WiMAX & Wi-Fi

Presented by
Muhibbul Muktadir Tanim
Assistant Manager
IT Infrastructure & Operations
QUBEE
mmtanim@gmail.com

Contents

- Standard Overview

Wi Fi

- Overview
- IEEE Standard
- 2.4 GHz Channel Distribution
- Security Standard
- Network Architecture
- How does it work
- Elements
- Security Enhancements
- WiMAX - Wi-Fi Internetworking
- WiMAX – Wi-Fi Hotspot

WIMAX

- Overview
- Functional Entities
- IEEE Standard & Improved Features
- Layers
- Principles
- Devices
- Network Reference Model
- Technical Features
- Mechanism / How does it work
- Architecture
- Security Enhancements
- Applications

- Comparison between WiMAX & Wi-Fi
- Deployment & Implementation Experience
- Operational Challenge

Standard Overview

802:11b to 102.16e

• The evolution of wireless LAN started with the introduction of the 802.11b standard in 1999.

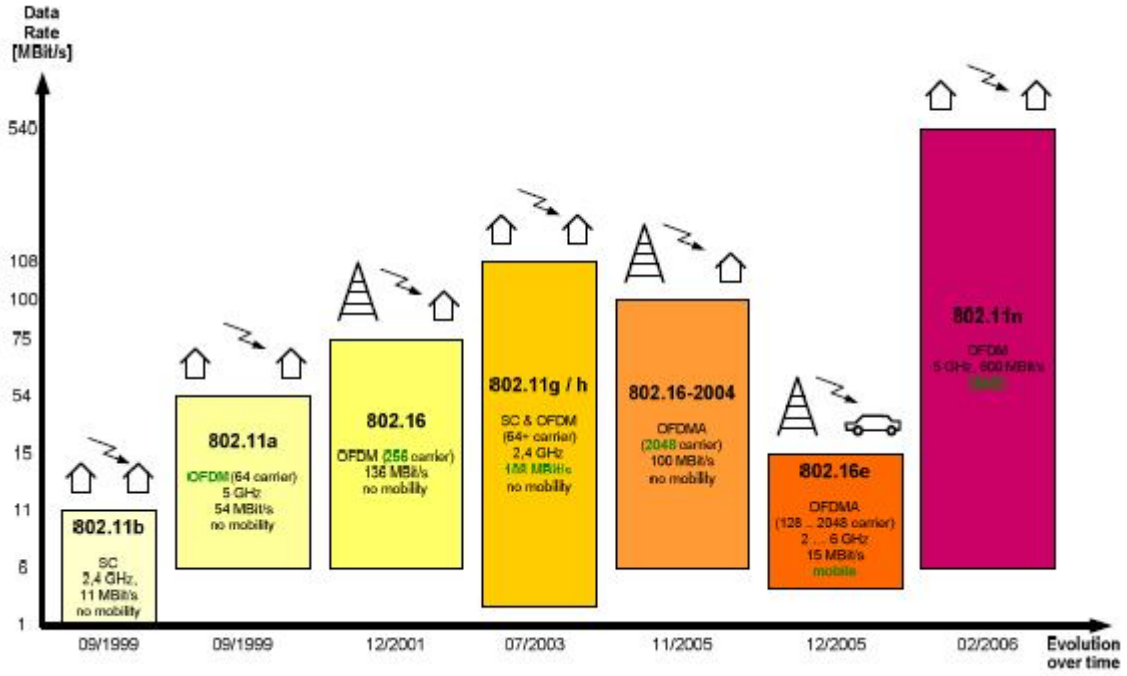
• In the same year, the 802.11a started introduced the Orthogonal Frequency Division Multiplexing (OFDM).

• In 2003, "the best" of both standards were joined to the 802.11g standard.

• While all former standards were used for "small networks" with no network operator required (SOHO), the first 802.16 standard, which was introduced at the end of 2001, provided an operator-based standard.

Standard Overview

802:11b to 102.16e



Wi-Fi

- Overview
- IEEE Standard
- 2.4 GHz Channel Distribution (Non-Overlap)
- Security Standard
- Network Architecture
- How does it work
- Elements
- Security Enhancements
- WiMAX - Wi-Fi Internetworking
- WiMAX – Wi-Fi Hotspot

Wi-Fi : Overview

- 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

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

Wi-Fi : IEEE Standard

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

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

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

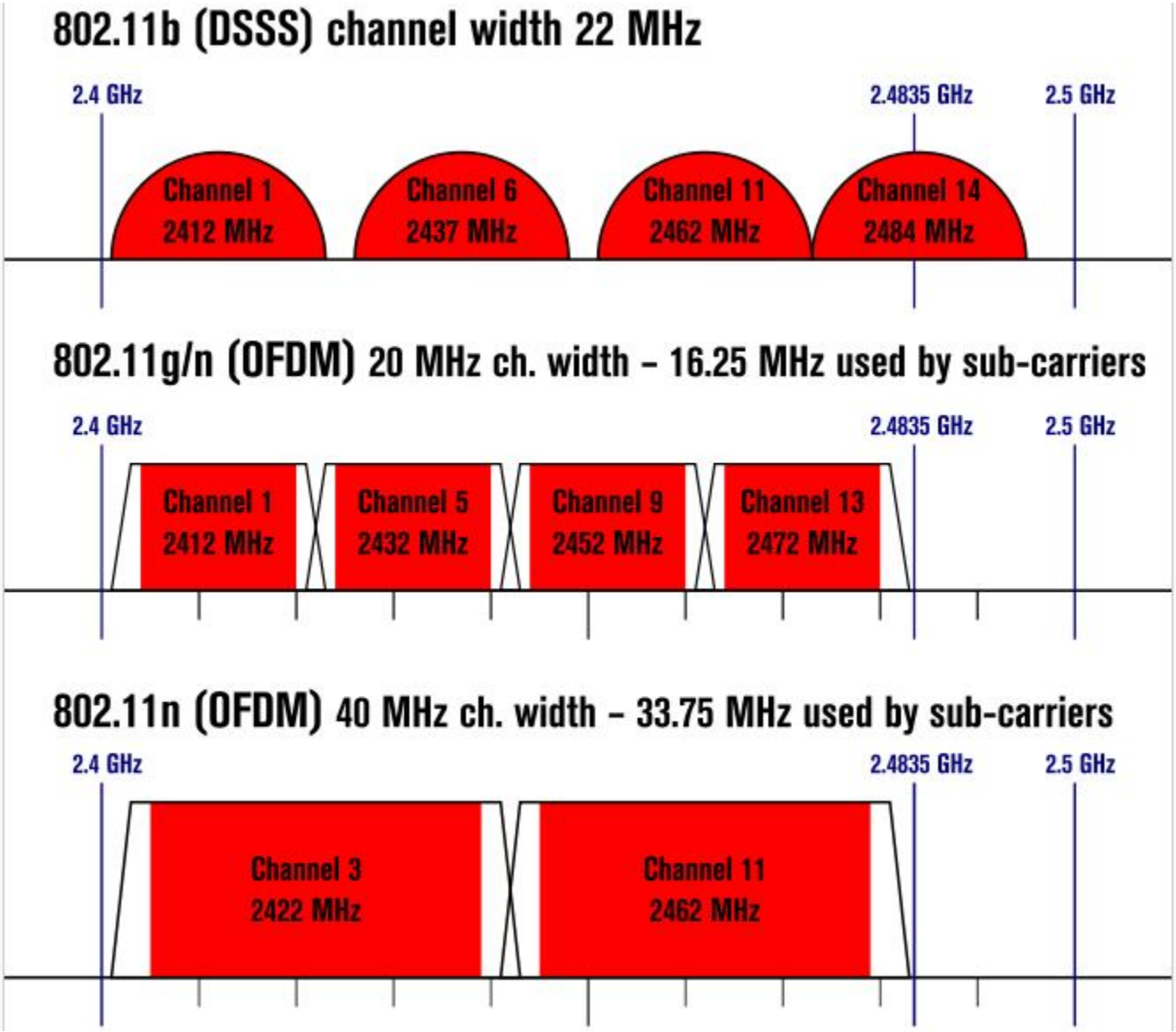
IEEE 802.11g

- 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’

IEEE 802.11n

- Introduced in 2009
- Improve Network throughput over 802.11a and 802.11g
- 175 feet range
- 300 Mbps speed
- Multiple Input Multiple Output (MIMO) added
- 40 MHz channels to the PHY (physical layer), and frame aggregation to the MAC layer
- 2.4/5 GHz radio frequencies

Non Overlapping Channels for 2.4GHz WLAN



Wi-Fi : Security Standard

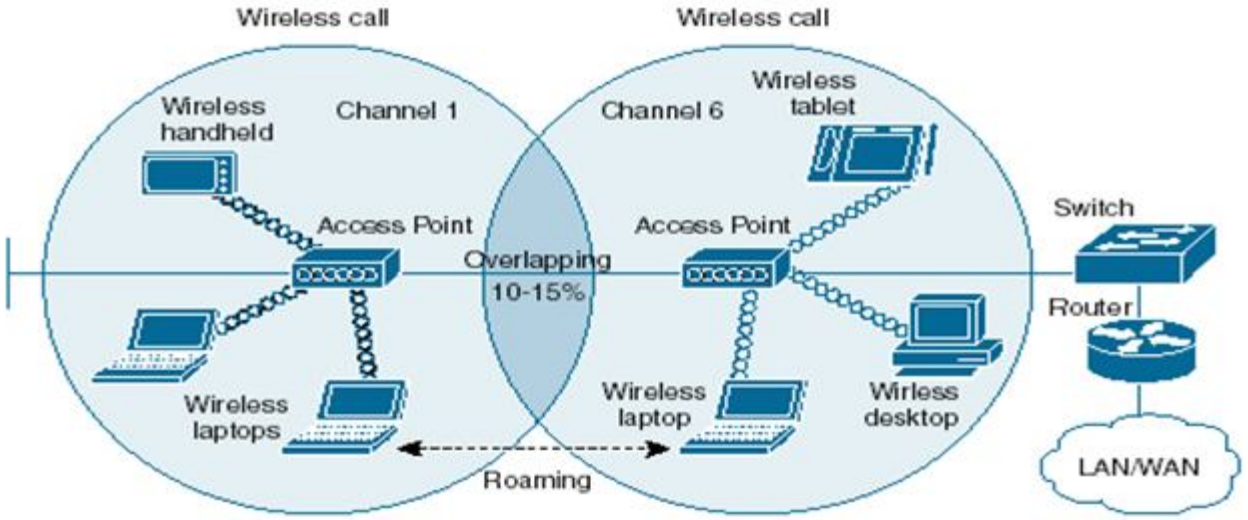
- Wi-Fi Protected Access (WPA) is a certification program developed by the Wi-Fi alliance to secure wireless computer Networks
- Builds upon WEP (Wired Equivalent Privacy)
- WPA2 encryption standard is ratified by IEEE and still considered secure, as of 2009
- WPA comes in two flavors, that is WPA-802.1x 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

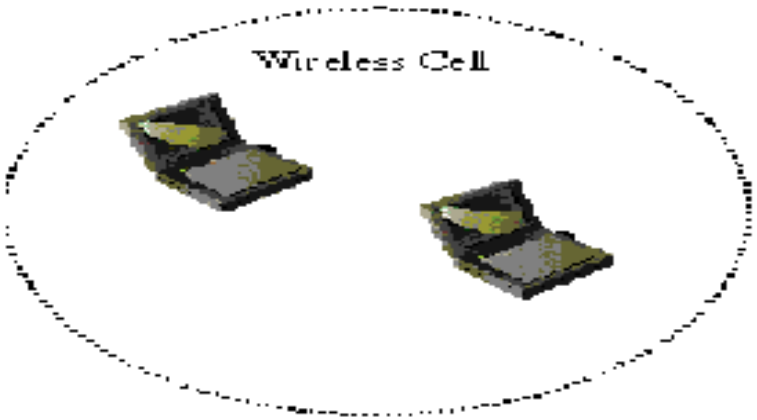
- The client communicate through Access Point.
- BSA-RF coverage provided by an AP.
- ESA-It consists of 2 or more BSA.
- ESA cell includes 10-15% overlap to allow roaming.



