể xác định rõ một mức độ nào đó về những gì thông tin yêu cầu kết nối phải chứa. Những điều kiện này nhằm đảm bảo tính chính xác của nghi thức. Tuy nhiên nó rất tốn thời gian và giảm tốc độ kết nối. Lưu lượng được định tuyến qua tường lửa có thể được ghi vào để phân tích và kiểm tra các khả năng bị xâm phạm hay bị tấn công. Chỉ có các gói dữ liệu khi đi qua tường lửa thì mới bị kiểm tra.

❖ **Network Firewall:**

Network Firewall có nhiều khuynh hướng và trạng thái khác nhau. Chúng hạn chế những gói tin từ đơn giản đến phức tạp bao gồm những trạng thái và đặc tính kiểm tra sâu hơn. Ví dụ bạn có thể cấu hình ACLs (Access List) đơn giản trên router để ngăn chặn kẻ tấn công truy cập vào hệ thống.

Hình bên dưới chỉ cho ta cách cấu hình router ngăn chặn truy cập không hợp pháp host và user trên mạng Internet.



Router có thể cấu hình từ chối tất cả các lưu lượng đi vào từ các host ngoài Internet. Chẳng hạn, một kẻ tấn công cố gắng scan mạng được bảo vệ từ Internet, thì router sẽ đánh rớt tất cả các lưu lượng.

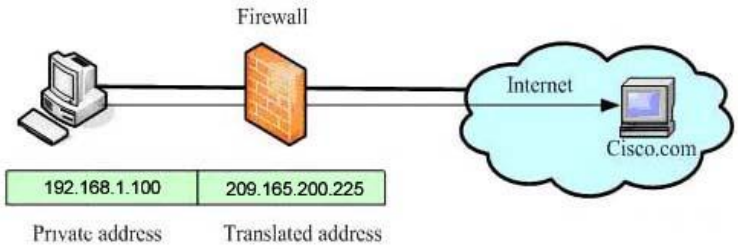
Mục đích của việc lọc gói là điều khiển truy cập mạng bằng cách định nghĩa lưu lượng mạng có thể đi qua chúng. Việc lọc gói sẽ kiểm tra lưu lượng đến tại lớp giao vận của mô hình OSI. Ví dụ, việc lọc gói có thể phân tích xem các gói là TCP hay UDP và xem xét chúng có chống lại các quy luật được xác định trước hay không, quá trình này được gọi là ACLs (Access List). Chúng kiểm tra các yếu tố sau:

Địa chỉ nguồn
Địa chỉ đích
Port nguồn
Port đích
Giao thức

❖ **Network Address Translation (NAT):**

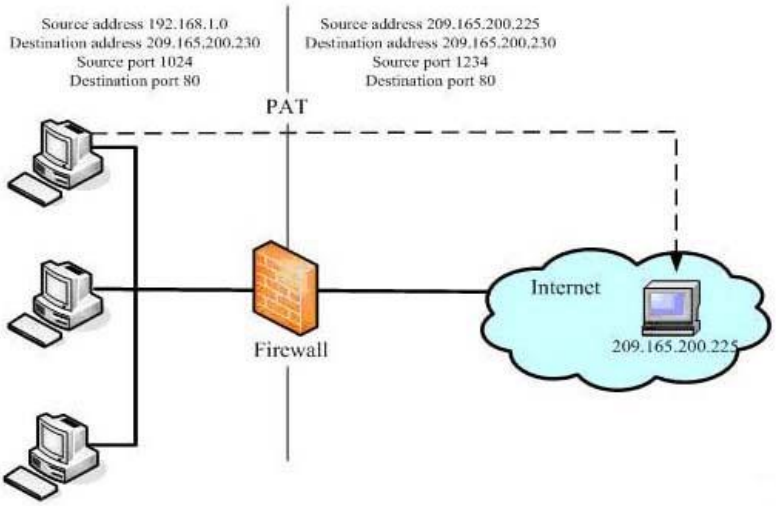
Firewall có thể cung cấp các dịch vụ NAT. Chúng có thể dịch địa chỉ IP private sang địa chỉ Public. Địa chỉ private là địa chỉ dùng trong mạng nội bộ, không có ý nghĩa ngoài mạng internet. Địa chỉ public là địa chỉ đơn nhất trên mạng internet và không bị trùng.

Hình 4.13 chỉ cách dịch địa chỉ của host trong mạng nội bộ (192.168.1.100) thành địa chỉ IP public (209.165.200.225) khi host này cố gắng truy cập đến trang Cisco.com



Hình 4.13. Kỹ thuật NAT

Kỹ thuật NAT cũng có nhiều loại khác nhau. Các phương pháp chung nhất là PAT (Port Address Translation) và NAT tĩnh. PAT cho phép nhiều thiết bị trong một phân đoạn mạng có thể biên dịch sang một địa chỉ IP bằng cách kiểm tra thông tin lớp 4 (lớp transport) của gói đó. Hình 4.14 minh họa cách 3 máy khác nhau trong tổ chức mạng biên dịch sang một địa chỉ IP public.



Hình 4.14. Kỹ thuật PAT

Việc kiểm tra trạng thái kết nối của firewall thông qua giao diện của nó bằng các khảo sát không chỉ nội dung header của gói tin mà cả các lớp ứng dụng thông tin. Điều này được thực hiện để tìm ra sự giao dịch hơn là tìm ra địa chỉ nguồn, đích và những port. Điển hình, firewall theo dõi trạng thái kết nối và duy trì một bảng thông tin ở lớp network và transport. Những Firewall phức tạp thực hiện sự phân tích lớp trên được gọi là deep-packet inspection (kiểm tra chuyên sâu gói tin).

