Wimax & WiFi

Presented by
Muhibbul Muktadir Tanim
System & Database Administrator
QUBEE
mmtanim@gmail.com

Contents

WIMAX

- Overview
- Standard
- Functional Entities
- Layers
- Devices
- Support
- Mechanism / How does it work
- Architecture
- Security Enhancements
- Applications

Wi Fi

- Technology
- Standard
- Architecture
- How does it work
- Devices
- Security Enhancements

Wimax : Overview

• Worldwide Interoperability for Microwave Access

• WIMAX is an IP based, wireless broadband access technology that provides performance similar to 802.11/Wi-Fi networks with the coverage and QOS (quality of service) of cellular networks.

• Protocol that provide fixed and mobile Internet Access

• A standard based technology that enable the delivery of last mile wireless broadband access as an alternative to cable and DSL

• Provide fixed, nomadic, portable and eventually mobile wireless broadband without the need for direct LOS to base station.

• Current Wimax revision provides up to 40Mbps in typical 3-10 km base station radius

Standard

• Current Wimax revision is based upon IEEE Std 802.16e-2005.

• Actual Standard is IEEE Std 802.16d-2004, IEEE 802.16e-2005 improves upon IEEE 802.16-2004 by:

- Adding Support for Mobility
- Scaling of the Fast Fourier Transform (FFT) to the channel bandwidth
- Advanced antenna diversity schemes, and hybrid Automatic repeat-request (HARQ)
- Adaptive Antenna Systems (AAS) and MIMO Technology
- Adding an extra QOS for VOIP Applications
- Introducing downlink sub-channelization

Wimax: Network Model
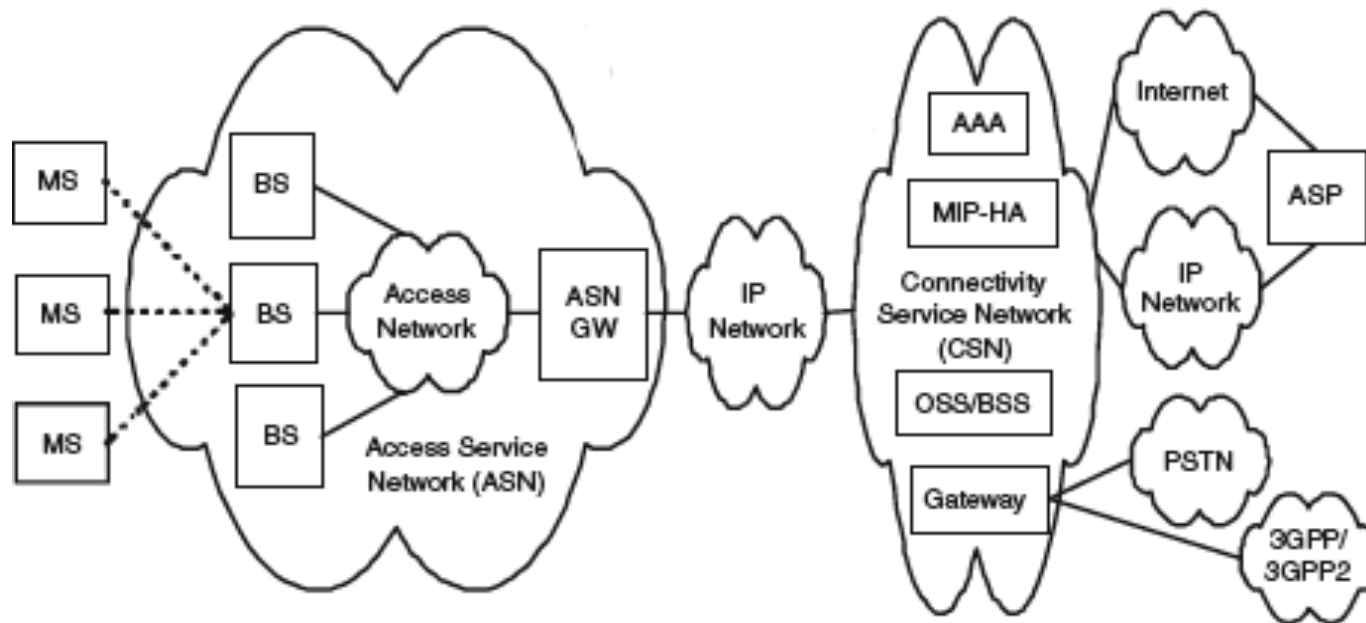
▪ Mobile Stations (MS) used by the end user to access the network.
▪ The access service network (ASN), which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.
▪ Connectivity service network (CSN), which provides IP connectivity and all the IP core network functions.

Wimax: Network Model

Functional Entities

- Base Station

- Access Service Network Gateway

- Connectivity Service Network
  - AAA
  - DHCP
  - DNS
  - HA
  - PCRF
  - Firewall/Switch/Router
  - Database

Wimax: Network Model

Functional Entities

- **Base Station**

  o Provide Air Interface to MS
  o Micro mobility Management functions such as handoff triggering and tunnel establishment
  o Radio Resource Management
  o QOS Policy enforcement
  o Traffic Classification
  o Key Management, Session Management
  o Multicast Group Management

Wimax: Network Model

Functional Entities

- **Access Service Network Gateway**

  - o Act as Layer 2 traffic aggregation point within Access Service Network area
  - o Intra ASN Location Management and Paging
  - o Radio Resource Management and Admission Control
  - o Caching of Subscriber profiles and encryption keys
 - o AAA Client functionality
  - o Routing to the Selected CSN

Wimax: Network Model

Functional Entities

- **Connectivity Service Network**

    - Authorize, Authenticate and Accounting
    - Connectivity to the Internet or other Networks
    - User Policy Management and Rating
    - QOS Confirmation
    - IP Resolution
    - IP Address Management
    - Location Management between different ASN's
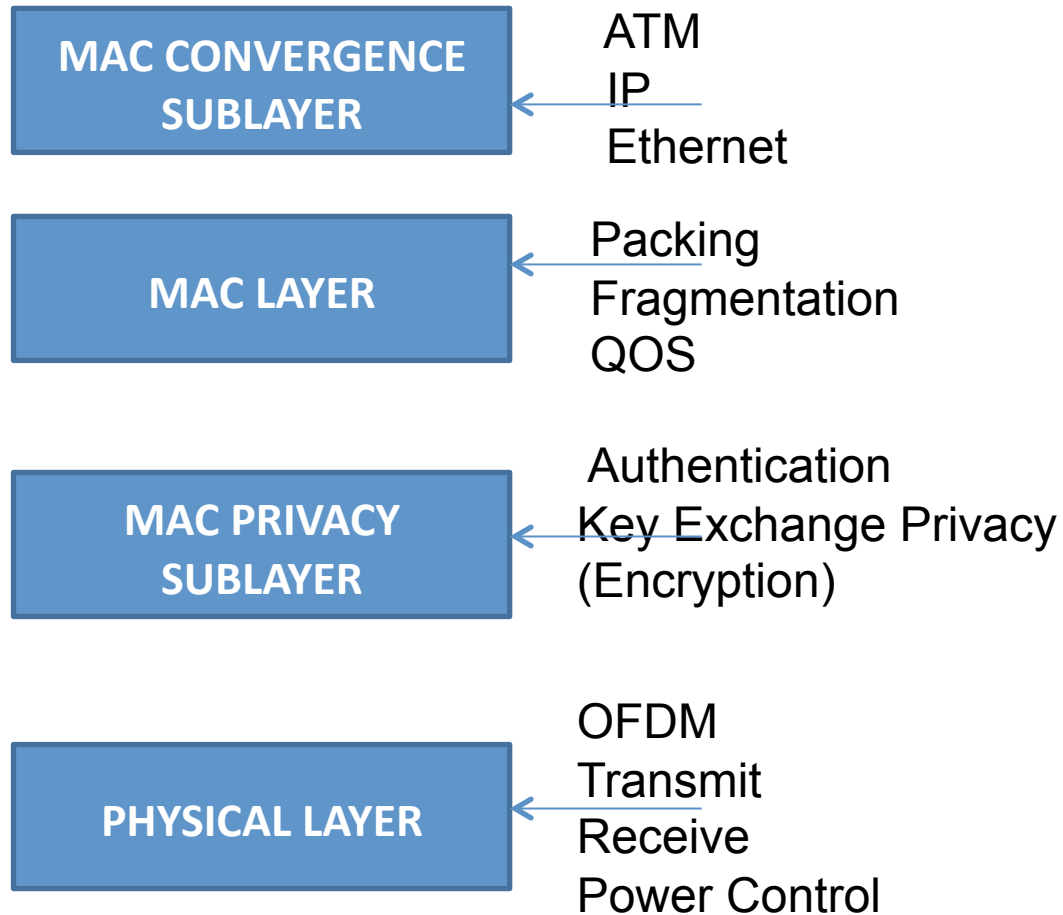
Network Reference Model
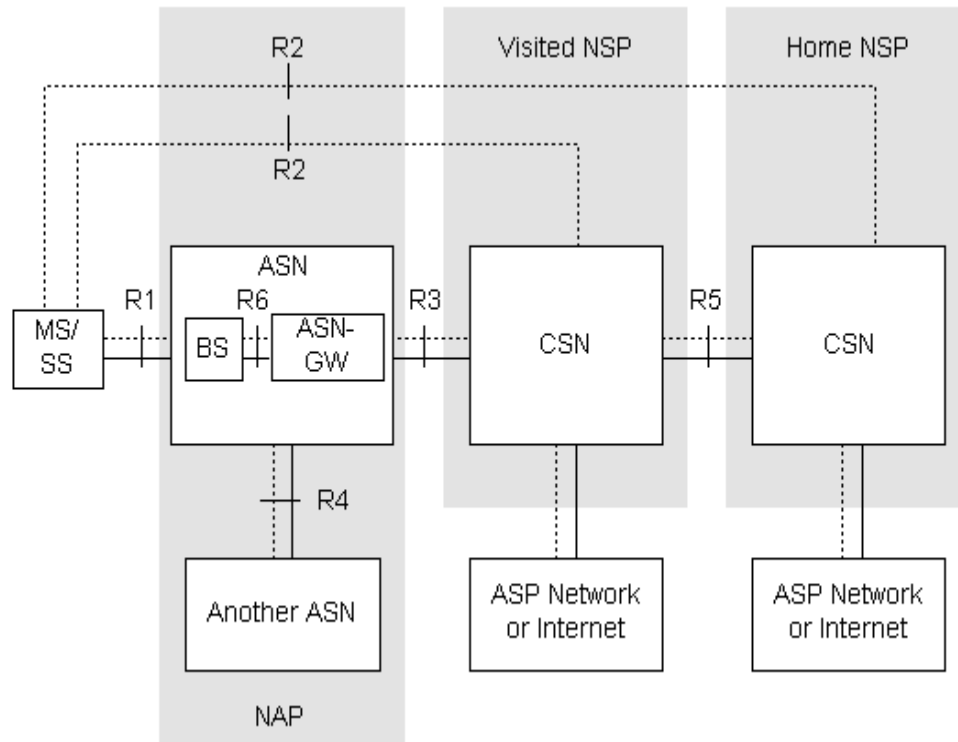
Logical Interfaces