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



Point to Multi-point (Enterprise) Network

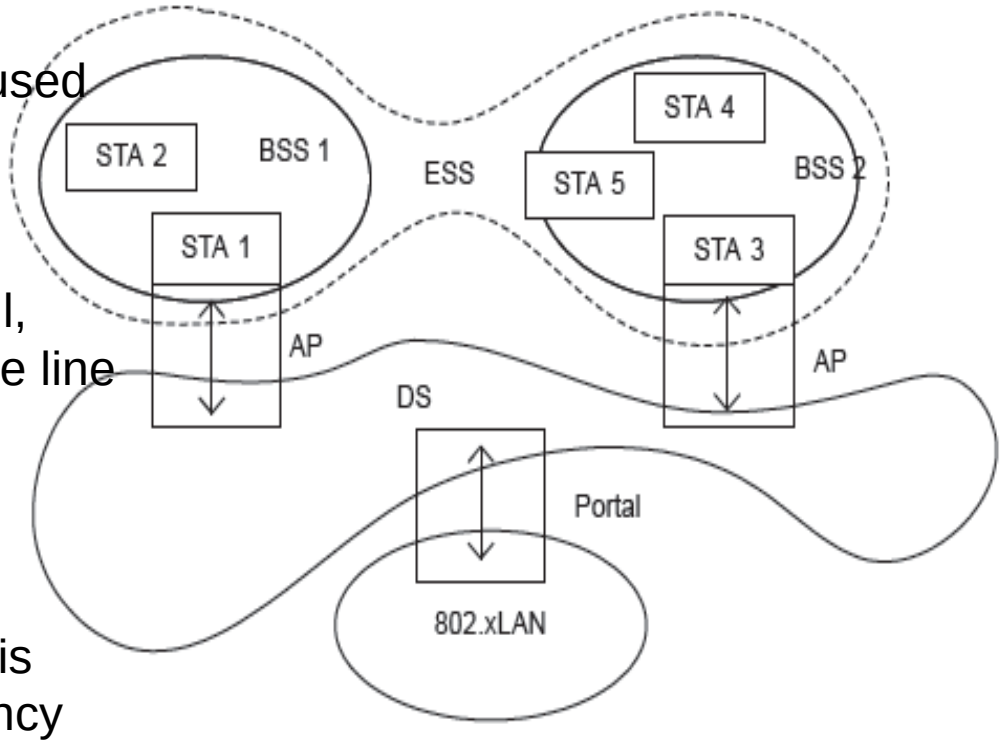
• WLAN with two AP's through DS

• 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
ESS – Extended Service Set
STA – Station
DS -- Distribution System

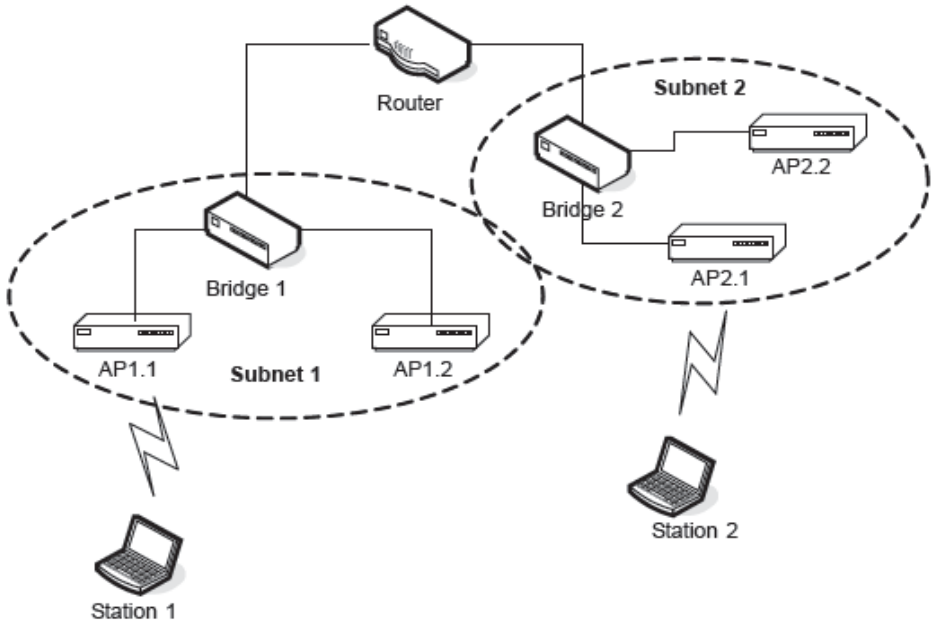
Layer-2 & 3 with 802.11

• 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)

- Safe guards - Firewalls and anti-virus software protect networks from uninvited users and keep information secure.

Security Enhancements

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

Security Enhancements

- 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

Security Enhancements

- 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

WIMAX

- Overview
- Functional Entities
- IEEE Standard & Improved Features
- Layers
- Principles
- Devices
- Network Reference Model
- Technical Features
- Mechanism / How does it work
- Architecture
- Security Enhancements
- Applications

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 & Improved Features

- 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
  - Adaptive Antenna Systems (AAS) and MIMO Technology
  - Adding an extra QOS for VOIP Applications
  - Introducing downlink sub-channelization

Functional Entities

- Base Station (Access Network)
- Access Service Network Gateway
- Connectivity Service Network
  - AAA
  - DHCP
  - DNS
  - HA
  - PCRF
  - Firewall/Switch/Router
  - Database

Functional Entities

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

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

Functional Entities

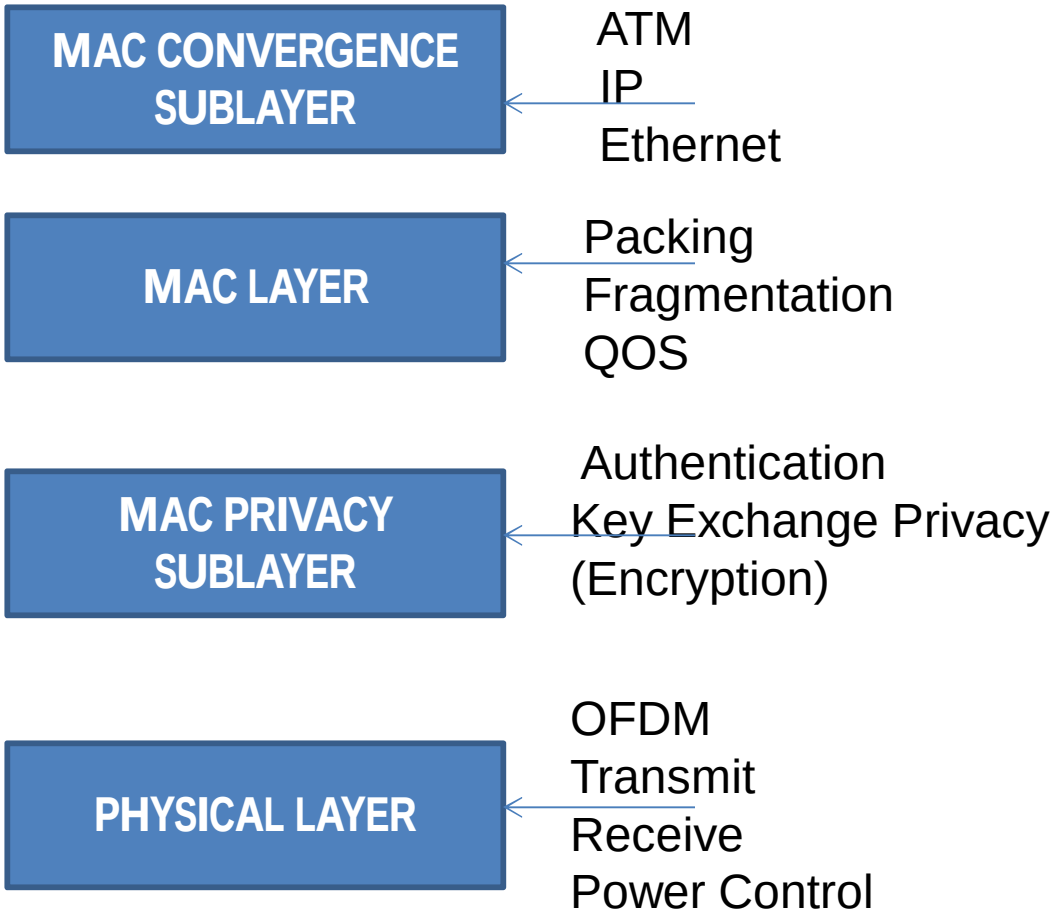
- **Connectivity Service Network**
  - Authorize, Authenticate and Accounting
  - Connectivity to the Internet or other Networks
  - User Policy Management and Rating
  - QOS Confirmation
  - IP Resolution
  - IP Address Management
  - Location Management between different ASN’s

WiMAX: Principles

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



WiMAX Physical Layer

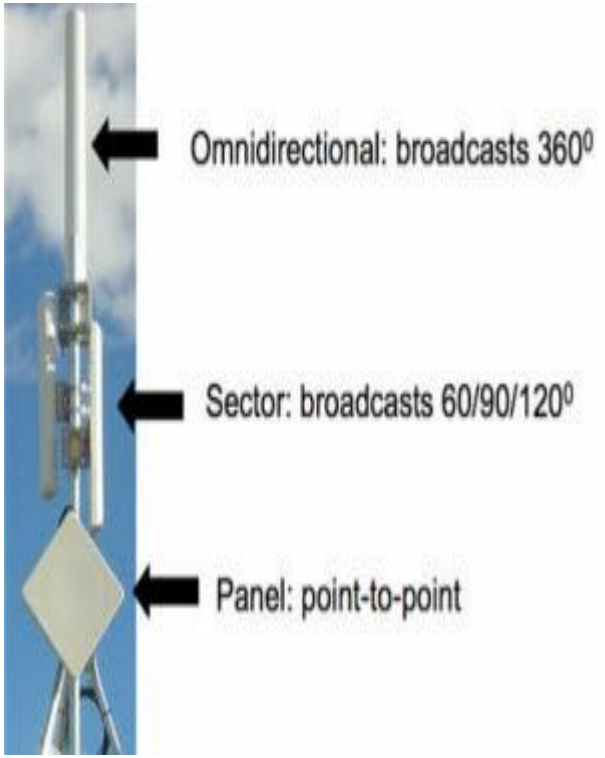
- Based on orthogonal frequency division multiplexing (OFDM)
- OFDM is the transmission scheme of choice to enable high-speed data, video, and multimedia communications and is used by a variety of commercial broadband systems
- OFDM is an elegant and efficient scheme for high data rate transmission in a non-line-of-sight or multipath radio environment.

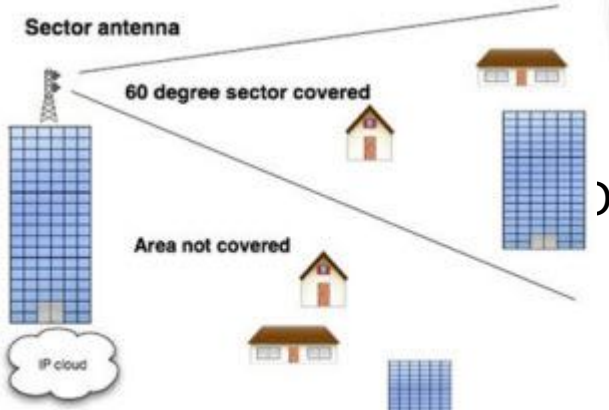
	Downlink	Uplink
Modulation	BPSK, QPSK, 16 QAM, 64 QAM; BPSK optional for OFDMA-PHY	BPSK, QPSK, 16 QAM; 64 QAM optional
Coding	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6	Mandatory: convolutional codes at rate 1/2, 2/3, 3/4, 5/6
	Optional: convolutional turbo codes at rate 1/2, 2/3, 3/4,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

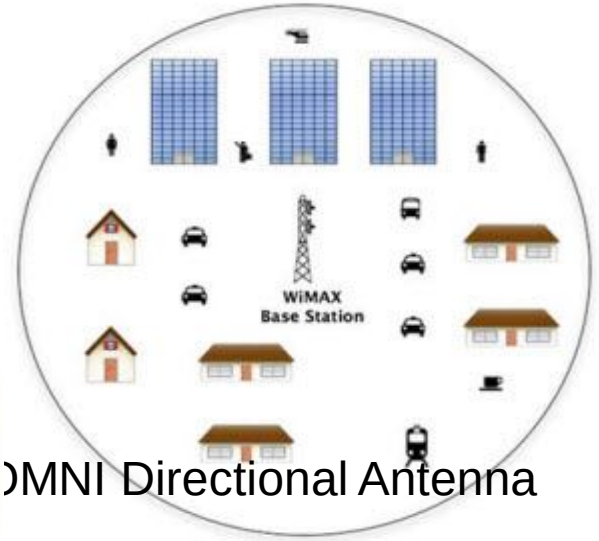
- The IEEE 802.16 MAC was designed for point-to-multipoint broadband wireless access applications.
- Provide an interface between the higher transport layers and the physical layer.
- MAC service data units (MSDUs).and organizes them into MAC protocol data units (MPDUs) for transmission over the air.
- 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 Devices: Antenna