❖ **Deep Packet Inspection:**

Một vài ứng dụng yêu cầu việc dùng các gói tin đặc biệt khi chúng đi qua Firewall. Điều này bao gồm các giao thức và các ứng dụng nhúng thông tin địa chỉ IP vào trường dữ liệu hoặc mở kênh động thứ hai gán cho port. Những Firewall phức tạp và những ứng dụng bảo mật như Cisco ASA, Cisco PIX Firewall và Cisco IOS Firewall kiểm tra những ứng dụng nhúng các thông tin địa chỉ cho phép những ứng dụng và các giao thức đề cập trước được hoạt động. Việc kiểm tra ứng dụng, những ứng dụng bảo mật có thể kiểm tra tại các port động và cho phép trao đổi dữ liệu trên port này trong suốt thời gian xảy ra kết nối.

Với Deep Packet Inspection, Firewall có thể kiểm tra các trường đặc biệt ở lớp 7 application để bảo vệ chống lại các mối đe dọa bảo mật.

❖ **VoIP-Aware Firewall**

Với việc hiểu cơ bản về NAT, mã hóa và kỹ thuật Firewall, thì có thể đánh giá được những thách thức cho việc giữ an toàn lưu lượng mạng VoIP mà không tách các luồng thoại ra khỏi Firewall hay ngăn cản chúng. Vấn đề cơ bản ở đây là: người quản trị Firewall miễn cưỡng mở các port cao (>1024) cho phép các kết nối không kiểm soát được giữa các host bên ngoài và bên trong, và Firewall ghi lại thông tin cần thiết cho lưu lượng báo hiệu VoIP thành công. Trong trường hợp đầu tiên, lưu lượng cuộc gọi, lưu lượng truyền thông và điều khiển truyền thông đi qua các port cao chuyên quyền. Trong trường hợp thứ hai, quy tắc chung trong phần này của bộ giao thức H.323 là thông tin địa chỉ IP và số port được trao đổi trong chuỗi dữ liệu của trường mào đầu kết nối. Dĩ nhiên, SIP và H.323 là hai giao thức riêng biệt, chúng cũng có những yêu cầu khác nhau đối với Firewall.

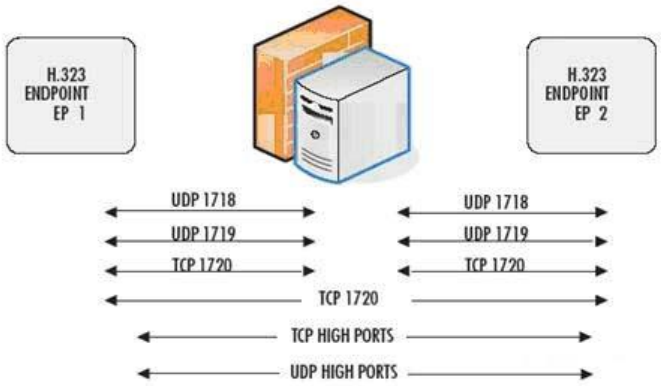
❖ **H.323 Firewall**

Thoại cơ bản cài đặt H.323 yêu cầu các port được chỉ ra trong bảng

FUNCTION	PORT	PROTOCOL
Gatekeeper discovery	1718	UDP
Gatekeeper RAS	1719	UDP
Q.931 Call Signaling (Setup)	1720	TCP
H.245 Signaling (Call parameters)	1024–65535	TCP

Bảng 4.16. Thiết lập cuộc gọi cơ bản

Một ví dụ được đưa ra trong hình 4.17, ở đây giả thiết có 1 gatekeeper và 2 endpoint



Hình 4.17. Thông tin port H.323

Vì H.323 tin cậy trên các port động, việc lọc gói trên Firewall không phải là một giải pháp đặc biệt thuận lợi, trong khi các port lớn hơn 1024 phải được mở cho cuộc gọi diễn ra. Vì vậy, giải pháp Firewall hỗ trợ H.323 là phải tháo dỡ và kiểm tra các gói báo hiệu (H.245, H.225.0) và trạng thái mở các port Firewall cho cả gói điều khiển H.245 và các gói phương tiện truyền thông hai chiều.

Hiện nay, các sản phẩm Firewall như Check point, Cisco PIX,... đều có cơ chế hỗ trợ H.323 với khi sử dụng NAT, không NAT mà vẫn đảm bảo tính bảo mật.

❖ SIP Firewall

Không giống như H.323, cú pháp SIP dựa vào H.323. ASCII được phân tích là kinh tế hơn so với mã hóa đóng gói PDU. Một phiên SIP có thể bị bẻ gãy bởi ba phần tử: định vị người gọi, thiết lập phiên, và vận chuyển truyền thông.

Trong ngữ cảnh đi qua Firewall và NAT, vấn đề sơ cấp của SIP liên quan đến xác định địa chỉ IP thật của người dùng cuối mà thường được định vị trong vùng địa chỉ IP private. Không giống như H.323, SIP không nối tiếp các địa chỉ IP và số port bên trong các gói điều khiển. Tuy nhiên như trong trường hợp H.323, SIP khi sử dụng như một ứng dụng VoIP, mở hai chiều phương tiện truyền thông UDP ngẫu nhiên ở các port cao. Các port cao của kênh truyền thông RTP đàm phán trong suốt quá trình thiết lập phiên, duy trì thời gian gọi, và sẽ đóng ngay lập tức sau điểm cuối cùng cuộc gọi.