• R1 indicates the air interface between the ASN and an MS

• R2 indicates the logical interface between an MS and a CSN.

• R3 indicates the logical interface between ASN and CSN

• R4 Indicates between ASN GWs

• R5 indicates between CSN and home CSN

• R8 indicates interface between BSs.

Wimax Technology

The design of WiMAX network is based on the following major principles:

- **Spectrum** . able to be deployed in both licensed and unlicensed spectra.

- **Topology** . supports different Radio Access Network (RAN) topologies.

- **Interworking** . independent RAN architecture to enable seamless integration and interworking with WiFi, 3GPP and 3GPP2 networks and existing IP operator core network.

- **IP connectivity** . supports a mix of IPv4 and IPv6 network interconnects in clients and application servers.

- **Mobility management** . possibility to extend the fixed access to mobility and broadband multimedia services delivery.

WIMAX LAYERS

MAC CONVERGENCE SUBLAYER

ATM
IP
Ethernet

MAC LAYER

Packing
Fragmentation
QOS

MAC PRIVACY SUBLAYER

Authentication
Key Exchange Privacy
(Encryption)

PHYSICAL LAYER

OFDM
Transmit
Receive
Power Control
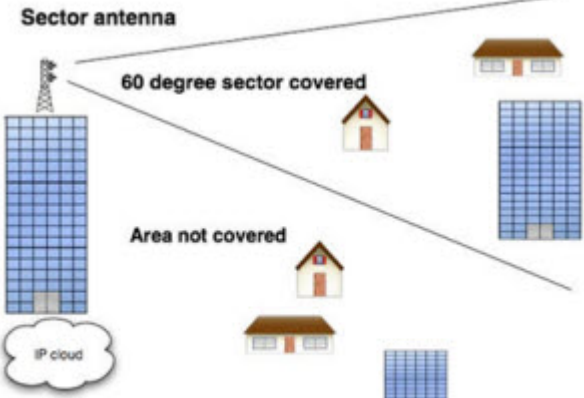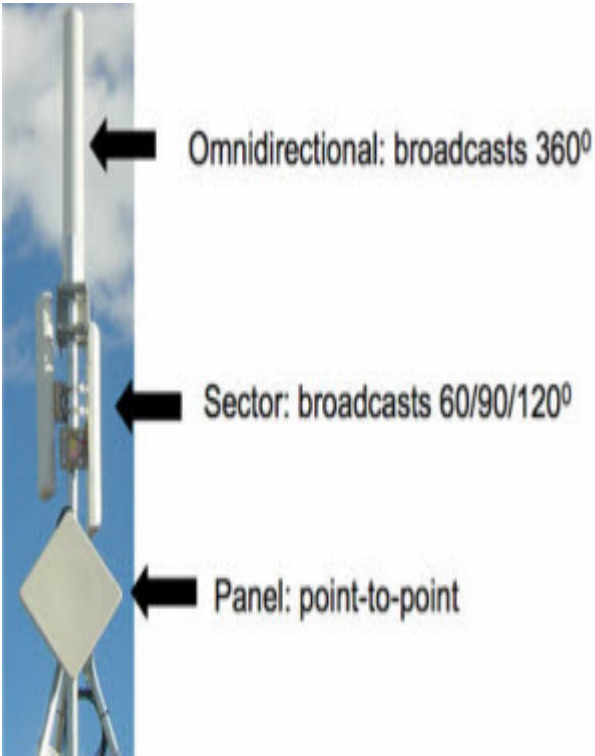
Wimax Physical Layer

- Based on orthogonal frequency division multiplexing (OFDM)

- OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications and is used by a variety of commercial broadband systems

- OFDM is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment.

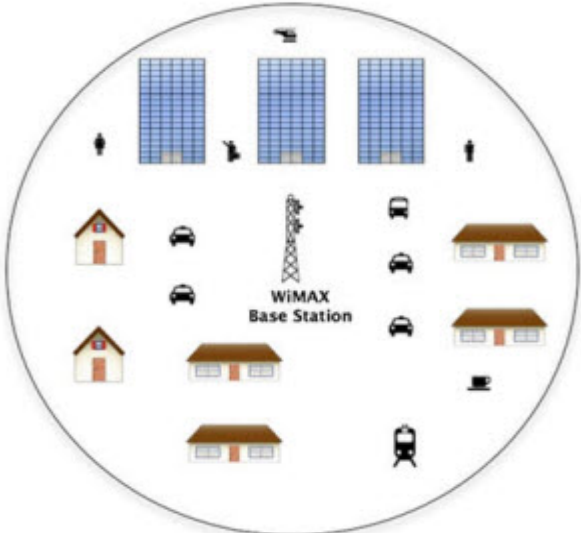|	Downlink	Uplink
Modulation	BPSK, QPSK, 16 QAM, 64 QAM; BPSK optional for OFDMA-PHY	BPSK, QPSK, 16 QAM; 64 QAM optional
Coding	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6
	Optional: convolutional turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC, RS-Codes for OFDM-PHY	Optional: convolution turbo codes at rate 1/2, 2/3, 3/4, 5/6; repetition codes at rate 1/2, 1/3, 1/6, LDPC

Wimax MAC Layer

- The IEEE 802.16 MAC was designed for point-to-multipoint broadband wireless access applications.

- Provide an interface between the higher transport layers and the physical layer.

- MAC service data units (MSDUs).and organizes them into MAC protocol data units (MPDUs) for transmission over the air.

- Broadcast and multicast support.

- Manageability primitives.

- High-speed handover and mobility management primitives.

- Three power management levels, normal operation, sleep and idle.

- Header suppression, packing and fragmentation for efficient use of spectrum.

WIMAX Antennas

Omnidirectional: broadcasts 360⁰

Sector: broadcasts 60/90/120⁰

Panel: point-to-point

Sector antenna

60 degree sector covered

Area not covered

IP cloud

Sector Antenna

WiMAX Base Station

OMNI Directional Antenna

Panel Antenna

Subscriber Stations

Outdoor CPE device

▪ maximize reception via a line of sight connection to the base station not possible with indoor CPE

Indoor CPE device

▪ Instant Installation by the Users

Wimax Mobility Support

WiMAX envisions four mobility-related usage scenarios :

▪ **Nomadic**: The user is allowed to take a fixed subscriber station and reconnect from a different point of attachment.

▪ **Portable**: Nomadic access is provided to a portable device, such as a PC card, with expectation of a best-effort handover.

▪ **Simple mobility**: The subscriber may move at speeds up to 60 kmph with brief interruptions (less than 1 sec) during handoff.