Sector Antenna



)MNI Directional Antenna

Panel Antenna

WIMAX Devices: Subscriber Stations

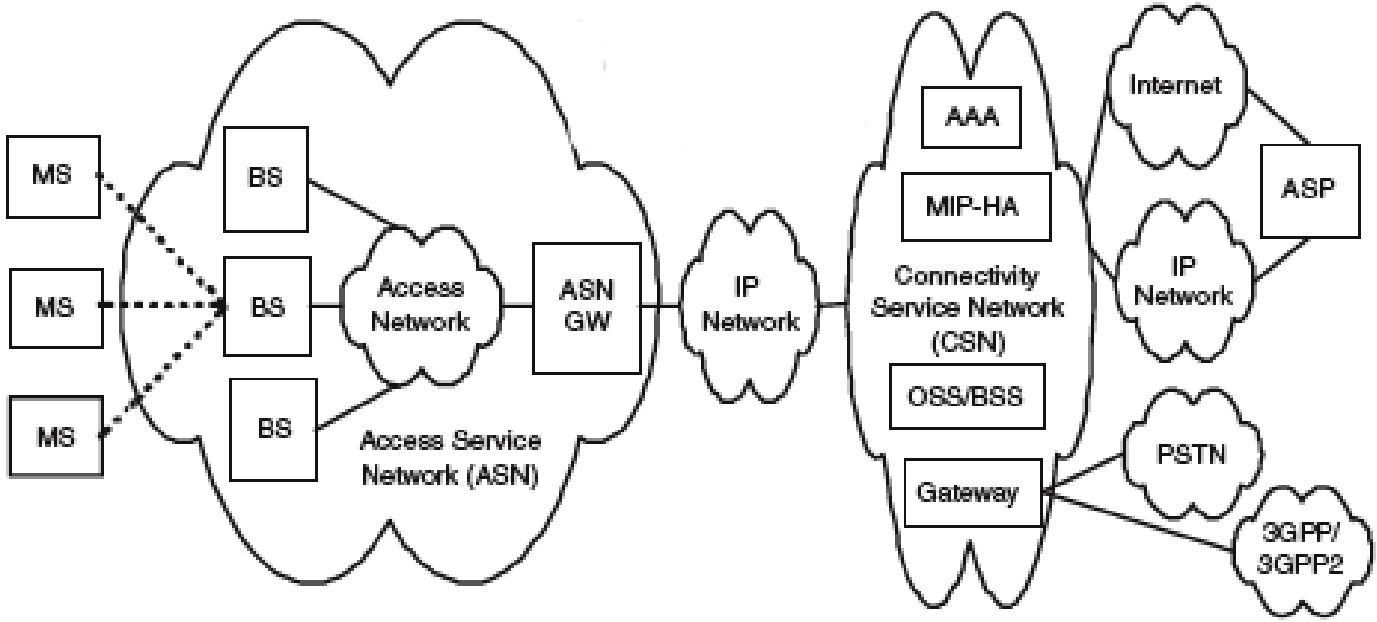
Outdoor CPE device

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

Indoor CPE device

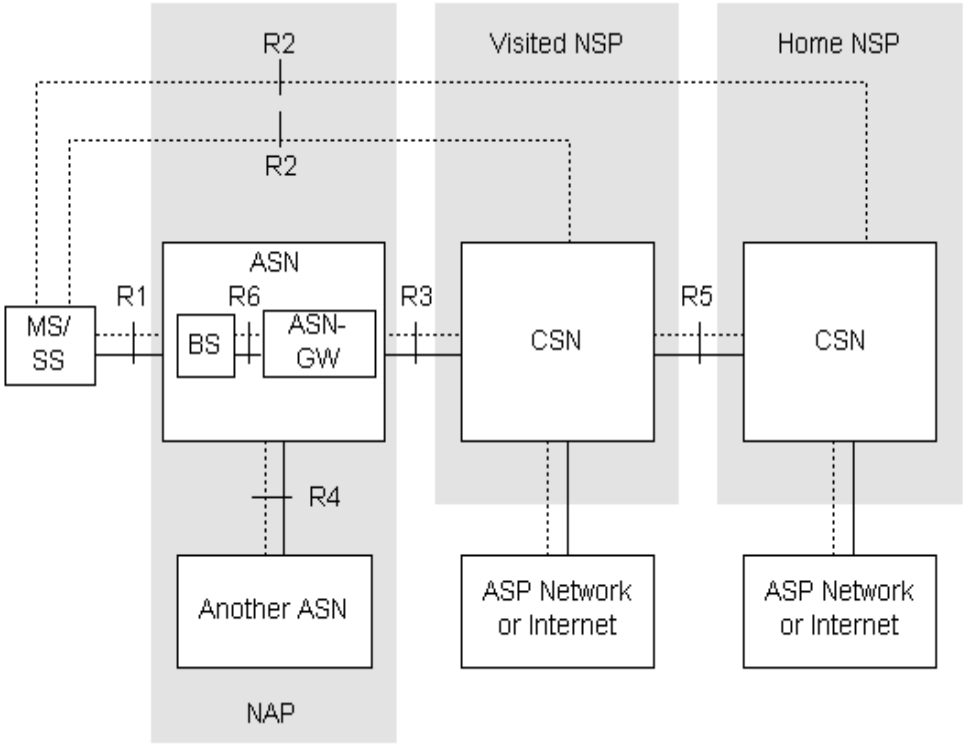
- Instant Installation by the Users

WiMAX: Network Reference 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.

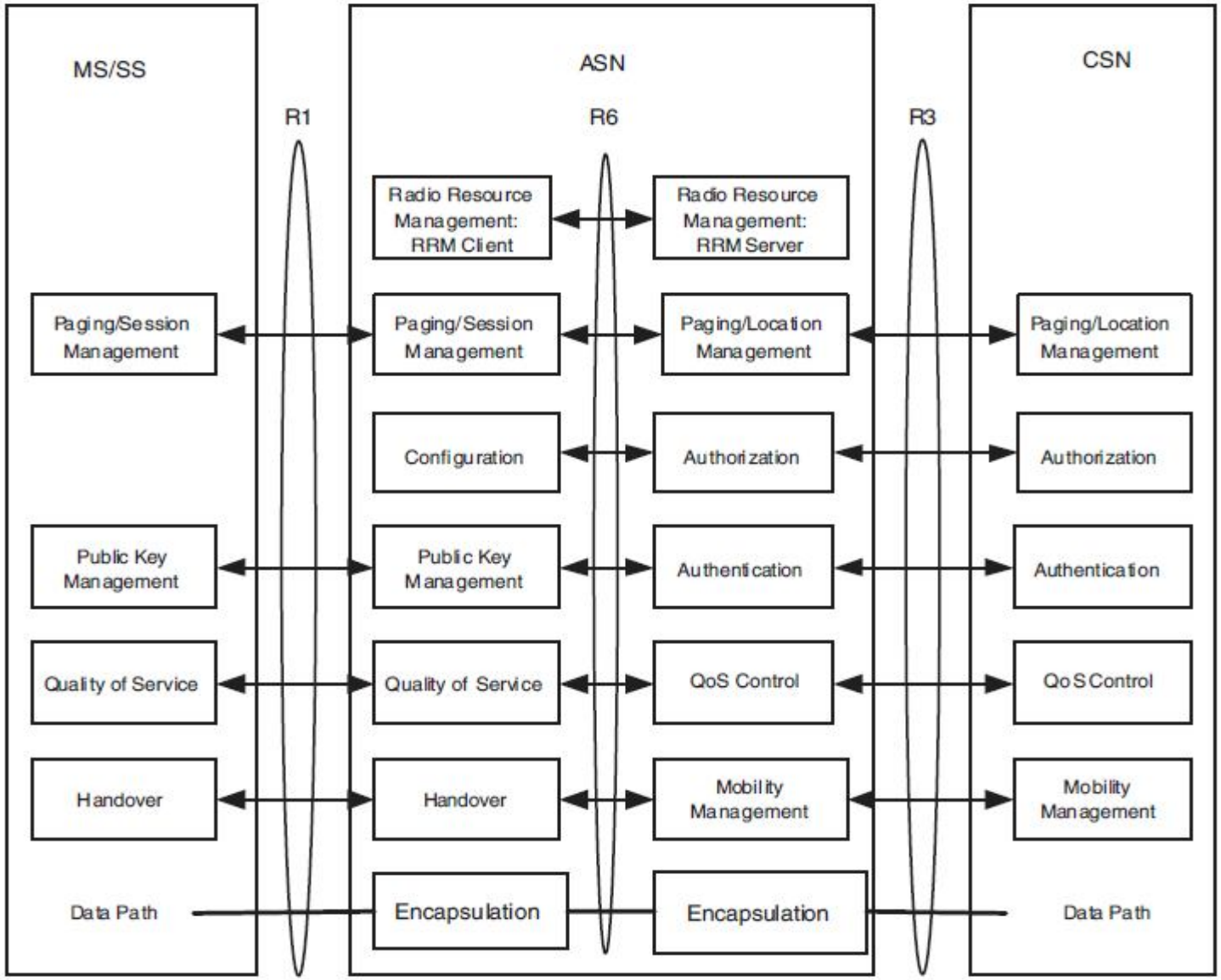
Network Reference Model



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.

Network Functional Model



CSN: AAA

Access Control system has three elements:

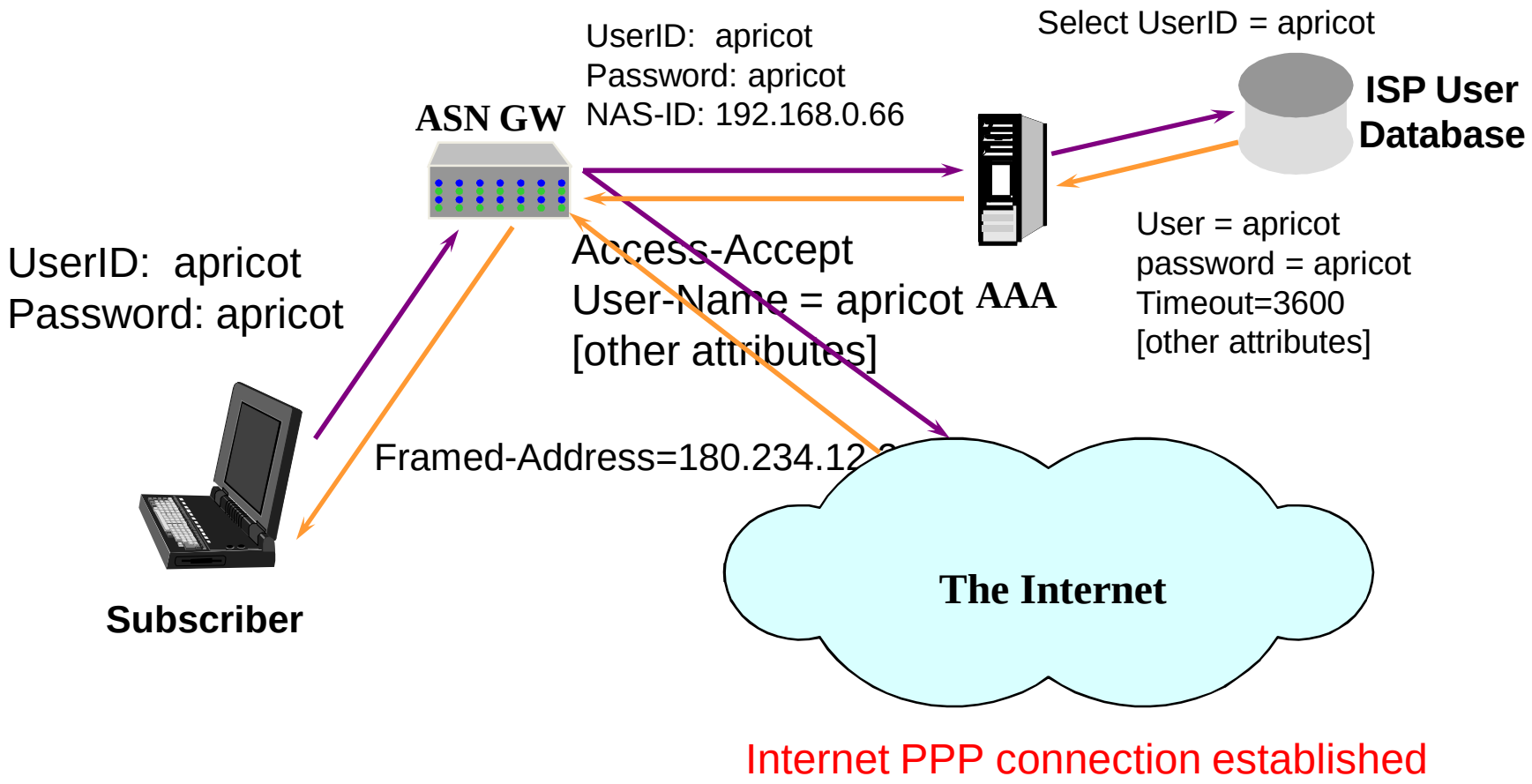
1. An entity that desires to get access: the supplicant.
2. An entity that controls the access gate: the authenticator.
3. An entity that decides whether the supplicant should be admitted: the authentication server.

