ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN
……..*……..

BÙI PHI LONG

NGHIÊN CỨU VẤN ĐỀ AN NINH MẠNG INTERNET KHÔNG DÂY VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2009

ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN

……..*……..

BÙI PHI LONG

NGHIÊN CỨU VẤN ĐỀ AN NINH MẠNG INTERNET KHÔNG DÂY VÀ ỨNG DỤNG

***Chuyên nghành*: KHOA HỌC MÁY TÍNH**
***Mã số* : 60.48.01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

***Người hướng dẫn khoa học*: PGS.TS NGUYỄN VĂN TAM**

THÁI NGUYÊN - 2009

MỤC LỤC

Trang

TRANG PHỤ BÌA…….

LỜI CÁM ƠN……...…….

LỜI CAM ĐOAN...……..

MỤC LỤC…….i

DANH MỤC CÁC KÝ HIỆU, CHỮ CÁI VIẾT TẮT…….……..…..v

DANH MỤC CÁC BẢNG…….……..…...…ix

DANH MỤC CÁC HÌNH…….……..……x

MỞ ĐẦU……...1

CHƯƠNG 1. TỔNG QUAN VỀ MẠNG INTERNET……....3

1.1. Giới thiệu công nghệ mạng Internet không dây và ứng dụng …….……..3

1.1.1. Công nghệ mạng Internet không dây……3

1.1.2. Ưu và nhược điểm của công nghệ mạng Internet không dây……....4

1.1.2.1. Ưu điểm.…….……..4

1.1.2.2. Nhược điểm…….5

1.2. Kiến trúc cơ bản của mạng LAN không dây…….5

1.2.1. Giới thiệu chung về mạng LAN không dây – WLAN……...5

1.2.2. Chuẩn 802.11 ……6

1.2.2.1. Nhóm lớp vật lý PHY bao gồm các chuẩn:…….……7

1.2.2.2. Nhóm lớp liên kết dữ liệu MAC bao gồm các chuẩn:…….8

1.2.3. Các mô hình WLAN (chuẩn 802.11)…….9

1.2.3.1. Trạm thu phát – STA…….. 9

1.2.3.2. Điểm truy cập – AP…… 9

1.2.3.3. Mạng 802.11 linh hoạt về thiết kế, gồm 3……..…… 10

1.2.3.4. WEP – Wired Equivalent Privacy ……... 14
1.2.3.5. WEP key lengths ……..14
1.2.3.6. WPA – Wi- fi Protected Access ……...15
1.2.3.7. WPA2 – Wi- fi Protected Access 2 ……..…. 15
1.3. Kiến trúc cơ bản của mạng WAN không dây……..16
1.3.1. Thế hệ thứ 1 (1G) …….…….. 17
1.3.2. Thế hệ thứ 2 (2G) ……17
1.3.3. Thế hệ di động thứ 3 (3G)……... 18
1.4. Kiến trúc cơ bản của Internet không dây…….22
1.4.1. Kiến trúc cơ bản của Internet không dây – chuẩn WAP…….22
1.4.1.1. Sơ bộ về WAP……..……..22
1.4.1.2. Các mô hình giao tiếp trên WAP ……..24
1.4.1.3. Ưu và nhược điểm của WAP ……28
1.4.1.4. Các thành phần của WAP…… 30
1.4.2. Kiến trúc cơ bản của mạng WPAN không dây……..…… 37
1.4.3. Kiến trúc cơ bản của mạng WMAN không dây ……..49
1.4.3.1. Đặc điểm nổi bật của WiMAX di động ……40
1.4.3.2. Mô hình ứng dụng WiMAX……..40
1.4.4. Mạng không dây WRAN……42
1.5. Tổng kết……...42
CHƯƠNG 2. TỔNG QUAN VỀ AN NINH MẠNG INTERNET KHÔNG DÂY …..44

2.1. Một số kỹ thuật tấn công Internet không dây.....44
2.1.1. Tấn công bị động – Passive attacks……44
2.1.1.1. Định nghĩa……44
2.1.1.2. Kiểu tấn công bị động cụ thể - Phương thức bắt gói tin (Sniffing)…...45
2.1.2. Tấn công chủ động – Active attacks……47
2.1.2.1. Định nghĩa……47
2.1.2.2. Các kiểu tấn công chủ động cụ thể……..48
2.1.3. Tấn công kiểu chèn ép - Jamming attacks ……54
2.1.4. Tấn công theo kiểu thu hút - Man in the middle attacks……. 55
2.1.5. Tấn công vào các yếu tố con người …….……55
2.1.6. Một số kiểu tấn công khác ……...…56
2.2. Giải pháp an ninh cho mạng Internet không dây (WAP)…….…57
2.2.1. Vấn đề bảo mật trên WAP……..57
2.2.1.1. So sánh các mô hình bảo mật……57
2.2.1.2. WAP Gateway……..63
2.2.1.3. TLS và WTLS……...66
2.3. Tổng kết ……..…….……68
CHƯƠNG 3: MẠNG INTERNET KHÔNG DÂY VÀ THỬ NGHIỆM ……70
3.1. Thiết kế mô hình mạng Internet không dây trong trường Việt Đức TN…….70
3.1.1. Nguyên tắc thiết kế……70
3.1.2. Mô hình logic và sơ đồ phủ sóng vật lý tổng thể tại trường……...71
3.1.2.1. Mô hình thiết kế logic……...71
3.1.1.2. Sơ đồ phủ sóng vật lý tổng thể tại trường……...71
3.1.3. Thiết kế chi tiết của hệ thống……..73
3.1.3.1. Mô hình thiết kế chi tiết hệ thống mạng không dây……...…73
3.1.3.2. Thiết bị sử dụng trong hệ thống mạng không dây…….……73
3.1.3.3. Phân bổ thiết bị sử dụng trong hệ thống……75

3.2. Giải pháp bảo mật trong mạng không dây tại CĐCN Việt Đức Thái Nguyên …..75
3.2.1. Yêu cầu bảo vệ thông tin……...76
3.2.1.1. Bảo vệ dữ liệu:……77
3.2.1.2. Bảo vệ các tài nguyên sử dụng trên mạng:……77
3.2.1.3. Bảo vệ danh tiếng cơ quan:……78
3.2.2. Các bước thực thi an toàn bảo mật cho hệ thống……..78
3.2.2.1. Các hoạt động bảo mật ở mức một……78
3.2.2.2. Các hoạt động bảo mật ở mức hai……..79
3.3. Chương trình thực tế đã xây dựng……...79
3.4. Đánh giá kết quả……..80
3.5. Một số hướng dẫn để bảo vệ máy tính an toàn khi dùng Internet không dây…….80
3.5.1. Tối ưu hóa Wi-Fi cho các VoIP, Video Game……80
3.5.2. Ưu tiên hóa tải gói dữ liệu…….….. 81
3.5.3. Tắt Wi-Fi khi không dùng đến ……83
3.5.4. Theo dõi những người không mời mà đến trên mạng Wi-Fi của bạn……..83
3.5.5. Loại bỏ điểm kết nối không dây an toàn…… 84
3.5.6. Vô hiệu hóa Peer-to-Peer Wi-Fi ……85
3.6. Tấn công Website – Cách xử lý……..…….…….87
3.7. Tổng kết……...……..88
KẾT LUẬN ……...90
TÀI LIỆU THAM KHẢO……..92
PHỤ LỤC……...94

DANH MỤC CÁC KÝ HIỆU, CHỮ CÁI VIẾT TẮT

AAA - Authentication Authorization Audit

ACL - Access control lists

ACS - Access Control Server

ACU - Aironet Client Utility

AES – Advanced Encryption Standard

AP - Access point

APOP - Authentication POP

BSS - Basic Service Set

BSSID - Basic Service Set Identifier

CA - Certificate Authority

CCK - Complimentary Code Keying

CDMA - Code Division Multiple Access

CHAP - Challenge Handshake Authentication Protocol

CMSA/CD - Carrier Sense Multiple Access with Collision Detection

CRC - Cyclic redundancy check

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CTS - Clear To Send

DES - Data Encryption Standard

DFS - Dynamic Frequency Selection

DHCP - Dynamic Host Configuration Protocol

DMZ - Demilitarized Zone

DOS - Denial of service

DRDOS - Distributed Reflection DOS

DS - Distribution System

DSSS - Direct Sequence Spread Spectrum

EAP - Extensible Authentication Protocol

EAPOL - EAP Over LAN

EAPOW - EAP Over Wireless

ESS - Extended Service Set

ETSI - European Telecommunications Standards Institute

FCC - Federal Communications Commissio

FHSS – Frequency Hopping Spread Spectrum

GPS - Global Positioning System

HiperLAN - High Performance Radio LAN

HTML -HyperText Markup Language

HTTP - HyperText Transfer Protocol

IBSS - Independent Basic Service Set

ICMP -Internet Control Message Protocol

ICV – Intergrity Check Value

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IR - Infrared Light

IKE - Internet Key Exchange

IP - Internet Protocol

IPSec - Internet Protocol Security

IrDA - Infrared Data Association

ISDN -Integrated Services Digital Network

ISM - Industrial Scientific and Medical

ISP - Internet Service Provider

ITU - International Telecommunication Union

IV - Initialization Vector

LAN - Local Area Network

LCP – Link Control Protocol

LEAP - Light Extensible Authentication Protocol

LLC - Logical Link Control

LOS - Light of Sight

MAC - Media Access Control

MAN - Metropolitan Area Network

MIC - Message Integrity Check

MSDU - Media Access Control Service Data Unit

OCB - Offset Code Book

OFDM - Orthogonal Frequency Division

OSI - Open Systems Interconnection

OTP - One-time password

PAN - Person Area Network

PBCC - Packet Binary Convolutional Coding

PCMCIA - Personal Computer Memory Card International Association

PDA - Personal Digital Assistant

PEAP - Protected EAP Protocol

PKI-Public Key Infrastructure

PRNG - Pseudo Random Number Generator

QoS - Quality of Service

RADIUS - Remote Access Dial-In User Service

RF - Radio frequency

RFC - Request For Comment

RTS - Request To Send

SIG - Special Interest Group

SSH - Secure Shell

SSID - Service Set ID

SSL - Secure Sockets Layer

STA - Station

SWAP - Standard Wireless Access Protocol

TACACS - Terminal Access Controller Access Control System

TCP - Transmission Control Protocol

TFTP - Trivial File Transfer Protocol

TKPI - Temporal Key Integrity Protocol

TLS - Transport Layer Security

TPC - Transmission Power Control

UDP - User Datagram Protocol

UWB – Ultra Wide Band

UNII - Unlicensed National Information Infrastructure

VLAN - Virtual LAN

WAN - Wide Area Network

WECA - Wireless Ethernet Compatibility

WEP - Wired Equivalent Protocol

Wi-Fi - Wireless fidelity

WLAN - Wireless LAN

WPAN - Wireless Personal Area Network

DANH MỤC CÁC BẢNG

Bảng 1.1. Technology Features Comparison ……22

Bảng 1.2. Pre-4G Technology Requirement Comparison ……..22

Bảng 2.1. So sánh sự khác nhau giữa WTLS và TLS ……..…..67

Bảng 3.1. Các đặc tính kỹ thuật của AP TP-Link 108Mbits 1 Port (TL-WA601G)…. 74

DANH MỤC CÁC HÌNH VẼ

Hình 1.1. Mô hình mạng AD HOC ……..…...10
Hình 1.2. Mô hình mạng cơ sở …….……..11
Hình 1.3. Mô hình mạng mở rộng…….…… 12
Hình 1.4. Mô hình mạng không dây kết nối với mạng có dây …….……..13
Hình 1.5. Mô hình 2 mạng có dây kết nối với nhau bằng kết nối không dây……..……14
Hình 1.6. Con đường phát triển của các công nghệ mạng……..……16
Hình 1.7. WAP dùng truy cập Internet…….……...24
Hình 1.8. WAP được dùng truy cập trong Intranet ……..……...25
Hình 1.9. Wap Client……..…….30
Hình 1.10. Wap Stack……..……31
Hình 1.11. Wap Stack……..……31
Hình 1.12. Yêu cầu không tin cậy……..…….34
Hình 1.13. Yêu cầu tin cậy…….…… 34
Hình 1.14. Yêu cầu tin cậy với thông điệp kết quả…….……35
Hình 1.15. Mô hình làm việc của Wap gateway…….……36
Hình 1.16. Mô hình ứng dụng Wimax…….……...41
Hình 2.1. Các phương thức dùng trong tấn công bị động …….…….45
Hình 2.2. Phần mềm bắt gói tin Ethereal …….……..46
Hình 2.3. Phần mềm thu thập thông tin hệ thống mạng không dây NetStumbler …….….47
Hình 2.4. Tấn công chủ động …….……48
Hình 2.5. Mô tả quá trình tấn công DOS tầng liên kết dữ liệu …….…….50
Hình 2.6. Mô tả quá trình tấn công mạng bằng AP giả mạo …….……52
Hình 2.7. Mô tả quá trình tấn công theo kiểu chèn ép……..…….. 54
Hình 2.8. Mô tả quá trình tấn công theo kiểu thu hút……..……55
Hình 2.9. Mô hình bảo mật trên Internet ……..……..57
Hình 2.10. Mô hình bảo mật trên WAP……..…… 59

Hình 2.11. WAP 1.0…….. 60
Hình 2.12. WAP 2.0 ……..61
Hình 2.13. WAP…… 61
Hình 2.14. Sử dụng WAP proxy/gateway…… 63
Hình 2.15. Các bước thực hiện khi tiến hành một phiên giao dịch WAP ……64
Hình 2.16. Quá trình biên dịch các yêu cầu tại gateway chuyển đổi giao thức…… 65
Hình 2.17. Mô tả chức năng mã hóa/ giải mã của WAP gateway…… 65
Hình 3.1. Mô hình logic mạng không dây tại trường ……...71
Hình 3.2. Mô hình phủ sóng tại trường CĐCN Việt Đức Thái Nguyên ……..……..72
Hình 3.3. Access Point (AP) TP-Link 108Mbits 1 Port (TL-WA601G)…….…… 73
Hình: 3.4. Mô phỏng kiến trúc hiện tại hệ thống mạng Internet không dây……..… 80
Hình 3.5. Cấu hình của Router Linksys…… 81
Hình 3.6. Tối ưu cho gói dữ liệu gửi nhận thông qua thiết lập tren Rounter…… 82
Hình 3.7. Cấp quyền ưu tiên ……..…82
Hình 3.8. Tắt Wi-Fi khi không dùng đến ……..…83
Hình 3.9. Thiết lập theo dõi khách không mời mà đến…….…… 84
Hình 3.10. Loại bỏ điểm kết nối không dây an toàn ……..…...…….84
Hình 3.11. Vô hiệu hóa Peer-to-Peer Wi-Fi …….……..85
Hình 3.12. Vô hiệu hóa Peer-to-Peer Wi-Fi …….……..86
Hình 3.13. Vô hiệu hóa Peer-to-Peer Wi-Fi …….……..86
Hình PL1. Nokia Mobile Internet Toolkit…….…… 97
Hình PL2. Nokia WAP Gateway Simulator……..……..98
Hình PL3. Nokia WAP Gateway……...…… 99
Hình PL4. Nokia Browser Simulator…….. 99
Hình PL5. Hệ thống Menu Nokia……..…… 100

MỞ ĐẦU

1. Nền tảng và mục đích.

Mạng Internet không dây hiện nay được áp dụng trong rất nhiều lĩnh vực bởi những ưu thế nổi trội của nó so với mạng Internet hữu tuyến truyền thống: người dùng có thể di chuyển trong phạm vi cho phép, có thể triển khai mạng Internet không dây ở những nơi mà mạng Internet hữu tuyến không thể triển khai được. Tuy nhiên, khác với mạng Internet hữu tuyến truyền thống, mạng Internet không dây sử dụng kênh truyền sóng điện từ, và do đó nó đặt ra nhiều thách thức trong việc xây dựng đặc tả và triển khai thực tế mạng này. Một trong những thách thức đó và cũng là vấn đề nóng hổi hiện nay là vấn đề an ninh cho mạng Internet không dây.

Đã có nhiều giải pháp an ninh ra đời nhằm áp dụng cho mạng Internet không dây, trong đó chuẩn WAP được đặc tả với tham vọng mang lại khả năng an toàn cao cho mạng Internet không dây. Tuy vậy, việc hỗ trợ các phần cứng cũ cộng với việc đặc tả cho phép các nhà sản xuất phần cứng được quyết định một số thành phần khi sản xuất khiến cho các mạng Internet không dây khi triển khai không những không đồng nhất mà còn có những rủi ro an ninh riêng.

Do đó, mục đích của luận văn này là nghiên cứu, phân tích những đặc điểm của mạng Internet không dây, những kỹ thuật tấn công mạng Internet không dây để từ đó đưa ra những giải pháp an ninh, bảo mật cho mạng Internet không dây dựa trên các tiêu chí: tính bảo mật, tính toàn vẹn, xác thực hai chiều và tính sẵn sàng. Trên cơ sở đó, đề xuất xây dựng một mô hình an ninh, bảo mật cho mạng Internet không dây tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên.

2. Cấu trúc của luận văn.

Ngoài phần mở đầu và kết luận, nội dung của luận văn được bố cục như sau:

Chương 1: Trình bày các kiến thức tổng quan về mạng Internet và đặc biệt là mạng Internet không dây. Kiến trúc cơ bản của: mạng LAN không dây, mạng WAN không dây, mạng Internet không dây (chuẩn WAP và các chuẩn mới) để từ đó có được cái nhìn bao quát về cách thức hoạt động của mạng Internet không dây.

Chương 2: Đi sâu vào nghiên cứu các kỹ thuật tấn công mạng Internet không dây (các tầng trên – WAP) để từ đó đưa ra các giải pháp an ninh, bảo mật cho mạng Internet không dây dựa trên hai khía cạnh: đảm bảo an toàn dữ liệu và toàn vẹn dữ liệu. Bên cạnh việc cung cấp tổng quát về quá trình phát triển cũng như cải tiến các phương pháp, chương nay cũng sẽ chỉ ra những rủi ro an ninh phổ biến trong mạng Internet không dây.

Chương 3: Từ những kiến thức đã nghiên cứu ở hai chương trước, chương 3 giới thiệu ứng dụng mạng Internet không dây vào xây dựng mô hình an ninh, bảo mật cho mạng Internet không dây tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên. Ngoài ra, còn giới thiệu một số kỹ thuật bảo vệ an toàn máy tính khi sử dụng Internet không dây, cách xử lý khi website bị tấn công.

Cuối cùng là phần phụ lục và tài liệu tham khảo.

CHƯƠNG 1. TỔNG QUAN VỀ MẠNG INTERNET

1.1. Giới thiệu công nghệ mạng Internet không dây và ứng dụng

1.1.1. Công nghệ mạng Internet không dây.

Mạng Internet từ lâu đã trở thành một thành phần không thể thiếu đối với nhiều lĩnh vực trong đời sống xã hội, từ các cá nhân hộ gia đình, đơn vị, doanh nghiệp dùng mạng Internet phục vụ cho công việc, học tập, hoạt động tổ chức kinh doanh, quảng bá..v.v…cho đến hệ thống mạng Internet toàn cầu mà cả xã hội, cả thế giới đang hàng ngày hàng giờ sử dụng. Các hệ thống mạng hữu tuyến và vô tuyến đang ngày càng phát triển, phát huy vai trò của mình trong đó mạng Internet không dây nổi lên như một phương thức truy nhập Inetrnet phổ biến dần thay thế cho mạng Internet có dây khó triển khai, lắp đặt.

Mặc dù mạng Internet không dây đã xuất hiện từ nhiều thập niên nhưng cho đến những năm gần đây, với sự bùng nổ các thiết bị di động thì nhu cầu nghiên cứu và phát triển các hệ thống mạng Internet không dây ngày càng trở nên cấp thiết. Nhiều công nghệ, phần cứng, các giao thức, chuẩn lần lượt ra đời và đang được tiếp tục nghiên cứu và phát triển.

Mạng Internet không dây có tính linh hoạt, hỗ trợ các thiết bị di động nên không bị ràng buộc cố định và phân bố địa lý như trong mạng Internet hữu tuyến. Ngoài ra, ta còn có thể dễ dàng bổ sung hay thay thế các thiết bị tham gia mạng Internet mà không cần phải cấu hình lại toàn bộ toplogy của mạng. Tuy nhiên, hạn chế lớn nhất của mạng Internet không dây là khả năng bị nhiễu và mất gói tin so với mạng Internet hữu tuyến. Bên cạnh đó, tốc độ truyền cũng là vấn đề rất đáng để chúng ta quan tâm.

Hiện nay, những hạn chế trên đang dần được khắc phục. Những nghiên cứu về mạng Internet không dây hiện đang thu hút các Viện nghiên cứu cũng như các Doanh nghiệp trên thế giới. Với sự đầu tư đó, hiệu quả và chất lượng của hệ thống mạng Internet không dây sẽ ngày càng được nâng cao, hứa hẹn những bước phát triển trong tương lai.

Trong các hệ thống mạng Internet hữu tuyến, dữ liệu nhận và truyền từ các máy chủ tới hệ thống các Website thông qua các dây cáp hoặc thiết bị trung gian. Còn đối với mạng Internet không dây, các máy chủ truyền và nhận thông tin từ Internet thông qua sóng điện từ, sóng radio.

Tín hiệu Internet được truyền trong không khí trong một khu vực gọi là vùng phủ sóng Internet. Thiết bị nhận Internet chỉ cần nằm trong vùng phủ sóng Internet của thiết bị phát Internet thì sẽ nhận được tín hiệu.

1.1.2. Ưu và nhược điểm của công nghệ mạng Internet không dây.

1.1.2.1. Ưu Điểm

- Tính tiện lợi, di động: Cho phép người dùng truy xuất tài nguyên trên mạng Internet ở bất kỳ nơi đâu trong khu vực được triển khai (công viên, nhà hay văn phòng), điều này rất khó đối với mạng Internet có dây vì khó triển khai ngay lập tức, không cơ động, khó đối với nhiều khu vực không kéo dây được, mất nhiều thời gian, tiền của..v.v...Tính di động này sẽ tăng năng xuất và tính kịp thời thỏa mãn những nhu cầu thông tin mà mạng Internet hữu tuyến không thể có được.

- Tính hiệu quả: Người dùng có thể duy trì kết nối mạng Internet khi họ đi từ nơi này đến nơi khác trong phạm vi vùng phủ sóng của mạng Internet không dây (trong một tòa nhà, một khu vực nhất định).

- Tiết kiệm chi phí lâu dài: Việc thiết lập hệ thống mạng Internet không dây ban đầu chỉ cần 1 Accesspoint và Accesspoint này có kết nối với Internet thông qua Switch hoặc Modem. Nhưng từ 1 Accesspoint này rất nhiều máy tính có thể truy cập Internet, tiết kiệm chi phí rất nhiều so với phải kéo dây trong mạng Internet hữu tuyến, chi phí dài hạn có lợi nhất trong môi trường động cần phải di chuyển và thay đổi thường xuyên, các chi phí về thời gian tồn tại của mạng Internet hữu tuyến có thể thấp hơn đáng kể so với mạng Internet không dây.

- Khả năng mở rộng: Mạng Internet không dây có thể đáp ứng tức thì khi gia tăng số lượng người dùng (điều không thể đối với mạng Internet có dây vì phải lắp đặt thêm thiết bị,…).

- ***Tính linh hoạt:*** Dễ dàng bổ xung hay thay thế các thiết bị tham gia mạng mà không cần phải cấu hình lại toàn bộ topology mạng.

1.1.2.2. Nhược điểm.

- ***Bảo mật:*** Môi trường kết nối Internet không dây là không khí -> khả năng bị tấn công của người dùng là rất cao.

- ***Phạm vi:*** Một mạng chuẩn 802.11g với các thiết bị chuẩn chỉ có thể hoạt động tốt trong phạm vi vài chục mét, ngoài phạm vi đó các thiết bị truy cập Internet không thể nhận được tín hiệu hoặc nhận được tín hiệu thì rất yếu, ngắt quãng không đảm bảo .

- ***Chất lượng:*** Vì mạng Internet không dây sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác (lò vi sóng....) là không tránh khỏi.

- ***Tốc độ:*** Tốc độ của mạng Internet không dây (1 – 125 Mbps) rất chậm so với mạng sử dụng cáp (100 Mbps đến hàng Gbps).

1.2. Kiến trúc cơ bản của mạng LAN không dây.

1.2.1. Giới thiệu chung về mạng LAN không dây – WLAN.

Wireless LAN (Wireless Local Area Network) sử dụng sóng điện từ (thường là sóng radio hay tia hồng ngoại) để liên lạc giữa các thiết bị trong phạm vi trung bình. So với Bluetooth, Wireless LAN có khả năng kết nối phạm vi rộng hơn với nhiều vùng phủ sóng khác nhau, do đó các thiết bị di động có thể tự do di chuyển gữa các vùng với nhau. Phạm vi hoạt động từ 100m đến 500m với tốc độ truyền dữ liệu trong khoảng 1Mbps – 54 Mbps (100Mbps)

IEEE (Institute of Electrical and Electronic Engineers) là tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng LAN với đề án IEEE 802 nổi tiếng bắt đầu triển khai từ năm 1980 và kết quả là hàng loạt chuẩn thuộc họ IEEE 802.x ra đời, tạo nên một sự hội tụ quan trọng cho việc thiết kế và cài đặt các mạng LAN trong thời gian qua.

802.11 là một trong các chuẩn của họ IEEE 802.x bao gồm họ các giao thức truyền tin qua mạng không dây. Trước khi giới thiệu 802.11 chúng ta sẽ cùng điểm qua một số chuẩn 802 khác:

- 802.1: các Cầu nối (Bridging), Quản lý (Management) mạng LAN, WAN
- 802.2: điều khiển kết nối logic
- 802.3: các phương thức hoạt động của mạng Ethernet
- 802.4: mạng Token Bus
- 802.5: mạng Token Ring
- 802.6: mạng MAN
- 802.7: mạng LAN băng rộng
- 802.8: mạng quang
- 802.9: dịch vụ luồng dữ liệu
- 802.10: an ninh giữa các mạng LAN
- 802.11: mạng LAN không dây – Wireless LAN
- 802.12: phương phức ưu tiên truy cập theo yêu cầu
- 802.13: chưa có
- 802.14: truyền hình cáp
- 802.15: mạng PAN không dây
- 802.16: mạng không dây băng rộng

Chuẩn 802.11 chủ yếu cho việc phân phát các MSDU (đơn vị dữ liệu dịch vụ của MAC) giữa các kết nối LLC (điều khiển liên kết logic).

1.2.2. Chuẩn 802.11

Chuẩn 802.11 được chia làm hai nhóm: nhóm lớp vật lý PHY và nhóm lớp liên kết dữ liệu MAC.

1.2.2.1. Nhóm lớp vật lý PHY bao gồm các chuẩn:

a. Chuẩn 802.11b

802.11b là chuẩn đáp ứng đủ cho phần lớn các ứng dụng của mạng. Với một giải pháp rất hoàn thiện, 802.11b có nhiều đặc điểm thuận lợi so với các chuẩn không dây khác. Chuẩn 802.11b sử dụng kiểu trải phổ trực tiếp DSSS, hoạt động ở dải tần 2,4 GHz, tốc độ truyền dữ liệu tối đa là 11 Mbps trên một kênh, tốc độ thực tế là khoảng từ 4-5 Mbps. Khoảng cách có thể lên đến 500 mét trong môi trường mở rộng. Khi dùng chuẩn này tối đa có 32 người dùng / điểm truy cập.

Đây là chuẩn đã được chấp nhận rộng rãi trên thế giới và được triển khai rất mạnh hiện nay do công nghệ này sử dụng dải tần không phải đăng ký cấp phép phục vụ cho công nghiệp, dịch vụ, y tế.

Nhược điểm của 802.11b là hoạt động ở dải tần 2,4 GHz trùng với dải tần của nhiều thiết bị trong gia đình như lò vi sóng , điện thoại mẹ con ... nên có thể bị nhiễu.

b. Chuẩn 802.11a

Chuẩn 802.11a là phiên bản nâng cấp của 802.11b, hoạt động ở dải tần 5 GHz , dùng công nghệ trải phổ OFDM. Tốc độ tối đa từ 25 Mbps đến 54 Mbps trên một kênh, tốc độ thực tế xấp xỉ 27 Mbps, dùng chuẩn này tối đa có 64 người dùng / điểm truy cập. Đây cũng là chuẩn đã được chấp nhận rộng rãi trên thế giới.

c. Chuẩn 802.11g

Các thiết bị thuộc chuẩn này hoạt động ở cùng tần số với chuẩn 802.11b là 2,4 Ghz. Tuy nhiên chúng hỗ trợ tốc độ truyền dữ liệu nhanh gấp 5 lần so với chuẩn 802.11b với cùng một phạm vi phủ sóng, tức là tốc độ truyền dữ liệu tối đa lên đến 54 Mbps, còn tốc độ thực tế là khoảng 7-16 Mbps. Chuẩn 802.11g sử dụng phương pháp điều chế OFDM, CCK – Complementary Code Keying và PBCC – Packet Binary Convolutional Coding. Các thiết bị thuộc chuẩn 802.11b và 802.11g hoàn toàn tương thích với nhau. Tuy nhiên cần lưu ý rằng khi bạn trộn lẫn các thiết bị của

hai chuẩn đó với nhau thì các thiết bị sẽ hoạt động theo chuẩn nào có tốc độ thấp hơn. Đây là một chuẩn hứa hẹn trong tương lai nhưng hiện nay vẫn chưa được chấp thuận rộng rãi trên thế giới.

1.2.2.2. Nhóm lớp liên kết dữ liệu MAC bao gồm các chuẩn:

a. Chuẩn 802.11d

Chuẩn 802.11d bổ xung một số tính năng đối với lớp MAC nhằm phổ biến WLAN trên toàn thế giới. Một số nước trên thế giới có quy định rất chặt chẽ về tần số và mức năng lượng phát sóng vì vậy 802.11d ra đời nhằm đáp ứng nhu cầu đó. Tuy nhiên, chuẩn 802.11d vẫn đang trong quá trình phát triển và chưa được chấp nhận rộng rãi như là chuẩn của thế giới.

b. Chuẩn 802.11e

Đây là chuẩn được áp dụng cho cả 802.11 a, b, g. Mục tiêu của chuẩn này nhằm cung cấp các chức năng về chất lượng dịch vụ - QoS cho WLAN. Về mặt kỹ thuật, 802.11e cũng bổ xung một số tính năng cho lớp con MAC. Nhờ tính năng này, WLAN 802.11 trong một tương lai không xa có thể cung cấp đầy đủ các dịch vụ như voice, video, các dịch vụ đòi hỏi QoS rất cao. Chuẩn 802.11e hiện nay vẫn đang trong qua trình phát triển và chưa chính thức áp dụng trên toàn thế giới.

c. Chuẩn 802.11f

Đây là một bộ tài liệu khuyến nghị của các nhà sản xuất để các Access Point của các nhà sản xuất khác nhau có thể làm việc với nhau. Điều này là rất quan trọng khi quy mô mạng lưới đạt đến mức đáng kể. Khi đó mới đáp ứng được việc kết nối mạng không dây liên cơ quan, liên xí nghiệp có nhiều khả năng không dùng cùng một chủng loại thiết bị.

d. Chuẩn 802.11h

Tiêu chuẩn này bổ xung một số tính năng cho lớp con MAC nhằm đáp ứng các quy định châu Âu ở dải tần 5GHz. Châu Âu quy định rằng các sản phẩm dùng

dải tần 5 GHz phải có tính năng kiểm soát mức năng lượng truyền dẫn TPC - Transmission Power Control và khả năng tự động lựa chọn tần số DFS - Dynamic Frequency Selection. Lựa chọn tần số ở Access Point giúp làm giảm đến mức tối thiểu can nhiễu đến các hệ thống radar đặc biệt khác.

e. Chuẩn 802.11i

Đây là chuẩn bổ xung cho 802.11 a, b, g nhằm cải thiện về mặt an ninh cho mạng không dây. An ninh cho mạng không dây là một giao thức có tên là WEP, 802.11i cung cấp những phương thức mã hóa và những thủ tục xác nhận, chứng thực mới có tên là 802.1x. Chuẩn này vẫn đang trong giai đoạn phát triển.

