MỤC LỤC

[DANH MỤC THUẬT NGỮ VIẾT TẮT 5](#_Toc20426641)

[DANH MỤC HÌNH ẢNH 6](#_Toc20426642)

[CHƯƠNG 1: NGHIÊN CỨU LÝ THUYẾT VỀ HỆ THỐNG TRUYỀN THANH RADIO SỐ 7](#_Toc20426643)

[1.1. Nghiên cứu và tìm hiểu các công nghệ, kỹ thuật đang sử dụng trên các hệ thống truyền thanh tại việt nam Khánh D15 7](#_Toc20426644)

[1.1.1. Phương thức truyền thanh hữu tuyến( truyền thanh có dây) 8](#_Toc20426645)

[1.1.2. Phương thức truyền thanh vô tuyến( truyền thanh không dây phát sóng FM) 9](#_Toc20426646)

[1.1.3. Nhược điểm của các phương thức cũ 18](#_Toc20426647)

[1.2. Nghiên cứu, tìm hiểu một số hệ thống truyền thanh tiên tiến trên thế giới hiện nay Khánh D15 21](#_Toc20426648)

[1.3. Nghiên cứu lí thuyết về truyền thanh radio số trong hệ thống truyền thanh không dây đồng nhất 3 cấp Khánh D15 27](#_Toc20426649)

[1. 3.1. Điều kiện tiên quyết kỹ thuật để Internet Radio 27](#_Toc20426650)

[1.3.2. Sự khác biệt giữa Radio Internet và Radio cổ điển 29](#_Toc20426651)

[1.3.3. Khía cạnh kỹ thuật của Radio Internet 30](#_Toc20426652)

[1.3.4. Công nghệ truyền dẫn 31](#_Toc20426653)

[1.3.5. Công nghệ SHOUTCAST 33](#_Toc20426654)

[1.3.6. PODCASTING 36](#_Toc20426655)

[1.3.7. Nén và chất lượng của chương trình 37](#_Toc20426656)

[1.3.8. Nâng cao chất lượng bản ghi 40](#_Toc20426657)

[1.3.9. Yêu cầu của mạng 41](#_Toc20426658)

[1.4. Nghiên cứu các giải pháp về bảo mật dịch vụ trong mạng IP Hiếu D16 42](#_Toc20426659)

[1.4.1. Đặt vấn đề 42](#_Toc20426660)

[1.4.2. Các kiểu tấn công mạng phổ biến 43](#_Toc20426661)

[1.4.3. Nguyên lý thiết kế hệ thống bảo mật 49](#_Toc20426662)

[1.5. Nghiên cứu lí thuyết về kỹ thuật truyền dữ liệu số radio DATA SYSTEM RDS ứng dụng trong hệ thống truyền thanh không dây đồng nhất 3 cấp Khoa D16 66](#_Toc20426663)

[1.5.1. Giới thiệu chung 66](#_Toc20426664)

[1.5.2. Lý thuyết chung về điều tần 69](#_Toc20426665)

[1.5.3. Hệ thống RDS (Radio Data System) 76](#_Toc20426666)

[1.6. Nghiên cứu lí thuyết hệ thống bảo mật bằng One Time Password (OPT) và ứng dụng trong hệ thống truyền thông không dây đồng nhất 3 cấp Vũ D16 90](#_Toc20426667)

[1.6.1. Tổng quan về OTP 90](#_Toc20426668)

[1.6.2. Facebook Account Kit 99](#_Toc20426669)

[CHƯƠNG 2: KHẢO SÁT HIỆN TRẠNG HỆ THỐNG TRUYỀN THANH CỦA VIỆT NAM HIỆN NAY NÓI CHUNG VÀ ĐẮK LẮK NÓI RIÊNG 103](#_Toc20426670)

[CHƯƠNG 3: THIẾT KẾ MÔ HÌNH TỔNG QUÁT HỆ THỐNG TRUYỀN THÔNG KHÔNG DÂY ĐỒNG NHẤT 3 CẤP 104](#_Toc20426671)

[3.1. Nghiên cứu, thiết kế mô hình cơ sở dữ liệu của hệ thống máy chủ nội dung Phúc D16 104](#_Toc20426672)

[3.1.1. Tổng quan về hệ quản trị cơ sở dữ liệu 104](#_Toc20426673)

[3.1.2. Phân tích, thiết kế mô hình cơ sở dữ liệu của hệ thống máy chủ nội dung 114](#_Toc20426674)

[3.2. Nghiên cứu, thiết kế chức năng phần mềm lưu trữ và quản lí dữ liệu trên máy chủ nội dung Phúc D16 117](#_Toc20426675)

[3.2.1. Tổng quan về SQL 117](#_Toc20426676)

[3.2.2. Phân quyền đăng bài*,* quyền kiểm duyệt, quyền sửa/xóa/tải về và quyền truy cập CSDL. 125](#_Toc20426677)

[3.2.3. Tạo các yêu cầu ưu tiên, chứng thực người dùng. 129](#_Toc20426678)

[3.3. Nghiên cứu, thiết kế chức năng phần mềm quản lý hệ thống máy chủ phát sóng Trung D16 131](#_Toc20426679)

[3.3.1. Khái niệm máy chủ phát sóng âm thanh (Broadcasting audio server) 131](#_Toc20426680)

[3.3.2.Kiến trúc đề xuất sử dụng trong mạng không đồng nhất 133](#_Toc20426681)

[3.3.3. Chức năng tự động phát sóng 138](#_Toc20426682)

[3.3.4. Lập lịch phát thanh 139](#_Toc20426683)

[3.3.5. Xác thực người nghe 140](#_Toc20426684)

[3.3.6. Hệ thống cảnh báo khẩn cấp 141](#_Toc20426685)

[3.3.7. Chứng thực thiết bị đầu cuối 142](#_Toc20426686)

[3.4. Nghiên cứu, thiết kế mô hình phần cứng của hệ thống Khoa D16 146](#_Toc20426687)

[3.4.1. Máy chủ nội dung 146](#_Toc20426688)

[3.4.2. Steaming server: 151](#_Toc20426689)

[3.4.3. Máy tính trạm hay máy Workstation là gì 159](#_Toc20426690)

[3.4.4. Máy thu internet radio 162](#_Toc20426691)

[3.4.5. Máy giải mã RDS\_OTP 162](#_Toc20426692)

[3.4.6. Máy phát FM 166](#_Toc20426693)

[3.4.7. Thiết bị đầu cuối là gì 168](#_Toc20426694)

[TÀI LIỆU THAM KHẢO 170](#_Toc20426695)

**DANH MỤC THUẬT NGỮ VIẾT TẮT**

**DANH MỤC HÌNH ẢNH**

[*Hình 1. 1: 9*](#_Toc20427884)

[*Hình 1. 2: 11*](#_Toc20427885)

[*Hình 1. 3 13*](#_Toc20427886)

[*Hình 1. 4 14*](#_Toc20427887)

[*Hình 1. 5 14*](#_Toc20427888)

[*Hình 1. 6 15*](#_Toc20427889)

[*Hình 1. 7 15*](#_Toc20427890)

[*Hình 1. 8 16*](#_Toc20427891)

[*Hình 1. 9 16*](#_Toc20427892)

[*Hình 1. 10 17*](#_Toc20427893)

[*Hình 1. 11 18*](#_Toc20427894)

[*Hình 1. 12 23*](#_Toc20427895)

[*Hình 1. 13 33*](#_Toc20427896)

[*Hình 1. 14 34*](#_Toc20427897)

[*Hình 1. 15 46*](#_Toc20427898)

[*Hình 1. 16 47*](#_Toc20427899)

[*Hình 1. 17 48*](#_Toc20427900)

[*Hình 1. 18 48*](#_Toc20427901)

[*Hình 1. 19 51*](#_Toc20427902)

[*Hình 1. 20 51*](#_Toc20427903)

[*Hình 1. 21 56*](#_Toc20427904)

[*Hình 1. 22 57*](#_Toc20427905)

[*Hình 1. 23 61*](#_Toc20427906)

[*Hình 1. 24 62*](#_Toc20427907)

[*Hình 1. 25 63*](#_Toc20427908)

[*Hình 1. 26 64*](#_Toc20427909)

[*Hình 1. 27 73*](#_Toc20427910)

[*Hình 1. 28: 81*](#_Toc20427911)

[*Hình 3. 1 107*](#_Toc20427857)

[*Hình 3. 2 111*](file:///E:\New%20folder\LHV\DakLak\Báo%20cáo%20DakLak.docx#_Toc20427858)

[*Hình 3. 3 116*](#_Toc20427859)

[*Hình 3. 4 118*](file:///E:\New%20folder\LHV\DakLak\Báo%20cáo%20DakLak.docx#_Toc20427860)

[*Hình 3. 5 127*](#_Toc20427861)

[*Hình 3. 6 129*](#_Toc20427862)

[*Hình 3. 7 131*](#_Toc20427863)

[*Hình 3. 8 132*](#_Toc20427864)

[*Hình 3. 9 132*](#_Toc20427865)

[*Hình 3. 10 135*](#_Toc20427866)

[*Hình 3. 11 136*](#_Toc20427867)

[*Hình 3. 12 136*](#_Toc20427868)

[*Hình 3. 13 138*](#_Toc20427869)

[*Hình 3. 14 138*](#_Toc20427870)

[*Hình 3. 15 139*](#_Toc20427871)

[*Hình 3. 16 140*](#_Toc20427872)

[*Hình 3. 17 141*](#_Toc20427873)

[*Hình 3. 18 142*](#_Toc20427874)

[*Hình 3. 19 142*](#_Toc20427875)

[*Hình 3. 20: 147*](#_Toc20427876)

[*Hình 3. 21 149*](#_Toc20427877)

[*Hình 3. 22 154*](#_Toc20427878)

[*Hình 3. 23 156*](#_Toc20427879)

[*Hình 3. 24 158*](#_Toc20427880)

[*Hình 3. 25 160*](#_Toc20427881)

[*Hình 3. 26 163*](#_Toc20427882)

[*Hình 3. 27 170*](#_Toc20427883)

**CHƯƠNG 1: NGHIÊN CỨU LÝ THUYẾT VỀ HỆ THỐNG TRUYỀN THANH RADIO SỐ**

**1.1. Nghiên cứu và tìm hiểu các công nghệ, kỹ thuật đang sử dụng trên các hệ thống truyền thanh tại việt nam Khánh D15**

Phát thanh Việt Nam là phương tiện truyền thông đại chúng quan trọng trong xã hội, khẳng định vai trò to lớn trong việc tuyên truyền đường lối, phổ biến các chủ trương chính sách của Đảng và Nhà nước, quảng bá các thông tin về kinh tế, chính trị, khoa học giáo dục văn hóa xã hội và thông tin dịch vụ cho mọi tầng lớp nhân dân trong xã hội. Cùng với sự phát triển của công nghệ điện tử - viễn thông và tin học, ngành phát thanh đã không ngừng hiện đại hóa về các trang thiết bị và ứng dụng các công nghệ mới nhằm đáp ứng nhu cầu nghe ngày càng đa dạng, chất lượng cao, góp phần đưa ngành phát thanh trở thành một ngành công nghiệp giải trí đem lại lợi nhuận lớn, đóng góp tích cực vào mức tăng trưởng kinh tế chung của đất nước, góp phần làm giảm khoảng cách về công nghệ so với các nước phát triển.

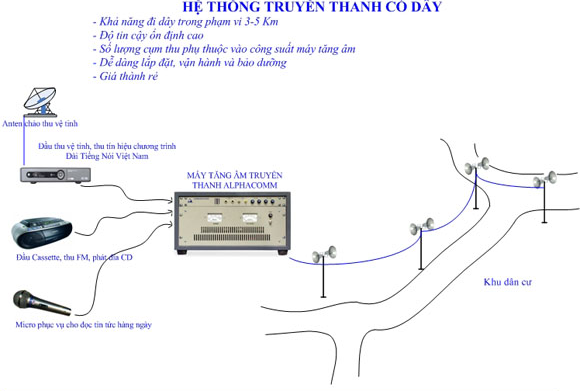
Tuy nhiên, hiện nay Đài truyền thanh xã, phường, thị trấn chủ yếu hoạt động theo 2 phương thức đây đều là phát thanh Analog AM và FM:

* truyền thanh hữu tuyến *(truyền thanh có dây) .*
* truyền thanh vô tuyến *(truyền thanh không dây phát sóng FM).*

Ngoài ra các đề án thử nghiệm truyền thanh số cũng đang được triển khai như Sáng 28-3-2017, tại Đài Tiếng nói Việt Nam 58 Quán Sứ, Hà Nội, Công ty cổ phần Phát triển phát thanh truyền hình (BDC) phối hợp với Trung tâm kỹ thuật phát thanh (Đài Tiếng nói Việt Nam) tổ chức Hội thảo Thử nghiệm phát thanh số theo tiêu chuẩn DAB+ tại Việt Nam.

### 1.1.1. **Phương thức truyền thanh hữu tuyến( truyền thanh có dây)**

Truyền thanh hữu tuyến là hệ thống chuyển tải âm thanh từ điểm phát tới các điểm thu thông qua đường truyền hữu tuyến. Tín hiệu âm thanh được chuyển đổi thành tín hiệu điện được truyền tải trên đường đây kim loại bằng đồng và được khôi phục lại thành tín hiệu âm thanh ở phía thu. Hiện nay ở rất nhiều địa phương trên nước ta vẫn đang sử dụng phương thức truyền thanh này.



Hình 1. 1:

Đầu thu kết nối với Anten chảo thu vệ tinh thu tín hiệu từ chương trình Đài Tiếng Nói Việt Nam thu được tín hiệu,hoặc tín hiệu thu từ đầu casesette,thu FM, đĩa CD, từ các Micro phục vụ chính quyền thông báo các tin tức hàng ngày đến người dân, các tín hiệu này được đưa đến máy tăng âm, từ máy tăng âm đưa đến các cụm loa ở khu dân cư thông qua dây dẫn kim loại.

Truyền thanh tăng âm được sử dụng hiệu quả ở các trụ sở thôn, khu phố hoặc những vùng lõm do đồi núi cao che chắn sóng phát thanh FM không vươn tới được. Truyền thanh tăng âm (truyền thanh hữu tuyến) có ưu điểm không gây ảnh hưởng và cũng không bị ảnh hưởng của các hệ thống thu phát sóng sóng điện từ khác. Bên cạnh đó, việc sử dụng hệ thống truyền thanh hữu tuyến cũng bộc lộ nhiều nhược điểm như: Gây mất mỹ quan đô thị do các tuyến dây dẫn kết nối giữa các thiết bị thu với máy phát trên các tuyến đường liên thôn, khu phố; âm thanh phát không đồng nhất (âm thanh phát ra ở những điểm đầu gần máy phát thì quá to gây khó chịu cho người nghe, trong khi đó âm thanh phát ra ở các điểm phát cuối thì quá nhỏ làm cho người nghe không nghe rõ tuyên truyền nội dung gì) và không đồng bộ (độ trễ và sự suy hao của của tín hiệu điện lan truyền trên dây dẫn); dễ bị chập vào hệ thống điện lưới gây cháy nổ khi có gió giật mạnh hoặc do giông sét gây ra trong mùa mưa bão.

### 1.1.2. **Phương thức truyền thanh vô tuyến( truyền thanh không dây phát sóng FM)**

Hệ thống truyền thanh không dây cho phường xã không còn xa lạ gì đối với mọi người dân. Nó là thứ rất quen thuộc với mọi người dân. Mỗi chiều tối hay sáng sớm nghe những câu nói như: “ Đây là Đài Tiếng Nói Việt Nam, phát thanh từ Hà Nội, thủ đô nước Cộng hòa xã hội chủ nghĩa Việt Nam,..“. Dưới đây là sơ đồ của hệ thống truyền thanh không dây lắp đặt cho xã phường:



Hình 1. 2:

**\* Các thiết bị chính trong hệ thống truyền thanh không dây cho phường xã:**

1. Máy phát sóng FM 50W . Với model : INT-OP-50W

2. Bộ anten phát sóng FM inox/nhôm, vô hướng, phân cực đứng. Với model :SGETFM-LB

3. Cáp dẫn sóng cao tần RG8 hoặc 1/2” gồm 2 đầu connecter. Với model :RG8 A/U

4. Cụm thu truyền thanh không dây kỹ thuật số 60W/120W. Với model: RCV60L, RCV120L,RCV60H, RCV120H

5. Loa phóng thanh Việt Nam 25W/16 Ohm vành loa nhựa với model KT-25 hoặc loa TOA 30W  với model TC-631

6. Bộ phát mã điều khiển RDS, điều khiển từ xa các đầu thu không dây FM. Với Model : CTR 08

7. Bàn trộn âm thanh (Mixer)

8. Bộ Micro thông báo để bàn

9. Đầu thu sóng FM chuyên dụng, có lập lịch hẹn giờ tự động phát đài. Với model : FM-02CD

10.Tai nghe không dây FM kiểm âm ( kiểm tra chất lượng âm thanh phát sóng).Với model: C-360

11. Ổn áp 3KVA

12. Bộ loa kèn phát thanh công suất lớn đặt tại trung tâm. Với model : LK-50KVH, LK-75KVH, LK-150KVH

13.Tăng âm truyền thanh dùng cho loa kèn. với model: PA-200, PA-400

14. Bộ máy vi tính để bàn, dùng thu và phát chương trình phát thanh.

15. Bộ lọc chống nhiễu ghép qua đường nguồn : Với model: SGET NF

16. Thiết bị cắt lọc sét lan truyền 1 pha cho đường nguồn. Với model: SGET 1P

17.Thiết bị chống sét trên đường dây feeder: Với model: KO-3GN, KO-4GN, KO-5GN, KO-6GN

18. Hệ thống tiếp đất cho phòng máy.

19. Bàn,ghế để máy ( hoặc tủ Rack 19”).

20. Trụ anten phát sóng FM cao từ 21m tới 30m.

**\* Chức năng thiết bị trong hệ thống truyền thanh không dây cho phường xã dùng sóng FM:**

**1. Máy phát sóng FM 50W**

Máy phát sóng FM là trái tim của hệ **thống phát sóng không dây phường xã dùng sóng FM** , đây là thiết bị có nhiệm vụ điều chế tín hiệu âm thanh với tín hiệu cao tần để có thể truyền đi xa. Đồng thời kết hợp cả tín hiệu điều khiển RDS thành sóng mang để điều khiển các cụm thu không dây FM.



Hình 1. 3

**2. Bộ anten phát sóng FM inox/nhôm, vô hướng, phân cực đứng.**

Đây là thiết bị bức xạ sóng cao tần ra không gian để truyền đi những nơi mong muốn.anten phát sóng FM được làm bằng chất liệu Inox hoặc nhôm định hình cao cấp nên có độ bền rất cao, không bị gỉ sét. Model thường sử dụng là ***SGETFM-LB***.



Hình 1. 4

**3. Cáp dẫn sóng cao tần RG8 A/U hoặc 1/2” gồm 2 đầu connecter.**

**Cáp dẫn sóng cao tần** thường sử dụng là RG8 hoặc cáp 1/2”,để dẫn sóng cao tần từ máy phát tới Anten bức xạ. Thông thường cáp này không nên dài quá 100 mét sẽ cho chất lượng phát sóng tốt nhất.



Hình 1. 5

**4. Cụm thu truyền thanh không dây kỹ thuật số 60W/120W .**

Đây là thiết bị đầu cuối của hệ thống, [cụm truyền thanh không dây cho phường xã FM](http://giaiphapamthanh.org/truyen-thanh-khong-day/cac-thiet-bi-trong-he-thong-truyen-thanh-khong-day-cho-phuong-xa) ( hay còn gọi là đầu thu không dây FM hoặc bộ thu không dây FM). Là thiết bị sẽ thu sóng cao tần từ đài phát tại trung tâm, sau đó giải mã tín hiệu đó thành tín hiệu âm tần và tín hiệu điều khiển RDS .Sau đó sẽ khuếch đại tín hiệu lên và phát ra loa để phục vụ nhân dân. Thường sử dụng model: **RCV60L**, **RCV120L**, **RCV60H**,  **RCV120H**



Hình 1. 6

**5. Loa phóng thanh Việt Nam 25W/16 Ohm vành loa nhựa hoặc loa TOA 30W (TC631).**

Đây là thiết bị gắn vào cụm thu FM không dây và phát ra âm thanh truyền đi xa. Ngày trước chúng ta hay dùng loa trung quốc vành nhôm hoặc loa Việt nam vành nhựa, nhưng cả 2 loại chất lượng không ổn định, độ bền thấp gây ra mất niềm tin vào chất lượng hệ thống. Hiện nay chúng tôi sử dụng loa TOA TC-631, vành bằng thép, sơn phủ chống nắng mưa rất tốt, dộ bền gấp mấy lần loa Việt Nam.



Hình 1. 7

**6. Bộ phát mã tín hiệu RDS, điều khiển từ xa các đầu thu không dây FM.**

**Bộ phát mã tín hiệu RDS** hay còn gọi là tín hiệu điều khiển, sẽ phát 1 tín hiệu điều chế chung với sóng cao tần.Sau đó tới máy thu sẽ được giải mã để điều khiển tắt mở cụm thu FM từ xa hoặc chống nhiễu khi có những tín hiệu lạ cùng tần số phát.



Hình 1. 8

**7. Bàn trộn âm thanh (Mixer)**

Đây là thiết bị có chức năng trộn và chọn các loại tín hiệu âm thanh để phát đi. Hiện nay loại này rất đa dạng và nhiều mẫu mã khác nhau, nhưng chọn loại từ 8 đường tới 12 đường đủ cho hệ thống FM này.



Hình 1. 9

**8. Bộ Micro thông báo để bàn**

Micro để bàn bạn cũng có thể dễ dàng lựa chọn, loại có đế hoặc đế rời.Hãng thì tùy giá cả và chất lượng mà chọn như Shure hay TOA…

**9. Đầu thu sóng FM chuyên dụng, có lập lịch hẹn giờ tự động phát đài. Với model : FM-02CD**

Máy Radio thì thường chọn loại Radio SONY. Còn đầu thu sóng FM chuyên dụng thì lên dùng loại TU-6200 của Inter-M. Đây là những thiết bị tốt chuyên dùng để tiếp âm các đài truyền thanh cấp trên.



Hình 1. 10

**10. Tai nghe không dây kiểm âm ( kiểm tra chất lượng âm thanh phát sóng).**

Đây là loại tai nghe FM chuyên dụng, có thể thu bất kỳ tần số FM nào mà các đài phát. Vì vậy để kiểm tra chất lượng âm thanh của đài phát đi thì ta nên sử dụng bộ này.

**11. Ổn áp 3KVA**

Để ổn định nguồn cho các thiết bị khác hoạt động ổn định và tránh được một số tác động từ nguồn bên ngoài vào.

**12. Bộ loa phóng thanh cự ly xa (Loa kèn) đặt tại trung tâm.**

Đây là bộ loa phóng công suất lớn, đặt tại trụ trung tâm, có thể phát rất xa . Đem lại hiệu quả cao trong việc tuyên truyền ngay tại Ủy Ban Xã Phường.



Hình 1. 11

**13. Tăng âm truyền thanh dùng cho loa kèn.**

Là bộ tăng âm để phát cho 3 hoặc 4 loa kèn tại trung tâm. Với các model : ***PA-200, PA-400, PA-600…***

**14. Bộ máy vi tính để bàn, dùng thu và phát chương trình phát thanh.**

Để thu chương trình phát thanh, biên tập, phát các chương trình phát thanh FM.Thiết bị này rất thuận tiện cho việc phát đi phát lại các chương trình phát thanh, thuận tiện cho người sử dụng .

**15. Bộ lọc chống nhiễu ghép qua đường nguồn**

Thiết bị này để gắn vào các thiết bị như Radio, máy vi tính…để giảm nhiễu cho các thiết bị.Model thường dùng **SGET NF**.

**16. Hộp điện cắt sét lan truyền 1 pha cho đường nguồn.**

Đây là thiết bị cắt sét lan truyền cho đường nguồn tới các thiết bị. Linh kiện lắp ráp chính hãng Thái Lan do công ty SGET lắp ráp. Model thường sử dụng  **SGET 1P.**

**17. Thiết bị chống sét trên đường dây feeder**

Đây là thiết bị cắt lọc sét trên đường cáp dẫn sóng từ máy phát sóng FM tới Anten phát sóng.Đây cũng là thiết bị rất quan trọng vì Anten rất hay hút sét, máy phát lại có giá trị lớn nên cần được bảo vệ.

**18. Hệ thống tiếp đất cho phòng máy.**

Đây là hệ thống tiếp đất chống giật cho phòng máy, vừa có chức năng thoát sét, thoát nhiễu, chống giật do nguồn gây ra. Thông thường sử dụng 3 tới 5 cọc mạ đồng 2,4m chôn dưới đất sau đó kết nối những cọc này lại với nhau.

**19.Bàn, ghế để máy ( hoặc tủ Rack 19”).**

Đây là phụ kiện để thiết bị cho gọn gàng, sạch sẽ và cũng là nơi làm việc cho kỹ thuật.

**20. Trụ Anten tam giác cao từ 21m tới 30m.**

Đây là trụ trung tâm cho việc phát sóng và phát thanh của truyền thanh không dây cho phường xã, là nơi gắn Anten phát sóng và Loa phóng thanh công suất lớn.Trụ thường cao từ 21 mét tới 30 mét tùy địa hình.Là trụ tam giác dây néo ( giá cả thấp nhưng tốn diện tích đất nhiều) hoặc trụ tự đứng ( không tốn diện tích đất nhưng giá thành cao).

**1.1.3. Nhược điểm của các phương thức cũ**

* **Với hệ thống truyền thanh có dây cũ:**
* Hệ thống truyền thanh có dây bằng dây đồng và tăng âm [(***Amply- tăng âm truyền thanh***)](http://viethungaudio.vn/tang-am-truyen-thanh.htm) đã được xây dựng và tồn tại ở Việt Nam trên 30 năm qua, công nghệ thiết bị lạc hậu, chất lượng âm thanh kém và không đồng đều trên toàn tuyến.
* Truyền thanh có dây thường xảy ra sự cố đường dây trong mùa mưa bão. Việc bảo trì sửa chữa đường dây rất vất vả và nguy hiểm do sét đánh, chập điện lưới vào dây truyền thanh …
* Khi triển khai hệ thống truyền thanh có dây ở vùng sâu, vùng xa có nhiều đồi núi hoặc sông rạch thì việc trồng cột trụ và kéo dây sẽ rất gian nan và tốn kém.
* **Với các hệ thống truyền thanh không dây thế hệ cũ:**
* Hệ thống không dây công nghệ cũ phát sóng ở băng tần FM (87.5108MHz), tuy khắc phục được 3 nhược điểm của mạng có dây, nhưng lại phát sinh 3 nhược điểm mới.
* Các cụm [loa truyền thanh](http://viethungaudio.vn/loa-truyen-thanh.htm) không dây công nghệ cũ rất dễ bị nhiễu sóng lạ, phát tiếng ồn vào ban đêm, gây phiền hà cho người dân.
* Việc tiếp tục sử dụng băng tần FM (87.5108MHz) cho truyền thanh cơ sở là đi ngược lại với lộ trình phát triển toàn cầu và vi phạm các luật lệ Quốc tế về viễn thông và phát thanh truyền hình (ITU-T và ITU-R). Hiện nay thế giới, các nước chỉ sử dụng băng tần FM này cho phát thanh cấp tỉnh và huyện thị … không sử dụng nó cho truyền thanh cấp xã phường. Do vậy khi gia nhập WTO, hoạt động của các hệ thống truyền thanh không dây công nghệ cũ (FM 87,5-108 MHz) sẽ  bị đình chỉ là điều tất yếu.
* Do sử dụng tần số không phù hợp, cho nên khi thiết kế chọn tần số FM để phân chia cho mỗi Xã (phường) là điều rất nan giải! Phải làm sao để tần số của một xã A không trùng với tần số các xã khác trong Huyện và các xã của Huyện lân cận, không trùng tần số với các Đài Huyện, Đài Tỉnh của chính nó và vùng lân cận …. Khó khăn nhất là hiện tượng sóng đài FM của Xã sẽ gây nhiễu sóng truyền hình và xóa sóng FM của Đài Huyện, gây cản trở cho việc tiếp sóng chương trình Đài Huyện. Tình trạng này làm giảm hiệu quả của Hệ thống truyền thanh 3 cấp dẫn đến khó đồng bộ.

***Hệ thống chưa đảm bảo chất lượng***

Như đã nói ở trên, do có quá nhiều nhà cung cấp và vấn để hợp chuẩn chưa được quan tâm dẫn đến rất nhiều hạng mục chưa đảm bảo chất lượng:

- Máy phát kém chất lượng, hãng sản xuất không uy tín

- Cụm thu FM độ nhạy thấp, kém ổn đinh, thiếu mỹ quan

- Loa truyền thanh chất lượng kém, gây phản ứng tiêu cực cho người nghe

- Vị trí treo loa, cụm thu, cột loa thường là tận dụng cột điện, cột tre, gây lộn xộn, rất thiếu thẩm mỹ và mất an toàn. Đây là vấn đề gần đây được báo chí quan tâm với cụm từ “Loa phường”.

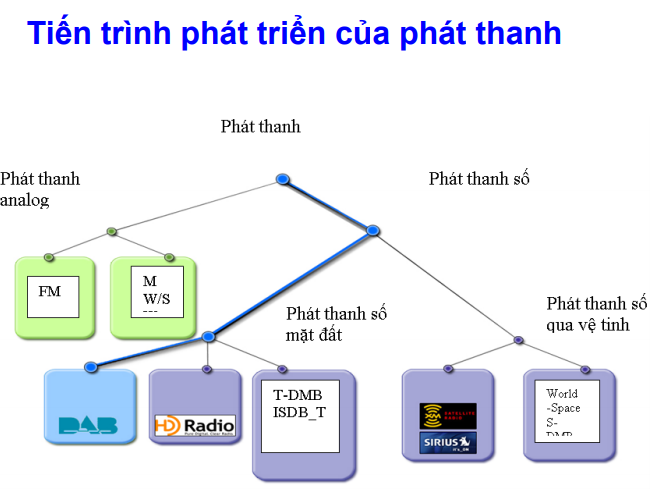
***Hệ thống thiếu an toàn, tin cậy***

Khác với hệ thống truyền thanh có dây, hệ thống truyền thanh không dây FM có ưu điểm trong việc triển khai, không phụ thuộc nhiều vào địa hình, dễ dàng bổ sung thêm điểm thu đầu cuối, không làm ảnh hưởng đến công suất máy phát tại trung tâm. Tuy nhiên, do đặc thù công nghệ là dùng sóng vô tuyến, nên độ ổn định, tin cậy phụ thuộc nhiều vào chất lượng của máy phát và ăn-ten đặt tại trung tâm. Trong bối cảnh các máy phát không được chuẩn hóa, chất lượng của các nhà cung cấp nội địa cũng rất khác nhau, làm ảnh hưởng chung đến chất lượng của toàn mạng lưới. Mặt khác, vì là sóng vô tuyến nên vấn đề bảo mật đường truyền là cần thiết, tránh tình trạng thu sóng ngoài ý muốn hoặc thu sóng của đài phát nước ngoài có mục đích xấu. Trên thực tế, vấn đề bảo mật đường truyền của các nhà cung cấp nói chung là rất sơ sài, thậm chí là không dùng bất kể phương thức bảomật nào.

Yếu điểm về tính an toàn, độ tin cậy thể hiện rất rõ tại các tỉnh Tây Nguyên nói chung, Đắk lắk nói riêng, luôn là điểm nóng về an ninh, quốc phòng trong những năm gần đây. Việc các đài phát thanh bị tấn công dẫn đến phát những bản tin tuyên truyền tiếng nước ngoài, hay chống phá nhà nước vẫn còn xảy ra.

**1.2. Nghiên cứu, tìm hiểu một số hệ thống truyền thanh tiên tiến trên thế giới hiện nay Khánh D15**

Tại những nước trên thế giới như Mỹ hay trong khu vực như Đài Loan, Hàn Quốc, Trung Quốc... hay như những quốc gia lớn tại châu Âu, hệ thống truyền thanh vẫn được duy trì và phát triển, tùy vào đặc thù và cách thức khác nhau của từng nước.



Hình 1. 12

**Tại Hoa Kỳ :**

Vào ngày 7 tháng 11 năm 1994, WXYC (89.3 FM Chapel Hill, North Carolina , USA) đã trở thành đài phát thanh truyền thống đầu tiên thông báo phát sóng trên Internet. WXYC đã sử dụng đài FM kết nối với hệ thống tại SunSite, sau này được gọi là Ibiblio , chạy phần mềm CU-SeeMe của Cornell . WXYC đã bắt đầu thử nghiệm phát sóng và thử nghiệm băng thông vào đầu tháng 8 năm 1994. WREK (91.1 FM, Atlanta , GA USA) bắt đầu truyền phát cùng ngày bằng phần mềm tùy chỉnh của riêng họ có tên CyberRadio1. Tuy nhiên, không giống như WXYC, đây là phiên bản beta ra mắt của WREK và luồng không được quảng cáo cho đến một ngày sau đó.

**Tại Vương quốc Anh :**

Tại Vương quốc Anh, BBC bắt đầu phát sóng FM vào năm 1955, với ba mạng lưới quốc gia sử dụng băng tần 88.0–94.6 MHz. Băng tần 94.6–97.6 MHz sau đó được sử dụng cho BBC và các dịch vụ thương mại địa phương. Tuy nhiên, chỉ khi phát sóng thương mại đã được giới thiệu đến Anh vào năm 1973 FM mới được trở nên phổ biến tại Anh. Với sự phổ biến của cộng đồng người dùng (đặc biệt là các dịch vụ công cộng như cảnh sát, cứu hoả và cấp cứu) và việc mở rộng băng tần FM lên 108.0 MHz trong giai đoạn 1980 và 1995, FM đã mở rộng nhanh chóng khắp các đảo Anh. Trong năm 2010, khoảng 450 giấy phép như vậy đã được ban hành.

**Tại Italya :**

Ý đã thông qua phát sóng FM rộng rãi vào đầu những năm 1970, nhưng các thí nghiệm đầu tiên được thực hiện bởi RAI từ năm 1950, khi "phong trào phát thanh miễn phí" nở rộ, buộc phải công nhận quyền tự do ngôn luận thông qua việc sử dụng "phương tiện vô tuyến miễn phí như máy phát sóng". Tòa án cuối cùng đã quyết định ủng hộ Đài phát thanh miễn phí. Chỉ vài tuần sau khi quyết định cuối cùng của tòa án có một "bùng nổ radio FM" liên quan đến các đài phát thanh riêng nhỏ trên toàn quốc. Vào giữa những năm 1970, mỗi thành phố ở Ý đều có một đài phát thanh FM đông đúc. Hiện nay FM vẫn đang được sử dụng rộng rãi.

**Tại Đức:**

Ở Đức có hơn 65 triệu người sử dụng Internet, 16% trong số họ nghe radio trên Internet (6% mỗi tháng một lần,10% ít hơn). Cơ sở hạ tầng tiên tiến và gia tăng dân số tiềm năng làm cho Đức một thị trường hấp dẫn đối với sự phát triển của Internet Radio. Điều này cũng đúng đối với các đài truyền hình của đài phát thanh truyền thống. Trang web Radiophony có một cơ hội để ảnh hưởng đến Áo và phần nói tiếng Đức của Thụy Sĩ. Các đài phát thanh ở Đức một mình có cơ hội để đạt được nhiều triệu người sử dụng Internet. Các phần lớn của thị trường vẫn là với các đài truyền hình phát thanh truyền thống. Một ví dụ về một đài phát thanh lớn mà truyền chỉ trên Internet là RadioMelodie.net. Nó được thành lập vào năm 2002 và được phát sóng từ 20 địa điểm bao gồm Tây Ban Nha, Mỹ và Đức. Những người nhận của đài phát thanh này chủ yếu là người Đức (80%), cũng như các công dân của Áo, Thụy Sĩ và Hoa Kỳ. Nó là một đài phát thanh khá thú vị, bởi vì ngoài việc nghe nhạc,nó cũng cung cấp các cuộc phỏng vấn với những người nổi tiếng và các chương trình gốc- như radio truyền thống. Tại Đức hơn 200 đài phát thanh Internet là chi nhánh tại Radio-ring.Nó là một tổ chức mà chủ yếu cung cấp một diễn đàn để trao đổi kinh nghiệm giữa các đài truyền hình. Ngoài ra,nó đại diện cho quyền lợi của các thành viên và các tổ chức công cộng khác.

**Tại Ba Lan:**

Tại Ba Lan, khoảng 50% hộ gia đình có truy cập Internet băng thông rộng, trong khi vào năm 2009 30% có Internet, và trung bình của EU là 56%.Tốc độ tăng trưởng nhanh có thể vượt qua mức trung bình này trong năm 2011. Nên Radio Internet được phát triển. Năm 2008 Ba Lan đã được xếp hạng thứ 20 trong số các nước Liên minh châu Âu về số lượng người dùng với quyền truy cập vào Internet băng thông rộng. Thực tế là, theo một nghiên cứu được tiến hành bởi Văn phòng Truyền thông điện tử (UKE),chỉ một phần năm số người dùng Internet sử dụng truy cập di động vào Internet cũng đáng được chú ý. Mặc dù các dữ liệu không phải là rất thuận lợi,nhiều chuyên gia cho rằng Ba Lan có tiềm năng lớn trong việc tiếp cận thị trường. Một yếu tố đó là lợi ích của một số lượng lớn các công dân của đất nước, hoặc với gốc Ba Lan,sống và làm việc ở nước ngoài (12-15 triệu). Do vậy, mặc dù cơ sở hạ tầng Ba Lan thích hợp cho các đài phát thanh Internet, nó có một cơ hội tuyệt vời để đạt được cộng đồng Ba Lan. Nó cũng quan trọng là người dân Ba Lan cư trú ở các nước phát triển chủ yếu, chẳng hạn như Canada,Hoa Kỳ và Úc. Hầu hết các đài truyền hình truyền thống ở Ba Lan phát sóng các chương trình của họ thông qua Internet. Ví dụ về các đài truyền hình như vậy là RMF FM, Đài phát thanh Zet và đài phát thanh Ba Lan. Các đài phát thanh FM RMF, mà đã không hơn hai năm trước, có khán giả lớn nhất và thiết lập một cổng web tại địa chỉ miastomuzyki.pl. Một số đài phát thanh Internet cũng có sẵn thông qua cổng thông tin này, ngoài các trạm phát sóng truyền thống.RMF FM đã phát sóng qua mạng kể từ 1996. Điều này là do phương tiện truyền thông như đài truyền hình Internet có khả năng tiếp cận với những sinh viên nước ngoài và vượt ra ngoài tầm với của sóng radio.

Ngoài FM, hiện nay, một trong những công nghệ tiên tiến nhất đang được phát triển và triển khai rộng rãi là “phát sóng âm thanh kỹ thuật số” (DAB). Đây là một tiêu chuẩn vô tuyến kỹ thuật số để phát sóng các dịch vụ vô tuyến âm thanh kỹ thuật số, được sử dụng ở các quốc gia trên khắp Châu Âu, Trung Đông và Châu Á Thái Bình Dương. Tiêu chuẩn DAB được khởi xướng như một dự án nghiên cứu châu Âu vào những năm 1980. Công nghệ này đã có mặt ở nhiều quốc gia kể từ cuối những năm 1990. DAB hiệu quả hơn trong việc sử dụng phổ tần hơn so với đài FM hay AM, và do đó có thể cung cấp nhiều dịch vụ vô tuyến hơn cho cùng băng thông đã cho. DAB mạnh mẽ hơn đối với nhiễu để nghe di động, mặc dù chất lượng tiếp nhận DAB giảm nhanh khi cường độ tín hiệu giảm xuống dưới ngưỡng quan trọng, trong khi chất lượng tiếp nhận FM giảm chậm với tín hiệu giảm, cung cấp độ che phủ hiệu quả diện tích lớn hơn.

Khái niệm radio số không còn bị bó hẹp trong khuôn khổ của chiếc radio thu sóng vô tuyến dạng số nữa, mà ngày nay đã được đưa vào rất nhiều công nghệ truyền dẫn, phổ biến nhất là truyền dẫn trên nền tảng Internet.

Công nghệ radio số mới (truyền phát qua Internet) cho phép tương tác hai chiều giữa trung tâm và các thiết bị đầu cuối, chính điều này đã cho phép một hệ thống radio công nghệ số dễ dàng trở thành một hệ thống âm thanh thông báo trên diện rộng và cũng có thể thông báo trong phạm vi nhỏ, tùy theo lựa chọn từ trung tâm. Không những thế, tại mỗi điểm đầu cuối cũng có thể trở thành điểm thu thập thông tin và yêu cầu hỗ trợ từ phía người dân thông qua hệ thống camera gắn tại mỗi điểm đầu cuối. Hệ thống này cho phép gửi thông tin một cách đồng bộ đến tất cả các điểm đầu cuối trong những trường hợp thiên tai, địch họa hay trong tình huống khẩn cấp khác. Hệ thống này là một phần trong một thế giới hiện đại, nó tích hợp với các hệ thống khác như an ninh, cứu hỏa, cứu thương... Nó tương tác một cách tự động và linh hoạt trong những tình hống các hệ thống khác. Ví dụ, trong tình huống báo cháy từ một khu chung cư tại Đài Loan, người dân yêu cầu hỗ trợ từ trung tâm cứu nạn, từ trung tâm này họ kích hoạt hệ thống âm thanh thông báo tại khu nhà để cảnh báo người dân toàn khu vực lân cận, đồng thời các loa thông báo trên toàn tuyến đường di chuyển của xe cứu nạn và cứu hỏa đều phát đi bản tin yêu cầu nhường đường tạo điều kiện cho xe ưu tiên. Hay một ví dụ khác tại Hàn Quốc, một trụ gắn thiết bị đầu cuối radio số, cho phép phát đi thông báo khẩn dành cho người dân địa phương, cũng cho phép phát đi bản tin giới thiệu du lịch một cách ngắn gọn. Không những thế, nếu một người dân cần được trợ giúp y tế hay hỗ trợ an ninh, có thể bấm vào nút KHẨN CẤP đặt tại chân trụ điện để liên lạc với trung tâm thông tin.