4.2.2.7. Logging

Việc ghi nhận được tạo ra bởi các server, gateway, firewall, proxy, router và switch thường chứa đựng những thông tin liên quan đến an toàn. Nhưng những người quản trị hệ thống bình thường vô tình xóa đi ghi nhận với việc cấu hình và bảo trì lặt vặt khác. Chìa khóa thành công trong việc phân tích những ghi nhận là chấp nhận những công cụ thích hợp cho việc tự động phân tích, báo cáo lại kết quả ghi nhận dữ liệu.

- **Syslog**

Giao thức syslog cung cấp một sự chuyên chở cho phép các máy gửi những sự kiện thông điệp thông báo băng qua mạng IP đến những người thu gom những sự kiện thông điệp này, được biết như là syslog server. Syslog là một giao thức lẻ được thực hiện trên nhiều nền tảng trước khi giao thức này được thông qua bởi tổ chức IEEE. Những thông điệp syslog sử dụng UDP/514 cho việc chuyên chở, tăng khả năng mất gói, và không được chú ý, điều này tạo sự dễ dàng cho bất cứ ai trong việc làm giả các gói tin, cũng như việc chèn thêm việc ghi nhận sự kiện hay làm tràn ngập server.

Vào thời điểm này, syslog không quy định sự mã hóa, vì thế các thông điệp được gửi đến có thể bị lộ với bất kỳ ai trên đường dây. Gần đây một phác thảo được đề xướng mô tả một cơ chế thêm vào nguồn gốc sự chứng thực, tính toàn vẹn thông điệp, sự phát lại, sự chống cự, sự thông báo, sự sắp xếp lại thứ tự và phát hiện ra những syslog bị mất, nhưng điều này thông thường không được thực hiện.

Một vài sự thay thế syslog phổ biến có thể dùng TCP cho việc phân phát tin cậy và thêm một số kiểm tra hoặc chữ ký mã hóa cho mỗi sự kiện ghi

nhận. Thông điệp syslog có thể được gửi đến ghi nhận cục bộ, điều khiển cục bộ, server syslog từ xa, hay một syslog chuyển tiếp từ xa.

Syslog sử dụng tính nghiêm khắc (hay độ ưu tiên) để phân loại những ghi nhận thông điệp quan trọng. Các mức độ ưu tiên bao gồm:

0: Mức khẩn cấp: Hệ thống không dùng được.

1: Báo động: Hành động phải được nắm bắt ngay.

2: Phê bình: Những điều kiện phê bình.

3: Lỗi: Những điều kiện lỗi.

4: Cảnh báo: Những điều kiện cảnh báo.

5: Chú ý: Những điều kiện bình thường mà quan trọng.

6: Thông tin: Những thông báo thông tin.

7: Gỡ lỗi: Gỡ lỗi-những thông báo mức.

4.2.2.8. Các phương pháp xác thực phụ

Bảo mật thông tin được định nghĩa ở một số lớp. Cơ sở cho ý tưởng này là tất cả thời gian và địa điểm hay trở ngại vật lý được tạo ra nhằm mục đích ngăn chặn tấn công. 802.1X/EAP và PKI là những lớp rộng lớn, phức tạp mà khi thực hiện và bảo trì cần phải chính xác, kết quả là việc truy cập sẽ an toàn hơn. Có một số biện pháp chi phí không cao, không tốn nhiều sức mà người quản trị có thể đưa ra để hạn chế việc truy nhập mạng đến những thiết bị cho phép.

- Công cụ MAC (MAC Tool): quy tắc bảo mật cơ bản là các điểm cuối không thể được tin cậy khi nó chưa được kiểm chứng xác thực. Với VoIP, một phương pháp cho chứng thực cho các điện thoại IP là phần cứng hay địa chỉ MAC. MAC là một địa chỉ gồm 6 byte được biểu diễn bằng số HEX. Ba byte đầu đại diện ID nhà cung cấp, ba byte còn lại hình thành một địa chỉ đơn nhất cho bất kỳ mạng nào được nối tới thiết bị.
- ARP spoofing: Nguyên lý của nó đã được trình bày ở trên. Để hạn chế việc giả mạo ARP này thì những chỉ định về điều khiển an toàn về mặt vật lý và một password tốt là điều kiện tiên quyết cần phải được thực hiện.
- Port Security: Khi chuẩn 802.1X ra đời, thì không có thiết bị nào hỗ trợ cho nó. Thiết bị không hỗ trợ 802.1X có thể được điều khiển bởi

xác thực địa chỉ MAC. Các thiết bị không hỗ trợ 802.1X như máy in và một số điện thoại IP có thể điều tiết bằng cách dùng port security. Và các thiết bị này cần phải được đặt vào trong VLAN.

Chương 5

CẤU HÌNH VOIP CƠ BẢN VÀ TRIỂN KHAI TRÊN MẠNG CỤC BỘ ỨNG DỤNG CHO DOANH NGHIỆP NHỎ

5.1. CẤU HÌNH VOIP CƠ BẢN MÔ HÌNH PHÒNG LAP [5]

Trong mô hình này sử 2 router 2600 trên phòng Lap (Học viện mạng Bách Khoa Hà Nội), đóng vai trò là 2 Gateway hỗ trợ VoIP. Thiết bị đầu cuối sử dụng 2 máy tính có cài đặt phần mềm Cisco IP Communication. Để sử dụng phần mềm Cisco IP Communication hoạt động như một ephone phải cài đặt gói quản lý CME (Call manger Express) cho các router.