▪ **Full mobility:** Up to 120 kmph mobility and seamle
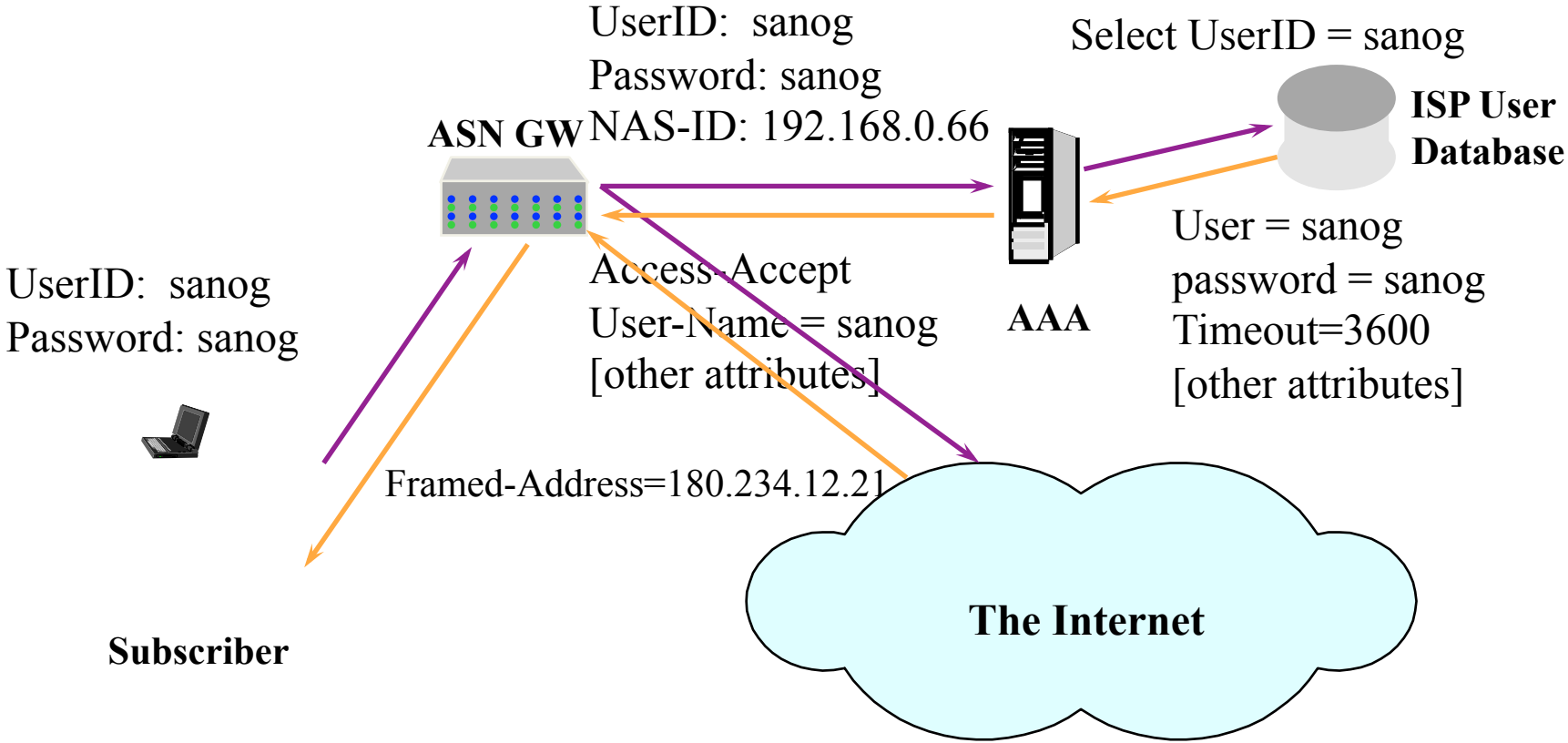
Wimax Authentication

Access Control system has three elements:

1. An entity that desires to get access: the supplicant.
2. An entity that controls the access gate: the authenticator.
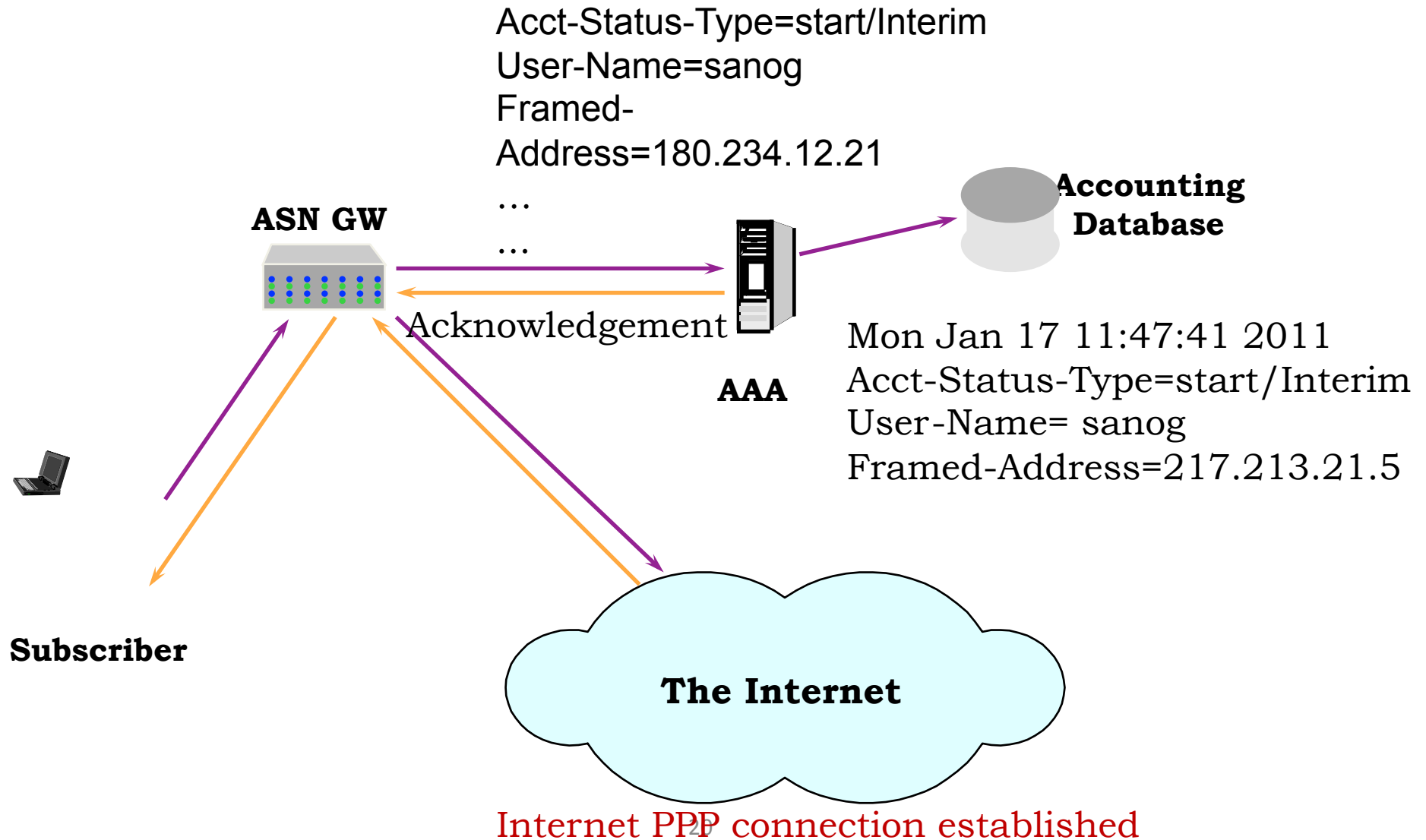3. An entity that decides whether the supplicant should be admitted: the authentication server.