Qua khảo sát tại một số nước, hệ thống radio hầu hết đã được nâng cấp thành hệ thống số, hàm chứa nhiều công nghệ, làm thay đổi hoàn toàn cách nhìn về một hệ thống radio truyền thống. Cũng trong khảo sát này, mục đích chủ yếu của hệ thống là âm thanh thông báo, cảnh báo và phục vụ cứu hộ cứu nạn.

Trong quá trình xây dựng hệ thống truyền thanh số, một trong những yêu cầu quan trọng bậc nhất là bảo mật trên hệ thống. Các phương pháp đã được nghiên cứu, triển khai là sử dụng Radio Data System (RDS) và One Time Password (OTP) (sẽ được trình bày ở phần sau).

**1.3. Nghiên cứu lí thuyết về truyền thanh radio số trong hệ thống truyền thanh không dây đồng nhất 3 cấp Khánh D15**

### 1. 3.1. Điều kiện tiên quyết kỹ thuật để Internet Radio

Sự phát triển của Internet radio sẽ không thể thực hiện được nếu không có sự phát triển của Internet. Truy cập Internet rất quan trọng, bởi vì nó đòi hỏi một đài phát thanh có khả năng giao tiếp với một mạng lưới toàn cầu. Hiện nay, các thiết bị sử dụng phổ biến nhất chủ yếu là máy tính, cả hai máy tính để bàn và điện thoại di động (máy tính xách tay và máy tính xách tay). Chúng ta không thể quên về điện thoại di động, đặc biệt là cái gọi là điện thoại thông minh, và PDA,cũng như một số các nhạc MP3 và MP4 cao cấp hơn players MP3MP4. Ví dụ nổi tiếng nhất của loại thiết bị này là một loạt iPod do Apple. Trong năm 2010 và 2011 viên đã trở thành xu hướng mới trong việc phát triển khả năng kết nối Internet. Mục đích chính của việc sử dụng thuốc viên là cung cấp cho người dùng truy cập vào một loạt các nội dung thông tin, đặc biệt là thông qua các mạng truyền thông toàn cầu. Kết nối Internet tương tự có thể được thực hiện cả trong cách truyền thống –cho ví dụ - thông qua cáp kết nối được đến thiết bị- thông qua việc sử dụng công nghệ không dây. Ví dụ về các công nghệ như là sóng radio, chẳng hạn như Wi-Fi, lò vi sóng, như WiMAX, và tín hiệu vệ tinh hoặc cơ sở hạ tầng điện thoại di động, cho phép chuyển nhượng một vài Megabit mỗi giây qua HSPA. Sự phát triển của Internet là cần thiết nhưng chưa đủ cho Internet Radio.Sự xuất hiện của Internet radio sẽ không thể thực hiện được mà không phát triển đáng kể của công nghệ để chuyển âm thanh trong một dòng suối trong thời gian thực trên một khoảng cách dài. Với mục đích này cần phải có kết nối Internet với băng thông cao, cái gọi là băng thông rộng, cái gọi là băng thông rộng. định nghĩa rõ ràng thông số kỹ thuật cho phép sử dụng một kết nối Internet băng thông rộng nhanh là vô cùng khó khăn vì những thay đổi rất nhanh chóng trong lĩnh vực này.

Tầm quan trọng của quyền truy cập vào thông số kỹ thuật cụ thể của phương tiện này không thể được phóng đại. Điều này là do chủ yếu để chi phí gửi văn bản. Đặc biệt trong trường hợp đa phương tiện, đòi hỏi kết nối Internet tốc độ cao, chi phí đang tăng lên tương ứng với số lượng người dùng quan tâm đến phương tiện truyền thông nhất định. May mắn thay, sự cạnh tranh ngày càng tăng trên thị trường ISP được kết quả là giá dần dần thấp hơn kết hợp với chi phí vận hành thấp hơn cho mỗi đài truyền hình Internet. Công nghệ tiến bộ kỹ thuật trong việc truyền tải hiệu quả của âm thanh cũng là một yếu tố quan trọng. Trong số những thứ khác, có những phương pháp mới và hiệu quả hơn của nén dữ liệu. Với nén hiệu quả,dữ liệu nhỏ hơn các gói dữ liệu cần phải được truyền đi. Do đó cần ít băng thông để gửi cùng một lượng dữ liệu. Hiệu quả của sự ra đời của nén dữ liệu là sự phát triển của trực tuyến, công nghệ mà cho phép bạn chơi âm thanh và video trong luồng. Tuy nhiên, không có các gói dữ liệu Internet,mà có thể lấy thông tin được truyền tới máy tính trong thời gian thực. Đây không phải là có thể cho đến khi sự ra đời của tiến bộ kỹ thuật cho phép truyền phát trực tiếp qua Internet. Nếu không có việc sử dụng các công nghệ này, Internet radio sẽ không thực hiện được.

Phổ biến của công nghệ streaming có thể được thực hiện bởi phần mềm độc quyền để truyền và nhận sóng vô tuyến sử dụng công nghệ streaming. Việc đầu tiên của các chương trình này đã được trình bày vào tháng Tư năm 1996 khi Công ty Real Networks,tác giả của phần mềm Real Player nổi tiếng và codec đặc trưng bởi tỷ lệ nén tốt. Kết quả là các định dạng phương tiện truyền thông trực tuyến cạnh tranh đã được giới thiệu bởi những người khổng lồ CNTT lớn.Microsoft đã phát triển định dạng file WMA (Windows Media Audio) và Windows Media Player. Apple Computer đã chứng minh media player của nó và codec trong một loạt các Quick Time. Một công nghệ.SHOUTcast được phát triển như một phương pháp cho phép truyền phát các file nhạc ở định dạng MP3. Công nghệ sử dụng để phát sóng radio trên Internet được gọi là podcasting. Nó sử dụng một sự kết hợp của các yếu tố cụ thể để phát thanh Internet với các phương pháp khác nhau thu thập dữ liệu. Podcasting cho phép tự động lựa chọn và tải các chương trình này, có thể được chơi trong tương lai, ví dụ,trên một thiết bị đa phương tiện cầm tay. Một tính năng quan trọng là phương pháp này cho phép bạn bỏ qua các chương trình phân phối máy tính cá nhân như một máy thu, cho phép người dùng tận hưởng sự nhanh nhẹn của họ. Phát triển của Internet radio buộc việc chuyển đổi thị trường nghe nhìn. Nó dẫn đến các thiết bị đặc biệt mà làm cho nó có thể để nghe đài phát thanh Internet mà không cần sử dụng máy tính. Họ thường sử dụng Wi Fi.

### 1.3.2. Sự khác biệt giữa Radio Internet và Radio cổ điển

Sự khác biệt giữa các đài phát thanh cổ điển và đài phát thanh Internet không phải là duy nhất trong công nghệ. Phát sóng trên Internet ở hầu hết các nước trên thế giới, cũng như tại Việt Nam, không được điều chỉnh bởi pháp luật. Trước hết, không có cần phải xin giấy phép như trong trường hợp của đài phát thanh truyền thống. Điều này là do không có nhu cầu về phân bổ tần số. Internet là một phương tiện để chung tất cả, và tất cả mọi người trên thế giới có thể sử dụng nó. Một vấn đề tương tự là quy định nội dung chương trình.Ví dụ, không có giới hạn về độ dài của quảng cáo ban nhạc. Trong trường hợp của đài phát thanh Internet, các mặt hàng này chỉ đơn giản là ra khỏi phạm vi quyền hạn pháp lý. Trong đa số trường hợp, những quy định này phải tự chịu trách nhiệm của người gửi.

Internet đã làm cho đài phát thanh vừa e phù hợp với cấu trúc toàn cầu.Waldemar Dubaniowski tại hội thảo "Dịch vụ nghe nhìn trên Internet và bản quyền bảo vệ trong môi trường kỹ thuật số " lưu ý rằng sự phát triển hiện đại của phương tiện truyền thông như phát thanh truyền hình đã chọn một hướng đi khác nhau. Hơn thế nữa,trong trường hợp của đài phát thanh Internet đã có một sự gia tăng đột ngột trong chi phí phát triển. Radio Internet là rất nhỏ so với các Radio cổ điển.

Radio Internet nghiệp dư không tốn kém có thể bắt đầu hoạt động quảng bá. Có rất nhiều đài phát thanh mà ban đầu được coi như là một sở thích và cuối cùng trở thành trạm thịnh vượng. Vì độc lập và tính chất đặc biệt, phát thanh truyền hình Internet có thể được nhắm mục tiêu rất hạn hẹp cho các nhóm rất cụ thể, ví dụ, sinh viên của nhạc phim, các bài hát tôn giáo,tồi tàn, vv Bằng cách này, ngày càng có nhiều đài phát thanh Internet được lấp đầy khoảng trống đã tồn tại nhiều năm trong phát thanh truyền hình truyền thống. Chúng tương ứng với các yêu cầu và nhu cầu của khán giả mà các đài phát thanh truyền thống, vì nhiều lý do, sẽ không bao giờ có thể cung cấp cụ thể.

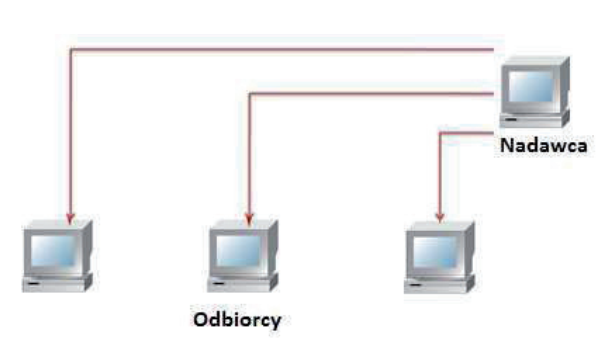
Tóm lại, các Radio truyền thống có một phạm vi rộng lớn, chất lượng âm thanh tốt, nhưng thiếu một con đường trở lại thuận tiện cho công nghệ thử nghiệm và chứng minh và các chi phí liên quan đến biên nhận. Bên cạnh đó, chúng được quy định . Chúng được yêu cầu phải có giấy phép được cấp bởi cơ quan có thẩm quyền. Mặt khác, phát thanh truyền hình Internet có thể được mô tả như một hình thức giao tiếp với phạm vi không giới hạn (vì nó có thể được chọn từ bất cứ nơi nào trên thế giới), và một kênh trở lại đó là tương tác với người nghe. Tuy nhiên, nó vẫn còn trong một giai đoạn phát triển và tăng trưởng và đòi hỏi phải thu đắt hơn.Bên cạnh đó, phát sóng Internet không phải là quy định đối tượng và không đòi hỏi một giấy phép như một trạm phát thanh.

### 1.3.3. Khía cạnh kỹ thuật của Radio Internet

Radio Internet không chỉ là một danh sách nhạc. Để hoạt động Internet radio nó làm cho cảm giác cũng trở thành một trang web với các diễn đàn và chat. Truyền thống trực tuyến cũng nên được kết nối với podcasting cho phép người dùng nghe radio ra khỏi máy tính. Đây là một điều đáng suy nghĩ, bởi vì tại thời điểm này chỉ có đài phát thanh thương mại lớn cung cấp chức năng này. Internet radio sẽ đòi hỏi một lưu trữ thương mại tốt cho streaming. Các nhà cung cấp dịch vụ đó phổ biến nhất bao gồm inten.pl và hostcast.net.

### 1.3.4. Công nghệ truyền dẫn

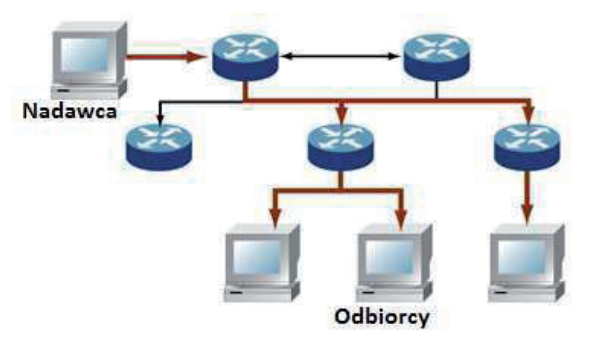
**a) UNICAST**

****

Hình 1. 13

UNICAST là một loại truyền dữ liệu trong đó các gói dữ liệu điểm duy nhất được gửi trực tiếp đến một điểm duy nhất. chính xác đó là một trong những người gửi và một máy thu**.** Card mạng Ethernet được thực hiện một cách chính xác cho loại truyền tải này. Nó được dựa trên các giao thức: TCP, HTTP, SMTP, FTP, ARP. Unicast đòi hỏi một kết nối riêng biệt từ máy chủ đến mọi khách hàng. Điều này có thể rất nhanh chóng tiêu thụ hầu hết băng thông rộng, nếu dữ liệu được gửi tới nhiều người cùng một lúc. Do đó, Ethernet được sử dụng chủ yếu cho việc xây dựng mạng lưới khu vực địa phương.

**b) MULTICAST**



Hình 1. 14

Multicast là một cách để phân phối thông tin, nơi số người nhận thông tin này được giả định là ngẫu nhiên. Người nhận được chia thành các nhóm riêng biệt mà sau này được phát hành theo một địa chỉ IP duy nhất, một nhóm multicast. Đối với truyền dẫn đến n thính giả trong mạng truyền dữ liệu đến một nút một lần trong phương pháp UNICAST n lần đến n khách hàng. Nói cách khác, sử dụng nhiều luồng MULTICAST, gửi cùng một thông điệp được tránh. Nó cung cấp các khoản tiết kiệm lớn nhất trên băng thông,đặc biệt là nơi các phần của dữ liệu là tuyệt vời.

*Công nghệ MULTICAST phụ thuộc vào một số giao thức mạng:*

* IGMP **-** Internet Group Management Protocol,
* MLD - Multicast Listener Discovery
* PIM-SM - Protocol Independent Multicast - Sparse Mode
* PIM-DM - Protocol Independent Multicast - Dense Mode
* MRD - Multicast Router Discovery.

MULTICAST có thể được định nghĩa theo cách khác nhau: như một cách để cung cấp dữ liệu đến hết trạm đóng vai trò như một splitter. Một máy chủ duy nhất đóng vai trò như một máy phát gửi tín hiệu đến các máy chủ khác như người nhận. Điều này có thể được hình như một hoặc một đến nhiều như Source Specific Multicast (SSM) mô hình. Mô hình truyền khác, Any Source Multicast (ASM) , cũng tương tự như một nhiều-nhiều nơi nhiều đài truyền hình truyền host-to-host với nhiều người nhận. Mô hình SSM có liên quan chặt chẽ với các đài truyền hình các ứng dụng, trong đó chủ yếu bao gồm phát sóng đài phát thanh truyền hình ,nơi nó xuất phát từ các máy phát tín hiệu cá nhân triệu đăng ký nhận. ASM, đến lượt nó, đề cập đến ví dụ tốt nhất của dòng trên hoặc hội nghị qua điện thoại hoặc hội nghị video. Trong quá trình truyền bởi unicast, mỗi bên phải được gán một địa chỉ IP cụ thể. Trong trường hợp của multicast, một hạn chế như không tồn tại, bởi vì việc truyền dữ liệu trực tiếp tới toàn bộ nhóm các địa chỉ trong nhóm D, đó là 224.0.0 phạm vi.0 - 239.255.555.255. Lưu ý, tuy nhiên, giống như multicasting, mỗi công nghệ đều có những ưu nhược điểm của nó. Đây chắc chắn là vấn đề kỹ thuật đầu tiên với phần cứng mạng mà chỉ đơn giản là không hỗ trợ IP chung giải quyết trong lớp D. Do đó, tại thời điểm multicasting có thể được sử dụng trong mạng cục bộ. Hy vọng cho sự thay đổi triệt để trong tình trạng này là sự thay thế sắp tới của IPv4 sang IPv6, trong đó có hỗ trợ đầy đủ cho MULTICAST.

Tại thời điểm này, các giải pháp được áp dụng trên toàn cầu kết hợp unicast hỗn hợp và multicast. Các dòng được gửi từ máy chủ kết hợp 1-1, thường tạo đường hầm đến hub mạng nội bộ, có vai trò có thể thực hiện như một máy tính khác hoặc router,nơi suối được gửi đến các máy tính trên một mạng lưới khép kín sử dụng multicast. Theo cách như vậy, các mạng ảo trên Internet, gọi Mbone104 (Multicast xương - Bus multicast), đó là bằng cách sử dụng các kết nối đường hầm để việc truyền tải toàn cầu, cho phép kết hợp cả hai phương pháp truyền.

### 1.3.5. Công nghệ SHOUTCAST

Hệ thống SHOUTcast là tên đề cập gần đây, được phát triển bởi Nullsoft (công ty đã tạo ra WinAmp, trong số những phần mềm khác),và được sử dụng cho việc truyền âm thanh hoặc hình ảnh trong hình thức của một dòng dữ liệu,sử dụng giao thức HTTP. Hệ thống này được phát triển cho các ứng dụng như Winamp.

*1) Hệ thống SHOUTcast chứa hai mô-đun:*

* SHOUTcast DSP, module nguồn, được sử dụng để truyền tải các luồng dữ liệu nguồn trực tiếp từ các ứng dụng, tái tạo các mô-đun phân phối.Phiên bản chính thức của các mô-đun chỉ có sẵn cho người dùng dưới dạng plug-in cho Winamp. Ngoài ra còn có phần mềm để người chơi khác, hoặc các ứng dụng playback riêng biệt được tạo ra bởi các bên thứ ba.

*2) SHOUTcast DNAS (Distributed Mạng âm thanh gọi là Server) là một mô-đun phân phối, nơi máy chủ sẽ gửi một dòng cho khách hàng,mà có thể hoạt động ở hai chế độ:*

* Radio - dòng nhận được từ các mô-đun mã nguồn sẽ được chuyển cho các khách hàng đang kết nối với DNAS.Bằng cách, âm thanh và hình ảnh đầu ra này từ ứng dụng mã nguồn module, hỗ trợ ví dụ bằng cách DJ, đạt đến khán giả.Nó đã được thực hiện trong đơn trình bày trong bài báo này.
* Theo yêu cầu (DNAS) - sau khi yêu cầu khách hàng được phát sóng dòng, được lựa chọn trước đây bởi các tập tin âm thanh thu, hoặc video được lưu trữ trên máy chủ DNAS đĩa.

Truyền phát có thể hoạt động trong trường hợp này, thông qua các hoạt động của giao thức HTTP. máy chủ DNAS sử dụng cổng 8000 theo mặc định.Phân phối dựa trên âm thanh Mpeg 1 lớp 3,thường được gọi là MP3. Phân phối dựa trên âm thanh Mpeg 1 lớp 3, thường được gọi dưới dạng MP3. Nó là sự kết hợp của media player MP3, Winamp mà được quyết định bởi sự thành công trên thị trường của cả hai sản phẩm. Mã hóa MP3 một cuộc cách mạng trên thị trường và làm cho nó có thể để thuận tiện chuyển các tập tin âm thanh. Quan trọng hơn SHOUTcast là hoàn toàn phần mềm miễn phí có sẵn cho hầu như bất kỳ nền tảng phần cứng, và bản thân công nghệ rất hiệu quả và dễ sử dụng. Các nguồn âm thanh để phát có thể là một tập tin MP3 hoặc tín hiệu âm thanh đến từ dòng đầu vào, microphone,hoặc bất kỳ nguồn nào khác có hỗ trợ âm thanh trực tiếp. Phiên bản mới nhất của phần mềm cho phép bạn dễ dàng chuyển đổi giữa các thiết bị và trộn âm thanh.các đoạn audio có thể được truyền trong băng thông từ 16kbps đến 160kbps, cho phép hầu như bất kỳ người nghe để nhận được một dòng thanh chất lượng đầy đủ.

Được sử dụng trong SHOUTcast như giao thức lớp trên ISO / OSI, HTTP được sử dụng để chuyển các trang web. Các máy chủ gửi các dòng trực tiếp cho người sử dụng (người nghe) hoặc đến các máy chủ proxy đó cung cấp các chức năng tương tự như một máy chủ tổng thể đầy đủ với một mắt xích yếu để cài đặt các máy chủ nhưđóng với mạng xương sống. Một tùy chọn khác thú vị là sử dụng máy chủ proxy (SHOUTcast Rơ le Servers), cũng được truyền đi trong một dòng duy nhất.Sử dụng một máy chủ proxy giúp giảm thiểu tải trong khi cho phép truy cập Internet hiệu quả để truyền cho khán giả. Ứng dụng máy chủ được phát triển cho các hệ thống Windows, Linux dựa và Solaris. Cũng thú vị là vào thời điểm khi máy chủ đang chạy, bắt đầu gửi một stream, gửi nó vào một cơ sở dữ liệu toàn cầu của radio Internet (www.shoutcast.com) thông tin về các broadcast stream, cung cấp tên của đài phát thanh, phong cách ưa thích của âm nhạc, địa chỉ và cổng của máy chủ mà từ đó nó có thể được lấy đi,tốc độ dòng chảy, số lượng tối đa và hiện tại của người nghe,và bổ sung các thông tin khác về trạm. Server theo chu kỳ nhất định cũng gửi tin nhắn về tên ca khúc chơi MP3 hiện tại và lãi suất trên một phần của Internet radio. Tất cả các thông tin này hiện có sẵn trên máy chủ web và tự động quảng cáo trạm.

Người nghe phải có một chương trình mà đóng file MP3 với sự hỗ trợ cho các stream. Để kết nối với một máy chủ trên máy nghe nhạc MP3 của bạn, nhập địa chỉ và cổng của máy chủ HTTP. Phải mất vài giây từ thời điểm bạn nhận được một dòng cho đến khi bạn nghe thấy âm thanh. Điều này là do các yêu cầu điền vào bộ đệm trước khi phát lại, để bảo vệ chống lại cúp tạm thời, giảm tốc độ dòng chảy, vv. Hiện nay, hầu như tất cả người chơi, ngay cả những trình duyệt Web riêng của mình, có thể đọc các dòng dữ liệu âm thanh.

### 1.3.6. PODCASTING

Podcasting được xuất bản âm thanh và nội dung video qua mạng trong một loạt các tập phim với một chủ đề chung. Tên đến từ iPod - máy nghe nhạc của Apple.Tập được kèm theo một tập tin gọi là "feed" cho phép người nghe để đăng ký và tự động nhận được một loạt các tập phim mới. Về mặt kỹ thuật, đó là mô hình "host" thuê bao là điểm khác biệt podcasting từ các đỉnh núi thường lệ trong việc xuất bản web. Một số người, tuy nhiên, sử dụng thuật ngữ "podcast" liên quan đến bất kỳ phân phối âm thanh hoặc video xuất hiện trên mạng.

Tạo nội dung thú vị và có giá trị là một cách tự nhiên các lao động và nhiều tài nguyên phần hầu hết podcasting. Nó bao gồm việc lập kế hoạch, viết và ghi lại nội dung, cũng như âm thanh và chỉnh sửa video và nén tập tin.

Sản xuất đòi hỏi phải có thiết bị pha trộn và phần mềm để chỉnh sửa đoạn âm thanh video. Bên cạnh đó, một người sáng tạo podcast phải tạo một nguồn cấp dữ liệu RSS. Các feed là một file XML đơn giản có chứa tên của vị trí trong các podcast. Nó chứa các thông tin tập tin podcast, chẳng hạn như thời điểm phát hành, tiêu đề, và mô tả về từng loạt và tập. Tập tin này có thể được tạo bằng tay hoặc sử dụng các chương trình chuyên biệt. Audio / Video và RSS feed này sau đó được nạp trên máy chủ. Trong loạt podcast đầu tiên, đó là luôn luôn mở cửa cho các thuê bao mới, tác giả podcast phải thông báo cho khách hàng rằng podcast là thông qua các RSS feed. Nhiều podcast cung cấp một liên kết đến các podcast trên các blog, các trang web của họ, hoặc những nơi công cộng khác trên Internet. Người tạo podcast có thể làm phong phú nó với rất nhiều thông tin bổ sung. Một thính giả (thuê bao) để podcast có thể đăng ký với nó bằng cách sử dụng aggregator podcast cái gọi là (phần mềm để kiểm tra các podcast thực tế và nuôi chúng trong từng thời kỳ). Bước này đòi hỏi chỉ một lần - khi người nghe đã được thêm vào podcast, kết thúc của một thuê bao có thể chỉ được thực hiện thông qua các lệnh.

Khi thính giả thêm một RSS feed mới, aggregator lấy về tất cả các tập phim được liệt kê trong RSS feed hiện hành. Sau đó, đều đặn, kiểm tra aggregator các bản cập nhật và tải về tất cả các tập bổ sung sau. Học sinh(Sinh viên) có thể truy cập trực tiếp đến các podcast thông qua máy tính của họ hoặc thông qua thiết bị MP3 / video của họ. Thích sự thoải mái của các thiết bị di động, hầu hết các tập hợp sẽ tự động tải file podcast và đồng bộ hóa chúng ngay lập tức với các thiết bị.

Podcatcher (nghĩa đen: "podcast catcher") gọi podcast chương trình phần mềm máy khách sử dụng để tải về một loạt các tập tin đa phương tiện thông qua RSS hoặc XML. podcast của khách hàng được biết đến chủ yếu từ việc chuyển giao các tập tin âm nhạc (chủ yếu là MP3) trên một máy nghe di động. Các khách hàng podcast đầu tiên được thiết kế vào năm 2003.

### 1.3.7. Nén và chất lượng của chương trình

Các định dạng âm thanh phổ biến nhất là MP3, tên đầy đủ là MPEG 1/2 Audio Layer 3. Kết quả nén âm thanh của nó rất tốt , thực tế là nó là một phương pháp nén lossy, thực sự không hoàn hảo của hệ thống thính giác của con người. Tùy theo điều kiện trong thời gian nén, nó có thể mất thông tin rằng một người đàn ông sẽ không thể nghe. Nói cách khác, nó sử dụng một mô hình psychoacoustic xác định những loại thông tin âm thanh được phát hiện bởi tai con người và không. Nó cũng ngăn cách thông tin liên quan đến tai con người từ không thích hợp. Người ta cho rằng một người nghe thấy âm thanh của dải đến 20kHz. Trên thực tế, tuy nhiên, giá trị này được giảm xuống còn 16 kHz. Trong trường hợp của âm nhạc, âm thanh vượt quá con số này này là khác nhau tùy thuộc vào thính giác và khuynh hướng của con người. Nó rất có ý nghĩa đặc biệt là ở trẻ em và thanh thiếu niên, nhưng mất dần theo tuổi tác. Người đàn ông tốt nhất nghe trong dải 2-4 kHz. Nghe có vẻ ngoài phạm vi này ít nghe đến con người, vì vậy bạn có thể tiết kiệm những thái cực tần số với độ chính xác ít hơn nhiều. Trong trường hợp nén MP3 nó sử dụng hiện tượng mặt nạ. Nó được dựa trên thực tế là âm thanh mềm mại đang bị đàn áp bởi khối lượng lớn, và do đó cũng có thể được lưu trữ trong một chất lượng thấp hơn. Hiện tượng này xảy ra trong hệ thống thính giác và là sự gia tăng của tín hiệu phát hiện che giấu bởi sự hiện diện của một tín hiệu gọi masker. Bạn có thể phân biệt mặt nạ đồng thời, mà xảy ra khi masker xảy ra ngay sau hoặc trước khi tín hiệu. Những hiện tượng này có liên quan rất chặt chẽ đến sự thích nghi của hệ thống thính giác. Định dạng này được phát triển vào năm 1991 tại Viện Fraunhofer cho Integrierte Schaltungen ở Đức. Điều thú vị là tại thời điểm các codec được sử dụng bài hát Suzanne Vega mang tên "Dinner của Tom". Cô từng là nhà phát triển điều chỉnh nén để âm thanh của giọng nói con người là tốt nhất. File ở định dạng này có phần mở rộng \*.MP3.

Một phương pháp phổ biến nén lossy là Vorbis. Nó thuộc về gia đình của các codec OGG, và vì lý do này nó thường được sử dụng kết hợp với OGG container, mang tên sau đó kết hợp OGG Vorbis,Tuy nhiên, và do đó thường nó được rút ngắn xuống còn nhầm lẫn OGG. Đó là khả năng xử lý âm thanh 255- kênh 16 bit cho tần số của 6 kHz đến 48 kHz. Giấy phép của nó là trong lĩnh vực công cộng, vì vậy nó là miễn phí và phân phối theo GNU GPL. mở rộng tập tin của nó là \* .ogg hoặc \* .crew.

Các thuật toán nén tổn hao chất lượng cao hơn Vorbis đặt những con sóng âm thanh dẫn với khả năng tương thích của nó với bản gốc. Nén trong khi âm thanh không phải là 100% phản ánh hành vi không nén chất lượng cao. Kết quả phương pháp này trong một mức độ cao của nén ở mức 48 - 128kbps. Trong các thông số xác định trước, chất lượng nén của tập tin âm thanh kết quả là tốt hơn so với MP3, nhưng so sánh với AAC. Tuy nhiên, trước khi bạn sử dụng nó, bạn phải nhớ rằng trong tự nhiên,nó chỉ cho phép việc sử dụng các VBR (như bên dưới) và đó là căng thẳng hơn trong giải mã hơn MP3.

Được biết đến và thường được sử dụng như WMA (Windows Media Audio), nó được phát triển bởi Microsoft để cạnh tranh trực tiếp với MP3. Lý do thực sự để tạo của nó là tác giả của sáng chế đảm bảo rằng Microsoft không thể tham gia các định dạng MP3 sang Windows. Mặc dù tác giả của định dạng ban đầu tuyên bố rằng WMA cho kết quả tốt hơn so với nén MP3 và đĩa CD chất lượng được thực hiện bằng một tỷ lệ tương đương với 64 kbps, kiểm tra độc lập một cách nhanh chóng phủ nhận những quan điểm.

Nó chỉ ra rằng dưới tốc độ bit của 96kbps, WMA âm thanh tốt hơn so với MP3, nhưng nó là xa chất lượng CD. Trên giới hạn này của bộ codec đó cạnh tranh luôn luôn là tốt hơn.

Khi thảo luận về các codec phổ biến nhất và phương pháp nén âm thanh,nó là không thể không đề cập đến các giá trị mà xác định thông số nén. Chắc chắn, các khái niệm về một tỷ lệ bit, trong đó xác định số bit truyền trên một đơn vị thời gian,là rất quan trọng. Nó xác định có bao nhiêu bit của bộ nhớ được sử dụng để truyền tải âm thanh. Nói chung, càng có chất lượng của việc ghi chép, cao hơn tốc độ bit là.các thuật toán nén hiện đại sử dụng CBR (hằng số bitrate) và VBR (Variable). Trong trường hợp của CBR mỗi giây một dòng sử dụng chính xác cùng một lượng bộ nhớ, và trong trường hợp thứ hai, giá trị đang thay đổi.113 mảnh Sound giàu được mã hóa với tốc độ lấy mẫu cao hơn.VBR đã được phát triển bởi XING, không sử dụng một lượng lớn bộ nhớ, nhưng để tiết kiệm thời gian, chẳng hạn như khi các track âm thanh là ít phức tạp. Một tốc độ bit của 128Kb / s tương ứng với chất lượng ghi âm của một đĩa CD. Trong trường hợp nén MP3, 2.4 MB dữ liệu là đủ để lưu năm phút âm thanh với tốc độ bit 64Kb / s.

Các tín hiệu âm thanh stereo là một vấn đề đáng nói. Có thể nói rằng có giống ba chính của tín hiệu: mono, stereo, và stereo doanh.Mono và stereo khá rõ ràng và không yêu cầu lời giải thích; Tuy nhiên, âm thanh stereo doanh có thể. Nó là sự kết hợp của hai giống khác.Các tín hiệu âm thanh stereo được mã hóa trong một phần riêng biệt của tín hiệu tương tự cho hai kênh mono. Chúng được mã hóa trong mono.Tuy nhiên, các yếu tố khác nhau của các kênh truyền hình được mã hóa riêng biệt. Đây là một cách khác để tiết kiệm bộ nhớ, và do đó cũng phù hợp với mã hóa các dòng âm thanh radio Internet.

### 1.3.8. Nâng cao chất lượng bản ghi

Sự can thiệp là một vấn đề phổ biến mà có thể xảy ra trong suốt buổi ghi hình cuộc phỏng vấn hoặc các chương trình (ví dụ như việc sử dụng một micro) trong Internet radio.Đối với truyền dẫn chuyên nghiệp, chất lượng phải được cải thiện. Nó có thể phục vụ nhiều ứng dụng, một trong số đó là CoolEdit PRO.Nếu bạn chia một file WAV thành các file nhỏ hơn, mỗi trong đó sẽ tổ chức một track âm thanh duy nhất.

Vấn đề phổ biến nhất là nhiễu. Có, tất nhiên, một số cách để ghi lại. Chúng bao gồm trung bình lọc, phương tiện truyền thông dựa-thuật toán như lỗi dự đoán (phương pháp tự động hồi quy) chế biến,giảm nhiễu băng rộng liên quan đến việc lập dự toán lọc nhiễu Wiener dựa trên tín hiệu (lọc không chịu bất cứ mối tương quan với sự giao thoa tín hiệu),Kalman lọc áp dụng cho nhiễu Gaussian (dựa vào việc giảm thiểu các autocovariance lỗi) phổ trừ có thể được sử dụng nếu chúng ta giả định tính dừng của nhiễu,và lấy mẫu nhiễu cuối cùng,một số phương pháp dựa trên mô hình thống kê của tín hiệu và wavelet lọc (cho phép lựa chọn một tập hợp các wavelets dựa vào bản chất của sự can thiệp).

Phần khó khăn nhất là sự xáo trộn của nhiễu không cố định, phụ gia tiếng ồn khi tín hiệu và phổ nhiễu chồng chéo và phổ nhiễu khác nhau theo thời gian,do đó chúng ta không thể có được mẫu. Nó là tương đối dễ dàng để loại bỏ nhiễu xung (lọc trung bình) --- thống nhất, nhiễu tĩnh với một quang phổ được biết đến (hiệu quả cao phổ trừ).

Nhiễu, tuy nhiên, không phải là vấn đề duy nhất mà bạn có thể gặp phải trong quá trình ghi. Thường thì nó đã tạo ra một khoảng trống trong buổi ghi hình,với thiếu phần của mặt nạ và một tín hiệu liên tục. Phương pháp Burga cho phép bạn để giải quyết vấn đề này. Nó liên quan đến việc sử dụng dự đoán tuyến tính (cả phía trước và phía sau) trên các mẫu thích hợp trước và sau khi thiệt hại. Trong một phần của thuật toán, hệ số dự báo được xác định cho những đoạn có liên quan,và sau đó chúng được ngoại suy bằng việc tiếp tục đáp ứng bộ lọc với xâm nhập tương tự. Các thông số thuật toán dự đoán Burg được ước tính mà không cần tính tự tương quan bởi vì họ được lấy từ những quan sát.Các giả định chỉ cần thiết cho các hoạt động đúng đắn của thuật toán là các chuỗi thời gian phải được cố định và khoảng thời gian quan sát phải được biết.

### 1.3.9. Yêu cầu của mạng

Để cung cấp chương trình riêng của mình trên Internet và quảng bá âm nhạc chất lượng tốt trên mạng, bạn cần phải có kết nối Internet vĩnh viễn và hiệu quả theo ý của bạn. Một tham số đặc biệt quan trọng là tốc độ gửi dữ liệu tới Internet, cái gọi là lên tức thì. Tải lên một tham số liên quan chặt chẽ đến số lượng tối đa người dùng có thể đồng thời kết nối với server radio. Đây là một câu hỏi quan trọng, bởi vì quyền truy cập không giới hạn có thể dẫn đến quá tải máy chủ,và do đó thất bại hay trục trặc của nó. Đối với SHOUTcast bạn có thể chỉnh sửa các tập tin sc\_serv.ini, trong đó có ba thông số hữu ích. Đầu tiên là PortBase định nghĩa mà cổng được gửi đến dòng âm thanh. Giá trị mặc định là cổng 8000, nhưng chúng ta có thể thay đổi nó với bất kỳ khác. tham số khác là một mật khẩu, trong đó chúng ta có thể xác định mật khẩu cho người sử dụng và quản trị viên. Thông số khác rất quan trọng là người sử dụng tối đa, kiểm soát có bao nhiêu người có thể được kết nối với máy chủ của chúng tôi.Nó quy định cụ thể số lượng khe cắm sử dụng có sẵn.

Do đó, trước khi tiếp tục đến các vấn đề kỹ thuật, một giai đoạn rất quan trọng của việc chuẩn bị được ước tính kích thước của các đối tượng có thể có khả năng quan tâm đến đài phát thanh của chúng tôi. Chỉ trên cơ sở phân tích này là nó có thể tương thích với quy hoạch và thực hiện các cơ sở hạ tầng kỹ thuật. Cần lưu ý rằng cả hai chất lượng âm thanh và băng thông được đo bằng kilobit mỗi giây. Trong trường hợp của truyền unicast, mỗi kết nối sẽ chiếm rất nhiều băng thông cho một chương trình. Ví dụ, với một liên kết 512kbps, chỉ có hai người sẽ có thể nhận được 192kbps chất lượng phát sóng. Giảm tỷ lệ bit trong nửa sẽ cho phép năm người nghe buổi phát sóng. Do đó, cần thiết để tìm một thỏa hiệp giữa chất lượng và băng thông truyền dẫn. Điều đáng chú ý là một số loại âm nhạc với các cấu trúc âm thanh phức tạp ít cho phép người nghe để thưởng thức đầy đủ chất lượng âm thanh với tốc độ bit thấp hơn đáng kể so với những người khác.

## **1.4. Nghiên cứu các giải pháp về bảo mật dịch vụ trong mạng IP Hiếu D16**

### 1.4.1. Đặt vấn đề

Hệ thống truyền thanh Radio số đồng nhất 3 cấp được kết nối bằng Internet từ máy chủ phát sóng đến các máy thu Internet radio. Khi triển khai hệ thống trên mạng Internet, một trong những mối quan tâm hàng đầu là tính bảo mật, an toàn và tin cậy của hệ thống. Do đó cần phải tìm hiểu về các giải pháp về bảo mật dịch vụ trong mạng IP.

Một số tiêu chí đánh giá bảo mật trong mạng IP:

|  |  |
| --- | --- |
| **TT** | **CÁC TIÊU CHÍ ĐÁNH GIÁ** |
| 1 | Hệ thống mạng thiết kế đúng chuẩn và triển khai mô hình mạng nào (Miền hay nhóm)? |
| 2 | Hệ thống  website và các ứng dụng có hệ thống cân bằng tải hay không? |
| 3 | Triển khai hệ thống tường lửa chưa? Phần cứng hay phần mềm? |
| 4 | Hệ điều hành, phần mềm có cập nhật vá lỗi chưa? |
| 5 | Ghi nhật ký truy nhập và giám sát hệ thống chưa? |
| 6 | Báo về dữ liệu và sao lưu dự phòng như thế nào? |
| 7 | Có hệ thống phát hiện và ngăn chặn xâm nhập không? |
| 8 | Hệ thống quét virus theo mô hình chủ- khách không? |
| 9 | Hệ thống được triển khai các phương pháp bảo mật nào? |
| 10 | Thường xuyên kiểm tra, đánh giá về khả năng bảo mật của hệ thống hay không? |

### 1.4.2. Các kiểu tấn công mạng phổ biến

**DoS** :

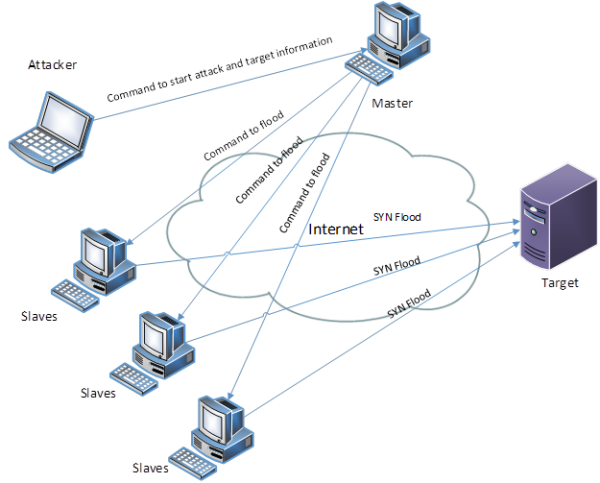
DoS (Denial of Services Attack) hay còn gọi là “Tấn Công Từ Chối Dịch Vụ” là một dạng tấn công mà người thực hiện có thể dùng để khiến cho một hệ thống không thể sử dụng được hoặc làm chậm hệ thống lại, khiến nó không thể phục vụ cho những người dùng truy cập vào dịch vụ của server. Nguyên lý hoạt động cơ bản của nó là làm quá tải tài nguyên của hệ thống làm cho server không thể đáp ứng các yêu cầu từ các máy Client và Server sẽ nhanh chóng bị ngừng hoạt động hoặc reboot. Mục tiêu của DoS Attack không phải để chiếm quyền truy cập vào máy tính, dữ liệu hay kiểm soát 1 hệ thống mà là để ngăn cản những người dùng (User) sử dụng dịch vụ đó. Kẻ tấn công có thể cố thực hiện những việc sau:

• Làm ngập lụt mạng, sẽ làm nghẽn việc lưu thông trong mạng.