5.1.1. Cấu hình giao thức mặc định của Gateway

5.1.1.1. Một số câu lệnh chính trong bài lab

Cấu hình định tuyến cho Gateway

Có nhiều giao thức định tuyến khác nhau có thể được chọn để định đường đi cho gói tin. Trong bài lab này sẽ cấu hình định tuyến với giao thức RIP.

- Router(config)#**router rip**. Chọn giao thức định tuyến RIP.
- Router(config-router)#**network** *net-ip-address*. Khai báo các mạng mà router kết nối trực tiếp để thông qua các giao diện đó RIP sẽ học được các giao diện khác không kết nối trực tiếp với router. Trong một router có thể có nhiều kết nối trực tiếp, vì vậy khi dùng giao thức RIP thì phải khai báo đầy đủ các kết nối trực tiếp này.
- Router(config-router)#**exit**. Thoát khỏi mode cấu hình định tuyến.

Cấu hình quản lý ephone

Để cấu hình quản lý một cisco CME phone, có thể cấu hình rất nhiều tham số đầy đủ để một phone hoạt động và hiển thị đầy đủ các hiện thị giờ, bí danh, tên, hay các kiểu chuông... Dưới đây là một số câu lệnh cơ bản để hỗ trợ CME phone đăng ký và quản lý CME phone.

- Router(config)#**telephony-service**. Lệnh này chọn chế độ cấu hình dịch vụ là telephone.
- Router(config-telephony)#**max-ephones** *digit***.** Câu lệnh đặt số IP phone tối đa được hỗ trợ bởi Gateway.
- Router(config-telephony)#**max-dn** *digit.*
- Router(config-telephony)#**ip source-address** *ipaddress***.** Lệnh này chỉ ra địa chỉ IP cổng của router mà tại đó ephone sẽ đăng ký.
- Router(config-telephony)#**create cnf-files.** Lệnh cho phép cấu hình file XML.
- Router(config-telephony)#**secondary-dialtone 9.** Lệnh này để tạo một âm khác khi ấn số 9 gọi ra ngoài mạng.
- Router(config-telephony)#**timeouts interdigit** *digit***.** Lệnh thiết đặt thời gian timeout giữa các lần nhấn số liên tiếp. Đợn vị thời gian tính theo giây.
- Router(config-telephony)#**timeouts ringing** *digit***.** Lệnh đặt thời gian ring chuông cho phép. Nếu quá thời gian trên mà bên kia không nhấc máy thì cuộc gọi chấm dứt.
- Router(config-telephony)#**date-format** *dd-mm-yy***.** Lệnh đặt kiểu hiển thị thời gian trên ephone.
- Router(config-telephony)#**exit.** Kết thúc mode telephone service.
- Router(config)#**ephone-dn 1 dual-line.** Tạo một đường điện thoại với 2 dây.
- Router(config-ephone-dn)#**number** *ephone-number***.** Thiết lập số điện thoại cho ephone. Có chiều dài từ 3 đến 5 số.
- Router(config-ephone-dn)#**name** *name***.** Lệnh này cho phép đặt tên thay cho số điện thoại.
- Router(config)#**ephone 1.** Cấu hình cổng giao diện vật lý cho

ephone.

- Router(config-ephone)#**mac-address** *MAC***.** Khai báo địa chỉ mác của máy tính cài đặt ephone.
- Router(config-ephone)#**button** *1:1*.
- Router(config-ephone)#**exit.** Kết thúc mode.

Cấu hình Dial-peer cho Cisco CME Phones

- Router(config)#**voice service voip.** Lệnh cấu hình và chỉ rõ loại hình dịch vụ voice là voip.
- Router(config-voi-serv)#**allow-connections h323 to sip.** Lệnh cho phép một đầu cuối H.323 có thể kết nối được với một đầu cuối SIP trong mô hình IP – to IP Gateway.
- Router(config-voi-serv)#**exit**.
- Router(config)#**dial-peer voice** *tag Peer type***.** Lệnh định nghĩa một dial - peer cụ thể. Giá trị *tag* thay đổi từ 1 đến 2147483647. *Peer type* bao gồm có POST, VoIP, VoFR, VoATM, đây là những kiểu kết nối. Kiểu POST kết nối đến (PSTN, PBX, telephone, and fax) hay là các WAN riêng sử dụng VoIP, VoFR, VoATM. Trong bài lab này kiểu được dùng là VoIP.
- Router(config-dial-peer)#**destination-pattern** *string*. Lệnh xác định đích cho cuộc gọi dial-peer.
- Router(config-dial-peer)#**session target ipv4:***ipaddress*. Lệnh chỉ ra địa chỉ của cổng router mà tại đó cuộc gọi được nhận.
- Router(config-dial-peer)#**dtmf-relay** *type-channel*. Lệnh này cho phép chọn phương thức mạng thông tin báo hiệu **dtmf.** Router cisco hỗ trợ các phương thức mang **dtmf** như hình dưới đây.

```
R1(config-dial-peer)#dtmf-relay ?
  cisco-rtp           Cisco Proprietary RTP
  h245-alphanumeric   DTMF Relay via H245 Alphanumeric IE
  h245-signal         DTMF Relay via H245 Signal IE
  rtp-nte             RTP Named Telephone Event RFC 2833
  sip-notify          DTMF Relay via SIP NOTIFY messages
```