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]

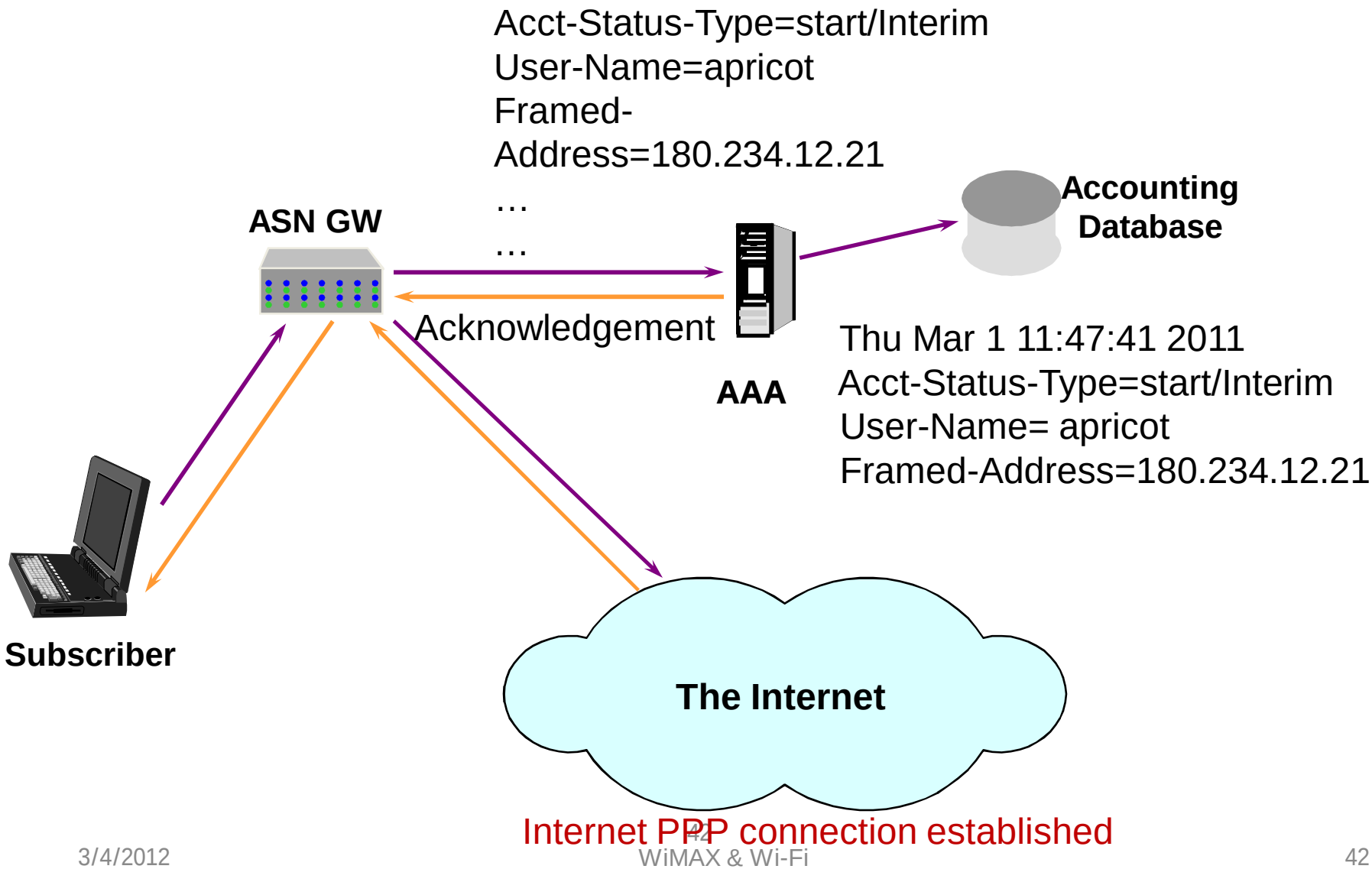
CSN: AAA

Basic Authentication Flow



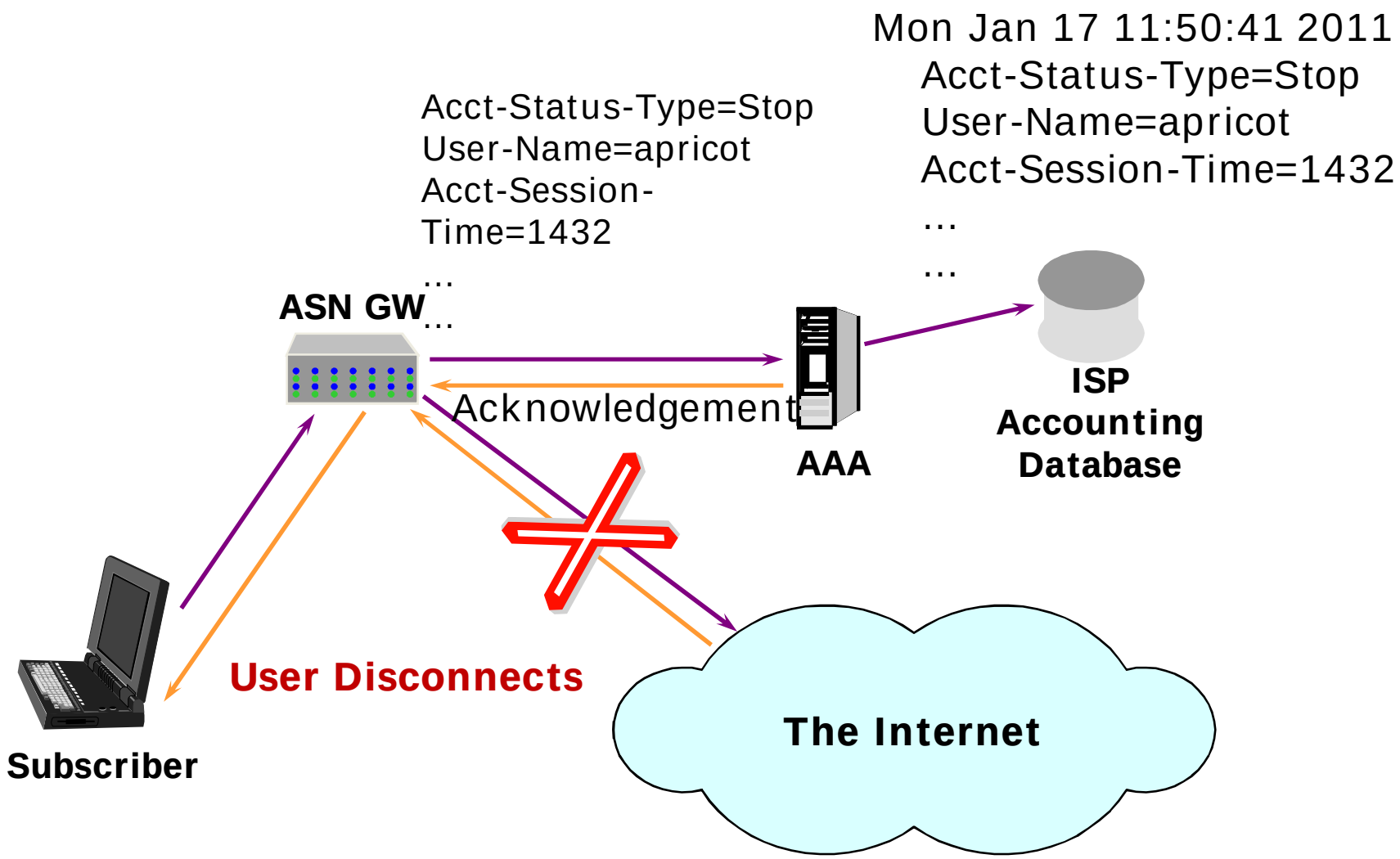
CSN: AAA

Basic Accounting Flow

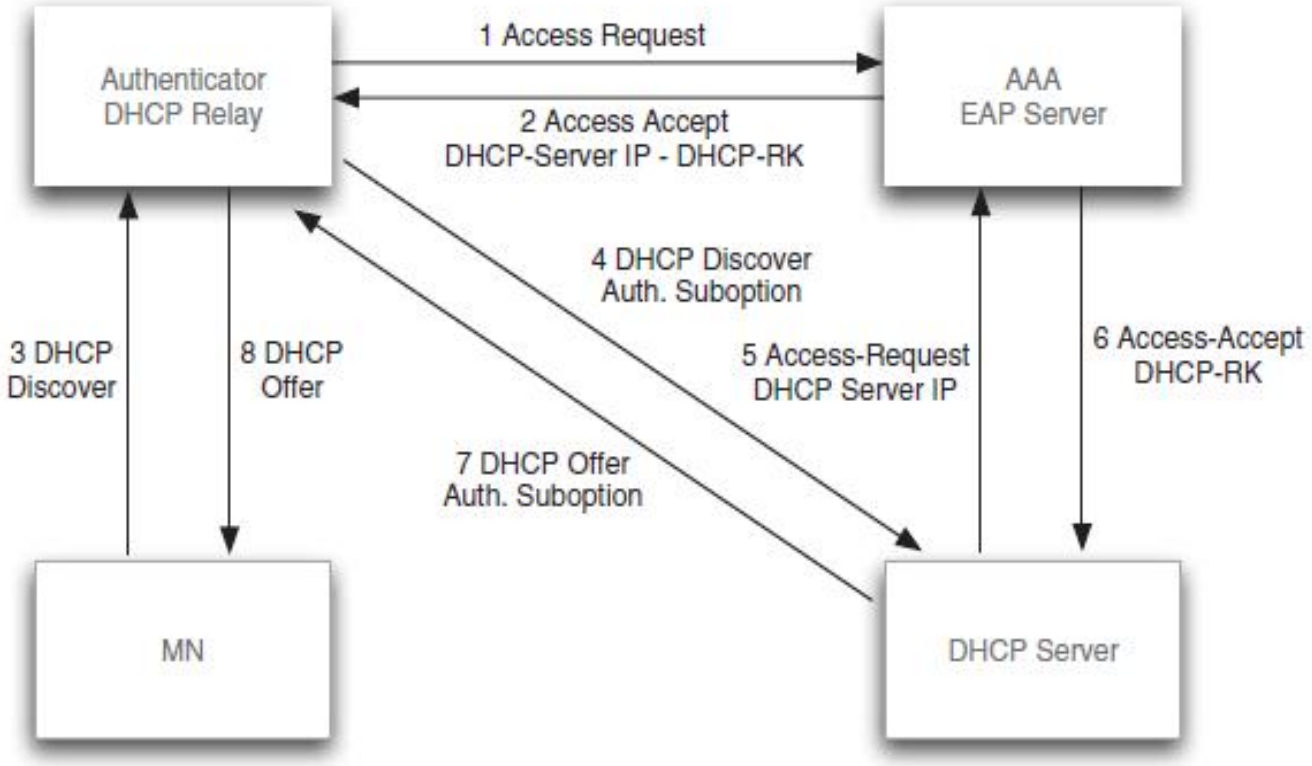


CSN: AAA

Basic Accounting Flow



CSN: DHCP IP Management



WiMAX Technical Features

•OFDM-based physical layer: The WiMAX physical layer (PHY) is based on orthogonal frequency division multiplexing, a scheme that offers good resistance to multipath, and allows WiMAX to operate in NLOS conditions.
• Very high peak data rates: WiMAX is capable of supporting very high peak data rates.
• Scalable bandwidth and data rate support
• Adaptive Modulation and coding (AMC)
• Link-layer retransmissions
• Support for TDD and FDD
• Orthogonal frequency division multiple access (OFDMA)
• Flexible and dynamic per user resource allocation
• Support for advanced antenna techniques
• Quality-of-service support
• Robust security
• Support for mobility
• IP-based architecture

WiMAX Mobility Features

WiMAX envisions four mobility-related usage scenarios :

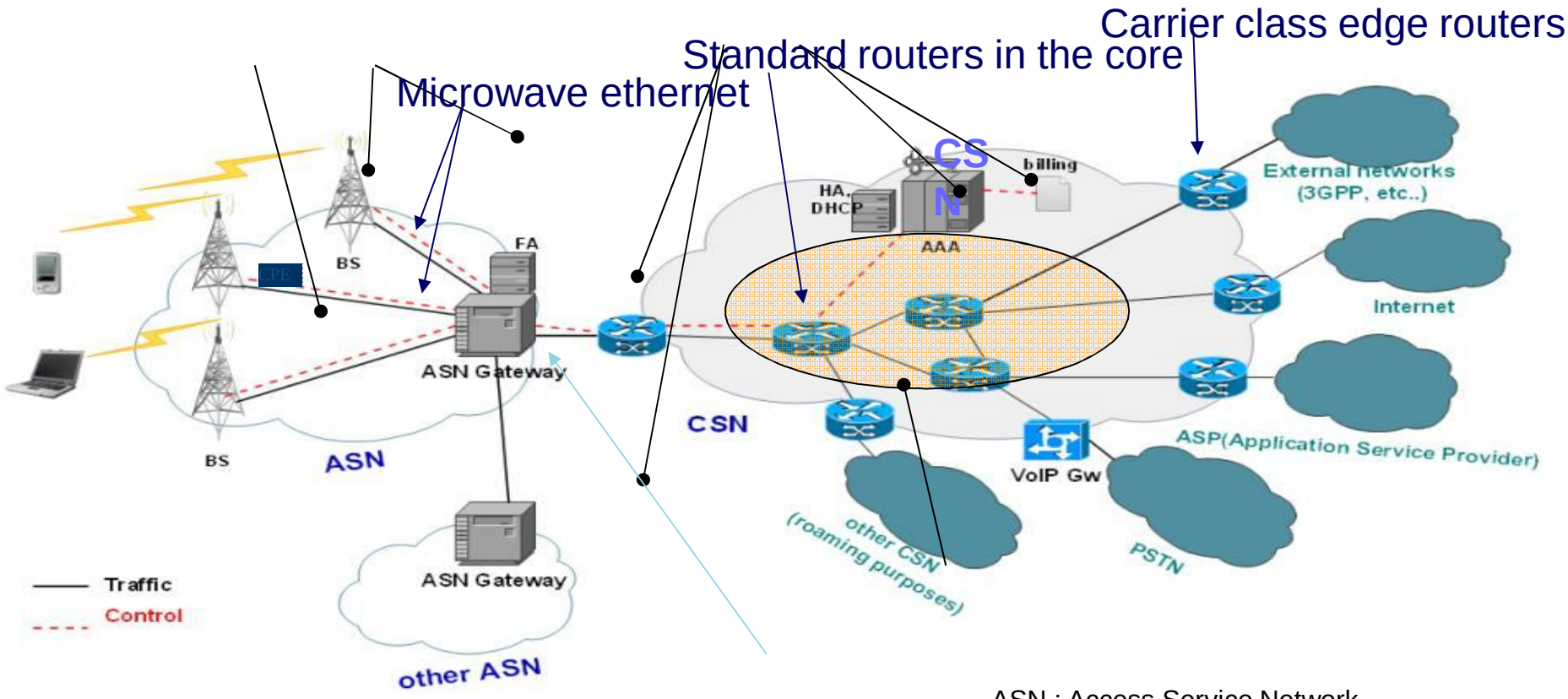
- **Nomadic**: The user is allowed to take a fixed subscriber station and reconnect from a different point of attachment.