• Làm gián đoạn kết nối giữa 2 máy tính,sẽ ngăn cản việc truy cập, sử dụng dịch vụ của server.

• Ngăn chặn 1 cá nhân nào đó truy cập, sử dụng dịch vụ của server.

• Làm gián đoạn việc cung cấp dịch vụ đến một hệ thống hay một user nào đó.

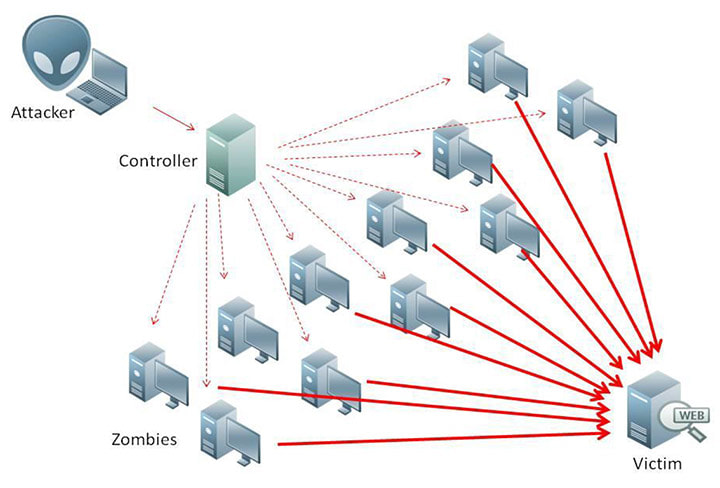
[](http://www.vnpro.vn/wp-content/uploads/2015/07/DoS.png)

Hình 1. 15

**DDOS**

Trên Internet tấn công Distributed Denial of Service là một dạng tấn công từ nhiều máy tính tới một đích, nó gây ra từ chối các yêu cầu hợp lệ của các user bình thường. Bằng cách tạo ra những gói tin cực nhiều đến một đích cụ thể, nó có thể gây tình trạng tương tự như hệ thống bị shutdown. Nó được tấn công từ một hệ thống các máy tính cực lớn trên Internet, và thường dựa vào các dịch vụ có sẵn trên các máy tính trong mạng botnet.

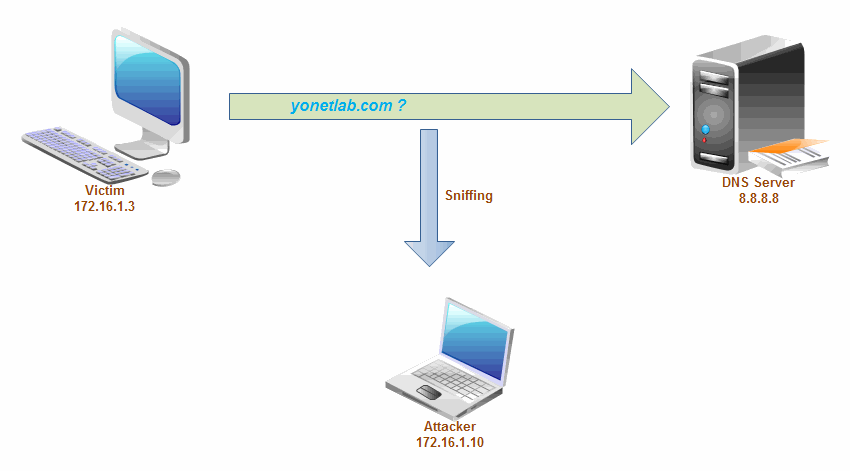
Các dịch vụ tấn công được điều khiển từ những "primary victim" trong khi các máy tính bị chiếm quyền sử dụng trong mạng Bot được sử dụng để tấn công thường được gọi là "secondary victims". Là dạng tấn công rất khó có thể phát hiện bởi tấn công này được sinh ra từ nhiều địa chỉ IP trên Internet. Nếu một địa chỉ IP tấn công một công ty, nó có thể được chặn bởi Firewall. Nếu nó từ 30.000 địa chỉ IP khác, thì điều này là vô cùng khó khăn. Thủ phạm có thể gây nhiều ảnh hưởng bởi tấn công từ chối dịch vụ DoS, và điều này càng nguy hiểm hơn khi chúng sử dụng một hệ thống mạng Bot trên internet thực hiện tấn công DoS và đó được gọi là tấn công DDoS.



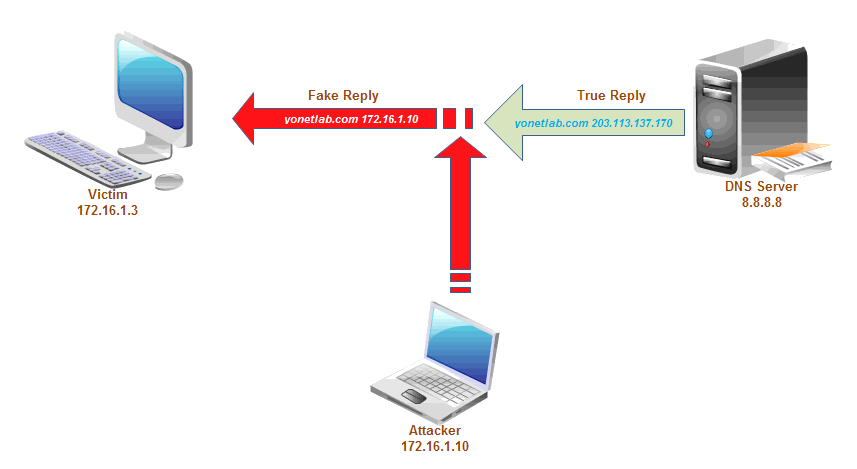
Hình 1. 16

**Giả mạo DNS**

Giả mạo DNS là một kỹ thuật MITM được sử dụng nhằm cung cấp thông tin DNS sai cho một host để khi người dùng duyệt đến một địa chỉ nào đó. Giả mạo DNS: Có nhiều cách để có thể thực hiện vấn đề giả mạo DNS. Mỗi truy vấn DNS được gửi qua mạng đều có chứa một số nhận dạng duy nhất, mục đích của số nhận dạng này là để phân biệt các truy vấn và đáp trả chúng. Điều này có nghĩa rằng nếu một máy tính đang tấn công có thể chặn một truy vấn DNS nào đó được gửi đi từ một thiết bị cụ thể, thì tất cả những gì cần thực hiện là tạo một gói giả mạo có chứa số nhận dạng đó để gói dữ liệu đó được chấp nhận bởi mục tiêu.



Hình 1. 17



Hình 1. 18

**Chiếm quyền điều khiển Session**

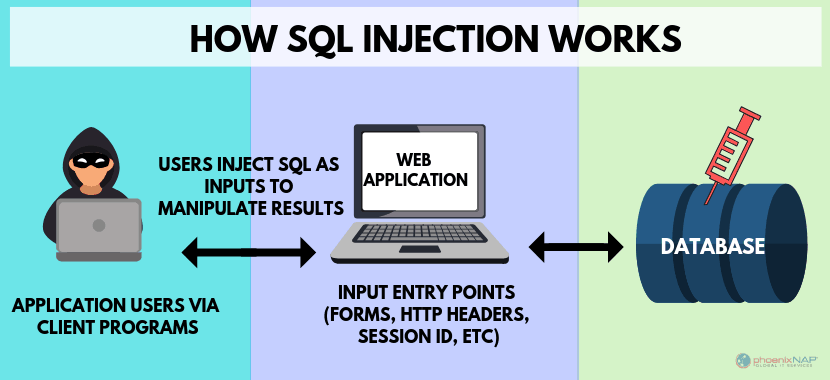
Thuật ngữ chiếm quyền điều khiển session (session hacking) chứa đựng một loạt các tấn công khác nhau. Nhìn chung, các tấn công có liên quan đến sự khai thác session giữa các thiết bị đều được coi là chiếm quyền điều khiển session. Khi đề cập đến một session, chúng ta sẽ nói về kết nối giữa các thiết bị mà trong đó có trạng thái đàm thoại được thiết lập khi kết nối chính thức được tạo, kết nối này được duy trì và phải sử dụng một quá trình nào đó để ngắt nó.

Không có thứ gì khi đi qua mạng được an toàn, và dữ liệu session cũng không có gì khác biệt. Nguyên lý ẩn phía sau hầu hết các hình thức chiếm quyền điều khiển session là nếu có thể chặn phần nào đó dùng để thiết lập một session, khi đó bạn có thể sử dụng dữ liệu đó để thủ vai một trong số những thành phần có liên quan trong truyền thông và từ đó có thể truy cập các thông tin session.

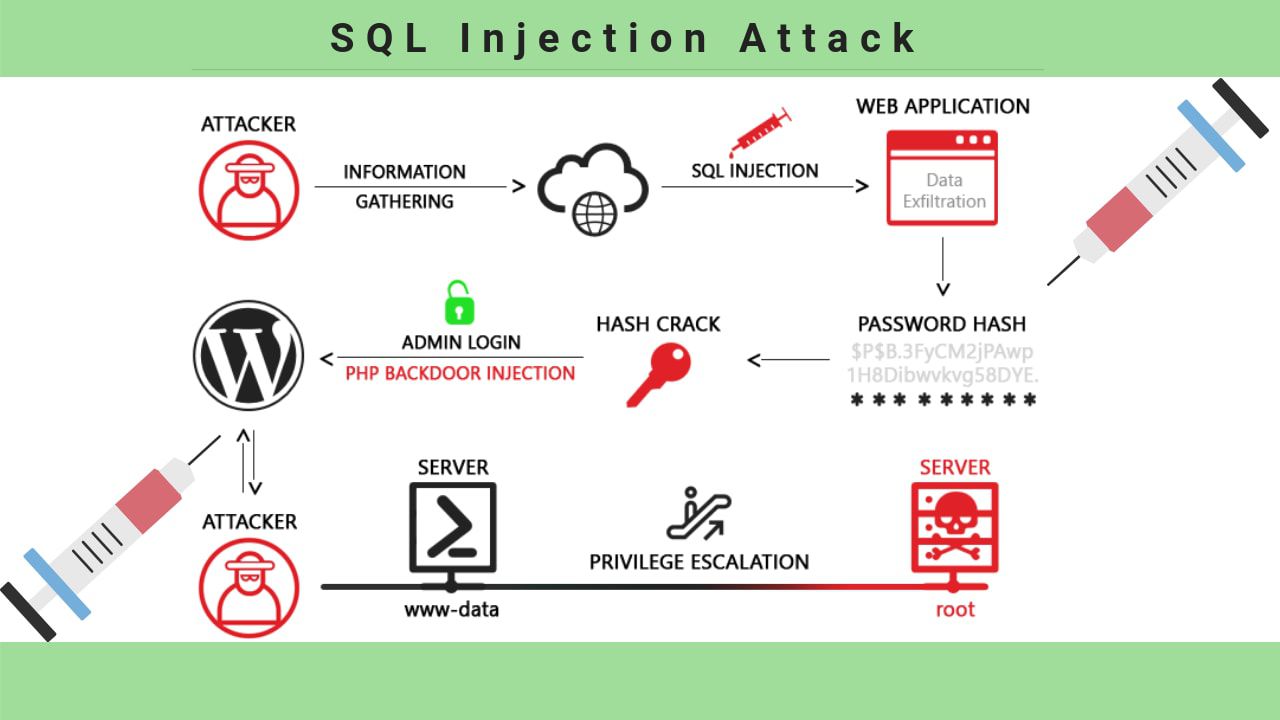
**SQL Injection**

Việc thiết kế và đưa website vào hoạt động luôn đòi hỏi các nhà phát triển phải quan tâm đến vấn đề về an toàn, bảo mật nhằm giảm thiểu tối đa khả năng bị tin tặc tấn công. Thường các nhà phát triển tập trung vào các vấn đề an toàn của hệ điều hành, hệ quản trị CSDL, webserver... Chẳng hạn như hổng bảo mật trên IIS.

Tuy nhiên, có một nguy cơ tiềm ẩn ít được quan tâm đó là các đoạn mã của ứng dụng. Một trong số đó là tấn công bằng SQL Injection. SQL Injection là một kĩ thuật cho phép những kẻ tấn công thi hành các câu lệnh truy vấn SQL bất hợp pháp (người phát triển không lường trước được) bằng cách lợi dụng lỗ hổng trong việc kiểm tra dữ liệu nhập từ các ứng dụng web. Hậu quả này rất tai hại vì nó cho phép kẻ tấn công có toàn quyền, hiệu chỉnh... trên cơ sở dữ liệu của ứng dụng. Lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lí bằng các hệ quản trị CSDL như SQL Server, Oracle, DB2, Sysbase.



Hình 1. 19



Hình 1. 20

**Trojan – Virus – Worm**

Trojan:Là một đoạn mã chương trình không có tính chất lây lan. Trojan dùng để đánh cắp thông tin quan trọng trên máy tính nạn nhân để gửi về cho Hacker hoặc xóa dữ liệu.

Backdoor:Loại Trojan khi được cài đặt vào máy nạn nhân sẽ tự mở ra một cổng dịch vụ cho phép hacker có thể kết nối từ xa và thực hiện lệnh mà hacker đưa ra.

Virus: chương trình có kích thước rất nhỏ tồn tại độc lập ,có khả năng tự thực thi và bám kí sinh vào các chương trình ứng dụng trên hệ thống.

Worms: Là loại chương trình có khả năng tự sao chép,lây lan từ máy tính này sang máy khác thông qua mạng và nó là sự kết hợp giữa sức phá hoại (Virus), âm thầm (Trojan) và sự lây lan.

### ****1.4.3. Nguyên lý thiết kế hệ thống bảo mật****

An ninh mạng phải được thiết lập dựa trên các nguyên tắc sau:

* Bảo vệ có chiều sâu (defense in depth): Hệ thống phải được bảo vệ theo chiều sâu, phân thành nhiều tầng và tách thành nhiều lớp khác nhau. Mỗi tầng và lớp đó sẽ được thực hiện các chính sách bảo mật hay ngăn chặn khác nhau. Mặt khác cũng là để phòng ngừa khi một tầng hay một lớp nào đó bị xâm nhập thì xâm nhập trái phép đó chỉ bó hẹp trong tầng hoặc lớp đó thôi và không thể ảnh hưởng sang các tầng hay lớp khác.
  + Cho ví dụ: thông thường có 7 lớp bảo vệ sau: data (password, encryption, access control list), application  (tùy ứng dụng mà có cách cấu hình đảm bảo an toàn riêng), host (anti-virus, update management, OS hardening), internal network (network-based IDS/IPS, VLAN-based network segmentation), perimeter network (firewall,router,VPN),physical(camera,lock,guard),policy/procedure/awareness (security policy, disaster recovery plan, security training).
* Sử dụng nhiều công nghệ khác nhau: Không nên tin cậy vào chỉ một công nghệ hay sản phẩm công nghệ bảo đảm an ninh cho mạng của một hãng nào đó. Bởi nếu như sản phẩm của hãng đó bị hacker tìm ra lỗ hổng thì dễ dàng các sản phẩm tương tự của hãng đó trong mạng cũng sẽ bị xuyên qua và việc phân tầng, phân lớp trong chính sách phòng vệ là vô nghĩa. Vì vậy khi tiến hành phân tầng, tách lớp, nên sử dụng nhiều sản phẩm công nghệ của nhiều hãng khác nhau để hạn chế nhược điểm trên. Đồng thời sử dụng nhiều cộng nghệ và giải pháp bảo mật kết hợp để tăng cường sức mạnh hệ thống phòng vệ như phối hợp Firewall làm công cụ ngăn chặn trực tiếp, IDS làm công cụ “đánh hơi”, phản ứng phòng vệ chủ động, Anti-virus để lọc virus…v.v
* Các tiêu chuẩn đáp ứng: Các sản phẩm bảo mật phải đáp ứng một số chứng nhận tiêu chuẩn như Common Criteria, ISO/IEC 15408:2005 và ISO/IEC 18405:2005 EAL4, ICSA Firewall và VPN, FIPS-140…
* Đặc quyền tối thiểu: Người dùng, máy tính hay ứng dụng chỉ được cấp các quyền hạn đủ để thực hiện yêu cầu, công việc của họ. Ngoài ra, kiểm soát chặt chẽ việc cấp thêm quyền hạn mới và thu hồi các quyền hạn không dùng tới.
* Ví dụ: nhân viên thông thường chỉ cần chạy email, web, VoIP, các ứng dụng nghiệp vụ như ERP, CRM thì chỉ cần cấp cho họ quyền hạn của một người dùng bình thường (không có quyền cài đặt phần mềm, cấu hình mạng, bật tắt dịch vụ của hệ điều hành, v.v..) là đủ. Khi nhân viên chuyển sang bộ phận khác hoặc nghỉ việc thì xem xét và thay đổi lại quyền hạn cho phù hợp.
* Giữ cho hệ thống được tinh gọn: Loại bỏ các chức năng, tài khoản, chương trình không dùng đến, chỉ giữ lại những thứ đang thực sự cần thiết thôi. Điều này giúp giảm thiểu khả năng bị khai thác các lỗ hổng có thể có trong các thành phần dư thừa và giảm lượng tài nguyên tính toán bị tiêu tốn cũng như giúp cho việc quản lý và giám sát hệ thống được thuận tiện hơn.
* Ví dụ: loại bớt các services, startup apps có thể không cần đến như telnet, printing, remote access, v.v.. tắt các user account không cần dùng, v.v..
* Điểm yếu nhất: Một hệ thống có mức độ an toàn chỉ bằng độ an toàn của điểm yếu nhất của hệ thống đó. Vì vậy mà cần xác định đâu là điểm yếu nhất của hệ thống để tìm cách gia cố và bảo vệ nó.
* Ví dụ: con người thường là đối tượng để kẻ tấn công khai thác, đạt được quyền truy nhập vào hệ thống. Vì vậy, ngoài các biện pháp bảo vệ cho các thành tố thuần kỹ thuật như server, network thì cũng cần quan tâm tới việc đào tạo, giúp đỡ người dùng tiếp cận và sử dụng hệ thống sao cho đúng cách và đảm bảo an toàn.
* Trạng thái an toàn khi có lỗi: Hệ thống không tránh khỏi có lúc gặp sự cố. Lúc đó thì cần thiết phải đặt hệ thống ở chế độ từ chối các khả năng bị kẻ tấn công xâm nhập. Và đôi lúc có thể cấm truy cập với cả người dùng hợp lệ cho tới khi hệ thống được khôi phục nhưng điều này vẫn chấp nhận được (thay vì để lọt cho kẻ tấn công giả dạng đi vào).
* Ví dụ: nếu bộ lọc gói tin của router bị lỗi thì không một gói tin nào được phép đi qua nó.

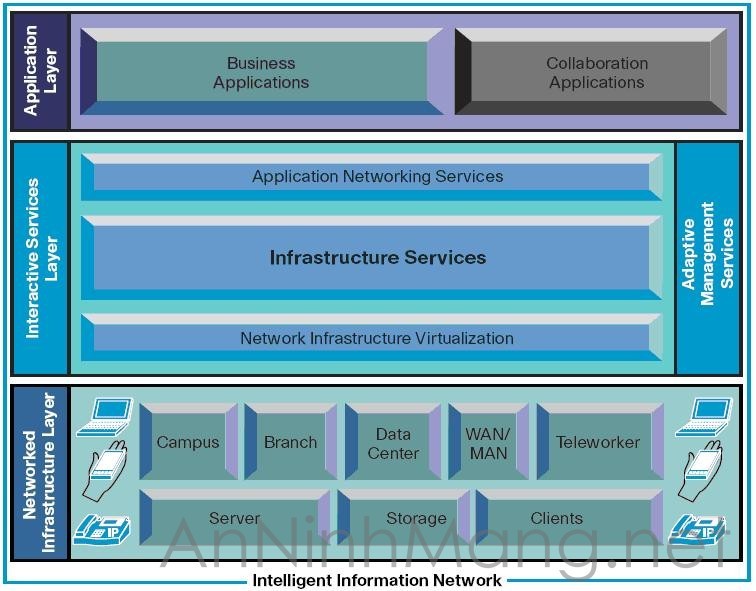
**Từ các tiêu chí và nguyên tắc trên chúng tôi xin đưa ra một số nhóm giải pháp sau ở mục sau.**

**1.4.4. Các nhóm giải pháp**

**a) Nhóm giải pháp về quy hoạch, thiết kế**

Thiết kế, quy hoạch một hệ thống mạng lớn không đơn thuần là phát triển thêm các thiết bị hỗ trợ người dùng mà phải dựa trên mô hình chuẩn đã và đang áp dụng cho các hệ thống mạng tiên tiến tại các cơ quan, doanh nghiệp phát triển trên thế giới, đó chính là mô hình mạng Định hướng Kiến trúc Dịch vụ (Service-Oriented Architecture – SOA).

**Thiết kế cơ sở hạ tầng theo mô hình SOA:**



Hình 1. 21

Kiến trúc SOA gồm có 3 lớp:

***Lớp cơ sở hạ tầng mạng (networked infrasstructure layer):*** là lớp mạng liên kết các khối chức năng theo kiến trúc phân tầng, có trật tự.

***Lớp dịch vụ tương tác (Interactive services layer):*** bao gồm sự kết hợp một số kiến trúc mạng đầy đủ với nhau tạo thành các chức năng cho  phép nhiều ứng dụng có thể sử dụng trên mạng.

***Lớp ứng dụng (Application layer):*** Bao gồm các loại ứng dụng cộng tác và nghiệp vụ. Các ứng dụng này kết hợp với các dịch vụ tương tác cung cấp ở lớp dưới sẽ giúp triển khai nhanh và hiệu quả

Trong phần này, tôi xin giới thiệu sơ lược về các phương thức thiết kế mạng và bảo mật được sử dụng trong việc thiết kế các hệ thống mạng lớn và hiện đại của các tổ chức và doanh nghiệp lớn. Tương ứng với kiến trúc SOA là thuộc lớp Cơ sở hạ tầng mạng.

**Phương thức thiết kế phân lớp – Hierarchical:**

Một mạng là gồm nhiều mạng LAN trong một hoặc nhiều toà nhà, tất cả các kết nối thường nằm trong một khu vực địa lý. Thông thường các Campus gồm có Ethernet, Wireless LAN, Gigabit Ethernet, FDDI (Fiber Distributed Data Interface). Được thiết kế theo các tầng, khu vực khác nhau; trên mỗi tầng, mỗi khu vực được triển khai các thiết bị, các chính sách mạng tương ứng.



Hình 1. 22

**Khu vực LAN:**

Từ mô hình trên ta cũng thấy được rằng khu vực này được thiết kế theo tầng. Tầng lõi, tầng phân tán, tầng truy xuất vừa đảm bảo tính dự phòng đường truyền, lưu lượng mạng được phân bố đều, toàn mạng được chia thành nhiều phân đoạn để dễ dàng kiểm soát và bảo mật.

**Khu vực kết nối WAN:**

Đây là vùng cung cấp các kết nối ra môi trường Internet và các cơ quan thành viên, đối tác. Tại  đây phải đảm bảo tính sẵn sàng cao và tính dự phòng đường truyền. Vì vậy hệ thống cân bằng tải và dự phòng đường truyền WAN cần được triển khai.

**Khu vực các máy chủ public**

Khu vực này thường được biết đến với tên là vùng phi quân sự (DMZ-demilitarized zone) có nghĩa rằng tại khu vực này được hệ thống tường lửa kiểm soát vào ra các máy chủ rất chặt chẽ nhằm ngăn chặn các cuộc tấn công của Hacker, người dùng trong LAN…

* Ưu điểm: dự phòng, dễ phát triển, hiệu năng cao, dễ khắc phục sự cố, thích hợp với môi trường đào tạo và nghiên cứu ở các trường đại học và cao đẳng, doanh nghiệp lớn.
* Khó khăn khi xây dựng mạng theo phân lớp là chi phí khá cao, cần đội ngũ quản trị hệ thống chuyên nghiệp

**Mô hình triển khai dịch vụ và quản lý người dùng**

Mô hình này được triển khai trên cơ sở hạ tầng đã thiết kế là yếu tố quyết định đến hiệu năng hoạt động và cách thức quản lý hệ thống.

Thực tế một số cơ quan, doanh nghiệp hiện nay đang triển khai hệ thống mạng theo mô hình mạng ngang hàng. Mô hình này chỉ triển khai cho các tổ chức có quy mô nhỏ hẹp. Khi quy mô hệ thống có trên hàng trăm máy tính, nhiều phòng ban, chức năng thì việc quản lý theo mô hình ngang hàng không còn phù hợp nữa. Giải pháp triển khai dịch vụ và quản lý người dùng theo mô hình chủ-khách là giải pháp tối ưu, hiệu quả nhất. Hệ thống này có nhiều thuận lợi và tính năng tối ưu như:

* Phần quyền truy nhập vào các tài nguyên dùng chung trên mạng.
* Triển khai cấu hình các phần mềm, dịch vụ tự động cho các máy khách, người dùng nhanh chóng.
* Triển khai một chính sách bảo mật cho toàn đơn vị một cách dễ dàng, thống nhất, tập trung, ví dụ: Khi người dùng không sử dụng trong thời gian nhất định, hệ thống sẽ tự lock, luôn yêu cầu người dùng đặt mật khẩu cho hệ điều hành ở chế độ phức tạp, thường xuyên thay đổi mật khẩu…nhằm tránh các hacker dùng các phần mềm giải mã mật khẩu.
* Dễ dàng giám sát an ninh, bảo mật, logging v.v

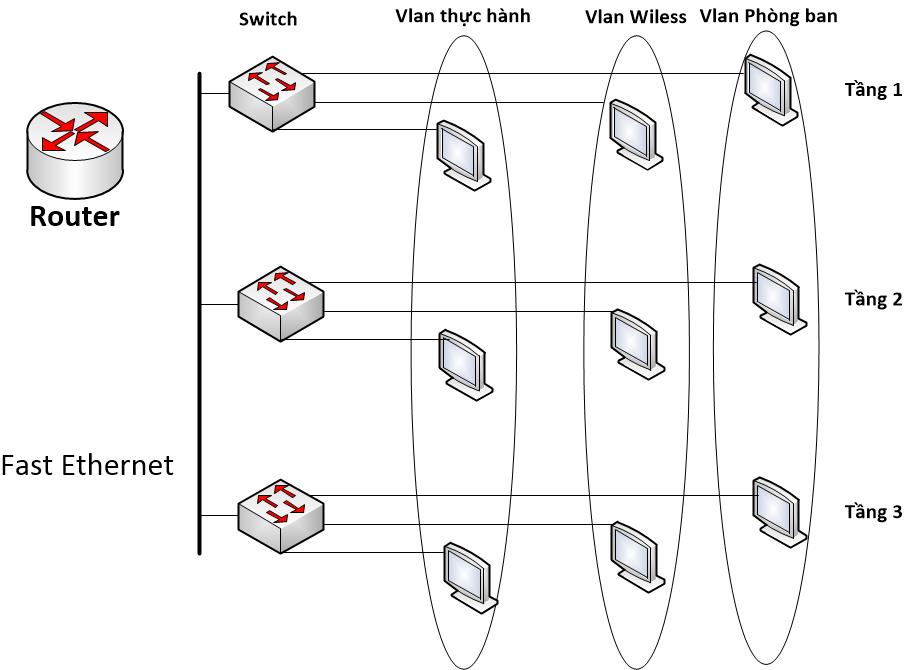
**Phân hoạch VLAN (LAN ảo)**

Thực trạng hệ thống mạng ở một số doanh nghiệp hiện nay được phân chia thành các khu vực, chưa kiểm soát được lưu lượng download và upload cũng như băng thông truy xuất Internet của người dùng. Mô hình mạng như vậy là một miền quảng bá, mỗi gói tin kiểu quảng bá thì ở bất kỳ máy nào cũng có thể tới được tất cả các máy tính khác trong mạng nên có những vấn đề sau:

* + Về băng thông: Toàn doanh nghiệp là một vùng quảng bá rất lớn, số máy tính, số người dùng sẽ tăng lên khi đơn vị phát triển thêm các khu vực khác. Do vậy băng thông, hiệu năng của toàn mạng sẽ giảm, thậm chí thường gây tắc nghẽn.
  + Về bảo mật: Việc kiểm soát bảo mật gặp rất nhiều khó khăn khi hệ thống trải rộng khắp toàn cơ quan, doanh nghiệp.

Để giải quyết các vấn đề trên, chúng ta đưa ra giải pháp chia mạng thành nhiều mạng LAN ảo. VLAN được định nghĩa là một nhóm logic các thiết bị mạng, và được thiết lập dựa trên các yếu tố chức năng, bộ phận, ứng dụng của tổ chức. Việc chia VLAN thành các phân hệ khác nhau giúp khả năng bảo mật, quản lý và hiệu năng đạt kết quả cao nhất.

Ví dụ: Tất cả các máy tính thuộc các phòng thực hành, thí nghiệm trong toàn trường thì thuộc vlan01; các phòng ban thuộc vlan02, các wireless thuộc vlan03 v.v. Các VLAN đó mặc định sẽ không liên lạc được với nhau. Khi muốn có sự liên lạc giữa các VLAN với nhau ta tiến hành cấu hình trên thiết bị định tuyến router và kiểm soát băng thông giữa các Vlan. (hình 2)



Hình 1. 23

**b) Nhóm giải pháp về hệ thống ngăn chặn, phát hiện tấn công**

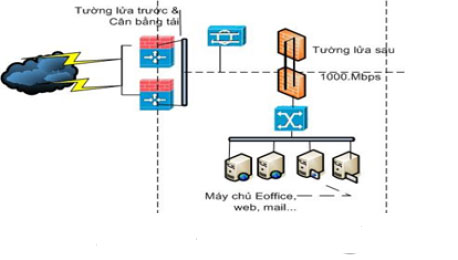
**Hệ thống tường lửa đa tầng:**

Hệ thống tường lửa là hệ thống kiểm soát truy nhập giữa mạng Internet và mạng nội bộ. Tường lửa có 2 loại: phần cứng và phần mềm. Mỗi loại có các ưu điểm khác nhau. Phần cứng có hiệu năng ổn định, không phụ thuộc vào hệ điều hành, virus, mã độc, ngăn chặn tốt giao thức ở tầng mạng trong mô hình tham chiếu TCP/IP. Phần mềm rất linh hoạt trong những cấu hình ở giao thức tầng ứng dụng trong mô hình TCP/IP.

Ví dụ, tường lửa tầng thứ nhất (thường là phần cứng) đã loại bỏ hầu hết các kiểu tấn công trực diện vào hệ thống máy chủ web, máy chủ mail như kiểu tấn công phân tán  (DDOS), tức hacker dùng các công cụ tạo các yêu cầu truy xuất tới máy chủ từ nhiều máy tính khác trên mạng với tần suất cao để nhằm làm cho máy chủ quá tải và dẫn tới ngừng phục vụ.

Nhưng hacker cũng không dừng tại đó, chúng có thể vượt qua hệ thống tường lửal tầng thứ nhất với những gói tin hợp lệ để vào hệ thống mạng LAN. Bằng các giao thức tầng ứng dụng chúng có thể lại đạt được mục đích. Chính vì thế triển khai hệ thống tường lửa phần mềm sẽ hỗ trợ và làm gia tăng tính bảo mật cho toàn mạng. Trong trường hợp, một hệ thống tường lửa gặp sự cố thì hệ thống còn lại vẫn kiểm soát được.

Sau đây là giải pháp thiết kế hệ thống tường lửa thường đa tầng, nó bao gồm ít nhất 2 tầng chính sau: tường lửa trước và tường lửa sau (hình 3).

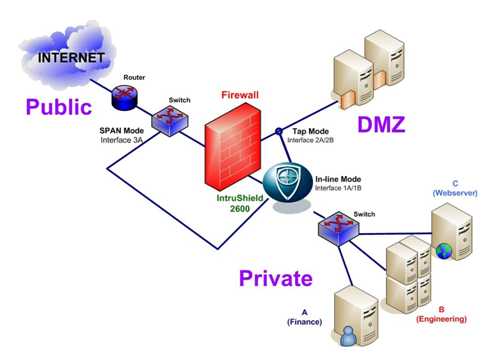


Hình 1. 24

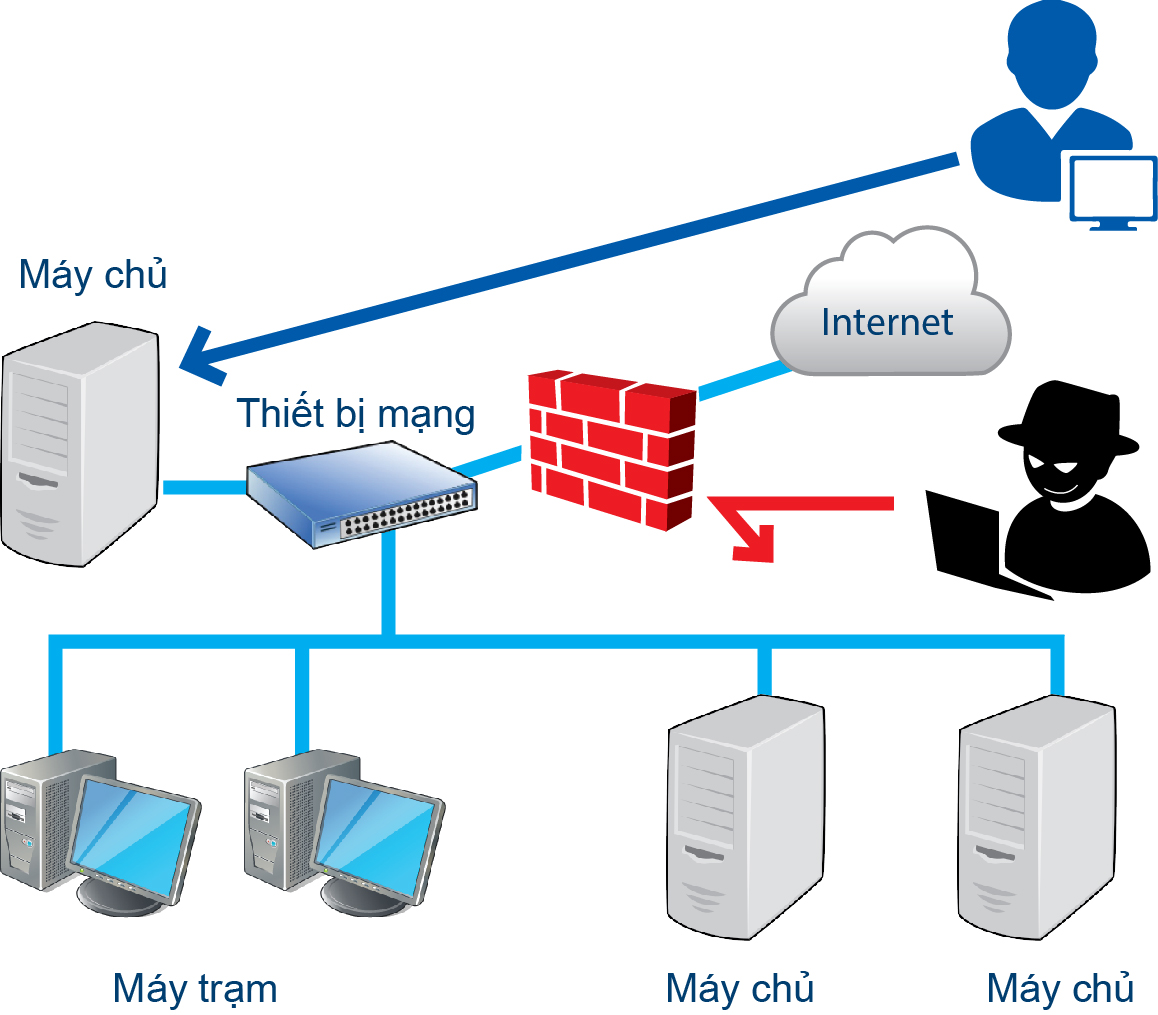
**Hệ thống phát hiện và chống xâm nhập IDS/IPS:**

Hiện nay các hình thức tấn công của người có ý đồ xấu ngày càng nhiều và tinh vi. Ví dụ: Trong đơn vị có thể tự cài đặt các công cụ  (Ethereal, Cain & abel…) trên máy tính làm việc hoặc máy tính xách tay để tiến hành nghe lén hay quét trực tiếp lên các máy chủ, từ đó có thể lấy các tài khoản email, Web, FTP, SQL server nhằm thay đổi điểm thi, tiền học phí đã nộp, thay đổi lịch công tác…các hình thức tấn công kiểu này, hệ thống tường lửa không thể phát hiện [3].

Giải pháp hữu hiệu cho thực trạng này là xây dựng hệ thống IDS/IPS (Intrusion Detection System/Intrusion prevention system). IDS/IPS là hệ thống bảo mật vô cùng quan trọng, nó có khả năng phát hiện ra các cuộc tấn công dựa vào các dấu hiệu thiết lập sẵn hoặc các đoạn mã độc hại, bất thường trên giao thông mạng; đồng thời có thể loại bỏ chúng trước khi có thể gây hại cho hệ thống.



Hình 1. 25



Hình 1. 26

**Danh sách điều khiển truy xuất, an toàn cổng thiết bị, lọc địa chỉ mạng**:

***Danh sách điều khiển truy xuất:***

Tình trạng các phòng ban, …đang tự triển khai mạng wireless và mở rộng mạng LAN, nhất là tại các phòng có nhiều thiết bị di động, laptop dẫn tới số kết nối vào mạng nội bộ tăng, băng thông toàn mạng giảm và khó kiểm soát bảo mật.

Danh sách truy nhập là gồm các luật cho phép hay ngăn chặn các gói tin sau khi tham chiếu vào thông tin trong tiêu đề của gói tin để giới hạn các người dùng có thể truy xuất vào các hệ thống máy chủ nội bộ v.v.

***Bảo mật cổng của thiết bị, lọc địa chỉ vật lý của thiết bị mạng:***

Ở các điểm truy nhập mạng công cộng, việc mở rộng LAN của người dùng; việc truy xuất vào các máy chủ nội bộ cần được kiểm soát.

Các giải pháp như cấu hình **bảo mật cổng của thiết bị**, quản lý địa chỉ vật lý là giải pháp cực kỳ an ninh và hiệu quả trong trường hợp này.

* + Cấu hình **bảo mật cổng của thiết bị**trên các switch nhằm đảm bảo không thể mở rộng LAN khi chưa có sự đồng ý của người quản trị hệ thống, nếu vi phạm điều đó, port trên switch đó sẽ chuyển về trạng thái cấm hoặc trạng thái ngừng hoạt động.
  + Địa chỉ vật lý là địa chỉ được cài đặt sẵn từ nhà sản xuất. Về nguyên tắc tất cả các máy tính trên mạng sẽ không trùng nhau về địa chỉ này. Sự kiểm soát theo địa chỉ này là rất cụ thể tới từng máy tính trong mạng, trừ khi người dùng có quyền cài đặt phần mềm và làm giả địa chỉ này ở máy tính đó, hoặc là mở máy tính rồi thay thế card giao tiếp mạng mới.
  + Các thiết bị mạng hiện nay đều được trang bị chức năng ngăn theo địa chỉ vật lý này giúp quản trị mạng kiểm soát được người dùng sử dụng mạng, nhất là muốn triển khai trên hệ thống wireless.

**c)** **Nhóm giải pháp khác**

**Xây dựng hệ thống cập nhật,  sửa lỗi tập trung**

Công đoạn đầu tiên của hacker khi tiến hành tấn công là khảo sát hệ thống đích để tìm ra các lỗi của hệ điều hành, của các dịch vụ, của các ứng dụng khi chúng chưa được cập nhật trên website của nhà cung cấp.

Thực trạng ở các cơ quan, doanh nghiệp cho thấy việc sử dụng các sản phẩm phần mềm hầu như ít cập nhật các bản vá lỗi, có chăng cũng đang riêng lẻ trên các máy tính cá nhân, đó chính là cơ hội cho hacker dùng các công để khai thác lỗ hổng bảo mật. Để cập nhật bản vá lỗi cho tất cả các máy khách trong toàn bộ hệ thống qua Internet mất thời gian và tốn nhiều băng thông đường truyền và không thống nhất.

Giải pháp xây dựng hệ thống tự động cập nhật từ nhà cung cấp trên Internet về máy chủ rồi từ máy chủ này, triển khai cho tất cả các máy khách trong toàn mạng.

Hệ thống WSUS (Windows Server Update Services) của Microsoft không những cập nhập bản vá lỗi cho hệ điều hành Windows mà còn cập nhật bản vá lỗi cho tất cả các sản phẩm khác của hãng bao gồm Internet Explorer, SQL server, Office, Mail, máy chủ Web  v.v.

**Ghi nhật ký, theo dõi, giám sát hệ thống**

***Ghi nhật ký:***

Giải pháp ghi lại các phiên kết nối, các phiên đăng nhập của người dùng, các tiến trình hoạt động sẽ giúp quản trị mạng có thể tìm lại dấu vết của người dùng, hacker và các lỗi có thể gây ra cho hệ thống trước đó. Các  máy chủ Web , máy chủ Email và máy chủ ứng dụng khác cần được kích hoạt tính năng ghi nhật ký, việc quản lý lưu trữ các thông tin này là rất cần thiết. Hacker chuyên nghiệp khi đã xâm nhập thành công vào hệ thống, việc không thể bỏ qua chính là việc xóa dấu vết đã được ghi. Chính vì thế triển khai hệ thống ghi nhật ký tập trung tại một máy chủ chuyên dụng khác là rất hiệu quả.