Hình 5.1. Các phương thức mạng thông tin dtmf

- Router(config-dial-peer)#**codec** *g711ulaw***.** Lệnh chỉ ra chuẩn mã hóa voice. Trong router cisco hỗ rất nhiều chuẩn mã hóa:

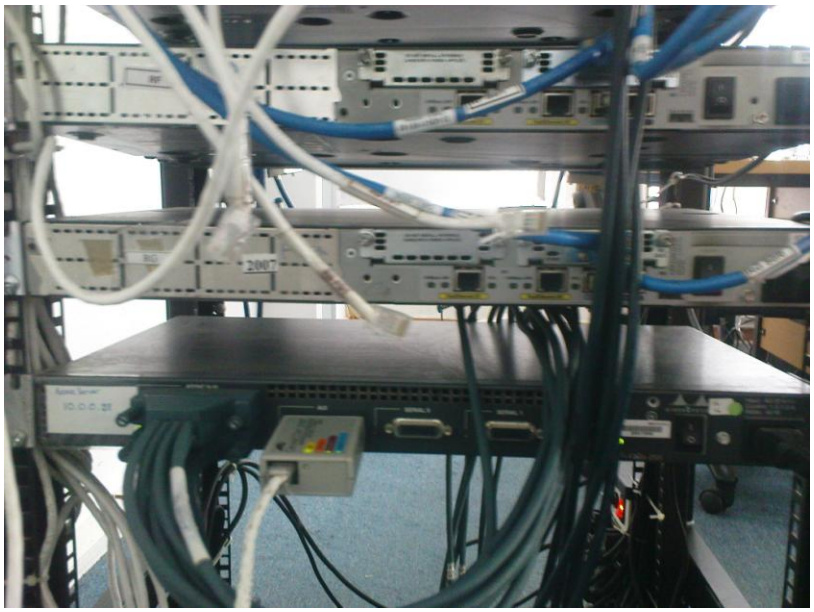
```
R1(config-dial-peer)#codec
R1(config-dial-peer)#codec ?
  clear-channel  Clear Channel 64000 bps (No voice capabilities: data transport
                 only)
  g711alaw       G.711 A Law 64000 bps
  g711ulaw       G.711 u Law 64000 bps
  g723ar53       G.723.1 ANNEX-A 5300 bps (contains built-in vad that cannot be
                 disabled)
  g723ar63       G.723.1 ANNEX-A 6300 bps (contains built-in vad that cannot be
                 disabled)
  g723r53        G.723.1 5300 bps
  g723r63        G.723.1 6300 bps
  g726r16        G.726 16000 bps
  g726r24        G.726 24000 bps
  g726r32        G.726 32000 bps
  g728           G.728 16000 bps
  g729br8        G.729 ANNEX-B 8000 bps (contains built-in vad that cannot be
                 disabled)
  g729r8         G.729 8000 bps
  gsmefr         GSMEFR 12200 bps (contains built-in vad that cannot be
                 disabled)
  gsmfr          GSMFR 13200 bps
```

Hình 5.2. Các chuẩn mã hóa router cisco hỗ trợ

- Router(config-dial-peer)#**no vad**. Không cho phép tự động dò tìm voice trong các cuộc gọi dial-peer.
- Router(config-dial-peer)#**end**. Cấu hình xong và thoát khỏi mode cấu hình.

5.1.1.2. Thực hiện và kết quả

Nối 2 router 2600 bởi cáp serial, 2 PC nối với router bằng cáp chéo cross-over và cài đặt phần mềm Cisco Communicator trên các PC để chúng là các soft-phone. Các cổng console của routerA và routerB được nối với một router access 2500 giúp ta có thể config router thông qua telnet thay vì cổng Com.



Hình 5.3. RouterA, router B và router Access trong phòng Lap

Việc thực hiện cấu hình địa chỉ IP các cổng trên router và PC khá đơn giản nên em xin đi vào cấu hình các phần chính.

- **Router A**

RA(config)#**router rip**
RA(config-router)#**network** *172.16.2.0*
RA(config-router)#**network** *172.16.3.0*
RA(config-router)#**exit**
RA(config)#**telephony-service**
RA(config-telephony)#**max-ephones** *3*
RA(config-telephony)#**max-dn** *3*
RA(config-telephony)#**ip source-address** *172.16.3.1*
RA(config-telephony)#**create cnf-files**
RA(config-telephony)#**secondary-dialtone** *9*
RA(config-telephony)#**timeouts interdigit** *20*
RA(config-telephony)#**timeouts ringing** *100*
RA(config-telephony)#**time-format** *24*
RA(config-telephony)#**date-format** *dd-mm-yy*
RA(config-telephony)#**exit**
RA(config)#**ephone-dn 1 dual-line**
RA(config-ephone-dn)#**number** *101*
RA(config-ephone-dn)#**name** *dotuan101*
RA(config)#**ephone 1**
RA(config-ephone)#**mac-address** *0021.977B.AB93*
RA(config-ephone)#**button** *1:1*
RA(config-ephone)#**exit**
RA(config)#**voice service voip**
RA(config-voi-serv)#**allow-connections h323 to sip**
RA(config-voi-serv)#**exit**
RA(config)#**dial-peer voice** *1 voip*
RA(config-dial-peer)#**destination-pattern** *102*
RA(config-dial-peer)#**session target ipv4:***172.16.2.2*
RA(config-dial-peer)#**dtmf-relay** cisco-*rtp*

RA(config-dial-peer)#**codec** *g711ulaw*
Router(config-dial-peer)#**no vad**
Router(config-dial-peer)#**end**

- **Router B**

  Thực hiện tương tự router A nhưng với số phone là 102, name: dotuan102, MAC 0021.977A.609E

Dưới đây là kết quả cấu hình. Bằng cách sử dụng các lệnh show running-config để thấy được hoàn thành cấu hình router.