1.2.3. Các mô hình WLAN (chuẩn 802.11).

1.2.3.1. Trạm thu phát - STA

STA – Station, các trạm thu/phát sóng. Thực chất ra là các thiết bị không dây kết nối vào mạng như máy vi tính, máy Palm, máy PDA, điện thoại di động, vv... với vai trò như phần tử trong mô hình mạng ngang hàng Pear to Pear hoặc Client trong mô hình Client/Server. Trong phạm vi luận văn này chỉ đề cập đến thiết bị không dây là máy vi tính (thường là máy xách tay cũng có thể là máy để bàn có card mạng kết nối không dây). Có trường hợp trong luận văn này gọi thiết bị không dây là STA, có lúc là Client, cũng có lúc gọi trực tiếp là máy tính xách tay. Thực ra là như nhau nhưng cách gọi tên khác nhau cho phù hợp với tình huống đề cập.

1.2.3.2. Điểm truy cập – AP

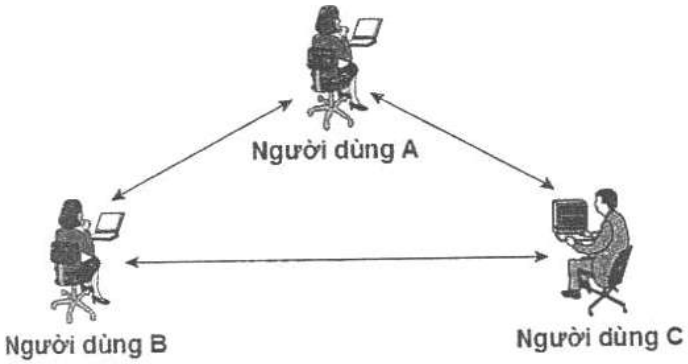
Điểm truy cập – Acces Point là thiết bị không dây, là điểm tập trung giao tiếp với các STA, đóng vai trò cả trong việc truyền và nhận dữ liệu mạng. AP còn có chức năng kết nối mạng không dây thông qua chuẩn cáp Ethernet, là cầu nối giữa mạng không dây với mạng có dây. AP có phạm vi từ 30m đến 300m phụ thuộc vào công nghệ và cấu hình.

1.2.3.3. Mạng 802.11 linh hoạt về thiết kế, gồm 3 mô hình mạng sau:

- Mô hình mạng độc lập – mạng Adhoc
- Mô hình mạng cơ sở (BSSs).
- Mô hình mạng mở rộng (ESSs).

a. Mô hình mạng độc lập Adhoc

Mỗi máy tính trong mạng giao tiếp trực tiếp với nhau thông qua các thiết bị card mạng không dây mà không dùng đến các thiết bị định tuyến hay thu phát không dây.



Hình 1.1. Mô hình mạng AD HOC

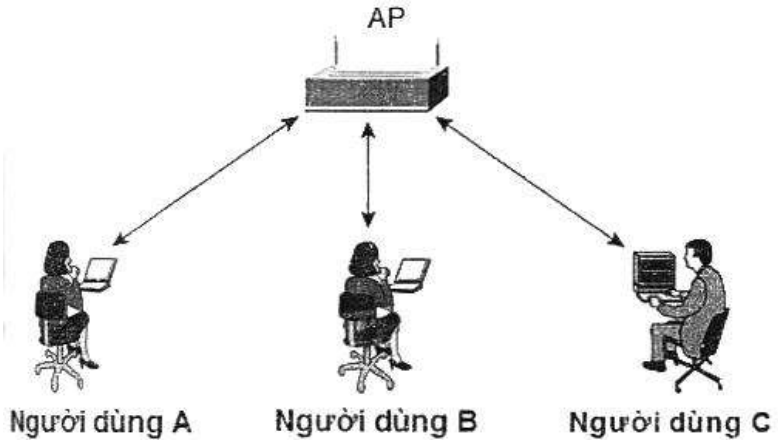
b. Mô hình mạng cơ sở (Basic Service (BSSs)).

Bao gồm các điểm truy nhập AP (Access Point) gắn với mạng đường trục hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell. AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP. Các cell có thể chống lấn lên nhau khoảng 10 – 15% cho phép các trạm di động có thể di chuyển mà không bị mất kết nối vô tuyến và cung cấp vùng phủ sóng với chi phí thấp nhất. Các trạm di động sẽ chọn AP tốt nhất để kết nối. Một điểm truy nhập nằm ở trung tâm có thể điều khiển và phân phối truy nhập cho các nút tranh chấp, cung cấp truy

nhập phù hợp với mạng đường trục, ấn định các địa chỉ và các mức ưu tiên, giám sát lưu lượng mạng, quản lý chuyển đi các gói và duy trì theo dõi cấu hình mạng. Tuy nhiên giao thức đa truy nhập tập trung không cho phép các nút di động truyền trực tiếp tới nút khác nằm trong vùng với điểm truy nhập như trong cấu hình mạng WLAN độc lập. Trong trường hợp này, mỗi gói sẽ phải được phát đi 2 lần (từ nút phát gốc và sau đó là điểm truy nhập) trước khi nó tới nút đích, quá trình này sẽ làm giảm hiệu quả truyền dẫn và tăng trễ truyền dẫn.

BSS độc lập – IBSS: Trong mô hình IBSS – Independent BSS, là các BSS độc lập, tức là không có kết nối với mạng có dây bên ngoài. Trong IBSS, các STA có vai trò ngang nhau. IBSS thường được áp dụng cho mô hình Adhoc bởi vì nó có thể được xây dựng nhanh chóng mà không phải cần nhiều kế hoạch.

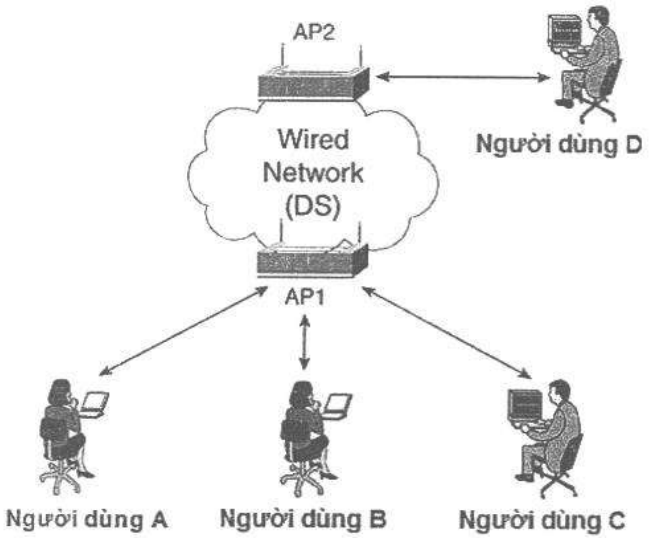
Hệ thống phân tán – DS: Người ta gọi DS – Distribution System là một tập hợp của các BSS. Mà các BSS này có thể trao đổi thông tin với nhau. Một DS có nhiệm vụ kết hợp với các BSS một cách thông suốt và đảm bảo giải quyết vấn đề địa chỉ cho toàn mạng



Hình 1.2. Mô hình mạng cơ sở

c. Mô hình mạng mở rộng (Extended Service Set(ESSs))

Mạng 802.00 mở rộng phạm vi di động tới một phạm vi bất kỳ thông qua ESS. Một ESS là một tập hợp các BSSs nơi mà các Access Point giao tiếp với nhau để chuyển lưu lượng từ một BSS này đến một BSS khác để làm cho việc giao tiếp thông qua hệ thống phân phối. Hệ thống phân phối làm một lớp mỏng trong mỗi Access Point mà nó xác định đích đến cho một lưu lượng được nhận từ một BSS. Hệ thống phân phối được tiếp sóng trở lại một đích trong cùng một BSS, chuyển tiếp trên hệ thống phân phối tới một Access Point khác, hoặc gửi tới một mạng có dây tới đích không nằm trong ESS. Các thông tin nhận bởi Access Point từ hệ thống phân phối được truyền tới BSS sẽ được nhận bởi trạm đích.



Hình 1.3. Mô hình mạng mở rộng

Như rất nhiều tài liệu nghiên cứu về bảo mật trong mạng Wireless thì để có thể bảo mật tối thiểu cần một hệ thống có 2 thành phần sau:

- Authentication - chứng thực cho người dùng, quyết định cho ai có thể sử dụng mạng WLAN.

- Encryption - mã hoá dữ liệu: cung cấp tính bảo mật dữ liệu.

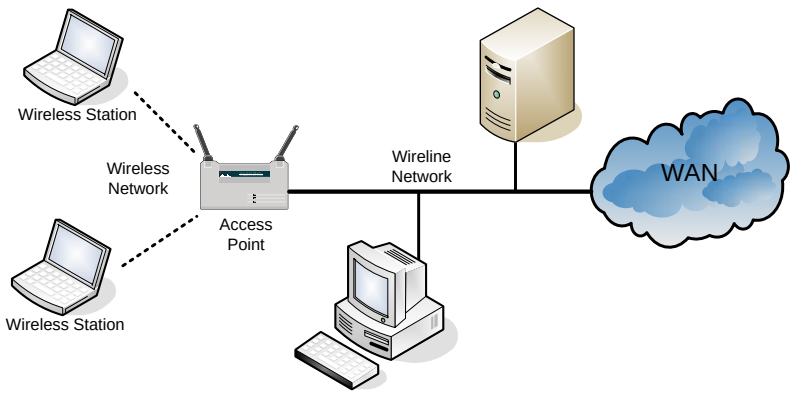
- Authentication + Encryption = Wireless Security.

Bởi vì mạng Wireless truyền và nhận dữ liệu dựa trên sóng radio và vì AP phát sóng lan truyền trong bán kính cho phép nên bất cứ thiết bị nào có hỗ trợ truy cập Wireless đều có thể bắt sóng này, sóng Wireless có thể truyền xuyên qua các vật liệu như bêtông, nhựa, sắt,... Cho nên rủi ro thông tin bị các attacker đánh cắp hoặc nghe trộm rất cao, vì hiện tại có rất nhiều công cụ hỗ trợ cho việc nhận biết và phân tích thông tin của sóng Wireless sau đó dùng thông tin này có thể dò khoá WEP (như AirCrack, AirSnort,...)

d. Các mô hình thực tế

Trên thực tế thì có rất nhiều mô hình mạng không dây từ một vài máy tính kết nối Adhoc đến mô hình WLAN, WWAN, mạng phức hợp. Sau đây là 2 loại mô hình kết nối mạng không dây phổ biến, từ 2 mô hình này có thể kết hợp để tạo ra nhiều mô hình phức tạp, đa dạng khác.

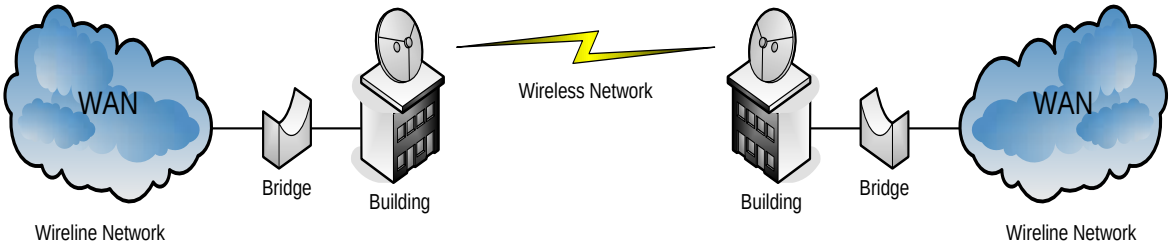
d1. Mạng không dây kết nối với mạng có dây



Hình 1.4. Mô hình mạng không dây kết nối với mạng có dây

AP sẽ làm nhiệm vụ tập trung các kết nối không dây, đồng thời nó kết nối vào mạng WAN (hoặc LAN) thông qua giao diện Ethernet RJ45, ở phạm vi hẹp có thể coi AP làm nhiệm vụ như một router định tuyến giữa 2 mạng này

d2. Hai mạng có dây kết nối với nhau bằng kết nối không dây



Hình 1.5. Mô hình 2 mạng có dây kết nối với nhau bằng kết nối không dây

Kết nối không dây giữa 2 đầu của mạng 2 mạng WAN sử dụng thiết bị Bridge làm cầu nối, có thể kết hợp sử dụng chảo thu phát nhỏ truyền sóng viba. Khi đó khoảng cách giữa 2 đầu kết nối có thể từ vài trăm mét đến vài chục km tùy vào loại thiết bị cầu nối không dây.

1.2.3.4. WEP – Wired Equivalent Privacy

WEP là một hệ thống mã hoá dùng cho việc bảo mật dữ liệu cho mạng Wireless, WEP là một phần của chuẩn 802.11 gốc và dựa trên thuật toán mã hoá RC4, mã hoá dữ liệu 40bit để ngăn chặn sự truy cập trái phép từ bên ngoài. Thực tế WEP là một thuật toán được dùng để mã hoá và giải mã dữ liệu.

- Đặc tính kỹ thuật của WEP:

+ Điều khiển việc truy cập, ngăn chặn sự truy cập của những Client không có khóa phù hợp.

+ Sự bảo mật nhằm bảo vệ dữ liệu trên mạng bằng cách mã hoá chúng và chỉ cho những Client nào đó đúng khoá WEP giải mã.

1.2.3.5. WEP key lengths

Một khoá WEP chuẩn sử dụng khoá 64 bits mã hoá theo thuật toán RC4. Trong 64 bits có 40 bits được ẩn. Nhiều nhà cung cấp sử dụng nhiều tên khác nhau cho khóa WEP như: “standar WEP” “802.11 – compliant WEP”, “40- bits WEP”, “40 + 24 bits WEP” hoặc thậm chí là “64 bits WEP”. Nhưng hiện tại thì 64 bits WEP thường được nhắc đến hơn hết. Nhưng với những thiết bị sử dụng 64 bits

WEP thường thì tính bảo mật không cao và dễ dàng bị tấn công. Hiện nay có một chuẩn tốt hơn đó là 128 – bits WEP, hầu hết các doanh nghiệp, cá nhân đều dần chuyển sang 128 bits WEP sử dụng thuật toán RC4 mã hoá, tính bảo mật cao hơn, các Attacker cũng khó khăn trong việc dò thấy khoá WEP. Nhưng về sau tính bảo mật của khoá WEP 128 bits cũng không có khó khăn nữa đối với các Attacker nhờ sự hỗ trợ của các công cụ dò tìm khoá WEP, thì lúc đó Wi–fi Protected Access – WPA là một chuẩn bảo mật cao cấp hơn WEP được ra đời (chúng ta sẽ nghiên cứu sâu hơn về WPA trong phần sau).

1.2.3.6. WPA – Wi- fi Protected Access

WPA được thiết kế nhằm thay thế cho WEP vì có tính bảo mật cao hơn. Temporal Key Intergrity Protocol (**IP) còn được gọi là WPA key hashing là một sự cải tiến dựa trên WEP, là vì nó tự động thay đổi khoá, điều này gây khó khăn rất nhiều cho các Attacker dò thấy khoá của mạng.

Mặc khác WAP cũng cải tiến cả phương thức chứng thực và mã hoá. WPA bảo mật mạng hơn WEP rất nhiều. Vì WPA sử dụng hệ thống kiểm tra và bảo đảm tính toàn vẹn của dữ liệu tốt hơn WEP.

1.2.3.7. WPA2 – Wi- fi Protected Access 2

WPA2 là một chuẩn ra đời sau đó và được kiểm định lần đầu tiên vào ngày 1/9/2004 . WAP2 được National Institute of Standards and Technology (NIST) khuyến cáo sử dụng, WPA2 sử dụng thuật toán mã hoá Advance Encryption Standar (AES).

WPA2 cũng có cấp độ bảo mật rất cao tương tự như chuẩn WPA, nhằm bảo vệ cho người dùng và người quản trị đối với tài khoản và dữ liệu.

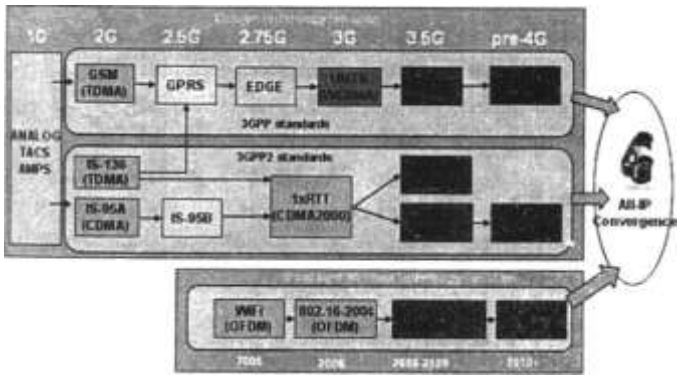
Nhưng trên thực tế WPA2 cung cấp hệ thống mã hoá mạnh hơn so với WPA và đây cũng là nhu cầu của các tập đoàn và doanh nghiệp có quy mô lớn. WPA2 sử dụng rất nhiều thuật toán để mã hoá dữ liệu như **IP, RC4, AES và một vài thuật toán khác. Những hệ thống sử dụng WPA2 đều tương thích với WPA.

1.3. Kiến trúc cơ bản của mạng WAN không dây.

Mạng vô tuyến diện rộng: Nhóm này bao gồm các công nghệ mạng thông tin di động như UMTS/GSM/CDMA 2000.... Vùng phủ của nó cũng tầm vài km đến tầm chục km.

Với sự ra đời của mạng thông tin di động tế bào, chúng ta đã chứng kiến sự tăng vọt về nhu cầu dịch vụ không dây & di động. Chúng ta đã và đang chứng kiến sự phát triển đến chóng mặt của mạng không dây: Năm 2002 đánh dấu thời điểm lịch sử của mạng viễn thông với số thuê bao di động vượt số thuê bao cố định. Theo ITU, tháng 9 năm 2005, số thuê bao di động trên thế giới đã vượt con số 2 tỷ. Theo thống kê của GSA (Global mobile Supplies Association) gần đây, con số này đã vượt 3 tỷ. Tuy nhiên, lịch sử của mạng tế bào còn rất ngắn ngủi. Nó mới trải qua 3 thế hệ và ở nhiều quốc gia nó vẫn còn đang ở thế hệ thứ 2.

Trong mạng thông tin di động tế bào, mỗi một thập kỷ chứng kiến một thế hệ mạng mới. Thế hệ đầu tiên (1G) khởi đầu từ những năm 80s. Đó là thế hệ điện thoại di động analog. Thế hệ thứ 2 (2G) bắt đầu nổi lên từ những năm của thập niên 90. Thế hệ thứ 2G là công nghệ di động kỹ thuật số, cung cấp dịch vụ voice và cả data. Thế hệ thứ 3 (3G) bắt đầu từ năm 2001 ở Nhật Bản, đặc trưng bởi dịch vụ thoại dữ liệu và đa phương tiện với tốc độ cao. Hệ thống tiền 4G, những viên đã tảng cho thế hệ thứ 4G, hy vọng sẽ được thương mại hoá vào khoảng đầu năm 2010. Một thế hệ 4G sẽ cất cánh vào những năm 2012. Con đường phát triển của các công nghệ mạng tế bào được thể hiện ở hình dưới đây.



Hình 1.6. Con đường phát triển của các công nghệ mạng

1.3.1. Thế hệ thứ 1 (1G)

Mạng di động thế hệ thứ nhất khơi mào ở Nhật vào năm 1979. Đây là hệ thống truyền tín hiệu tương tự (analog). Những công nghệ chính thuộc thế hệ thứ nhất này có thể kể đến là AMPS (Advanced Mobile Phone System), TACS (Total Access Communication System), JTACS (Japan TACS) NMT (Nordic Mobile Telephone). Tuy nhiên chưa hoàn hảo về mặt công nghệ kỹ thuật, thế hệ thông tin di động 1G này thực sự là một mốc phát triển quan trọng của ngành viễn thông (khái niệm di động (mobile)) đã bắt đầu đi vào phục vụ nhu cầu liên lạc của con người trong đời sống hàng ngày. Những điểm yếu nổi bật của thế hệ 1G liên quan đến chất lượng truyền tin kém, vấn đề bảo mật và việc sử dụng kém hiệu quả tài nguyên tần số.

1.3.2. Thế hệ thứ 2 (2G)

Hệ thống mạng 2G được đặc trưng bởi công nghệ chuyển mạch kỹ thuật số (digital circuit – switched). kỹ thuật này cho phép sử dụng tài nguyên băng tần hiệu quả hơn nhiều so với 1G/. Hầu hết các thuê bao di động trên thế giới hiện đang dùng công nghệ 2G này. Công nghệ 2G sẽ còn tồn tại thêm một thời nữa trước khi 3G thay thế hoàn toàn nó. Những chuẩn di động 2G chính bao gồm GSM (Global System for Mobile Communication)IS – 136 và CdmaOne.

GSM sử dụng kỹ thuật đa truy cập TDMA và song công FDD. GSM đã trở thành công nghệ truyền thông có tốc độ phát triển nhanh nhất từ trước đến nay và là một chuẩn di động được triển khai rộng rãi trên thế giới.

- IS – 136 được biết đến với tên D – AMPS (Digital - AMPS) sử dụng kỹ thuật đa truy cập TDMA và song công TDD . Công nghệ này được triển khai nhiều ở Châu Mĩ, đặc biệt là ở Mỹ và Canada. IS – 136 được triển khai như một mạng overlay kỹ thuật số, phủ trên nền hạ tầng mạng AMPS.IP – 136 cho tốc độ dữ liệu lên đến 30 Kbps.

- CdmaOne là tên gọi của chuẩn di động ITU IS – 95 sử dụng kỹ thuật đa truy cập CDMA. CDMA được chuẩn hoá năm 1993. Ngày nay, có 2 phiên bản IS – 95 gọi là IS – 95 B. IS – 95A dùng FDD với độ rộng kênh là 1,25 MHz cho mỗi hướng

lên và xuống. Tốc dộ dữ liệu tối đa của IS – 95 A là 14,4 Kbps. IS – 95 B có thể cung ứng tốc độ dữ liệu lên đến 115 Kbps bằng cách gộp 8 kênh lại với nhau. Với tốc độ này, IS – 95B còn được phân loại như là công nghệ 2,5 G.

Thế hệ 2,5 G : Thế hệ 2,5 G đặc trưng bởi dịch vụ dữ liệu tốc độ cải tiến. Chuẩn chính của thế hệ này là GPRS, EDGE và IS – 95 B. GPRS là một bước phát triển tiếp theo để cung cấp dịch vụ dữ liệu tốc độ cao cho người dùng GMS và IS – 136. Lý thuyết mà nói thì GPRS có thể cung ứng tốc độ dữ liệu lên đến 172, 2 Kbps. GPRS là một giải pháp chuyển mạch gói. Đây cũng là một bước đệm trong quá trình chuyển từ thế hệ 2G lên 3G của các nhà cung cấp dịch vụ GSM/ IS – 136 . Trên con đường dài đi đến 3G, EDGE đã ra đời để cải tiến tốc độ dữ liệu hơn nữa (tốc độ tối đa tầm 384 Kbps). EDGE đôi khi còn được trích dẫn như công nghệ 2,75 G.

1.3.3. Thế hệ di động thứ 3 (3G)

Mạng 3G đặc trưng bởi tốc độ dữ liệu cao, capacity của hệ thống lớn tăng hiệu quả sử dụng phổ tần và nhiều cải tiến khác. Có một loạt các chuẩn công nghệ di động 3G, tất cả đều dựa trên CDMA bao gồm: UMTS (dùng cả FDD lẫn TDD) , CDMA 2000 và TD SCDMA.

- UMTS (đôi khi còn được gọi là 3GSM) sử dụng kỹ thuật đa truy cập WCDMA. UMTS được chuẩn hoá bởi 3GSM - UMTS là công nghệ 3G được lựa chọn bởi hầu hết các nhà cung cấp dịch vụ GSM/GPRS để đi lên 3G. Tốc độ dữ liệu tối đa là 1920 Kbps (gần 2Mbps). Nhưng trong thực tế tốc độ này chỉ tầm 384 Kbps thôi. Để cải tiến tốc độ dữ liệu của 3G hai kỹ thuật HSDPA và HSUPA đã được đề nghị. Khi cả 3 kỹ thuật này được triển khai, người ta gọi chung là HSPA. HSPA thường được biết đến như là công nghệ 3,5G.

+ HSDPA: Tăng tốc độ downlink (đường xuống, từ NodeB về người dùng di động). Tốc độ tối đa lý thuyết là 14,4 Mbps, nhưng trong thực tế nó chỉ đạt tầm 1,8 Mbps (hoặc tốt lắm là 3,6 Mbps). Theo một báo cáo của GSA tháng 7 năm 2008, 207 mạng HSDPA đã và đang bắt đầu triển khai, trong đó 207 đã thương mại hoá ở 89 nước trên thế giới.

+ HSUPA: Tăng tốc độ uplink (đường lên) và cải tiến QoS. Kỹ thuật này cho phép người dùng upload thông tin với tốc độ lên đến 5,8 Mbps (lý thuyết). Cũng trong cùng báo cáo trên của GSA, 51 nhà cung cấp dịch vụ thông tin di động đã triển khai mạng HSUPA ở 35 nước và 17 nhà cung cấp mạng lên kế hoạch triển khai mạng HSUPA.

- CDMA 2000 là người " nối giõi" của 2G CdmaOne đại diện cho họ công nghệ bao gồm CDMA 2000 1xRTT (Radio Transmission Technology), CDMA 2000 EV – DO (Evolution – Data Optimized) và CDMA 2000 EV – DO (Evolution – Data and voice). CDMA 2000 được chuẩn hoá bởi 3GPP2. Lẽ thường tình thì CDMA 2000 là công nghệ 3G được lựa chọn bởi các nhà cung cấp mạng CdmaOne.

+ CDMA 2000 1xRTT: Chính thức được công nhận như là một công nghệ 3G, tuy nhiên nhiều người xem nó như là một công nghệ 2,75 G đúng hơn là 3G. Tốc độ của 1xRTT có thể đạt đến 307 Kbps, song hầu hết các mạng đã triển khai chỉ giới hạn tốc độ peak ở 144 Kbps.

+ CDMA 2000 EV- DO: Sử dụng một kênh dữ liệu 1,25 MHz chuyên biệt và có thể cho tốc độ dữ liệu đến 2,4 Mbps cho đường xuống và 153 Kbps cho đường lên. 1xEV – DO Rev hỗ trợ truyền thông gói IP, tăng tốc độ đường xuống đến 3,1 Mbps và đặc biệt có thể đẩy tốc độ đường lên đến 1,2 Mbps. Bên cạnh đó, 1xEV-DO Rev B cho phép nhà cung cấp mạng gộp đến 15 kênh 1,25 MHz lại để truyền dữ liệu với tốc độ 73,5 Mbps. Theo một báo cáo trên www.cdg.org site, 3G CDMA 2000 EV – DO đã vượt con số 83 triệu thuê bao vào tháng 9 năm 2007.

+ CDMA 2000 EV- DV : Tích hợp thoại và dữ liệu trên cùng một kênh 1,25MHz CDMA 2000 EV-DV cung cấp tốc dộ peak đến 4,8 Mbps cho đường xuống và đến 307 Kbps cho đường lên. Tuy nhiên từ năm 2005, Qualcomm đã dừng vô thời hạn việc phát triển của 1xEV- DV vì đa phần các nhà cung cấp mạng CDMA như Verizon Wireless và Sprint đã chọn EV – DO.

+ TD- SCDMA là chuẩn di động được đề nghị bởi "China Communications Standards" và được ITU duyệt vào năm 1999. Đây là chuẩn 3G của Trung Quốc.

TD- SCDMA dùng song công TDD. TD – SCDMA có thể hoạt động trên một dải tần hẹp 1,6MHz (cho tốc độ 2Mbps) hay 5MHz (cho tốc độ 6Mbps). Ngày xuất hành của TD – SCDMA đã bị đẩy lùi nhiều lần. Nhiều thử nghiệm về công nghệ này đã diễn ra từ đầu năm 2004.

+ Hệ thống 3GPP LTE là bước tiếp theo cần hướng tới của hệ thống mạng không dây 3G dựa trên công nghệ di động GSM/UMTS và là một trong những công nghệ tiềm năng nhất cho truyền thông 4G. Liên minh Viễn thông Quốc Tế (ITU) đã định nghĩa truyền thông di động thế hệ 4 là IMT Advanced và chia thành hai hệ thống dùng cho di động tốc độ cao và di động tốc độ thấp. 3GPPLTE là hệ thống dùng cho di động tốc độ cao. Ngoài ra, đây còn là công nghệ hệ thống tích hợp đầu tiên trên thế giới ứng dụng cả chuẩn moddm3GPP LTE và các chuẩn dịch vụ ứng dụng khác, do đó NSD có thể dễ dàng thực hiện cuộc gọi hoặc truyền dữ liệu giữa các mạng LTE và các mạng GSM/GPRS hoặc UMTS dựa trên WCDMA.

- 3GPP LTE có khả năng cấp phát phổ tần linh động và hỗ trợ các dịch vụ đa phương tiện với tốc độ trên 100Mb/s khi di chuyển ở tốc độ 3 km/h và đạt 30 Mb/s khi di chuyển ở tốc độ cao 120 km/ h. Tốc độ này nhanh hơn gấp 7 lầ n so với tốc độ truyền dữ liệu cho công nghệ HSDPA (truy nhập gói dữ liệu tốc độ cao). Do công nghệ này cho phép sử dụng các dịch vụ đa phương tiện tốc độ cao trong khi di chuyển ở bất kỳ tốc độ nào nên nó có thể hỗ trợ sử dụng các dịch vụ nội dung có dung lượng lớn với độ phân giải cao ở điện thoại di động, máy tính bỏ túi PDA, điện thoại thông minh...

Ưu điểm nổi bật:

Dung lượng truyền trên kênh đường xuống có thể đạt 100Mbps và trên kênh đường lên có thể đạt 50 Mbps.

Tăng tốc độ truyền trên cả người sử dụng và các mặt phẳng điều khiển. Sẽ không còn chuyển mạch kênh. Tất cả sẽ dựa trên IP.VoIP sẽ dùng cho dịch vụ thoại.

Kiến trúc mạng sẽ đơn giản hơn so với mạng 3G hiện thời. Tuy nhiên mạng 3G LTE vẫn có thể tích hợp một cách dễ dàng với mạng 3G và 2G hiện tại. Điều

này hết sức quan trọng cho nhà cung cấp mạng triển khai 3GPP LTE vì không cần thay đổi toàn bộ cơ sở hạ tầng mạng đã có.