Các phần mềm mã nguồn mở như: Syslog-ng: (http://www.balabit.com); SyslogAgent: (http://syslogserver.com) là giải pháp tốt. Hệ thống sẽ giúp chúng ta ghi các cảnh báo, thông báo từ các thiết bị phần cứng như: tường lửa, router, switch, từ các máy chủ Web, Database, và các hệ thống khác.

***Theo dõi, giám sát:***

Theo dõi, giám sát là công việc thường xuyên và quan trọng của nhà quản trị mạng chuyên nghiệp, đó chính là công việc phòng chống hiệu quả trước khi sự cố xuất hiện. Theo dõi, giám sát có thể:

* Phát hiện trên hệ thống mạng có nhiều virus phát tán.
* Giám sát các máy tính trong mạng LAN và trên môi trường Internet.
* Theo dõi hiệu năng hoạt động các phần cứng của máy chủ để tiến hành nâng cấp, bảo trì, bảo dưỡng.
* Phát hiện hacker đang dùng các công cụ nghe lén mật khẩu, quét các lỗi của hệ thống và các ứng dụng.
* Thống kê số lượng các kết nối, các session cũng như những lưu lượng bất thường trên hệ thống mạng v.v

**Giải pháp mã hóa dữ liệu và đường truyền**

Dữ liệu trên máy chủ, máy tính cá nhân của các cơ quan, doanh nghiệp hiện chưa an toàn vì không được mã hóa nội dung và kể cả khi đi trên đường truyền. Dữ liệu ấy có thể được đọc bởi:

* Người dùng đăng nhập thành công vào máy tính
* Hacker dùng các phần mềm capture (bắt) thông tin trên đường truyền
* Tại các máy chủ và máy tính có lưu trữ dữ liệu nhạy cảm, có dữ liệu cần chia sẽ; tại các thiết bị lưu trữ cần thiết phải tiến hành mã hóa nội dung, điều đó đảm bảo rằng nếu có mất thiết bị lưu trữ, máy tính, người tấn công cũng không thể giải mã được dữ liệu.

Giải pháp Ipsec sẽ được triển khai tại các hệ thống máy chủ và máy người dùng cũng như các thiết bị mạng phải được cấu hình.

**Đào tạo người dùng**

Theo các thống kê về an ninh mạng của CERT (Computer Emergency Response Team-<http://www.cert.org/>) cho thấy, có khoảng 70% số trường hợp bị thất thoát thông tin có liên quan tới yếu tố con người bên trong các hệ thống còn 30% là xuất phát từ bên ngoài mạng nội bộ của các tổ chức thông qua các hành vi truy nhập trái phép hệ thống của hacker.

Theo chuẩn quản lý an ninh thông tin (Information Security Management) ISO 17799/BS-7799, trong đó có tiêu chí về “An ninh về nhân sự (Personnel Security)” mô tả trách nhiệm của nhân viên, vai trò của các cá nhân trong an ninh thông tin, nhằm giảm thiểu các sai sót do lỗi của con người, do ăn cắp hoặc lạm dụng tài sản công.Do vậy việc đào tạo người dùng để họ tự bảo vệ các tài nguyên cho máy tính họ và cho cả tổ chức là nhiệm vụ hết sức quan trọng.

Đào tạo người dùng biết cách phòng chống các thủ đoạn của hacker như lừa đảo qua email. Ví dụ: hacker thường lợi dụng tính tò mò của người dùng khi tham gia Internet để lấy thông tin khi yêu cầu người dùng nhập vào.

Đào tạo người dùng sử dụng các công cụ, phần mềm đúng trình tự, khi cần thiết phải kịp thời báo cáo với người quản trị hệ thống.v.v.

Đào tạo người dùng phải tuân thủ nguyên tắc bảo mật và an toàn thông tin của tổ chức, kể cả khi họ không tham gia làm việc tại cơ quan.

**Hệ thống chống virus**

Để cải thiện tốc độ xử lý của tường lửa, thông thường quản trị mạng không cấu hình kích hoạt tính năng lọc cao cấp của tường lửa (tường lửa ở các vị trí phải xử lý lưu lượng lớn). Khi đó các chương trình quét virus được cài đặt nhằm phát hiện và ngăn chặn các đoạn mã độc, các chương trình gián điệp, các email có tệp tin virus đính kèm.v.v. Nhưng trên thực tế để đầu tư một khối lượng lớn các chương trình virus cho tất cả các máy tính toàn cơ quan thì kinh phí đầu tư khá cao.

Để giảm chi phí bản quyền, giải pháp là triển khai mô hình chống virus chủ –khách. Hiện nay có nhiều hãng nỗi tiếng như Norton, Kaspersky, Trend micro .v.v có thể triển khai theo mô hình này. Lợi ích khi triển khai hệ thống là:

* Chi phí giảm hơn nhiều so với cài đặt trên từng máy khách
* Việc cập nhật phiên bản mới của các máy khách dễ dàng, nhanh chóng và hiệu quả cao.

## **1.5. Nghiên cứu lí thuyết về kỹ thuật truyền dữ liệu số radio DATA SYSTEM RDS ứng dụng trong hệ thống truyền thanh không dây đồng nhất 3 cấp Khoa D16**

### 1.5.1. Giới thiệu chung

RDS được phát triển vào năm 1974 bởi các đài truyền hình (được nhóm lại trong Liên minh Phát thanh Châu Âu , EBU) và các nhà sản xuất Châu Âu, theo sáng kiến ​​của ORTF 1 , Kopitz .

Vào thời điểm đó, một hệ thống có tên Autofahrer-Rundfunk-Informationsystem (ARI) sẽ được triển khai ở Đức , điều này sẽ giúp thông báo cho những người lái xe về việc phát thông tin nhanh về giao thông. ARI rất thú vị, nhưng chỉ giới hạn ở việc xác định các chương trình đường bộ và quá cụ thể đối với tổ chức phát thanh truyền hình Đức, theo vùng. Do đó, ý tưởng của EBU là tiếp tục dịch vụ cơ bản do ARI cung cấp và bổ sung cho nó nhiều dữ liệu hữu ích cho các kiểm toán viên.

Một nhóm làm việc đã được thành lập. Ông bắt đầu nghiên cứu các khả năng sử dụng truyền dữ liệu kỹ thuật số gắn liền với chương trình radio FM. Đặc biệt, các hệ thống có kinh nghiệm tại thời điểm đó ở Phần Lan , Hà Lan và Thụy Điển đã được nghiên cứu. Các thử nghiệm toàn diện đầu tiên diễn ra vào năm 1980 tại Berne - Interlaken , một khu vực nơi tiếp nhận VHF đặc biệt khó khăn: dữ liệu thử nghiệm được phát hành và ghi lại từ nhiều địa điểm khác nhau để nghiên cứu những khó khăn của việc tiếp nhận di động. Năm 1981, một thỏa thuận đã được đưa ra để điều chế được sử dụng cho dữ liệu số.

Một số quốc gia, bao gồm Pháp , Phần Lan, Đức, Hà Lan, Thụy Điển và Vương quốc Anh đã bắt đầu thử nghiệm. Nhưng do đặc điểm kỹ thuật của hệ thống khá mơ hồ, mỗi quốc gia đã sử dụng biến thể của riêng mình, hoặc thậm chí là hai . Năm 1982, tám hệ thống khác nhau đã được thử nghiệm. EBU sau đó đã đánh giá chúng trong các thử nghiệm kích thước cuộc sống mới ở Stockholm . Vào cuối các thử nghiệm này, hệ thống Thụy Điển, đã được sử dụng cho hệ thống phân trang MBS , đã được chọn. Chế độ điều chế sau đó có thể được quyết định chính xác và dứt khoát, trước một chiến dịch thử nghiệm thứ hai ở Bern -Interlaken cho phép chỉ định dữ liệu được truyền và cấu trúc của chúng. Năm 1983, đặc điểm kỹ thuật của RDS đã bị dừng lại.

Vào thời điểm đó, hệ thống ARI đã được triển khai ở Đức, Áo , Thụy Sĩ và Luxembourg , với một số thành công. Do đó, RDS được thiết kế để tương thích với ARI (cả hai hệ thống được cho là có thể sử dụng đồng thời và bởi cùng một trạm), nhưng vào năm 1983, các nhà sản xuất ô tô vẫn lo lắng về khả năng can thiệp. Do đó, các thử nghiệm được tiến hành ở Đức, trong một khu vực khó khăn như Berne-Interlaken, Munich , năm 1983. RDS đã vượt qua thử nghiệm này mà không gặp vấn đề gì.

Thông số kỹ thuật đầu tiên của RDS được EBU xuất bản năm 1984. Quyết định triển khai RDS được đưa ra vào năm 1985, và trong cùng năm đó, các thử nghiệm tiền vận hành quy mô lớn đã được tiến hành ở Đức. Triển khai bắt đầu vào năm 1987, thông qua việc phổ biến dữ liệu bởi các mạng truyền hình lớn và giới thiệu radio xe tương thích. Ban đầu, các đài truyền hình phát sóng dữ liệu RDS và điều chế bằng thiết bị do họ tự phát triển. Sau đó, một thị trường cụ thể phát triển.

Việc phát sóng RDS ở châu Âu đã diễn ra rất nhanh, do đó những người quảng bá của nó nói về "cuộc cách mạng im lặng" :

1987: triển khai ở Ireland , Pháp và Thụy Điển. Ở Pháp, việc triển khai đầu tiên là công việc của TDF trên các máy phát của đài phát thanh FIP .

1988: Triển khai tại Áo, Bỉ , Đan Mạch , Đức, Ý và Vương quốc Anh.

1989: Triển khai tại Hà Lan, Bồ Đào Nha và Thụy Sĩ.

Tiêu chuẩn RDS đầu tiên ( CENELEC EN 50067) được xuất bản năm 1990, sau một số bổ sung.

Việc triển khai RDS tại Hoa Kỳ được dự kiến ​​vào năm 1990. Nó đã được quyết định chiếm hầu hết các tiêu chuẩn châu Âu và chỉ sửa đổi các điểm nhỏ khi cần điều chỉnh các đặc điểm của Bắc Mỹ. Tiêu chuẩn của Mỹ, được gọi là RBDS , được thông qua vào tháng 1 năm 1993. Thuật ngữ RBDS chỉ được sử dụng để chỉ định tiêu chuẩn: đối với công chúng, hệ thống được gọi là RDS, như ở châu Âu và sử dụng cùng một logo.

Diễn đàn RDS, cơ quan cập nhật tiêu chuẩn, gặp gỡ hàng năm gần Geneva và tập hợp các nhà sản xuất, đài truyền hình, nhà sáng lập và biên tập viên nội dung từ khắp nơi trên thế giới.

Phiên bản mới nhất của tiêu chuẩn RDS, IEC 62106: 2018 được xuất bản vào ngày 10 tháng 10 năm 2018 . Đây là một bản cập nhật quan trọng: đáng chú ý là nó giới thiệu một phần mở rộng của hệ thống, được gọi là "RDS2", giúp tăng đáng kể tốc độ truyền dữ liệu .

### 1.5.2. Lý thuyết chung về điều tần

**a) Lý thuyết chung về điều chế tần số**

Điều chế tần số được áp dụng trong kỹ thuật vô tuyến điện và kỹ thuật xử lý tín hiệu. Người ta truyền thông tin trên một sóng mang cao tần bằng cách thay đổi tần số sóng mang theo tín hiệu cần truyền, trong khi biên độ của sóng mang cao tần không thay đổi .

Sóng mang thường có tần số cao hơn so với tần số của tín hiệu mà nó truyền tải. Sóng mang thường dùng để truyền các thông tin xuyên qua không gian như một sóng điện từ (ví dụ như liên lạc bằng sóng vô tuyến) hay cho phép vài sóng mang tần số khác nhau có thể chia sẻ chung một môi trường phát sóng vật lý bằng phương pháp ghép kênh phân chia theo tần số (ví dụ như trong trường hợp của hệ thống truyền hình cáp).

FM (Frequency Modulation) là phương pháp điều chế biến đổi tần số của sóng mang cao tần theo biên độ của tín hiệu tin tức. Việc truyền tín hiệu âm thanh qua hệ thống radio FM là phổ biến nhất. Tuy nhiên, máy phát FM cũng có thể truyền dữ liệu số tốc độ thấp được gọi là hệ thống dữ liệu radio (Radio Data System - RDS) ở châu Âu và hệ thống radio dữ liệu (Radio Broadcast Data System - RBDS).

Từ năm 1940 khi bắt đầu phát hiện thấy ưu điểm chống can nhiễu của kỹ thuật điều tần, kỹ thuật mới này được được sử dụng mạnh mẽ. Hiện nay kỹ thuật này được sử dụng rộng rãi trong phát thanh, hệ thống vô tuyến hai chiều, hệ thống ghi băng từ và hệ thống truyền dẫn video. Trong hệ thống vô tuyến, điều tần với băng thông đủ lớn giúp ích lớn cho việc loại bỏ tạp âm trong khi truyền.

**b) Tín hiệu điều chế FM**

Điều chế tần số được áp dụng trong kỹ thuật vô tuyến điện và kỹ thuật xử lý

tín hiệu. Người ta truyền thông tin trên một sóng mang cao tần bằng hai cách. Thay

đổi tần số sóng mang theo tín hiệu cần truyền khi biên độ của sóng mang cao tần

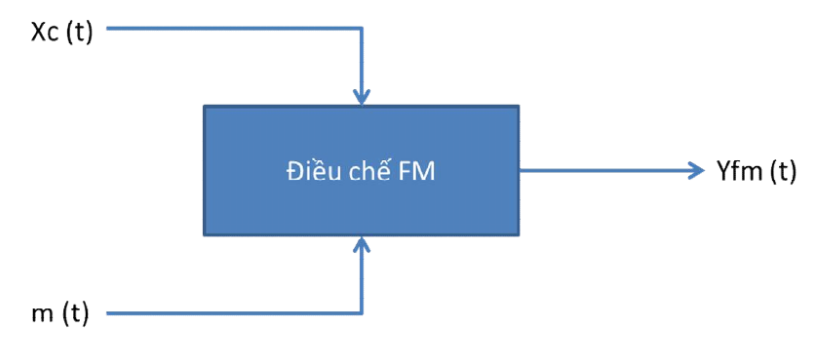
không thay đổi, đó là kỹ thuật điều chế tần số. Và điều chế biên độ của sóng mang

theo tín hiệu cần truyền mà tần số sóng mang vẫn giữ nguyên. Ngoài ra còn nhiều

phương pháp điều chế khác, như điều chế pha, điều chế mạch xung, điều chế biên

mã, điều chế đơn biên...

Tín hiệu điều chế FM :



Hình 1. 27

Tín hiệu sóng mang cao tần chưa điều chế là đơn hài, xác định bởi:

 (1.1)

Trong đó: 

là pha tức thời của dao động cao tần, xác định trạng thái tín hiệu tại thời điểm t.

* là tần số sóng mang
* là pha ban đầu.

Giữa tần số và pha có quan hệ:

 (1.2)

 (1.3)

* là hệ số

Khi đó tín hiệu điều chế FM có dạng:



Độ dịch tần số (frequency deviation): là lượng mà tần số sóng mang sai lệch

so với tín hiệu sóng mang chưa được điều chế. Đối với một hệ thống FM, độ dịch

tần số cho phép cực đại là độ lệch tần số lớn nhất kể từ tần số trung tâm, nó là một

đại lượng quan trọng và được xem như là tốc độ dịch hệ thống fd (rated system deviation). Khi fd được xác lập nó sẽ xác định biên độ của điều chế tần số. Ở hầu hết mọi thời điểm, điện áp điều chế đều nhỏ hơn giá trị cực đại này và khi đó, độ lệch tần số là 

Chỉ Số Điều Chế (modulation index) là độ lệch pha đỉnh của tín hiệu FM, ký

hiệu là mf.



Tỉ số độ lệch (deviation ratio): Khi một hệ thống FM được thiết kế, cần phải sử

dụng những giá trị cho phép tối đa cho cả độ lệch của sóng mang lẫn tần số tín hiệu

điều chế. Do đó, chỉ số điều chế được biết như là độ lệch D:



Độ lệch của một hệ thống FM xác định là không đổi, trong khi đó chỉ số điều chế thay đổi không ngừng cùng với sự thay đổi của điện áp và tần số tín hiệu.

**c) Phổ của tín hiệu điều tần**

Tín hiệu điều chế và pha ban đầu sóng mang θ = 0. Tín hiệu FM có dạng như sau:



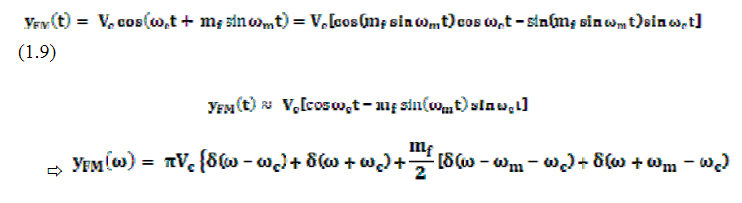
Với:

 :chỉ số điều chế

 :độ di tần

+ FM dải hẹp (NBFM: )

Nếu độ di tần nhỏ (mf <0.25), ta có:

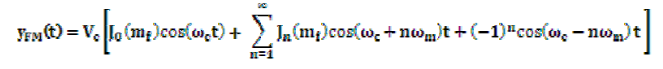
****

Phổ tín hiệu FM dải hẹp gồm sóng mang và hai biên tương tự AM

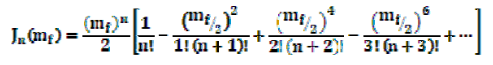
+ FM dải rộng (WBFM: wideband FM mf > 0.25)

****

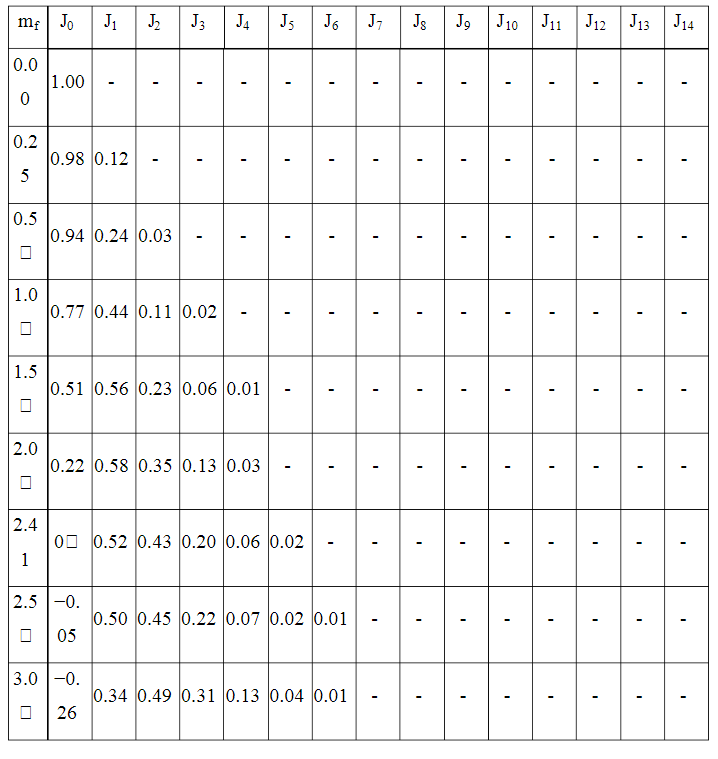
có thể khai triển theo các hệ số của hàm Bessel như sau:

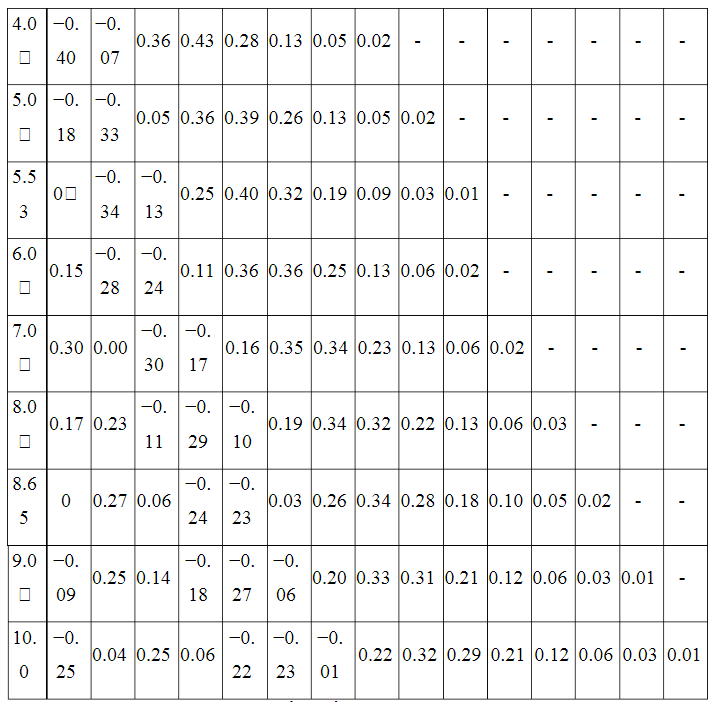
(1.11)

Biên độ của chúng tỷ lệ với hàm Bessel bậc n:

(1.12)

Bảng 1.1 Các hệ số của hàm Bessel tương ứng với một số chỉ số điều chế mf





+Băng thông của tín hiệu điều chế FM

Về lý thuyết độ rộng băng thông cao tần tín hiệu FM vô cùng lớn, tuy nhiên thực

tế quy định giới hạn băng thông FM đến thành phần phổ biên 

Băng thông này tính theo công thức: BFM ≈ 2(Δf + fm) = 2(mf + 1)fm, với fm

là tần số tín hiêu điều chế tần thấp băng gốc.

### 1.5.3. Hệ thống RDS (Radio Data System)

Hệ thống truyền dữ liệu vô tuyến RDS (Radio Data System) là một công nghệ được phát triển để cung cấp dịch vụ dữ liệu giá trị gia tăng sử dụng cho các trạm phát vô tuyến FM có tần số từ 87.5MHz đến 108 MHz. Mục đích của RDS là làm tăng thêm chức năng của hệ thống truyền dẫn vô tuyến, đặc biệt là khi người sử dụng thu tín hiệu vô tuyến khi đang di động. RDS chuẩn hóa một số loại thông tin được truyền, bao gồm thời gian, mã trạm và thông tin chương trình. Đài phát thanh có thể sử dụng RDS để gửi đi các bản tin quảng bá ngắn gọn cho người sử dụng hiển thị trên màn hình như thông tin thời tiết, giá cả, tình hình giao thông, thông tin quảng cáo. Đặc biệt có thể phát thanh chia theo từng khu vực và nội dung phát thanh không bị ảnh hưởng. Sóng FM sử dụng băng tần UHF (tần số từ 87.5 tới 108 Mhz) cho phép phủ sóng trong vòng bán kính từ 80 tới 160 km. Trạm phát sóng FM sử dụng phương pháp đa truy nhập theo tần số (FDMA) để chia sẻ băng tần UHF, một trạm phát FM có thể truyền một hoặc nhiều kênh.

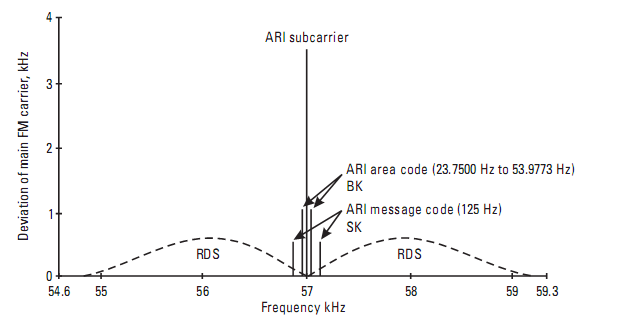
Hệ thống này cho phép các trạm phát sóng truyền thêm các loại thông tin thông qua các tín hiệu số được mã hóa, các tín hiệu này sau đó được nhận và hiển thị trên thiết bị thu tín hiệu. Nhờ đó mà có thể hiển thị được trên máy thu tiêu đề, tên ca sĩ hoặc tên bài hát đang phát, các thông tin về giao thông, số điện thoại của nhà quảng cáo,… trong khi vẫn phát các chương trình hiện tại mà không làm ảnh hưởng đến chất lượng của chương trình đang phát.

RDS được phát triển chủ yếu tại châu Âu, nơi mà nó được hình thành và triển khai. Ý tưởng cơ bản về RDS được đưa ra bởi nhà cung cấp dịch vụ truyền hình của Pháp ORTF, nay là đài truyền hình Pháp. Đề xuất này được bắt nguồn từ một hệ thống xác định giao thông công cộng gọi là ARI, cùng được phát triển ở Đức bởi trung tâm nghiên cứu phát thanh truyền hình công cộng IRT và nhà sản xuất radio cho xe hơi Blaupunkt. Tại Đức, hệ thống này được phát triển để truyền các thông tin về giao thông đồng thời với tín hiệu phát thanh quảng bá FM. RDS sử dụng dải tần trong khoảng 55 KHz tới 59 KHz với phương pháp điều chế theo pha tín hiệu (PSK), cho tốc độ truyền 1187.5 bps. Nếu trừ đi các bit sử dụng để phát hiện, sửa lỗi và đồng bộ hóa thì tốc độ truyền thực tế khoảng 731 bps. Giao thức RDS được phát triển bởi Hiệp hội liên minh phát thanh châu Âu (EBU) và được công bố phiên bản đầu tiên vào năm 1984. Từ đó đã trở thành một tiêu chuẩn quốc tế được công nhận bởi tổ chức IEC(International Electrotechnical

Commission).

RDS hoạt động bằng cách chèn thêm dữ liệu số (data) vào tín hiệu băng cơ bản được sử dụng để điều chế sóng mang tần số vô tuyến. Phương thức này không làm nhiễu tín hiệu trong khi vẫn cho phép truyền dữ liệu tại tốc độ thích hợp. Cùng với việc sóng mang phụ họat động tại các tần số hài của tín hiệu pilot, việc này sẽ giảm thiểu xuyên nhiễu gây ra cho các tín hiệu audio.

Việc lựa chọn sóng mang phụ rất quan trọng trong việc đáp ứng yêu cầu làm giảm thiểu nhiễu tín hiệu dữ liệu vào các kênh âm thanh ở các máy thu hiện nay. Một tham số quan trọng khác để đạt được mục đích này là mức xâm nhập của dữ liệu. Mức xâm nhập của dữ liệu càng cao thì dịch vụ dữ liệu càng thô (more rugged); tuy nhiên dưới điều kiện truyền dẫn đa đường, nhiễu ở các kênh âm thanh cũng sẽ tăng lên. Các thử nghiệm nhận thấy sóng mang phụ có độ lệch tối thiểu là ±1 kHz, và thường được chọn ở mức ±2 kHz. Tại mức này, không phát hiện thấy nhiễu từ kênh dữ liệu trong quá trình nghe radio.



Hình 1. 28:

Hình 1.28 mô tả chi tiết hơn phổ dữ liệu RDS trong hệ thống ARI. Phổ tín hiệu RDS có hình dạng như vậy không ảnh hưởng gì tới các tín hiệu ARI. RDS sử dụng một lược đồ điều chế mà trước đây được phát triển để sử dụng cho hệ thống MBS của Thụy Điển và sử dụng sóng mang phụ 57kHz được nén điều chế biên độ hai băng tần bên và sử dụng phương pháp mã hóa dữ liệu lưỡng pha (thường được gọi là mã hóa “Manchester”). Tác dụng của loại mã hóa và điều chế này là tạo ra một phổ có dạng bậc thang như hình 8, giúp tín hiệu ARI vẫn không bị ảnh hưởng bởi RDS. Vì vậy , hai hệ thống có thể dễ dàng tồn tại song song. Việc sử dụng tín hiệu dữ liệu được mã hóa 2 pha cũng giúp hệ thống này tương thích với các tín hiệu chương trình âm thanh vì các thành phần có liên quan xung quanh tần số 57 kHz sẽ gây nhiễu xuyên kênh tại các máy thu sử dụng bộ giải mã dùng vòng khóa pha (PLL- phase-locked loop), một kỹ thuật giải điều chế thường được sử dụng ngày nay .

Năm 1974, hệ thống RDS thử nghiêm này được Liên minh phát thanh truyền hình châu Âu EBU quan tâm, khi Ủy ban kỹ thuật của họ đề xuất tiếp tục nghiên cứu phát triển dự án này của Đức để truyền đồng thời cả các thông tin giao thông và các dữ liệu khác nữa. Thử nghiệm này nhằm mục đích tìm ra một công nghệ linh hoạt hơn, có khả khả năng ứng dụng cho tất cả các trạm phát FM, đồng thời cho phép tự động điều chỉnh một máy thu khi nó ra khỏi vùng phủ sóng của một trạm phát để có thể thu được tín hiệu tốt nhất trong một mạng các máy phát phát sóng cùng một chương trình phát thanh, đồng thời có thể cung cấp các tính năng như thông tin về chương trình,…Hệ thống này dần được hoàn thiện để đáp ứng một số yêu cầu về chức năng như:

1. Các tín hiệu chứa dữ liệu vô tuyến phải tương thích với nhau, chúng phải không gây ảnh hưởng đến việc nhận các tín hiệu chương trình âm thanh tại các đầu thu hiện đang sử dụng hoặc tới hoạt động của các máy thu sử dụng hệ thống ARI.

2. Trong cùng một vùng phủ sóng thì các tín hiệu mang dữ liệu phải có khả năng được thu tương tự như các tín hiệu mang chương trình FM chính.

3. Tốc độ dữ liệu có thể sử dụng được cung cấp bởi kênh dữ liệu phải hỗ trợ được các yêu cầu cơ bản của trạm phát và nhận dạng chương trình, và đáp ứng được cho sự phát triển của hệ thống trong tương lai.

4. Định dạng tin nhắn (message format) phải linh hoạt, cho phép chỉnh sửa nội dung tin nhắn nhằm đáp ứng nhu cầu của các trạm phát thanh vào bất cứ lúc nào.

5. Hệ thống này phải có thể thu được từ các máy thu rẻ tiền.

Những yêu cầu này ảnh hưởng đáng kể đến việc lựa chọn các tham số sẽ được điều chế và các đặc tính mã hóa băng cơ bản .

Sự phát triển rộng rãi trên toàn châu Âu kéo dài 10 năm với nhiều thử nghiệm và ít nhất đã có 5 giải pháp được đề xuất. Hệ thống điều chế được lấy từ một hệ thống phân trang Thụy Điển đã được đề xuất trước đây và công nghệ mã hóa băng cơ bản (baseband) được phát triển bởi tập đoàn phát thanh truyền hình Anh BBC và Tập đoàn phát thanh Ailen IRT. Mọi công nghệ đều được EBU phối hợp cẩn thận, và ở giai đoạn phát triển cuối cùng, ngành công nghiệp sản xuất radio cho xe hơi tại châu Âu đã được mời tham gia nhiều thử nghiệm. Hai trong số các tiêu chí quan trọng nhất phải đáp ứng là các dữ liệu được thêm vào chương trình phát thanh quảng bá FM phải hoàn toàn không nghe được, ngay cả trong chế độ nghe quan trọng nhất (most critical listening mode), ví dụ sử dụng tai nghe và chỉ cho phép nhiễu tần số radio gây ra bởi tín hiệu RDS là không đáng kể. Vào tháng 3/1983, các đặc tính kỹ thuật đầu tiên của hệ thống RDS đã được EBU công bố. Sau đó các công ty sản xuất radio cho xe hơi tại châu Âu đã thoả thuận với các công ty phát thanh truyền hình là sẽ nhanh chóng thực hiện các hệ thống trên tất cả các mạng của họ để ngành công nghiệp sản xuất radio công nghệ RDS châu Âu có thể ra mắt thị trường vào giữa năm 1987. Tuy nhiên, việc áp dụng công nghệ RDS trong các máy thu radio lại khá chậm, những chiếc radio trên xe hơi dùng công nghệ RDS đầu tiên khá đắt. Tuy nhiên, trong vòng 10 năm, đã có hơn 50 triệu radio RDS cho xe hơi được bán ra, và đến năm 2004, đã đạt tổng số 200 triệu chiếc.

Tiêu chuẩn về RDS sau đó được phát triển vào năm 1991 với việc thêm vào chức năng thay đổi tần số luân phiên và được xuất bản dưới sự bảo hộ của Ủy ban châu Âu cho các tiêu chuẩn kỹ thuật điện CENELEC (European Committee for Electrotechnical Standardization). Tiêu chuẩn của CENELEC được cập nhật vào năm 1992, trong đó thêm kênh hội thoại giao thông (Traffic Message Channel) và năm 1998 với các ứng dụng dữ liệu mở, và vào năm 2000, RDS đã được xuất bản rộng rãi khắp thế giới bằng tiêu chuẩn IEC 62106.

Tại Bắc Mỹ, ý tưởng phát triển hệ thống này được tiếp nhận và Cộng đồng hệ thống âm thanh quốc gia Hoa Kỳ (US National Radio Systems Committee) đã phát hành phiên bản của riêng họ - RBDS (Radio Broadcast Data System) năm 1992. Cả 2 phiên bản RDS và RBDS đều truyền dữ liệu tại tốc độ 1187,5 bit/s trên sóng mang phụ 57 kHz, do đó có chính xác 48 chu kỳ của sóng mang trong mỗi bit dữ liệu (cycles of subcarrier during every data bit).

Kể từ năm 2005, ngành công nghiệp sản xuất máy thu FM RDS đã bùng nổ thực sự nhờ sự ra đời của một thế hệ mới các IC FM RDS rất rẻ tiền và kích thước rất nhỏ gọn, làm cho công nghệ RDS cũng có thể sử dụng cho các thiết bị cầm tay như máy nghe nhạc và điện thoại di động. Kể từ đó, mỗi năm có thêm 200 triệu thiết bị được sản xuất và bán ra thị trường. Ngoài ra dự án phát triển RDS\_TMC khu vực châu Âu đã dẫn đến việc sử dụng rộng rãi RDS-TMC, ngày nay được sử dụng nhiều cho các radio dùng cho xe hơi và trong các thiết bị điều hướng, đã có một tác động đáng kể vào sự thành công của công nghệ RDS.

**a) Tính năng RDS**

Hiển thị radio RDS: cuộn tên trạm (PS) và cuộn văn bản radio (RT).

RDS có khả năng cung cấp nhiều dịch vụ, nhưng những dịch vụ này thường được các đài truyền hình khai thác, đặc biệt là ở Pháp . Trong số các dịch vụ phổ biến nhất, chúng tôi tìm thấy:

*PS (Dịch vụ chương trình):*

Tên của trạm, bao gồm tám ký tự chữ và số, có thể được hiển thị trên màn hình máy thu. Trừ những trường hợp đặc biệt, tất cả các trạm đều cung cấp dịch vụ này. Tiêu chuẩn RDS nói rằng tám ký tự phải được cố định và thể hiện tên của trạm 6 . Trên thực tế, một số radio đã chuyển hướng dịch vụ này để truyền tải thông tin động. Tại Pháp, CSA cấp phép cho thử nghiệm thực hành này cho đến cuối năm 2009. Tuy nhiên, RDS bao gồm một dịch vụ phù hợp với thông tin động, radiotexte (xem infra).

*AF (Tần suất thay thế) :*

Các máy phát phát danh sách tần số của các máy phát lân cận của cùng một trạm. Do đó, radio xe hơi có thể tìm kiếm tần số tốt nhất có sẵn. Do đó, bạn có thể nghe cùng một trạm từ đầu này sang đầu kia mà không thay đổi tần số theo cách thủ công (tần số được "tải xuống" vào RAM của radio trên ô tô).

*CT (Giờ đồng hồ) :*

RDS cho phép truyền thời gian, và do đó cài đặt đồng hồ của máy thu. Dịch vụ này được cung cấp bởi nhiều trạm, nhưng không có gì đảm bảo độ tin cậy của thời gian truyền (một cách tốt cho các trạm là đồng bộ hóa bộ mã hóa RDS trên đồng hồ điều khiển vô tuyến , ví dụ như trên máy phát DCF77 của Frankfurt ở Đức Kopitz 2 ).

*TP (Chương trình giao thông) / TA (Thông báo giao thông) :*

TP là một lá cờ cho biết liệu trạm nhận được có khả năng đưa ra thông báo đường bộ hay không. Hầu như tất cả các đài phát hành cờ này, ngay cả khi họ không bao giờ phát sóng trong thực tế quảng cáo đường bộ. Thật vậy, nhiều đài phát thanh xe hơi bỏ qua trong các trạm chế độ tìm kiếm tự động nơi không có cờ TP ; do đó phát thải của nó được khuyến nghị 7 . Đối với một trạm mà chương trình phát sóng cờ TP, cờ TA chỉ ra rằng trạm truyền tại thời điểm quảng cáo xe buýt. Người nhận sử dụng mã này để tăng âm lượng hoặc, trong trường hợp radio xe hơi , để chuyển đổi giữa phát lại CD hoặc băng cassette và thu sóng radio.

*EON (Mạng khác nâng cao) :*

Thông tin EON được tham chiếu chéo giữa các chương trình khác nhau thuộc cùng một mạng. Mỗi trạm phát các tham chiếu của các trạm khác trong mạng: tên (PS), mã nhận dạng (PI), tần số (AF), loại chương trình (PTY), phổ biến thông tin giao thông (TP / TA). Điều này cho phép người nhận chuyển sang trạm khác khi quảng cáo trên đường được phát. Việc chuyển đổi chỉ kéo dài thời gian phát sóng thông báo; người nhận sau đó tính toán lại trên chương trình gốc. Ví dụ, ở Pháp, các bộ đàm của nhóm Radio France đề cập đến nhau, cũng như 107,7 MHz, tần số đường cao tốc. Do đó, khi một người lái xe nghe một trong những chiếc radio này, anh ta có thể hưởng lợi từ thông tin giao thông được phát trên bất kỳ thiết bị nào khác.

Hiển thị văn bản radio trong đài phát thanh trên xe hơi: khẩu hiệu của trạm KBPI ( khu vực Denver ), "KBPI Rocks the Rockies".

*RT (Văn bản vô tuyến) :*

Các radiotexte cho phép khuếch tán các văn bản thông qua RDS. Các văn bản trong câu hỏi sau đó có thể được hiển thị theo yêu cầu trên màn hình máy thu. Ví dụ như radiotexte được sử dụng để truyền tải các tiêu đề của các chương trình hoặc tác phẩm âm nhạc đang được phát sóng.

*RT + :*

RT + là một dịch vụ bổ sung cho radiotexte (RT) được giới thiệu vào năm 2008 trong phiên bản mới của tiêu chuẩn RDS, bao gồm việc gắn nhãn một số đoạn văn bản của tin nhắn radiotext với siêu dữ liệu mô tả bản chất của chúng. Ví dụ: có thể chỉ ra rằng một đoạn tin nhắn nhất định là tên bài hát, tên nghệ sĩ hoặc số điện thoại của radio. Do đó, các thiết bị đầu cuối có thể trình bày thông tin này một cách có cấu trúc. Đây là ví dụ trường hợp của thế hệ thứ năm iPod nano (phát hành vào tháng 9 năm 2009) mà sử dụng RT + để xác định các danh hiệu và các nghệ sĩ của bài hát trên đài phát thanh 8. Để đi xa hơn, một điện thoại di động được trang bị đầu thu radio có RT + có thể đề xuất tự động quay số của radio vì nó sẽ xác định nó là 9 như vậy .

*PTY (Loại chương trình) và PTYN (Tên loại chương trình)*:

Bạn có thể chỉ định loại chương trình phát từ 32 loại đặt trước (tính năng PTY). Một số máy thu cho phép quét chọn lọc các trạm được lưu trữ, tùy thuộc vào loại chương trình bạn thích. Một số trạm liên tục sửa đổi mã PTY của họ để phù hợp nhất với lượng khí thải của họ, nhưng những trạm khác không muốn chỉ định loại chương trình để chúng được đưa vào thường xuyên trong các lần quét. Nhờ dịch vụ liên kết PTYN, về mặt lý thuyết có thể tinh chỉnh loại chương trình bằng cách phát hành một tiêu đề trên tám ký tự (ví dụ: PTY tương ứng với loại "thể thao" chung, PTYN có chứa văn bản "bóng đá"). PTYN không được sử dụng trong thực tế.

Màn hình dịch vụ của đài phát thanh xe hơi, hiển thị mã PI của trạm đã nhận ( France Musique , mã PI F203 thập lục phân ), cũng như trạm quét (bigFM ở Saarland, mã PI 1B02).

*PI (Ấn định chương trình) và ECC (Mã quốc gia mở rộng) :*

Mã PI là một mã duy nhất được gán cho mỗi trạm, cho phép người nhận xác định mã đó chắc chắn trong quá trình thay đổi tần số. Mã PI là mã 16 bit, 4 mã đầu tiên xác định quốc gia 10 . Do đó, điều này chỉ cung cấp 16 khả năng cho sự lựa chọn của quốc gia: tính duy nhất của mã IP thực sự chỉ có được đối với các quốc gia láng giềng [ref. cần thiết] . Do đó, mã PI được bổ sung bởi mã quốc gia ECC: cặp PI + ECC là một định danh thực sự duy nhất của một trạm ở cấp độ toàn cầu;

*TMC ( Kênh tin nhắn giao thông ) :*

RDS hiện là kênh truyền tải chính cho dữ liệu thông tin lưu lượng có cấu trúc TMC.

*Dịch vụ bổ sung :*

RDS có thể được sử dụng cho các mục đích khác: truyền dữ liệu công cộng (TDC, kênh dữ liệu minh bạch ) hoặc riêng tư (IH, ứng dụng nội bộ ), phân trang , các dịch vụ công khai khác và đăng ký hợp lệ (ODA, ứng dụng dữ liệu mở ) .