RA#show running-config	**RB#show running-config**
hostname RA	hostname RB
voice service voip	voice service voip
allow-connections h323 to sip	allow-connections h323 to sip
interface FastEthernet0/0	interface FastEthernet0/0
ip address 172.16.3.1 255.255.255.0	ip address 172.16.1.1 255.255.255.0
duplex auto	duplex auto
speed auto	speed auto
interface Serial0/1	interface Serial0/0
ip address 172.16.2.1 255.255.255.0	ip address 172.16.2.2 255.255.255.0
clockrate 64000	
dial-peer voice 1 voip	dial-peer voice 2 voip
destination-pattern 102	destination-pattern 101
session target ipv4:172.16.2.2	session target ipv4:172.16.2.1
dtmf-relay cisco-rtp	dtmf-relay cisco-rtp
codec g711ulaw	codec g711ulaw
no vad	no vad
telephony-service	telephony-service
max-ephones 3	max-ephones 3
max-dn 3	max-dn 3
ip source-address 172.16.3.1 port 2000	ip source-address 172.16.1.1 port 2000

timeouts interdigit 20 timeouts ringing 100 time-format 24 date-format dd-mm-yy secondary-dialtone 9 ephone-dn 1 dual-line number 101 name dotuan101 ephone 1 mac-address 0021.977B.AB93 button 1:1 end	timeouts interdigit 20 timeouts ringing 100 time-format 24 date-format dd-mm-yy secondary-dialtone 9 ephone-dn 1 dual-line number 102 name dotuan102 ephone 2 mac-address 0021.977A.609E button 1:1 end

Trong mô hình cơ bản này nếu giao thức không được chỉ ra thì Gateway mặc định sử dụng giao thức H.323 low, tức là H.323 version 1. Sau khi đã thiết lập cấu hình đầy đủ cho các Gateway và các PC, nhận được kết quả khi kết nối các cuộc gọi. Vì thực hiện trên hai router thật với khoảng cách ngắn lại và đường truyền chỉ có tín hiệu voice nên chất lượng thoại rất tốt.

Giao diện ephone khi đã kết nối thành công như sau:

5.2. TRIỂN KHAI TRÊN MẠNG CỤC BỘ ỨNG DỤNG CHO DOANH NGHIỆP NHỎ [5],[8],[9]

Dựa theo cấu hình cơ bản phần trên đưa ra mô hình triển khai ứng dụng cho doanh nghiệp nhỏ trên mạng cục bộ.

Với mô hình cơ bản việc thiết lập tạo cuộc gọi, xác thực ephone number, người gọi… đều dựa trên cấu hình mặc định gateway là xác thực theo địa chỉ vật lý MAC, điều này khiến có thể dễ dàng thay đổi để trỏ đến địa chỉ MAC của kẻ tấn công. Phương pháp này là tấn công *man in the middle* đã được trình bày trong chương 4, kẻ tấn công sẽ là trung gian trong cuộc đàm thoại giữa hai đầu cuối, việc lấy cắp thông tin nghe trộm cuộc gọi bây giờ thật đơn giản.

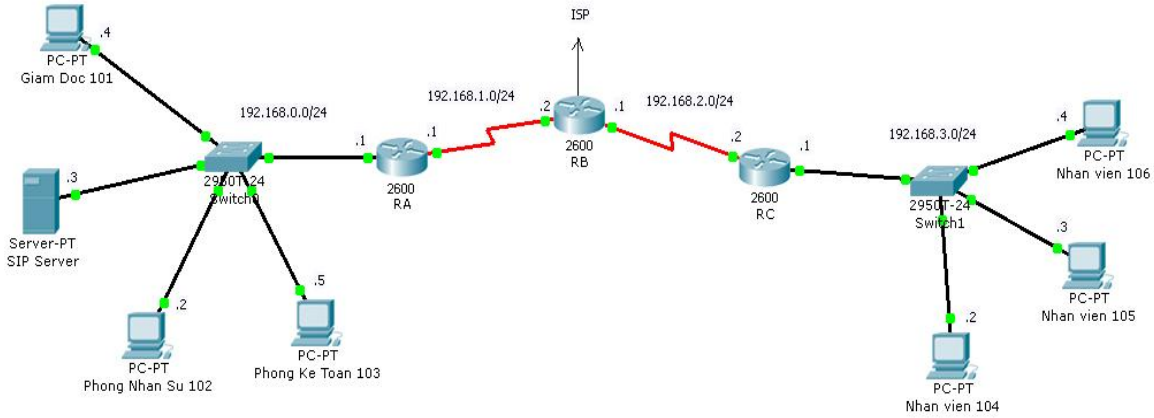
Trong doanh nghiệp mọi thông tin kinh doanh đều tuyệt đối quan trọng, vấn đề bảo mật thông tin cần được ưu tiên hàng đầu. Do đó cần khắc phục những sơ hở trong cấu hình cơ bản VoIP khi đưa vào ứng dụng. Biện pháp đưa ra là sử dụng SIP server. SIP server cung cấp cho mỗi người dùng một tài khoản và mật khẩu truy nhập riêng. Khi thực hiện đăng nhập khởi tạo cuộc gọi, SIP server sẽ xác thực tài khoản, mật khẩu và địa chỉ IP thay vì sử dụng địa chỉ vật lý MAC. Hơn nữa những thông tin này chỉ có thể thay đổi bởi người quản trị.