OFDMA và MIMO được sử dụng trong 3G LTE thay vì CDMA như trong 3G.

Chuẩn UMB

Chuẩn UMB hiện nay được phát triển bởi 3GPP2 với kế hoạch là sẽ thương mại hoá trước 2009.

Một số đặc điểm kỹ thuật như sau:

Các kỹ thuật Miltiple radio và antenna tiên tiến.

Multiple Input Multiple Output (MIMO), đa truy nhập phân chia theo không gian (Spatial Division Multiple Access (SDMA)) và kỹ thuật beamforming antenna.

Các kỹ thuật quản lý nhiễu tiên tiến (Improved interference management techniques).

Tốc độ dữ liệu cao nhất (peak data rates).

Lên tới 288 Mbps đường lên, 75 Mbps đường xuống.

Lên tới 1000 người sử dụng VoIP đồng thời (với sự cấp phát 20 MHz FDD).

Chuẩn IEEE 802.x.

Chuẩn này bắt nguồn từ mạng WiFi, sau đó tiến lên 802.16e rồi 802.16m và bây giờ là 802.20. Chuẩn IEEE 802.20 còn được gọi là truy nhập vô tuyến băng rộng di động WBMA (Mobile Broadband Wireless Access). Nó có thể hỗ trợ ngay cả khi đã di chuyển với tốc độ lên tới 250 km/h.

Trong khi chuyển vùng (roaming) của WiMAX nhìn chung bị giới hạn trong một phạm vi nhất định, thì chuẩn IEEE 802.20 giống như 3G có khả năng hỗ trợ chuyển vùng toàn cầu. Ngoài ra, cũng giống như WiMAX, IEEE 802.20 cũng hỗ trợ các kỹ thuật QoS nhằm cung cấp những dịch vụ có yêu cầu cao về độ trễ, jitter... Trong mạng EEE 802.20 việc đồng bộ giữa đường lên và đường xuống đều được thực hiện hiệu quả. Dự kiến chuẩn IEEE 802.20 tương lai sẽ kết hợp một số tính năng của IEEE 802.16e và các mạng dữ liệu 3G, nhằm cung cấp và tạo ra một truyền thông đa dạng (rich communication).

Feature	HSPA	1x EV-DO	Mobile WiMAX	WiFi
Standard	3GPP R6	3GPP2	IEEE 802.16e-2005	IEEE 802.11n
Peak DL data rate	14.4Mbps using all 15 codes	3.1Mbps (Rev A) 4.6Mbps (Rev B)	46Mbps @ 3:1, 2x2, 10Mhz	100Mbps
Peak UL data rate	5.8Mbps	1.8Mbps	7Mbps @3:1, 10Mhz	100Mbps
Bandwidth	5MHz	1.25MHz	3.5, 7, 5,10,8.75MHz	20, 40MHz
Duplexing	FDD	FDD	TDD initially	TDD
Multiplexing	TDM CDMA	TDM CDMA	TDM OFDMA	CSMA-CA
Coverage	1-5km	1-5km	3.5km	100m
Mobility	High	High	Mobile	Low

Bảng 1.1. Technology Features Comparison

Feature	LTE	UMB	WiMAX 802.16m
Peak data rate (per sector @20MHz)	DL: 288Mbps (4x4) UL: 98Mbps (2x4)	DL:250Mbps (4x4) UL: 100Mbps (4x4)	DL: ~ 350Mbps (4x4) UL: ~ 200Mbps (2x4)
Latency	Link-Layer Access: <5 ms Handover: <30ms	LLA: <10ms Handover: <20ms	LLA: <10ms Handover: <20ms
MIMO configuration	DL: 2x2, 2x4, 4x2, 4x4 UL: 1x2, 1x4, 2x2, 2x4	DL: 2x2, 2x4, 4x2, 4x4 UL: 1x2, 1x4, 2x2, 2x4	DL: 2x2, 2x4, 4x2, 4x4 UL: 1x2, 1x4, 2x2, 2x4
Bandwidth (MHz)	1.25, 1.6, 2.5, 5, 10, 15, 20	1.25 to 20	5, 10, 20, 40
Duplexing	TDD,FDD	TDD,FDD	TDD,FDD
Multiplexing	OFDMA and SC-FDMA	OFDMA	SOFDMA
Mobility	Up to 350 km/h	Up to 250 km/h	Up to 350 km/h

Bảng 1.2. Pre-4G Technology Requirement Comparison

1.4. Kiến trúc cơ bản của Internet không dây (Chuẩn WAP và các chuẩn mới (WPAN, WRAN, WMAN)).

1.4.1. Kiến trúc cơ bản của Internet không dây – chuẩn WAP

1.4.1.1. Sơ bộ về WAP.

Nhu cầu truy cập thông tin từ các thiết bị di động đã mở đường cho các công nghệ không dây phát triển mạnh mẽ. Yếu tố quan trọng nhất trong sự ra đời của Internet không dây là Digital Cellphone trong những năm gần đây. Việc mở rộng mạng Digital Cellphone và dịch vụ thông tin cá nhân PCS (Personal Communication Services).

Wireless Application Protocol (WAP) là một dạng đặc tả theo chuẩn công nghiệp mở cho các ứng dụng thực thi trên môi trường mạng không dây, chú trọng vào các ứng dụng trên thiết bị di động, đặc biệt là điện thoại di động. Các tiêu chuẩn này được đưa ra bởi WAP Forum, nhóm này hình thành vào thành 6 năm 1997 bởi

Erison, Nokia, Motorola và Unwired Planet và hiện tại đã được hàng trăm công ty khác tham gia, bao gồm IBM, Hewlett Packard, Visa và Microsoft. Theo thống kê chính thức của WAP Forum, những thành viên thuộc WAP Forum là đại diện cho trên 90% nhà sản xuất điện thoại di động trên toàn thế giới. WAP đã và sẽ được hỗ trợ trên nhiều loại thiết bị, từ đơn giản như điện thoại di động thông thường cho đến những thiết bị thế hệ mới – các điện thoại " thông minh" với màn hình rộng có thể chạy được nhiều ứng dụng, thậm chí là những máy trợ lý cá nhân kỹ thuật số (PDA), các palmtop hay các máy tính với kích thước nhỏ hơn. Tất cả các thiết bị di động rồi sẽ được áp dụng công nghệ WAP, trực tiếp từ nhà sản xuất hay từ phiên bản nâng cấp nào đó thuộc nhóm các công ty thứ ba (third – party). Mỗi một thiết bị có một cách hiển thị khác nhau và các phương thức nhập liệu khác nhau. Công việc của công nghệ WAP là sắp xếp lại " mớ hỗn độn" đó và cung cấp một khung làm việc (framework) chung cho phép các ứng dụng chạy được trên tất hệ nền khác nhau này.

Mô hình WAP còn chính là mô hình WWW (World Wide Web) với một số tính năng nâng cao. Trong đó, hai tính năng quan trọng nhất là: đẩy (Push) và hỗ trợ thoại. Nội dung thông tin WAP được truyền tải nhờ một tập các giao thức truyền thông tiêu chuẩn trong tập giao thức WAP. WAP định nghĩa một tập các thành phần tiêu chuẩn cho phép truyền thông giữa thiết bị đầu cuối và máy chủ mạng gồm:

- Mô hình tên tiêu chuẩn: Các URL được sử dụng để nhận dạng nội dung WAP trên các máy chủ, URI được sử dụng để nhận dạng tài nguyên trong một thiết bị, ví dụ như chức năng điều khiển cuộc gọi.
- Kiểu nội dung: Được đưa ra trên kiểu đặc trưng giống như WWW.
- Các khuôn dạng nội dung tiêu chuẩn: dựa trên công nghệ WWW và bao gồm ngôn ngữ đánh dấu, thông tin lịch, các đối tượng, hình ảnh và ngôn ngữ kịch bản (*Script*).

- Các giao thức truyền thông tiêu chuẩn: Cho phép truyền thông các yêu cầu đầu cuối di động tới máy chủ mạng thông qua cổng WAP. Các tiêu chuẩn này tối ưu theo hướng của thiết bị đầu cuối sử dụng.

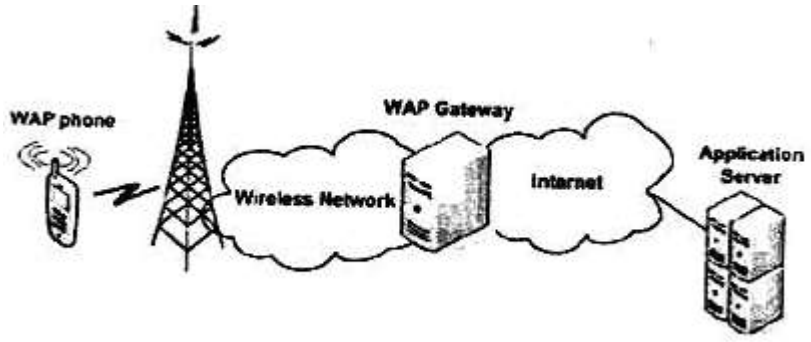
Để tạo ra một Website có khả năng thâm nhập qua thiết bị không dây thật sự là một thử thách vì vậy chỉ có một phần nhỏ trong hơn 1 tỷ Website cung cấp thành phần Internet không dây. WAP được thiết kế để làm việc với bất kỳ dịch vụ không dây nào tồn tại như:

- Dịch vụ nhắn tin ngắn SMS (Short Message Service).
- Dữ liệu chuyển mạch tốc độ cao CSD (High-speed Circuit-switched Data).
- Dịch vụ GPRS (General Packet Radio Service).
- Dữ liệu dịch vụ bổ sung không cấu trúc USSD (Unstructured Supplementary Services Data).

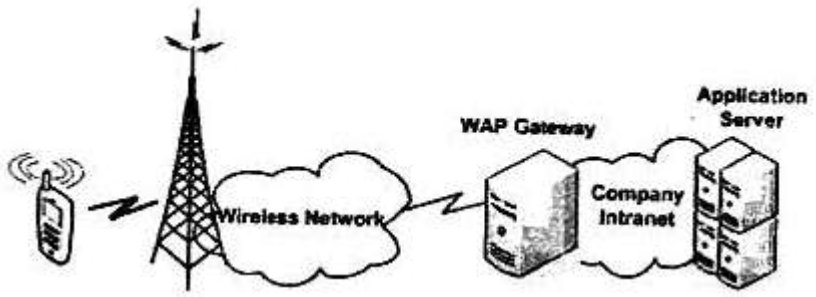
Các giao thức WAP được thiết kế trên nền của các giao thức web. Mục đích cuả WAP là sử dụng lại cấu trúc cơ sở của web, để từ đó nâng cao quá trình giao tiếp giữa nhà cung cấp và các thiết bị di động, giúp quá trình này trở nên hiệu quả và tốn ít thời gian hơn là sử dụng chính các giao thức web.

1.4.1.2. Các mô hình giao tiếp trên WAP

Do kiến trúc của WAP được thiết kế gần giống với Web, nên nó cũng kế thừa mô hình client – server được dùng trên Internet của Web. Điểm khác nhau chính là sự có mặt của WAP Gateway dùng cho việc chuyển đổi giữa HTTP và WAP.



Hình 1.7. WAP dùng truy cập Internet



Hình 1.8. WAP được dùng truy cập trong Intranet

Để truy cập vào một ứng dụng trên server, client khởi tạo một nối kết với WAP gateway và gửi đi yêu cầu của mình. Gateway sẽ chuyển đổi những yêu cầu này sang định dạng được dùng trên Internet (HTTP) và sau đó chuyển chúng đến server cung cấp dịch vụ. Nội dung trả về được gửi từ server đến gateway, tại đây nó sẽ được chuyển sang định dạng WAP, để sau đó gửi về cho thiết bị di động. Như vậy, gateway đã giúp Internet có thể giao tiếp với môi trường mạng không dây.

Các ngăn xếp của giao thức WAP được chia thành các lớp cho phép dễ dàng mở rộng, thay đổi và phát triển (tương tự mô hình OSI). Giao thức truy nhập ứng dụng vô tuyến WAP gồm có 5 lớp:

- Lớp truyền tải: Giao thức datagram vô tuyến (WDP)
- Lớp bảo mật: Giao thức lớp truyền tải vô tuyến (WTLS)
- Lớp giao vận: Giao thức giao vận vô tuyến (WTP)
- Lớp phiên: Giao thức phiên vô tuyến (WSP)
- Lớp ứng dụng: Môi trường ứng dụng vô tuyến (WAE)

Tất cả các ngăn xếp giao thức WAP đều được thiết kế để phù hợp với các điều kiện ràng buộc của mạng di động. Mỗi một lớp cung cấp một tập các chức năng hoặc các dịch vụ tới các dịch vụ và ứng dụng khác qua tập giao diện tiêu chuẩn.

Kiến trúc WAP tách các giao tiếp dịch vụ từ các giao thức cung cấp dịch vụ để cho phép mở rộng các đặc tính và tự do lựa chọn các giao thức thích hợp cho một nội dung cụ thể. Rất nhiều các dịch vụ trong ngăn xếp có thể được hỗ trợ bởi một hoặc nhiều giao thức. Ví dụ dịch vụ truyền đa phương tiện được hỗ trợ bởi 2 giao thức HTTP và WSP.

Các giao thức trên lớp này được thiết kế và chọn lựa để điều hành trên nhiều dịch vụ mang khác nhau, bao gồm nhắn tin ngắn SMS, dữ liệu chuyển mạch kênh và dữ liệu gói. Các kênh mang đưa ra nhiều mức chất lượng dịch vụ khác nhau tương ứng với thông lượng, tỉ lệ lỗi, và độ trễ. Các giao thức lớp mang thông tin được tạo ra nhằm khắc phục các điểm yếu của kênh mang thông tin, tùy biến theo từng loại hình dịch vụ.

a. Lớp dịch vụ truyền tải

Lớp này cung cấp sự hội tụ giữa các dịch vụ mang với các phần còn lại của ngăn xếp WAP. Giao thức dữ liệu vô tuyến WDP (Wireless Datagram Protocol) chứa một tập các kết nối kênh mang khác nhau và hỗ trợ các kỹ thuật để các giao thức chạy trên nó. Các tập kết nối này thay đổi theo hạ tầng cơ sở mạng và các dịch vụ truyền thông cần cung cấp. WDP truyền và nhận các dữ liệu từ các thiết bị đầu cuối mạng, WDP cũng thực hiện việc phân đoạn gói tin và đóng gói các datagram cho phù hợp với đặc tính của kênh mang thông tin. Giao thức bản tin điều khiển vô tuyến WSMP là một phần mở rộng của WDP là giao thức báo cáo lỗi có cơ chế tương tự ICMP trong Internet, giao thức này hữu dụng khi WAP không sử dụng trên kênh mang IP hoặc cho mục đích thu thập thông tin và chẩn đoán mạng.

b. Lớp bảo mật

Mục tiêu của bảo mật lớp truyền tải vô tuyến WTLS (Wireless Transport Layer Security) là đảm bảo tính năng bảo mật giữa các thiết bị đầu cuối WAP và cổng/ủy quyền WAP. WTLS đưa ra khung làm việc cho các kết nối an toàn cho các

ứng dụng truyền thông 2 chiều. WTLS sử dụng các thành phần từ các giao thức bảo mật cơ bản của Internet như lớp socket an toàn SSL (Socket Security Layer) và bảo mật lớp truyền tải TLS (Transport Layer Security). Nguyên tắc của WTLS cho phép chứng nhận các dữ liệu gốc, xác nhận bản quyền của bản tin. Để đảm bảo tính riêng tư và tính toàn vẹn của dữ liệu, các kỹ thuật mã hoá và các mã nhận thực bản tin được sử dụng. Để thiết lập các đấu nối an toàn, trong pha thiết lập được tạo ra các tham số cần thiết như: đặt tham số, chuyển đổi khoá và nhận thực. Giống như các giao thức khác của WAP, WTLS tối ưu cho các kênh truyền thông băng hẹp.

c. Lớp giao vận

Giao thức giao vận vô tuyến WTP (Wireless Transaction Protocol) có nhiệm vụ đáp ứng các yêu cầu và trả lời về phương tiện truyền thông từ người sử dụng tới máy chủ ứng dụng và ngược lại. WTP tương thích với các điều kiện ràng buộc về băng thông hẹp của môi trường vô tuyến, trong đó nó tối thiểu tiêu đề giao thức qua việc tối thiểu số lượng lần phát lại. Các đặc tính chủ chốt của WTP là cung cấp các dịch vụ giao vận cho các hoạt động trực tuyến như duyệt Web.

WTP được thiết kế để tăng số lượng các pha giao vận, giảm các thủ tục phát lại, xác nhận và thủ tục giải phóng. Ngoài ra, WTP còn có thể mở rộng chức năng phân đoạn và tạo lại bản tin. Tổ hợp giao thức giao vận vô tuyến WTP và giao thức phiên vô tuyến WSP (Wireless Session Protocol) cung cấp dịch vụ truyền tải siêu văn bản (hypermedia) giữa các phần tử mạng qua truyền tải phi kết nối, trong khi giao thức truyền tải siêu văn bản HTTP cung cấp dịch vụ truyền tải siêu văn bản qua truyền tải có hướng kết nối.

d. Lớp phiên

Giao thức lớp phiên vô tuyến WSP hỗ trợ lớp ứng dụng của WAP mô tả trong phiên với một giao tiếp của 2 dịch vụ phiên: Kết nối có hướng đảm bảo độ tin cậy

và phi kết nối không đảm bảo độ tin cậy. WTP cung cấp các phương tiện truyền thông như:

- Hỗ trợ chức năng HTTP, để giảm tải cho WSP thì sử dụng phiên bản HTTP 1.1.
- Ghép nối người dùng vào thành viên của phiên truyền thông dữ liệu có thời gian truyền lớn.
- Yêu cầu cho các máy chủ đẩy dữ liệu tới người sử dụng.
- Tạo ra một chuỗi thủ tục cho phép ứng dụng máy chủ xác định người dùng có hoặc không hỗ trợ các phương tiện và cấu hình giao thức thích hợp.
- Khả năng ngừng và tái tạo phiên.

WSP hỗ trợ cơ chế cache tiêu đề để tăng hiệu quả kênh truyền. Giao thức HTTP truyền thống không hỗ trợ cache tiêu đề nên khoảng 90% các yêu cầu chứa các tiêu đề cố định vẫn phải chuyển trên mạng.

e. Lớp ứng dụng

Môi trường ứng dụng vô tuyến WAE (Wireless Application Enviroment) nằm trong lớp ứng dụng cung cấp môi trường cho phép mở rộng miền các ứng dụng được sử dụng trên các thiết bị vô tuyến bao gồm cả dịch vụ tin nhắn đa phương tiện [3]. WAP có hai kiểu tác nhân (agent) trong thiết bị vô tuyến: tác nhân sử dụng WML (Wireless Markup Language) và agent sử dụng WTA (Wireless Telephony Application) để hỗ trợ thoại.

1.4.1.3. Ưu và nhược điểm của WAP

WAP ứng dụng ngôn ngữ WML để triển khai và thể hiện các trang Web tiêu chuẩn cho phù hợp với các thiết bị di động. Sử dụng khuôn dạng tín hiệu dữ liệu tối ưu, WAP được thiết kế để duyệt các nội dung web tới thiết bị vô tuyến thông qua loại bỏ các thành phần đồ họa nhằm hiển thị trên màn hình nhỏ và hạn chế băng thông. Thực tế rất nhiều mã WML được sửa đổi từ mã HTML.

Mặc dù WAP hỗ trợ cho hầu hết các thiết bị di động nhưng nó vẫn tồn tại một số điểm hạn chế trong giao thức này:

- ***Độ trễ:*** WAP dựa trên giao thức TCP/IP và không tự xây dựng hệ thống bảo mật riêng cũng như khả năng tự đẩy dữ liệu, điều này sẽ ảnh hưởng tới những ứng dụng cần được chạy ngay khi người dùng đang truyền dữ liệu trên ứng dụng khác. Nếu triển khai ứng dụng kiểu này sẽ tăng độ phức tạp của hệ thống lên rất lớn và ảnh hưởng trực tiếp tới phần cứng và băng thông yêu cầu.

- ***Bảo mật:*** WAP là hệ thống giao thức điển hình không chứa bảo mật riêng, điều đó có nghĩa là dữ liệu không được mã hoá khi truyền. Các phần mềm bảo mật có thể được hỗ trợ cho WAP nhưng bị giới hạn vì độ ổn định, giá thành và thời gian thực hiện. Gateway: Giải pháp WAP yêu cầu có gateway vô tuyến, vì vậy nó sẽ làm tăng giá thành của hệ thống.

- ***Kết nối liên tục***: Các ứng dụng WAP được xây dựng dựa trên kiến thức yêu cầu/ đáp ứng vì vậy nó sẽ kết nối liên tục không giống như trên các trình duyệt trên các máy PC. Một số người sử dụng thường di chuyển vượt qua vùng phủ sóng và gây ra các lỗi kết nối. Vấn đề này có thể giải quyết bằng phương pháp "lưu và chuyển tiếp", giải pháp thêm vào này cũng làm tăng giá thành và độ phức tạp của hệ thống. Trên thực tế, việc thêm vào khả thường yêu cầu phần cứng kèm theo và tăng thêm băng thông sử dụng.

- ***Triển khai dịch vụ***: WAP Được tạo ra để duyệt nội dung các trang web, các nhà cung cấp nội dung được yêu cầu quản lý và duy trì các bản sao cho mỗi website. Các bản sao như vậy thực sự là không hiệu quả vì nó làm tăng giá thành khi mở rộng và bảo dưỡng hệ thống.

- ***Tương tác thấp:*** WAP rất khó tích hợp với các ứng dụng có sẵn trên các thiết bị, đây là giới hạn thường thấy của các giải pháp trên các đầu cuối có năng lực xử lý và giao diện màn hình nhỏ.

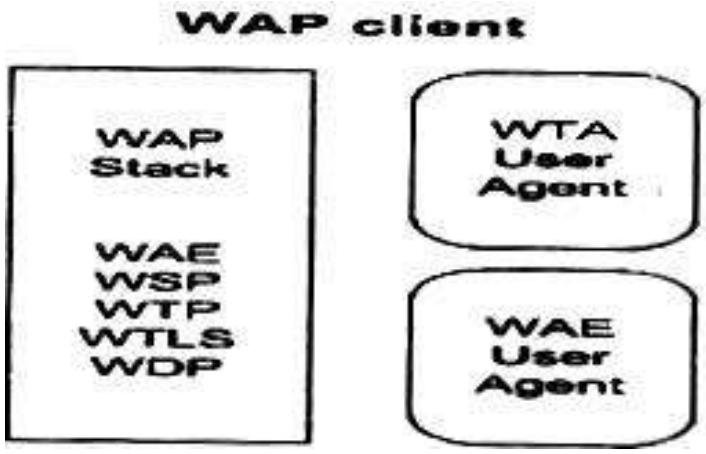
- ***Khả năng đẩy và kéo:*** Các giải pháp WAP yêu cầu người sử dụng gửi các thông tin trước khi họ nhận chúng. Như vậy, email, cảnh báo không thể nhận ngay tức khắc. Thuật ngữ "kéo" liên quan tới khả năng của thiết bị để cảnh báo người sử

dụng khi có dữ liệu của họ đến. Chức năng đẩy là chức năng có sẵn của WAP nhưng nó yêu cầu thêm một lớp kiến trúc và như vậy sẽ làm tăng nguy cơ xảy ra lỗi và trễ.

1.4.1.4. Các thành phần của WAP

Các đặc tả WAP cho phép những nhà sản xuất di động có nhiều lựa chọn cho riêng mình. Nó không bắt buộc thiết bị WAP phải trông như thế nào hay sẽ hiển thị nội dung nhận được từ Internet ra sao, mà nó gắn liền với giao diện người dùng với tổ chức bên trong của chức năng điện thoại.

Yêu cầu duy nhất cho một thiết bị hỗ trợ WAP đó là nó phải cung cấp một tác nhân người dùng WAE (WAE User Agent) một tác nhân người dùng WTA (WTA User Agent) một tác nhân người dùng WTA (WTA User Agent) và ngăn xếp WAP (WAP Stack)



Hình 1.9. Wap Client

a. WAE User Agent.

Là một loại trình duyệt nhỏ (microbrowser) thực hiện hoàn trả nội dung phục vụ việc hiển thị. Nó nhận vào WML, WML Script đã được biên dịch và các hình ảnh từ WAP gateway, sau đó xử lý hoặc hiển thị chúng lên màn hình. WAE User

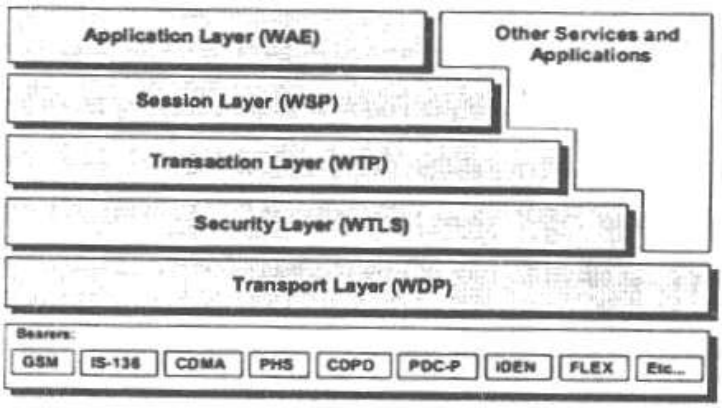
Agent cũng quản lý việc giao tiếp với người dùng, chẳng hạn như nhập liệu văn bản, thông báo lỗi hay các thông điệp cảnh báo khác.

b. WTA User Agent.

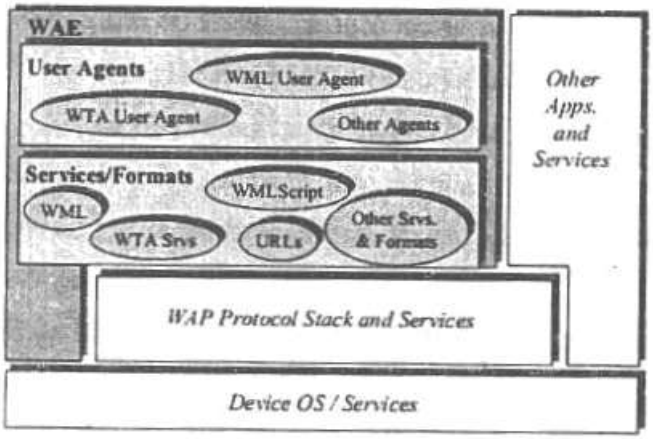
Nhận các tập tin WTA được biên dịch từ WTA server và thực thi chúng. WTA User Agent bao gồm việc truy cập vào giao diện điện thoại và các chức năng mạng như quay số, trả lời cuộc gọi, tổ chức phonebook, quản lý thông điệp và các dịch vụ định vị.

c. WAP Stack.

Cho phép điện thoại nối kết với WAP gateway sử dụng các giao thức WAP.



Hình 1.10. Wap Stack



Hình 1.11. Wap Stack

c.1. Wireless Sesion Layer – WSP.

Wireless Session Protocol cho phép các dịch vụ trao đổi dữ liệu với các ứng dụng theo một cách có tổ chức. Nó bao gồm hai giao thức khác nhau:

- Dịch vụ phiên hướng kết nối (Connection orented session services) hoạt động nhờ vào Wireless Transaction Protocol (WTP).

- Dịch vụ phiên phi kết nối (Connectionless session services) hoạt động trực tiếp trên Wireless Transport layer (WDP).

Các dịch vụ phiên (session services) là những chức năng giúp cho việc thiết lập kết nối giữa và một server. Dịch vụ này được phân phối thông qua việc dùng các "primitives" mà nó cung cấp.

Primitives là các thông điệp được định nghĩa mà một client dùng để gửi cho server yêu cầu dịch vụ. Chẳng hạn như trong WSP, một trong những primitives là SConnect, với nó chúng ta có thể yêu cầu việc tạo lập một nối kết với server.

c.1.1. Dịch vụ phiên hướng kết nối (Connection – oriented session service).

Cung cấp khả năng quản lý một phiên làm việc và vận chuyển dữ liệu tin cậy giữa client và server. Phiên làm việc tạo ra có thể được hoãn lại và phục hồi sau đó nếu như việc truyền tải dữ liệu không thể thực hiện đượC. Trong kỹ thuật push, dữ liệu không mong muốn có thể được gửi đi từ server đến client theo hai cách: được xác nhận hoặc là không được xác nhận.

- Trường hợp được xác nhận (confirmed push), client sẽ thông báo cho server khi nhận được dữ liệu.

- Trường hợp không được xác nhận (confirmed push) server không được thông báo khi dữ liệu push được nhận.

Phần lớn các chức năng được cung cấp bởi dịch vụ phiên hướng kết nối (connection – oriented session service) đều được xác nhận: client gửi các thông điệp yêu cầu (Request primitive) và nhận lại thông điệp xác nhận (confirm prtimitive), server gửi các thông điệp phản hồi (Response primitive) và nhận lại thông điệp chi dẫn (Indication primitive).

c.1.2. Dịch vụ phiên phi kết nối (Connectionless session service).

Chỉ cung cấp các dịch vụ không được xác nhận (non – confirmed servicess). Trong trường hợp này các client có thể chỉ sử dụng thông điệp yêu cầu (Request primitive) và các server cũng chỉ có thể dùng thông điệp chỉ dẫn (Indication primitive).

Để bắt đầu một phiên làm việc mới, client yêu cầu một WSP primitive cung cấp một số tham số như địa chỉ server, địa chỉ client và các client header. Các tham số này có thể được liên kết với các tiêu đề HTTP của client và có thể được server dùng để nhận ra loại tác vụ người dùng bên trong WAP client (có thể là phiên bản và loại của trình duyệt). Điều này có ích khi ta muốn định dạng lại phần đầu ra khác đi, tuỳ thuộc vào loại thiết bị ở phía client.

Chẳng hạn như một điện thoại có thể có một màn hình hiển thị chứa được 20 ký tự; nhưng thiết bị khác thì lại chỉ hiển thị được 16 ký tự.

WSP về cơ bản đó chính là một dạng nhị phân của HTTP. WSP cung cấp tất cả các phương thức được định nghĩa bởi HTTP/1.1 và cho phép đàm phán nhằm đạt được sự tương thích với chuẩn HTTP/1.1 này.

c.2. Wireless Transaction Layer – WTP.

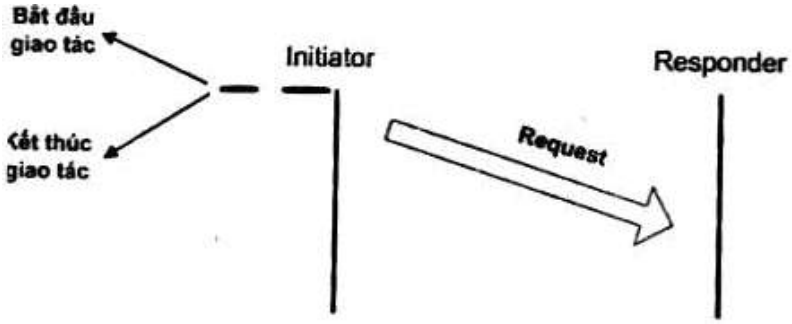
Wireless Transaction Protocol cung cấp các dịch vụ nhằm thực hiện các giao tác tin cậy và không tin cậy, nó làm việc trên tầng WDP hay tầng an ninh WTLS. Cũng như tất cả các tầng khác trong WAP, WTP được tối ưu cho phù hợp với băng thông nhỏ của giao tiếp trên sóng vô tuyến, cố gắng giảm số lượng các giao tác thực hiện lại giữa client và server.