**b) Mô tả kỹ thuật**

+Chế độ điều chế (lớp vật lý)

Phổ của phát sóng FM trước khi điều chế , với âm thanh nổi và RDS.

Phổ trong RDS2 (không có âm thanh) trước khi điều chế (không có âm thanh, chỉ có dữ liệu RDS).

Trong hệ thống RDS cơ bản (như được chỉ định trong những năm 1980), dữ liệu số điều chỉnh sóng mang con 57 kHz . Đây là bản hòa âm thứ ba của âm thử 19 kHz có trong các chương trình phát sóng stereo FM . Tại thời điểm thiết kế RDS, sóng mang con 57 kHz đã được hệ thống ARI sử dụng ; RDS đã được thiết kế sao cho nó có thể được sử dụng cùng lúc với ARS (hai tín hiệu không can thiệp). Phiên bản 2018 của tiêu chuẩn cung cấp khả năng tăng tốc độ truyền bằng cách sử dụng ba sóng mang con bổ sung ở 66,5 kHz , 71,25 kHz và 76 kHz(Hệ thống "RDS2"). Việc điều chế và mã hóa được sử dụng trên các sóng mang con bổ sung này giống như trên sóng mang con "chính" ở 57 kHz .

Dữ liệu nhị phân được định dạng bởi một bộ lọc. Tín hiệu thu được điều biến sóng mang con bằng cách điều chế biên độ sóng mang (MAPS) bị triệt tiêu. Con số này thực hiện một điều chế bằng cách thay đổi giai đoạn nhị phân (BPSK).

Sóng mang con được đưa vào như một thành phần mới của tín hiệu ghép kênh của sóng vô tuyến. Nó nằm trong băng thông của máy phát và máy thu, nhưng nó hoàn toàn bên ngoài các tín hiệu âm thanh, và do đó không gây nhiễu âm thanh.

Các bit rate chọn để RDS là 1 187,5 bit mỗi giây. Tốc độ này được chọn vì nó là thương số của 48 tần số của sóng mang ở mức 57 kHz : do đó, một đồng hồ duy nhất có thể được sử dụng để tạo sóng mang và lấy mẫu dữ liệu, cả trên máy phát Chỉ trên máy thu.

Trước khi điều chế, dữ liệu nhị phân được mã hóa khác nhau để tín hiệu không nhạy cảm với các nghịch đảo.

**c) Cấu trúc của dữ liệu nhị phân (lớp liên kết)**

+ Cấu trúc chung của một nhóm RDS.

Do chế độ truyền ( phát mà không có kênh trả về), điều đặc biệt quan trọng là dữ liệu RDS được kèm theo thông tin đồng bộ hóa, phát hiện lỗi và sửa lỗi. Với mục đích này, 10 bit dự phòng được truyền sau mỗi từ 16 bit thông tin hữu ích. Do đó, dữ liệu đồng bộ hóa và phát hiện / sửa lỗi chiếm 38,5% dữ liệu được truyền.

Dữ liệu RDS được cấu trúc theo nhóm 104 bit. Một nhóm chứa 4 khối 26 bit mỗi nhóm (một từ thông tin 16 bit, 10 bit dự phòng). Trong một nhóm, chúng tôi biểu thị các khối bằng 1, 2, 3 và 4.

Mã được sử dụng để phát hiện và sửa lỗi Kopitz 3 là mã tuần hoàn có đa thức trình tạo là:

{\ displaystyle g (x) = x ^ {10} + x ^ {8} + x ^ {7} + x ^ {5} + x ^ {4} + x ^ {3} +1}{\ displaystyle g (x) = x ^ {10} + x ^ {8} + x ^ {7} + x ^ {5} + x ^ {4} + x ^ {3} +1}.

Trước khi truyền, N 1 được thêm vào các khối (trên 26 bit) và chính xác hơn là 10 bit điều khiển, một từ vị trí ( từ bù ) dành riêng cho khối được đề cập trong nhóm (từ A cho nhóm 1, B cho nhóm 2, C hoặc C 'cho nhóm 3, D cho nhóm 4). Từ này cho phép người nhận đồng bộ hóa trên luồng dữ liệu nhị phân, không chỉ ở cấp độ khối, mà đặc biệt là ở cấp độ nhóm. Từ quan điểm của người nhận, các từ vị trí được coi là một lỗi kênh. Các giá trị của chúng được chọn để tránh nhầm lẫn chúng với các lỗi từ 5 bit trở xuống.

Khi tiếp nhận, để đồng bộ hóa máy thu liên tục tính toán hội chứng của 26 bit cuối cùng nhận được. Khi nó ở cuối khối và trong trường hợp không có lỗi, nó sẽ tìm thấy một hội chứng null nếu từ thay đổi không được thêm vào. Trong thực tế, anh ta tìm thấy một đặc điểm hội chứng của khối (A, B, C, C 'hoặc D), có thể được suy ra từ từ thay đổi tương ứng. Bằng cách nhận ra hội chứng đặc trưng này, người nhận có được đồng thời hóa đồng bộ khối và đồng bộ hóa nhóm. Sau khi đồng bộ hóa, người nhận có thể sử dụng mã để từ chối các khối lỗi và / hoặc có thể sửa lỗi.

Ví dụ, đối với khối 1, từ bù (được gọi là A) là 0011111100 và hội chứng đặc trưng tương ứng là 0101111111.

Do tốc độ bit là 1.187,5 bit / s , nó được phát khoảng 11,4 nhóm mỗi giây.

**d) Định dạng tin nhắn (Lớp phiên và lớp trình bày)**

Có 32 loại nhóm, được đánh số 0A, 0B, 1A, 1B, ..., 15B. Bất kể loại nhóm nào, do đó, có một định danh loại nhóm tại một vị trí cố định, trên 5 bit. Chữ cái (A hoặc B) được gọi là phiên bản nhóm. Do đó, có thể xem xét rằng có 16 loại nhóm, mỗi loại có sẵn trong phiên bản A hoặc B.

Các nhóm được thiết kế để truyền đạt thông tin quan trọng nhất có thể. Ví dụ: chỉ báo TP (chương trình có khả năng phát thông báo đường bộ), PI (nhận dạng trạm) và PTY (nhận dạng loại chương trình) được bao gồm trong mỗi loại nhóm có thể. Do đó, một người nhận nhận được khối bù A biết rằng đó là khối số 1 trong một nhóm và biết rằng nó chứa mã PI, bất kể phần còn lại của nhóm (có thể, có thể, có thể không được nhận chính xác, mà không làm phiền việc nhận mã PI). Thông tin này được truyền trong tất cả các nhóm là những thông tin cho phép tìm kiếm các chương trình: tìm kiếm một chương trình nhất định nhờ mã PI, tìm kiếm

Thông tin chi tiết chung cho tất cả các nhóm. Các khu vực nở tương ứng với các lĩnh vực tùy thuộc vào loại nhóm.

Vì mã PI được coi là đặc biệt quan trọng, các nhóm phiên bản B mang nó hai lần: một lần trong khối 1, như trong tất cả các nhóm, nhưng cũng một lần trong khối 3. Bằng cách phát sóng các nhóm loại B, nó là do đó có thể tăng gấp đôi tần số truyền của mã PI, gây bất lợi cho băng thông được phân bổ cho thông tin khác. Ý tưởng đằng sau các nhóm phiên bản B là cải thiện việc nhận mã PI ngay cả khi các nhóm được nhận không đầy đủ (ví dụ, khối 1 bị thiếu). Tuy nhiên, trong sơ đồ tổng quát, cần phải nhận chính xác khối 2 để xác định loại nhóm và do đó để giải thích các khối sau. Điều này là để khắc phục sự cần thiết phải tiếp nhận chính xác khối 2 cho việc giải thích hai độ lệch có thể có cho khối 3 (C và C '). Phần bù C được sử dụng cho các nhóm trong phiên bản A, phần bù C 'cho các nhóm trong phiên bản B. Do đó, nếu người nhận nhận được một khối phần bù C', thì chắc chắn, như khi nhận được một khối bù A, chứa mã PI, bất kể nội dung của phần còn lại của nhóm. Nói chung, đối với một số lượng nhất định, các nhóm A và B mang cùng loại thông tin, với các chi tiết bổ sung có sẵn trong phiên bản A. Tuy nhiên, các nhóm phiên bản B được sử dụng rất ít trong thực tế. Chỉ có 14B là thường xuyên, tuy nhiên không phải vì sự khuếch tán kép của mã PI, mà bởi vì nó khuếch tán thông tin không có sẵn trong 14A.

Để minh họa hiến pháp của các nhóm RDS, chúng ta có thể phân tích nhóm loại 0A, thường xuyên nhất vì nó mang thông tin cơ bản của RDS (tần số thay thế, tên của trạm, chỉ báo thông tin đường bộ TA). Hiến pháp của các nhóm khác tuân theo các nguyên tắc tương tự.

Chi tiết về nhóm 0A, phổ biến nhất.

Sau phần cố định chung cho tất cả các nhóm, chúng tôi tìm thấy:

* một bit Thông báo giao thông (TA), được đặt thành 1 khi thông báo giao thông đang được phát.
* một chút MS (Âm nhạc / Bài phát biểu): 0 trong khi nói chương trình, 1 khi phát nhạc.
* hai trường 8 bit trong khối 3, mỗi trường có thể mã hóa tần số xen kẽ, theo bảng mã được chỉ định trong tiêu chuẩn.
* hai trường 8 bit trong khối 4, mã hóa hai ký tự từ tên trạm (Dịch vụ chương trình, PS), trong số tám trường. Tên của trạm được truyền bốn lần, nhờ bốn phân đoạn của hai ký tự, được truyền liên tiếp. Số phân đoạn, được gọi là địa chỉ , được mã hóa trên 2 bit ở cuối khối 2 (trường được đánh dấu @ trong sơ đồ). Các ký tự được mã hóa trên 8 bit, trong phiên bản mở rộng của mã ASCII thích nghi với các ngôn ngữ châu Âu.
* bit DI (Nhận dạng bộ giải mã) mang thông tin bổ sung, chẳng hạn như chỉ báo phát ở chế độ đơn âm hoặc âm thanh nổi hoặc ký tự tĩnh hoặc động của PTY. Bit DI mã hóa một trong bốn thông tin bit có số được mã hóa bởi trường địa chỉ.
* Trình tự phát sóng của các nhóm khác nhau có thể được để lại theo quyết định của đài truyền hình. Tuy nhiên, khuyến nghị rằng các nhóm quan trọng nhất, nghĩa là những nhóm có chứa thông tin cơ bản, nên được gửi thường xuyên hơn. Ví dụ: tiêu chuẩn khuyến nghị phát sóng ít nhất bốn nhóm 0A mỗi giây.

Các loại nhóm phổ biến nhất là:

* 0A: thông tin cơ bản (tên trạm và tần số thay thế);
* 2A: vô tuyến điện;
* 4A: tín hiệu đồng hồ;
* 14A, 14B: tăng cường các mạng khác .

**e) Bộ mã hóa RDS**

Dữ liệu RDS được tạo bởi bộ mã hóa RDS . Các lập trình viên đầu tiên được sản xuất nội bộ bởi các đài truyền hình và sau đó một thị trường phát triển. Bắt đầu từ năm 1994, một tiêu chuẩn để giao tiếp với các lập trình viên RDS đã được phát triển bởi Diễn đàn RDS: UECP, cho Giao thức truyền thông mã hóa toàn cầu. Giao thức này cho phép kiểm soát một cách thống nhất các bộ mã hóa RDS khác nhau từ các nhà sản xuất khác nhau. Phiên bản mới nhất của UECP là từ tháng 2 năm 2010.

## **1.6. Nghiên cứu lí thuyết hệ thống bảo mật bằng One Time Password (OPT) và ứng dụng trong hệ thống truyền thông không dây đồng nhất 3 cấp Vũ D16**

### 1.6.1. Tổng quan về OTP

**a) Otp- One Time Password là gì ?**

Mã OTP là từ viết tắt của One Time Password. Có nghĩa là mật khẩu sử dụng một lần. Mã xác thực OTP là một chuỗi số hoặc một chuỗi kết hợp cả số với ký tự. Nhưng khác mật khẩu thông thường, mã xác thực OTP được tạo ra ngẫu nhiên không phải từ người dùng, chỉ sử dụng được một lần và sau đó không còn tác dụng. Thậm chí, thời hạn của mật khẩu OTP thường rất ngắn, có thể chỉ sau 30 giây, 60 giây hay một vài phút, nó sẽ vô tác dụng và lại được thay thế bằng mã mới. OTP sẽ giảm thiểu nguy cơ bị đánh cắp dữ liệu,cung cấp sự bảo vệ tốt hơn nhiều cho các tài khoản ngân hàng trực tuyến, mạng công ty và các hệ thống khác có chứa dữ liệu nhạy cảm. Nó cung cấp kỹ thuật bảo mật nâng cao hơn so với mật khẩu tĩnh (Không thay đổi qua các phiên đăng nhập khác nhau). OTP hoạt động thông qua các thuật toán ngẫu nhiên, luôn được tạo mới và ngẫu nhiên với mỗi phiên đăng nhập hoặc giao dịch. Vì vậy, tin tặc hay cracker không thể đoán được mật khẩu kế tiếp.

**b) Các loại mã OTP được dùng phổ biến hiện nay**

Hiện nay có 3 hình thức cung cấp mã OTP chủ yếu gồm:

***SMS OTP :***

Mã OTP sẽ được gửi bằng tin nhắn SMS về số điện thoại đã đăng ký. Để thực hiện được giao dịch bạn cần phải nhập mã OTP được gửi về số điện thoại đã đăng ký. Đa số các ngân hàng tại Việt Nam hiện nay đều có sử dụng mã OTP theo hình thức này.

Hình thức này không chỉ được các ngân hàng sử dụng mà cả các công ty công nghệ lớn trên thế giới như Google, Facebook cũng áp dụng để tạo lớp bảo mật thứ hai cho tài khoản của bạn. Và lớp bảo vệ này sẽ xuất hiện khi phát hiện bất kỳ hoạt động không rõ ràng nào từ tài khoản của bạn. Một hạn chế của SMS OTP chính là người dùng không thể sử dụng được ở nơi không có sóng di động, hoặc di chuyển ra nước ngoài. Khi đó, các hình thức OTP khác sẽ được sử dụng.

***Tokey Key (Tokey Card) :***

Đây là thiết bị có thể giúp tạo mã OTP, nó có thể sinh ra tự động sau mỗi phút mà không cần kết nối internet. Mỗi tài khoản cần đăng ký Tokey Key riêng cho mỗi tài khoản, và sau một thời gian quy định thì ngân hàng sẽ đổi Tokey Key của bạn.

***Smart OTP ( Smart Token) :***

Hiện nay, tại Việt Nam thì có các ngân hàng như Vietcombank và TPBank đang sử dụng hình thức xác thực bằng Smart OTP hoạt động song song SMS OTP. Ngoài ra, Google cũng áp dụng Smart OTP và tạo ra một ứng dụng của riêng mình mang tên là Google Authenticator. Để sử dụng Smart OTP người dùng cần phải đăng ký với ngân hàng hoặc các nhà cung cấp dịch vụ. Ngoài ra, không thể có nhiều thiết bị sử dụng chung một ứng dụng tạo ra mã OTP.

**c) Nguyên lý hoạt động**

Sau khi dã dăng ký dịch vụ, mỗi lần muốn đăng nhập (log in), người dùng sẽ được cung cấp một mật khẩu tạo ra bởi đầu đọc và thẻ thông minh hay thiết bị tạo mật khẩu cầm tay (token) nhờ vào kết nối internet với máy chủ cung cấp dịch vụ OTP; hoặc cũng có thể thông qua thẻ OTP được tạo sẵn hay điện thoại di động. Mật khẩu này sẽ tự mất hiệu lực sau khi người dùng đăng xuất (log out) ra khỏi hệ thống. Như vậy, nếu bị lộ mật khẩu thì người có được mật khẩu đó cũng không thể dùng được, và do đó giải pháp OTP có tính bảo mật cao.

Quá trình tạo mật khẩu mới sẽ lặp lại mỗi lần người dùng đăng nhập vào hệ thống được bảo mật bằng OTP. Công nghệ OTP được dùng nhiều trong chứng thực trực tuyến (thương mại trực tuyến). Hiện nay người dùng các thiết bị cầm tay như iPhone, Blackberry cũng có thể tự cài đặt cơ chế bảo mật OTP bằng các chương trình như VeriSign, RSA SecureID hay SafeNet MobilePASS.

Sử dụng công nghệ OTP khiến cho việc truy cập bất hợp pháp đến những tài nguyên được giới hạn, ví dụ như một tài khoản máy tính trở nên khó khăn hơn. Thông thường, mật khẩu cố định có thể bị người dùng bất hợp pháp truy cập trong trường hợp họ có đủ thời gian và số lần truy cập.

**d) Các kỹ thuật mật mã sử dụng trong công nghệ OTP**

* Kiểu thứ nhất : Dùng một thuật toán để tạo ra một mật khẩu mới dựa trên mật khẩu trước đó, dựa trên phương pháp của Leslie Lamport là dùng một hàm một chiều (hàm f). Hệ thống OTP làm việc bằng cách khởi đầu với một giá trị s, sau đó sản sinh ra các mật khẩu với giá trị: f(s), f(f(s)), f(f(f(s))),.., rất nhiều lần tương đương với số lần sử dụng. Chú ý rằng, các mật khẩu này khi dùng thì được lấy theo thứ tự ngược lại. Nếu như một người nào đó thấy được mật khẩu sử dụng một lần, họ chỉ có thể truy cập được một phiên duy nhất, nó sẽ không thể lặp lại lần nữa khi phiên truy cập đó kết thúc. Để có được mật khẩu trong dãy từ mật khẩu của lần truy cập trước đó, người đó phải tìm cách để tính ngược được hàm nghịch đảo (f-1). Vì hàm f là hàm một chiều nên điều này cực kỳ khó để thực hiện. Nếu f là một hàm băm mật mã (cryptographic hash function) thì nó hầu như không thể nào tính toán được.
* Kiểu thứ hai được dựa trên sự đồng bộ thời gian giữa nhà cung cấp dịch vụ (authentication server) và khách hàng (client) được cung cấp mật khẩu. Mật khẩu sử dụng một lần kiểu đồng bộ thời gian luôn có mối quan hệ mật thiết với một thiết bị phần cứng gọi là token (ví dụ một người được cung cấp thiết bị token cá nhân để tạo một mật khẩu sử dụng một lần). Bên trong thiết bị này là 1 đồng hồ chính xác được đồng bộ với đồng hồ của nhà cung cấp dịch vụ. Trong hệ thống OTP này, thời gian là một phần quan trọng của thuật toán tạo ra mật khẩu, từ đó việc tạo ra mật khẩu mới dựa trên thời gian hiện tại khác với việc dựa trên mật khẩu trước đó hay là một từ khóa. Trường hợp này, điện thoại di động hoặc PDA cũng có thể được dùng để tạo ra OTP....
* Kiểu thứ ba cũng sử dụng một thuật toán nhưng mật khẩu thì được căn cứ dựa trên một giao thức sử dụng tham số gọi là “thách thức” (challenge). Ví dụ, một số ngẫu nhiên được chọn bởi máy chủ xác thực hoặc các chi tiết của cuộc giao dịch và/hoặc một bộ đếm.
* Ngoài ra còn một phương pháp khác là dùng một giao thức xác thực sử dụng mật mã đối xứng. Phương pháp này có thể áp dụng theo tiêu chuẩn ISO/IEC 9798- 2: Xác thực lẫn nhau dùng mật mã đối xứng. Mã khối đối xứng có thể dùng AES.

**e) Ưu điểm của công nghệ OTP**

* An toàn: Giải quyết tốt các vấn đề giả mạo, đánh cắp, Key logger. Đối với hai yếu tố xác thực, thiết bị này có thể được kết hợp với một mã PIN hoặc mật khẩu.
* Dễ dàng sử dụng: Việc nhận dạng và xác thực được thực hiện trong vài giây tránh được nguy cơ bị lỗi khi gõ các mã OTP dài qua các mã từ một thiết bị chứng thực vào một máy tính (Ví dụ OTP Token sử dụng màn hình hiển thị). Nó hoạt động với tài nguyên và đăng nhập được trên tất cả các nền tảng máy tính, và trình duyệt không cần phần mềm cài đặt Client. Nhanh chóng và tích hợp dễ dàng vào bất kỳ ứng dụng web nào (Windows, Linux, Mac, Internet Explorer, Firefox,...).
* Linh hoạt: Người dùng dễ dàng sử dụng cho các máy tính khác nhau và dễ mang theo bên mình.
* Mã nguồn mở: Sẵn sàng tích hợp với nhiều ứng dụng mã nguồn mở.

**f) Phương thức xác thực OTP**

* Đồng bộ hóa thời gian : Máy chủ đăng nhập biết rằng mật khẩu một lần là hợp lệ vì khóa USB tạo mật khẩu ngẫu nhiên dựa trên thời gian hiện tại.
* Mật khẩu trước đó : Máy chủ đăng nhập giữ một bản ghi mật khẩu cuối cùng được nhập bởi thiết bị OTP và có thể sử dụng thông tin này để xác thực mật khẩu một lần hiện tại.
* Phản hồi thách thức : Máy chủ đăng nhập có thể đưa ra một thử thách duy nhất cho khóa USB, trong đó chỉ có một phản hồi duy nhất.

**g) Ứng dụng công nghệ OTP vào lĩnh vực ngân hàng**

*Đặc điểm chính:*

Đối với các giao dịch xác minh đăng nhập với tài khoản ngân hàng điện tử , thanh toán trực tuyến , email hay mạng xã hội, mã OTP được coi là lớp bảo mật rất riêng biệt.

Mã này giúp ngăn chặn những rủi ro tấn công khi mật khẩu bị lộ hoặc tài khoản của khách hàng bị xâm nhập bởi hacker. Bạn không thể tạo ra và cũng không thể thay đổi mã. Điều này khác với bình thường khi tạo một tài khoản nào đó, mật khẩu sẽ do bạn tự chọn, đồng thời giúp tăng cường bảo mật đối với các giao dịch thanh toán online. Ngay cả khi bạn để lộ mã cũ và mật khẩu tài khoản ngân hàng sau khi giao dịch thì kẻ gian cũng không thể lấy được tiền của bạn.

*Làm thế nào để có mã OTP?*

Để có mã OTP khá đơn giản, giả sử bạn muốn chuyển tiền sang số tài khoản khác bằng Internet Banking, bạn tiến hành đăng nhập bình thường bằng tên tài khoản và mật khẩu tài khoản đã đăng ký. Sau khi bạn hoàn tất các thông tin giao dịch như người nhận, số tiền chuyển, hình thức chuyển,... ứng dụng Internet Banking của ngân hàng sẽ yêu cầu bạn kiểm tra lại thông tin giao dịch một lần nữa kèm theo nút "Lấy mã OTP".

Sau khi nhấn vào nút "Lấy mã OTP", một đoạn mã bằng số thường gồm 4 đến 6 ký tự (tùy ngân hàng) sẽ được gửi về điện thoại của bạn trong vòng vài phút. Lúc này bạn chỉ cần nhập mã OTP trên ứng dụng để xác nhận yêu cầu giao dịch lần cuối. Cách sử dụng mã OTP rất đơn giản và gần như là tự động, mã sẽ được ngân hàng gửi về số điện thoại đăng ký trên thông tin tài khoản ngân hàng.

Ngoài ra, khi nhập thông tin thanh toán online dùng thẻ ghi nợ, thẻ tín dụng, mặc định mã OTP cũng sẽ được gửi về số điện thoại để người dùng xác nhận giao dịch. Bằng cách này, dù bạn có bị mất thẻ thì kẻ gian cũng chưa chắc lấy được tiền của bạn.

*Sử dụng mã OTP như thế nào?*

Mã OTP là lớp bảo mật cuối cùng trước khi tiền được chuyển ra khỏi tài khoản của bạn. Vì vậy, hãy luôn kiểm tra kỹ lý do và số tiền (nếu có trong tin nhắn xác thực giao dịch) trước khi nhập mã OTP để thanh toán.

Với SMS OTP thì cách bảo mật tốt nhất là luôn đặt mật khẩu cho điện thoại nếu điện thoại của bạn có chức năng này. Thứ hai là đừng cho người mà bạn không cảm thấy tin tưởng mượn điện thoại. Và thứ ba là phải báo ngay cho ngân hàng để khóa tạm thời tính năng SMS OTP khi bạn mất điện thoại.

Với Token, bạn hãy giữ nó như giữ khóa cửa của gia đình bạn vậy. Hãy luôn mang theo bên mình. Nếu Token có thể đặt mật khẩu thì hãy đặt mật khẩu phức tạp một chút. Đừng sử dụng ngày tháng năm sinh hay những mật khẩu có thể dễ đoán (như abc123, qwerty...).

*Vì sao cần bảo vệ mã OTP cẩn thận:*

Đây là lớp bảo mật cuối cùng, để xác nhận thực hiện thanh toán nên mã OTP cần được bảo vệ. Hiện nay, mã OTP được dùng chủ yếu là SMS OTP nên bạn cần đặt mật khẩu cho điện thoại, để kẻ gian không lợi dụng sơ hở, lấy mã OTP từ điện thoại. Đồng thời cũng phải đặt mật khẩu cho ứng dụng.

Ngay khi bạn bị mất điện thoại hoặc mất thẻ tín dụng, bạn cần khóa thẻ hoặc tài khoản ngân hàng ngay bằng cách gọi trực tiếp cho trung tâm khách hàng của ngân hàng hoặc các đơn vị dịch vụ. Điều này sẽ đảm bảo an toàn cho tài khoản của bạn.

Mã OTP được xem là lớp bảo mật an toàn thứ hai. Với lớp bảo mật này, bạn hoàn toàn yên tâm rằng các hoạt động của bạn sẽ được bảo vệ. Tuy nhiên, cũng không ít trường để sơ hở để lộ OTP, nên bạn cũng bảo vệ lớp mật khẩu này.

*Smart OTP – Hình thức nhận mã chủ yếu hiện nay*

Smart OTP là một phần mềm được cài đặt trên thiết bị di động, cho phép người dùng chủ động lấy mã xác thực OTP. Smart OTP khắc phục được nhược điểm của phương thức xác thực qua tin nhắn SMS OTP và qua Token hiện tại đang áp dụng, hạn chế tối đa việc kẻ gian lợi dụng lỗ hổng bảo mật để tấn công tài khoản khách hàng.

Theo chuyên gia công nghệ ngân hàng, SMS OTP được gửi thông qua nhiều lớp trung gian và nhà mạng dẫn đến dễ bị thất thoát. Chẳng hạn, khi điện thoại của khách hàng bị cài phần mềm đọc trộm SMS, số OTP gửi đến điện thoại khách hàng đăng ký được tự động chuyển đến số điện thoại khác mà khách hàng không biết; Đơn giản hơn, khách hàng có thể bị kẻ gian chiếm quyền sử dụng Sim. SMS OTP còn bị lệ thuộc vào bảo mật của các nhà mạng, đòi hỏi khách hàng phải roaming khi đi nước ngoài . Còn Token Key là thiết bị rời có một thiết kế nhỏ gọn giống như USB nên rất dễ bị kẻ gian ăn cắp hoặc thất lạc. Một số Token Key có thiết kế đơn giản nên rất dễ bị xem trộm mã OTP, trong khi một số có thiết kế hiện đại hơn thì có thể khiến người dùng cảm thấy rườm rà khi mang bên mình.

Smart OTP là ứng dụng cung cấp mã OTP nên khách hàng sẽ chủ động lấy khi có nhu cầu giao dịch điện tử. Smart OTP được sinh ra ngay trên điện thoại của khách hàng và được mã hóa với hệ thống bảo vệ nhiều lớp phức tạp và khó có thể can thiệp được. Thiết bị di động cài đặt Smart OTP cũng không yêu cầu phải kết nối internet hay kết nối mạng viễn thông sau khi đã kích hoạt (Smart OTP hoạt động không cần có sim điện thoại, không cần mạng viễn thông nên không phải roaming khi giao dịch ở nước ngoài). Tuy nhiên, Smart OTP cũng có thể rủi ro đối với những khách hàng sử dụng điện thoại bị bẻ khóa máy hoặc tự ý cài thêm các phần mềm độc hại, không rõ nguồn gốc.

**h) Dịch vụ VOICE OTP là gì ?**

Voice OTP là dịch vụ gọi thoại để cung cấp mã OTP. Theo đó, hệ thống sẽ thiết lập để tự động gọi đến số điện thoại người dùng đã đăng ký để cung cấp mã OTP theo file ghi âm sẵn đã được cá nhân hóa kịch bản thoại. Trong khi yêu cầu bảo mật thông tin ngày càng tăng và được áp dụng phổ biến trên nhiều lĩnh vực, dịch vụ Voice OTP được ứng dụng nhằm giải quyết yêu cầu làm thế nào để giúp doanh nghiệp tiết kiệm chi phí với lượng giao dịch không lồ mà vẫn đảm bảo tính tiện lợi, nhanh chóng và bảo mật. Nếu thiết bị token phức tạp với chi phí sản xuất cao, SMS với chi phí khá lớn đối với các doanh nghiệp có lượng đăng nhập / giao dịch cao thì Voice OTP chắc chắc sẽ là một lựa chọn đáng cân nhắc với chi phí chỉ bằng một nửa.

**Ưu điểm của Voice OTP:**

* Tích hợp đơn giản: tương tự API gửi SMS mà khách hàng đang dùng. Khách hàng có thể tự thu âm và cá nhân hoá kịch bản thoại theo mong muốn một cách dễ dàng.
* Có thể đọc được cả chuỗi ký tự chữ và/hoặc số, số tiền tùy biến trong API.
* Có thể tuỳ chọn tự động lặp lại mã OTP X lần.
* Có thể tuỳ chọn tự động gọi lại sau X phút nếu user chưa bắt máy hoặc máy bận. Ngoài ra, hệ thống có thống kê tình trạng máy cuối: đang bận, từ chối cuộc gọi, số máy không tồn tại…
* Voice OTP còn giúp kiểm soát được chi phí bằng cách quản lý thời lượng ghi âm gọi ra. Vì vậy chi phí cực kì rẻ so với SMS và thiết bị token.
* Chỉ phát sinh phí khi gọi thành công. Các cuộc gọi không bắt máy hoặc máy bận hoàn toàn không bị tính phí. Thậm chí, có thể tuỳ chọn Khách hàng trả phí cho cuộc gọi hoặc Khách hàng trả phí cho cuộc gọi.
* Và Brand hoàn toàn có thể dùng đầu số CSKH hiện có để gọi ra, nếu người dùng đã quen với đầu số này.

### 1.6.2. Facebook Account Kit

**a) Giới thiệu chung**

Account Kit giúp người dùng đăng ký và đăng nhập ứng dụng một cách nhanh chóng và dễ dàng bằng việc sử dụng số điện thoại hoặc địa chỉ email của họ làm thông tin đăng nhập không cần mật khẩu. Account Kit được hệ thống gửi SMS và email của Facebook hỗ trợ mang lại hiệu quả tin cậy và mở rộng với phạm vi tiếp cận toàn cầu. Do sử dụng xác thực bằng email và số điện thoại, Account Kit không yêu cầu tài khoản Facebook và là phương thức thay thế lý tưởng để đăng nhập mạng xã hội.

Account Kit được xây dựng cho thế giới của điện thoại di động, cung cấp các phiên làm việc lâu dài, dễ dàng quản lý tài khoản, và đặc biệt là không cần phải nhớ password.

Khi một người đăng nhật bằng email của họ, Account Kit sẽ gửi một liên kết một lần (one-time link) đến địa chỉ email của người đó. SDK sẽ xác định khi nào thì địa chỉa email đó được xác thực (verified).

Khi người dùng đăng nhập bằng số điện thoại của họ, Account Kit sẽ hoặc là gửi SMS có mã xác nhận tới số đó hoặc là xác thực trực tiếp số điện thoại (xem Xác minh nhanh.

Luồng đăng nhập đăng nhập của Accout Kit bao gồm cả đăng ký và đăng nhập tài khoản. Nên chúng ta không cần phải kiểm tra rằng tài khoản đã tồn tài hay là phải tạo một luồng mới để đăng ký user. Sau khi đăng nhập hoặc đăng ký thành công, Account Kit cung cấp cho ứng dụng của bạn thông tin đăng nhập xác thức của người dùng.

Android SDK cung cấp một activity và tất cả những gì chúng ta cần làm là khởi tạo và start activity đó. Activity cung cấp result tương ứng với đăng nhập thành công hay thất bại. Và bạn hoàn toàn có thể custom lại giao diện màn hình đăng nhập.

**b) Cách thức hoạt động của Account Kit**

Account Kit tạo cơ sở dữ liệu cho ứng dụng. Bạn có thể truy xuất dữ liệu này bất cứ lúc nào thông qua REST API. Khi người dùng đăng nhập ứng dung, cơ sở dữ liệu này sẽ được cập nhật số điện thoại hoặc địa chỉ email cùng với Account IDs có thể sử dụng trong ứng dụng. Các Account IDs này là duy nhất cho ứng dụng của bạn. Nếu bạn cũng sử dụng Facebook Login cho ứng dụng của bạn thì bạn có thể yên tâm rằng sẽ không bao giờ có sự xung đột với ID của người dùng trong ứng dụng của Facebook. Account Kit có 2 luồng đăng nhập, phụ thuộc vào việc người dùng chọn xác thực bằng số điện thoại hay là email.

*Luồng xác minh bằng số điện thoại:*

1. Gọi API Account Kit bằng số điện thoại để khởi tạo đăng nhập hoặc đăng ký.
2. Server Account Kit sẽ gửi SMS kèm mã xác nhận để tiếp tục đăng nhập. Nếu người dùng không nhận được mã qua SMS, Account Kit cung cấp 2 tùy chọn dự phòng để người dùng lựa chọn:

* Gọi điện thoại — Người dùng có thể chọn nhận cuộc gọi điện thoại để lấy mã SMS. Để biết danh sách ngôn ngữ mà hỗ trợ cuộc gọi, hãy xem danh sách Ngôn ngữ được hỗ trợ cho cuộc gọi điện thoại.
* Thông báo trên Facebook — Nếu số điện thoại được liên kết với một tài khoản Facebook, người dùng có thể chọn nhận thông báo chứa SMS được gửi tới tài khoản đó.
* Account Kit cũng có thể xác minh trực tiếp số điện thoại mà không gửi mã SMS.

1. SDK xác minh mã xác nhận qua SMS.
2. Nếu ứng dụng đã bật Luồng mã truy cập ứng dụng, ứng dụng của bạn sẽ nhận được mã truy cập chứa account ID sau khi đăng nhập thành công. Nếu ứng dụng chưa bật Luồng mã truy cập ứng dụng, ứng dụng của bạn sẽ nhận được mã ủy quyền mà server của ứng dụng có thể sử dụng để yêu cầu mã truy cập một cách an toàn.

*Luồng xác minh bằng email:*

1. Gọi API Account Kit bằng địa chỉ email để khởi tạo đăng nhập hoặc đăng ký.
2. Server Account Kit sẽ gửi email xác nhận đến địa chỉ email.
3. SDK giám sát trạng thái của email xác nhận.
4. Nếu ứng dụng đã bật Luồng mã truy cập ứng dụng, ứng dụng của bạn sẽ nhận được mã truy cập chứa account ID sau khi đăng nhập thành công. Nếu ứng dụng chưa bật Luồng mã truy cập ứng dụng, ứng dụng của bạn sẽ nhận được mã ủy quyền mà server của ứng dụng có thể sử dụng để yêu cầu mã truy cập một cách an toàn.

# CHƯƠNG 2: KHẢO SÁT HIỆN TRẠNG HỆ THỐNG TRUYỀN THANH CỦA VIỆT NAM HIỆN NAY NÓI CHUNG VÀ ĐẮK LẮK NÓI RIÊNG

# CHƯƠNG 3: THIẾT KẾ MÔ HÌNH TỔNG QUÁT HỆ THỐNG TRUYỀN THÔNG KHÔNG DÂY ĐỒNG NHẤT 3 CẤP

## **3.1. Nghiên cứu, thiết kế mô hình cơ sở dữ liệu của hệ thống máy chủ nội dung Phúc D16**

### 3.1.1. Tổng quan về hệ quản trị cơ sở dữ liệu

**a) Ðịnh nghĩa**

Hệ quản trị cơ sở dữ liệu (Database Management System - DBMS): Là một hệ thống phần mềm cho phép tạo lập cơ sở dữ liệu và điều khiển mọi truy nhập đối với cơ sở dữ liệu đó. Trên thị trường phần mềm hiện nay ở Việt Nam đã xuất hiện khá nhiều phần mềm hệ quản trị cơ sở dữ liệu như: Microsoft Access, Foxpro, DB2, SQL Server, Oracle…

Hệ quản trị cơ sở dữ liệu quan hệ (Relation Database Management System - RDBMS) là một hệ quản trị cơ sở dữ liệu theo mô hình quan hệ.

**b) Các khả năng của hệ quản trị CSDL**

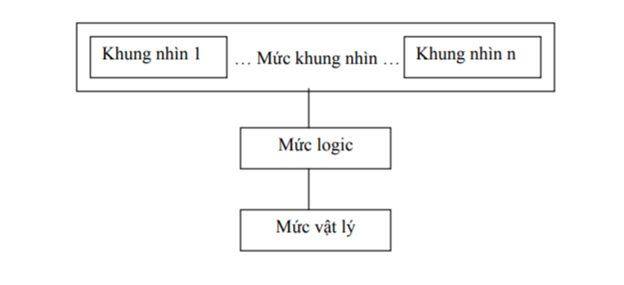
Có hai khả năng chính cho phép phân biệt các hệ quản trị cơ sở dữ liệu với các kiểu hệ thống lập trình khác:

* Khả năng quản lý dữ liệu tồn tại lâu dài: đặc điểm này chỉ ra rằng có một cơ sở dữ liệu tồn tại trong một thời gian dài, nội dung của cơ sở dữ liệu này là các dữ liệu mà hệ quản trị CSDL truy nhập và quản lý.
* Khả năng truy nhập các khối lượng dữ liệu lớn một cách hiệu quả. Ngoài hai khả năng cơ bản trên, hệ quản trị CSDL còn có các khả năng khác mà có thể thấy trong hầu hết các hệ quản trị CSDL đó là:
* Hỗ trợ ít nhất một mô hình dữ liệu hay một sự trừu tượng toán học mà qua đó người sử dụng có thể quan sát dữ liệu.
* Ðảm bảo tính độc lập dữ liệu hay sự bất biến của chương trình ứng dụng đối với các thay đổi về cấu trúc trong mô hình dữ liệu.
* Hỗ trợ các ngôn ngữ cao cấp nhất định cho phép người sử dụng định nghĩa cấu trúc dữ liệu, truy nhập dữ liệu và thao tác dữ liệu.
* Quản lý giao dịch, có nghĩa là khả năng cung cấp các truy nhập đồng thời, đúng đắn đối với CSDL từ nhiều người sử dụng tại cùng một thời điểm.
* Ðiều khiển truy nhập, có nghĩa là khả năng hạn chế truy nhập đến các dữ liệu bởi những người sử dụng không được cấp phép và khả năng kiểm tra tính đúng đắn của CSDL. Phục hồi dữ liệu, có nghĩa là có khả năng phục hồi dữ liệu, không làm mất mát dữ liệu với các lỗi hệ thống.

**c) Đặc điểm của một hệ quản trị CSDL**

*Sự trừu tượng hoá dữ liệu:*

Ðể cho hệ thống có thể sử dụng được, hệ quản trị CSDL phải tra cứu hay tìm kiếm dữ liệu một cách có hiệu quả. Ðiều này dẫn đến việc thiết kế các cấu trúc dữ liệu phức tạp để biểu diễn dữ liệu trong CSDL này. Người phát triển che dấu tính phức tạp này thông qua một số mức trừu tượng để đơn giản hoá các tương tác của người sử dụng đối với hệ thống.



Hình 3. 1

- Mức vật lý: Mức thấp nhất của sự trừu tượng mô tả dữ liệu được lưu trữ một cách thực sự như thế nào. Tại mức vật lý, các cấu trúc dữ liệu mức thấp phức tạp được mô tả chi tiết.

- Mức logic: Mức cao tiếp theo của sự trừu tượng hoá mô tả những dữ liệu nào được lưu trữ và các mối quan hệ nào tồn tại giữa các dữ liệu này. Mức logic của sự trừu tượng được xác định người quản trị CSDL, cụ thể phải quyết định những thông tin gì được lưu trữ trong CSDL.

- Mức khung nhìn: Mức cao nhất của sự trừu tượng mô tả chỉ một phần của toàn bộ CSDL. Mặc dù sử dụng các cấu trúc đơn giản mức logic, một số phức tập vẫn còn tồn tại do kích thước lớn của CSDL. Thực chất những người sử dụng chỉ cần truy nhập đến một phần CSDL, do vậy sự tương tác của họ với hệ thống này là đơn giản hoá và mức khung nhìn của sự trừu tượng được xác định. Hệ thống có thể được cung cấp nhiều khung nhìn đối với cùng một cơ sở dữ liệu.

*Ngôn ngữ cơ sở dữ liệu:*

Một hệ quản trị cơ sở dữ liệu thường cung cấp hai kiểu ngôn ngữ khác nhau đó là: ngôn ngữ mô tả sơ đồ cơ sở dữ liệu và ngôn ngữ biểu diễn các truy vấn và các cập nhật cơ sở dữ liệu.