Protocol

- PPP [Password Protected Protocol]
- RADIUS [Remote Dial In User Service]
- PAP [Password Authentication Protocol]
- EAP [Extensible Authentication Protocol]
- CHAP [Challenge Handshake Authentication Protocol]
- EAP-TLS [Extensible Authentication Protocol Transport Layer Security]
-

Basic Authentication Flow
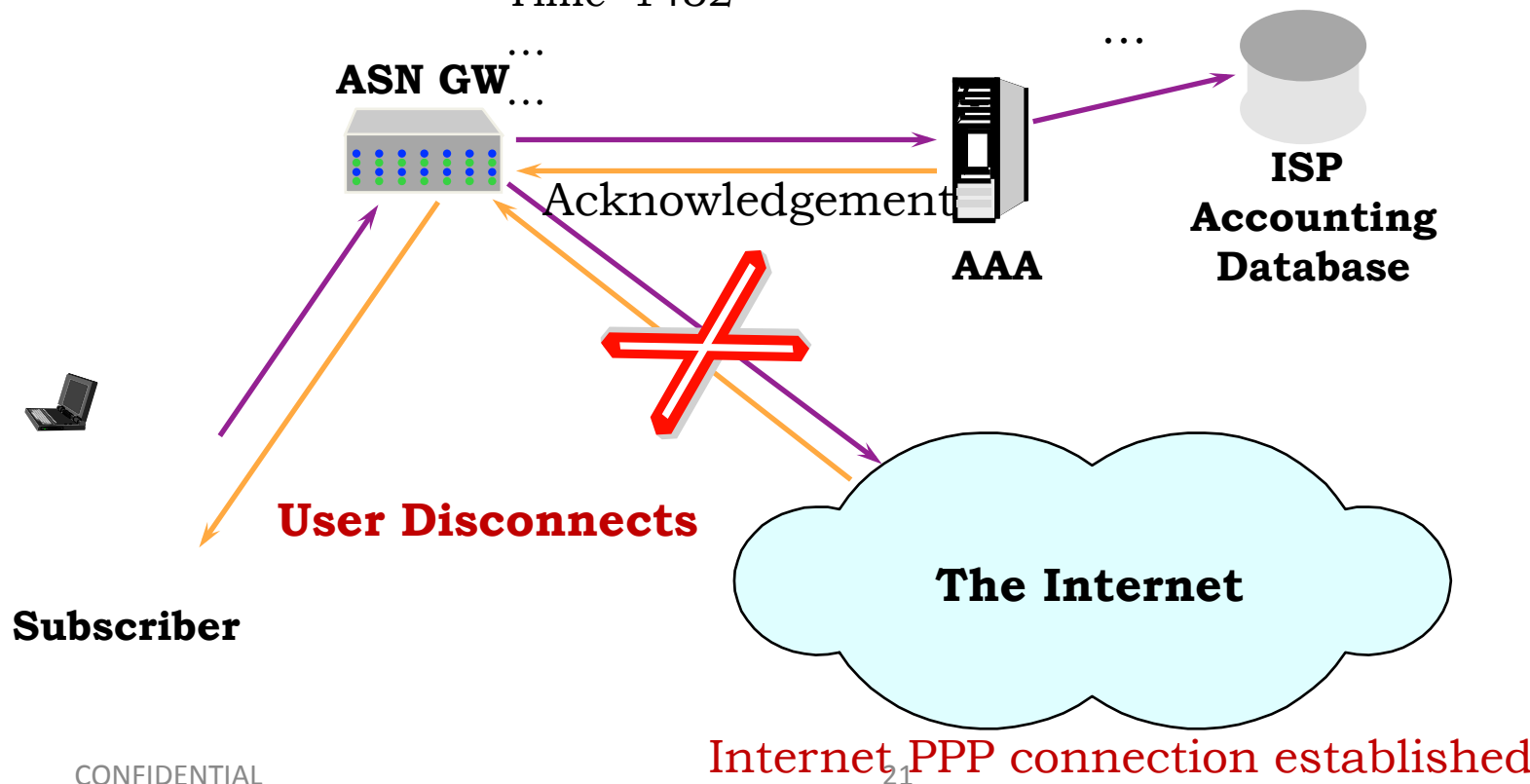
Basic Accounting Flow

Acct-Status-Type=start/Interim
User-Name=sanog
Framed-
Address=180.234.12.21
…
…

ASN GW

**Accounting
Database**

Acknowledgement

AAA

Mon Jan 17 11:47:41 2011
Acct-Status-Type=start/Interim
User-Name= sanog
Framed-Address=217.213.21.5

Subscriber

The Internet

Internet PPP connection established
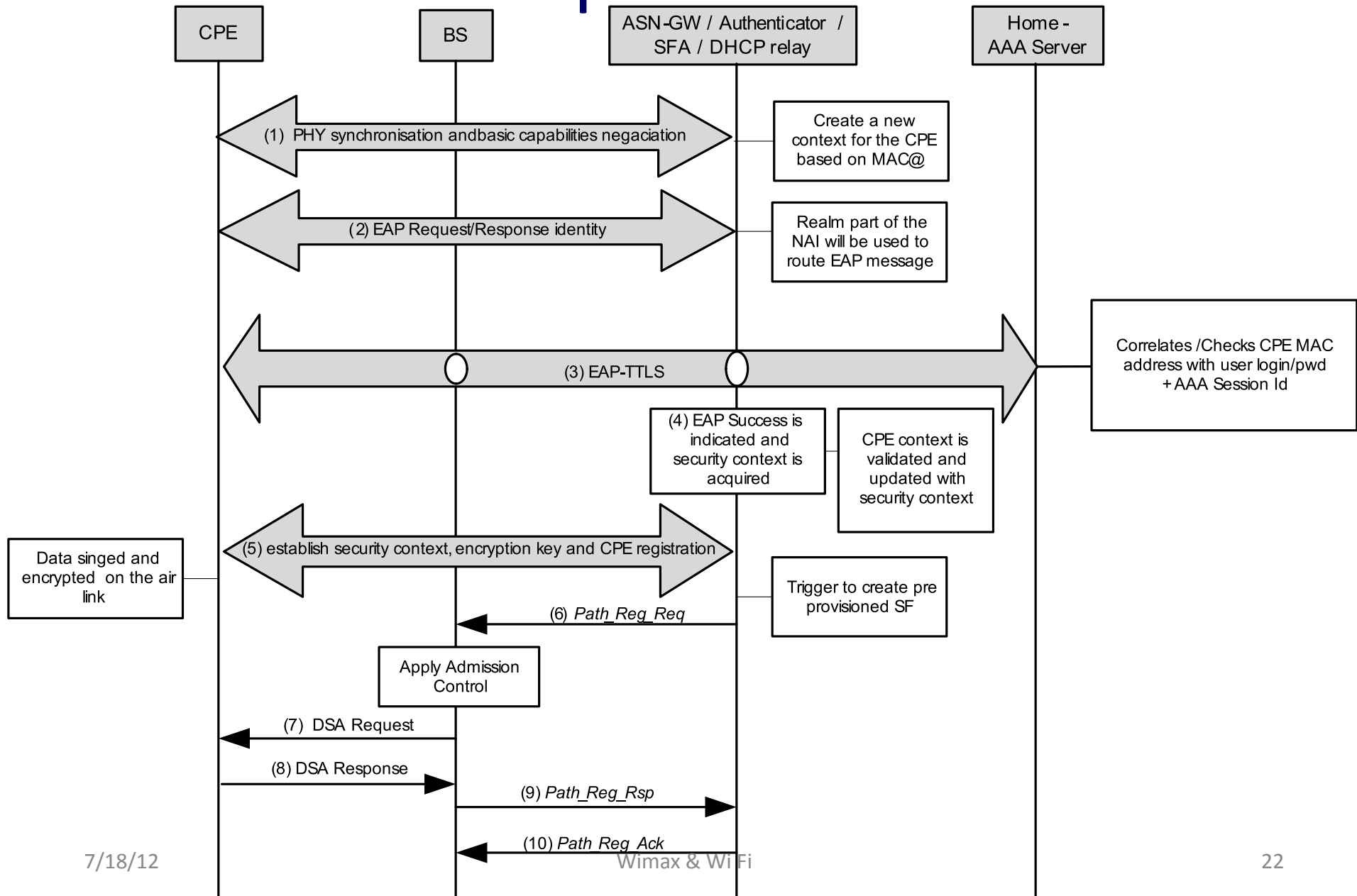
Basic Accounting Flow