Cụ thể, có ba lớp khác nhau của các dịch vụ giao tác cung cấp cho các tầng bên trên là:

- Các yêu cầu không tin cậy – Unreliable requests
- Các yêu cầu có thể tin cậy – Reliable requests
- Các yêu cầu tin cậy với một thông điệp kết quả.

c.2.1. Yêu cầu không tin cậy - Unreliable requests.

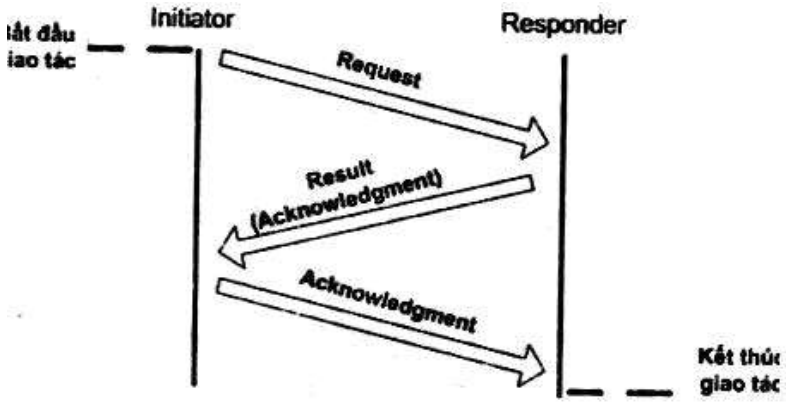
Trình khởi đầu (Inititor) (trong trường hợp này là một server chứa nội dung – content server) gửi yêu cầu đến trình đáp ứng (Responder) (tác nhân người dùng) và không có một thông điệp xác nhận nào được gửi trả về. Giao tác này không có trạng thái và kết thúc ngay thông điệp yêu cầu được gửi đi.



Hình 1.12. Yêu cầu không tin cậy

c.2.2. Yêu cầu có thể tin cậy - Reliable requests.

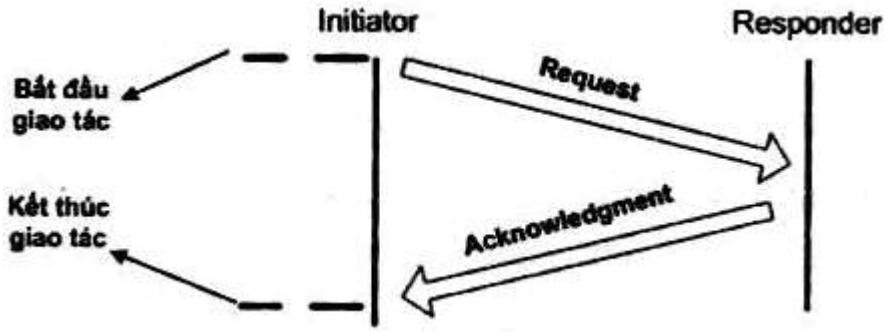
Trình khởi đầu gửi một yêu cầu đến cho trình đáp ứng, trình này sẽ trả lời lại khi nhận được yêu cầu. Trình đáp ứng lưu trữ thông tin trạng thái của giao tác trong một thời gian để nó có thể gửi lại thông điệp xác nhận (acknowledgement message) nếu như server có yêu cầu lại lần nữa. Giao tác kết thúc tại trình khởi đầu khi trình này nhận được thông điệp xác nhận:



Hình 1.13. Yêu cầu tin cậy

c.2.3. Yêu cầu tin cậy và một thông điệp kết quả.

Trình khởi đầu gửi yêu cầu đến cho trình đáp ứng, khi nhận được yêu cầu trình này sẽ gửi trả lại một thông điệp kết quả. Trình khởi đầu nhận thông điệp này, duy trì thông tin trạng thái của giao tác trong một thời gian sau khi xác nhận được gửi đi, phòng trường hợp thông báo gửi đi không đến được đích. Giao tác kết thúc tại trình đáp ứng khi nó nhận được thông điệp xác nhận.



Hình 1.14. Yêu cầu tin cậy với thông điệp kết quả

c.3. Wireless Transprot Layer Security – WTL

WTLS được cung cấp bởi WAP Forum, đây là một giải pháp cho vấn đề bảo mật trên WAP. WTLS là một tầng lớp chọn hoạt động trên tầng vận chuyển (WDP) và được xây dựng dựa trên hai giao thức Internet đó là TLS (Transport Layer Security) v1.0, tầng này cũng dựa trên một tầng khác đó là SSL (Secure Sockets Layer) v3.0.

WTLS cũng có các đặc điểm cơ bản như tất cả các tầng trước đây trong ngăn xếp WAP: nó là điều chỉnh của một giao thức Internet cho phù hợp với điều kiện độ trễ cao, băng thông thấp, cùng với bộ nhớ và khả năng xử lý giới hạn của các thiết bị WAP. WTLS cũng cố gắng giảm bớt chi phí liên quan đến việc thiết lập một kết nối an toàn giữa hai ứng dụng. WTLS cung cấp cùng một mức độ bảo mật như ở SSL 3.0 nhưng giảm đi khoảng thời gian giao tác. Các dịch vụ mà nó cung cấp là:

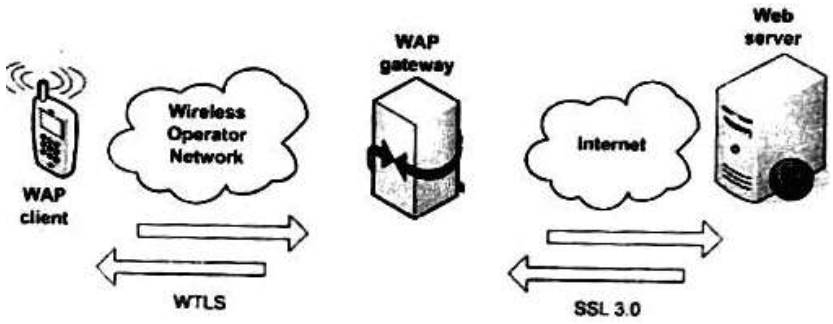
- Tính bảo mật (Privacy) bảo đảm dữ liệu gửi đi giữa server và client không thể được truy cập từ bất kỳ người nào khác. Không ai có thể giải mã thông điệp cho họ có thể nhìn thấy các thông điệp này ở dạng đã được mã hoá.

- Định danh server đảm bảo một server thật sự.

- Định danh client giúp server gốc giới hạn khả năng truy cập đến những nội dung mà nó cung cấp. Xác định chỉ một số client nào đó mới có thể truy cập vào những trang nào đó cho phép mà thôi.

- Bảo toàn dữ liệu sẽ đảm bảo nội dung dữ liệu trên đường truyền giữa server và client sẽ không bị chỉnh sửa mà không được thông báo.

Hình dưới đây mô tả cách WAP gateway điều khiển các phiên làm việc an toàn. Một phiên SSL chuẩn được mở ra giữa web server và WAP gateway và một phiên WTLS được khởi tạo giữa gateway và thiết bị di động. Nội dung mã hoá được gửi đi thông qua nối kết này từ server đến gateway, gateway biên dịch và gửi nó đến cho điện thoại di động.



Hình 1.15. Mô hình làm việc của Wap gateway

Sau đó WTLS giao quyền lại cho giao thức SSL làm việc trên Internet. Việc chuyển đổi giữa SSL và WTLS thực hiện bên trong bộ nhớ của WAP gateway . Điều quan trọng là các thông tin không được mã hoá sẽ không được lưu trữ bên trong gateway, vì như thế sẽ làm mất tác dụng tất cả các phương pháp bảo mật được dùng để bảo vệ dữ liệu lưu trữ với những người không được định danh.

Mặc dù các WAP gateway được cung cấp nhiều chức năng để bảo đảm ở cấp an toàn cao nhất, thế nhưng vẫn cón nhiều vấn đề liên quan đến giải pháp an toàn cho WAP.

WTLS là một tầng tuỳ chọn trong ngăn xếp WAP. Điều này có nghĩa là cơ chế bảo mật trong WAP chỉ có giá trị khi được yêu cầu và không được xây dựng như là một chức năng trong kiến trúc WAP. Do đó, thông tin lưu chuyển đến và đi qua WAP gateway thường không được mã hoá, trừ phi chúng ta dùng các kết nối SSL để giao tiếp giữa các server gốc và gateway.

c.4. Wireless Datagram Protocol – WDP

WDP là lớp dưới cùng trong ngăn xếp WAP và là một trong những phần tử làm cho WAP trở thành một giao thức cực kỳ di động, có thể thực thi trên nhiều loại mạng di động khác nhau. WDP che chở các tầng bên trên nhờ vào các dịch vụ nền mà mạng cung cấp. Các dịch vụ nền bao gồm: SMS, CSD, DECT và CDMA.

1.4.2. Kiến trúc cơ bản của mạng WPAN không dây

Kể từ khi Bluetooth được triển khai, đã có rất nhiều lời bàn luận về các mạng vùng cá nhân không dây. Hầu hết các mối quan tâm đối với mạng PAN đều liên quan đến việc sử dụng nó trong các điện thoại di động thông minh, chẳng hạn như để đồng bộ hoá với phần mềm máy tính hoặc để sử dụng các tai nghe không dây. Nó cũng bắt đầu được sử dụng cho các thiết bị như các tai nghe có gắn micro không dây, với việc truyền âm thanh số cung cấp âm thanh rõ nét. Việc triển khai công nghệ Bluetooth hiện nay có xu hướng sử dụng nó như một sự thay thế cáp ngoại vi cho một số lượng hạn chế các thiết bị hơn là một công cụ nhằm cho phép một số lượng lớn các thiết bị trong nhà hoặc văn phòng có thể giao tiếp trực tiếp.

Những viễn cảnh dài hạn thì lớn hơn nhiều. Nhiều thiết bị gia đình có thể hưởng lợi từ kết nối không dây. Chúng ta nói đến các bàn điều khiển trò chơi vốn có thể trò chuyện vô tuyến với các router, các hộp truyền tín hiệu số vốn có thể truyền

tín hiệu TV số tới máy tính hoặc tới nhiều màn hình trong nhà, các máy chủ đường truyền vốn có thể phát quảng bá vô tuyến âm nhạc tới các bộ tai nghe tuỳ ý nằm trong phạm vi truyền, các máy ảnh vốn có thể giao tiếp trực tiếp với các máy in và các đầu in, các đầu chơi MP3 cầm tay vốn có thể gửi tệp âm nhạc tới hệ thống âm thanh tại nhà. Đây là các loại ứng dụng liên thông mà những người tiêu dùng hàng điện tử "mơ". Nhưng Bluetooth không đủ nhanh cho các ứng dụng video và chắc chắn là không bao giờ. Bluetooth hiện nay chỉ có khả năng truyền với tốc độ 1 đến 2 Mbits/s trong một phạm vi khoảng 10m với một công suất ở đầu ra khoảng 100mW. Như vậy là quá tốt cho âm thanh và cho máy in, các thiết bị nhập như TV số đòi hỏi một tốc độ tối thiểu 7Mbits/s. Nếu muốn truyền tín hiệu TV độ phân giải cao, phải cần một hệ thống có khả năng xử lý 20 – 24 Mbits/s. Công nghệ xuất sắc hiện nay cho các mạng vùng cá nhân là UWB, còn được biết đến với cái tên 802.15.3a (một chuẩn IEEE khác). Đây được coi là công nghệ PAN mà tất cả các công nghệ PAN khác phải chịu khuất phục. Lý do chúng được quan tâm đến vậy là vì UWB có rất nhiều tiềm năng. UWB truyền những đoạn dữ liệu cực ngắn, ít hơn một nanô giây qua một dải phổ rộng.

Trong những khoảng cách rất ngắn, công nghệ UWB có khả năng truyền dữ liệu với vận tốc lên tới 1Gbits/s với một nguồn công suất thấp (khoảng 1mW). Với dải phổ rộng của nó, UWB ít có khả năng bị ảnh hưởng bởi suy luận méo hơn các công nghệ không dây và bởi vì công suất truyền thấp như vậy, nó gây ra rất ít nhiễu trong các thiết bị khác. Phạm vi dự tính của nó chỉ khoảng 10m và vì các vấn đề về chuẩn của nó, người ta dự tính rằng công nghệ UWB sẽ có một vị trí trong cả phiên bản không dây của USB và trong sự lặp lại tiếp theo của công nghệ không dây. Dự báo của Intel (06/ 2006) và những người ủng hộ UWB khác là UWB sẽ hoạt động như một loại lớp vận chuyển đa năng cho các ứng dụng không dây phạm vi ngắn. Trong dự báo này, một phiên bản tương lai của Bluetooth sử dụng UWB như một lớp kiểm soát truy nhập đường truyền và vận chuyển của nó, cũng giống như sử dụng USB không dây. Các giao thức cấp cao hơn đảm trách việc triển khai cụ thể ứng dụng. UWB được xem là một thành phần cốt lõi của thế giới được kết nối

không dây, được điều khiển bởi các chuẩn mở vốn cho phép tất cả các thiết bị giao tiếp với nhau. Ở phạm vi ngắn công nghệ UWB có thể được sử dụng trong WPAN với những vai trò:

- Thay cáp IEEE1394 nối giữa thiết bị điện tử đa phương tiện dân dụng như máy quay phim, máy chụp hình số, thiết bị phát MP3.

- Thiết lập tuyến bus chung không dây tốc độ cao nối giữa PC với thiết bị ngoại vi, gồm máy in, máy quét và thiết bị lưu trữ gắn ngoài.

- Thay cáp và Bluetooth trong các thiết bị thế hệ mới, như điện thoại di động 3G, kết nối IP/ UPnP cho thế hệ thiết bị di động/ điện tử dân dụng/ máy tính dùng IP.

- Tạo kết nối không dây tốc độ cao cho thiết bị điện tử dân dụng, máy tính và điện thoại di động.

1.4.3. Kiến trúc cơ bản của mạng WMAN không dây

WMAN hay còn gọi là WiMAX. WiMAX là từ viết tắt của Worldwide Interoperability for Microwave Access có nghĩa là khả năng tương tác toàn cầu với truy nhập vi ba. Công nghệ WiMAX hay còn gọi là chuẩn 802.16 là công nghệ không dây băng thông rộng đang phát triển rất nhanh với khả năng triển khai trên phạm vi rộng và được gọi là có tiềm năng to lớn để trở thành giải pháp " dặm cuối" lý tưởng nhằm mang lại khả năng kết nối Internet tốc độ cao tới các gia đình và công sở.

Trong khi công nghệ quen thuộc Wi- Fi(802.11 a, b, g) mang lại khả năng kết nối tới các khu vực nhỏ như trong văn phòng hay các điểm truy cập công cộng hotspot, công nghệ WiMAX có khả năng phủ sóng rộng hơn, bao phủ cả một khu vực thành thị hay một khu vực nông thôn nhất định. Công nghệ này có thể cung cấp với tốc độ truyền dữ liệu đến 75 Mbps tại mỗi trạm phát sóng với tầm phủ sóng từ 2 đến 10km. Với băng thông như vậy, công nghệ này có đủ khả năng để hỗ trợ cùng lúc (thông qua một trạm phát sóng đơn lẻ) khả năng kết nối của hơn 60 doanh

nghiệp với tốc độ kết nối của đường T1/E1 và hàng trăm gia đình với tốc độ kết nối DSL.

1.4.3.1. Đặc điểm nổi bật của WiMAX di động

WiMAX di động cũng có những đặc điểm giống EV- DO hoặc HSxPA nhằm tăng tốc độ truyền thông (data rate). Những đặc điểm đó bao gồm: Mã hoá và điều chế thích nghi (Adaptive Modulation and Coding - AMC), kỹ thuật sửa lỗi bằng dò – lặp (Hybrid Automatic Repeat Request – HARQ), phân bố nhanh (Fast Scheduling) và chuyển giao mạng (handover) nhanh và hiệu quả.

Không giống như công nghệ 3G dựa trên CDMA được xây dựng nhằm vào dịch vụ thoại, WiMAX được thiết kế để đáp ứng dịch vụ truyền dữ liệu dung lượng lớn (trong đó có cả dịch vụ thoại VoIP), WiMAX được sử dụng kỹ thuật trái phổ SOFDMA và hạ tầng mạng xây dựng trên nền IP.

WiMAX cung cấp khả năng kết nối Internet không dây nhanh hơn so với WiFi, tốc độ uplink và downlink cao hơn, sử dụng được nhiều ứng dụng hơn và quan trọng là vùng phủ sóng rộng hơn và không bị ảnh hưởng bởi địa hình. WiMAX có thể thay đổi một cách tự động phương thức điều chế để có thể tăng vùng phủ bằng cách giảm tốc độ truyền và ngược lại. Để tăng vùng phủ, chuẩn WiMAX hoặc sử dụng mạng Mesh hoặc sử dụng antenna thông minh hoặc MIMO. Dự liệu truyền trong mạng WiMAX được phân chia thành 5 lớp dịch vụ với những ưu tiên khác nhau nhằm cung ứng QoS. ngoài ra bảo mật cũng là một đặc điểm vượt trội của WiMAX với WIFI.

1.4.3.2. Mô hình ứng dụng WiMAX.

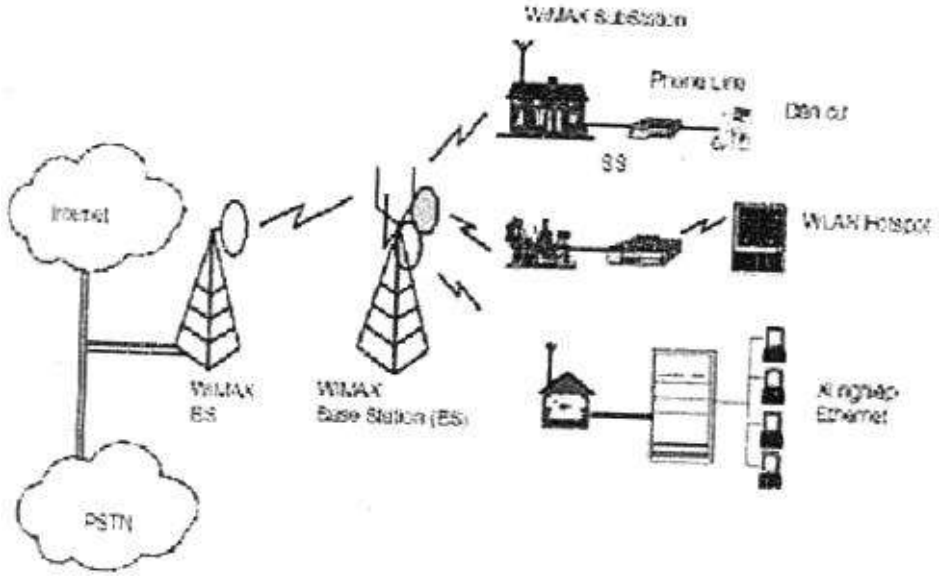
Tiêu chuẩn IEEE 802.16 đề xuất 2 mô hình ứng dụng.

- Mô hình ứng dụng cố định.
- Mô hình ứng dụng di động.

a. Mô hình ứng dụng cố định (Fixed WiMAX)

Mô hình cố định sử dụng các thiết bị theo tiêu chuẩn IEEE.802.16 – 2004. Tiêu chuẩn này gọi là "không dây cố định" vì thiết bị thông tin làm việc với các

anten đặt cố định tại nhà các thuê bao. Anten đặt trên nóc nhà hoặc trên cột tháp tương tự như chảo thông tin vệ tinh.



Hình 1.16. Mô hình ứng dụng Wimax

Tiêu chuẩn IEEE 802.16 – 2004 cũng cho phép đặt anten trong nhà nhưng tất nhiên tín hiệu thu không khỏe bằng anten ngoài trời. Băng tần công tác (theo quy định và phân bố của quốc gia) trong băng 2,5 GHz hoặc 3,5 GHz. Độ rộng băng tầng là 3,5 MHz. Trong mạng cố định, WiMAX thực hiện cách tiếp nói không dây đến các modem cáp, đến các đôi dây thuê bao của mạch xDSL hoặc mạng Tx/Ex (truyền phát/chuyển mạch) và mạch OC – x (truyền tải qua sóng mạch). WiMAX cố định có thể chuyển phục vụ cho các loại người dùng (user) như: các xí nghiệp, các khu dân cư nhỏ lẻ, mạng cáp truy nhập WLAN công cộng nối tới mạng đô thị, các trạm gốc BS của mạng thông tin di động và các mạch điều khiển trạm BS. Về cách phân bố theo địa lý, các user có thể phân tán tại các địa phương như nông thôn và các vùng sâu vùng xa khó đưa mạng cáp hữu tuyến đến đó.

Sơ đồ kết cấu mạng WiMAX được đưa ra trên Hình 1.18. Trong mô hình này bộ phận vô tuyến gồm các trạm gốc WiMAX BS (làm việc với anten đặt trên tháp cao) và các trạm phụ SS (SubStation). Các trạm WiMAX BS nối với mạng đô thị MAN hoặc mạng PSTN.

b. Mô hình ứng dụng WiMAX di động.

Mô hình WiMAX di động sử dụng các thiết bị phù hợp với tiêu chuẩn IEEE 802.16e. Tiêu chuẩn 802.16e bổ sung cho tiêu chuẩn 802.16 -2004 hướng tới các user cá nhân di động, làm việc trong băng tần thấp hơn 6GHz. Mạng lưới này phối hợp cùng MLAN, mạng di động cellular 3G có thể tạo thành mạng di động có vùng phủ sóng rộng. Hy vọng các nhà cung cấp viễn thông digital truy nhập không dây có phạm vi phủ sóng rộng thoả mãn được các nhu cầu đa dạng của thuê bao. Tiêu chuẩn IEEE 802.16e được thông qua trong năm 2005.

1.4.4. Mạng không dây WRAN

Mạng vô tuyến khu vực. Nhóm này đại diện là công nghệ 802.22 đang được nghiên cứu và phát triển bởi IEEE. Vùng phủ có nó sẽ lên tầm 40- 100km. Mục đích là mang công nghệ truyền thông đến các vùng xa xôi hẻo lánh, khó triển khai các công nghệ khác. Nó sẽ sử dụng băng tần mà TV analog không dùng để đạt được vùng phủ rộng.

1.5. Tổng kết

Nội dung chương này đã trình bày các kiến thức tổng quan về công nghệ mạng Internet và đặc biệt là giới thiệu về công nghệ mạng Internet không dây, kiến trúc cơ bản của: mạng LAN không dây (chuẩn 802.11), của mạng WAN không dây và của Internet không dây (chuẩn WAP và các chuẩn mới). Tính đến nay, sau hơn 10 năm kể từ khi ra đời, việc áp dụng công nghệ mạng Internet không dây rộng rãi trong nhiều lĩnh vực đã chứng tỏ được tính ưu việt và hiệu quả của nó so với công nghệ mạng Internet có dây truyền thống.

Cũng giống như mọi công nghệ mạng Internet khác, vấn đề an ninh trong mạng Internet không dây cũng được đặt ra và đặc biệt trong hoàn cảnh được sử dụng rộng rãi như hiện nay thì vấn đề an ninh cho mạng Internet không dây trở nên là một vấn đề nóng hổi, cấp thiết trong lĩnh vực điện toán và công nghệ mạng. Do

đó, nội dung chương tiếp theo sẽ đi giới thiệu, nghiên cứu các kỹ thuật tấn công mạng Internet không dây để từ đó đưa ra những giải pháp an ninh cho mạng Internet không dây, nghiên cứu chi tiết phương pháp bảo mật và đảm bảo toàn vẹn dữ liệu bên trong các giải pháp đó.

CHƯƠNG 2. TỔNG QUAN VỀ AN NINH MẠNG INTERNET KHÔNG DÂY

2.1. Một số kỹ thuật tấn công Internet không dây.

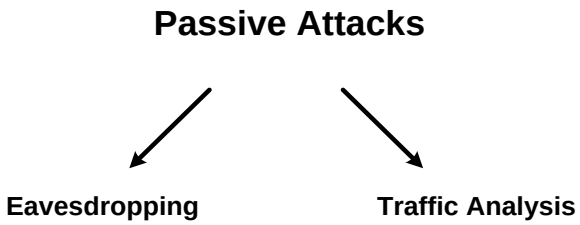
Mạng máy tính Internet không dây cũng mang những đặc trưng cơ bản của một mạng máy tính Internet vì thế việc tấn công và các biện pháp đối phó cũng dựa theo các nguyên lý trình bầy ở các chương trước. Ngoài ra từ những đặc thù riêng của mạng Internet không dây về không gian truyền sóng nên nó chịu những kiểu tấn công khác và có những biện pháp đối phó khác. Có nhiều cách phân loại an ninh mạng Internet, chương này sẽ phân tích dựa vào phân loại theo tính chất tấn công.

2.1.1. Tấn công bị động – Passive attacks

2.1.1.1. Định nghĩa

Tấn công bị động là kiểu tấn công không tác động trực tiếp vào thiết bị nào trên mạng, không làm cho các thiết bị trên mạng biết được hoạt động của nó, vì thế kiểu tấn công này nguy hiểm ở chỗ nó rất khó phát hiện. Ví dụ như việc lấy trộm thông tin trong không gian truyền sóng của các thiết bị sẽ rất khó bị phát hiện dù thiết bị lấy trộm đó nằm trong vùng phủ sóng của mạng chứ chưa nói đến việc nó được đặt ở khoảng cách xa và sử dụng anten được định hướng tới nơi phát sóng, khi đó cho phép kẻ tấn công giữ được khoảng cách thuận lợi mà không để bị phát hiện.

Các phương thức thường dùng trong tấn công bị động: nghe trộm (Sniffing, Eavesdropping), phân tích luồng thông tin (Traffic analyst).



Hình 2.1. Các phương thức dùng trong tấn công bị động

2.1.1.2. Kiểu tấn công bị động cụ thể - Phương thức bắt gói tin (Sniffing)

a. Nguyên lý thực hiện

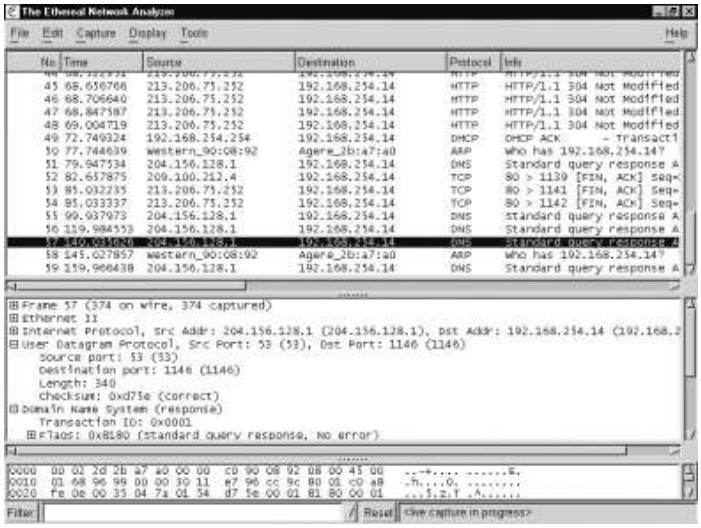
Bắt gói tin – Sniffing là khái niệm cụ thể của khái niệm tổng quát "Nghe trộm – Eavesdropping" sử dụng trong mạng máy tính. Có lẽ là phương pháp đơn giản nhất, tuy nhiên nó vẫn có hiệu quả đối với việc tấn công WLAN. Bắt gói tin có thể hiểu như là một phương thức lấy trộm thông tin khi đặt một thiết bị thu nằm trong hoặc nằm gần vùng phủ sóng. Tấn công kiểu bắt gói tin sẽ khó bị phát hiện ra sự có mặt của thiết bị bắt gói dù thiết bị đó nằm trong hoặc nằm gần vùng phủ sóng nếu thiết bị không thực sự kết nối tới AP để thu các gói tin.

Việc bắt gói tin ở mạng có dây thường được thực hiện dựa trên các thiết bị phần cứng mạng, ví dụ như việc sử dụng phần mềm bắt gói tin trên phần điều khiển thông tin ra vào của một card mạng trên máy tính, có nghĩa là cũng phải biết loại thiết bị phần cứng sử dụng, phải tìm cách cài đặt phần mềm bắt gói lên đó, vv.. tức là không đơn giản. Đối với mạng không dây, nguyên lý trên vẫn đúng nhưng không nhất thiết phải sử dụng vì có nhiều cách lấy thông tin đơn giản, dễ dàng hơn nhiều. Bởi vì đối với mạng không dây, thông tin được phát trên môi trường truyền sóng và ai cũng có thể thu được.

Những chương trình bắt gói tin có khả năng lấy các thông tin quan trọng, mật khẩu, .. từ các quá trình trao đổi thông tin trên máy bạn với các site HTTP, email, các instant messenger, các phiên FTP, các phiên telnet nếu những thông tin trao đổi

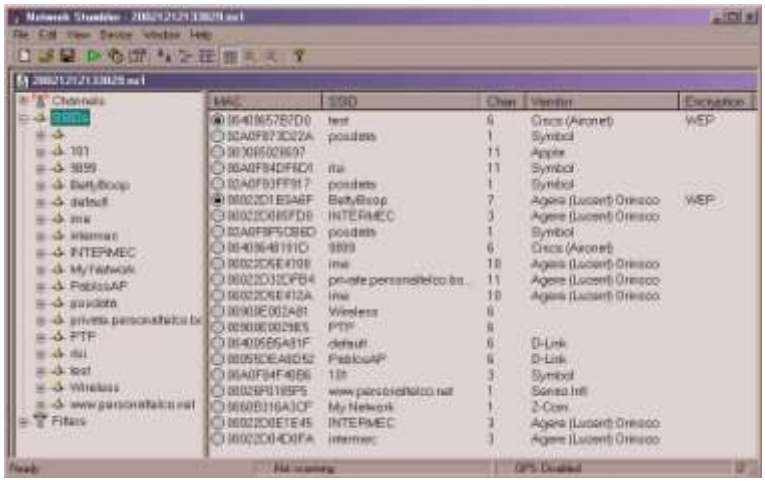
đó dưới dạng văn bản không mã hóa (clear text). Có những chương trình có thể lấy được mật khẩu trên mạng không dây của quá trình trao đổi giữa Client và Server khi đang thực hiện quá trình nhập mật khẩu để đăng nhập. Cũng từ việc bắt gói tin, có thể nắm được thông tin, phân tích được lưu lượng của mạng (Traffic analysis), phổ năng lượng trong không gian của các vùng. Từ đó mà kẻ tấn công có thể biết chỗ nào sóng truyền tốt, chỗ nào kém, chỗ nào tập trung nhiều máy.

Như bắt gói tin ngoài việc trực tiếp giúp cho quá trình phá hoại, nó còn gián tiếp là tiền đề cho các phương thức phá hoại khác. Bắt gói tin là cơ sở của các phương thức tấn công như ăn trộm thông tin, thu thập thông tin phân bố mạng (wardriving), dò mã, bẻ mã (Key crack), vv ..