- **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

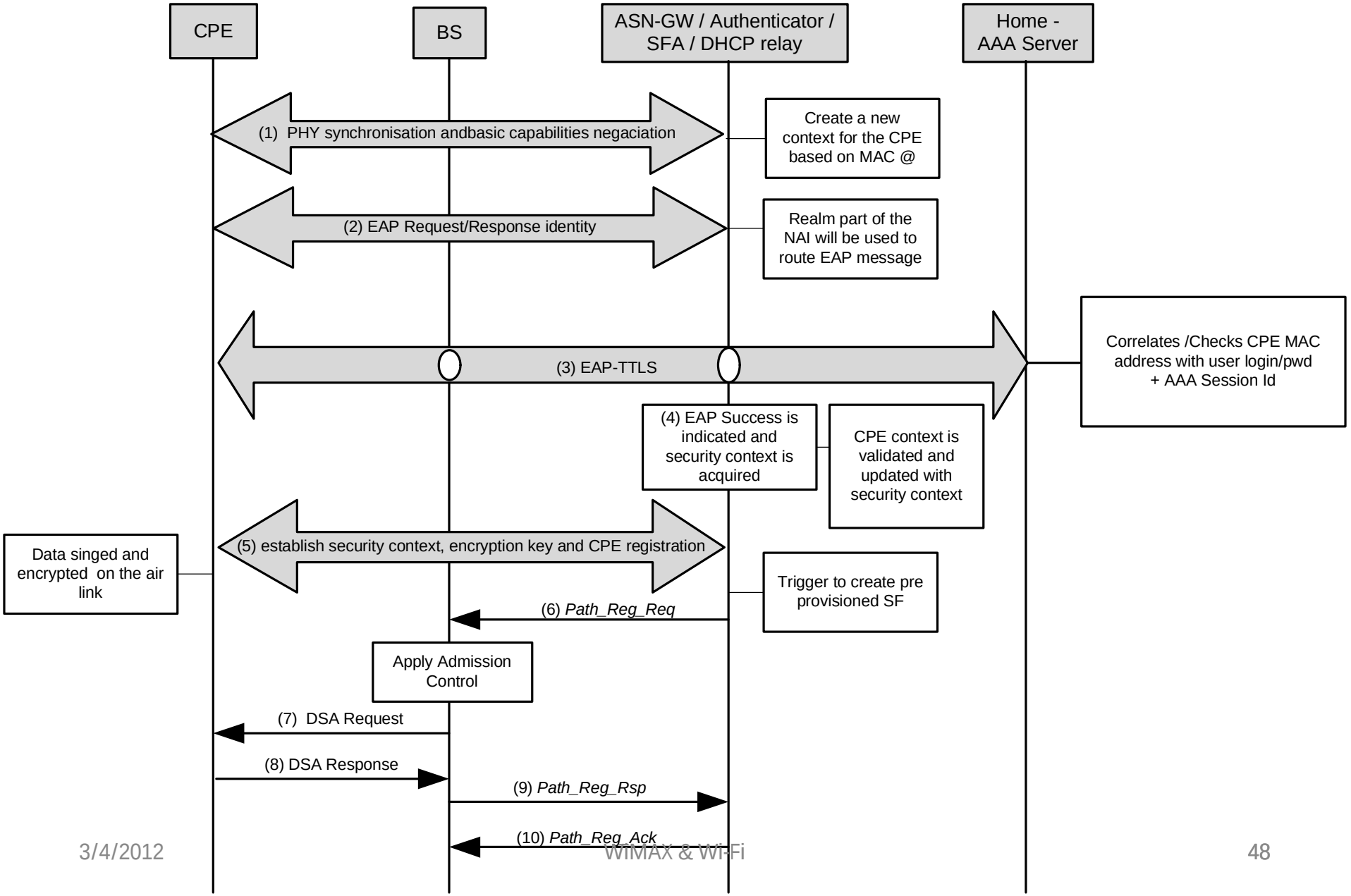
Basic Architecture



May need router co-located with ASN
Manufacturer dependent

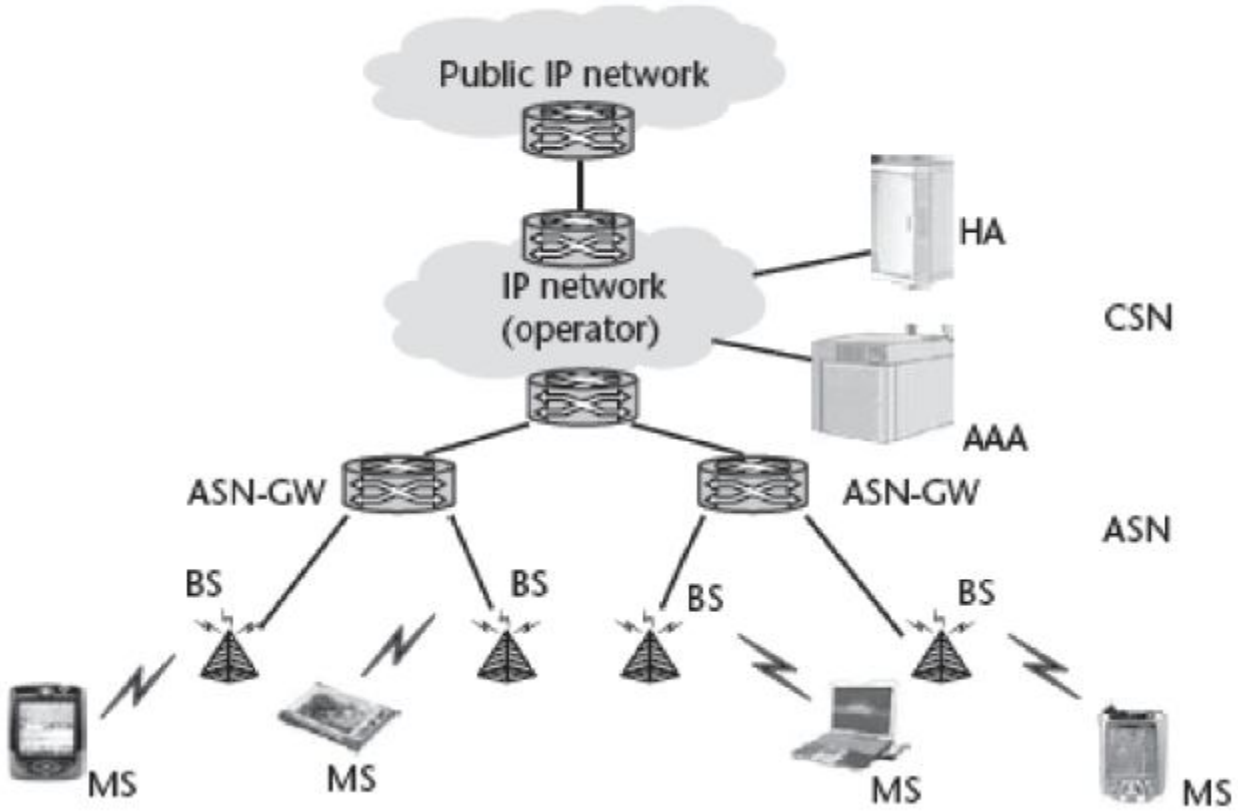
ASN : Access Service Network
CSN : Core Service Network
CPE : Customer Premises Equipment
AAA : Authentication, Accounting, Authorization
FA: foriegn agent
HA : Home Agent
DHCP : Dynamic Host Configuration Protocol

Control plane 802.16e

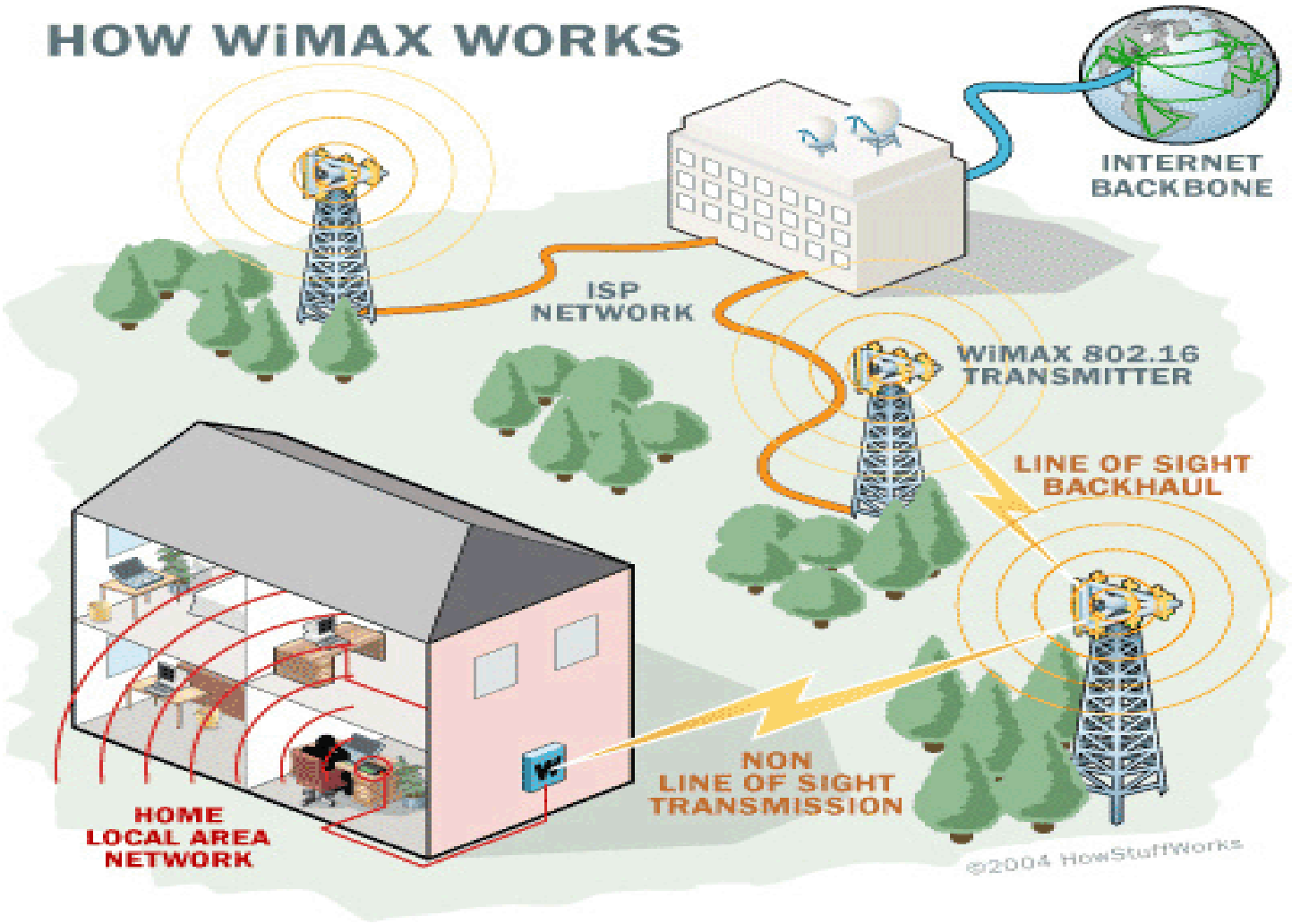


WiMAX: Topology

- 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.