- Ngôn ngữ định nghĩa dữ liệu (Data Definition Language - DDL):

+ Một sơ đồ CSDL đặc tả bởi một tập các định nghĩa được biểu diễn bởi một ngôn ngữ đặc biệt được gọi là ngôn ngữ định nghĩa dữ liệu. Kết quả của việc dịch các ngôn ngữ này là một tập các bảng được lưu trữ trong một tệp đặc biệt được gọi là từ điển dữ liệu hay thư mục dữ liệu.

+ Một từ điển dữ liệu là một tệp chứa các siêu dữ liệu có nghĩa là các dữ liệu về dữ liệu. Tệp này được tra cứu trước khi dữ liệu thực sự được đọc hay được sửa đổi trong hệ CSDL.

+ Cấu trúc và các phương pháp truy nhập được sử dụng bởi hệ CSDL được đặc tả bởi một tập các định nghĩa trong một kiểu đặc biệt của DDL là ngôn ngữ định nghĩa và lưu trữ dữ liệu.

- Ngôn ngữ thao tác dữ liệu (Data Manipulation Language - DML):

+ Các yêu cầu về thao tác dữ liệu bao gồm:

* Tìm kiếm thông tin được lưu trữ trong CSDL.
* Thêm thông tin mới vào CSDL.
* Xoá thông tin từ CSDL.
* Thay đổi thông tin được lưu trữ trong CSDL.

+ Một ngôn ngữ thao tác dữ liệu (DML) là một ngôn ngữ cho phép người sử dụng truy nhập hay thao tác dữ liệu được tổ chức bởi mô hình dữ liệu thích hợp. Có hai kiểu ngôn ngữ thao tác dữ liệu cơ bản:

* Các DML thủ tục đòi hỏi người sử dụng phải đặc tả dữ liệu nào cần tìm kiếm và tìm kiếm những dữ liệu này như thế nào.
* Các DML phi thủ tục đòi hỏi người sử dụng đặc tả dữ liệu nào cần tìm kiếm mà không phải đặc tả tìm kiếm những dữ liệu này như thế nào.

*Xử lý câu hỏi:*

Công việc của bộ xử lý câu hỏi là biến đổi một truy vấn hay một thao tác CSDL có thể được biểu diễn ở các mức cao thành một dãy các yêu cầu đối với các dữ liệu lưu trữ trong CSDL.

Thường phần khó nhất của nhiệm vụ xử lý câu hỏi là tối ưu hoá câu hỏi, có nghĩa là lựa chọn một kế hoạch tốt nhất đối với hệ thống lưu trữ để trả lời truy vấn này nhanh nhất.

*Quản trị giao dịch:*

Thông thường một số thao tác trên CSDL hình thành một đơn vị logic công việc. Ðiều này có nghĩa là hoặc tất cả các thao tác được thực hiện hoặc không thao tác nào được thực hiện. Hơn nữa sự thực hiện các thao tác này phải đảm bảo tính nhất quán của CSDL.

Một giao dịch là một tập hợp các thao tác mà xử lý như một đơn vị không chia cắt được. Các hệ quản trị CSDL điển hình cho phép người sử dụng một hay nhiều nhóm thao tác tra cứu hay thay đổi CSDL thành một giao dịch.

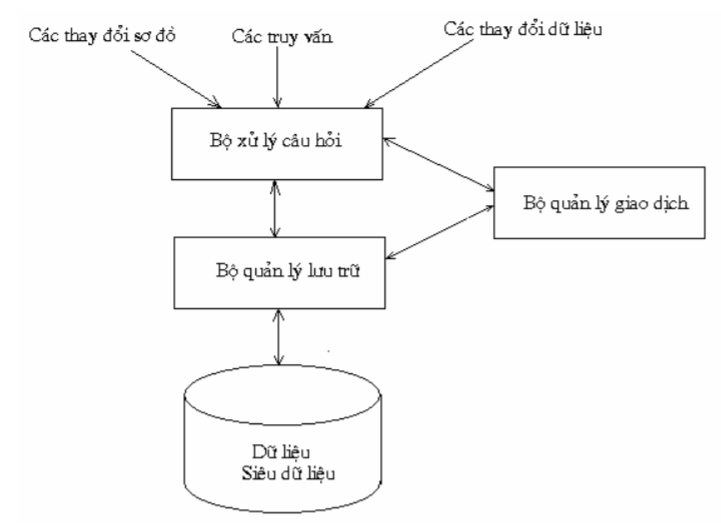
*Quản lý lưu trữ:*

Các CSDL thường đòi hỏi một khối lượng lớn không gian lưu trữ. Do bộ nhớ chính của máy tính không thể lưu trữ nhiều thông tin như vậy, các thông tin này được lưu trữ ở các thiết bị nhớ ngoài như đĩa cứng, đĩa mềm…

Khi xử lý, dữ liệu cần phải được di chuyển từ đĩa từ vào bộ nhớ chính; sự di chuyển này là khá chậm so với tốc độ xử lý của bộ nhớ trung tâm, do vậy các hệ CSDL phải tổ dữ liệu vật lý sao cho tốt, tối thiểu hoá số yêu cầu chuyển dữ liệu giữa đĩa từ vào bộ nhớ chính.

**d) Kiến trúc của một hệ quản trị CSDL**

Chúng ta sẽ phác thảo kiến trúc và thấy cách thức của một hệ quản trị CSDL điển hình. Ta có sơ đồ kiến trúc sau.



Hình 3. 2

- Dữ liệu, siêu dữ liệu: Ðáy kiết trúc là thiết bị nhớ ngoài lưu trữ dữ liệu và siêu dữ liệu. Trong phần này không chỉ chứa dữ liệu được trữ trong CSDL mà chứa cả các siêu dữ liệu, tức là thông tin cấu trúc của CSDL.

- Bộ quản lý lưu trữ: Nhiệm vụ của bộ quản lý lưu trữ là lấy ra các thông tin được yêu cầu từ những thiết bị lưu trữ dữ liệu và thay đổi những thông tin này khi được yêu cầu bởi các mức trên nó của hệ thống.

- Bộ xử lý câu hỏi: Bộ xử lý câu hỏi điều khiển không chỉ các câu hỏi mà cả các yêu cầu thay đổi dữ liệu hay siêu dữ liệu. Nhiệm vụ của nó là tìm ra cách tốt nhất một thao tác được yêu cầu và phát ra lệnh đối với bộ quản lý lưu trữ và thực thi thao tác đó.

- Bộ quản trị giao dịch: Bộ quản trị giao dịch có trách nhiệm đảm bảo tính toàn vẹn của hệ thống. Nó phải đảm bảo rằng một số thao tác thực hiện đồng thời không cản trở mỗi thao tác khác và hệ thống không mất dữ liệu thậm chí cả khi lỗi hệ thống xảy ra.

+ Nó tương tác với bộ xử lý câu hỏi, do vậy nó phải biết dữ liệu nào được thao tác bởi các thao tác hiện thời để tránh sự đụng độ giữa các thao tác và cần thiết nó có thể làm trễ một số truy vấn nhất định hay một số thao tác cập nhật để đụng độ không thể xảy ra.

+ Nó tương tác với bộ quản lý lưu trữ bởi vì các sơ đồ đối với việc bảo vệ dữ liệu thường kéo theo việc lưu trữ một nhật ký các thay đổi đối với dữ liệu. Hơn nữa, việc sắp thứ tự các thao tác một cách thực sự được nhật ký này sẽ chứa trong một bản ghi đối với mỗi thay đổi khi gặp lỗi hệ thống, các thay đổi chưa được ghi vào đĩa có thể được thực hiện lại.

- Các kiểu thao tác đối với hệ quản trị CSDL: Tại đỉnh kiến trúc, ta thấy có 3 kiểu thao tác:

+ Các truy vấn: Ðây là các thao tác hỏi đáp về dữ liệu được lưu trữ trong CSDL. Chúng được sinh ra theo hai cách sau:

* Thông qua giao diện truy vấn chung. Ví dụ: Hệ quản trị CSDL quan hệ cho phép người sử dụng nhập các câu lệnh truy vấn SQL mà nó được chuyển qua bộ xử lý câu hỏi và được trả lời.
* Thông qua các giao diện chương trình ứng dụng: Một hệ quản trị CSDL điển hình cho phép người lập trình viết các chương trình ứng dụng gọi đến hệ quản trị CSDL này và truy vấn CSDL.

+ Các cập nhật dữ liệu: Ðây là các thao tác thay đổi dữ liệu như xoá, sửa dữ liệu trong CSDL. Giống như các truy vấn, chúng có thể được phát ra thông qua giao diện chung hoặc thông qua giao diện của chương trình.

+ Các thay đổi sơ đồ: Các lệnh này thường được phát bởi một người sử dụng được cấp phép, thường là những người quản trị CSDL mới được phép thay đổi sơ đồ của CSDL hay tạo lập một CSDL mới.

**e) Các chức năng của hệ quản trị CSDL quan hệ**

*Các khái niệm trong mô hình dữ liệu quan hệ:*

- Miền (domain): là một tập các giá trị hoặc các đối tượng.

- Thực thể: Thực thể là một đối tượng cụ thể hay trừu tượng trong thế giới thực mà nó tồn tại và có thể phân biệt được với các đối tượng khác.

- Thuộc tính (Attribute): Là tính chất của thực thể.

+ Các thực thể có các đặc tính, được gọi là các thuộc tính. Nó kết hợp với một thực thể trong tập thực thể từ miền giá trị của thuộc tính. Thông thường, miền giá trị của một thuộc tính là một tập các số nguyên, các số thực, hay các xâu ký tự.

+ Một thuộc tính hay một tập thuộc tính mà giá trị của nó xác định duy nhất mỗi thực thể trong tập các thực thể được gọi là khoá đối với tập thực thể này.

+ Mỗi một thuộc tính nhận tập số các giá trị nhất định được gọi là domain của thuộc tính đó.

- Một quan hệ (Relation): Định nghĩa một cách đơn giản, một quan hệ là một bảng dữ liệu có các cột là các thuộc tính và các hàng là các bộ dữ liệu cụ thể của quan hệ.

- Các liên kết: Một liên kết là một sự kết hợp giữa một số thực thể (hay quan hệ). Ví dụ: Mối liên kết giữa phòng ban và nhân viên thể hiện: Một nhân viên A sẽ thuộc một phòng ban B nào đó.

+ Các liên kết một – một: đây là dạng liên kết đơn giản, liên kết trên hai thực thể là một – một, có nghĩa là mỗi thực thể trong tập thực thể này có nhiều nhất một thực thể trong tập thực thể kia kết hợp với nó và ngược lại.

+ Các liên kết một – nhiều: Trong một liên kết một – nhiều, một thực thể trong tập thực thể A được kết hợp với không hay nhiều thực thể trong tập thực thể B. Nhưng mỗi thực thể trong tập thực thể B được kết hợp với nhiều nhất một thực thể trong tập thực thể A.

+ Các liên kết nhiều – nhiều: Ðây là dạng liên kết mà mỗi thực thể trong tập thực thể này có thể liên kết với không hay nhiều thực thể trong tập thực thể kia và ngược lại.

- Mô hình dữ liệu quan hệ: Làm việc trên bảng hay trên quan hệ trong đó: Mỗi cột là một thuộc tính, mỗi dòng là một bộ (một bản ghi).

+ Các ưu điểm của mô hình dữ liệu quan hệ

* Cấu trúc dữ liệu dễ dùng, không cần hiểu biết sâu về kỹ thuật cài đặt.
* Cung cấp ngôn ngữ thao tác phi thủ tục.
* Tối ưu hoá cách truy xuất dữ liệu.

+ Khoá của quan hệ:

* Khoá của quan hệ (key): Là tập các thuộc tính dùng để phân biệt hai bộ bất kỳ trong quan hệ.
* Khoá ngoại của quan hệ (Foreign Key): Một thuộc tính được gọi là khoá ngoại của quan hệ nếu nó là thuộc tính không khoá của quan hệ này nhưng là thuộc tính khoá của quan hệ khác.

*Các chức năng của hệ quản trị CSDL quan hệ:*

Các chức năng của hệ quản trị CSDL quan hệ có thể được phân thành các tầng chức năng như hình 4.

- Tầng giao diện (Interface layer): Quản lý giao diện với các ứng dụng. Các chương trình ứng dụng CSDL được thực hiện trên các khung nhìn (view) của CSDL. Ðối với một ứng dụng, khung nhìn rất có ích cho việc biểu diễn một hình ảnh cụ thể về CSDL (được dùng chung bởi nhiều ứng dụng).

Khung nhìn quan hệ là một quan hệ ảo, được dẫn xuất từ các quan hệ cơ sở (base relation) bằng cách áp dụng các phép toán đại số quan hệ. Quản lý khung nhìn bao gồm việc phiên dịch câu vấn tin người dùng trên dữ liệu ngoài thành dữ liệu khái niệm. Nếu câu vấn tin của người dùng được diễn tả bằng các phép toán quan hệ, câu vấn tin được áp dụng cho dữ liệu khái niệm vẫn giữ nguyên dạng này

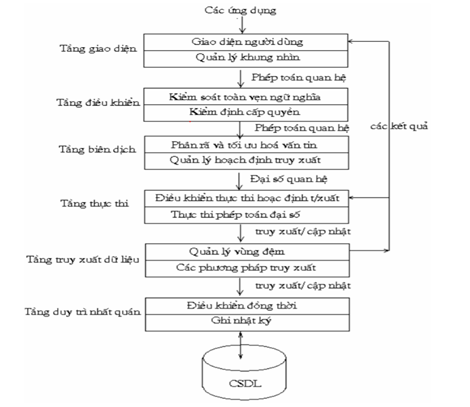
- Tầng điều khiển (Control Layer): chịu trách nhiệm điều khiển câu vấn tin bằng cách đưa thêm các vị từ toàn vẹn ngữ nghĩa và các vị từ cấp quyền.

- Tầng xử lý vấn tin (Query processing layer): chịu trách nhiệm ánh xạ câu vấn tin thành chuỗi thao tác đã được tối ưu ở mức thấp hơn. Tầng này liên quan đến vấn đề hiệu năng. Nó phân rã câu vấn tin thành một cây biểu thị các phép toán đại số quan hệ và thử tìm ra một thứ tự “tối ưu” cho các phép toán này. Kết xuất của tầng này là câu vấn tin được diễn tả bằng đại số quan hệ hoặc một dạng mã ở mức thấp.

- Tầng thực thi (Execution layer): Có trách nhiệm hướng dẫn việc thực hiện các hoạch định truy xuất, bao gồm việc quản lý giao dịch (uỷ thác, tái khởi động) và động bộ hoá các phép đại số quan hệ. Nó thông dịch các phép toán đại số quan hệ bằng cách gọi tầng truy xuất dữ liệu qua các yêu cầu truy xuất và cập nhật.

- Tầng truy xuất dữ liệu (data access layer): Quản lý các cấu trúc dữ liệu dùng để cài đặt các quan hệ (tập tin, chỉ mục). Nó quản lý các vùng đệm bằng cách lưu tạm các dữ liệu thường được truy xuất đến nhiều nhất. Sử dụng tầng này làm giảm thiểu việc truy xuất đến đĩa.

- Tầng duy trì nhất quán (Consistency layer): chịu trách nhiệm điều khiển các hoạt động đồng thời và việc ghi vào nhật ký các yêu cầu cập nhật. Tầng này cũng cho phép khôi phục lại giao dịch, hệ thống và thiết bị sau khi bị sự cố.



Hình 3. 3

### 3.1.2. Phân tích, thiết kế mô hình cơ sở dữ liệu của hệ thống máy chủ nội dung

**a) Phân tích yêu cầu thiết kế hệ thống**

*Tính đồng nhất*

Do yêu cầu của hệ thống là dữ liệu phát thanh phải đồng bộ từ cấp tỉnh, huyện đến xã tức là tại các đài phát thanh đặt tại 3 cấp tỉnh, huyện và xã sẽ tiếp sóng cùng một chương trình phát thanh tại một thời điểm. Việc này giúp cho việc truyền đạt thông tin đến mọi người một cách chính xác, nhất quán, tránh làm sai lệch thông tin.

Qua khảo sát tình hình thực tế của đài phát thanh truyền hình tỉnh Đắk lắk, đài truyền thanh truyền hình các huyện và các xã trên địa bàn tỉnh cho thấy một vấn đề, hệ thống phát thanh và truyền thanh trên địa bàn tỉnh chỉ mới dừng lại ở cấp quản lý về tin bài, cấp tỉnh nhận tin bài của cấp huyện cấp huyện có nhận một số tin bài của cấp xã chuyển lên, và có nhuận bút theo quy định trả cho tắc giả. Mới chỉ quản lý về chuyên môn. Việc quản lý nhà nước do sở thông tin truyền thông tỉnh quản lý. Theo quy trình phát sóng tuyên truyền các đường nối chủ trương chính sách của đảng, nhà nước, cấp xã ngoài việc thông báo các kế hoạch của đảng Uỷ xã, hội đồng nhân dân xã và các thông tin của các ban nghành đoàn thể khi có yêu cầu. Đồng thời đài truyền thanh xã cũng có chức năng viết bài, biên tập một số tình hình hiện trạng của các thôn bản của xã như người tốt việc tốt... Ngoài các thông tin nói trên đài truyền thanh xã có nhiệm vụ là tiếp sóng đài huyện và đài tiếng nói Việt Nam.

*Cơ chế quản lý:*

Do tính chất đặc thù ở khu vực DakLak nói riêng cung như Tây Nguyên nói chung là khu vực miền núi cao, địa bàn nhiều đồi núi gây khó khăn cho việc đi lại, phát triển kinh tế… Hơn nữa trên địa bàn tỉnh DakLak có nhiều dân tộc tiểu số, với ngôn ngữ rất đa dạng và phong phú cho nên việc truyền đạt thông tin đến toàn thể người dân trong khu vưc rất là khó khăn. Mỗi khu vực lại gồm một nhóm các dân tộc với tiếng nói riêng vì vậy nhưng khu vực mà có chung một ngôn ngữ, lịch sử … sẽ được phân quyền sử dụng chung dữ liệu.

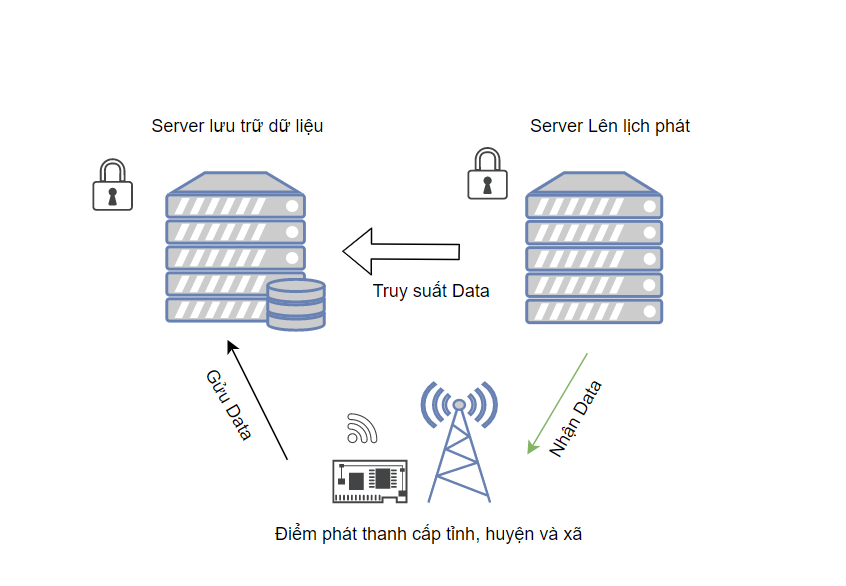
Như chúng ta đã biết Tây Nguyên là vùng có số dân ít, khoảng 5,5 triệu người và được phân bố không đồng đều, mật độ dân số thấp, nhưng lại đa dạng về dân tộc, trong đó có tới 30% số dân là người dân tộc thiểu số. Đây là vùng sinh sống khó khăn của đất nước, kèm theo những vấn đề còn tồn đọng về dân cư, việc làm, dân trí.

Các tỉnh Tây Nguyên nói chung, Đắk lắk nói riêng, luôn là điểm nóng về an ninh, quốc phòng trong những năm gần đây. Vì vậy hệ thống phát thanh phải được quản lý một cách nghiêm ngắt và dữ liệu được phát bởi các đài truyền thanh cấp cơ sở có thể được kiểm soát bởi đài truyền thanh, phát thanh cấp cao hơn để đảm bảo tính đồng nhất về nội dung phát thanh trên toàn tỉnh.

Trong hệ thống phát thanh và truyền thanh quản trị viên là người có quyền hạn lớn nhất tiếp đến là các user cấp tỉnh, huyện, xã. Ngoài những quyền được gán sẵn, user muốn truy cập vượt quyền thực hiện các nhiệm vụ khác nhau đề phải được quản trị viên xác nhận.

**b) Thiết kế mô hình cơ sở dữ liệu**

Mô hình Cơ sở dữ liệu của hệ thống được thiết kế theo mô hình Server-Client. Trong mô hình này thì Server lưu trữ có nhiệm vụ lưu trữ dữ liệu âm thanh được gửu về từ các điểm phát thanh 3 cấp tỉnh, huyện và thị xã. Sau đó server khác có nhiệm vụ lên lịch phát sóng các chương trình sẽ lấy dữ liệu từ server lưu trữ làm nội dụng rồi chuyển đến các Client.



Hình 3. 4

Client là các máy phát, thu Internet đặt tại các điểm phát sóng. Nhiệm vụ của Client là nhận dữ liệu từ server lên lịch phát sóng sau đó gửu đến các máy phát thanh để phát thanh chương trình phục vụ người dân trong khu vực. Tại cái điểm phát thanh cấp tỉnh, huyện, xã có thể tự tạo nội dung chương trình rồi đưa lên server lưu trữ dữ liệu. Không những thế, tại mỗi điểm đầu cuối cũng có thể trở thành điểm thu thập thông tin và yêu cầu hỗ trợ từ phía người dân thông qua hệ thống camera gắn tại mỗi điểm đầu cuối.

Ưu điểm của mô hình cơ sở dữ liệu:

* Do tài nguyên tập trung trên một máy tính cho nên việc quản lý tài nguyên trở nên dễ dàng Tài nguyên được quản lý tập trung vì vậy quản lý một cách dễ dàng.
* Dễ dàng kiểm soát việc truy cập và sử dụng
* Dễ dàng nâng cấp và mở rộng. Chúng ta hoàn toàn có thể nâng cấp và cải thiện hiệu suất của hệ thống bằng cách nâng cấp cấu hình của server.

Nhược điểm của mô hình cơ sở dữ liệu:

* Phụ thuộc vào mạng, mọi thao tác của cả Client và Server đều phụ thuộc vào mạng để truyền tải.
* Nếu mạng bị mất thì kết nối giữa Client và Server sẽ bị ngắt và các tệp tin truyền tải sẽ bị gián đoạn.
* Tốn kém chi phí khi mua và duy trì sự hoạt độnssg của Server.

## **3.2. Nghiên cứu, thiết kế chức năng phần mềm lưu trữ và quản lí dữ liệu trên máy chủ nội dung Phúc D16**

### 3.2.1. Tổng quan về SQL

Ngôn ngữ hỏi có cấu trúc (SQL) và các hệ quản trị cơ sở dữ liệu quan hệ là một trong những nền tảng kỹ thuật quan trọng trong công nghiệp máy tính. Cho đến nay, có thể nói rằng SQL đã được xem là ngôn ngữ chuẩn trong cơ sở dữ liệu. Các hệ quản trị cơ sở dữ liệu quan hệ thương mại hiện có như Oracle, SQL Server, Informix, DB2... đều chọn SQL làm ngôn ngữ cho sản phẩm của mình.

**a) SQL là ngôn ngữ cơ sở dữ liệu quan hệ**

SQL, viết tắt của *Structured Query Language* (ngôn ngữ hỏi có cấu trúc), là công cụ sử dụng để tổ chức, quản lý và truy xuất dữ liệu đuợc lưu trữ trong các cơ sở dữ liệu. SQL là một hệ thống ngôn ngữ bao gồm tập các câu lệnh sử dụng để tương tác với cơ sở dữ liệu quan hệ.

Tên gọi *ngôn ngữ hỏi có cấu trúc* phần nào làm chúng ta liên tưởng đến một công cụ (ngôn ngữ) dùng để truy xuất dữ liệu trong các cơ sở dữ liệu. Thực sự mà nói, khả năng của SQL vượt xa so với một công cụ truy xuất dữ liệu, mặc dù đây là mục đích ban đầu khi SQL được xây dựng nên và truy xuất dữ liệu vẫn còn là một trong những chức năng quan trọng của nó. SQL được sử dụng để điều khiển tất cả các chức năng mà một hệ quản trị cơ sở dữ liệu cung cấp cho người dùng bao gồm:

* **Định nghĩa dữ liệu:** SQL cung cấp khả năng định nghĩa các cơ sở dữ liệu, các cấu trúc lưu trữ và tổ chức dữ liệu cũng như mối quan hệ giữa các thành phần dữ liệu.
* **Truy xuất và thao tác dữ liệu:** Với SQL, người dùng có thể dễ dàng thực hiện các thao tác truy xuất, bổ sung, cập nhật và loại bỏ dữ liệu.
* **Điều khiển truy cập:** SQL có thể được sử dụng để cấp phát và kiểm soát các thao tác của người sử dụng trên dữ liệu, đảm bảo sự an toàn cho cơ sở dữ liệu
* **Đảm bảo toàn vẹn dữ liệu:** SQL định nghĩa các ràng buộc toàn vẹn trong cơ sở dữ liệu nhờ đó đảm bảo tính hợp lệ và chính xác của dữ liệu trước các thao tác cập nhật cũng như các lỗi của hệ thống.

Như vậy, có thể nói rằng SQL là một ngôn ngữ hoàn thiện được sử dụng trong các hệ thống cơ sở dữ liệu và là một thành phần không thể thiếu trong các hệ quản trị cơ sở dữ liệu. Mặc dù SQL không phải là một ngôn ngữ lập trình như C, C++, Java,... song các câu lệnh mà SQL cung cấp có thể được nhúng vào trong các ngôn ngữ lập trình nhằm xây dựng các ứng dụng tương tác với cơ sở dữ liệu.

**b) Vai trò của SQL**

Bản thân SQL không phải là một hệ quản trị cơ sở dữ liệu, nó không thể tồn tại độc lập. SQL thực sự là một phần của hệ quản trị cơ sở dữ liệu, nó xuất hiện trong các hệ quản trị cơ sở dữ liệu với vai trò ngôn ngữ và là công cụ giao tiếp giữa người sử dụng và hệ quản trị cơ sở dữ liệu.

Trong hầu hết các hệ quản trị cơ sở dữ liệu quan hệ, SQL có những vai trò như sau:

* **SQL là ngôn ngữ hỏi có tính tương tác:** Người sử dụng có thể dễ dàng thông qua các trình tiện ích để gởi các yêu cầu dưới dạng các câu lệnh SQL đến cơ sở dữ liệu và nhận kết quả trả về từ cơ sở dữ liệu
* **SQL là ngôn ngữ lập trình cơ sở dữ liệu**: Các lập trình viên có thể nhúng các câu lệnh SQL vào trong các ngôn ngữ lập trình để xây dựng nên các chương trình ứng dụng giao tiếp với cơ sở dữ liệu
* **SQL là ngôn ngữ quản trị cơ sở dữ liệu:** Thông qua SQL, người quản trị cơ sở dữ liệu có thể quản lý được cơ sở dữ liệu, định nghĩa các cấu trúc lưu trữ dữ liệu, điều khiển truy cập cơ sở dữ liệu,...
* **SQL là ngôn ngữ cho các hệ thống khách/chủ (client/server):** Trong các hệ thống cơ sở dữ liệu khách/chủ, SQL được sử dụng như là công cụ để giao tiếp giữa các trình ứng dụng phía máy khách với máy chủ cơ sở dữ liệu.
* **SQL là ngôn ngữ truy cập dữ liệu trên Internet:** Cho đến nay, hầu hết các máy chủ Web cũng như các máy chủ trên Internet sử dụng SQL với vai trò là ngôn ngữ để tương tác với dữ liệu trong các cơ sở dữ liệu.
* **SQL là ngôn ngữ cơ sở dữ liệu phân tán:** Đối với các hệ quản trị cơ sở dữ liệu phân tán, mỗi một hệ thống sử dụng SQL để giao tiếp với các hệ thống khác trên mạng, gởi và nhận các yêu cầu truy xuất dữ liệu với nhau.
* **SQL là ngôn ngữ sử dụng cho các cổng giao tiếp cơ sở dữ liệu:** Trong một hệ thống mạng máy tính với nhiều hệ quản trị cơ sở dữ liệu khác nhau, SQL thường được sử dụng như là một chuẩn ngôn ngữ để giao tiếp giữa các hệ quản trị cơ sở dữ liệu.

**c) BẢO MẬT TRONG SQL**

*Các khái niệm*

Bảo mật là một trong những yếu tố đóng vai trò quan trọng đối với sự sống còn của cơ sở dữ liệu. Hầu hết các hệ quản trị cơ sở dữ liệu thương mại hiện nay đều cung cấp khả năng bảo mật cơ sở dữ liệu với những chức năng như:

* Cấp phát quyền truy cập cơ sở dữ liệu cho người dùng và các nhóm người dùng, phát hiện và ngăn chặn những thao tác trái phép của người sử dụng trên cơ sở dữ liệu.
* Cấp phát quyền sử dụng các câu lệnh, các đối tượng cơ sở dữ liệu đối với người dùng.
* Thu hồi (huỷ bỏ) quyền của người dùng.

Bảo mật dữ liệu trong SQL được thực hiện dựa trên ba khái niệm chính sau đây:

* **Người dùng cơ sở dữ liệu (Database user):** Là đối tượng sử dụng cơ sở dữ liệu, thực thi các thao tác trên cơ sở dữ liệu như tạo bảng, truy xuất dữ liệu,... Mỗi một người dùng trong cơ sở dữ liệu được xác định thông qua tên người dùng (User ID). Một tập nhiều người dùng có thể được tổ chức trong một nhóm và được gọi là nhóm người dùng (User Group).
* **Các đối tượng cơ sở dữ liệu (Database objects):** Tập hợp các đối tượng, các cấu trúc lưu trữ được sử dụng trong cơ sở dữ liệu như bảng, khung nhìn, thủ tục, hàm được gọi là các đối tượng cơ sở dữ liệu. Đây là những đối tượng cần được bảo vệ trong chính sách bảo mật của cơ sở dữ liệu.
* **Đặc quyền (Privileges):** Là tập những thao tác được cấp phát cho người dùng trên các đối tượng cơ sở dữ liệu. Chằng hạn một người dùng có thể truy xuất dữ liệu trên một bảng bằng câu lệnh SELECT nhưng có thể không thể thực hiện các câu lệnh INSERT, UPDATE hay DELETE trên bảng đó.

SQL cung cấp hai câu lệnh cho phép chúng ta thiết lập các chính sách bảo mật trong cơ sở dữ liệu:

* Lệnh GRANT: Sử dụng để cấp phát quyền cho người sử dụng trên các đối tượng cơ sở dữ liệu hoặc quyền sử dụng các câu lệnh SQL trong cơ sở dữ liệu.
* Lệnh REVOKE: Được sử dụng để thu hồi quyền đối với người sử dụng.

*Cấp phát quyền*

Câu lệnh GRANT được sử dụng để cấp phát quyền cho người dùng hay nhóm người dùng trên các đối tượng cơ sở dữ liệu. Câu lệnh này thường được sử dụng trong các trường hợp sau:

* Người sở hữu đối tượng cơ sở dữ liệu muốn cho phép người dùng khác quyền sử dụng những đối tượng mà anh ta đang sở hữu.
* Người sở hữu cơ sở dữ liệu cấp phát quyền thực thi các câu lệnh (như CREATE TABLE, CREATE VIEW...) cho những người dùng khác.

**Cấp phát quyền cho người dùng trên các đối tượng cơ sở dữ liệu**

Chỉ có người sở hữu cơ sở dữ liệu hoặc người sở hữu đối tượng cơ sở dữ liệu mới có thể cấp phát quyền cho người dùng trên các đối tượng cơ sở dữ liệu.

**Cấp phát quyền thực thi các câu lệnh**

Ngoài chức năng cấp phát quyền cho người sử dụng trên các đối tượng cơ sở dữ liệu, câu lệnh GRANT còn có thể sử dụng để cấp phát cho người sử dụng một số quyền trên hệ quản trị cơ sở dữ liệu hoặc cơ sở dữ liệu. Những quyền có thể cấp phát trong trường hợp này bao gồm:

* Tạo cơ sở dữ liệu: CREATE DATEBASE.
* Tạo bảng: CREATE RULE
* Tạo khung nhìn: CREATE VIEW
* Tạo thủ tục lưu trữ: CREATE PROCEDURE
* Tạo hàm: CREATE FUNCTION
* Sao lưu cơ sở dữ liệu: BACKUP DATABASE

*Thu hồi quyền*

Câu lệnh REVOKE được sử dụng để thu hồi quyền đã được cấp phát cho người dùng. Tương ứng với câu lệnh GRANT, câu lệnh REVOKE được sử dụng trong hai trường hợp:

* Thu hồi quyền đã cấp phát cho người dùng trên các đối tượng cơ sở dữ liệu.

Thu hồi quyền thực thi các câu lệnh trên cơ sở dữ liệu đã cấp phát cho người dùng.

**d) Giao Tác SQL**

*Giao tác và các tính chất của giao tác*

Một giao tác (transaction) là một chuỗi một hoặc nhiều câu lệnh SQL được kết hợp lại với nhau thành một khối công việc. Các câu lệnh SQL xuất hiện trong giao tác thường có mối quan hệ tương đối mật thiết với nhau và thực hiện các thao tác độc lập. Việc kết hợp các câu lệnh lại với nhau trong một giao tác nhằm đảm bảo tính toàn vẹn dữ liệu và khả năng phục hồi dữ liệu. Trong một giao tác, các câu lệnh có thể độc lập với nhau nhưng tất cả các câu lệnh trong một giao tác đòi hỏi hoặc phải thực thi trọn vẹn hoặc không một câu lệnh nào được thực thi.

Các cơ sở dữ liệu sử dụng *nhật ký giao tác* (*transaction log*) để ghi lại các thay đổi mà giao tác tạo ra trên cơ sở dữ liệu và thông qua đó có thể phục hồi dữ liệu trong trường hợp gặp lỗi hay hệ thống có sự cố.

Một giao tác đòi hỏi phải có được bồn tính chất sau đây:

* **Tính nguyên tử (Atomicity):** Mọi thay đổi về mặt dữ liệu hoặc phải được thực hiện trọn vẹn khi giao tác thực hiện thành công hoặc không có bất kỳ sự thay đổi nào về dữ liệu xảy ra nếu giao tác không thực hiện được trọn vẹn. Nói cách khác, tác dụng của các câu lệnh trong một giao tác phải như là một câu lệnh đơn.
* **Tính nhất quán (Consistency):** Tính nhất quan đòi hỏi sau khi giao tác kết thúc, cho dù là thành công hay bị lỗi, tất cả dữ liệu phải ở trạng thái nhất quán (tức là sự toàn vẹn dữ liệu phải luôn được bảo toàn).
* **Tính độc lập (Isolation):** Tính độc lập của giao tác có nghĩa là tác dụng của mỗi một giao tác phải giống như khi chỉ mình nó được thực hiện trên chính hệ thống đó. Nói cách khác, một giao tác khi được thực thi đồng thời với những giao tác khác trên cùng hệ thống không chịu bất kỳ sự ảnh hưởng nào của các giao tác đó.
* **Tính bền vững (Durability):** Sau khi một giao tác đã thực hiện thành công, mọi tác dụng mà nó đã tạo ra phải tồn tại bền vững trong cơ sở dữ liệu, cho dù là hệ thống có bị lỗi đi chăng nữa.

*Mô hình giao tác trong SQL*

Giao tác SQL được định nghĩa dựa trên các câu lệnh xử lý giao tác sau đây:

* BEGIN TRANSACTION: Bắt đầu một giao tác
* SAVE TRANSACTION: Đánh dấu một vị trí trong giao tác (gọi là điểm đánh dấu).
* ROLLBACK TRANSACTION: Quay lui trở lại đầu giao tác hoặc một điểm đánh dấu trước đó trong giao tác.
* COMMIT TRANSACTION: Đánh dấu điểm kết thúc một giao tác. Khi câu lệnh này thực thi cũng có nghĩa là giao tác đã thực hiện thành công.
* ROLLBACK [WORK]: Quay lui trở lại đầu giao tác.
* COMMIT [WORK]: Đánh dấu kết thúc giao tác.

Một giao tác sẽ kết thúc trong các trường hợp sau:

* Câu lệnh COMMIT TRANSACTION (hoặc COMMIT WORK) được thực thi. Câu lệnh này báo hiệu sự kết thúc thành công của một giao tác. Sau câu lệnh này, một giao tác mới sẽ được bắt đầu.
* Khi câu lệnh ROLLBACK TRANSACTION (hoặc ROLLBACK WORK) được thực thi để huỷ bỏ một giao tác và đưa cơ sở dữ liệu về trạng thái như trước khi giao tác bắt đầu. Một giao tác mới sẽ bắt đầu sau khi câu lệnh ROLLBACK được thực thi.
* Một giao tác cũng sẽ kết thúc nếu trong quá trình thực hiện gặp lỗi (chẩng hạn hệ thống gặp lỗi, kết nối mạng bị “đứt”,...). Trong trường hợp này, hệ thống sẽ tự động phục hồi lại trạng thái cơ sở dữ liệu như trước khi giao tác bắt đầu (tương tự như khi câu lệnh ROLLBACK được thực thi để huỷ bỏ một giao tác). Tuy nhiên, trong trường hợp này sẽ không có giao tác mới được bắt đầu.

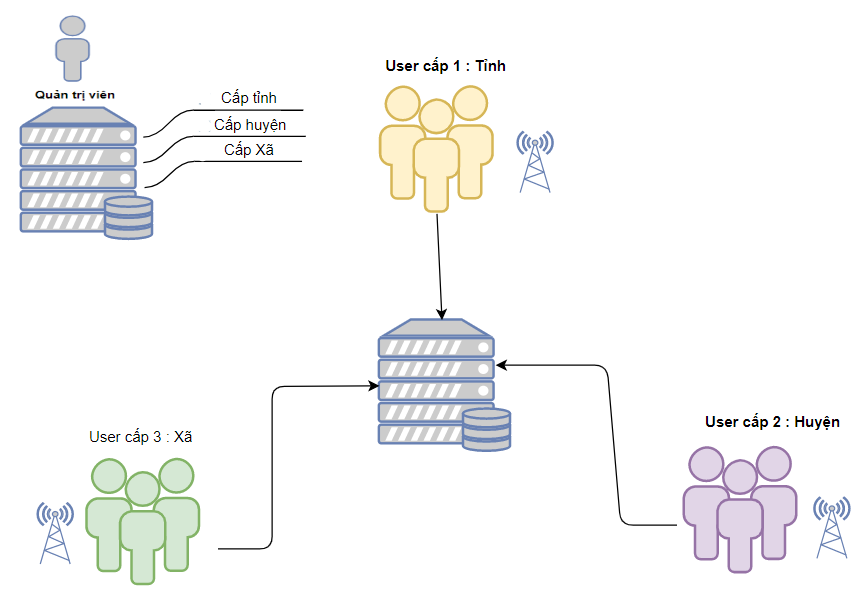
*Giao tác lồng nhau*

Các giao tác trong SQL có thể được lồng vào nhau theo từng cấp. Điều này thường gặp đối với các giao tác trong các thủ tục lưu trữ được gọi hoặc từ một tiến trình trong một giao tác khác.

### 3.2.2. Phân quyền đăng bài*,* quyền kiểm duyệt, quyền sửa/xóa/tải về và quyền truy cập CSDL.

**a) Phân quyền truy cập**

Như chúng ta đã biết yếu điểm về tính an toàn, độ tin cậy thể hiện rất rõ tại các tỉnh Tây Nguyên nói chung, Đắk lắk nói riêng, luôn là điểm nóng về an ninh, quốc phòng trong những năm gần đây. Việc các đài phát thanh bị hack dẫn đến phát những bản tin tuyên truyền tiếng nước ngoài, hay chống phá nhà nước, kích động người dân tham gia các cuộc biểu tình của các nhóm, tổ chức phản động trong và nhà nước có mưu đồ xấu đến an ninh chính trị, quốc phòng vẫn còn xảy ra.



Hình 3. 5

Vì vậy việc bảo đảm an toàn thông tin là một trong những vẫn đề được ưu tiên hàng đầu của hệ thống phát thanh radio số đồng nhất 3 cấp. Ngoài việc sử dụng công nghệ mã hóa RDS-OTP tại các điểm phát sóng và thu thì tại server lưu trữ dữ liệu các chương trình phát sóng cũng cần được bảo vệ.

Server lưu trữ các chương trình phát sóng của hệ thống được chia thành các vùng lưu trữ. Những user cùng một cấp không có quyền truy cập lẫn nhau.

* Phân cấp tỉnh: User cấp 1, quản trị viên có quyền truy cập.
* Phân cấp huyên: User cấp 1,2 và quản trị viên có quyền truy cập.
* Phân cấp xã: Tất cả các User cấp cao hơn và quản trị viên đều có quyền có quyền truy nhập.

Các điểm phát thanh thấp hơn hay là các User cấp thấp hơn muốn truy cập vào vùng lưu trữ của User cấp cao hơn phải đượ sự cho phép của User cấp cao hơn hay được sự cho phép của quản trị viên hệ thống. Trong hệ thống trên quản trị vị có quyền truy cập cao nhất và có thể cấp phát quyền cũng như hủy bỏ quyền truy cập của các user, việc này giúp cho việc kiểm soát hệ thống một cách đơn giản và dễ dàng.