Hình 2.2. Phần mềm bắt gói tin Ethereal

***Wardriving*:** là một thuật ngữ để chỉ thu thập thông tin về tình hình phân bố các thiết bị, vùng phủ sóng, cấu hình của mạng không dây. Với ý tưởng ban đầu dùng một thiết bị dò sóng, bắt gói tin, kẻ tấn công ngồi trên xe ô tô và đi khắp các nơi để thu thập thông tin, chính vì thế mà có tên là wardriving. Ngày nay những kẻ tấn công còn có thể sử dụng các thiết bị hiện đại như bộ thu phát vệ tinh GPS để xây dựng thành một bản đồ thông tin trên một phạm vi lớn.



Hình 2.3. Phần mềm thu thập thông tin hệ thống mạng không dây NetStumbler

b. Biện pháp đối phó

Vì "bắt gói tin" là phương thức tấn công kiểu bị động nên rất khó phát hiện và do đặc điểm truyền sóng trong không gian nên không thể phòng ngừa việc nghe trộm của kẻ tấn công. Giải pháp đề ra ở đây là nâng cao khả năng mã hóa thông tin sao cho kẻ tấn công không thể giải mã được, khi đó thông tin lấy được sẽ thành vô giá trị đối với kẻ tấn công.

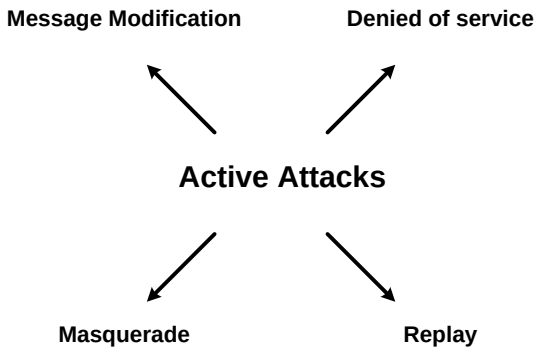
2.1.2. Tấn công chủ động – Active attacks

2.1.2.1. Định nghĩa

Tấn công chủ động là tấn công trực tiếp vào một hoặc nhiều thiết bị trên mạng ví dụ như vào AP, STA. Những kẻ tấn công có thể sử dụng phương pháp tấn công chủ động để thực hiện các chức năng trên mạng. Cuộc tấn công chủ động có thể được dùng để tìm cách truy nhập tới một server để thăm dò, để lấy những dữ liệu quan trọng, thậm chí thực hiện thay đổi cấu hình cơ sở hạ tầng mạng. Kiểu tấn công này dễ phát hiện nhưng khả năng phá hoại của nó rất nhanh và nhiều, khi phát hiện ra chúng ta chưa kịp có phương pháp đối phó thì nó đã thực hiện xong quá trình phá hoại.

So với kiểu tấn công bị động thì tấn công chủ động có nhiều phương thức đa dạng hơn, ví dụ như: Tấn công từ chối dịch vụ (DOS), Sửa đổi thông tin (Message

Modification), Đóng giả, mạo danh, che dấu (Masquerade), Lặp lại thông tin (Replay), Bomb, spam mail, v v...



Hình 2.4. Tấn công chủ động

2.1.2.2. Các kiểu tấn công chủ động cụ thể

a. Mạo danh, truy cập trái phép

a.1. Nguyên lý thực hiện

Việc mạo danh, truy cập trái phép là hành động tấn công của kẻ tấn công đối với bất kỳ một loại hình mạng máy tính nào, và đối với mạng Internet không dây cũng như vậy. Một trong những cách phổ biến là một máy tính tấn công bên ngoài giả mạo là máy bên trong mạng, xin kết nối vào mạng để rồi truy cập trái phép nguồn tài nguyên trên mạng. Việc giả mạo này được thực hiện bằng cách giả mạo địa chỉ MAC, địa chỉ IP của thiết bị mạng trên máy tấn công thành các giá trị của máy đang sử dụng trong mạng, làm cho hệ thống hiểu nhầm và cho phép thực hiện kết nối. Ví dụ việc thay đổi giá trị MAC của card mạng không dây trên máy tính sử dụng hệ điều hành Windows hay UNIX đều hết sức dễ dàng, chỉ cần qua một số thao tác cơ bản của người sử dụng. Các thông tin về địa chỉ MAC, địa chỉ IP cần giả mạo có thể lấy từ việc bắt trộm gói tin trên mạng.

a.2. Biện pháp đối phó

Việc giữ gìn bảo mật máy tính mình đang sử dụng, không cho ai vào dùng trái phép là một nguyên lý rất đơn giản nhưng lại không thừa để ngăn chặn việc mạo danh này. Việc mạo danh có thể xẩy ra còn do quá trình chứng thực giữa các bên còn chưa chặt chẽ, vì vậy cần phải nâng cao khả năng này giữa các bên.

b. Tấn công từ chối dịch vụ - DOS

b.1. Nguyên lý thực hiện

Với mạng máy tính không dây và mạng có dây thì không có khác biệt cơ bản về các kiểu tấn công DOS (Denied of Service) ở các tầng ứng dụng và vận chuyển nhưng giữa các tầng mạng, liên kết dữ liệu và vật lý lại có sự khác biệt lớn. Chính điều này làm tăng độ nguy hiểm của kiểu tấn công DOS trong mạng máy tính không dây. Trước khi thực hiện tấn công DOS, kẻ tấn công có thể sử dụng chương trình phân tích lưu lượng mạng để biết được chỗ nào đang tập trung nhiều lưu lượng, số lượng xử lý nhiều, và kẻ tấn công sẽ tập trung tấn công DOS vào những vị trí đó để nhanh đạt được hiệu quả hơn.

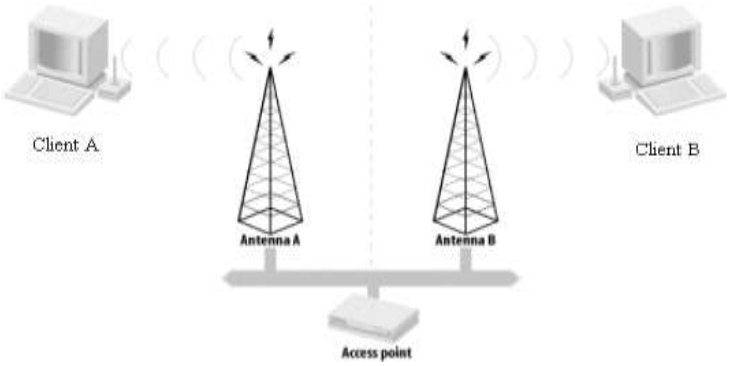
- Tấn công DOS tầng vật lý

Tấn công DOS tầng vật lý ở mạng có dây muốn thực hiện được thì yêu cầu kẻ tấn công phải ở gần các máy tính trong mạng. Điều này lại không đúng trong mạng không dây. Với mạng này, bất kỳ môi trường nào cũng dễ bị tấn công và kẻ tấn công có thể xâm nhập vào tầng vật lý từ một khoảng cách rất xa, có thể là từ bên ngoài thay vì phải đứng bên trong tòa nhà. Trong mạng máy tính có dây khi bị tấn công thì thường để lại các dấu hiệu dễ nhận biết như là cáp bị hỏng, dịch chuyển cáp, hình ảnh được ghi lại từ camera, thì với mạng không dây lại không để lại bất kỳ một dấu hiệu nào. 802.11 PHY đưa ra một phạm vi giới hạn các tần số trong giao tiếp. Một kẻ tấn công có thể tạo ra một thiết bị làm bão hòa dải tần 802.11 với nhiễu. Như vậy, nếu thiết bị đó tạo ra đủ nhiễu tần số vô tuyến thì sẽ làm giảm tín hiệu / tỷ lệ nhiễu tới mức không phân biệt được dẫn đến các STA nằm trong dải tần nhiễu sẽ bị ngừng hoạt động. Các thiết bị sẽ không thể phân biệt được tín hiệu mạng

một cách chính xác từ tất cả các nhiễu xảy ra ngẫu nhiên đang được tạo ra và do đó sẽ không thể giao tiếp được. Tấn công theo kiểu này không phải là sự đe doạ nghiêm trọng, nó khó có thể thực hiện phổ biến do vấn đề giá cả của thiết bị, nó quá đắt trong khi kẻ tấn công chỉ tạm thời vô hiệu hóa được mạng.

- Tấn công DOS tầng liên kết dữ liệu

Do ở tầng liên kết dữ liệu kẻ tấn công cũng có thể truy cập bất kì đâu nên lại một lần nữa tạo ra nhiều cơ hội cho kiểu tấn công DOS. Thậm chí khi WEP đã được bật, kẻ tấn công có thể thực hiện một số cuộc tấn công DOS bằng cách truy cập tới thông tin lớp liên kết. Khi không có WEP, kẻ tấn công truy cập toàn bộ tới các liên kết giữa các STA và AP để chấm dứt truy cập tới mạng. Nếu một AP sử dụng không đúng anten định hướng kẻ tấn công có nhiều khả năng từ chối truy cập từ các client liên kết tới AP. Anten định hướng đôi khi còn được dùng để phủ sóng nhiều khu vực hơn với một AP bằng cách dùng các anten. Nếu anten định hướng không phủ sóng với khoảng cách các vùng là như nhau, kẻ tấn công có thể từ chối dịch vụ tới các trạm liên kết bằng cách lợi dụng sự sắp đặt không đúng này, điều đó có thể được minh họa ở hình dưới đây:



Hình 2.5. Mô tả quá trình tấn công DOS tầng liên kết dữ liệu

Giả thiết anten định hướng A và B được gắn vào AP và chúng được sắp đặt để phủ sóng cả hai bên bức tường một cách độc lập. Client A ở bên trái bức tường, vì vậy AP sẽ chọn anten A cho việc gửi và nhận các khung. Client B ở bên trái bức tường, vì vậy chọn việc gửi và nhận các khung với anten B. Client B có thể loại client A ra khỏi mạng bằng cách thay đổi địa chỉ MAC của Client B giống hệt với

Client A. Khi đó Client B phải chắc chắn rằng tín hiệu phát ra từ anten B mạnh hơn tín hiệu mà Client A nhận được từ anten A bằng việc dùng một bộ khuếch đại hoặc các kĩ thuật khuếch đại khác nhau. Như vậy AP sẽ gửi và nhận các khung ứng với địa chỉ MAC ở anten B. Các khung của Client A sẽ bị từ chối chừng nào mà Client B tiếp tục gửi lưu lượng tới AP.

- Tấn công DOS tầng mạng

Nếu một mạng cho phép bất kì một client nào kết nối, nó dễ bị tấn công DOS tầng mạng. Mạng máy tính không dây chuẩn 802.11 là môi trường chia sẻ tài nguyên. Một người bất hợp pháp có thể xâm nhập vào mạng, từ chối truy cập tới các thiết bị được liên kết với AP. Ví dụ như kẻ tấn công có thể xâm nhập vào mạng 802.11b và gửi đi hàng loạt các gói tin ICMP qua cổng gateway. Trong khi cổng gateway có thể vẫn thông suốt lưu lượng mạng, thì dải tần chung của 802.11b lại dễ dàng bị bão hòa. Các Client khác liên kết với AP này sẽ gửi các gói tin rất khó khăn.

b.2. Biện pháp đối phó

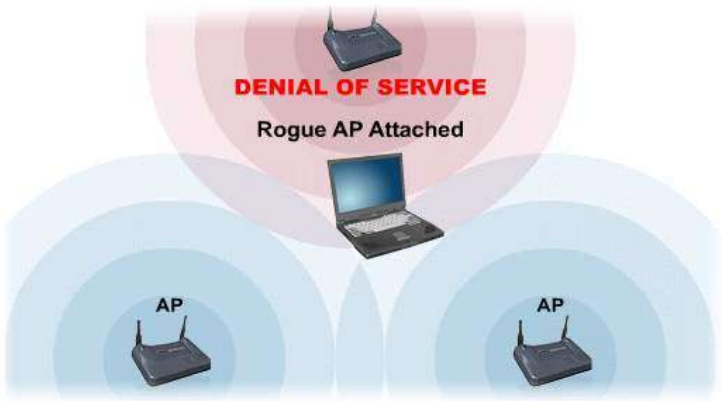
Biện pháp mang tính "cực đoan" hiệu quả nhất là chặn và lọc bỏ đi tất cả các bản tin mà DOS hay sử dụng, như vậy có thể sẽ chặn bỏ luôn cả những bản tin hữu ích. Để giải quyết tốt hơn, cần có những thuật toán thông minh nhận dạng tấn công – attack detection, dựa vào những đặc điểm như gửi bản tin liên tục, bản tin giống hệt nhau, bản tin không có ý nghĩa, vv.. Thuật toán này sẽ phân biệt bản tin có ích với các cuộc tán công, để có biện pháp lọc bỏ.

c. Tấn công cưỡng đoạt điều khiển và sửa đổi thông tin – Hijacking and Modification

c.1. Nguyên lý thực hiện

Có rất nhiều kỹ thuật tấn công cưỡng đoạt điều khiển. Khác với các kiểu tấn công khác, hệ thống mạng rất khó phân biệt đâu là kẻ tấn công cưỡng đoạt điều khiển, đâu là một người sử dụng hợp pháp.

Định nghĩa: Có nhiều các phần mềm để thực hiện Hijack. Khi một gói tin TCP/IP đi qua Switch, Router hay AP, các thiết bị này sẽ xem phần địa chỉ đích đến của gói tin, nếu địa chỉ này nằm trong mạng mà thiết bị quản lý thì gói tin sẽ chuyển trực tiếp đến địa chỉ đích, còn nếu địa chỉ không nằm trong mạng mà thiết bị quản lý thì gói tin sẽ được đưa ra cổng ngoài (default gateway) để tiếp tục chuyển đến thiết bị khác.Nếu kẻ tấn công có thể sửa đổi giá trị default gateway của thiết bị mạng trỏ vào máy tính của hắn, như vậy có nghĩa là các kết nối ra bên ngoài đều đi vào máy của hắn. Và đương nhiên là kẻ tấn công có thể lấy được toàn bộ thông tin đó lựa chọn ra các bản tin yêu cầu, cấp phép chứng thực để giải mã, bẻ khóa mật mã. Ở một mức độ tinh vi hơn, kẻ tấn công chỉ lựa chọn để một số bản tin cần thiết định tuyến đến nó, sau khi lấy được nội dung bản tin, kẻ tấn công có thể sửa đổi lại nội dung theo mục đích riêng sau đó lại tiếp tục chuyển tiếp (forward) bản tin đến đúng địa chỉ đích. Như vậy bản tin đã bị chặn, lấy, sửa đổi trong quá trình truyền mà ở phía gửi lẫn phía nhận không phát hiện ra. Đây cũng giống nguyên lý của kiểu tấn công thu hút (man in the back), tấn công sử dụng AP giả mạo (rogue AP).



Hình 2.6. Mô tả quá trình tấn công mạng bằng AP giả mạo

AP giả mạo - Rogue AP: là một kiểu tấn công bằng cách sử dụng 1 AP đặt trong vùng gần với vùng phủ sóng của mạng WLAN. Các Client khi di chuyển đến gần Rogue AP, theo nguyên lý chuyển giao vùng phủ sóng giữa ô mà các AP quản lý, máy Client sẽ tự động liên kết với AP giả mạo đó và cung cấp các thông tin của mạng WLAN cho AP. Việc sử dụng AP giả mạo, hoạt động ở cùng tần số với các AP khác có thể gây ra nhiễu sóng giống như trong phương thức tấn công chèn ép, nó cũng gây tác hại giống tấn công từ chối dịch vụ - DOS vì khi bị nhiễu sóng, việc trao đổi các gói tin không thành công nhiều và phải truyền đi truyền lại nhiều lần, dẫn đến việc tắc nghẽn, cạn kiệt tài nguyên mạng

c.2. Biện pháp đối phó

Tấn công kiểu Hijack thường có tốc độ nhanh, phạm vi rộng vì vậy cần phải có các biện pháp ngăn chặn kịp thời. Hijack thường thực hiện khi kẻ tấn công đã đột nhập khá "sâu" trong hệ thống, vì thế cần phải ngăn chặn từ những dấu hiệu ban đầu. Với kiểu tấn công AP Rogue, biện pháp ngăn chặn giả mạo là phải có sự chứng thực 2 chiều giữa Client và AP thay cho việc chứng thực một chiều từ Client đến AP.

d. Dò mật khẩu bằng từ điển – Dictionary Attack

d.1. Nguyên lý thực hiện

Việc dò mật khẩu dựa trên nguyên lý quét tất cả các trường hợp có thể sinh ra từ tổ hợp của các ký tự. Nguyên lý này có thể được thực thi cụ thể bằng những phương pháp khác nhau như quét từ trên xuống dưới, từ dưới lên trên, từ số đến chữ, vv... Việc quét thế này tốn nhiều thời gian ngay cả trên những thế hệ máy tính tiên tiến bởi vì số trường hợp tổ hợp ra là cực kỳ nhiều. Thực tế là khi đặt một mật mã (password), nhiều người thường dùng các từ ngữ có ý nghĩa, để đơn lẻ hoặc ghép lại với nhau, ví dụ như "cuocsong", "hanhphuc", "cuocsonghanhphuc", vv.. Trên cơ sở đó một nguyên lý mới được đưa ra là sẽ quét mật khẩu theo các trường hợp theo các từ ngữ trên một bộ từ điển có sẵn, nếu không tìm ra lúc đấy mới quét

tổ hợp các trường hợp. Bộ từ điển này gồm những từ ngữ được sử dụng trong cuộc sống, trong xã hội, vv.. và nó luôn được cập nhật bổ xung để tăng khả năng "thông minh" của bộ phá mã.

d.2. Biện pháp đối phó

Để đối phó với kiểu dò mật khẩu này, cần xây dựng một quy trình đặt mật khẩu phức tạp hơn, đa dạng hơn để tránh những tổ hợp từ, và gây khó khăn cho việc quét tổ hợp các trường hợp. Ví dụ quy trình đặt mật khẩu phải như sau:

- Mật khẩu dài tối thiểu 10 ký tự
- Có cả chữ thường và chữ hoa
- Có cả chữ, số, và có thể là các ký tự đặc biệt như !,@,#,$
- Tránh trùng với tên đăng ký, tên tài khoản, ngày sinh, vv..
- Không nên sử dụng các từ ngữ ngắn đơn giản có trong từ điển

2.1.3. Tấn công kiểu chèn ép - Jamming attacks

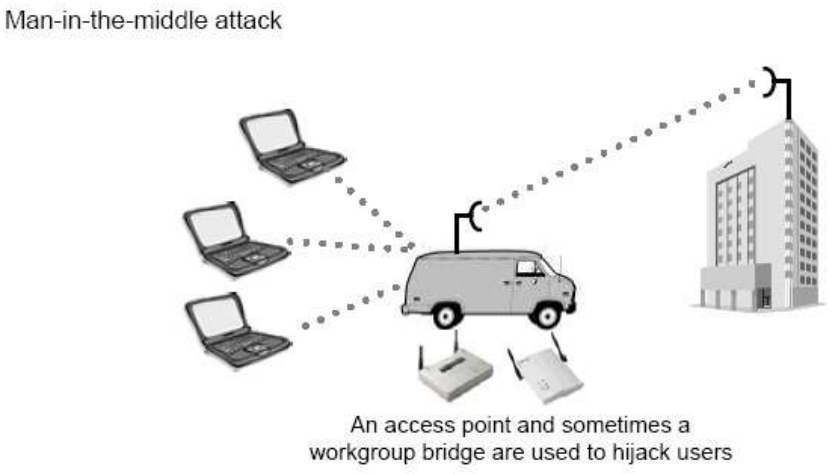
Ngoài việc sử dụng phương pháp tấn công bị động, chủ động để lấy thông tin truy cập tới mạng của bạn, phương pháp tấn công theo kiểu chèn ép. Jamming là một kỹ thuật sử dụng đơn giản để làm mạng của bạn ngừng hoạt động. Phương thức jamming phổ biến nhất là sử dụng máy phát có tần số phát giống tần số mà mạng sử dụng để áp đảo làm mạng bị nhiễu, bị ngừng làm việc. Tín hiệu RF đó có thể di chuyển hoặc cố định.

Hình 2.7. Mô tả quá trình tấn công theo kiểu chèn ép

Cũng có trường hợp sự Jamming xẩy ra do không chủ ý thường xảy ra với mọi thiết bị mà dùng chung dải tần 2,4Ghz. Tấn công bằng Jamming không phải là sự đe dọa nghiêm trọng, nó khó có thể được thực hiện phổ biến do vấn đề giá cả của thiết bị, nó quá đắt trong khi kẻ tấn công chỉ tạm thời vô hiệu hóa được mạng.

2.1.4. Tấn công theo kiểu thu hút - Man in the middle attacks

Tấn công theo kiểu thu hút - Man in the middle attacks có nghĩa là dùng một khả năng mạnh hơn chen vào giữa hoạt động của các thiết bị và thu hút, giành lấy sự trao đổi thông tin của thiết bị về mình. Thiết bị chèn giữa đó phải có vị trí, khả năng thu phát trội hơn các thiết bị sẵn có của mạng. Một đặc điểm nổi bật của kiểu tấn công này là người sử dụng không thể phát hiện ra được cuộc tấn công, và lượng thông tin mà thu nhặt được bằng kiểu tấn công này là giới hạn.



Hình 2.8. Mô tả quá trình tấn công theo kiểu thu hút

Phương thức thường sử dụng theo kiểu tấn công này là Mạo danh AP (AP rogue), có nghĩa là chèn thêm một AP giả mạo vào giữa các kết nối trong mạng.

2.1.5. Tấn công vào các yếu tố con người

Đây là một hình thức tấn công nguy hiểm nhất nó có thể dẫn tới những tổn thất hết sức khó lường. Kẻ tấn công có thể liên lạc với người quản trị hệ thống thay đổi một số thông tin nhằm tạo điều kiện cho các phương thức tấn công khác.

Ngoài ra, điểm mấu chốt của vấn đề an toàn, an ninh trên Internet không dây chính là người sử dụng. Họ là điểm yếu nhất trong toàn bộ hệ thống do kỹ năng, trình độ sử dụng máy tính, mạng internet không dây không cao. Chính họ đã tạo điều kiện cho những kẻ phá hoại xâm nhập được vào hệ thống thông qua nhiều hình thức khác nhau như qua email: Kẻ tấn công gửi những chương trình, virus và những tài liệu có nội dung không hữu ích hoặc sử dụng những chương trình không rõ nguồn gốc, thiếu độ an toàn. Thông thường những thông tin này được che phủ bởi những cái tên hết sức ấn tượng mà không ai có thể biết được bên trong nó chứa đựng cái gì. Và điều tồi tệ nhất sẽ xảy ra khi người sử dụng mở hay chạy nó. Lúc đó có thể thông tin về người sử dụng đã bị tiết lộ hoặc có cái gì đó đã hoạt động tiềm ẩn trên hệ thống của bạn và chờ ngày kích hoạt mà chúng ta không hề ngờ tới.

Với kiểu tấn công như vậy sẽ không có bất cứ một thiết bị nào có thể ngăn chặn một cách hữu hiệu chỉ có phương pháp duy nhất là giáo dục người sử dụng mạng Internet không dây về những yêu cầu bảo mật để nâng cao cảnh giác. Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào và chỉ có sự giáo dục cùng với tinh thần hợp tác từ phía người sử dụng mới có thể nâng cao độ an toàn của hệ thống bảo vệ.

2.1.6. Một số kiểu tấn công khác

Ngoài các hình thức tấn công kể trên, các hacker còn sử dụng một số kiểu tấn công khác như tạo ra các virus đặt nằm tiềm ẩn trên các file khi người sử dụng do vô tình trao đổi thông tin qua mạng Internet không dây mà người sử dụng đã tự cài đặt nó lên trên máy của mình. Ngoài ra hiện nay còn rất nhiều kiểu tấn công khác mà chúng ta còn chưa biết tới và chúng được đưa ra bởi những hacker.

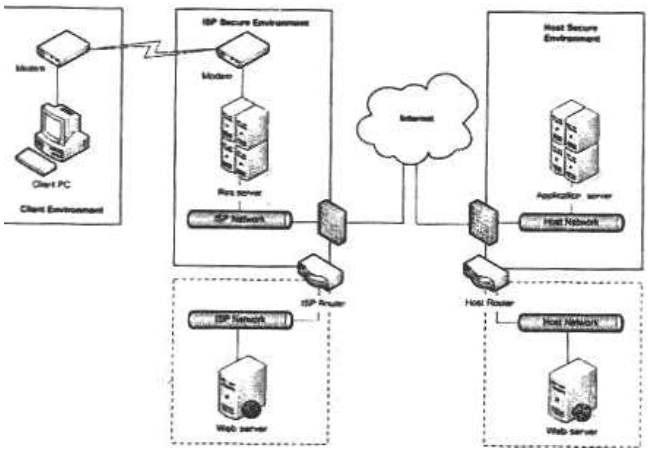
2.2. Giải pháp an ninh cho mạng Internet không dây (WAP).

2.2.1. Vấn đề bảo mật trên WAP.

Bảo mật luôn là vấn đề được rất nhiều người quan tâm. Ta đi vào so sánh vấn đề bảo mật trong môi trường WAP với một môi trường khá quen thuộc đó là Internet.

2.2.1.1. So sánh các mô hình bảo mật.

a. Bảo mật trên Internet.



Hình 2.9. Mô hình bảo mật trên Internet

Trong hình trên, giả sử thiết bị ở phía client là một PC được kết nối với Internet thông qua một ISP dùng modem và giao thức PPP (point – to – point protocol).

Người dùng được ISP định danh trước khi cho phép sử dụng mạng do mình cung cấp. Các giao thức định danh này thực hiện bằng cách sử dụng tên và mật khẩu mà người dùng cung cấp.

Khi việc định danh hoàn tất, thiết bị ở phía client được cung cấp một địa chỉ IP và đăng ký địa chỉ này với ISP. Tiếp theo, RAS server sẽ đóng vai trò như là một proxy đối với thiết bị client, thực hiện gửi đi các gói IP nhận được từ client và thu thập các gói tin gửi thẳng đến server và chuyển tiếp chúng thông qua nối kết PPP.

Mạng của ISP sẽ kết nối với mạng trục Internet (Internet backbne) thông qua một router hoặc là một gateway. Đồng thời với sự có mặt của bức tường lửa (firewall), nó sẽ bảo vệ mạng của ISP với những lưu chuyển bên ngoài mạng Internet (bức tường lửa có thể nằm độc lập hoặc tính hợp ngay vào trong router).

Khi ra được bên ngoài Internet, dữ liệu sẽ đi qua nhiều mạng chuyển mạch (circuit – switched) và chuyển gói (packet – switched) lưu chuyển từ router này qua router khác trước khi đi đến đích.

Phương thức bảo mật phổ biến nhất được dùng để bảo vệ đó là giao thức TLS (Transport Layer Security) trước đây là SSL (Secure Sockets Layer). Đây là một giao thức ở tầng vận chuyển.

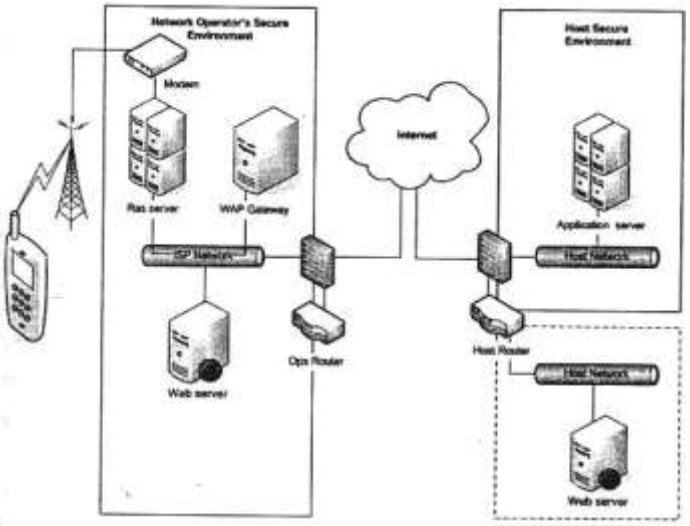
Khi client yêu cầu một phiên làm việc an toàn với server, các tham số của phiên sẽ được trao đổi giữa client và server trước khi phiên làm việc an toàn được thiết lập giữa chúng. Tất cả các giao tiếp giữa client và server đều được mã hoá bằng các thuật toán và khoá được trao đổi như là một phần của việc thiết lập phiên làm việc. Mặc dù kẻ nghe trộm có thể sẽ chặn được các gói tin thiết lập phiên, nhưng với sự có mặt của khoá đủ để đảm bảo rằng phiên làm việc không bị ảnh hưởng. Điều này đạt được là do các khóa phiên được hình thành nhờ vào sự phối hợp của các khoá chung và riêng (public key, private key) lại với nhau. Như vậy, để có được khóa của phiên giao dịch, kẻ nghe trộm phải sở hữu một trong số các khoá riêng này.

TLS cung cấp các giao tiếp an toàn dạng end – to – end giữa client và server.

Với hướng giao tiếp này, tất cả dữ liệu được mã hóa và không thể được giải mã bởi bất kỳ trạm trung gian nào giữa client và server.

b. Bảo mật trên WAP.

Cũng giống như Internet bảo mật được thực hiện ngay trên Tầng Vận chuyển: Mô hình trên mạng Internet thực thi phần lớn các chức năng bảo mật của mình trong TLS, còn WAP thì thực hiện phần lớn trong WTLS (WTLS dựa trên nền của TLS).



Hình 2.10. Mô hình bảo mật trên WAP

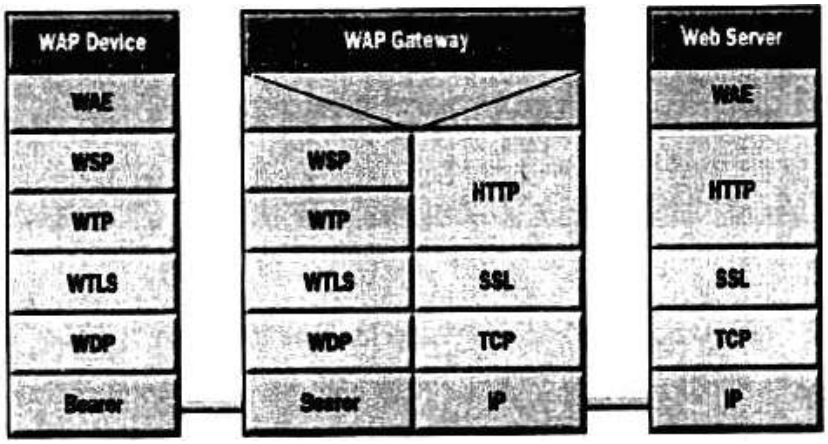
Trong mô hình này, nối kết được thiết lập thông qua điện thoại di động, nhưng lúc này kết nối được quản lý bởi người điều khiển mạng chứ không phải từ ISP. Khi điện thoại thực hiện cuộc gọi, tín hiệu sẽ được truyền đến cho người quản lý, nó thực hiện việc tìm đường đi thông qua một trong những modem của mình và nối kết với RAS server cũng giống như trong mô hình mạng Internet.

RAS server cũng sẽ thực hiện việc định dạng, nhưng một khi gói tin đi qua RAS server thì mọi thứ bắt đầu khác đi. Thay vì tìm đường trên Internet đến web server, dữ liệu được định tuyến đến WAP gateway. Tại đây, dữ liệu sẽ được biên dịch thành dạng nhị phân (nếu cần), sau đó được chuyển đi trong không khí. Gateway cũng hoạt động như là một proxy đối với điện thoại, việc giao tiếp với web server được thực hiện thông qua các giao thức HTTP 1.1. Web server không quan tâm rằng mình đang giao tiếp với một WAP gateway, nó xem gateway đơn giản như là một thiết bị client khác.