Mon Jan 17 11:50:41 2011
    Acct-Status-Type=Stop
    User-Name=sanog
    Acct-Session-Time=1432
    …
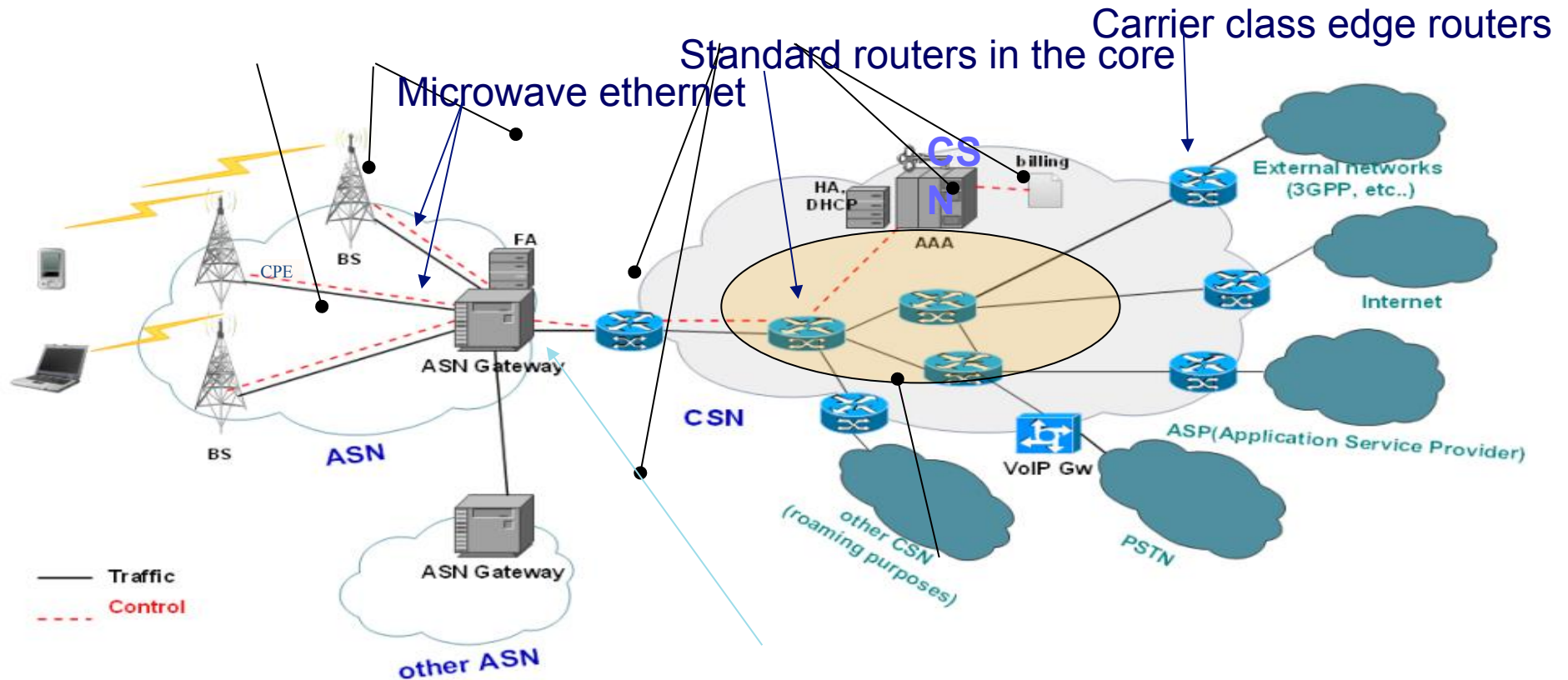   …

Acct-Status-Type=Stop
User-Name=sanog
Acct-Session-Time=1432
…
…

ASN GW

Acknowledgement

AAA

ISP Accounting Database

User Disconnects

The Internet

Subscriber

Internet PPP connection established

21

21

control plane 802.16e

CPE | BS | ASN-GW / Authenticator / SFA / DHCP relay | Home - AAA Server

(1) PHY synchronisation andbasic capabilities negaciation

Create a new context for the CPE based on MAC@

(2) EAP Request/Response identity

Realm part of the NAI will be used to route EAP message

(3) EAP-TTLS

Correlates /Checks CPE MAC address with user login/pwd + AAA Session Id

(4) EAP Success is indicated and security context is acquired

CPE context is validated and updated with security context

(5) establish security context, encryption key and CPE registration

Data singed and encrypted on the air link

Trigger to create pre provisioned SF

(6) Path_Reg_Req

Apply Admission Control

(7) DSA Request

(8) DSA Response

(9) Path_Reg_Rsp

(10) Path_Reg_Ack

802.16e-2005 basic architecture

Carrier class edge routers

Standard routers in the core

Microwave ethernet

May need router co-located with ASN
Manufacturer dependent

ASN : Access Service Network
CSN : Core Service Network
CPE : Customer Premises Equipment
AAA : Authentication, Accounting, Authorization
FA: foriegn agent
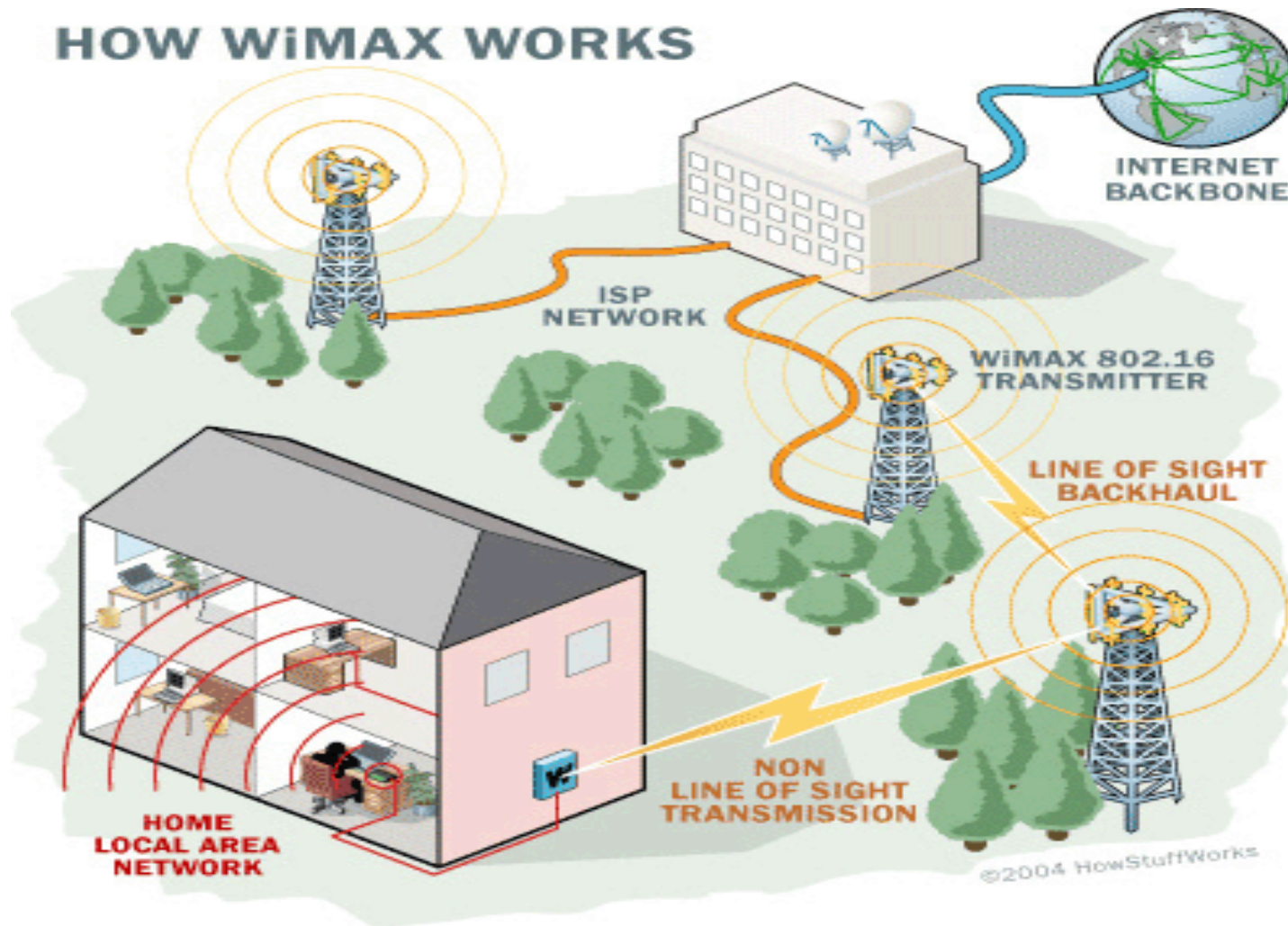HA : Home Agent
DHCP : Dynamic Host Configuration Protocol