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

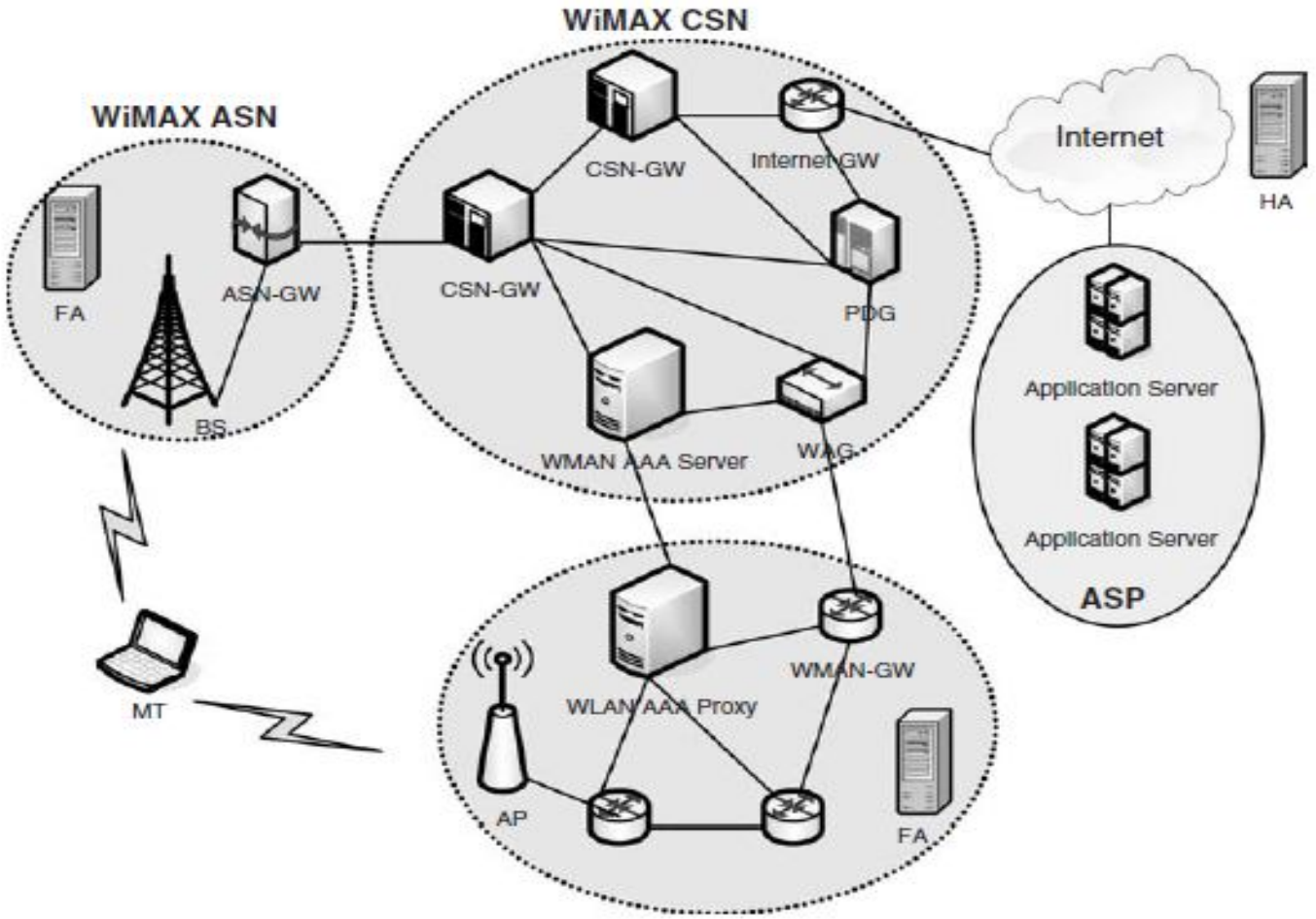
- Certificate File loaded into CPE which is verified by CSN AAA

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

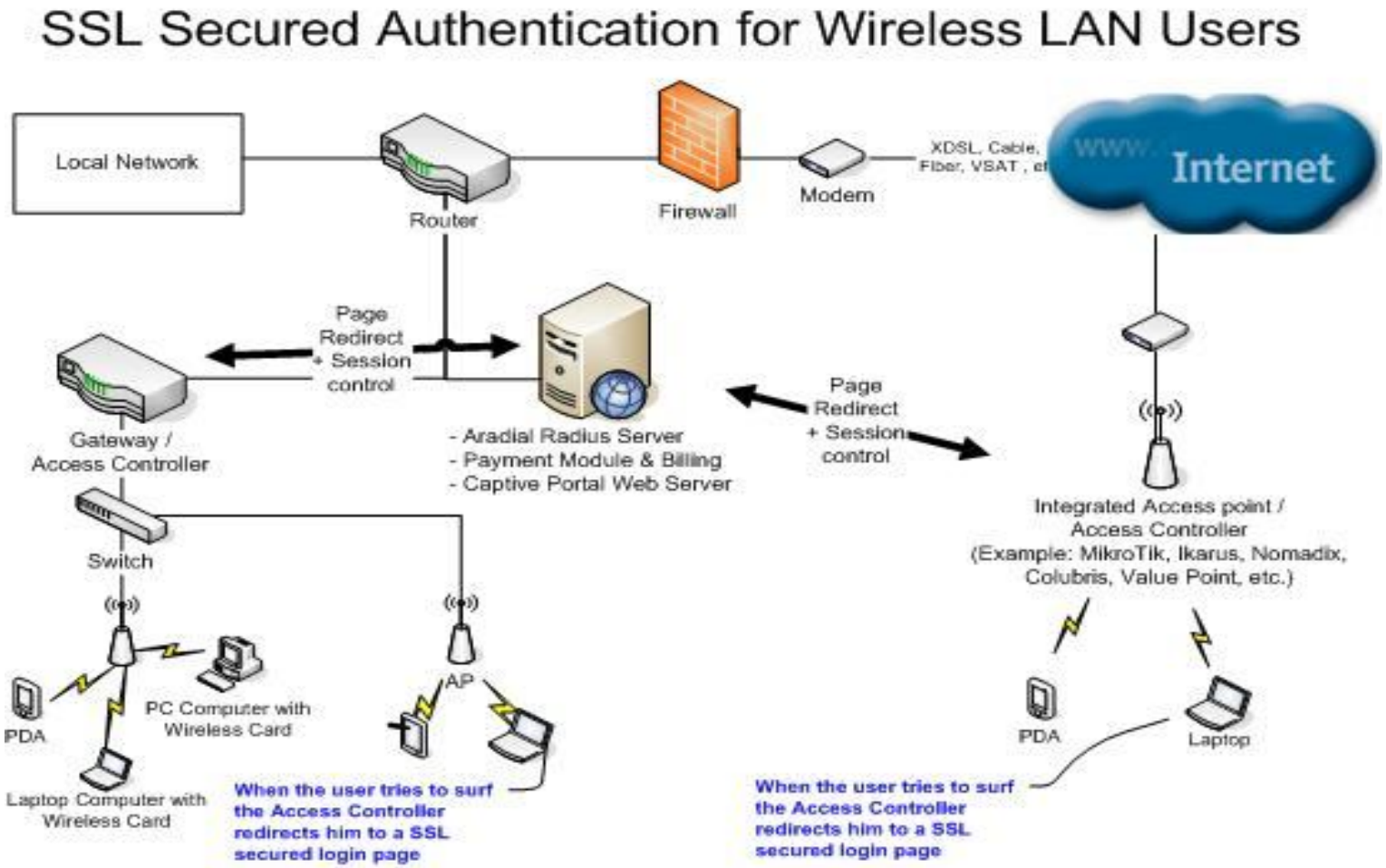
WIMAX Applications

- 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

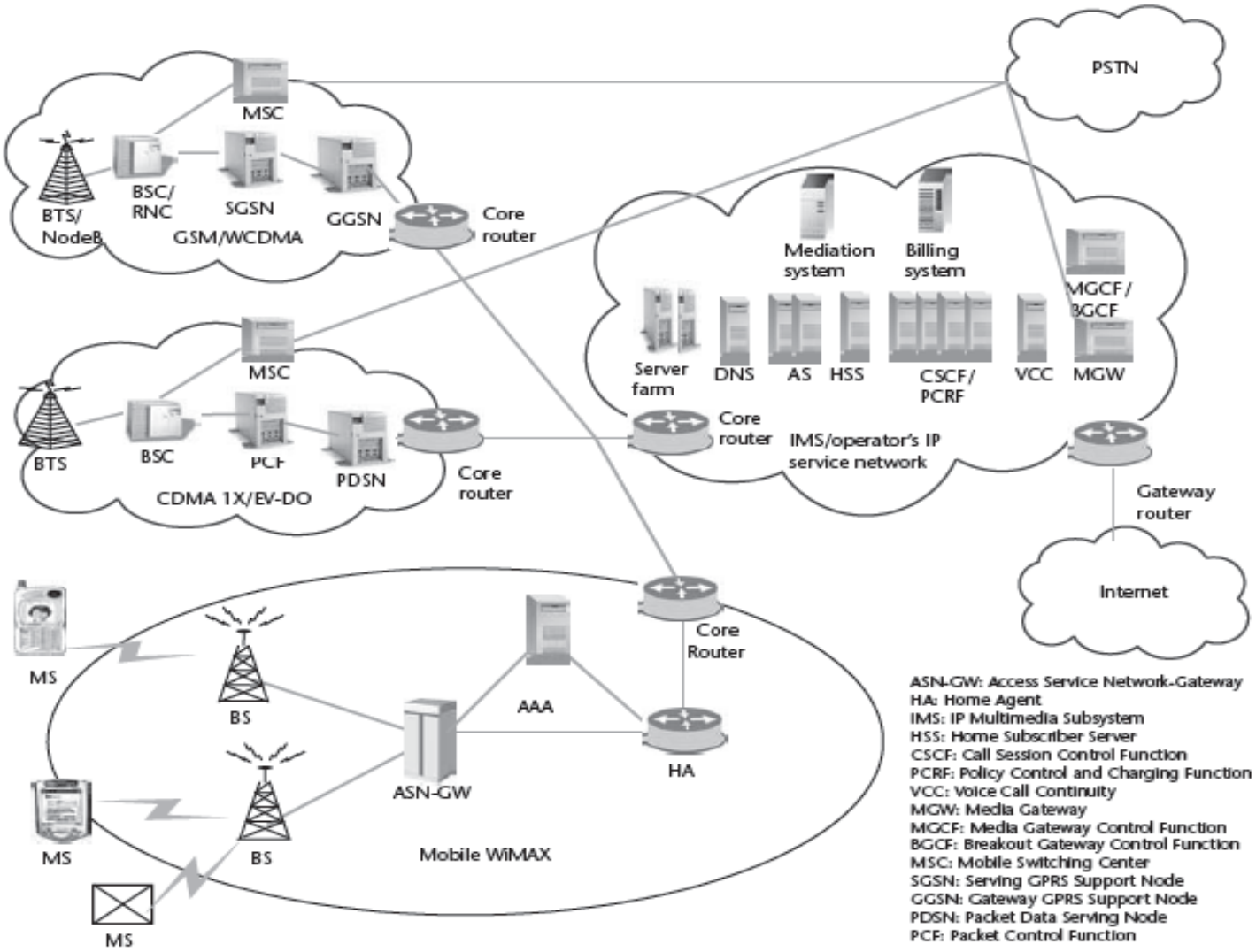
WiFi – WiMAX Internetworking Architecture



Wimax Wi Fi Hotspot



Mobile Wimax to Cellular Mobile Network Interworking

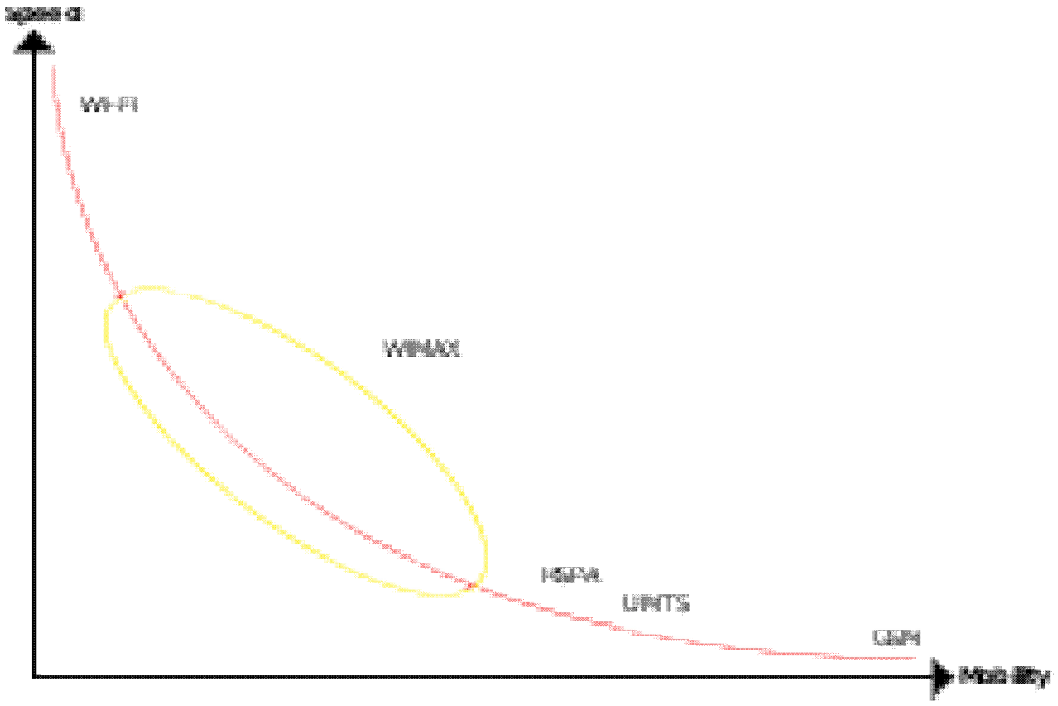


Comparison between WiMAX & Wi-Fi

Wi-Fi and WiMAX Difference

- Range
- Cost
- WiMAX is quiet MAN but Wi-Fi is LAN
- WiMAX network execute a connection oriented MAC while Wi-Fi 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 Wi-Fi user have to sort of fight to stay on connected with a specified access point.

SPEED vs MOBILITY



Deployment & Implementation Experience

WiMAX Access Network Deployment Experience

RF Survey

- RF survey is performed in a desired position which is with in 50 m from nominal point.
- A 360 degree photo is taken to have a clear view on clutter.
- Antenna height, tilt and azimuth are decided.
- Initial pole positions are also decided in this survey.