Web server có thể nằm ngay bên trong mạng hay cũng có thể thuộc một tổ chức bên ngoài khác. WAP gateway sẽ gửi các gói tin HTTP của mình qua bức tường lửa đến với web server thuộc mạng cần đến.

Nếu như WAP gateway hoạt động như là một proxy đối với điện thoại di động và sử dụng các giao thức HTTP 1.1 thông thường thì không có lý do gì TLS không được dùng đến để đảm bảo an toàn cho tất cả các giao tiếp giữa WAP gateway và web server, giống như trên Internet. Nhưng với hai chuẩn WAP đang được áp dụng hiện nay – WAP 1.x và WAP 2.0 – thì các giao thức được dùng cho việc bảo mật khác nhau.

WAP1.x. do TLS đòi hỏi một truyền tải tin cậy – thường là TCP – còn điện thoại thì lại không sử dụng TCP để giao tiếp với WAP gateway nên TLS không thể dùng để bảo mật các giao tiếp giữa điện thoại di động và WAP gateway. Thay vào đó là sử dụng một giao thức mới có tên là WTLS (có khả năng hoạt động trên WDP và UDP). Giao thức này được phát triển dựa trên TLS và cung cấp cùng một mức bảo mật giống như trong TLS.

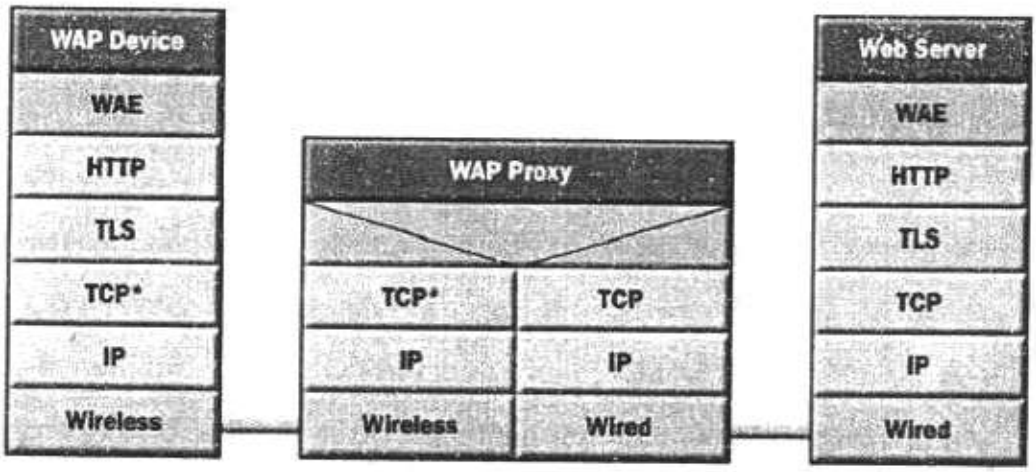


Hình 2.11. WAP 1.0

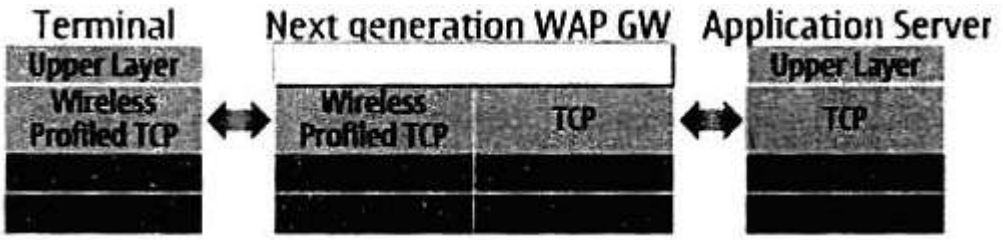
Như vậy, hệ thống phải sử dụng hai cơ chế bảo mật: Một được đặt từ thiết bị đến WAP gateway, một thì từ gateway đến web server. Điều này có nghĩa là phải có một sự chuyển đổi từ WTLS sang TLS tại gateway.

WAP 2.0. Do kiến trúc của ngăn xếp WAP 2.0 gần giống với kiến thức trên web, giao thức được sử dụng trên Tầng vận chuyển là wTCP/IP (Wireless Profile TCP/IP). wTCP/ IP được tối ưu hoá từ TCP/ IP nhằm vào mục đích phục vụ cho

hoạt động trên môi trường di động, giao thức này có thể phối hợp tốt giữa hai môi trường mạng đó là: di động và mạng Internet.



Hình 2.12. WAP 2.0



Hình 2.13. WAP

Khi muốn nối kết với ISP thì chúng ta cần phải cung cấp ID và mật khẩu người dùng để ISP thực hiện việc chứng thực. Hầu hết mọi người đều lưu trữ những thông tin này bên trong máy tính của mình và chúng sẽ đại diện cho người dùng mỗi khi cần đến.

Sẽ không có vấn đề gì nếu như mỗi người có một máy tính cho riêng mình, nhưng điều gì xảy ra khi có nhiều người cùng truy cập trên cùng một chiếc máy tính? Khi đó, người sử dụng sau có thể sử dụng thông tin của người sử dụng trước

đó để truy cập Internet, gửi nhận email, hay thậm chí có thể sử dụng cả những chứng nhận (certificate) của người dùng trước. Trường hợp này đòi hỏi hệ thống cần được quản lý bằng một cơ chế bảo mật nào đó.

Những vấn đề này lại nhỏ đủ có thế được bỏ qua trong môi trường có dây thông thường, trong thế giới không dây thì lại là cả một vấn đề. Có sự khác nhau rõ ràng giữa việc chứng thực thiết bị sử dụng và chứng thực người dùng, sự khác nhau này quan trọng hơn trong trường hợp có nhiều ứng dụng.

Mặc dù vấn đề này tồn tại trên môi trường thương mại điện tử cũng như trên môi trường di động, nhưng trong môi trường di động nó lại cao hơn, đơn giản chỉ bởi vì các thiết bị này di động. Khi số lượng điện thoại di động cũng như các thiết bị di động khác tăng lên thì tỷ lệ bị mất cắp cũng sẽ tăng theo. Một số tổ chức thậm chí còn không dùng các máy laptop cho đội ngũ bán hàng của mình, vì các máy laptop rất dễ bị mất cắp và dẫn đến việc mất thông tin quan trọng có trên máy.

Bảo mật không chỉ dùng giao thức mà trong nhiều hệ điều hành còn cung cấp nhiều dạng khác, chẳng hạn như bảo mật ở cập tập tin thông qua việc sử dụng các danh sách điều khiển truy xuất ACL (Access Control Lists). Nhưng nếu ACL được lưu trữ dưới dạng tập tin thì cũng có thể hệ thống khác sẽ đọc được nội dung này.

Về bản chất đây không phải là một vấn đề của WAP, nhưng nó lại là một vấn đề về di động và cần phải được quan tâm đến nếu như các thiết bị di động chứa các thông tin quan trọng.

Một cách để tránh được trường hợp này đó là không bao giờ lưu các thông tin quan trọng trên thiết bị di động nếu có thể. Một khả năng khác là thực hiện việc chứng thực người dùng. Sử dụng cách chứng nhận sẽ định danh một cách hiệu quả các thiết bị và thiết lập một kết nối an toàn và sau đó tất cả dữ liệu được truyền đi dưới dạng được mã hoá, yêu cầu người dùng nhập vào ID và mật khẩu. Chúng ta có thể dùng bất kỳ một kỹ thuật thông thường nào để xác nhận ID và mật khẩu này như: Kerberos, LDAP hay một sản phẩm chứng thực người dùng nào đó.

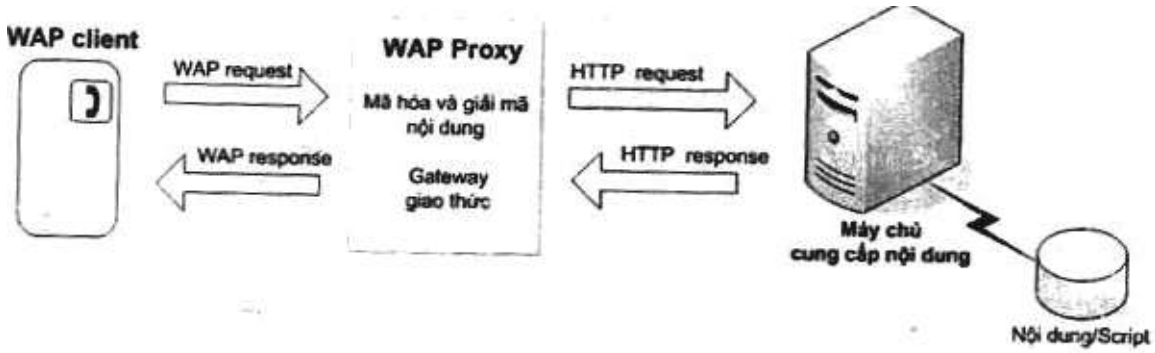
2.2.1.2. WAP Gateway.

Vấn đề trên WAP gateway có thể nhận thấy rõ ràng nhất là trên chuẩn WAP 1.x, do chuẩn này đòi hỏi WML và WMLScript phải được chuyển thành dạng nhị phân cho phù hợp với đặc điểm vận chuyển trên môi trường di động – có nhiều thách thức về băng thông và tài nguyên của thiết bị. WAP gateway chịu trách nhiệm thực hiện công việc này. Tuy nhiên:

- Một phiên bảo mật WTLS được thiết lập giữa điện thoại và WAP gateway, chứ không phải là trực tiếp với web server. Như vậy, dữ liệu chỉ được mã hoá giữa điện thoại và gateway, khi đến gateway chúng được giải mã trước khi lại được mã hoá và gửi đến cho web server qua một kết nối TLS.

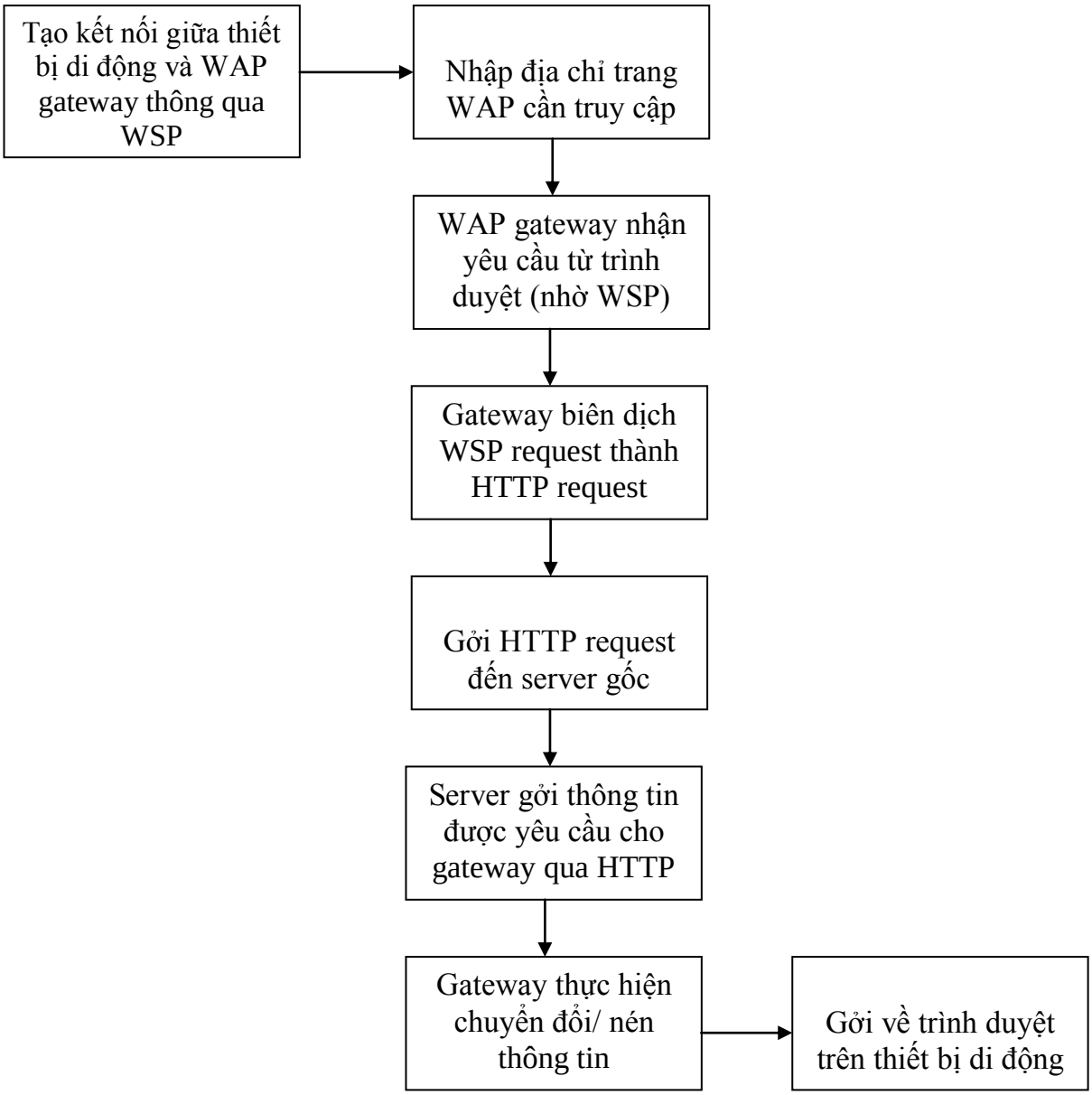
- Tại WAP gateway toàn bộ dữ liệu có thể được thấy một cách tường minh. Điều này cũng có nghĩa là tại gateway dữ liệu có thể sẽ bị mất mát. Trong kiến trúc WAP, một WAP gateway thật ra là một proxy. Nó được dùng để nối một vùng mạng không dây (wireless domain) với mạng Internet. Tuy nhiên, nó có thêm chức năng của gateway chuyển đổi giao thức (protocol gateway) và chức năng mã hoá / giải mã.

Hình dưới mô tả việc sử dụng một WAP proxy/ gateway.



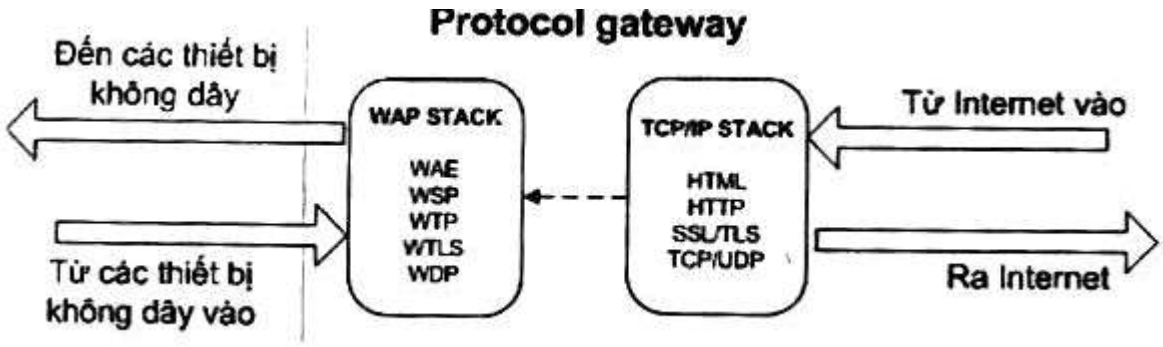
Hình 2.14. Sử dụng WAP proxy/gateway

Mỗi khi bắt đầu một phiên WAP (WAP session) trên điện thoại di động chúng ta đều phải thực hiện theo các bước như sau:



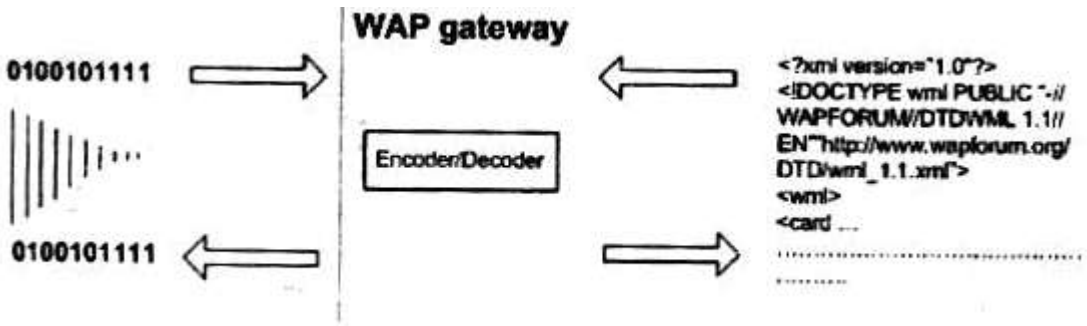
Hình 2.15. Các bước thực hiện khi tiến hành một phiên giao dịch WAP

Hình 2.15 mô tả quá trình biên dịch tại gateway chuyển đổi giao thức các yêu cầu được gửi và nhận về giữa thiết bị di động và mạng Internet.



Hình 2.16. Quá trình biên dịch các yêu cầu tại gateway chuyển đổi giao thức

Chức năng mã hoá/ giải mã (CODEC) bên trong gateway được dùng để chuyển đổi nội dung dạng WML và WML Script thành một dạng phù hợp với các mạng có băng thông thấp (thường ở dạng nhị phân). Quá trình này được mô tả trong hình dưới đây.



Hình 2.17. Mô tả chức năng mã hóa/ giải mã của WAP gateway

Một dịch vụ khác mà chức năng CODEC có thể cung cấp là biên dịch HTML hay văn bản thành WML/ XTHML. Tuy nhiên, việc sử dụng gateway như thế này còn rất nhiều giới hạn. Mặc dù HTTP và WML/XHTML đều được xây dựng dựa trên các nhưng HTML lại cho phép hiển thị các nội dung động cũng như các dạng dữ liệu đa truyền thông (multimedia) như hình ảnh, âm thanh, đồ hoạ, hay các cấu trúc phức tạp như các khung, các bảng lồng nhau... do đó với những giới hạn của thiết bị di động (bộ nhớ nhỏ, băng thông thấp, độ trễ cao) thì việc chuyển đổi đơn thuần sẽ gây không ít khó khăn cho việc hiển thị.

2.2.1.3. TLS và WTLS.

- Giống nhau: Cùng khái niệm phân biệt một phiên (Session) và một kết nối (connection).

+ Kết nối được đánh giá là ngắn hơn so với phiên.

+ Trong trường hợp mạng không dây, thời gian sống của một kết nối có thể tuỳ thuộc vào chất lượng thông tin nơi mà người sử dụng (vị trí địa lý, khí hậu...).

+ Các phiên bền hơn là các kết nối và có thể tồn tại qua nhiều kết nối và được xác định bằng một số ID của phiên (session ID).

+ Các tham số bảo mật cho mỗi phiên được sử dụng để bảo mật một kết nối, có nghĩa là khi một kết nối bị phá vỡ, phiên có thể tồn tại và có thể được phục hồi sau đó.

+ Phiên có thể được phục hồi, nghĩa là một phiên đang được thiết lập có thể sử dụng một tập tham số bảo mật với phiên trước đó. Phiên đó có thể là từ một kết nối hiện đang hoạt động, một kết nối khác cũng đang hoạt động hay là một kết nối đã hoạt động rồi. Việc phục hồi các phiên có thể được sử dụng để tạo nên các kết nối đồng thời cùng chia sẻ một tập tham số chung. Điều đó còn tuỳ thuộc vào server vì server có quyền quyết định xem có cho phép phiên được phục hồi hay không.

- Khác nhau:

WTLS	TLS
- Thuộc tầng vận chuyển, nhưng bên trên nó là WTP và WSP và tầng phiên. - Cách sắp xếp này cho phép chúng có thể độc lập với các dịch vụ được ứng dụng yêu cầu.	- Thực chất là một tầng thêm vào tầng vận chuyển dùng để can thiệp tầng ứng dụng và tầng vận chuyển " thực sự" nhằm vào mục đích bảo mật.
- Không đòi hỏi giao thức vận chuyển tin cậy (UDP, WDP).	- Đòi hỏi giao thức vận chuyển tin cậy (TCP).
- Dùng trường số tuần tự: Cho phép WTLS làm việc với các vận chuyển	- Không dùng trường số tuần tự (sequence number filed)

không tin cậy.	
- Không hỗ trợ phân đoạn, lắp ghép dữ liệu dưới dạng các gói tin.	- Cho phép phân đoạn, lắp ghép dữ liệu dưới dạng các gói tin nhận được từ các tầng trên.

Bảng 2.1. So sánh sự khác nhau giữa WTLS và TLS

WTLS cho phép chứng thực cả client và server gồm ba lớp thực hiện cùng với các đánh dấu chức năng là: Bắt buộc, tuỳ thuộc chọn hay loại trừ.

Class 1 chỉ yêu cầu hỗ trợ trao đổi khoá công khai (public key exchange) mã hoá và MACs (kiểm soát truy cập môi trường truyền thông), các chứng nhận bên phía client và server và một tuỳ chọn bắt tay bí mật có chia sẻ (một bắt tay bí mật có chia sẻ là trường hợp mà cả client và server đều đã biết được bí mật và chúng không cần trao đổi với nhau nữa.)

Các thuật toán nén và giao tiếp thẻ thông minh không được dùng trong quá trình thực hiện của class1. Các thực thi trên class 1 có thể vẫn chọn hỗ trợ cho việc chứng thực cả hai phía client và server thông qua các chứng nhận, nhưng nó không cần thiết. Class 2 hỗ trợ chứng nhận phía server là cố định. Class3, hỗ trợ cho cả client và server là cố định.

Hỗ trợ việc nén và giao tiếp thẻ thông minh là một tuỳ chọn ở class 2 và 3. Quá trình thực hiện.

- Client bắt đầu tiến trình thiết lập một phiên bảo mật bằng cách gửi thông điệp đến cho server yêu cầu đàm phán thiết lập phiên bảo mật.

- Server cũng có thể gửi thông điệp yêu cầu phía client bắt đầu một phiên đàm phán, thế nhưng nó còn tuỳ thuộc vào phía client có đồng ý hay không.

- Tại bất kỳ thời điểm nào trong phiên làm việc, phía client cũng có thể gửi thông điệp này để yêu cầu đàm phán lại các thiết bị này. Đàm phán lại các thiết lập giúp giới hạn lượng dữ liệu có thể thấy được khi kẻ nghe trộm tấn công bằng cách tạo ra một khoá an toàn mới.

- Khi client yêu cầu đàm phán một phiên bảo mật, nó cung cấp một danh sách các dịch vụ bảo mật mà nó có thể hỗ trợ. Phía client cũng cho biết rằng sau bao lâu thì các tham số bảo mật phải được làm mới lại. Trong phần lớn các trường hợp, phía client có thể yêu cầu các tham số này được làm mới qua mỗi thông điệp.

- Nếu cơ hội trao đổi khoá chung xác định không phải là kẻ mạo danh thì phía server phải gửi cho client một chứng nhận để xác định chính mình. Chứng nhận được gửi đi phải phù hợp với thuật toán trao đổi khóa đã được đồng ý.

- Chứng nhận ở phía gửi phải đến đầu tiên trong danh sách và mỗi chứng nhận đến tiếp theo phải chứng thực chứng nhận đến đó trước. Chứng nhận của CA gốc có thể được bỏ qua trong danh sách, về cơ bản có thể chấp nhận chứng nhận của CA gốc có giá trị tuỳ ý và có thể đã có sẵn ở phía client. Nếu không thì client cũng có thể dễ dàng quản lý được.

2.3. Tổng kết

Chương này đã giới thiệu các kỹ thuật tấn công mạng Internet không dây và từ đó đưa ra các giải pháp an ninh cho mạng Internet không dây (chủ yếu ở tầng trên – WAP). Việc tập trung đi sâu vào các kỹ thuật tấn công mạng Internet không dây như: tấn công bị động – Passive attacks, tấn công chủ động – Active attacks, tấn công kiểu chèn ép - Jamming attacks, tấn công kiểu thu hút - Man in the middle attacks và tấn công do yếu tố con người nhằm đưa ra một cái nhìn tổng thể về các kỹ thuật tấn công mạng Internet không dây của các hacker, để từ đó đưa ra được các giải pháp an ninh, bảo mật phù hợp với từng kỹ thuật tấn công. Các phương thức tấn công hầu hết thiên về thao tác kỹ thuật, ngoài ra phương thức tấn công do yếu tố con người còn đặc biệt quan trọng vì cách tấn công này không cần dùng nhiều thao tác kĩ thuật, nó do ý thức của từng con người quyết định, vì vậy việc giáo dục con người từ khi sinh ra là cực kỳ quan trọng.

Từ những kỹ thuật tấn công mạng Internet không dây, các giải pháp an ninh, bảo mật cũng được đưa ra và tập trung chủ yếu vào các tầng trên – WAP. Cả

Internet và WAP bảo mật được thực hiện ngay trên Tầng Vận chuyển: Mô hình trên mạng Internet không dây thực thi phần lớn các chức năng bảo mật của mình trong TLS, còn WAP thì thực hiện phần lớn trong WTLS (WTLS dựa trên nền của TLS). Ngoài ra nội dung của chương cũng đi sâu vào trình bày về các giải pháp an ninh cụ thể để ngăn chặn các cuộc tấn công bên trong và bên ngoài mạng như đã nêu trên.

Chương này đã giới thiệu các kỹ thuật tấn công mạng Internet không dây đồng thời cũng đưa ra được các giải pháp an ninh, bảo mật cho mạng Internet không dây này. Vậy trong cuộc sống, làm việc, học tập, kinh doanh thương mại,..v..v…an ninh, bảo mật của mạng Internet không dây đã được thử nghiệm và ứng dụng như thế nào? Để trả lời được câu hỏi này chúng ta đi vào nghiên cứu chương 3 – Mạng Internet không dây và thử nghiệm.

CHƯƠNG 3: MẠNG INTERNET KHÔNG DÂY VÀ THỬ NGHIỆM

ỨNG DỤNG THỰC TẾ MẠNG INTERNET KHÔNG DÂY TẠI TRƯỜNG CĐCN VIỆT ĐỨC THÁI NGUYÊN.

Trong chương 1 và 2 chúng ta đã đi sâu vào tìm hiểu về cơ sở lý thuyết cũng như các cơ chế, các nguyên tắc và một số vấn đề an ninh, bảo mật thông tin trong hệ thống mạng không dây nói chung và trong mạng Internet không dây nói riêng. Trong chương này sẽ trình bày cụ thể ứng dụng vào thực tế các lý thuyết về an ninh, bảo mật đó trong việc xây dựng hệ thống mạng Internet không dây tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên.

3.1. Thiết kế mô hình mạng Internet không dây trong trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên.

3.1.1. Nguyên tắc thiết kế

Hệ thống mạng Internet không dây được xây dựng tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên để:

- Đảm bảo truy cập không dây cho các thiết bị di động có hỗ trợ.

- Đảm bảo cung cấp được khả năng truy cập Internet không dây tại các khu vực làm việc chính trong trường (tòa nhà hiệu bộ, tòa nhà thư viện, tòa nhà làm việc của các khoa, hội trường) và một số khu vực khuôn viên bên ngoài các tòa nhà trên.

- Cung cấp các thông tin, tài nguyên, các giao tiếp giữa sinh viên với nhà trường như kế hoạch thời khoá biểu, lịch thi, thông tin về điểm học tập thông qua cổng thông tin điện tử của nhà trường như Website:

http://www.truongvietducthainguyen.edu.vn

- Đảm bảo việc truy cập vào hệ thống Server của trường để đăng ký môn học của sinh viên trong toàn trường (Đào tạo theo Hệ thống tín chỉ).

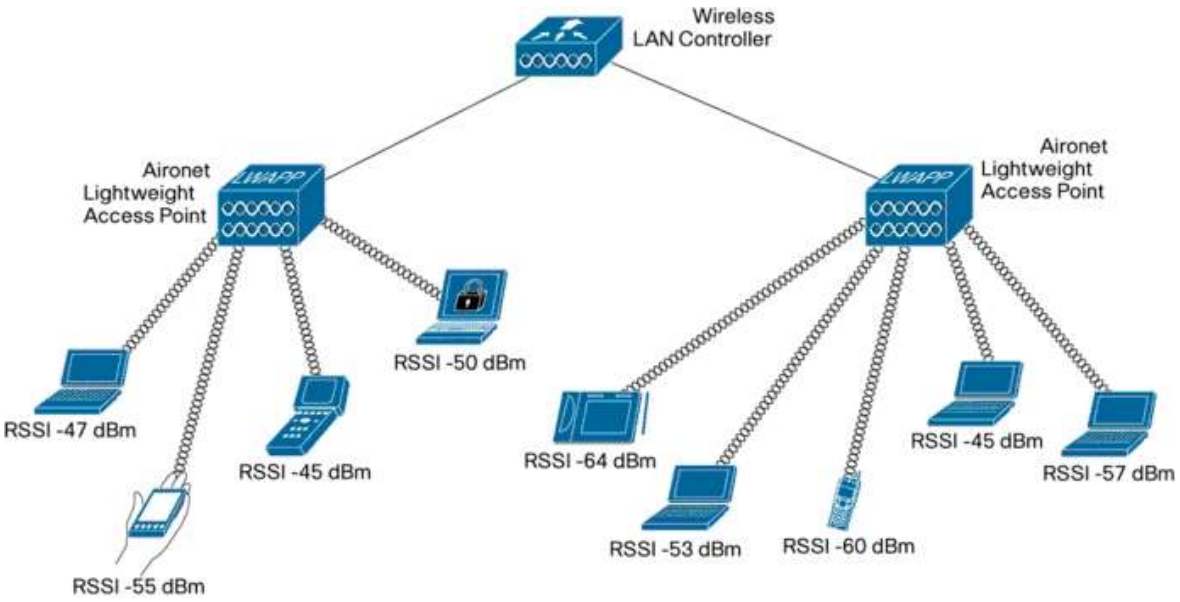
- Phải có khả năng cung cấp dịch vụ Roaming (Người dùng mạng Internet không dây có thể di truyền qua nhiều vùng phủ sóng của các Access Point khác nhau mà không bị ngắt quãng truy cập).

- Đảm bảo cung cấp các tính năng bảo mật phù hợp tin cậy để đảm bảo an toàn thông tin cho toàn bộ hệ thống cơ sở dữ liệu quan trọng của trường.

3.1.2. Mô hình logic và sơ đồ phủ sóng vật lý tổng thể tại trường

3.1.2.1. Mô hình thiết kế logic

Giải pháp bao gồm các Access point đặt tại các tòa nhà được liên kết với nhau dựa trên hệ thống mạng Internet có dây tại trường. Các Access Point được quản lý tập trung nhờ thiết bị WLAN controller đồng thời cung cấp dịch vụ roaming (kết nối liên tục trong khi di chuyển) và các dịch vụ bảo mật, chứng thực.