Access Network

- Data Centric Network based on the IP Technology
- Different from voice-centric mobile communications network
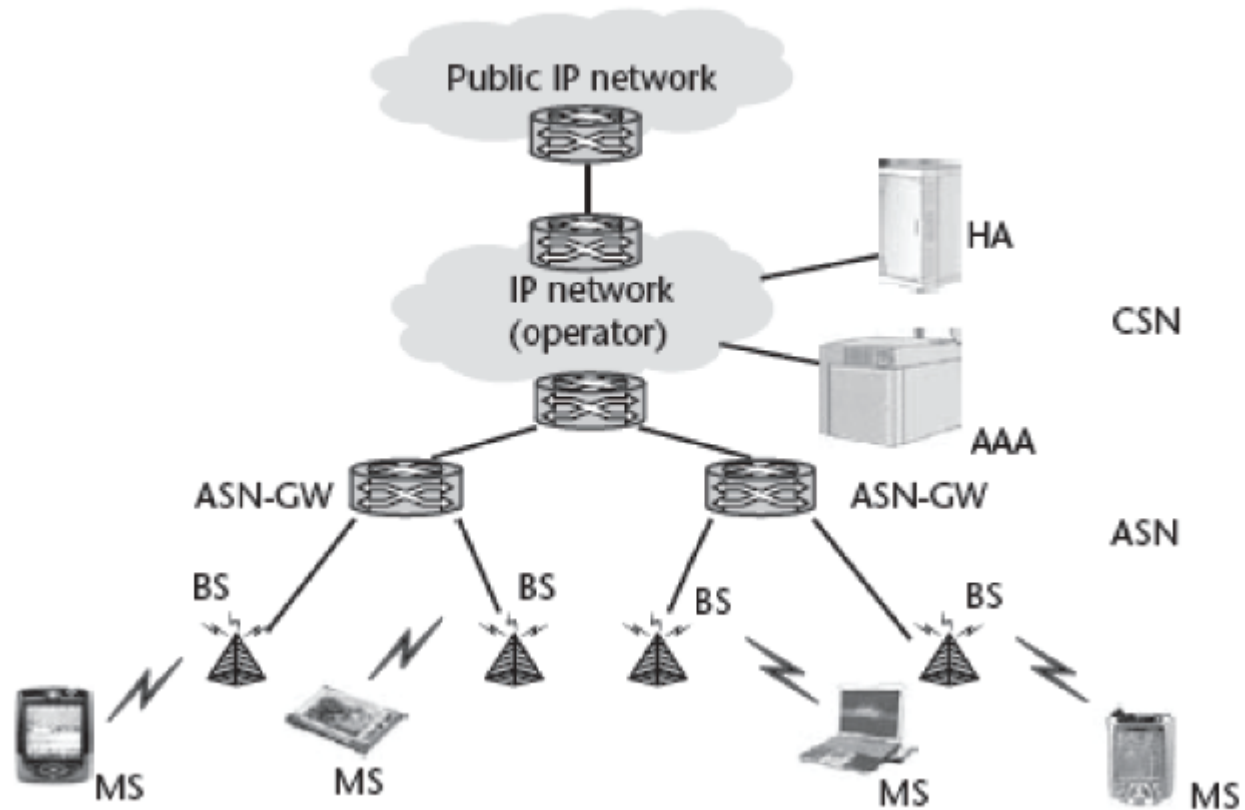
How Wimax Works

How Wimax Works

•   When a user send data from a subscriber device to a base station then that base station broadcast the wireless signal into channel which is called uplink and base station transmit the same or another user is called downlink.

• The base station of Wimax has higher broadcasting power, antennas and enhanced additional algorithms.

• When signal transmit form user to wimax base station or base to user (wimax receiver) the wireless channel faces many attenuation such as fraction, reflection, refraction, wall obstruction etc.

• OFDMA that prohibit interfering and be multiplexed also makes possible power prioritization for various sub carriers according to the link quality.

• Wimax is providing quality of service (Wimax QoS) which enables high quality of data like VoIP or TV broadcasts.

•   WiMAX technology support various protocol such as VLAN, ATM, IPv4 Ethernet etc.

Wimax Wi Fi Hotspot

SSL Secured Authentication for Wireless LAN Users
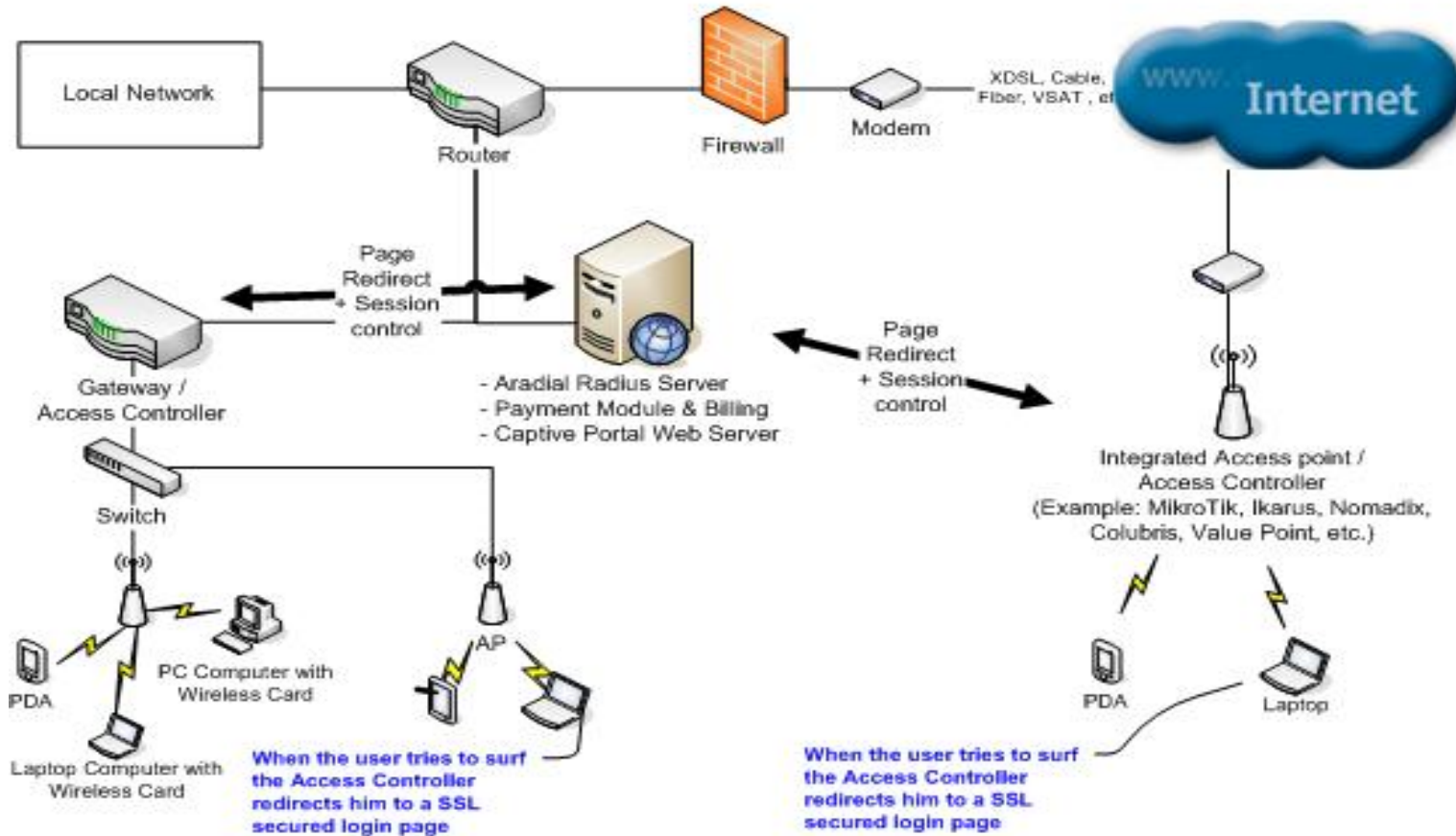
Security Enhancements

- Will the wireless protocol provide adequate security to prevent theft of service, thus protecting their investment in the wireless infrastructure?

- Encryption connection between BS and MS.

- Incorporation of two stage security: X.509 in the authentication process and 56-bit DES for the service flow

- Certificate File loaded into CPE which is verified by CSN AAA

- Lock with operator code so that it will not scan other frequency.

WIMAX Applications

• Portable broadband connectivity across cities through variety of devices.

• Wireless alternative for DSL and cable

• Providing data communications (VOIP) and IPTV Service (Tripple Play)

• Providing source of Internet connectivity as part of a business continuity plan

• Enterprise Data Service

• Peer to Peer access

• Varieties VAS

Access Network: Wifi

• Describes only narrow range of connectivity ensuring Wireless Local Area Network

• IEEE 802.11 Standard

• Establish and enforce standards for Interoperability and backward compatibility

Certification Process

o Requires conformance to the IEEE 802.11 radio standard
o WPA and WPA2 Security standards
o EAP Authentication standard

The Wi-Fi Technology

Wi-Fi Networks use Radio Technologies to transmit & receive data at high speed:

- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11g

IEEE 802.11b

- Appear in late 1999

- Operates at 2.4GHz radio spectrum

- 11 Mbps (theoretical speed) - within 30 m Range

- 4-6 Mbps (actual speed)

- 100 -150 feet range

- Most popular, Least Expensive

- Has 11 channels, with 3 non-overlapping

- Interference from mobile phones and Bluetooth devices which can reduce the transmission speed.

IEEE 802.11a

- Introduced in 2001
- Operates at 5 GHz (less popular)
- 54 Mbps (theoretical speed)
- 15-20 Mbps (Actual speed)
- 50-75 feet range
- More expensive
- Not compatible with 802.11b

IEEE 802.11g

- Introduced in 2003
- Combine the feature of both standards (a,b)
- 100-150 feet range
- 54 Mbps Speed
- 2.4 GHz radio frequencies
- Compatible with 'b'

Wi-Fi

- Channel Pollution

  ▪ Use of 2.45 GHz range is common in Bluetooth, ZigBee , WPAN-CSS etc
  ▪ Cause significant additional interference

- Network Security

  ▪ Simplified access compare to Wire
  ▪ Enabling wireless connectivity provides and attack vector, particularly if the network uses inadequate or no encryption.
  ▪ DNS spoofing attack

Wi-Fi

- Security Methods

  ▪ Service Set Identifier (SSID) is common but unproductive because SSID is broadcast in the clear in response to client SSID query.