Throughput Calculation

Downlink slots in per Sector	Maximum Slot Usability(90 %)	Over Head Control Channels (20%)	sub channel in one frame	Frame Per Second	Efficiency	FEC	Modulation	Maximum Throughput without HARQ(Mbps)
450	405	324	48	200	0.5	13	QPSK CTC 1/2	1.85
450	405	324	48	200	1		QPSK CTC 1/2	
450	405	324	48	200	2		16 QAM CTC 1/2	
450	405	324	48	200	3		64 QAM CTC 1/2	
450	405	324	48	200	4.5		64 QAM CTC 3/4	
450	405	324	48	200	5		64 QAM CTC 5/6	

$$Maxtmum\,Throughput\,without\,HARQ(Mbps) = \frac{Maximum\,Slot\,Usability(90\%) * sub\,channel\,in\,one\,frame * Frame\,Per\,Second * Efficiency}{1024 * 1024}$$

$$MIMO = Maximum\,Throughput\,without\,HARQ(Mbps) * 2$$

Modulation

- **Downlink Throughput(Mbps**)
- QPSK CTC 1/2 3.21 Mbps
- 16 QAM CTC 1/2 6.43 Mbps
- 64 QAM CTC 1/2 9.64 Mbps
- 64 QAM CTC 3/4 14.46 Mbps
- 64 QAM CTC 5/6 16.07 Mbps

Uplink	**Throughput(Mbps**)
QPSK CTC 1/2	1.281738
QPSK CTC 3/4	1.922607
16 QAM CTC 1/2	2.563477
16 QAM CTC 3/4	3.845215

Experience: Frequency Management

- Frequency: 2330 – 2365 MHz

- Sector 1: 2330 – 2340 MHz
  Sector 2: 2340 – 2350 MHz
  Sector 3: 2350 – 2360 MHz

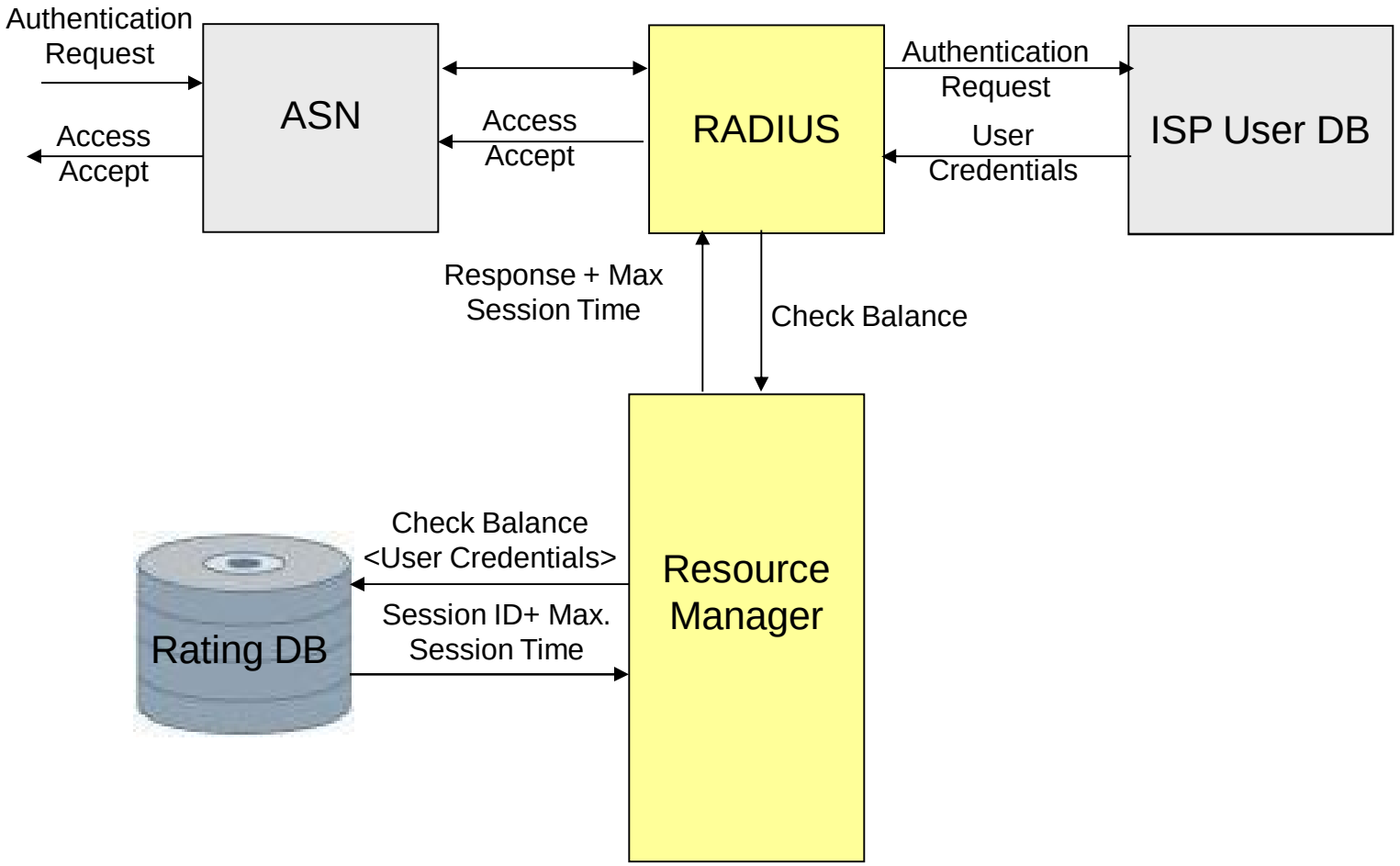
- Guard Band: 2360 – 2365 MHz
- Each Sector ensure 14Mbps download / Upload speed in Wimax 802.16e
- MIMO Optimization can ensure 25Mbps/ per sector

CSN (AAA) Experience

Authorization

- Once the user is authenticated, the RADIUS checks that the user is authorized to use the network service requested.
- For example, A given user may be allowed to use a company's wireless network, but not its VPN service.
- These information may be stored locally on RADIUS server or may be looked up in an external source like LDAP or Active Directory.
- RADIUS server conveys the authorization attributes to ASN GW stipulating the terms of access to be granted

Experience: Authentication and Authorization



Experience: RADIUS auth

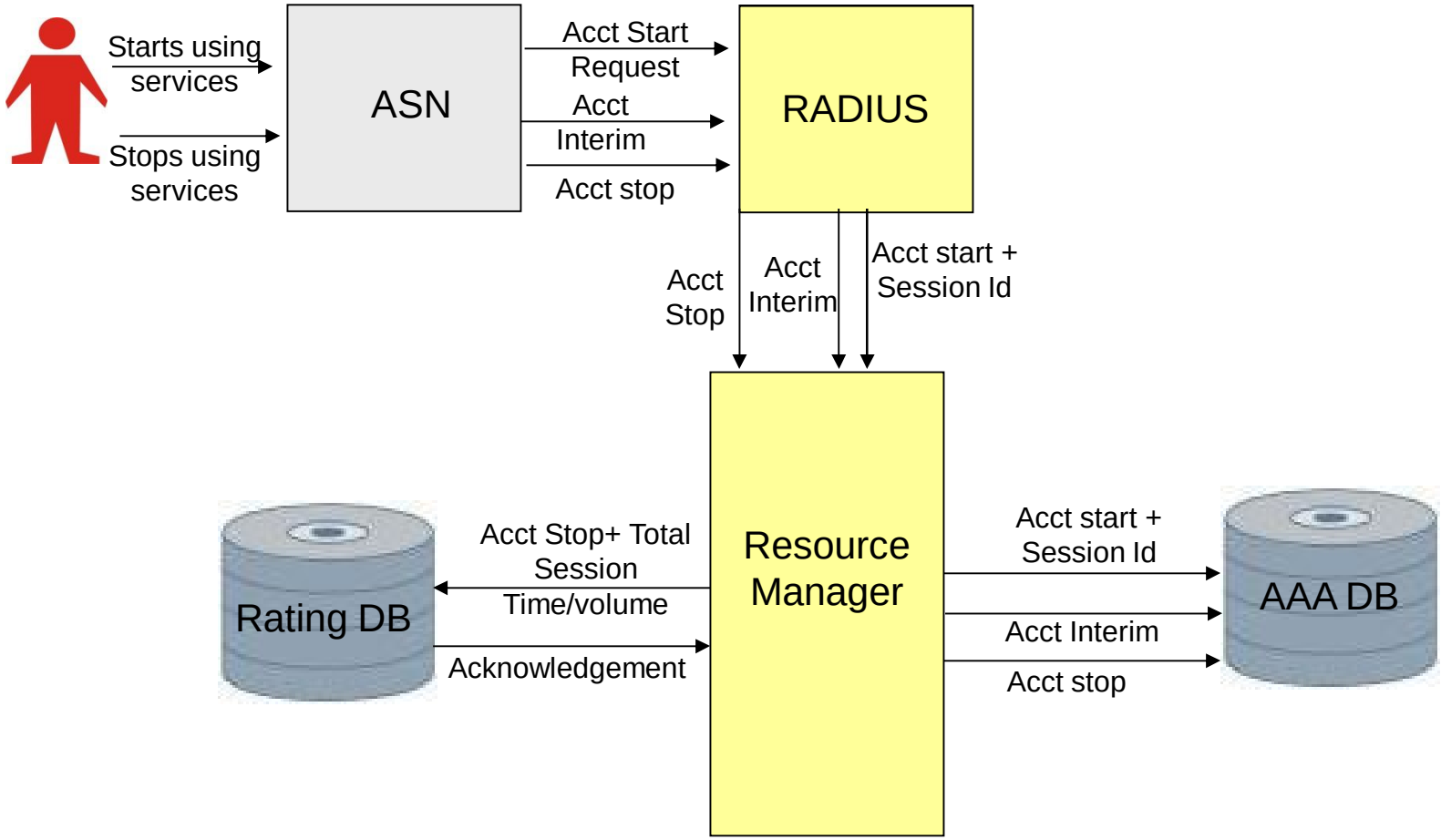
- The RADIUS Server returns one of the following three responses to ASN GW:

  - **Access Reject**
    The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive customer account

  - **Access Challenge**
    RADIUS server requests additional information from the user such as secondary password, PIN, token or card. Access Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the RADIUS server in a way that the user credentials are hidden from ASN GW

  - **Access Accept**
    The user is granted access and he can use the requested network service.

Experience: Accounting



Experience: Accounting

- After receiving an “Access-Accept” from the server, the ASN GW completes its access negotiation with the user. ASN GW then sends an acct-start message to Radius. This also signifies the beginning of a user session

- Acct-start request contains,
  - User identification
  - Network address
  - Point of attachment
  - Unique session identifier

- At configured intervals, the ASN GW sends an Interim-Acct message to Elite Radius comprising updated details of usage of the user

- Interim records convey the current session duration and information on current data usage

Experience: Accounting

- Finally when the user's network access is closed, the ASN GW sends an acct-stop message to Elite Radius, providing information on the final usage, in terms of
  - Time
  - Packets transferred
  - Data transferred
  - Reason for disconnect
  - Other information related to the user's network access

- The primary purpose of this data is that the user can be billed accordingly. These data can also be used for statistical purposes for general network monitoring

Operational Challenge

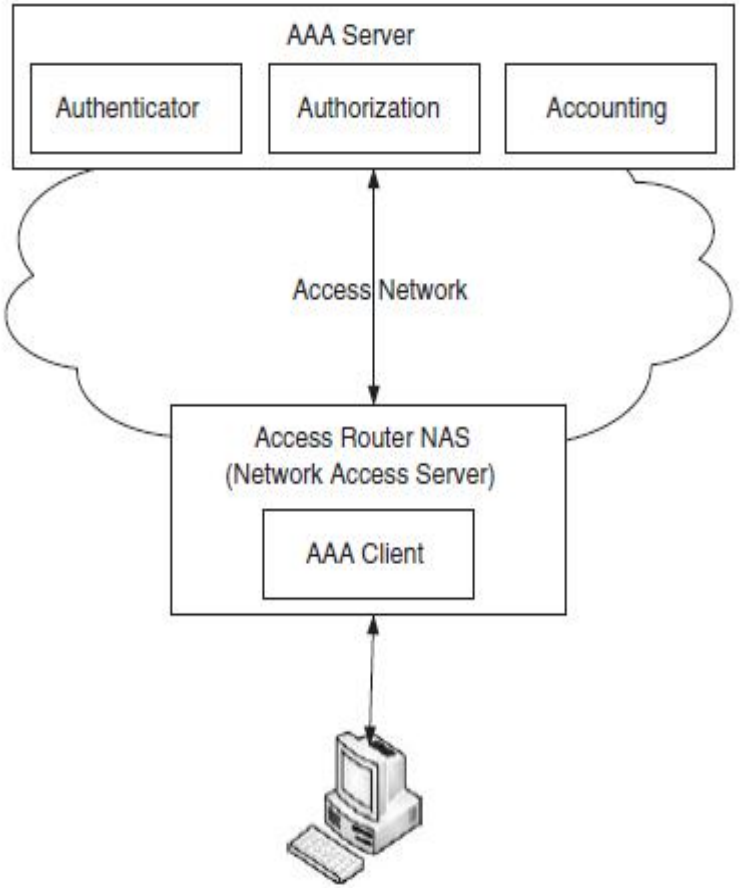
WiMAX Access Netork Experience and Way to solve

- MS Signal Receiving Problem
- MS Handover & Re-Authentication Problem
- Carrier Convergence Mode configuration
- Carrier Unavailable issue fixing
- BTS Time synchronization Problem
- Packet loss due to Microwave Bearer
- DHCP Start Alarm
- Call Drop due to PER Settings / ARQ/HARQ problem
- External Interference due to Illigal spectrum use of WiFi
- Service Usage problem after Handover
- Poor Coverage

NB. Experience details are to be discussed in board in class room.