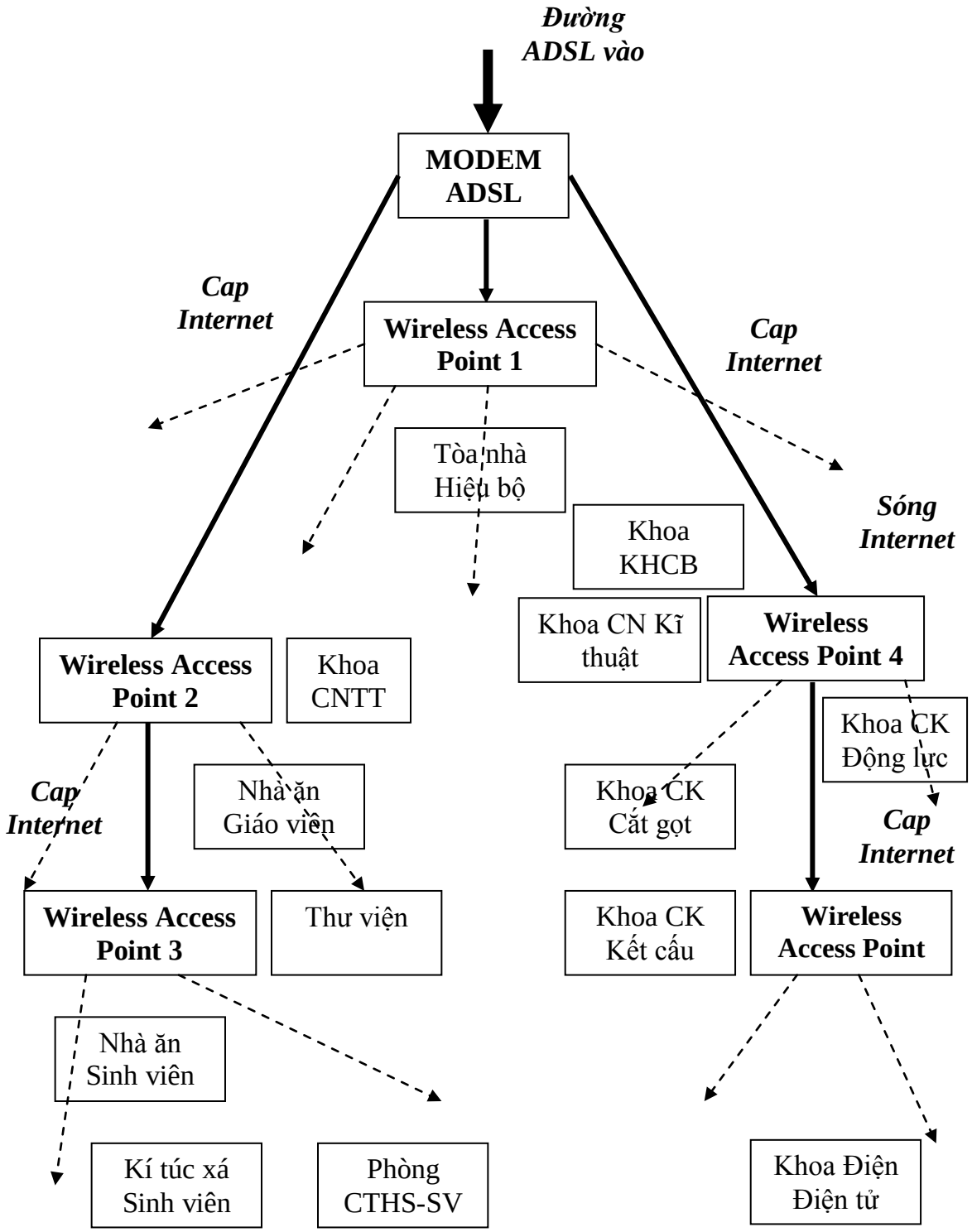
Hình 3.1. Mô hình logic mạng không dây tại trường

Các thiết bị có hỗ trợ kết nối không dây sẽ kết nối tới AP trong vùng phủ sóng, toàn bộ quá trình kết nối và các hoạt động truy cập của thiết bị sẽ được ghi lại tại file log của WLAN controller nhằm kiểm soát các hoạt động truy cập bất hợp pháp.

3.1.1.2. Sơ đồ phủ sóng vật lý tổng thể tại trường

Dựa trên quá trình khảo sát thực tế tại trường và việc tính toán chi tiết, đảm bảo khả năng tối ưu các vùng mà AP phủ sóng tới. Mặt khác không gian phủ sóng phải

liên kết một cách khoa học không rời rạc đảm bảo các yêu cầu về tín hiệu đường truyền. Từ đó chúng tôi đưa ra mô hình phủ sóng của toàn bộ hệ thống mạng không dây như sau:



Hình 3.2. Mô hình phủ sóng tại trường CĐCN Việt Đức Thái Nguyên

Trong mô hình trên ta thấy rằng việc phủ sóng tại các khu vực nhà làm việc và một số vùng khuôn viên của nhà trường được thực hiện như sau: Trong không gian tại các khu nhà làm việc các AP phát sóng indor theo dạng hình cầu bao phủ toàn bộ không gian làm việc của toà nhà. Dựa vào các thiết bị đo tín hiệu sao cho các điểm chết là ít nhất (điểm mà tại đó tín hiệu sóng wifi là ít nhất hoặc không có). Các AP sử dụng ăng ten loại yagi để phát sóng outdor theo nửa hình bán cầu ra khu vực khuôn viên của trường theo đúng thiết kế.

3.1.3. Thiết kế chi tiết của hệ thống

3.1.3.1. Mô hình thiết kế chi tiết hệ thống mạng không dây

Với phương án thiết kế, căn cứ trên các tiêu chí về ưu nhược điểm của từng phương án và hệ thống mạng hữu tuyến có dây sẵn có, mô hình thiết kế vật lý chi tiết hệ thống mạng không dây tại trường Đại học Kỹ thuật Công nghiệp Thái Nguyên

3.1.3.2. Thiết bị sử dụng trong hệ thống mạng không dây

Thiết bị sử dụng trong hệ thống bao gồm các Access Point (AP) TP-Link 108Mbits 1 Port (TL-WA601G) của TP-Link, mỗi AP sẽ được trang bị 1 antenna ngoài để hỗ trợ phủ sóng outdor ra bên ngoài khuôn viên.

Hình 3.3. Access Point (AP) TP-Link 108Mbits 1 Port (TL-WA601G)

a. Thiết bị này hỗ trợ các cơ chế bảo mật như:

- Authentication Security Standards
- WPA
- WPA2 (802.11i)
- IEEE 802.11 WEP keys of 40 bits and 128 bits

b. Một số tính năng như sau:

- Khả năng kiểm tra chính sách bảo mật của WLAN.
- Khả năng quản lý tập chung tường minh về môi trường sóng.
- Hoạt động với tốc độ cao nhờ khả năng hội tụ tin cậy và băng thông được tối ưu.
- Các tính năng di động cung cấp khả năng truy cập liên tục cho người dùng di chuyển.
- Khả năng mở rộng linh hoạch phù hợp với yêu cầu của khách hàng từ nhỏ đến lớn.
- Bảo vệ đầu tư, tiết kiệm chi phí vận hành nhờ mô hình và phương thức triển khai đơn giản, dễ vận hành.

c. Các đặc tính về kỹ thuật:

Item	Specification
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, IEEE 802.1Q VLAN tagging, and IEEE 802.1D Spanning Tree Protocol
Data Request For Comments (RFC)	• RFC 768 UDP • RFC 791 IP
Security Standards	• WPA • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm

Bảng 3.1. Các đặc tính kỹ thuật của AP TP-Link 108Mbits 1 Port (TL-WA601G)

- Cấu hình cho người dùng mạng cục bộ: Là cơ sở dữ liệu về người dụng cục bộ trên controller. Cơ sở dữ liệu về người dùng nội bộ lưu trữ các thông tin định

danh (username và password) của tất cả người dùng cục bộ, sau đó những thông tin này sẽ được dùng để chứng thực người dùng.

- LDAP: Tương tự như RADIUS hoặc cơ sở dữ liệu người dùng cục bộ, Cơ sở dữ liệu LDAP cho phép lưu trữ các thông tin định danh (username/password) của người dùng. Các thông tin này sẽ được dùng để xác thực người dùng. Ví dụ, EAP cục bộ có thể dùng LDAP để xác định username và password của người dùng.

- Local EAP: EAP cục bộ là phương thức cho phép người dùng và các thiết bị không dây có thể được chứng thực một cách cục bộ. Được thiết kế để cho các văn phòng từ xa muốn duy trì kết nối không dây khi hệ thống chứng thực không hoạt động hoặc các hệ thống backend bị gián đoạn hoạt động.

3.1.3.3. Phân bổ thiết bị sử dụng trong hệ thống

a. Tại mạng trung tâm ở nhà điều hành:

- Sử dụng 1 thiết bị AP TP-Link 108Mbits 1 Port (TL-WA601G) của TP-Link để phủ sóng wifi toàn bộ toà nhà hiệu bộ.

b. Tại các tòa nhà khác:

- Tổng cộng sẽ có 4 AP được phân bổ như sau:

- 01 AP TP-Link 108Mbits 1 Port (TL-WA601G) đặt tại Khoa CNTT.

- 01 AP TP-Link 108Mbits 1 Port (TL-WA601G) đặt tại Thư viện.

- 01 AP TP-Link 108Mbits 1 Port (TL-WA601G) đặt tại Khoa CN Kỹ thuật máy.

- 01 AP TP-Link 108Mbits 1 Port (TL-WA601G) đặt tại Khoa Cơ khí Kết cấu.

Sự phân bổ này dựa trên các tính toán thiết kế tối ưu về tầm phủ sóng và nhu cầu đặt ra tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên.

3.2. Giải pháp bảo mật trong mạng không dây tại CĐCN Việt Đức Thái Nguyên.

Trong mỗi một hệ thống thông tin nói chung thì một vấn đề vô cùng quan trọng và cần thiết đó chính là vấn đề bảo mật các thông tin chứa đựng trong hệ

thống đó. Hệ thống mạng Internet không dây tại trường CĐCN Việt Đức Thái Nguyên mới được lắp đặt thử nghiệm nên quy mô vẫn còn nhỏ, tuy nhiên trong tương lai không xa sẽ được nhà trường đầu tư thành 1 hệ thống mạng Internet không dây lớn, có tầm cỡ vì vậy việc trao đổi các thông tin liên quan giữa nhà trường và sinh viên sau này sẽ là rất lớn, hơn nữa các thông tin lại vô cùng quan trọng yêu cầu đặc biệt đặt ra là sự an toàn và bảo mật của các thông tin đó chống sửa chữa, thay đổi hay đánh cắp thông tin trên đường truyền. Từ thực tế sau này đó, các giải pháp bảo mật đã được ứng dụng trong hệ thống nhằm thực hiện các yêu cầu quan trọng nêu trên.

3.2.1. Yêu cầu bảo vệ thông tin

Để làm nổi bật rõ các yêu cầu bảo vệ thông tin tại trường chúng ta cần phân tích nguyên nhân của sự mất an toàn thông tin.

Ngày nay, Internet, một kho tàng thông tin khổng lồ, phục vụ hữu hiệu trong học tập và nghiên cứu, đã trở thành một phương tiện thuận lợi không thể thiếu trong việc trao đổi thông tin. Chính những điều quan trọng này đã trở thành đối tượng cho nhiều người tấn công với các mục đích khác nhau. Cùng với sự phát triển không ngừng của Internet và các dịch vụ trên Internet, số lượng các vụ tấn công trên Internet cũng tăng theo cấp số nhân. Trong khi các phương tiện thông tin đại chúng ngày càng nhắc nhiều đến Internet với những khả năng truy nhập thông tin dường như đến vô tận của nó, thì các tài liệu chuyên môn bắt đầu đề cập nhiều đến vấn đề bảo đảm an ninh và an toàn dữ liệu cho các máy tính được kết nối vào mạng Internet.

Không chỉ số lượng các cuộc tấn công tăng lên nhanh chóng, mà các phương pháp tấn công cũng liên tục được hoàn thiện. Nhu cầu bảo vệ thông tin của trường Cao đẳng Công nghiệp Việt Đức được chia thành ba loại gồm: Bảo vệ dữ liệu; Bảo vệ các tài nguyên sử dụng trên mạng và Bảo vệ danh tiếng của cơ quan:

3.2.1.1. Bảo vệ dữ liệu:

Đây là vấn đề đặc biệt quan trọng, toàn bộ cơ sở dữ liệu về quản lý đào tạo của nhà trường được lưu và thao tác tại các máy Server của trường. Bao gồm các dữ liệu như điểm của sinh viên, kế hoạch học tập, các thông tin về học phí...

Các dữ liệu này phải tuyệt đối an toàn đảm bảo không bị đánh cắp hoặc sửa chữa thông tin.

Hiện nay các biện pháp tấn công càng ngày càng tinh vi, sự đe doạ tới độ an toàn thông tin có thể đến từ nhiều nơi theo nhiều cách khác nhau vì vậy nhà trường đã đưa ra các chính sách và phương pháp đề phòng cần thiết. Mục đích cuối cùng của an toàn bảo mật là bảo vệ các giá trị thông tin và tài nguyên theo các yêu cầu sau:

Tính tin cậy: Đảm bảo sự chính xác các thông tin của sinh viên trong hệ thống. Đồng thời các thông tin đó không thể bị truy nhập trái phép bởi những người không có thẩm quyền.

Tính nguyên vẹn: Thông tin không thể bị sửa đổi, bị làm giả bởi những người không có thẩm quyền.

Tính sẵn sàng: Thông tin luôn sẵn sàng để đáp ứng sử dụng cho người có thẩm quyền khi có yêu cầu truy nhập thông tin vào đúng thời điểm cần thiết

Tính không thể từ chối: Thông tin được cam kết về mặt pháp luật của nhà trường cung cấp.

Trong các yêu cầu này, yêu cầu về bảo mật được coi là yêu cầu số 1 đối với thông tin lưu trữ trong hệ thống.

3.2.1.2. Bảo vệ các tài nguyên sử dụng trên mạng:

Trên thực tế, trong các cuộc tấn công trên Internet, kẻ tấn công, sau khi đã làm chủ được hệ thống bên trong, có thể sử dụng các máy này để phục vụ cho mục đích của mình như cài đặt các chương trình chạy ẩn để dò mật khẩu người sử dụng, ứng dụng các liên kết mạng sẵn có để lấy cắp các thông tin cần thiết hoặc tiếp tục tấn công các hệ thống khác vv...

3.2.1.3. Bảo vệ danh tiếng cơ quan:

Một phần lớn các cuộc tấn công không được thông báo rộng rãi, và một trong những nguyên nhân là nỗi lo bị mất uy tín của cơ quan, đặc biệt là gây sự hoang mang không tin tưởng vào các thông tin mà nhà trường cung cấp. Trong trường hợp bị tấn công gây mất an toàn về dữ liệu thì tổn thất về uy tín là rất lớn và có thể để lại hậu quả lâu dài.

3.2.2. Các bước thực thi an toàn bảo mật cho hệ thống

Phần này trình bày các bước thực thi an toàn bảo mật và các biện pháp nhằm tăng cường tính an toàn, bảo mật cho hệ thống mạng không dây tại trường theo các mức khác nhau. Để có được các chính sách bảo mật đem lại hiệu quả cao, cần xác định rõ các nhân tố tối thiểu về an toàn bảo mật cho hệ thống mạng của trường cùng với các kiến thức quản trị và kỹ năng để thực hiện các hoạt động tăng cường an toàn bảo mật.

3.2.2.1. Các hoạt động bảo mật ở mức một

Ở mức một, người thực thi bảo mật, quản trị hệ thống và mạng thực hiện làm cho môi trường mạng, máy tính ít bị lỗ hổng bảo mật hơn vì đã được sửa lỗi bằng các bản sửa lỗi hoặc bằng các biện pháp kỹ thuật. Thực hiện các cảnh báo ngay lập tức (trực tuyến) để nhắc nhở, thông báo mỗi người dùng trong mạng các quy tắc sử dụng mỗi khi truy nhập vào hệ thống mạng của trường. Xây dựng một mạng lưới bảo vệ, lọc, phát hiện và tiêu diệt virus, Spyware, Troyjan - trên tất các các máy trạm, máy chủ, và các cổng kết nối mạng (gateway). Đảm bảo cập nhật thường xuyên các phần mềm diệt virus.

Đảm bảo rằng hệ thống sao lưu dữ liệu hoạt động định kỳ, các tập tin có thể được khôi phục từ các bản sao lưu định kỳ đó, người quản trị hệ thống có đủ kiến thức cập nhật cần thiết để thực hiện sao lưu trên tất cả các hệ thống ngay lập tức trong trường hợp bị tấn công. Nếu không có dữ liệu được sao lưu tốt, một vấn đề nhỏ trong an toàn bảo mật có thể trở thành thảm họa.

Cho phép ghi nhật ký các sự kiện, hoạt động của người dùng khi đăng nhập vào hệ thống. Hệ thống nếu không có cơ chế ghi nhật ký thì nó gây khó khăn cho việc phát hiện và khắc phục các vụ tấn công.

Thực thi xác thực hệ thống, kiểm tra (audit) để kiểm soát người sử dụng hệ thống. Chống lại kẻ tấn công giả danh người sử dụng đăng nhập vào hệ thống và chiếm quyền điều khiển hệ thống.

3.2.2.2. Các hoạt động bảo mật ở mức hai

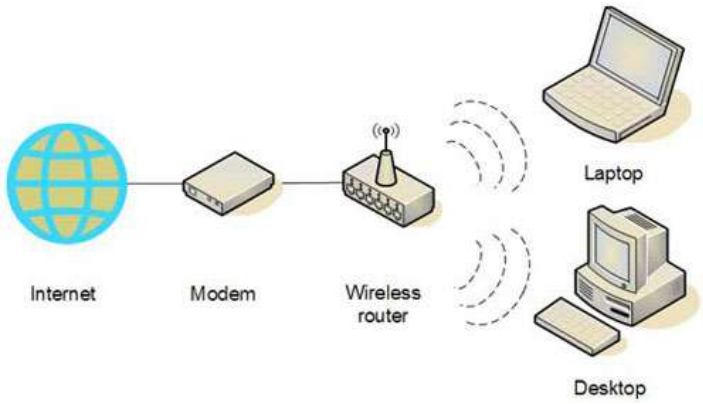
Các hoạt động an toàn bảo mật mức hai tập trung nhiều hơn vào việc xây dựng các chính sách truy nhập cụ thể của người dùng, cho phép hoặc không cho phép truy cập vào các tài nguyên mạng khác nhau trong hệ thống. Đưa ra các yêu cầu cụ thể đối với người dùng như việc đăng ký các thông tin cá nhân, đăng ký địa chỉ MAC của thiết bị truy cập, xây dựng cơ sở dữ liệu về tài khoản truy cập để xác thực mỗi khi đăng nhậnp hệ thống. Các hoạt động an toàn bảo mật mức hai cũng tập trung vào các hiểm họa bắt nguồn từ bên trong nội bộ và có chính sách giám sát các Server chứa thông tin quan trọng, hỗ trợ các chức năng nhiệm vụ quan trọng.

Trong hệ thống mạng không dây của nhà trường đã xây dựng một Server Proxy có cài đặt phần mềm chuyên dụng cho phép phát hiện truy nhập của người dùng được phép hoặc trái phép, lưu và phân tích kết quả truy nhập đó.

3.3. Chương trình thực tế đã xây dựng

Với cơ sở nền tảng lý thuyết về bảo mật hệ thống mạng không dây như đã nghiên cứu ở trên, đồng thời nhiều vấn đề trong bảo mật đã được phân tích, đánh giá một cách cụ thể, từ đó em đã đưa ra được những ưu điểm hay những hạn chế trong vấn đề bảo mật cho mạng không dây. Qua những kiến thức đã học được, em được nhà trường tin tưởng giao cho việc xây dựng hệ thống mạng không dây tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên, đồng thời áp dụng các phương pháp bảo mật đã nghiên cứu cho hệ thống nhằm đảm bảo sự an toàn về thông tin và cơ sở dữ liệu quan trọng của nhà trường. (Do hiện nay nhà trường mới

đang bắt đầu mua các thiết bị bảo mật mạng Internet không dây nên em chưa có điều kiện trình bầy rõ hơn trong luận văn này).



Hình: 3.4. Mô phỏng kiến trúc hiện tại hệ thống mạng Internet không dây của trường CĐCN Việt Đức

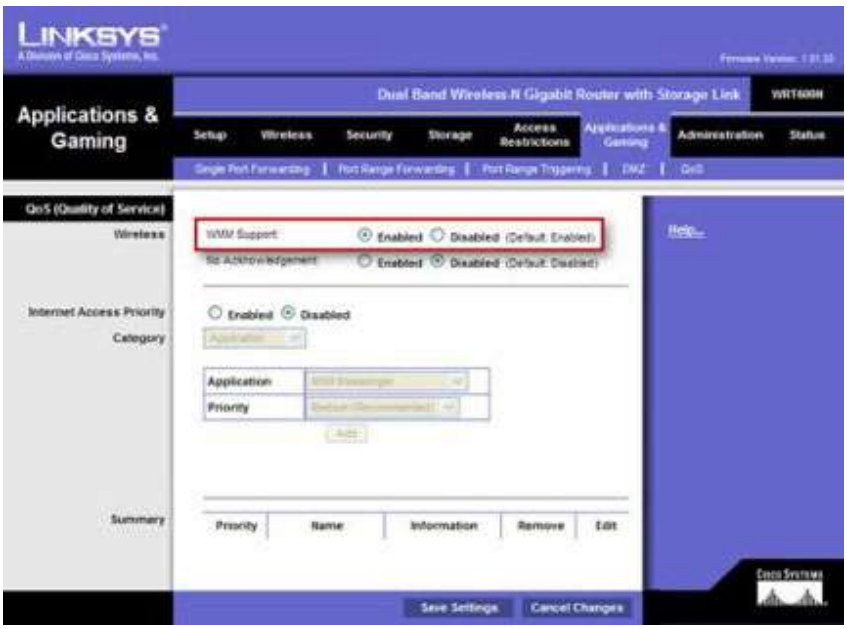
3.4. Đánh giá kết quả

Hệ thống mạng Internet không dây hiện tại đang được sử dụng tại trường CĐCN Việt Đức Thái Nguyên đang trong quá trình hoạt động thử nghiệm, nhưng trong toàn bộ khu vực nhà trường các thiết bị hỗ trợ kết nối không dây đều có thể truy cập mạng Internet bình thường và đây cũng là một tiền đề rất quan trọng để nhà trường đầu tư thêm. Hệ thống Internet không dây hiện nay gồm có 05 AP phủ sóng trong toàn trường, trong thời gian tới các thiết bị phục vụ cho việc bảo mật thông tin sẽ được nhà trường đầu tư và triển khai.

3.5. Một số hướng dẫn để bảo vệ máy tính an toàn khi dùng Internet không dây.

3.5.1. Tối ưu hóa Wi-Fi cho các VoIP, Video Game

Nếu trong lúc bạn đang đang VoIP với Skype, Second Life hoặc dùng iTune để tải nhạc thì có cảm giác như mạng bị chập chờn,bạn khoan hãy nghĩ đến chuyện mua một router mới. Hầu hết các router được sản xuất trong thời gian gần đây đều có tính năng quản lý chất lượng dịch vụ (QoS), nếu không có bạn có thể phải cập nhật firmware để kích hoạt nó.



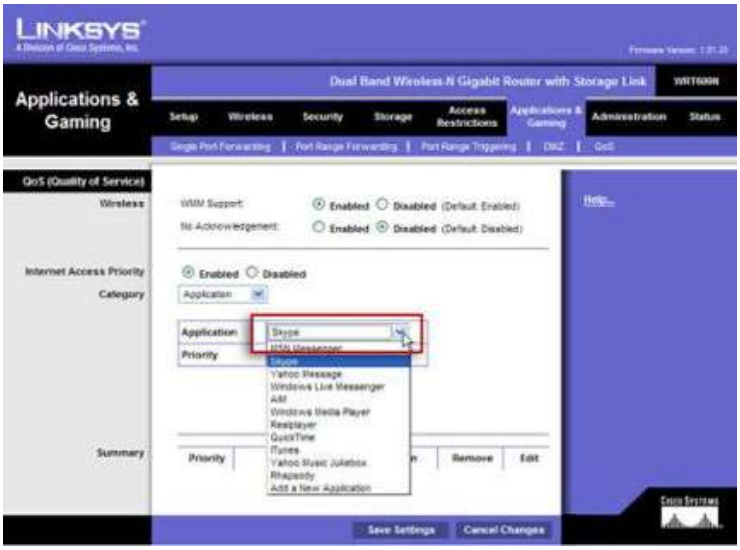
Hình 3.5. Cấu hình của Router Linksys

Ví dụ chương trình cấu hình của router Linksys ở hình trên, bạn chọn thẻ QoS có trong phần "Application & Gaming". Kiểm tra chắc chắn rằng phần "WMM Support" đã được chọn (Enable).

Bật chế độ tùy chọn "Internet Access Priority" dành cho các ứng dụng voice và media trong ứng dụng tương ứng từ danh sách sổ xuống (drop-down list).

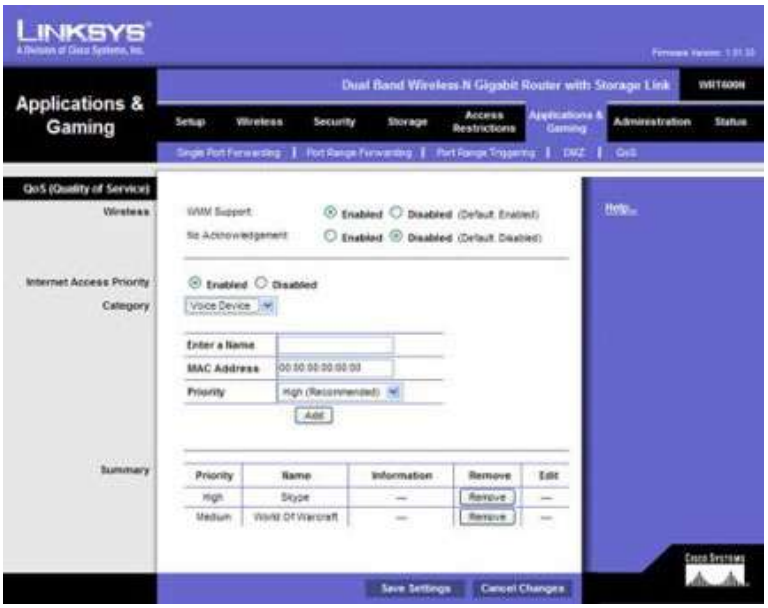
3.5.2. Ưu tiên hóa tải gói dữ liệu

Bạn có thể tối ưu cho gói dữ liệu gửi nhận thông qua thiết lập trên Rounter. Bạn có thể chọn "High", "Medium", "Normal" hay "Low" tùy theo độ ưu tiên bạn muốn gán cho gói dữ liệu, sau đó nhấn nút "Add".



Hình 3.6. Tối ưu cho gói dữ liệu gửi nhận thông qua thiết lập tren Rounter

Bạn có thể ưu tiên cho hoạt động hội thoại trên mạng bằng cách cấp quyền ưu tiên "Low" cho các dịch vụ download khác như BitTorrent hay IDM và cấp quyền ưu tiên "High" cho dịch vụ VoIP.



Hình 3.7. Cấp quyền ưu tiên

3.5.3. Tắt Wi-Fi khi không dùng đến

Điều này sẽ ngăn chặn việc bạn vô tình kết nối vào các điểm truy cập độc hại và nó cũng giúp kéo dài thời gian sử dụng pin cho laptop. Một vài sản phẩm máy tính xách tay có nút trên thân máy dùng để làm việc này (thường là phím mày xanh hiện chữ Fn và mang biểu tượng ăngten phát thu song). Bạn cũng có thể tắt Wi-Fi bằng cách nhấn phải lên biểu tượng kết nối không dây ở System tray và chọn "Disable"

Hình 3.8. Tắt Wi-Fi khi không dùng đến

Để bật lại kết nối Wi-Fi, bạn chỉ cần vào Control Panel và nhấp đúp chuột lên biểu tượng kết nối.

3.5.4. Theo dõi những người không mời mà đến trên mạng Wi-Fi của bạn

Các cơ chế mã hóa đặc biệt là WEP có thể bị bẻ gãy và thậm chí việc lọc địa chỉ MAC address cũng có thể bị qua mặt. Để ngăn các cuộc xâm nhập lạ mặt hãy tải về và cài đặt phiên bản miễn phí của phần mềm Network Magic (tải tại http://www.pcworld.com/downloads/file/fid,44361-order,1-page,1/description.html). Chương trình sẽ vẽ ra một bản đồ tất cả các thiết bị đang

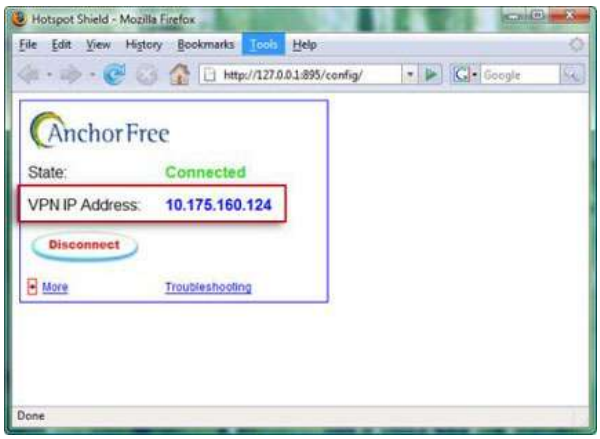
hiện diện trên mạng bao gồm máy tính, máy chủ, máy in và các thiết bị ngoại vi khác. Nhờ vậy bạn có thể dễ dàng xác định kẻ ẩn danh.

Để nhận được thông báo khi có một thiết bị mới tham gia vào mạng không dây bạn chọn "Options" từ trình đơn "Tools", nhấn vào tab "Notifications" và đánh dấu chọn mục "A new device joins the network".

Hình 3.9. Thiết lập theo dõi khách không mời mà đến.

3.5.5. Loại bỏ điểm kết nối không dây an toàn

Các điểm kết nối không dây công cộng là cơ hội cho hacker bởi vì nó được mở cho mọi người tham gia.



Hình 3.10. Loại bỏ điểm kết nối không dây an toàn

Trừ phi bạn sử dụng một phần mềm tạo mạng riêng ảo (VPN) nếu không thì bất cứ ai cũng có thể thấy được tất cả dữ liệu của bạn bao gồm mật khẩu và email.

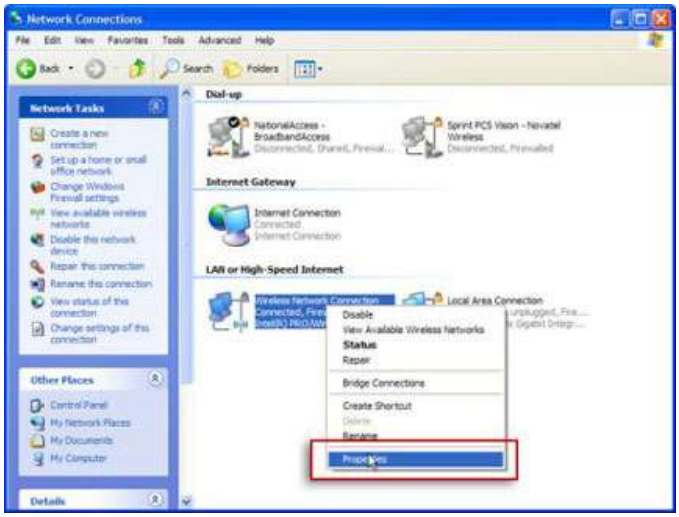
Nếu bạn chưa có một phần mềm VPN cho riêng mình thì hãy sử dụng bản miễn phí là Hotspot Shield của hãng AnchorFree (tải về tại http://www.hotspotshield.com/). Chỉ cần tải về và cài đặt, trình duyệt của bạn sẽ hiển như hình dưới đây. Nhấn vào "Run Hotspot Shield" vậy là việc bảo vệ đã bắt đầu.