  ▪ Allow computers with known MAC is also inefficient because MAC spoofing is a common hacking tool now.

  ▪ Wired Equivalent Policy (WEP) was designed to protect again casual snooping, but now deprecated as AirSnort or Aircrack-ng can quickly recover WEP encryption keys

Wi Fi Security Standards

- Wi-Fi Protected Access (WPA) is a certification program developed by the Wi-Fi alliance to secure wireless computer Networks

- Builds upon WEP (Wired Equivalent Privacy)

- WPA2 encryption standard is ratified by IEEE and still considered secure, as of 2009

- WPA comes in two flavors, that is WPA-802.1x and WPA-PSK.

- The Wi-Fi alliance has announced the inclusion of additional EAP (Extensible Authentication Protocol) types to its certification programs for WPA- and WPA2

Wi-Fi Network Architectures

- AP-based topology (Infrastructure Mode)

- Peer-to-peer topology (Ad-hoc Mode)

- Point-to-multipoint bridge topology

AP-based topology

- The client communicate through Access Point.
- BSA-RF coverage provided by an AP.
- ESA-It consists of 2 or more BSA.
- ESA cell includes 10-15% overlap to allow roaming.
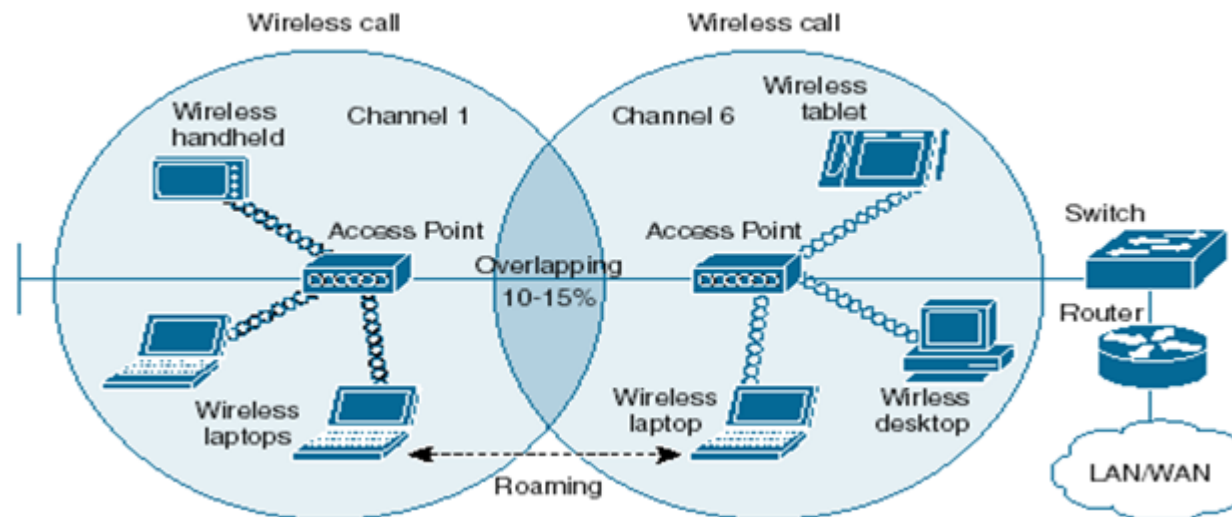
BSA – Basic Service Area
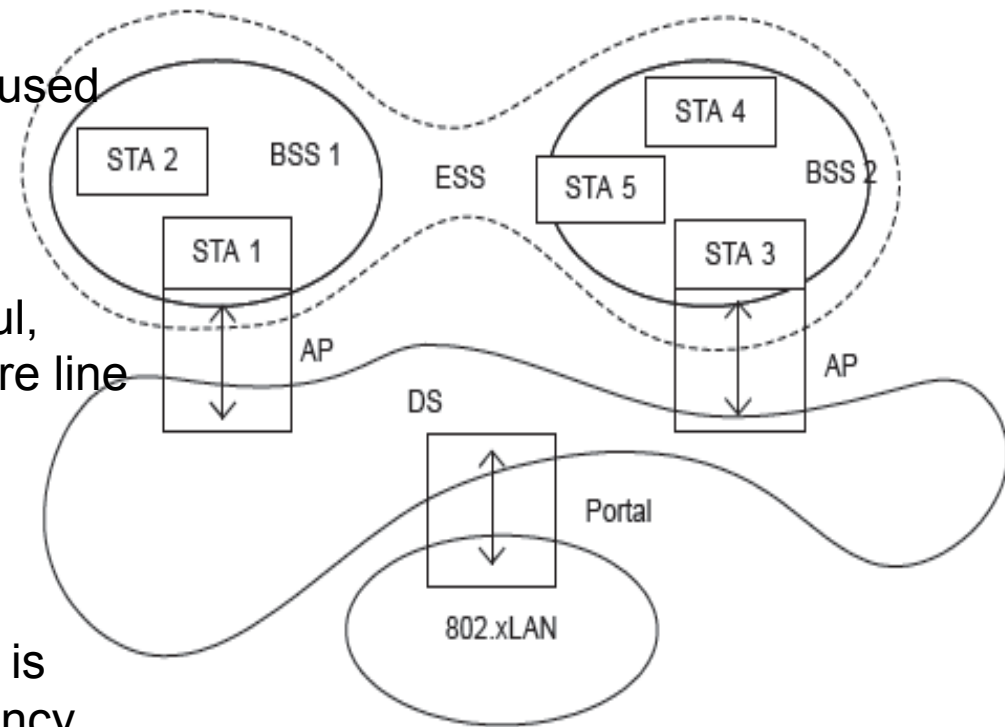ESA – Extended Service Area

Ad Hoc Topology

- AP is not required.
- Client devices within a cell can communicate directly with each other.
- It is useful for setting up of a wireless network quickly and easily.
- The scope of the 802.11 protocols is limited only up to the layer-2 MAC
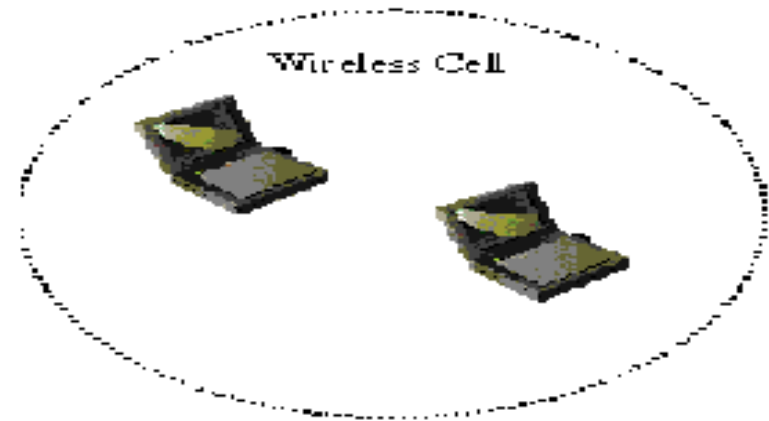
Enterprise Network

• WLAN with two AP's through DS

• DS represents a conceptual system used to interconnect a set of BSSs and integrated LANs to create an ESS

• One can interpret a DS as a backhaul, which is typically constructed using wire line (IEEE 802.3) or using 802.11 itself.

• An ESS is identified by a SSID

• To reduce co channel interference, it is desired to use non overlapping frequency channels for immediate Ap's.


BSS – Basic Service Set   STA – Station
ESS – Extended Service Set   DS -- Distribution System

Layer-2 & 3 with 802.11

• IEEE 802.1D-2004 MAC bridge allows communication between end stations attached to separate LANs, which could be of different kinds [802.11 and 802.3]

• Illustrates the relationship among router, bridge, and AP, where a layer-3 router connects two subsets.

• Each subset is composed of a single bridge; two Aps.

• End-to-end path is composed of two layer-3 hops and six layer-2 hops.
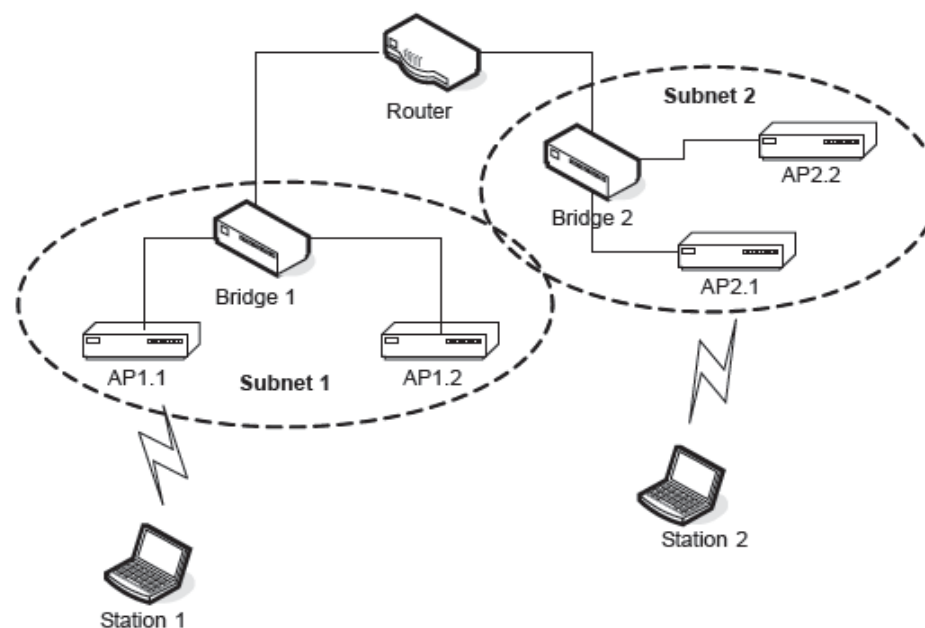
Router versus bridge

How a Wi-Fi Network Works

- Basic concept is same as Walkie talkies.