5.2.1. Mô hình mạng sử dụng SIP server

Thiết bị

- Các PC cài soft phone, 1 PC làm SIP server
- 3 Router, 2 Switch
- Softphone: X-lite (www.counterPath.com), SIP server: Brekeke Sip server (www.brekeke.com).

Mô hình



Hình 5.4. Mô hình mạng VoIP sử dụng SIP server

5.2.1.1. Cấu hình các thiết bị

- **PC SIP server:**

  - *Đặt địa chỉ cho PC SIP server*: 192.168.0.3
  - Subnet mask: 255.255.255.0
  - Default gateway: 192.168.0.1

- **Cài SIP server:**

  - Cài phần mềm SIP server sau đó login với user: sa , password: sa
  - Sau khi login ta sẽ thấy trạng thái của SIP server như sau.

Hình 5.5. Login vào SIP server

- Tiếp theo vào thẻ User Authentication chọn thẻ tiếp theo là New user.
- Tạo 1 user là: Giamdoc101, password: Giamdoc101 sau đó chọn add.

Hình 5.6. Tạo tài khoản user

- Tương tự tạo các user khác, sau khi hoàn thành trong phần view user hiển thị các user đã thiết lập:

Hình 5.7. Xác nhận tài khoản user

- **Cấu hình cho các PC softphone**

✧ Đặt địa chỉ cho PC Giamdoc101:

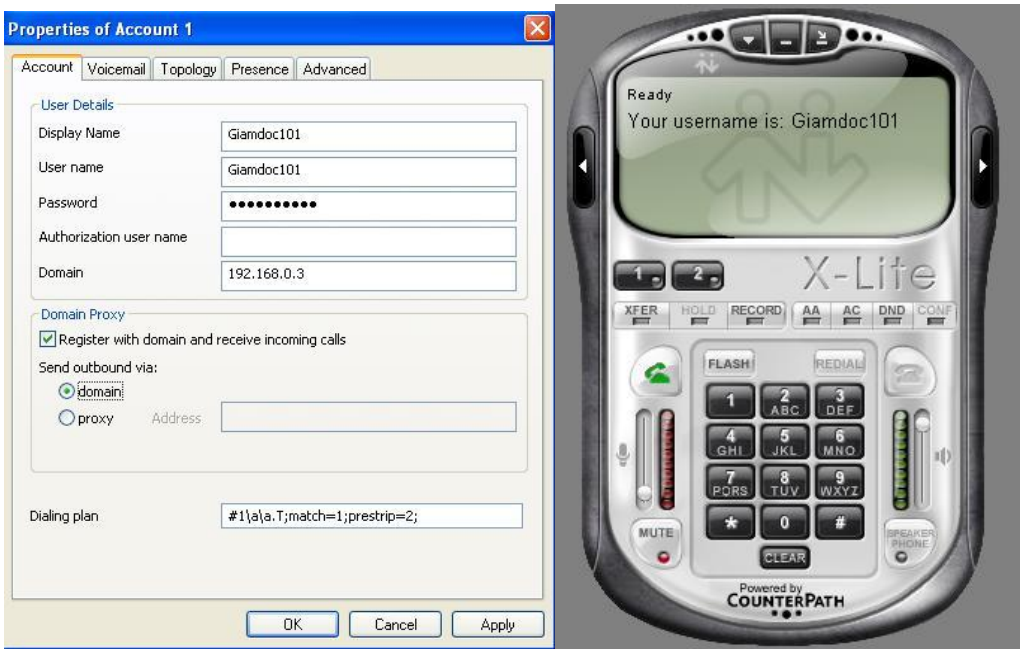
- Đặt địa chỉ: 192.168.0.4
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.0.1

✧ Cài Softphone là phần mềm X-lite:

- Sau khi cài đặt ta vào phần Sip account setting/add:
- Điền các thông tin giống như đã đăng ký trên SIP server (user: Giamdoc101, password: Giamdoc101)
- Trong phần Domain đặt địa chỉ IP của SIP server .

Sau đó chọn OK.

- Sau khi đăng nhập thành công trên softphone ta có thông tin sau:



Hình 5.8. Đăng nhập tài khoản trên X-lite

✧ Tương tự đặt địa chỉ cho PC Phòng kế toán 103

- Đặt địa chỉ IP: 192.168.0.5
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.0.1

- Cấu hình cho softphone: với user: Phongketoan103, password: Phongketoan103.

✧ Tương tự với các PC khác

- Đặt địa chỉ IP, subnet mask, default gateway theo mô hình 5.4

Lúc này tại SIP server trong phần Registered Clients các user đã kết nối và được xác thực tài khoản, nếu tài khoản là giả mạo, không trùng khớp với bảng user authentication sẽ không thể registed và thực hiện cuộc gọi.