**b) Phân quyền đăng bài**

Do hệ thống phát thanh được đặt tại 3 khu vực tỉnh, huyện và xã, tại mỗi điểm phát thanh đều có thể xây dựng nội dung số, biên tập các chương trình như là tấm gương tốt hay truyền tải những thông tin quan trọng, nhanh, chính xác, bảo mật đến người dân trong khu vực. Các chương trình này sẽ được gửu về server lưu trữ dữ liệu thông qua máy phát, thu Internet. Ngoài ra, hệ thống truyền thanh số qua Internet còn có một ưu điểm khác là tính tương tác hai chiều. Yêu cầu hoặc cảnh báo từ phía người nghe (thiết bị cuối) có thể dễ dàng.



Hình 3. 6

Quyền đăng bài sẽ được cấp cho tất cả các điểm phát thanh, do server lên lịch quản lý các chương trình phát tại các điểm ở cả 3 khu vực tỉnh, huyện và xã việc này giúp thông tin được truyền tải đến người dân một cách thống nhất.

Ngoài ra với những yêu cầu cầu cảnh báo tại mỗi điểm sẽ có mức ưu tiên cao hơn sẽ được phát trực tiếp tại khu vực phát. Nếu trong thời điểm đó có một chương trình đang phát sóng thì ngay lập tức dừng lại nhường sóng cho yêu cầu cảnh báo mà không cần phải được sự cho phép của server lên lịch phát sóng.

Việc đáp ứng các yêu cầu hoặc cảnh báo từ phía người nghe (thiết bị cuối) có thể dễ dàng và nhanh chóng chuyển về bộ phận điều khiển hệ thống, từ đó hệ thống có quy trình đáp ứng nhanh chóng trong những tính huống khẩn cấp như là cứu hộ, hay là các thảm họa tự nhiên khác... giúp cho việc phát hiện, ứng cứu một cách chính xác giảm tối đa những thiệt hại về con người và của cải vật chất. Hệ thống truyền thanh số đáp ứng được hết những yêu cầu trên được gọi là hệ thống truyền thanh thông minh. Trong hệ thống truyền thanh thông minh, nội dung được cập nhật nhanh chóng, đảm bảo tính thời sự, với từng khu vực nhỏ trong tỉnh.

**c) Phân quyền sửa, xóa, tải về**

Trên server lưu trữ, dữ liệu sẽ tạo các vùng lưu trữ phân cấp để dễ dàng quản lý các chương trình và được phân cấp như sau:

* Phân cấp tỉnh: Có thể chỉnh sửa các chương trình của mình cũng như các chương trình của huyện, xã gửu lên server lưu trữ.
* Phân cấp huyện: Có thể chỉnh sửa các chương trình của mình và của xã, không thể chỉnh sửa chương trình cấp tỉnh.
* Phân cấp xã: Chỉ có thể chỉnh sửa các chương trình của mình và không thể chỉnh sửa chương trình cấp huyện, tỉnh.

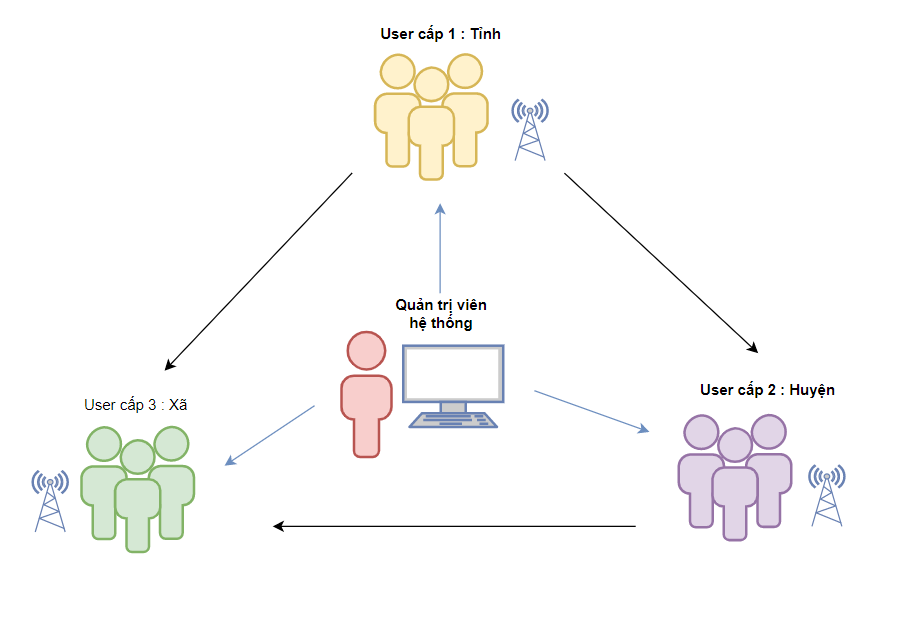
Người quản trị viên của hệ thống có quyền chỉnh sửa, xóa, tải về mọi thứ.

Về quyền xóa: Chỉ có quản trị viên của hệ thống mới có quyền xóa.

Về quyền tải xuống: Mọi điểm phát thanh để có thể tải chương trình phát sóng xuống.

**d) Phân quyền kiểm duyệt**

Quyền kiểm duyệt được thiết kế theo mô hình phân cấp, cấp đơn vị cao hơn thì có quyền kiểm duyệt các chương trình, bài phát thanh của cấp dưới do đó giúp kiểm soát các chương trình phát thanh một cách đồng nhất, đảm bảo cho việc một đài phát thanh không tự ý phát các chương trình mà chưa được cho phép.



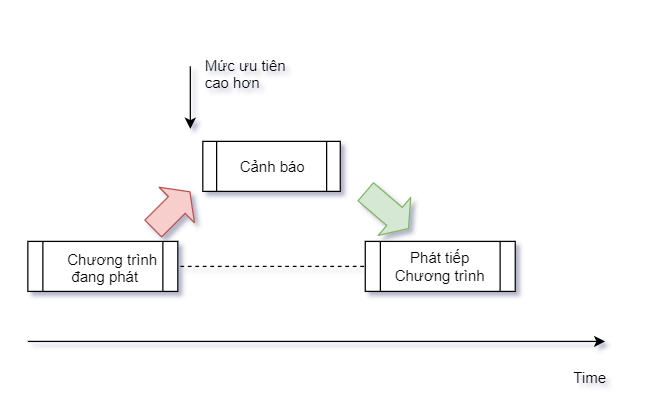
Hình 3. 7

Mô hình của hệ thống gồm quản trị viên và user chia làm 3 cấp : User cấp 1-tỉnh, User cấp 2-huyện và User câp 3-xã. Trong đó, quản trị viên hệ thống có quyền cao nhất kiểm soát cả 3 cấp tỉnh, huyện và xã. Nhiệm vụ của quản trị viên là quản lý các chương trình phát sóng, có quyết định cho chương trình này phát sóng hay không. Ngoài ra thì các user cấp cao hơn có thể kiểm duyệt các chương trình phát sóng của user cấp thấp hơn trước khi gửu lên quản trị viên xét duyệt để xem là chương trình có đáp ứng đủ những yêu cầu hay không. Việc này giúp cho quá trình vận hành hệ thống nhanh hơn cũng như làm giảm tải công việc phải xử lý cho quản trị viên.

### 3.2.3. Tạo các yêu cầu ưu tiên, chứng thực người dùng.

**a) Tạo các yêu cầu ưu tiên**

Đối với các bài phát thanh quan trọng, mỗi bài này sẽ được đánh mã ưu tiên của nó, mã có mức độ ưu tiên càng cao sau khi gửu lên server dữ liệu, bên phía máy phát sẽ lên lịch phát sóng cho nó, mã nào có mức độ ưu tiên cao hơn sẽ được phát trước.

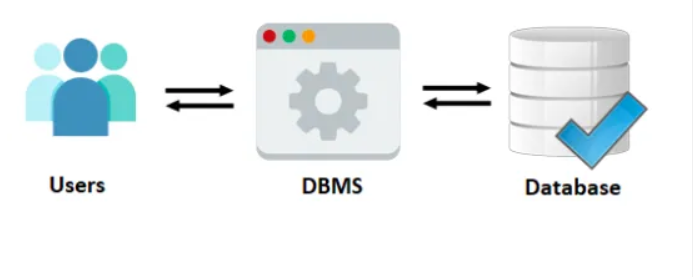


Hình 3. 8

Trong một chương trình phát nhạc phục vụ cho người dân, tại thời điểm đó nhận được cảnh bảo có động đất lúc này bản tin cảnh báo sẽ được gán được mức độ ưu tiên cao nhất lúc này sẽ dừng chương trình đang phát lại để phát tin cảnh báo cho mọi người dân sơ tán khẩn cấp.

**b) Chứng thực người dùng**

Chúng ta có 4 cấp user gồm quản trị viên, user cấp 1(tỉnh), user cấp 2 (huyện), user cấp 3 là (xã) mỗi user sẽ được cung cấp một tài khoản cũng như là password để có thể truy phép vào server lưu trữ dữ liệu , thực hiện các thao tác trong quyền hạn của mình.



Hình 3. 9

## **3.3. Nghiên cứu, thiết kế chức năng phần mềm quản lý hệ thống máy chủ phát sóng Trung D16**

### 3.3.1. Khái niệm máy chủ phát sóng âm thanh (Broadcasting audio server)

Truyền phát là một thuật ngữ được sử dụng để xác định hiển thị phương tiện video và âm thanh trong thời gian thực. Về cơ bản, có hai loại phát trực tuyến.

Truyền phát "real" đòi hỏi một dịch vụ đặc biệt phát thông tin âm thanh / video theo thời gian thực. Trình phát trên thiết bị của người sử dụng truy cập diễn giải luồng dữ liệu này và hiển thị nó ngay lập tức. Công nghệ như vậy đòi hỏi các server chuyên dụng mạnh mẽ vì nó cần rất nhiều tài nguyên để chạy chính xác. Chúng ta cần máy chủ như vậy nếu muốn phát âm thanh trực tiếp.

Hầu hết các công nghệ máy chủ phát trực tuyến ghi lại, mã hóa và phát file âm thanh trong thời gian thực làm cho chúng phù hợp với các trang web của các chương trình trực tiếp.

Truyền phát HTTP là một cách giải quyết phù hợp cho những người không muốn dành nhiều tài nguyên và tiền cho các máy chủ phát sóng đắt tiền. Hiệu quả của phát trực tiếp đạt được bằng cách đệm một phần của tệp âm thanh đã tải xuống và phát nó trong khi phần còn lại của tệp vẫn đang được tải xuống.

Trong trường hợp này, giao thức TCP được sử dụng. Mặc dù TCP là an toàn (có rất nhiều kiểm tra về việc mất gói trong giao thức này), nhưng nó không phù hợp để truyền phát video trong đó việc mất dữ liệu là bình thường và được mong đợi. Tuy nhiên, các trình phát Flash, QuickTime và RealMedia hiện đại kết hợp với một máy chủ nhanh, tuy nhiên, quản lý để phát các video như vậy mà không gặp nhiều vấn đề và để giảm thiểu thời gian đệm.

Nếu bạn muốn cho phép khách truy cập phát video đơn giản trên trang web của mình, bạn không cần một máy chủ phát trực tuyến thực sự. Kết quả tương tự có thể đạt được với phát trực tuyến giả. Việc sử dụng phổ biến nhất của phương pháp phát trực tuyến này là để hiển thị các phim flash có kích thước nhỏ và nhanh để tải xuống và phát.

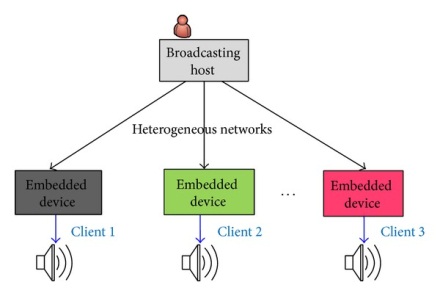
Mặt khác, nếu bạn muốn hiển thị các chương trình trực tiếp trên trang web của mình hoặc để truyền phát video dài, bạn cần một máy chủ phát trực tuyến thực sự. Lưu ý rằng các máy chủ như vậy tạo ra băng thông lớn và rất nhiều tải I / O trên máy chủ của bạn.

Chúng ta cần xây dựng một máy chủ phát trực tuyến cho phép các đài phát thanh phát âm thanh trực tuyến hiệu quả ( điều này được gọi là webcasting). Máy chủ được xây dựng cần phải mạnh mẽ và ổn định, có nghĩa là chúng ta có thể đưa tất cả lưu lượng dữ liệu của Internet Radio vào nó mà không xảy ra lỗi hay sự cố gì cả. Người sử dụng có thể truy cập vào hệ thống tại bất cứ đâu phủ sóng Internet. Phần mềm có ý nghĩa gắn kết và tự động chuyển người nghe từ Auto DJ sang Live stream và ngược lại mà không cần phải tự thao tác bất cứ thứ gì. Người nghe sẽ có thể kết nối với luồng MP3 của bạn từ khắp nơi trên thế giới, với tất cả các trình phát phương tiện phổ biến bao gồm Windows Media Player, iTunes, Winamp, Realplayer, XMMS và nhiều trình phát đa phương tiện khác bên cạnh.

Server có các điểm gắn kết có nghĩa là nó tự động chuyển người nghe từ Auto DJ sang Live streaming và quay lại mà không cần phải bật hoặc tắt thủ công. Vì vậy, bạn kết nối và tất cả người nghe được chuyển từ autodj sang phát trực tiếp và sau đó quay lại khi bạn kết thúc. Điều này, không giống như WHM Sonic hoạt động với các luồng MP3 để nó hoạt động với bất kỳ trình phát đa phương tiện nào (ví dụ: Windows Media, Real Player, I-Tunes, Win-Amp, thậm chí cả trình phát flash!).

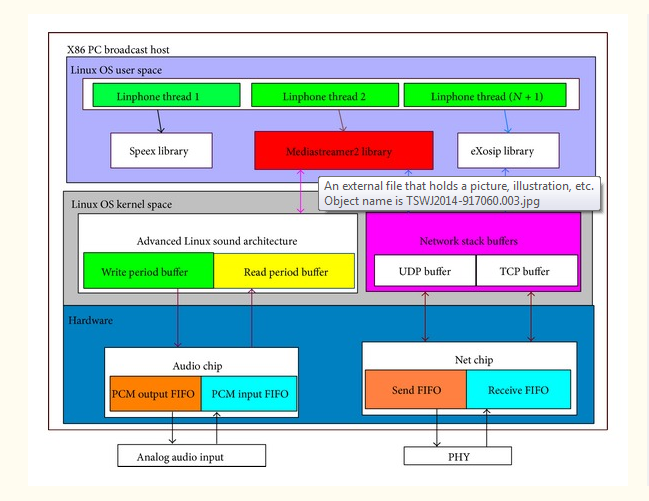
Máy chủ lưu trữ tương tự như Shoutcast theo nhiều cách, tuy nhiên cho phép phát trực tuyến bằng phương tiện được hỗ trợ MP3, Ogg, Aac + hoặc Opus. Tất cả các gói Hosting Icecast sẽ bao gồm DJ tự động miễn phí. Hệ thống autodj của chúng tôi sẽ cho phép bạn tải mp3 của bạn lên hệ thống và có thể chọn nhiều danh sách phát và phát 24/7 mà không cần có máy tính của bạn mọi lúc.

### 3.3.2.Kiến trúc đề xuất sử dụng trong mạng không đồng nhất

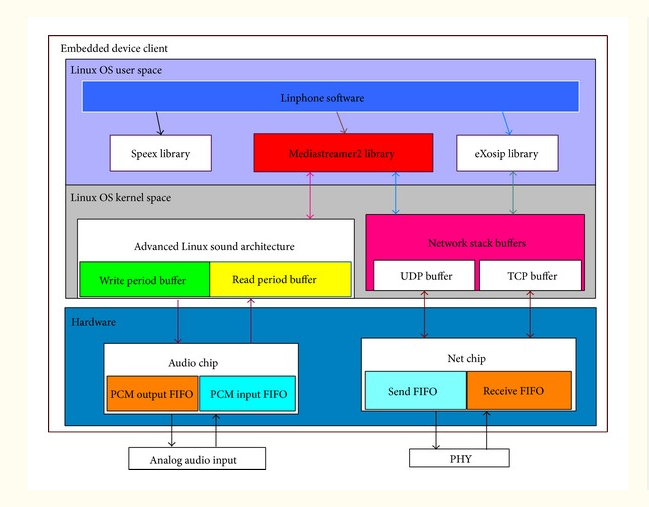


Hình 3. 10

Âm thanh analog được đưa vào máy chủ phát sóng và được phát đến các máy khách thiết bị nhúng qua các mạng không đồng nhất, chẳng hạn như WiFi, LAN và mạng 3G.



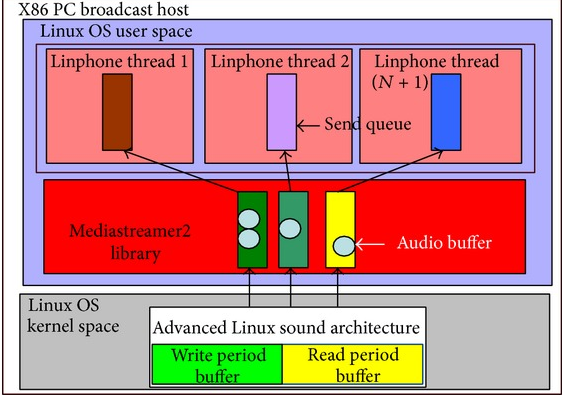
Hình 3. 11



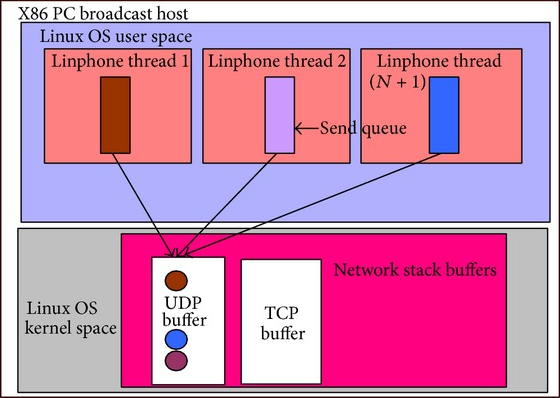
Hình 3. 12

Trong kiến ​​trúc của máy chủ phát sóng, tồn tại nhiều luồng Linphone, phù hợp với số lượng máy thu, chạy trong không gian người dùng. Mỗi luồng chia sẻ cùng một bộ nhớ, thư viện và tài nguyên hệ điều hành. Trong không gian của OS kernel, ALSA (Advanced Linux Sound Architecture) cung cấp các chức năng âm thanh và MIDI (giao diện kỹ thuật số nhạc cụ) của Linux. Bộ đệm ngăn xếp mạng được sử dụng để lưu trữ và gửi các gói UDP / TCP. Nếu bộ đệm lớn, hệ điều hành sẽ tích lũy nhiều gói hơn và sau đó chuyển các gói đến chip ở lớp thấp hơn. Theo cách này, CPU được giảm tải, nhưng gói đến có thể không phải là thời gian thực. Ngược lại, bộ đệm càng nhỏ thì gói đến thời gian thực càng nhiều. Ở lớp phần cứng, một chip âm thanh được sử dụng để chuyển đổi tín hiệu âm thanh analog gửi/nhận từ người dùng và chip mạng được sử dụng để gửi/nhận các gói âm thanh kỹ thuật số. Nghĩa là, giọng nói được trích xuất bởi một chip âm thanh và được lưu trong bộ đệm của chip âm thanh. Sau đó, dữ liệu âm thanh được nén bởi Linphone và chia thành các gói nhỏ. Các gói này sau đó được chuyển đến bộ đệm của chip mạng và được gửi đến các máy khách thông qua mạng. Về phía khách hàng, kiến ​​trúc tương tự như phía máy chủ. Sự khác biệt là chỉ có một luồng chạy ở phía máy khách, tương ứng với một trong nhiều luồng trên máy chủ phát sóng. Dữ liệu âm thanh được trích xuất từ ​​bộ đệm của chip mạng và được Linphone giải nén trước và sau đó ALSA gửi dữ liệu đến bộ đệm âm thanh để phát giọng nói.

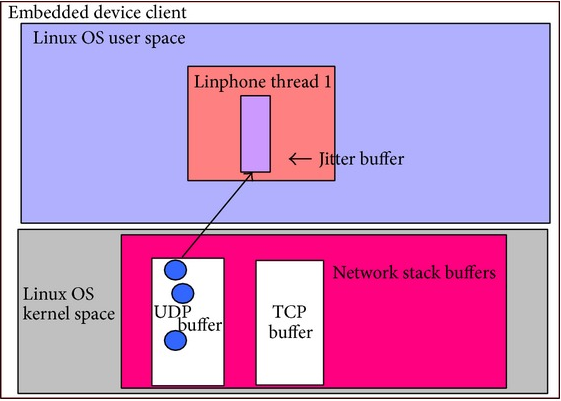
Kiến trúc hệ thống của chúng tôi được chạy trên các mạng không đồng nhất. Khi phân phối nội dung âm thanh từ máy chủ phát đến máy khách, mỗi luồng Linphone có bộ đệm âm thanh riêng. Đầu vào âm thanh analog sẽ được chuyển đổi thành các gói âm thanh kỹ thuật số bằng cách sử dụng một số Audio Codec như G.711, đây là một Codec phổ biến thường được sử dụng ở máy chủ. Khi bộ đệm âm thanh đầy, nó sẽ gửi các gói đến hàng đợi gửi của luồng tương ứng trong không gian người dùng Linux OS. Mỗi luồng tương ứng với một thiết bị nhúng khác nhau. Sau đó các gói được gửi đến bộ đệm UDP trong không gian nhân hệ điều hành Linux. Tiếp theo, mỗi gói ở phía máy chủ được gửi đến bộ đệm jitter trên mỗi thiết bị nhúng ở phía máy khách. Sau khi nhận gói âm thanh, mỗi thiết bị nhúng sẽ gửi phản hồi ACK đến máy chủ và sau đó máy chủ sẽ tiếp tục gửi các gói âm thanh sau đến các thiết bị nhúng khi nhận ACK. Luồng quy trình được minh họa tuần tự trong các hình dưới đây:



Hình 3. 13

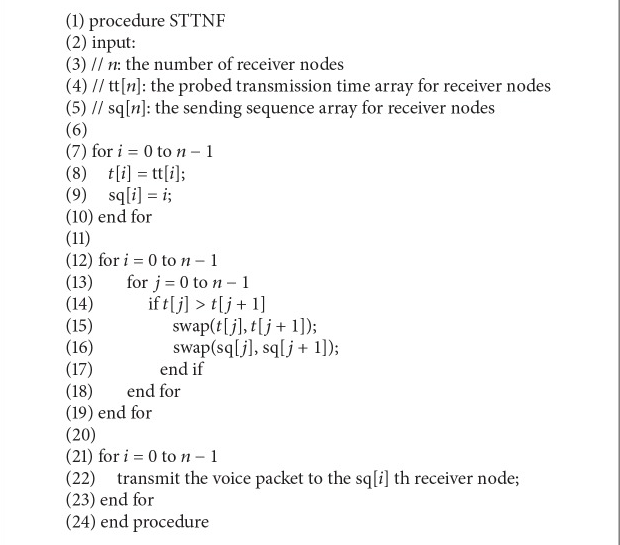


Hình 3. 14



Hình 3. 15

Vì nhiều người sử dụng hiện có thể nhận được giọng nói phát sóng, phía máy chủ sẽ gửi gói giọng nói để xâu chuỗi theo cách thức vòng tròn. Nếu máy chủ muốn truyền dữ liệu âm thanh đến các nút mạng khác nhau có tốc độ truyền khác nhau trong môi trường mạng không đồng nhất, tốt hơn hết là truyền các gói thoại đến nút mạng tốt hơn trước rồi đến kém hơn. Nút thời gian truyền ngắn nhất được đề xuất trước tiên có thể được trình bày như trong hình dưới:



Hình 3. 16

### 3.3.3. Chức năng tự động phát sóng

Hệ thống quản lý phương tiện của Open Broadcaster cung cấp tự động hóa dựa trên web đơn giản và hiệu quả với trình lập lịch biểu, quản lý thuận tiện đài của bạn từ mọi nơi, tạo danh sách nội dung có thể phát trên cả radio và TV trên mặt đất, bằng cách sử dụng kéo và thân thiện với thiết bị di động giao diện -drop '. Thiết lập nội dung lặp lại như nhận dạng đài, thông báo hoặc quảng cáo dịch vụ công cộng là "điểm và nhấp" dễ dàng, vì dựa trên web cung cấp một nền tảng tuyệt vời để lập trình chương trình hợp tác với khả năng gán thời gian cho người dùng bằng quản lý từ xa.

Sử dụng hệ thống cấp phép cực kỳ an toàn của Open Broadcaster, quản trị viên đài có thể cho phép truy cập cho các DJ và những người đam mê radio, trên toàn cầu, cho phép họ đăng nhập và lập trình chương trình của riêng họ ở bất cứ đâu trên thế giới.

Hệ thống tự động hóa vô tuyến của chúng tôi đi kèm với một ứng dụng logger tích hợp để duy trì nhật ký chương trình chi tiết để tuân thủ các cơ quan quản lý hoặc chỉ chứng minh cho khách hàng rằng quảng cáo của họ nhận được thời gian không khí mà họ xứng đáng, tạo ra nhật ký bạn yêu cầu chỉ với nỗ lực tối thiểu và mở rộng tuổi thọ hoạt động của các máy phát hiện có trong dịch vụ bằng [cách thêm các tính năng mới](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://openbroadcaster.com/added-features&xid=17259,15700022,15700186,15700191,15700256,15700259,15700262,15700265&usg=ALkJrhjH_pC1BDdWy676MK9EcBsPQ4PxWg) để có thêm cơ hội tạo doanh thu. Tự động phát sóng thực sự không an toàn với phương tiện truyền thông cộng đồng từ bất kỳ trình duyệt nào.

[](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://openbroadcaster.com/streaming-and-hosting&xid=17259,15700022,15700186,15700191,15700256,15700259,15700262,15700265&usg=ALkJrhhzFMdpT87EozPfA7fK_RXsobmumw)

Hình 3. 17

Quản lý tập trung:

Cơ sở hạ tầng đám mây như một dịch vụ cung cấp Tự động hóa Hệ thống Quản lý Phát sóng không an toàn với lệnh đa kênh và kiểm soát các kênh và thiết bị phát không giới hạn. Quản lý hơn 100.000 tệp nhạc và video và các bộ sưu tập nhạc lớn với siêu dữ liệu có tổ chức và có thể tìm kiếm. Quản lý nhiều thể loại âm thanh và video, danh mục, sách nói, podcast và phim gia đình và bản ghi từ điện thoại di động của bạn để chia sẻ trực tuyến hoặc với luồng Icecastcast ảo.

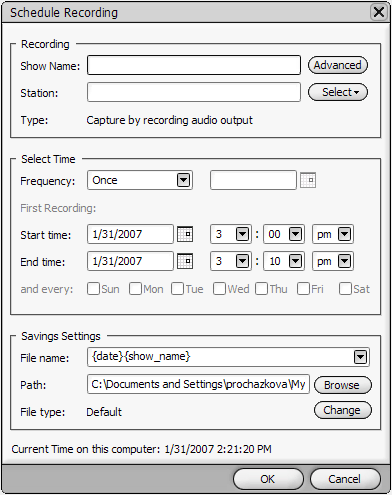
Quản lý thư viện phương tiện lớn. Phần mềm quản lý tài sản CNTT sao lưu kỹ thuật số phương tiện được lưu trữ trong một hệ thống an toàn, gửi đến mạng phân phối nội dung. Phương tiện truyền thông của bạn ở lại với bạn, trên đám mây riêng của bạn. Nghệ sĩ gắn thẻ trực quan, tiêu đề, nghệ thuật album và siêu dữ liệu tùy chỉnh khác.

* Quản lý tài sản truyền thông đám mây doanh nghiệp được thiết kế để phát sóng
* Dễ dàng tìm thấy các bài hát và các mục phương tiện với công cụ tìm kiếm tích hợp.
* Đầu phát sóng kỹ thuật số ảo kết thúc doanh nghiệp quản lý tài sản phi tập trung
* Tự động hóa đám mây với các tiện ích tự động hóa tiếp thị

### 3.3.4. Lập lịch phát thanh



Hình 3. 18



Hình 3. 19

Mở máy chủ đài phát thanh và các hệ thống lập lịch chạy các dịch vụ webcast radio và lập lịch cho phép tiện ích API. Sử dụng luân phiên lập lịch để tạo lập trình chia nguồn cấp dữ liệu, quản lý mạng lưới lịch biểu với thay thế ID / PSA. Phần mềm lập lịch phát thanh cho phép thực hiện các bộ đệm theo dõi giọng nói, quét, sting và ID trạm. Phần mềm lập lịch âm nhạc cho phép các phân đoạn nhạc dựa trên chủ đề được gán cho người dùng cập nhật từ máy tính ở nhà của họ bằng một trình duyệt đơn giản như một phần của hệ thống lập lịch phát phương tiện dựa trên thời gian tự động để xoay vòng quảng cáo chính xác.

### 3.3.5. Xác thực người nghe

Xác thực người nghe là một tính năng của phần mềm cho phép bảo mật một điểm gắn kết nhất định để để nghe, người nghe phải vượt qua một số kiểm tra để xác minh. Với tính năng này, có thể thực hiện thao tác trả tiền để sử dụng (ví dụ: user / password) hoặc một số bộ lọc dựa trên kết nối người nghe. Ở đây này sẽ thiết lập và duy trì những điều cơ bản của phần này.

Để xác định xác thực người nghe, một nhóm thẻ được chỉ định trong nhóm <mount> liên quan đến điểm gắn kết. Điều này có nghĩa là xác thực có thể áp dụng cho người nghe của các máy khách nguồn hoặc rơle.

Các cơ chế xác thực sau đây có thể áp dụng cho người nghe:

* htpasswd: tra cứu một tệp có tên cho tên người dùng và mật khẩu phù hợp
* URL: phát hành các yêu cầu web (ví dụ: PHP) để khớp với xác thực

Xác thực người nghe trong một giá trị được chỉ định trong cấu hình XML có thể áp dụng cho một luồng từ máy khách nguồn, rơle hoặc tệp dựa trên webroot. Chúng được áp dụng cho các tệp giới thiệu hoặc luồng dự phòng.

### 3.3.6. Hệ thống cảnh báo khẩn cấp

Giới thiệu:

Chúng tôi cung cấp các giải pháp EAS đáng tin cậy cho lĩnh vực phát sóng trên toàn cầu. Các hệ thống cảnh báo dân số khẩn cấp nguồn mở Ubuntu Linux của chúng tôi hoạt động ở mọi nơi bằng cách sử dụng các giao thức internet được tiêu chuẩn hóa với Giao thức [EAS](https://translate.googleusercontent.com/translate_c?depth=1&hl=vi&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://openbroadcaster.com/emergency-alerting-systems&xid=17259,15700022,15700186,15700191,15700256,15700259,15700262,15700265&usg=ALkJrhgwQLAKZ2Obx3OWdW6ApptFnzySJw) dựa trên phần mềm tự động vô tuyến của Google. Tất cả được thiết kế cho các hệ thống cảnh báo khẩn cấp trong nhiều môi trường kênh đa trạm bao gồm đài phát thanh trên không, TV kỹ thuật số ASTC và đèn LED hiển thị kỹ thuật số LED cảnh báo cho thảm họa cộng đồng và đóng cửa trường học. Hệ thống radio triển khai nhanh cung cấp các thông điệp cảnh báo không có giám sát, tự động ra lệnh và điều khiển các đài phát thanh, Truyền hình cáp CATV hoặc máy phát truyền hình kỹ thuật số để tạo các trạm phát khẩn cấp khi đang di chuyển. Tích hợp cắm và phát để phát trực tuyến EAS theo yêu cầu với thiết bị BARIX và hỗ trợ bảng điều khiển kỹ thuật số AoIP RTP Livewire.

Trong thực tế thường xuyên, EAS thường được sử dụng để phân phối thông tin liên quan đến các mối đe dọa sắp xảy ra đối với an toàn công cộng trong một khu vực nhỏ hơn, chẳng hạn như tình hình thời tiết khắc nghiệt (bao gồm lũ quét và lốc xoáy), Cảnh báo bắt cóc trẻ em và các trường hợp khẩn cấp khác.

Các tổ chức được ủy quyền có thể phổ biến và phối hợp các cảnh báo khẩn cấp và thông điệp cảnh báo thông qua EAS. Hệ thống cảnh báo và cảnh báo công cộng tích hợp (IPWAS) được sử dụng làm phụ trợ để phân phối thông tin cảnh báo thông qua EAS và các công nghệ liên quan như Cảnh báo khẩn cấp không dây (WEA), sử dụng Giao thức cảnh báo chung (CAP). [2] Tin nhắn EAS được truyền chủ yếu qua đài phát thanh và truyền hình vệ tinh mặt đất và truyền hình (bao gồm cả truyền hình và truyền hình đa kênh), được yêu cầu tham gia vào hệ thống.

Kỹ thuật sử dụng:

Các thông báo trong EAS bao gồm bốn phần: tiêu đề Mã hóa thông điệp khu vực cụ thể (SAME) được mã hóa kỹ thuật số, tín hiệu chú ý, thông báo âm thanh và điểm đánh dấu cuối tin nhắn được mã hóa kỹ thuật số.

### 3.3.7. Chứng thực thiết bị đầu cuối

Ngày nay hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức, đem lại khả năng xử lý thông tin, nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu. Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống  thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

Song song với việc xây dựng hệ thống thông tin hiện đại, đáp ứng nhu cầu của các cơ quan, tổ chức cần phải bảo vệ hệ thống thông tin, đảm bảo cho hệ thống đó hoạt động ổn định và tin cậy. An toàn và bảo mật thông tin là thiết yếu trong mọi cơ quan, tổ chức.

Vấn đề đặt ra là chính sách bảo mật xác định cần phải bảo vệ tài nguyên gì (bảo vệ tài nguyên vật lý, thông tin, bản quyền..), mức độ bảo vệ như thế nào ?

Do vậy, cần phải xây dựng phần mềm chứng thực thiết bị đầu cuối để không bị các thành phần xấu hack và lợi dụng hệ thống của chúng ta. Ở đây chúng ta sẽ sử dụng mã OTP:

OTP là viết tắt của One Time Password, có nghĩa là mật khẩu một lần. Đây là loại mật khẩu đặc biệt chỉ có thể sử dụng một lần và bị giới hạn thời gian sử dụng, thông thường sẽ bị mất hiệu lực trong vài phút. Bình thường, khi bạn tạo một tài khoản nào đó, mật khẩu là do bạn tự tạo ra nhưng với mật khẩu OTP thì khác, bạn không thể tạo ra OTP cũng không thể thay đổi OTP, loại mã này là do ngân hàng cung cấp, sẽ được gửi về máy điện thoại qua tin nhắn SMS mỗi lần bạn yêu cầu giao dịch. Đây được coi là loại mật khẩu cấp 2 trong chế độ bảo mật hai lớp khi sử dụng Internet Banking. Mã OTP giúp gia tăng sự an toàn đối với các giao dịch thanh toán online.

Như các bạn đã biết, mã OTP là loại mật khẩu chỉ được sử dụng một lần, nên sau khi giao dịch, ngay cả khi bạn để lộ mã OTP cũ và mật khẩu tài khoản ngân hàng thì kẻ gian cũng không lấy được tiền của bạn. Về bản chất, [**mã OTP**](https://topbank.vn/tu-van/ma-otp-la-gi-su-dung-ma-otp-nhu-the-nao-np20180502103020845) chính là một loại mã an toàn được gửi về điện thoại giúp bạn xác nhận lại giao dịch lần cuối. Với hình thức này, kẻ gian chỉ có thể lấy tiền hoặc thực hiện giao dịch online trên tài khoản của bạn nếu như hắn có trong tay cả mật khẩu Internet Banking, điện thoại cũng như mật khẩu mở khóa điện thoại để đọc được tin nhắn SMS. Nếu như các ngân hàng không sử dụng mã OTP mà chỉ sử dụng bảo mật một lớp như trước kia, trong bối cảnh tội phạm công nghệ đang phát triển như hiện nay, nguy cơ mất tiền trong tài khoản của khách hàng là rất cao.

**Cách sử dụng mã OTP** rất đơn giản và gần như là tự động, mã sẽ được ngân hàng gửi về số điện thoại đăng ký trên thông tin tài khoản ngân hàng. Giả sử bạn muốn chuyển tiền sang số tài khoản khác bằng Internet Banking, bạn tiến hành đăng nhập bình thường bằng tên tài khoản và mật khẩu tài khoản đã đăng ký. Sau khi bạn hoàn tất các thông tin giao dịch như người nhận, số tiền chuyển, hình thức chuyển,... ứng dụng Internet Banking của ngân hàng sẽ yêu cầu bạn kiểm tra lại thông tin giao dịch một lần nữa kèm theo nút "Lấy mã OTP". Sau khi nhất vào nút "Lấy mã OTP", một đoạn mã bằng số thường gồm 4 đến 6 ký tự (tùy ngân hàng) sẽ được gửi về điện thoại của bạn trong vòng vài phút. Lúc này bạn chỉ cần nhập mã OTP trên ứng dụng để xác nhận yêu cầu giao dịch lần cuối.

**[](https://img.topbank.vn/2018/05/02/jDFnkIeH/ma-otp-one-time-pass-6c73.png)**

Hình 3. 20:

Ngoài ra, khi nhập thông tin thanh toán online dùng thẻ ghi nợ, [**thẻ tín dụng**](https://topbank.vn/the-tin-dung), mặc định **mã OTP** cũng sẽ được gửi về số điện thoại để người dùng xác nhận giao dịch. Bằng cách này, dù bạn có bị mất thẻ thì kẻ gian cũng chưa chắc lấy được tiền của bạn.

Có thể nói, mã OTP sẽ an toàn tuyệt đối nếu như bạn tuân thủ đúng các nguyên tắc cũng như quy trình sử dụng dịch vụ Internet Banking mà ngân hàng đưa ra. Đây là loại mã xác nhận vốn rất an toàn nhưng sẽ vẫn có kẽ hở nếu như bạn chủ quan. Điều gì sẽ xảy ra nếu như bạn sử dụng máy tính công cộng để đăng nhập vào tài khoản Internet Banking, bạn có việc ra ngoài và để quên luôn cả điện thoại bên cạnh máy, điều này hết sức nguy hiểm vì tài khoản của bạn sẽ chỉ được tự động đăng xuất sau vài phút, nếu như kẻ gian đủ nhanh, rất có thể bạn sẽ bị mất tiền.

Cũng vì thế mà các ngân hàng luôn khuyến cáo các khách hàng của mình không nên giao dịch thanh toán online trên máy tính công cộng, không đưa mã OTP cho người khác trong bất kỳ trường hợp nào cũng như phải nhanh chóng báo ngân hàng khóa chức năng giao dịch online khi điện thoại bị mất.

Như vậy, **mã OTP** hay mật khẩu một lần là một lớp bảo mật thứ hai rất hữu ích và bảo mật cho người dùng khi giao dịch online qua ứng dụng Internet Banking hay qua [**các loại thẻ tín dụng**](https://topbank.vn/tu-van/the-tin-dung)**.** Hầu hết các ngân hàng trong nước cũng như quốc tế đều áp dụng hình thức gửi mã OTP để đảm bảo quyền lợi cho người dùng. Tuy nhiên, cũng không nên quá chủ quan khi nghĩ rằng tài khoản của chúng ta luôn an toàn vì có bảo mật hai lớp. Bất kỳ một giao dịch nào liên quan đến tài khoản cũng đều cần phải cận trọng và tuân thủ nhưng quy định do ngân hàng đưa ra.

## **3.4. Nghiên cứu, thiết kế mô hình phần cứng của hệ thống Khoa D16**

### 3.4.1. Máy chủ nội dung

Máy chủ (Tiếng anh là Server) là một máy tính được kết nối với một mạng máy tính hoặc internet, có IP tĩnh, có năng lực xử lý cao và trên đó người ta cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên. Như vậy về cơ bản máy chủ cũng là một máy tính, nhưng được thiết kế với nhiều tính năng vượt trội hơn, năng lực lưu trữ và xử lý dữ liệu cũng lớn hơn máy tính thông thường rất nhiều. Máy chủ thường được sử dụng cho nhu cầu lưu trữ và xử lý dữ liệu trong một mạng máy tính hoặc trên môi trường internet. Máy chủ là nền tảng của mọi dịch vụ trên internet, bất kỳ một dịch vụ nào trên internet muốn vận hành cũng đều phải thông qua một máy chủ nào đó.



Hình 3. 21

Có những loại máy chủ nào?

\*Căn cứ theo phương pháp tạo ra máy chủ người ta phân thành ba loại: Máy chủ ảo và máy chủ riêng và máy chủ đám mây.

Máy chủ riêng (Dedicated Server): là máy chủ chạy trên phần cứng và các thiết bị hỗ trợ riêng biệt gồm: HDD, CPU, RAM, Card mạng, . Việc nâp cấp hoặc thay đổi cấu hinh của máy chủ riêng đòi hỏi phải thay đổi phần cứng của máy chủ

Máy chủ ảo (Virtual Private Server - VPS): là dạng máy chủ được tạo thành bằng phương pháp sử dụng công nghệ ảo hóa để chia tách từ một máy chủ riêng thành nhiều máy chủ ảo khác nhau. Các máy chủ ảo có tính năng tương tự như một máy chủ riêng, nhưng chạy chia sẻ tài nguyên từ máy chủ vật lý gốc. Việc nâng cấp hoặc thay đổi cấu hình của máy chủ ảo rất đơn giản, có thể thay đổi trực tiếp trên phần mềm quản lý hệ thống. Tuy nhiên việc thay đổi tài nguyên của máy chủ ảo phụ thuộc và bị giới hạn bởi tài nguyên của máy chủ vật lý.