- A Wi-Fi hotspot is created by installing an access point to an internet connection.

- An access point acts as a base station.

- When Wi-Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.

- A single access point can support up to 30 users and can function within a range of 100 – 150 feet indoors and up to 300 feet outdoors.

- Many access points can be connected to each other via Ethernet cables to create a single large network.

- Has fairly high power battery consumption compare to Bluetooth and ZigBee

Elements of a WI-FI Network

- Access Point (AP) - The AP is a wireless LAN transceiver or "base station" that can connect one or many wireless devices simultaneously to the Internet.

- Wi-Fi cards - They accept the wireless signal and relay information.They can be internal and external.(e.g PCMCIA Card for Laptop and PCI Card for Desktop PC)

- Safeguards - Firewalls and anti-virus software protect networks from uninvited users and keep information secure.
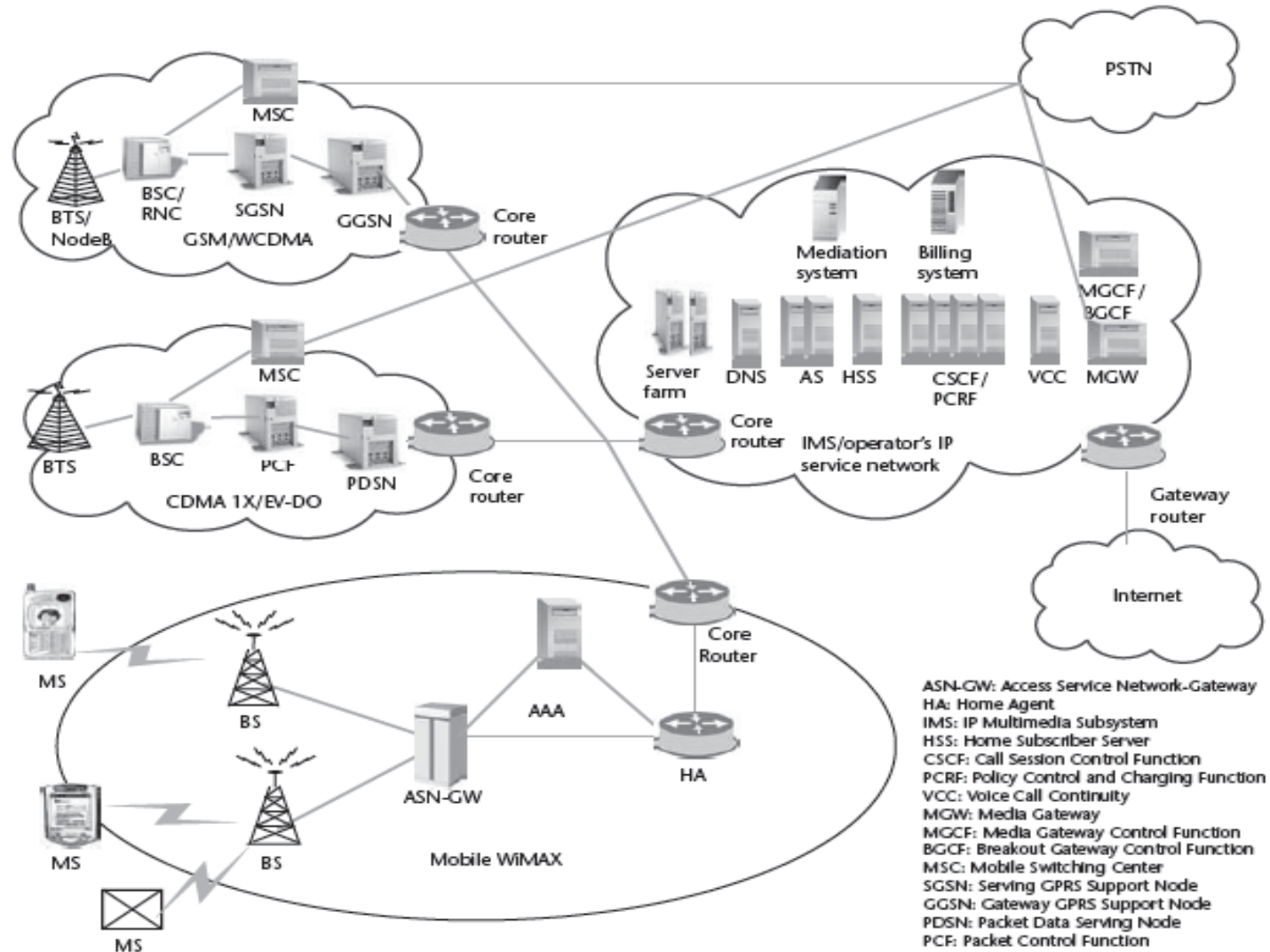
How to Secure Wi Fi

- Use Encryption:

  Encryption standards: WEP, WPA and WPA2
- Change Default account names and passwords.
- Segment the Network
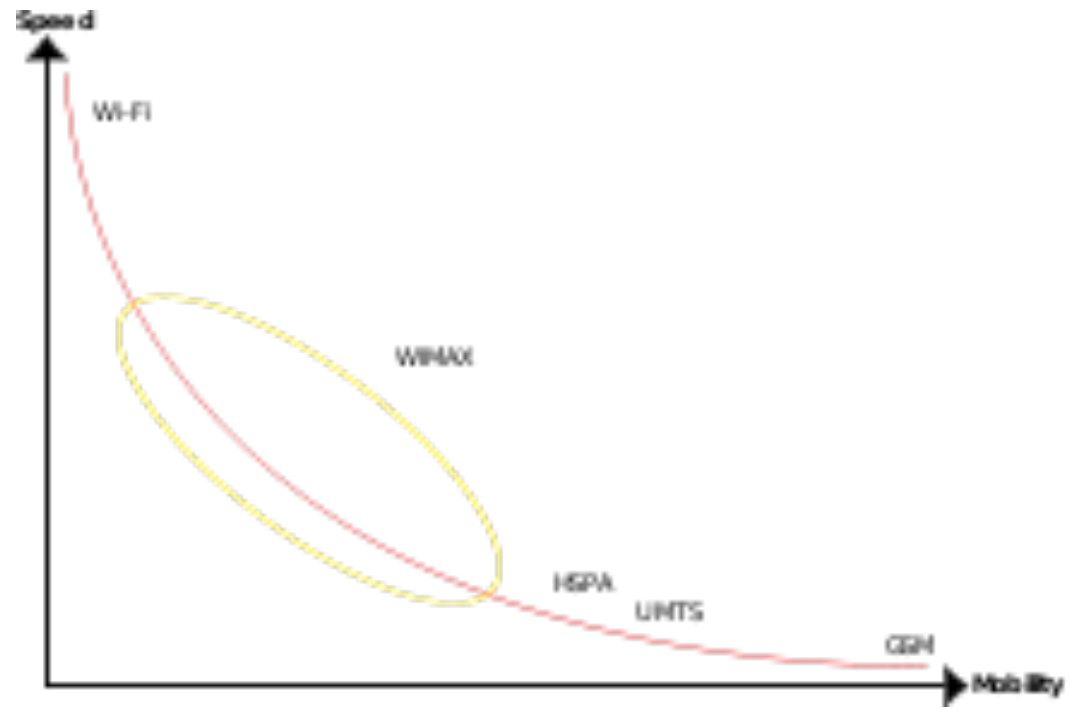- Authenticate users
- Update the firmware

Wi Fi and Wimax Difference

- Cost, Speed, Distance

- Wimax is quiet MAN but Wi Fi is LAN

- Wimax network execute a connection oriented MAC while Wifi runs on the CSMA/CA protocol, which is wireless and strife based.

- Wimax network providing QoS (Quality of Service) therefore a large number of people get access to tower at the same time. The built in algorithm automatically transfer the user to other tower or cell of Wimax station. Unlike WiFi user have to sort of fight to stay on connected with a specified access point.

Mobile Wimax to Cellular Mobile Network Interworking

SPEED vs MOBILITY

THANK YOU