Hình 5.9. Tài khoản đã được đăng kí sau khi xác thực

- **Cấu hình cho các Router**

Router RA:

+ Gán địa chỉ interface Ethernet 0/0: 192.168.0.1 Subnet mask: 255.255.255.0

+ Gán địa chỉ interface Serial 0/0: 192.168.1.1 Subnet mask: 255.255.255.0

+ Sử dụng giao thức định tuyến RIP.

Chi tiết:

RA(config-if)#**interface fastEthernet 0/0**

RA(config-if)#**ip address** *192.168.0.1 255.255.255.0*

RA(config-if)#**no shutdown**
RA(config)#**interface Serial 0/0**
RA(config-if)#**ip address** *192.168.1.1 255.255.255.0*
RA(config-if)#**clock rate** *64000*
RA(config-if)#**no shutdown**
RA(config)#**router rip**
RA(config-router)#**network** *192.168.1.0*
RA(config-router)#**network** *192.168.0.0*
RA(config-router)#**end**

Router RB:

+ Gán địa chỉ interface Serial 0/0: 192.168.1.2 Subnet mask: 255.255.255.0
+ Gán địa chỉ interface Serial 0/1: 192.168.2.1 Subnet mask: 255.255.255.0
+ Sử dụng giao thức định tuyến RIP.
+ Default route: 0.0.0.0 0.0.0.0 s1/0 tạo đường kết nối tới ISP.

Chi tiết:

RB(config)#**interface Serial 0/0**
RB(config-if)#**ip address** *192.168.1.2 255.255.255.0*
RB(config-if)#**no shutdown**
RB(config)#**interface Serial 0/1**
RB(config-if)#**ip address** *192.168.2.1 255.255.255.0*
RB(config-if)#**clock rate** *64000*
RB(config-if)#**no shutdown**
RB(config)#**router rip**
RB(config-router)#**network** *192.168.1.0*
RB(config-router)#**network** *192.168.2.0*
RB(config-router)#**end**
RB(config)#**ip route** *0.0.0.0 0.0.0.0 s1/0*

Router RC:

+ Gán địa chỉ interface Ethernet 0/0: 192.168.3.1 Subnet mask: 255.255.255.0

+ Gán địa chỉ interface Serial 0/0: 192.168.2.2 Subnet mask: 255.255.255.0

+ Sử dụng giao thức định tuyến RIP.

Chi tiết:

RC(config-if)#**interface fastEthernet 0/0**

RC(config-if)#**ip address** *192.168.3.1 255.255.255.0*

RC(config-if)#**no shutdown**

RC(config)#**interface Serial 0/0**

RC(config-if)#**ip address** *192.168.2.2 255.255.255.0*

RC(config-if)#**no shutdown**

RC(config)#**router rip**

RC(config-router)#**network** *192.168.2.0*

RC(config-router)#**network** *192.168.3.0*

RC(config-router)#**end**

Thực hiện gọi:

- Sau khi các máy đã đăng ký với SIP server, ta có thể thực hiện cuộc gọi.
- Ví dụ tại PC Phongketoan103 nhập: Giamdoc101 và gọi thì tại PC Giamdoc101 sẽ nhận được chuông báo và có thể nhấc tổ hợp bắt đầu đàm thoại.

Hình 5.10. Cuộc gọi thiết lập thành công

Với cơ sở hạ tầng yêu cầu đơn giản, chất lượng cuộc gọi VoIP khá tốt, bảo mật an toàn thông tin được đề cao, nhiều dịch vụ đi kèm như cuộc gọi kèm Video nếu có camera… mô hình này sẽ là lựa chọn khá tối ưu ứng dụng cho văn phòng doanh nghiệp nhỏ.

KẾT LUẬN

Trước hết em xin tóm tắt những vấn đề mà đồ án đã đạt được:

Lý thuyết

- Thế nào là VoIP, chỉ ra những ưu điểm, nhược điểm, các ứng dụng của VoIP.
- Nghiên cứu các mô hình mạng VoIP với các chuẩn giao thức khác nhau. Cụ thể là nền tảng IP và hai giao thức báo hiệu H.323/SIP. So sánh được sự khác nhau giữa hai giao thức báo hiệu.
- Nắm rõ phương thức tấn công để xây dựng phương thức bảo mật an toàn thông tin cho cơ quan, doanh nghiệp.

Thực nghiệm

- Thiết lập mạng VoIP cơ bản trong phòng Lap với các thiết bị viễn thông của Cisco.
- Thiết lập mô hình mạng VoIP sử dụng SIP server để xác thực tài khoản, ngăn sự sửa đổi thông tin cho mục đích xấu. Mô hình này tạo sự an toàn cùng với nhiều tiện lợi như dễ sử dụng, có dịch vụ đi kèm… sẽ là lựa chọn khá tối ưu cho doanh nghiệp.

Sau khi hoàn thành nội dung đồ án này, em đã có thể nắm vững được nền tảng nguyên lý hoạt động và các phương thức để đảm bảo an toàn thông tin trong VoIP, điều đó thực sự sẽ giúp ích cho em rất nhiều trong công việc sau này cũng như giúp em chắp nối kiến thức đã học trên lớp về mạng viễn thông.

Do hạn chế về thời gian, khuôn khổ của đồ án cũng như kinh nghiệm thực tiễn của em chưa nhiều nên không tránh khỏi những sai sót và những nhầm lẫn. Em rất mong được sự góp ý và phê bình của thầy cô và các bạn.

Một lần nữa em xin chân thành cảm ơn!

MỤC LỤC