Máy chủ đám mây (Cloud Server): là máy chủ được kết hợp nhiều từ máy chủ vật lý khác nhau cùng với hệ thống lưu trữ SAN với tốc độ truy xuất vượt trội giúp máy chủ hoạt động nhanh, ổn định, hạn chế mức thấp tình trạng downtime. Máy chủ Cloud được xây dựng trên nền công nghệ điện toán đám mây nên dễ dàng nâng cấp từng phần thiết bị trong quá trình sử dụng mà không làm gián đoạn quá trình sử dụng máy chủ.

Phân biệt 3 loại máy chủ (server): máy chủ ảo, máy chủ riêng, máy chủ đám mây:

Cloud server:

Tính sẵn sàng:

* Data lưu trữ taajo trung trên hệ thống SAN không lưu trên server vật lý
* Data đưuọc bakup đều đặn
* Nếu có một server vật lý bị lỗi, cloud server của bạn vẫn hoạt động bình thường

Khả năng mở rộng:

* Khả năng mở rộng là ngay lập tức khi có nhu cầu
* Hạ thấp server khi cảm thấy không cần sử dụng nhiều tài nguyên như thế
* Khả năng sử dụng tài nguyên linh hoạt giúp tiết kiệm chi phí

Chi phí:

* Bạn chỉ cần chỉ trả cho những gì bạn sử dụng( cpu, ram, dung lượng,...)
* Bạn có thể nâng cấp/ hạ cấp tài nguyên giúp bạn tiết kiệm được chi phí

Máy chủ riêng:

Tính sẵn sàng:

-Tất cả data sẽ được lưu trữ trên máy vật lý (Rủi ro cao)

-Chỉ cần 1 HDD bị hỏng có thể toàn bộ data của bạn sẽ mất

-Việc triển khai backup tốn nhiều chi phí

Khả năng mở rộng:

-Nâng cấp phức tạp vì phải mua thiết bị phần cứng chuyên dụng

-Thời gian downtime Server cao khi nâng cấp

-Chi phí phần cứng cao

Chi phí:

-Trả chi phí cho toàn bộ máy chủ vật lý

-Để duy trì Server bạn cần trả các khoản chi phí điện, hệ thống mạng, chi phí bảo trì Server

Máy chủ ảo:

Tính sẵn sàng:

-VPS được khởi tạo và chạy trên 1 máy chủ vật lý

-Vào thời gian cao điểm máy chủ vật lý có thể treo dẫn đến các VPS có thể tạm ngưng hoạt động

Khả năng mở rộng:

-Các tài nguyên được ảo hóa và cung cấp cho người dùng VPS

-Không thể nâng cấp tài nguyên lớn vì server vật lý sẽ không đủ tài nguyên cung cấp

Chi phí:

-Bạn phải chi trả số tiền theo cấu hình Vps của bạn đã mua

-Việc sử dụng chung Server vật lý khiến VPS của bạn bị phụ thuộc

Căn cứ theo công dụng, chức năng của máy chủ người ta phân ra các loại máy chủ: Web server, Database server, FTP server, SMTP server (email sever), DNS sever, DHCP server.

* Máy chủ web (Web Server) là máy chủ mà trên đó cài đặt phần mềm phục vụ web, đôi khi người ta cũng gọi chính phần mềm đó là web server. Tất cả các web server đều hiểu và chạy được các file \*.htm và \*.html. Tuy nhiên mỗi web server lại phục vụ một số kiểu file chuyên biệt chẳng hạn như llS của Microsoft dành cho \*.asp, \*.aspx…; Apache dành cho \*.php…; Sun Java system web server của SUN dành cho \*.jsp…
* Máy chủ Database (Database Server): máy chủ mà trên đó có cài đặt phần mềm Hệ quản trị cơ sở dữ liệu. Chúng ta có hệ quản trị CSDL chẳng hạn như: SQL server, MySQL, Oracle…
* Máy chủ FTP (FTP server): FTP (viết tắt của File Transfer Protocol dịch ra là "Giao thức truyền tập tin") thường được dùng để trao đổi tập tin qua mạng lưới truyền thông dùng giao thức TCP/IP (chẳng hạn như Internet - mạng ngoại bộ - hoặc intranet - mạng nội bộ). Hoạt động của FTP cần có hai máy tính, một máy chủ và một máy khách). Máy chủ FTP dùng chạy phần mềm cung cấp dịch vụ FTP, gọi là trình chủ, lắng nghe yêu cầu về dịch vụ của các máy tính khác trên mạng lưới. Máy khách chạy phần mềm FTP dành cho người sử dụng dịch vụ, gọi là trình khách, thì khởi đầu một liên kết với máy chủ.
* Máy chủ SMTP (SMTP server): SMTP (Simple Mail Transfer Protocol - giao thức truyền tải thư tín đơn giản) là một chuẩn truyền tải thư điện tử qua mạng Internet. SMTP server là máy chủ giúp bạn gửi mail đến các địa chỉ email khác trên internet.
* Máy chủ DNS (DNS Server) là máy chủ phân giải tên miền. Mỗi máy tính, thiết bị mạng tham gia vào mạng Internet đều kết nối với nhau bằng địa chỉ IP (Internet Protocol). Để thuận tiện cho việc sử dụng và dễ nhớ ta dùng tên (domain name) để xác định thiết bị đó. Hệ thống tên miền DNS (Domain Name System) được sử dụng để ánh xạ tên miền thành địa chỉ IP.
* Máy chủ DHCP (DHCP server): DHCP (Dynamic Host Configuration Protocol - giao thức cấu hình động máy chủ) là một giao thức cấu hình tự động địa chỉ IP. Máy tính được cấu hình một cách tự động vì thế sẽ giảm việc can thiệp vào hệ thống mạng. DHCP server là máy chủ có cài đặt dịch vụ DHCP, nó có chức năng quản lý sự cấp phát địa chỉ IP động và các dữ liệu cấu hình TCP/IP. Ngoài ra còn có nhiệm vụ trả lời khi DHCP Client có yêu cầu về hợp đồng thuê bao.

### 3.4.2. Steaming server:

Nếu bạn làm việc trong một môi trường có các hoạt động chia sẻ file thông qua một network, có thể bạn sẽ nghĩ ngay đến một máy tính được sử dụng làm server với rất nhiều dữ liệu chứa đựng bên trong.

Tuy nhiên, khi nói đến truyền phát video và audio trực tuyến, server lúc này không còn chỉ là một ổ cứng cực đại. Đó còn là phần mềm truyền dữ liệu đến máy tính của bạn. Một số streaming servers có thể xử lý rất nhiều kiểu file khác nhau, trong khi những nền tảng còn lại chỉ làm việc với các định dạng cụ thể. Ví dụ: Apple QuickTime Streaming Server có thể truyền trực tuyến các tệp QuickTime chứ không phải tệp Windows Media.

Cách thức hoạt động của streaming server:

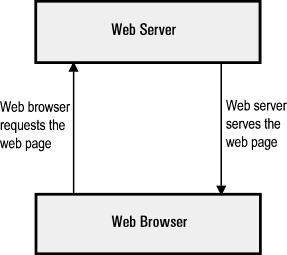
-Streaming server trong quá trình truyền dữ liệu cũng có sự tham gia của web server. Đầu tiên, bạn vào một web page (trang web) được lưu trữ trên web server. Khi bạn click vào file mình muốn truy cập, Web server sẽ truyền tín hiệu đến streaming server và cho server biết file mà bạn muốn dùng. Streaming server sẽ gửi dữ liệu trực tiếp trả về cho bạn, mà không cần qua Web server nữa.

-**Webser hoạt động như thế nào**?

Bất cứ khi nào bạn xem một trang web trên internet, có nghĩa là bạn đang yêu cầu trang đó từ một web server.

Khi bạn nhập URL trên trình duyệt của mình (ví dụ: https://tech.vccloud.vn), trình duyệt của bạn yêu cầu trang từ web server và web server sẽ gửi lại trang.

Biểu đồ bên là một trình bày đơn giản về những gì sẽ xảy ra.



Hình 3. 22

1. Trình duyệt phân giải tên miền thành địa chỉ IP

Trình duyệt web của bạn trước tiên cần phải xác định địa chỉ IP nào mà tên miền tech.vccloud.vn trỏ về. Nếu thông tin này không được lưu trữ sẵn trong bộ nhớ cache, trình duyệt sẽ yêu cầu thông tin từ một hoặc nhiều máy chủ DNS (thông qua internet). Máy chủ DNS sẽ cho trình duyệt biết địa chỉ IP nào tên miền sẽ trỏ đến (cũng là nới đặt trang web).

Lưu ý rằng địa chỉ IP sẽ được chỉ định khi trang web được tạo lần đầu trên máy chủ web.

2. Trình duyệt yêu cầu URL đầy đủ

Bây giờ trình duyệt web đã biết địa chỉ IP của trang web, nó có thể yêu cầu URL đầy đủ từ web server.

3. Web server gửi Trang được yêu cầu

Web server phản hồi bằng cách gửi lại trang được yêu cầu. Nếu trang không tồn tại (hoặc có lỗi khác xảy ra), nó sẽ gửi lại thông báo lỗi thích hợp.

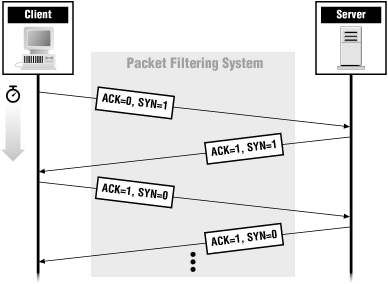
4. Trình duyệt hiển thị trang web

Trình duyệt web của bạn nhận được trang và hiển thị trang theo yêu cầu.

Khi nói đến các trình duyệt web và web server theo cách này, ta cũng co thể hiểu theo các khái niệm máy khách (trình duyệt web) và máy chủ (web server).

-Tất cả các dữ liệu này sẽ được chuyển đến nơi chúng cần phải đến nhờ một bộ quy tắc được gọi là giao thức với nhiệm vụ điều chỉnh cách dữ liệu truyền từ thiết bị này sang thiết bị khác. Trong đó có một giao thức gọi là giao thức truyền siêu văn bản (HTTP) xử lý các tài liệu siêu văn bản, hoặc các trang Web. Mỗi khi một người nào đó đang lướt web, người đó đang sử dụng HTTP.

-Có rất nhiều giao thức ví dụ như giao thức kiểm soát đường truyền TCP và giao thức chuyển giao file FTP chia nhỏ dữ liệu thành các gói tin. Giao thức này có thể gửi lại các gói tin bị mất hoặc hỏng và cho phép các gói ngẫu nhiên được tập hợp lại sau. Như vậy, việc tải xuống các tệp và lướt web sẽ trở nên thuận tiện hơn - nếu lưu lượng truy cập web chậm hoặc một số gói tin bị mất, bạn vẫn sẽ nhận được tệp của mình. Tuy nhiên, những giao thức này lại không cho kết quả tốt với truyền phát trực tuyến. Với truyền phát trực tuyến, dữ liệu cần đến nhanh chóng với tất cả các gói theo đúng thứ tự.



Hình 3. 23

Các giao thức như TCP chia dữ liệu thành các gói tin

-Vì lý do này, streaming audio và video sử dụng loại giao thức để truyền dữ liệu theo thời gian thực. Các giao thức sẽ chia nhỏ file thành các mảnh ghép dữ liệu nhỏ và gửi chúng đến một vị trí cụ thể với thứ tự cụ thể. Các giao thức này bao gồm;

Real-time transfer protocol (RTP)

-Giao thức vận chuyển thời gian thực đặc tả một tiêu chuẩn định dạng gói tin dùng để truyền âm thanh và hình ảnh qua internet. Tiêu chuẩn này được khai báo trong RFC 1889. Nó được phát triển bởi nhóm Audio Video Transort Woking và được ban hành lần đầu tien vào năm 1996.

-RTP và RTCP liên kết chặt chẽ với nhay –RTP truyền dữ liệu thực trong RICP được dùng để nhận thông tin phản hồi về chất lượng dịch vụ.

Real-time streaming protocol (RTSP)

-RTSP là một giao thức ở tầng ứng dụng trong bộ các giáo thức internet ( Internet Protocol Suite) để kiểm soát, truyền theo yêu cầu của dữ liệu thời gian thực, chẳng hạn như âm thanh và video.

- RTCP được sử dụng để thiết lập và quản lý các phiên làm việc giữa cám điểm truyền, phát tin đa phương tiện.

Real-time transport control protocol (RTCP)

-PTMP(Real Time Mesging Protocol) là giao thức công khai do Adobe phát triển và giữ bản quyền, được thiết kế cho ứng dụng thời gian thực, cho phép ứng dụng sử dụng video và âm thanh với tốc độ cao, hạn chế bị giật hình hoặc méo tiếng.

Các lựa chọn streaming

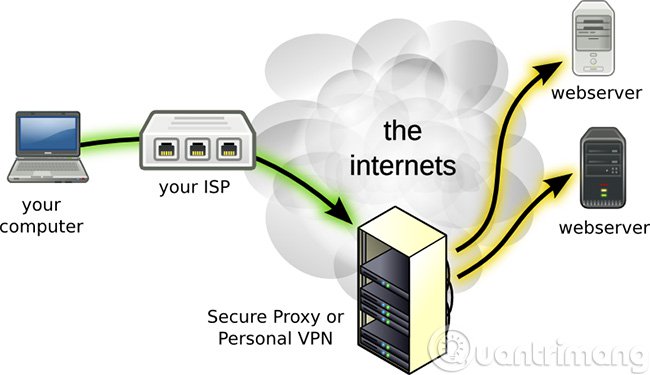
Các giao thức này hoạt động như một lớp được thêm vào các giao thức quản lý web traffic. Do đó, khi các giao thức real time đang truyền tải dữ liệu cần truyền đi, các giao thức Web khác vẫn hoạt động ngầm phía dưới. Các giao thức này cũng phối hợp với nhau để cân bằng tải cho server. Nếu có quá nhiều cùng truy cập 1 file vào cùng một thời điểm, server có thể ngừng khởi động một vài đường truyền phát cho tới khi những đường truyền khác đã tải xong.

Trực tiếp hoặc theo yêu cầu: Live webcast sẽ đòi hỏi một số thiết bị bổ trợ. Sẽ cần một máy tính cố định để nén, encode và truyền trực tuyến nguồn cấp dữ liệu video trong thời gian thực hoặc liên kết vệ tinh đến một công ty có thể thực hiện công việc này.

Unicast hoặc multicast: Trong unicast stream, mỗi người xem sẽ có nguồn data truyền phát riêng. Trong truyền phát multicast, một một luồng dữ liệu sẽ di chuyển đến một router, router này sẽ sao chép luồng dữ liệu đó và gửi tới nhiều người xem. Unicast stream đòi hỏi nhiều khả năng xử lý và băng thông hơn.

**VPN - Mạng riêng ảo:**

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.



Hình 3. 24

Một hệ thống VPN có thể kết nối được nhiều site khác nhau, dựa trên khu vực, diện tích địa lý... tượng tự như chuẩn Wide Area Network (WAN). Bên cạnh đó, VPN còn được dùng để "khuếch tán", mở rộng các mô hình Intranet nhằm truyền tải thông tin, dữ liệu tốt hơn. Ví dụ, các trường học vẫn phải dùng VPN để nối giữa các khuôn viên của trường (hoặc giữa các chi nhánh với trụ sở chính) lại với nhau.

Nếu muốn kết nối vào hệ thống VPN, thì mỗi 1 tài khoản đều phải được xác thực (phải có Username và Password). Những thông tin xác thực tài khoản này được dùng để cấp quyền truy cập thông qua 1 dữ liệu - Personal Identification Number (PIN), các mã PIN này thường chỉ có tác dụng trong 1 khoảng thời gian nhất định (30s hoặc 1 phút).

Khi kết nối máy tính hoặc một thiết bị khác chẳng hạn như điện thoại, máy tính bảng với một VPN, máy tính hoạt động giống như nó nằm trên cùng mạng nội bộ với VPN. Tất cả traffic trên mạng được gửi qua kết nối an toàn đến VPN. Nhờ đó, bạn có thể truy cập an toàn đến các tài nguyên mạng nội bộ ngay cả khi đang ở rất xa.

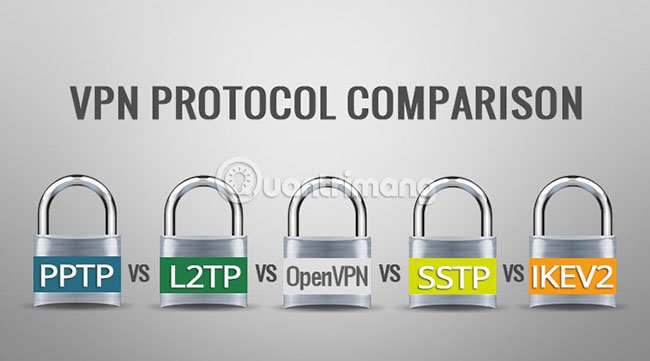
Bạn cũng có thể sử dụng Internet giống như đang ở vị trí của của VPN, điều này mang lại một số lợi ích khi sử dụng WiFi public hoặc truy cập trang web bị chặn, giới hạn địa lý.

Khi duyệt web với VPN, máy tính sẽ liên hệ với trang web thông qua kết nối VPN được mã hóa. Mọi yêu cầu, thông tin, dữ liệu trao đổi giữa bạn và website sẽ được truyền đi trong một kết nối an toàn.

**Các giao thức thường dùng trong VPN**

Bản chất của giao thức VPN là một tập hợp các giao thức:

PPTP, L2TP, OpenVPN, SSTP, IKEV2, SoftEther, IP security



Hình 3. 25

Các chức năng của VPN giải quyết được:

- Tunnelling (kỹ thuật truyền dữ liệu qua nhiều mạng có giao thức khác nhau) - Chức năng cơ bản của VPN là phân phối các gói (packet) từ điểm này đến điểm khác mà không để lộ chúng cho bất kỳ ai trên đường truyền. Để làm điều này, VPN đóng gói tất cả dữ liệu theo định dạng mà cả máy khách và máy chủ đều hiểu được. Bên gửi dữ liệu đặt nó vào định dạng tunnelling và bên nhận trích xuất để có được thông tin.

- Mã hóa: Tunnelling không cung cấp tính năng bảo vệ. Bất cứ ai cũng có thể trích xuất dữ liệu. Dữ liệu cũng cần phải được mã hóa trên đường truyền. Bên nhận sẽ biết cách giải mã dữ liệu từ một người gửi nhất định.

- Xác thực. Để bảo mật, VPN phải xác nhận danh tính của bất kỳ client nào cố gắng “giao tiếp” với nó. Client cần xác nhận rằng nó đã đến đúng máy chủ dự định.

- Quản lý phiên: Một khi người dùng được xác thực, VPN cần duy trì phiên để client có thể tiếp tục “giao tiếp” với nó trong một khoảng thời gian.

Nói chung các giao thức VPN coi việc tạo tunnel, xác thực và quản lý phiên như một gói. Điểm yếu trong bất kỳ chức năng nào đều là những lỗ hổng bảo mật tiềm ẩn trong giao thức. Mã hóa là một chuyên ngành, nó cũng rất khó, nên thay vì cố gắng tạo ra cái mới, các VPN thường sử dụng kết hợp nhiều giao thức mã hóa đáng tin cậy. Dưới đây là những giao thức VPN phổ biến và độ mạnh yếu của chúng.

Ưu, nhược điểm của VPN:

Khi áp dụng vào thực tế thì VPN sẽ có những ưu, nhược điểm như thế nào. Mời các bạn tiếp tục thảo luận với Quản Trị Mạng.

Để xây dựng 1 hệ thống mạng riêng, mạng cá nhân ảo thì dùng VPN là 1 giải pháp không hề tốn kém. Chúng ta có thể tưởng tượng thế này, môi trường Internet là cầu nối, giao tiếp chính để truyền tải dữ liệu, xét về mặt chi phí thì nó hoàn toàn hợp lý so với việc trả tiền để thiết lập 1 đường kết nối riêng với giá thành cao. Bên cạnh đó, việc phải sử dụng hệ thống phần mềm và phần cứng nhằm hỗ trợ cho quá trình xác thực tài khoản cũng không phải là rẻ. Việc so sánh sự tiện lợi mà VPN mang lại cùng với chi phí bỏ ra để bạn tự thiết lập 1 hệ thống như ý muốn, rõ ràng VPN chiếm ưu thế hơn hẳn.

Nhưng bên cạnh đó, có nhược điểm rất dễ nhận thấy như:

VPN không có khả năng quản lý Quality of Service (QoS) qua môi trường Internet, do vậy các gói dữ liệu - Data package vẫn có nguy cơ bị thất lạc, rủi ro. Khả năng quản lý của các đơn vị cung cấp VPN là có hạn, và có nguy cơ bị lấy dữ liệu.

### 3.4.3. Máy tính trạm hay máy Workstation là gì

Workstation là một dòng máy tính trạm được thiết kế dành riêng để chạy các ứng dụng kỹ thuật hoặc khoa học. Mục đích chính để tạo ra những chiếc máy tính này là phục vụ những người có nhu cầu sử dụng máy tính cao, nhất là các phần mềm nặng có thể kết nối với nhau qua mạng và phục vụ nhiều User cùng 1 lúc, có khả năng chạy liên tục hàng tháng hàng năm mà máy vẫn bền.

Hiện nay, máy tính trạm được cung cấp hiệu suất cao hơn máy tính để bàn, nhất là về CPU, đồ họa, bộ nhớ và khả năng xử lý đa nhiệm của máy. Máy tính được tối ưu hóa để xử lý các loại dữ liệu phức tạp khác nhau như các bản vẽ 3D trong cơ khí, mô phỏng trong thiết kế, hình ảnh động và logic toán học.

Về mục đích sử dụng của máy trạm Workstation:

Máy trạm chủ yếu dành cho nhu cầu sử dụng doanh nghiệp hay chuyên nghiệp (máy chủ, thiết kế, đồ họa,...), được thiết kế và cấu hình cho các ứng dụng kỹ thuật (CAD/CAM), phát triển phần mềm, các kiến trúc sư, nhà thiết kế đồ họa,... hay bất cứ ai có nhu cầu sức mạnh điện toán vừa phải, dung lượng bộ nhớ RAM lớn và các khả năng đồ họa tương đối cao cấp, đặc thù của máy trạm là được liên kết với nhau thành một mạng cục bộ LAN.



Hình 3. 26

Hai hệ điều hành chủ yếu thường được sử dụng cho máy trạm là Unix và Windows NT, máy trạm workstation vốn được những nhà sản xuất vô cùng tỉ mỉ, một số hãng máy trạm thành công nhất phải kể tới Sun Microsystems, Dell, IBM, HP.

Về khía cạnh hệ thống mạng lưới (network), thực tế là trong môi trường công ty ngày nay, nhiều nhân viên vẫn thường có những máy trạm workstation như vậy. Chúng đơn giản chỉ là những chiếc máy tính cá nhân được kết nối với mạng LAN để chia sẻ các nguồn tài nguyên của một hay nhiều máy tính lớn hơn và cũng vì chúng vốn là máy tính cá nhân, nên các máy trạm workstation có thể được sử dụng một cách độc lập khỏi máy Mainframe do chúng có những phần mềm ứng dụng riêng được cài đặt và có ổ đĩa cứng riêng.

Sự khác nhau giữa máy trạm và máy chủ?

Máy chủ :là một máy tính được nối mạng, nó quản lý tài nguyên của mạng, có IP tĩnh, có năng lực xử lý cao và trên máy đó người ta cài đặt các phần mềm để phục vụ cho các máy tính khác (máy trạm) truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên. Máy chủ đôi khi còn được gọi là hệ thống cuối

Ví dụ như, một máy dịch vụ tập tin là một máy tính hoặc là một thiết bị chuyên dụng để lưu trữ các tập tin. Bất kỳ người sử dụng nào trên mạng cũng có thể lưu trữ các tập tin trên máy chủ. Máy chủ Server thì có mục đích phục vụ cho nhiều nhu cầu của nhiều người. Các yêu cầu này được gởi tới từ các client trong quá trình hoạt động nhằm để lấy các thông tin dùng chung mà vì lý do phân cấp quản lý dữ liệu tập trung và chính sách bảo mật mà phải lưu trữ trên máy chủ

Máy trạm ( client) :Một máy tính dành cho cá nhân sử dụng nhưng có cấu hình mạnh hơn, chạy nhanh hơn, và có nhiều khả năng hơn một máy tính cá nhân thông dụng. Máy trạm chủ yếu dành cho nhu cầu sử dụng doanh nghiệp hay chuyên nghiệp (hơn là dùng cho nhu cầu gia đình hay giải trí). Nó được thiết kế và cấu hình cho các ứng dụng kỹ thuật (CAD/CAM), phát triển phần mềm, các kiến trúc sư, nhà thiết kế đồ họa,… hay bất cứ ai có nhu cầu sức mạnh điện toán vừa phải, dung lượng bộ nhớ RAM lớn, và các khả năng đồ họa tương đối cao cấp.

Hai hệ điều hành thường được dùng cho máy trạm là Unix và Windows NT.

Máy trạm chỉ là một máy tính dùng phục vụ nhu cầu làm việc, học hành, vui chơi của con người mà mỗi Client tùy theo mục đích sử dụng thì được trang bị các tính năng và chương trình riêng.

Cách lựa chọn Workstation phù hợp với nhu cầu:

Do tính chất đa dạng về mục đích của nhu cầu sử dụng máy trạm workstion và cũng một phần kinh nghiệm được tích lũy khi trao đổi với khách hàng, thì Máy Chủ Net có những gợi ý sẽ giúp cho các bạn có thể lựa chọn cho mình một máy trạm Workstation thích hợp.

Nếu chi phí cho phép, các bạn nên sử dụng các loại máy trạm workstation được lắp ráp và sản xuất tại hãng như DELL, HP, Lenovo,... Tốt nhất nên chọn các sản phẩm từ 2 hãng được nhiều người tin dùng như là DELL và HP. Các dòng máy trạm được sản xuất và lắp ráp tại hãng thường có giá cao hơn so với các máy tính Workstation được lắp ráp trong nước với cùng cấu hình. Nhưng thay vào đó bạn sẽ có được một máy trạm workstation đạt tiêu chuẩn và được hưởng những chính sách hỗ trợ tốt nhất từ chính hãng sản xuất.

### 3.4.4. Máy thu internet radio

### 3.4.5. Máy giải mã RDS\_OTP

RDS hoặc hệ thống dữ liệu radio là tiêu chuẩn trên hầu hết các đài phát thanh xe hơi và Hi-Fi tuners ngày hôm nay. RDS được sử dụng trên truyền phát sóng phát thanh VHF FM và cung cấp một số tiện ích được sử dụng rất lớn cho tất cả các thính giả Radio, nhưng đặc biệt là cho những người nghe radio trong xe hơi. RDS cho phép các báo cáo lưu lượng truy cập được nhận được dễ dàng hơn, và cung cấp nhiều tiện nghi bao gồm cho phép các đài phát thanh tên sẽ được hiển thị trên màn hình Radio.

Hệ thống này đã đạt được một số lượng đáng kể phổ biến và sử dụng rộng rãi ở châu Âu, nơi nó đã được thành lập trong nhiều năm.

RDS, phát triển hệ thống dữ liệu radio:

Phát triển hệ thống dữ liệu radio đã diễn ra chủ yếu ở châu Âu, nơi nó lần đầu tiên được phóng và triển khai.

Sự phát triển đầu tiên diễn ra tại Đức, nơi hệ thống đã được phát triển để đưa thông tin giao thông vào chương trình truyền hình FM sử dụng một subcarrier 57 kHz.

Sự phát triển thử nghiệm này đã được đưa lên bởi liên minh châu Âu Broadcasting, EBU khi trong 1974 Ủy ban kỹ thuật của họ đề xuất một sự phát triển của dự án Đức để thực hiện thông tin giao thông cũng như các dữ liệu khác. Nó cũng cho phép tự động điều chỉnh lại người nhận khi nó đi ra ngoài phạm vi của một máy phát, và nó cung cấp các tiện nghi như thông tin chương trình, v.v.

Sử dụng kinh nghiệm từ các chương trình ban đầu cũng như một định dạng điều chế từ một hệ thống phân trang Thụy Điển và baseband mã hóa được phát triển bởi British Broadcasting Corporation, BBC và đài phát thanh Ailen, IRT, các thông số kỹ thuật RDS đầu tiên đã được đưa ra trong 1984.

Tiêu chuẩn sau đó đã được tăng cường trong 1991 với các tính năng bao gồm cả chức năng tần số thay thế và nó đã được xuất bản dưới sự bảo trợ của Ủy ban châu Âu về tiêu chuẩn kỹ thuật điện, CENELEC.

Các tiện nghi của RDS:

Tại Bắc Mỹ ý tưởng này đã được đưa lên và Hoa Kỳ Đài phát thanh hệ thống quốc gia Ủy ban ban hành phiên bản của họ được gọi là đài phát thanh truyền dữ liệu hệ thống, RBDS trong 1992.

Các tiêu chuẩn CENELEC đã được Cập Nhật trong 1992 với việc bổ sung giao thông Message Channel và trong 1998 với các ứng dụng dữ liệu mở và, trong 2000, RDS đã được xuất bản trên toàn thế giới như là tiêu chuẩn IEC 62106.

Các tiện nghi của RDS:

Hệ thống RDS cung cấp một loạt các tiện nghi rất hữu ích. Một trong những công khai rộng rãi nhất là có thể cung cấp tin tức du lịch. Điều này có sẵn trên hầu hết các đài phát thanh địa phương. Tất cả các trạm truyền mã TP để xác định rằng tin nhắn du lịch được gắn cờ bởi RDS. Khi đài phát thanh được thiết lập cho tin tức du lịch, nó sẽ chỉ điều chỉnh cho các trạm mà thực hiện các chỉ dấu TP. Khi nhà ga là về để phát sóng một thông báo du lịch mã TA được truyền. Nếu một đĩa CD hoặc cassette đang được chơi sau đó hầu hết các bộ sẽ thực sự tạm dừng các đĩa CD hoặc băng và sau đó cho phép các thông báo đi du lịch để được lắng nghe. Ngoài ra, khối lượng này cũng có thể được thiết lập cao hơn một chút để cho phép thông báo được nghe dễ dàng hơn.

RDS tự động điều chỉnh:

AutotuningRDS mang lại trí thông minh vào điều chỉnh của một đài phát thanh. Các cơ sở tự điều chỉnh đi vào riêng của mình trên hành trình dài khi xe di chuyển từ khu vực dịch vụ của một máy phát để tiếp theo. Nếu không có RDS các đài phát thanh phải được điều chỉnh theo cách thủ công đến các trạm tiếp theo. Điều này không phải lúc nào dễ dàng bởi vì rất khó để phát hiện đáng tin cậy là trạm mạnh nhất.

Một tập RDS sẽ tìm kiếm nhận dạng chương trình hoặc mã PI. Một mạng lưới quốc gia sẽ được phát sóng từ một số lượng lớn các bộ truyền khác nhau trên khắp đất nước. Các trạm hoặc mạng ví dụ như đài phát thanh 4 sẽ có mã PI riêng của mình. Khi đài phát thanh di chuyển ra khỏi phạm vi của một phát radio sẽ tìm kiếm các tín hiệu mạnh trong đó có cùng một mã PI, cho phép các đài phát thanh để vẫn được điều chỉnh cho cùng một chương trình.

Khi radio được trang bị với RDS lưu trữ một tần số trạm, họ cũng lưu trữ mã PI cùng bên nó. Điều này có lợi thế là khi các đài phát thanh được bật ở một nơi bên ngoài vùng phủ sóng cho các tần số truyền được lưu trữ sau đó các đài phát thanh sẽ tìm kiếm các tín hiệu mạnh trong đó có mã PI đúng.

Đài phát thanh địa phương cũng có mã PI. Theo quan cảnh của bản chất địa phương của các trạm mã PI hoạt động hơi khác nhau.

Nếu trạm có hai hoặc nhiều truyền sau đó mã PI sẽ hoạt động theo cách bình thường khi nó là phạm vi của các bộ truyền này. Tuy nhiên khi các đài phát thanh di chuyển bên ngoài vùng phủ sóng này nó sẽ retune đến tín hiệu mạnh nhất của cùng một loại trạm.

Mã PI bao gồm bốn ký tự. Việc đầu tiên cho thấy nước xuất xứ và cho Vương Quốc Anh này là C. Một trong những kế tiếp cho biết loại bảo hiểm. Con số "2 " cho biết một trạm quốc gia, và hai nhân vật cuối cùng là tham khảo chương trình. Ví dụ Radio 3 có mã PI C203 và BBC GLR có C311.

Điều chỉnh nhanh RDS:

Phải mất một số giây cho các đài phát thanh để tìm kiếm các tín hiệu mạnh nhất với mã PI đúng. Trong thời gian này, các đài phát thanh tự câm và người nghe có một khoảng cách khó chịu lắng nghe. Để cho phép các thiết lập để điều chỉnh chính nó rất nhanh chóng từ một truyền vào mỗi máy phát sóng tiếp theo một danh sách ngắn các tần số của các bộ truyền liền kề. Điều này bao la làm giảm số lượng tìm kiếm mà các bộ phát thanh đã thực hiện. Thêm vào đó một kết thúc trước thứ hai thường được sử dụng để liên tục phát hiện sức mạnh của các truyền tần số thay thế. Điều này dẫn đến những thay đổi nhanh hơn nhiều trong cài đặt-đến mức người nghe không thể phát hiện khi Radio thay đổi từ một máy phát khác.

Một cơ sở khác liên quan đến điều chỉnh được gọi là tên dịch vụ chương trình (PS). Điều này cho phép thiết lập để hiển thị tên trạm. Điều này thường mất một hoặc hai thứ hai để đi lên trên màn hình sau khi trạm đã được điều chỉnh in Tuy nhiên nó là một cơ sở hữu ích nhất với số lượng ngày càng tăng của các trạm trên không khí.

Một tính năng mới đã được thêm vào RDS được gọi là nâng cao mạng khác (EON). Điều này cho phép thiết lập để nghe một trạm như một mạng lưới quốc gia, nhưng vẫn bị gián đoạn bởi tin tức du lịch từ một đài phát thanh địa phương. Tính năng này thậm chí cho phép thông báo được nghe trong khi đi du lịch trong im lặng hoặc nghe một băng.

EON đòi hỏi một số lượng lớn các phối hợp giữa các trạm khác nhau. Để đạt được điều này, BBC có một máy tính trung tâm đặc biệt cho mục đích này. Khi một đài phát thanh địa phương là về để truyền tải một thông điệp lưu lượng thực tế được gắn cờ vào máy tính. Lần lượt điều này chỉ đạo các phát sóng vô tuyến quốc gia có liên quan để cho biết điều này thực tế, qua đó cho phép các radio để thay đổi tần số cho đài phát thanh địa phương để nhận được tin nhắn. Sau khi tin nhắn hoàn tất, Đài phát thanh sẽ trở lại trạm ban đầu của nó.

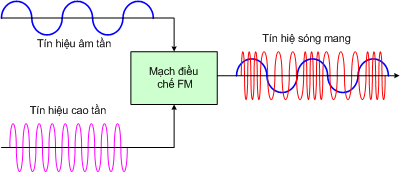
EON là tương đối mới và các bộ đầu tiên để có nó chỉ bao gồm xuất hiện trong 1991. Mặc dù nó đang được giới thiệu trên nhiều bộ, phần lớn vẫn không có nó. Tuy nhiên với các nhà sản xuất liên tục đưa bộ mới lên thị trường EON nên được bao gồm trên bộ nhiều hơn trong một hoặc hai năm.

### 3.4.6. Máy phát FM

FM là viết tắt của ( Fryquency Moducation : Điều chế tần số ) là điều chế theo phương thức làm thay đổi tần số của tín hiệu cao tần theo biên độ của tín hiệu âm tần, khoảng tần số biến đổi là 150KHz

Sóng FM là sóng cực ngắn đối với tín hiệu Radio, sóng FM thường phát ở dải tần từ 76MHz đến 108MHz

Mạch điều chế FM:



Hình 3. 27

Điều chế FM ( Fryquency Moducation : Điều chế tần số )

Với mạch điều chế tần số thì sóng mang có biên độ không đổi, nhưng tần số thay đổi theo biên độ của tín hiệu âm tần, khi biên độ tín hiệu âm tần tăng thì tần số cao tần tăng, khi biên độ âm tần giảm thì tần số cao tần giảm. Như vậy sóng mang FM có tần số tăng giảm theo tín hiệu âm tần và giới hạn tăng giảm này là +150KHz và -150KHz , như vậy tần số sóng mang điều tần có dải thông là 300KHZ.

Thí dụ nếu đài tiếng nói việt nam phát trên sóng FM 100MHz thì nó truyền đi một dải tần từ 99,85 MHz đến 100,15 MHz.

Quá trình phát sóng FM:

Điều chế FM là quá trình điều chế tín hiệu tần số thấp( như tín hiệu âm tần, tín hiệu video ) vào tần số cao tần theo phương thức => Biến đổi biên độ tín hiệu cao tần theo hình dạng của tín hiệu âm tần => Tín hiệu cao tần thu được gọi là sóng mang. Sóng mang sau khi điều chế cũng được khuếch đại rồi đưa ra An ten để phát xạ truyền đi xa.

Ưu và nhược điểm của sóng FM :

Sóng FM có nhiều ưu điểm về mặt tần số, dải tần âm thanh sau khi tách sóng điều tần có chất lượng rất tốt, cho âm thanh trung thực và có thể truyền âm thanh Stereo , sóng FM ít bị can nhiễu hơn só với sóng AM.

Nhược điểm của sóng FM là cự ly truyền sóng ngắn, chỉ truyền được cự ly từ vài chục đến vài trăm Km , do đó sóng FM thường được sử dụng làm sóng phát thanh trên các địa phương

Truyền FM cung cấp chất lượng hoàn hảo và khi một trong các máy phát được sử dụng trong một ngôi nhà và nhận được trên một đài phát thanh có chất lượng tốt, bạn không thể nói nếu người đang thực sự nói chuyện trong phòng kế tiếp hoặc thông qua một liên kết FM, nghe radio.

Hệ thống máy phát FM cấp huyện (88-108 MHz/500W) sử dụng công suất 500W phát công suất lớn bao trùm toàn huyện. Hệ thống máy phát FM cấp xã (54-68 MHz/50W) thì dùng công suất nhỏ hơn. Máy phát của huyện và xã không sử dụng chung một tuần số, chỗng bị nhiễu đường truyền. Máy phát đều thích hợp máy phát mã RDS-OTP để truyền dữ liệu liên kết giữa các xã và huyện.

### 3.4.7. Thiết bị đầu cuối là gì

Bất cứ thiết bị nào có thể kết nối với mạng trung tâm của doanh nghiệp đều được coi là một thiết bị đầu cuối. Thiết bị đầu cuối là các điểm xâm nhập tiềm ẩn cho các mối đe dọa an ninh mạng và cần được bảo vệ chặt chẽ vì chúng thường là mắt xích yếu nhất trong bảo mật mạng.

Quản lý bảo mật thiết bị đầu cuối là gì?

Đây là bộ quy tắc xác định mức độ bảo mật mà mỗi thiết bị kết nối với mạng doanh nghiệp phải tuân thủ. Những quy tắc này có thể bao gồm việc sử dụng hệ điều hành (HĐH) được phê duyệt, cài đặt mạng riêng ảo (VPN) hoặc chạy phần mềm chống virus mới nhất. Nếu thiết bị kết nối với mạng không đạt mức bảo mật bạn muốn, thiết bị có thể phải kết nối qua mạng khách và bị giới hạn quyền truy cập mạng.

Phần mềm bảo mật thiết bị đầu cuối là gì?

Các chương trình giúp bảo vệ thiết bị của bạn. Phần mềm Endpoint protection có thể được xây dựng trên nền điện toán đám mây và hoạt động như SaaS (Phần mềm dạng Dịch vụ). Ngoài ra, phần mềm bảo mật thiết bị đầu cuối có thể được cài đặt riêng trên từng thiết bị dưới dạng ứng dụng độc lập.

Bảo mật thiết bị đầu cuối là gì?

Bảo mật thiết bị đầu cuối là thuật ngữ được dùng rộng rãi, đề cập đến một số biện pháp bảo mật, nhưng vẫn nằm trong phạm trù bảo mật mạng nói chung. Các biện pháp bảo mật thiết bị đầu cuối sẽ giúp bảo vệ mạng doanh nghiệp trong khi các thiết bị di động hoặc từ xa, chẳng hạn như máy tính xách tay, máy tính bảng và điện thoại di động đang truy cập mạng. Chỉ tính riêng trong năm 2018, đã có tới gần 100 triệu cuộc tấn công mạng, vấn đề an ninh mạng thực sự quan trọng đến mức không thể bỏ qua.

Giải pháp phát hiện và ứng phó cho thiết bị đầu cuối (EDR) là gì?

Giải pháp phát hiện và ứng phó cho thiết bị đầu cuối (EDR) sẽ phân tích các tập tin và chương trình, cũng như báo cáo mọi mối đe dọa tìm được. Giải pháp EDR liên tục giám sát các mối đe dọa nguy hiểm, giúp xác định sớm các cuộc tấn công và ứng phó nhanh trước một loạt mối đe dọa.

# TÀI LIỆU THAM KHẢO