Để tắt Hotspot Shield chỉ cần nhấn chuột phải vào biểu tượng màu xanh ở System tray là chọn "Disconnnect" biểu tượng sẽ chuyển sang màu đó. Để bật lại chỉ việc làm như trên và chọn "Connect".

Trong khi đang kết nối, bạn có thể chọn "Properties" từ biểu tượng Hotspot Shhield để xem địa chỉ IP hiện thời của mình.

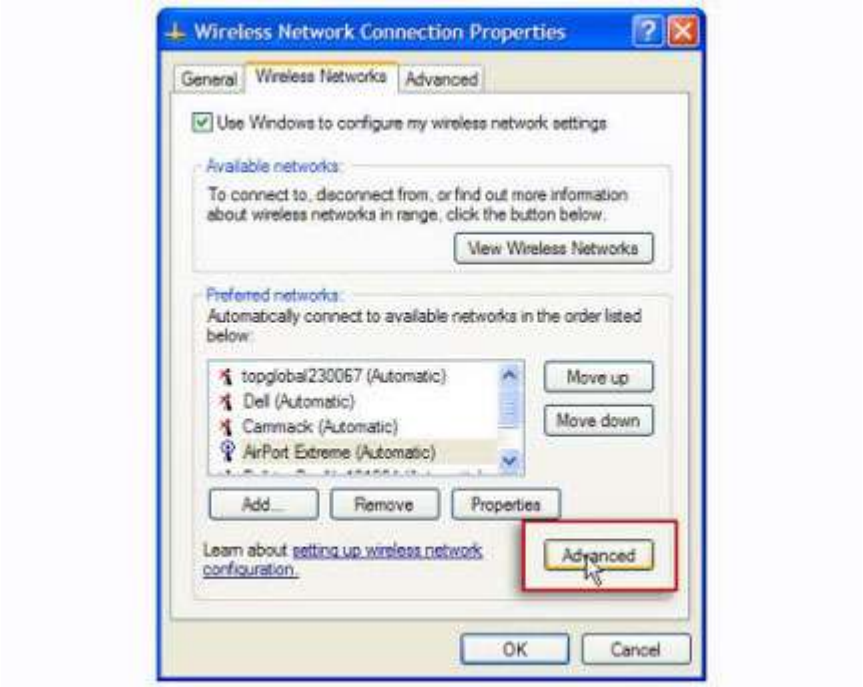
3.5.6. Vô hiệu hóa Peer-to-Peer Wi-Fi

Mở cửa sổ "Network Connections" trong Control Panel, nhấn phải chuột vào biểu tượng wireless và chọn "Properties"



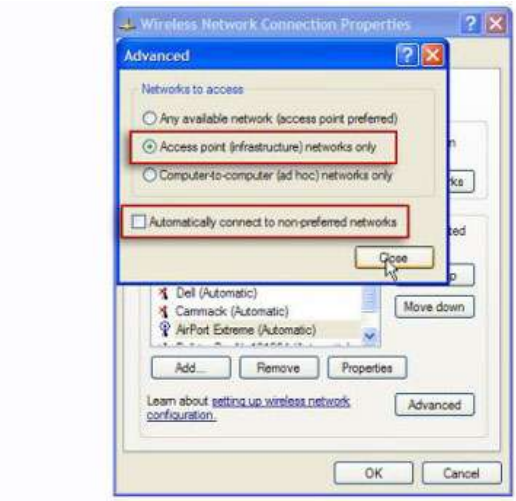
Hình 3.11. Vô hiệu hóa Peer-to-Peer Wi-Fi

Chọn tab "Wireless Networks" và nhấn vào nút "Advanced"



Hình 3.12. Vô hiệu hóa Peer-to-Peer Wi-Fi

Chọn "Access point (infrastructure) networks only". Chắc chắn rằng mục "Automatically connect to non-preferred networks" không được đánh dấu.



Hình 3.13. Vô hiệu hóa Peer-to-Peer Wi-Fi

Như vậy, với việc kiểm soát các dòng thông tin ra vào, kiểm tra tính an toàn của các AP, ta có thể giảm rủi ro bị tấn công bởi các hacker.

3.6. Tấn công Website – Cách xử lý.

Với sự phát triển của Internet hiện nay, việc một công ty hay một tổ chức tạo cho mình một website không còn là một chuyện khó khăn nữa. Chỉ với một khoản chi phí không lớn họ đã có được một website để giao dịch cũng như quảng bá thương hiệu của mình trên toàn thế giới thông qua mạng internet. Ta có thể thấy rõ lợi ích của website mang lại cho công ty hay tổ chức. Đó là nơi mà khách hàng trên toàn thế giới biết đến công ty của bạn, biết được lĩnh vực hoạt động của công ty của bạn để có quyết định hợp tác làm ăn. Chính các doanh nghiệp Việt Nam cũng đã từng ký kết được nhiều hợp đồng với các đối tác nước ngoài qua tìm hiểu các thông tin trên website của họ và kịp thời liên hệ.

Với sự phát triển rầm rộ của thương mại điện tử thì các hoạt động kinh doanh trên mạng cũng khá là phát triển và mạng lại lợi nhuận không nhỏ cho nhà cung cấp dịch vụ trực tuyến.

Tuy nhiên, song song với những thuận lợi và tiện ích mà website của bạn có được thì bạn cũng gặp không ít khó khăn trong hoạt động của mình liên quan tới website đó. Đơn giản nhất là việc duy trì, cập nhật thông tin đã khiến bạn tốn khá nhiều thời gian và thường phải có một người chuyên làm công việc này.

Vậy thì website có ảnh hưởng gì cho công ty của bạn không? Tất nhiên là có rồi, công ty của bạn càng phát triển thì website chính là bộ mặt của bạn để mọi người truy cập vào tìm hiểu thông tin. Do đó, sẽ có nhiều người muốn cạnh tranh không lành mạnh, muốn phá hoại website của bạn. Họ có thể nhờ các hacker mũ đen tìm cách xâm nhập trang web của bạn, phá hoại trang web của bạn

- Họ thay đổi thông tin trang web, đưa những thông tin không đúng về công ty của bạn khiến đối tác hiểu nhầm và không hợp tác với công ty của bạn.
- Họ tìm cách tấn công trang web của bạn, khiến trang web truy cập rất chậm khiến người truy cập chán nản và không truy cập trang web nữa, một phương thức tấn công điển hình đó là DDOS.
- Đánh sập trang web của bạn, nếu bạn không backup dữ liệu thì việc khôi phục lại website là cả một vấn đề.

Vậy, khi website của bạn có hiện tượng bị tấn công thì bạn phải làm gì ?

- Lưu lại hết các file log truy cập vào website để tiện cho việc truy tìm kẻ tấn công.
- Thiết lập tường lửa bằng phần mềm để giảm bớt sự quá tải cho website. Nếu bạn đủ khả năng tài chính thì hãy trang bị cho mình thiết bị phát hiện và phòng chống tấn công.
- Nếu việc tấn công là liên tục thì hãy báo với các cơ quan chức năng như C15, Vncert (http://vncert.gov.vn) hay Bkis để họ có phương án truy tìm thủ phạm tấn công website. Trước đây, các cơ quan này đã phối hợp với nhau để tìm ra thủ phạm tấn công chợ điện tử đó là Huy remy hay việc DanTruongX tấn công DDOS công ty Việt Cơ.

Theo tôi được biết thì các cơ quan liên quan đang phối hợp với nhau để đưa ra các khung hình phạt cho các loại tội phạm này, kể cả việc xử lý hình sự đối với các hành vi phá hoại an toàn an ninh mạng. Chỉ có các hình phạt thích đáng thì mới đủ sức răn đe các hành vi phá hoại đó.

3.7. Tổng kết.

Chương này đã giới thiệu việc ứng dụng công nghệ mạng vào xây dựng hệ thống mạng Internet không dây tại trường CĐCN Việt Đức Thái Nguyên nơi tôi công tác. Trường CĐCN Việt Đức Thái Nguyên mới đưa vào thử nghiệm hệ thống mạng Internet không dây từ tháng 01/2009 nên vẫn còn rất nhiều khó khăn về hạ

tầng, cơ sở vật chất. Vấn đề an ninh, bảo mật trong hệ thống mạng không dây này được đưa ra và là một phần hết sức quan trọng không thể thiếu được trong công tác duy tu bảo trì hệ thống mạng Internet không dây. Vấn đề này sẽ được triển khai khi nhà trường trang bị hệ thống các thiết bị an ninh, bảo mật cho mạng Internet không dây.

Ngoài ra chương này cũng đề cập đến một số kỹ thuật bảo vệ máy tính an toàn khi máy tính kết nối Internet không dây và cách xử lí khi Website bị tấn công.

KẾT LUẬN

Vấn đề bảo mật cho hệ thống mạng Internet không dây luôn là một vấn đề hết sức khó khăn và được đặt ở vị trí rất quan trọng trong hầu hết các bản thiết kế mạng. Tuy nhiên, để có thể có được một giải pháp hoàn hảo cho mọi tình huống là một điều gần như rất khó. Chính vì vậy, khi thiết kế hệ thống mạng Internet không dây, chúng ta phải dựa trên cơ sở, yêu cầu thực tế của hệ thống, cân nhắc giữa các lợi hại của các phương pháp để đưa ra các chính sách an ninh, bảo mật hợp lý nhất. Trong thực tế xây dựng hệ thống mạng Internet không dây cho nhà trường đều có sự tham gia của các thành phần khác nhau và có những yêu cầu bảo mật khác nhau. Phân tích kỹ lưỡng các điều này giúp ta quyết định biện pháp nào là phù hợp nhất với hệ thống.

1. Kết quả đạt được.

Với mong muốn giúp các nhà quản trị mạng có thể xây dựng được các giải pháp bảo mật tốt hơn cho hệ thống mạng Internet không dây, trong sự phát triển mạnh mẽ của công nghệ Internet không dây hiện nay và trong tương lai, luận văn "Nghiên cứu vấn đề an ninh mạng Internet không dây và ứng dụng" của em đã nghiên cứu và đạt được một số kết quả sau:

- Tìm hiểu tổng quan về hệ thống mạng không dây, mạng Internet không dây, các chuẩn giao tiếp mới, các giao thức, cách truyền dẫn dữ liệu, khả năng chống nhiễu, dải tần, cũng như một số vấn đề về kỹ thuật của hệ thống mạng không dây.

- Trình bày được các đặc điểm về mạng Internet không dây và một số các điểm yếu trong an ninh, bảo mật cũng như các hệ thống bảo mật sẵn có của hệ thống mạng Internet không dây.

- Tìm hiểu một số các phương pháp tấn công cơ bản trong hệ thống mạng Internet không dây. Từ đó xây dựng các giải pháp phù hợp cho hệ thống.

- Nghiên cứu một số phương pháp đã được sử dụng để cải thiện tính bảo mật của hệ thống mạng Internet không dây, đề xuất sử dụng các phương pháp trong việc thiết kế hệ thống mạng.

- Đã ứng dụng thực tế một phần vấn đề an ninh trong hệ thống mạng Internet không dây tại trường Cao đẳng Công nghiệp Việt Đức Thái Nguyên, đã đem lại kết quả tốt.

2. Hạn chế.

Trong khuôn khổ của luận văn này, việc nghiên cứu mới chỉ dừng lại ở mức phân tích và đưa ra một số các nhận xét về các biện pháp và công cụ an ninh, bảo mật đã có cũng như các phương thức bảo mật đang được phát triển và sử dụng với hệ thống mạng Internet không dây. Nhằm cung cấp thêm cho người quản trị mạng có cái nhìn tổng quan hơn về các công nghệ hiện hành và khả năng bảo mật thật sự của hệ thống mạng Internet không dây, từ đó ra quyết định lựa chọn phương án an ninh, bảo mật cho hệ thống của mình.

Tuy nhiên do thời gian có hạn và còn nhiều hạn chế về kiến thức cũng như điều kiện, môi trường để ứng dụng hệ thống mạng Internet không dây nên trong quá trình thực hiện luận văn, không tránh khỏi có những sai sót như: như chưa tiến hành thực nghiệm được các hệ thống thực tế nhất là đối với kiến trúc hoạt động của WAP, WAP Gateway và các hướng bảo mật của WAP.

Em mong rằng sẽ nhận được những ý kiến đóng góp của các thầy cô và các bạn để luận văn hoàn thiện hơn, có ích hơn trong thực tế và trong công việc hàng ngày của e.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1) Mạng máy tính và các hệ thống mở (Nguyễn Thúc Hải)

2) Bài giảng mạng máy tính (Phạm Thế Quế)

3) Website Bách khoa toàn thư mở http://vi.wikipedia.org/wiki/WAP

Tiếng Anh

4) http://www.wapforum.org/what/technical.htm

5) http://www.javvin.com/protocolWAP.html

6) http://www.vocw.edu.vn/content/m10027/latest/

7) http://www.alliedtelesyn.com/media/pdf/wireless_lan_basics_wp_b.pdf

8) http://www.wap.com/

9) http://atrak.usc.edu/~massoud/Papers/remoteprocessing-dac03-talk.pdf

10) BASAVARAJ PATIL,YOUSUF SAIFULLAH, IP in wireless Network, Prentice Hall PTR, January 2003. (chapter 13).

11) Strategic Planning Bureau of the Information Technology Division, "Network Management Architecture Guidelines".

12) Brett McLaughlin, "Java&XML, 2nd Edition".

13) www.w3c.com

14) Wireless Local Area Netwozzrks *(Pierfranco Issa 1999)*

15) Designing A Wireless Network *(Syngress Publishing 2001)*

16) Building A Cisco Wireless LAN *(Syngress Publishing 2002)*

17) Building Wireless Community Networks *(O'Reilly 2002)*

18) Configuring the Cisco Wireless Security Suite *(Cisco System 2002)*

19) Wireless Security and Privacy: Best Practices and Design Techniques *(Addison Wesley 9/2002)*

20) Building Secure Wireless Networks with 802.11 *(Wiley Publishing 2003)*

21) Wireless Security: Critical Issues and Solutions *(Craig J. Mathias 2003)*

22) WAP – 195 – WAEOverview Version 29 – March - 2000

Wireless Application Protocol – Wireless Application Environment Overview Version 1.3.

23) WAP – 199 – WTLS Version 18 – Feb - 2000

Wireless Application Protocol – Wireless Transport Layer Security Specification

24) WAP – 200 – WDP Approved version 19 – Feb – 2000

Wireless Application Protocol – Wireless Datagram Protocol

25) WAP 203 – WSP Approved Version4 – May - 2000

Wireless Application – Protocol – Wireless session Protocol Specification

26) WAP – 201 – WTP Approver –Version 19 – February 2000

Wireless Application Protocol – Wireless Transaction Protocol Specification

PHỤ LỤC

Bộ công cụ Nokia Mobli Toolkit

1. Nokia Mobli Internet Toolkit v4.1

a. Giới thiệu

Nokia Mobli Internet Toolkit (NMIT) bao gồm một tập hợp các trình soạn thảo dùng để tạo nên nhiều loại nội dung khác nhau trên môi trường Internet di động. NIMT cho phép hiển thị các nội dung này trên nhiều bộ SDK của điện thoại.

Những bộ nhớ SDK của điện thoại được cài đặt riêng lẻ. Khi khởi động NMIT sẽ tự động dò tìm, những bộ SDK điện thoại được hỗ trợ sẽ được thêm vào bảng danh sách trong phần SDK Control Pannel của nó. Bảng danh sách này có thể được hiển thị phần nội dung chỉ nhấp chuột vào nút Show trên trình soạn thảo.

Nhiều trình soạn thảo NMIT được dùng để tạo ra những nội dung dựa trên XML được định nghĩa bởi Document Type Defnition (DTDs). Những trình soạn thảo này thực hiện việc xác nhận nội dung để kiểm tra chúng với DTD và còn cung cấp những tính năng cho việc chọn lựa các phần tử một cách dễ dàng và các chức năng cho việc chèn thêm dựa trên vị trị hiện tại của con trỏ. Thêm vào đó, NMIT còn cung cấp một trình quản lý DTD mà qua nó bạn có thể nhập thêm vào các DTD mới dùng cho các trình soạn thảo NMIT.

b. Các chức năng

Các chức năng chính của NMIT bao gồm.

Một tập các trình soạn thảo hỗ trợ cho việc tạo lập và sửa đổi nội dung Internet trên di động. Những tính năng này có thể được truy xuất bằng cách sử dụng lệch File > New hoặc File > Open. Bảng sau đây mô tả một cách ngắn gọn về các trình soạn thảo này.

Browsing Editor

Tạo lập một tài liệu WML. Hỗ trợ WML 1.3 DTD tương thích với đặc tả WAP tháng 6/ 2000. Có hỗ trợ các tài liệu WML 1.1 và 1.2.

WML Script.

Tạo lập nội dung WML Script, WML Script bắt nguồn từ ECMA Script và được dùng để thêm các luận lý logic vào một WML Deck, ví dụ như các tính toán.

WBMP Image

Tạo lập một hình ảnh Wireless Bitmap (WBMP). Cũng giống như hầu hết các trình xử lý ảnh, trình soạn thảo WBMP cho phép tạo lập và chỉnh sửa các hình ảnh dạng WBMP, cũng như chuyển đổi những hình ảnh sẵn có từ định dạng GIF và JPEG sáng WBMP.

XHTML – MP

Tạo lập một tài liệu XHTM dựa trên XHTML Moble Profile DTD

XHTML – MP + CHTML

Tạo lập một tài liệu XHTML dựa trên XHTML Moble Profile DTD với các phần tử cà thuộc tính cộng thêm Compact HTML.

CSS

Tạo lập một bảng mẫu Cascading Style Sheet (CSS). CSS chứa các kiểu mẫu định dạng sẽ được áp dụng cho các phần tử được chỉ ra trong một tài liệu XHTML.

Select DTD From List

Tạo lập một tài liệu dựa trên một hệ thống DTD đã được chọn lựa, đó chính là một DTD từ một danh sách kèm theo là do bạn tự tạo ra.

Push Content Editors

Service Indication (SI)Editor

Tạo một thông điệp Service Indication Push, thông điệp này được gởi đến người dùng thông báo rằng nội dung mới đã được sẵn sàng.

Service Loading (SL)Editor

Tạo một thông điệp Service Loading (SL)Editor, thông điệp này được gởi đến để bắt buộc một dịch vụ người dùng đang chạy trên thiết bị khách cần phải tải về nội dung mới (không thông báo cho người dùng).

Cache Operation (CO) Edtor

Tạo một thông điệp Cache Operation Edtor, thông điệp này được gởi đi nhằm làm mất hiệu lực nội dung nằm trong cache của dịch vụ người dùng (vì thế buộc phải nạp lại nội dung nếu người dùng yêu cầu nội dung đó lần tiếp theo).

Multipart Message Editor

Tạo một thông điệp đa phần, đây là một loại của thông điệp Push chứa nhiều hơm một phần, mỗi một phần được thực thi riêng lẻ bởi dịch vụ người dùng . Trình soạn thảo sẽ tập hợp và sắp xếp lại những phần có sẵn (các tập tin) vào trong một thông điệp đa phần.

Messaging Editor

MMS Wizard

Tạo tập tin thông điệp đa phương tiện (Multimedia Messging) chứa một hay nhiều phần, mỗi phần bao gồm văn bản, hình ảnh, hoặc âm thanh.

MMS Messag Edior

Tạo lập hoặc sửa đổi một thông điệp MMS. các chức năng chính cho phép bạn thêm, xoá hoặc sắp xếp lại các phần truyền thông, sửa đổi các tiêu đề MMS và tiêu đề của các phần riêng; sau đó đẩy thông điệp này cho bộ SDK được lựa chọn.

SMIL Editor

Tạo một tập tin SMIL (Synchronized Multimedia Integration Langue), cho việc chỉ ra các tuỳ chọn trình diễn của một thông điệp MMS.

Deployment Editor

DRM Editor

Tạo một thông điệp DRM và các thứ tự của nó.

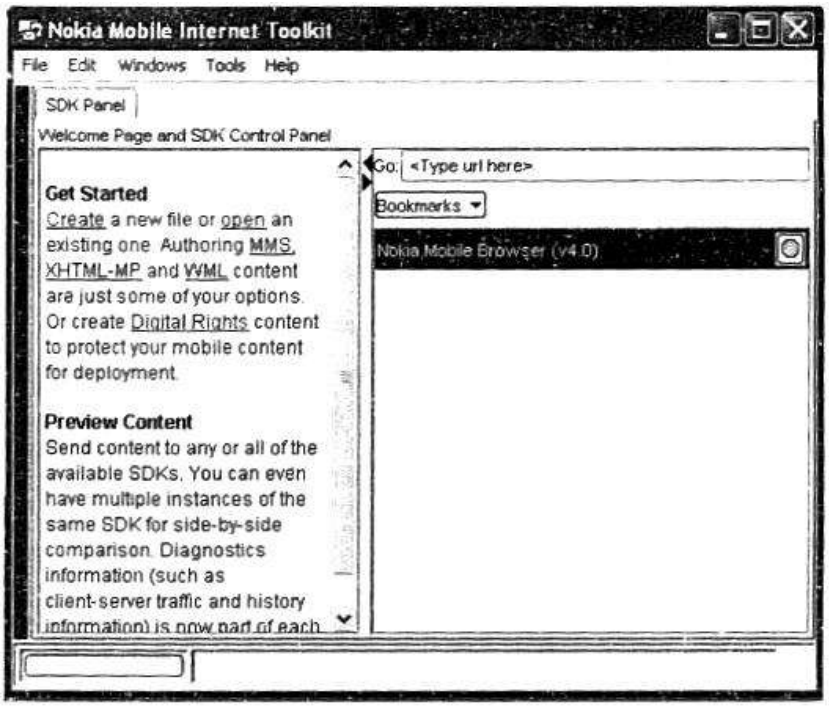
Right Editor

Soạn thảo các thứ tự trong một trình soạn thảo XML

Download Descriptor Editor

Tạo nên một Download Descriptor, dùng để mô tả nội dung để người sử dụng điện thoại có thể quyết định xem liệu nội dung này có thể được tải lên điện thoại hay không.

SDK Control Panel được dùng, đến khi bạn muốn chọn một hay nhiều bộ SDK điện thoại được cài đặt sẵn để hiển thị nội dung từ một trình soạn thảo hay từ Internet. Pannel là một thẻ nằm trên cửa sổ chính và được hiển thị như bên dưới đây.



Hình PL1. Nokia Mobile Internet Toolkit

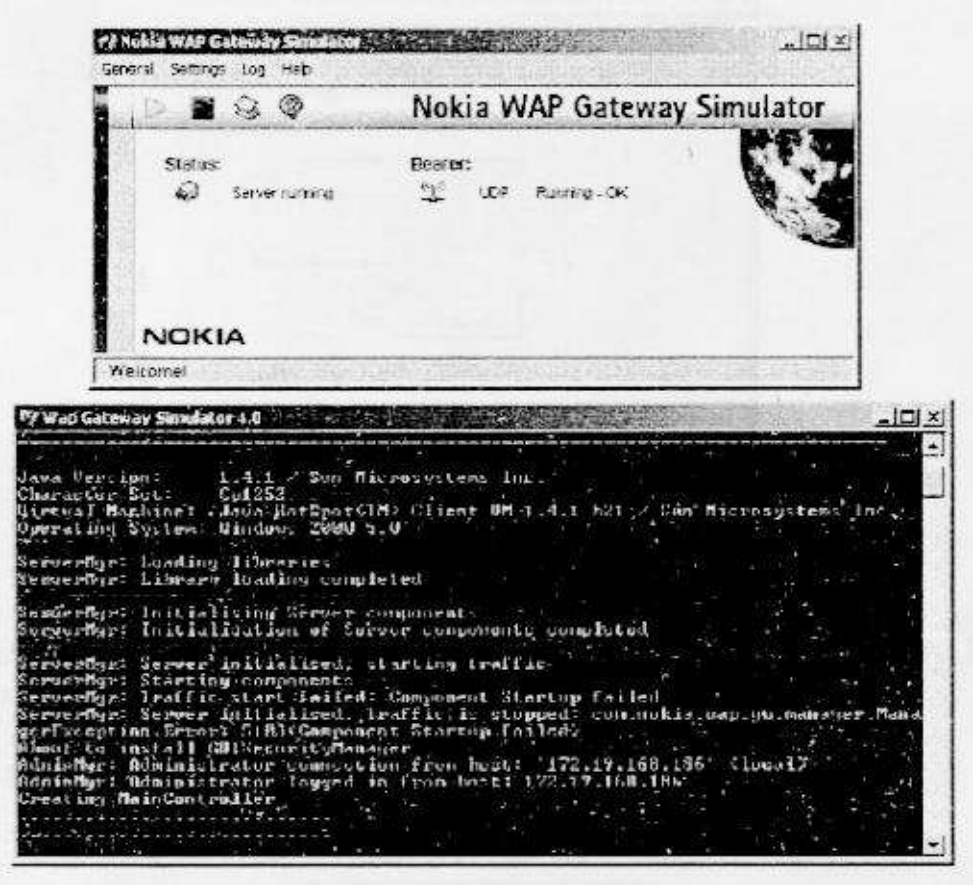
2. Nokia WAP Gateway Simulator

Nokia WAP Gateway Simulator, sau đây được đề cập đến dưới tên NWGS, là một WAP Gateway người dùng đơn dựa trên Nokia Active Server đa người dùng, không được tích hợp chung với NMIT . Khi được cài đặt trên một máy tính, NWGS cho phép người dùng trên máy tính đó có thể truy cập vào mạng Internet trên di động thông qua các chương trình giao tiếp sử dụng giao thức WAP ví dụ như Nokia Mobile Browser Simulator 4.0 SDK.

NWGS bao gồm một trình giải mã các yêu cầu đến từ các dịch vụ WAP khách, chẳng hạn như các trình giả lập điện thoại di động (SDKs) để sau đó chúng có thể được gởi tiếp qua giao thức HTTP đến các server Internet. Nó cũng gồm một trình

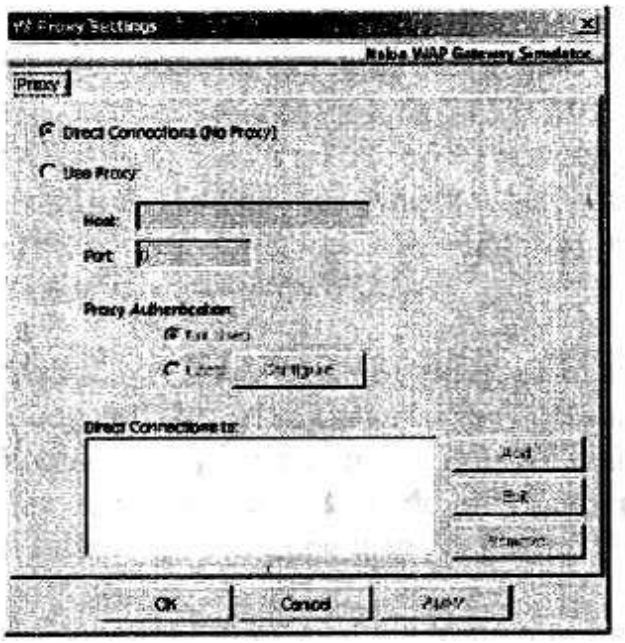
mã hoá được dùng để mã hoá các trả lời từ server (HTTP) trước khi gởi chúng về cho yêu cầu của các client.

Lúc bắt đầu chạy chương trình, NWGS hiển thị cả cửa sổ quản trị và ứng dụng chủ đang chạy trong cửa sổ Command Prompt, như hình bên dưới đây.



Hình PL2. Nokia WAP Gateway Simulator

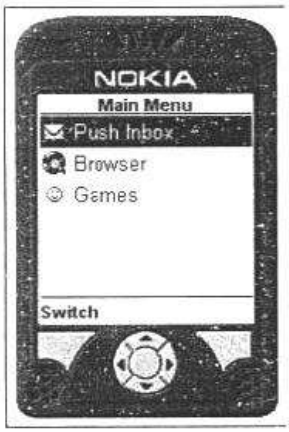
Tuỳ thuộc vào cấu hình mạng của mình, bạn có thể phải chỉ ra một HTTP proxy server. Chẳng hạn như nếu máy tính của bạn nằm bên trong một nhóm, Intranet sử dụng HTTP proxy server như là gateway để ra Internet. Nếu như thế, chọn trên menu của NWGS tuỳ chọn Setting > Proxy và sau đó nhập vào tên host và cổng cho proxy trong dialog hiển thị như bên dưới đây.



Hình PL3. Nokia WAP Gateway

Nếu bạn cần thêm thông tin về NWGS, tham khảo trong Nokia WAP Gateway Simulator User's Guide.

3. Nokia Browser Simulator.



Hình PL4. Nokia Browser Simulator

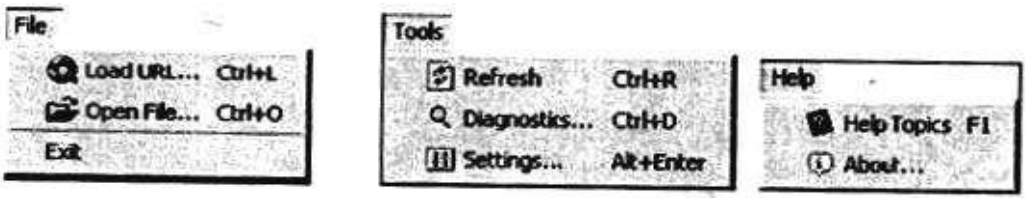
NMB là một công cụ được phát triển nhằm đến các nhà phát triển nội dung Internet trên di động, họ mong muốn xem trước phần nội dung của họ trông như thế nào trước khi nó được thử trên một điện thoại cầm tay thật.

Sử dụng NMB, các nhà phát triển nội dung có thể hiển thị bất kỳ nội dung Internet trên di động nào được phát triển dùng Nokia Mobile Internet Toolkit (NMIT), cũng như nội dung tập tin tại cục bộ và nội dung thường trú trên các server Internet và truy cập vào thông qua nối kết WAP. Các nối kết WAP có thể được hình thành thông qua WAP Gateway server hoặc qua trình giả lập WAP gateway của Nokia (NWGS).

NMB sử dụng phần mềm Nokia Mobile Browser, phần mềm này được Nokia phát triển dùng cho việc triển khai trên các điện thoại cầm tay thật. Tuy nhiên, NMB không được thiết kế tương ứng với chức năng của bất kỳ một thiết bị cầm tay riêng biệt nào mà nó chỉ mở ra một phạm vi mới cho các nhà phát triển Internet trên di động theo công nghệ hiện nay.

Nokia Mobile Browser có thể được sử dụng trong một môi trường độc lập để nạp nội dung cục bộ hay trên Internet di động. Nó có thể quản lý tất cả các dạng nội dung có thể được tạo ra trong NMIT ngoại trừ thông điệp đa truyền thông MMS.

Hệ thống Menu:



Hình PL5. Hệ thống Menu Nokia