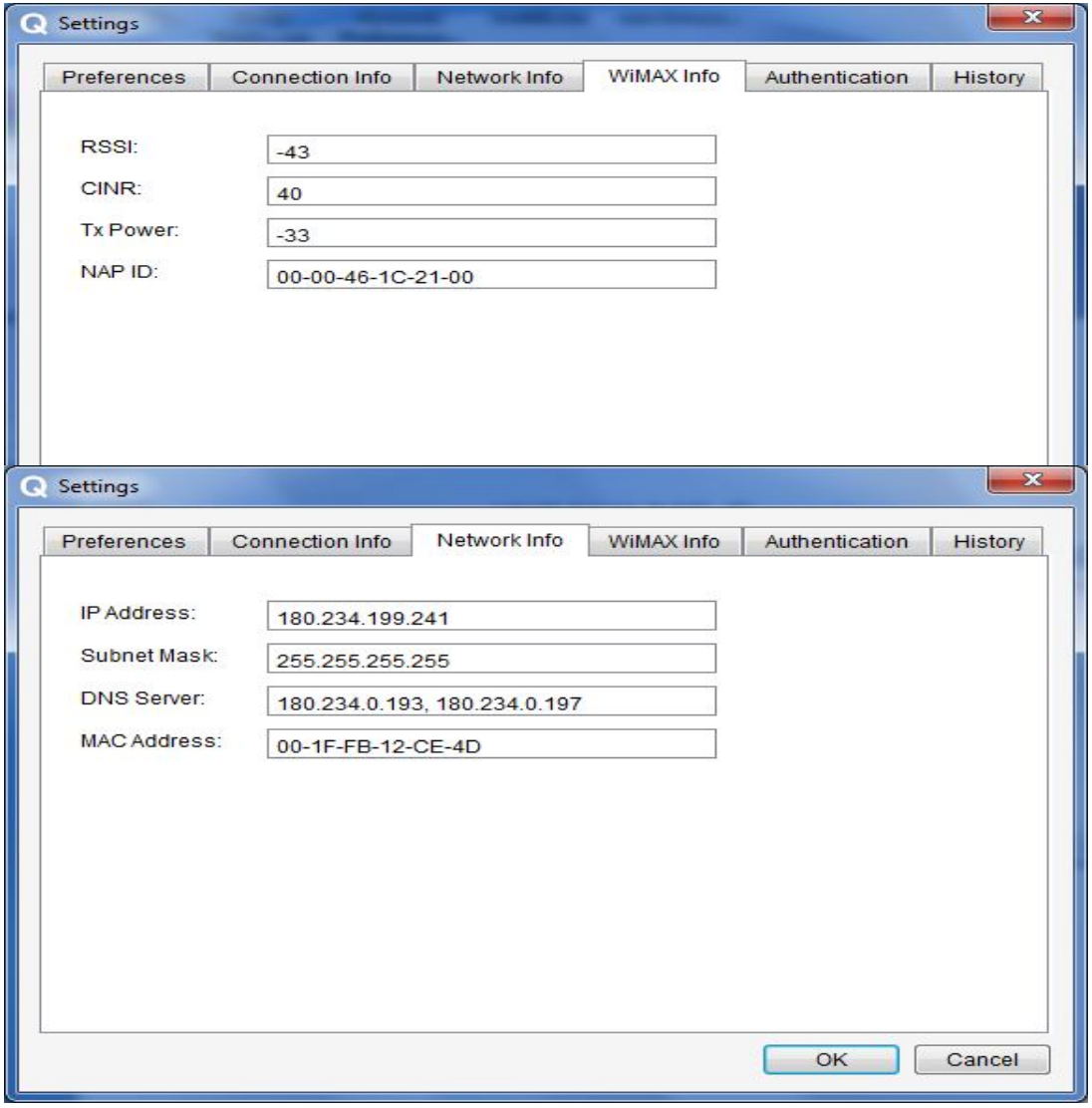
WiMAX CSN Experience

- AAA Problem
- DNS/DHCP Problem
- NTP Synchronization
- Caching Trouble
- Radius Load handling limitation
- Port Traffic Analysis
- Miscellaneous



NB. Experience details are to be discussed in board in class room.

WiMAX MS(usb modem) Experience



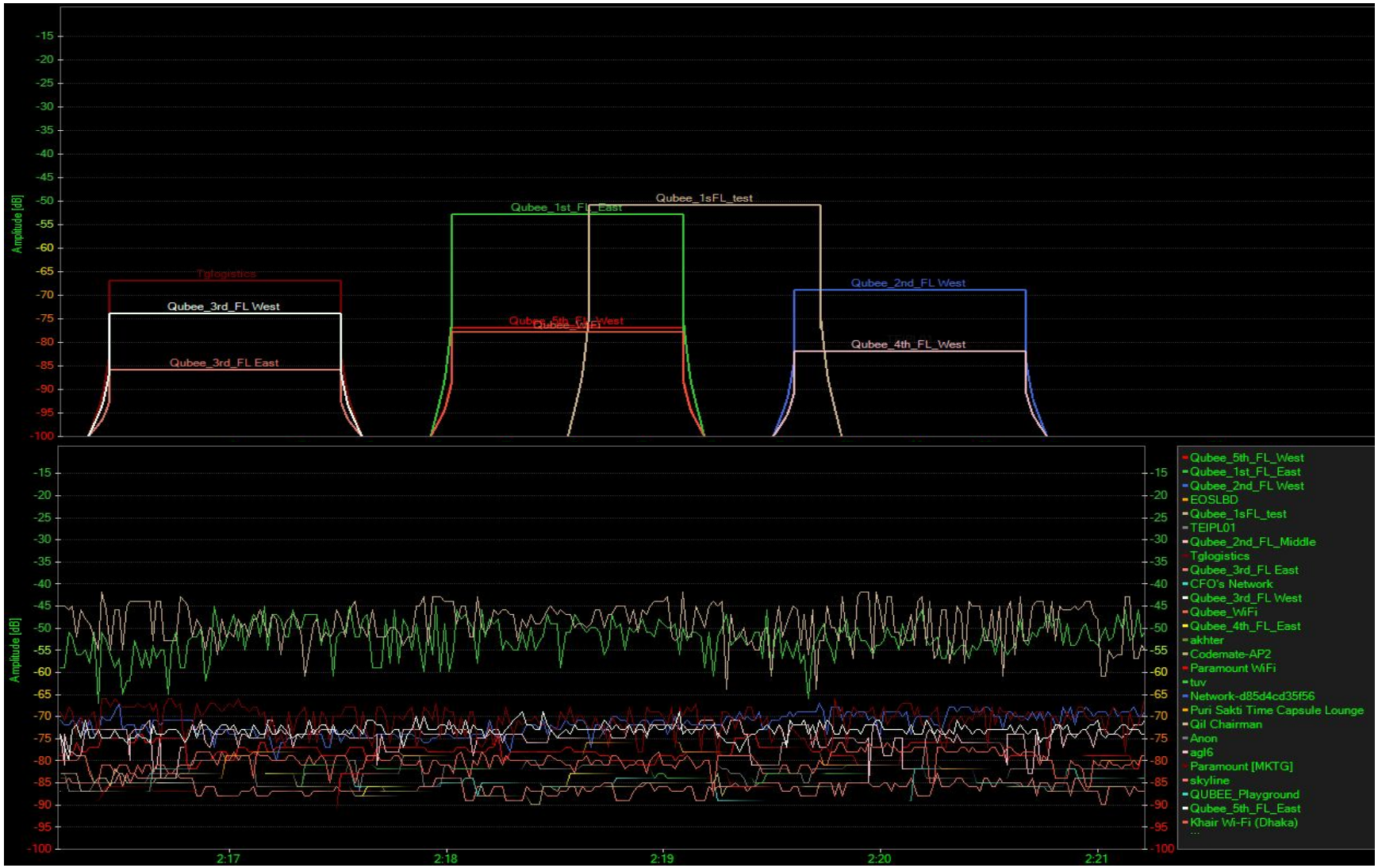
NB. Experience details are to be discussed in board in class room.

Wi-Fi Channel Overlap Experience

MAC Address	SSID	RSSI	Channel	Vendor	Privacy	Max Rate	Network Type	First Seen	Last Seen	Latitude	Longitude
BC:AE:C5:E7:22:DC	akhter	-87	6		RSNA-CCMP	72 (N)	Infrastructure	1:49:10 PM	2:17:42 PM	0.000000	0.000000
A0:21:B7:7A:2C:52	CFO's Network	-85	6		RSNA-CCMP	72 (N)	Infrastructure	1:49:10 PM	2:18:09 PM	0.000000	0.000000
00:27:0D:05:93:59	Codemate-AP2	-88	3	Cisco Systems	RSNA-CCMP	130 (N)	Infrastructure	1:49:14 PM	2:18:08 PM	0.000000	0.000000
D8:5D:4C:CB:35:B0	EOSLBD	-86	7	TP-LINK Technol...	RSNA-CCMP	150 (N)	Infrastructure	1:49:10 PM	2:10:29 PM	0.000000	0.000000
D8:5D:4C:D3:5F:56	Network-d85d4cd35f56	-89	8	TP-LINK Technol...	RSNA-CCMP	150 (N)	Infrastructure	1:49:38 PM	2:08:49 PM	0.000000	0.000000
54:E6:FC:EB:25:9C	Paramount WiFi	-83	11		RSNA-CCMP	54	Infrastructure	1:49:26 PM	2:17:30 PM	0.000000	0.000000
00:1F:F3:C3:F5:BB	Puri Sakti Time Capsule Lounge	-79	6	Apple, Inc	RSNA-CCMP	144 (N)	Infrastructure	1:50:27 PM	2:17:47 PM	0.000000	0.000000
A0:21:B7:7A:1F:66	Qubee_1sFL_test	-46	9		RSNA-CCMP	54	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
A0:21:B7:7A:3E:0E	Qubee_1st_FL_East	-55	6		RSNA-CCMP	72 (N)	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
00:26:F2:68:2F:F4	Qubee_2nd_FL West	-74	11	Netgear	RSNA-CCMP	54	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
A0:21:B7:7A:3D:8C	Qubee_2nd_FL_Middle	-76	11		RSNA-CCMP	72 (N)	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
00:1F:33:BC:13:24	Qubee_3rd_FL East	-86	1	Netgear Inc.	RSNA-CCMP	54	Infrastructure	1:49:10 PM	2:18:12 PM	0.000000	0.000000
00:24:B2:94:FC:06	Qubee_3rd_FL West	-74	1	Netgear	RSNA-CCMP	54	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
A0:21:B7:7A:39:A0	Qubee_4th_FL_East	-86	6		RSNA-CCMP	72 (N)	Infrastructure	1:49:10 PM	2:17:37 PM	0.000000	0.000000
A0:21:B7:7A:3D:72	Qubee_5th_FL_West	-80	6		RSNA-CCMP	72 (N)	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
F4:EC:38:DD:EA:76	Qubee_WiFi	-81	6 + 10		RSNA-CCMP	150 (N)	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
00:1E:E5:86:4C:51	TEIPL01	-82	11	Cisco-Linksys, LLC	WEP	54	Infrastructure	1:49:10 PM	2:18:01 PM	0.000000	0.000000
E0:91:F5:F5:15:F8	Tglogistics	-72	1	NETGEAR	WPA-TKIP	54	Infrastructure	1:49:10 PM	2:18:15 PM	0.000000	0.000000
00:23:F8:36:3E:0F	tuv	-82	6	ZyXEL Communic...	WPA-TKIP	54	Infrastructure	1:49:34 PM	2:18:02 PM	0.000000	0.000000
BC:AE:C5:E7:26:98	Qil Chairman	-87	5		RSNA-CCMP	54	Infrastructure	1:50:49 PM	2:16:18 PM	0.000000	0.000000
02:16:EA:03:09:2D	Anon	-89	11		WEP	11	Adhoc	1:51:24 PM	1:51:24 PM	0.000000	0.000000
00:18:B9:F6:D2:10	agl6	-89	7	Cisco Systems	WEP	54	Infrastructure	1:51:55 PM	2:13:43 PM	0.000000	0.000000
00:1F:33:BB:5C:7C	Paramount [MKTG]	-87	1	Netgear Inc.	RSNA-CCMP	54	Infrastructure	1:52:05 PM	2:16:43 PM	0.000000	0.000000

NB. Experience details are to be discussed in board in class room.

Wi-Fi Channel Overlap Experience



NB. Experience details are to be discussed in board in class room.

THANK YOU