VoIP via IEEE 802.11
“VoWLAN”

Sami Alshuwair
Saudi Aramco Oil Company
Agenda

- Evolution of Enterprise Telephony
- Why Deploy Vice over Wireless LAN
- Market Trends
- Challenges and Solution
  - 802.11-Quality of Service
  - Power Management
  - Security
  - Coverage/Handover
  - Capacity
- Deployment
- Recommendations
Evolution of Enterprise Telephony

From circuit-switched to packet-switched

• Traditionally private branch exchange (PBX)
  – Analog/digital phones, proprietary

• Internet Protocol PBX began a new era
  – Converge voice/data, IP-based enterprise network

• Session Initiation Protocol (SIP) emerges
  – Consistent call control, messaging & voice services
  – Applies to soft phones, single mode & dual mode devices

• VoIP extends coverage to include WLANs
  – SIP-based, VoWLAN phones provide comm.

• Fixed Mobile Convergence (FMC) solution emerging
  – Seamless handoff between mobile cellular and Wi-Fi networks
Why Deploy VoWLAN?

• Reduce mobile cellular minutes
  – VoWLAN conversations are “free” calls
• Improve in-building voice coverage
  – Deploy more access points to improve coverage
• Integrate mobile & enterprise telephony systems
  – Single device for two numbers (Cell & Office)
  – Single contact list
• When cellular phones are not an option
  – VoWLAN signals use 2.4 GHz or 5 GHz bands
• Provide wireless foundation for unified comm.
  – Voice, video, IM, all over common IP network
• Leverage existing VoIP network “VoIP Mobility”
• Most people < 30 years don’t install residential lines
• Fixed line attrition is a serious problem for fixed line operators
• Mobile phone penetration among the adult populations > 75%
• Mobile operators look at enterprises as a new source of revenue growth
• 30% of office calls are now received on mobile devices instead of desktop phones

penetration rates can exceed 100% when subscribers own more than one phone
VoWLAN Market Trends

Growing becoming pervasive
- Integrate enterprise Telephony + Mobility (FMC)
  - Call forwarding, three-way calling, call transfer
  - Wired + wireless; desire equivalent features
- Vendors integrate their voice solutions
  - Handset, WLAN equipment, IP-PBX
  - SIP signaling, presence/collaboration
- Vendor consolidation
  - Motorola/Symbol, Cisco/Orative
  - Avaya/Traverse, Siemens/Chantry
  - Polycom/Spectralink
- IEEE 802.11 tech. improving
  - 802.11e Quality of Service and prioritization
  - 802.11k, 802.11v, 802.11r- better performance
- Mobile cellular technology improving
  - Expanding coverage
  - Faster data performance
VoWLAN Solutions Improve Productivity

- Enterprise:
  - Increased staff mobility across all industries
    - 120+ Million US workers considered “mobile”
    - 70% of office workers are away from desk 40%
  - Increased capabilities ease wireless migration
    - Today: Wired by default, wireless by exception
    - 2-4 years: Wireless by default, wired by exception

- Vertical applications show direct benefit:
  - Healthcare:
    - Better patient care in Hospitals
  - Warehouse/retail:
    - Effective customer services

- Don’t expect immediate cost savings, look to value add:
  - Improved cross department communications
  - More efficient workflow and staff productivity
  - Rapid problem resolution
VoWLAN Challenges

• Packet Loss:
  – Challenge: RTP: packet loss < 3% “MOS = 4”
• Latency: length of time a word leaving a Mic till heard
  – Challenge: One way latency “G.114” <= 150 mSec
• Jitter: inter-arrival time variation from packet to packet
  – Challenge: Packet arrival time <= 30 mSec
• Handset Battery Life
• Coverage & Capacity
  – Challenge: Pervasive coverage, no dropped call, etc.
• Roaming
  – Challenge: Maintain connection/quality <50 ms
• Security
  – Challenge: avoid eavesdropping, maintain access control
• Location Tracking “E911/E112”
# 802.11 WLAN Physical Layer Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Bandwidth (MHz)</th>
<th>Op. Frequency</th>
<th>PHY</th>
<th>MAC</th>
<th>Throughput (Typ)*</th>
<th>Theoretical Rate</th>
<th>Service Interference</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11a</td>
<td>20 MHz</td>
<td>5 GHz</td>
<td>OFDM</td>
<td>CSMA/CA</td>
<td>23 Mbit/s</td>
<td>54 Mbps @ 20MHz</td>
<td>- Cordless phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Amateur Radio</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Aeronautical Radio</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Navigation</td>
</tr>
<tr>
<td>IEEE 802.11b</td>
<td>20 MHz</td>
<td>2.4 GHz</td>
<td>DSSS, CCK</td>
<td>CSMA/CA</td>
<td>4.3 Mbit/s</td>
<td>11 Mbps @ 20MHz</td>
<td>- MW Oven</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Bluetooth Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- Amateur Radio</td>
</tr>
<tr>
<td>IEEE 802.11g</td>
<td>20 MHz</td>
<td>2.4 GHz</td>
<td>OFDM, CCK</td>
<td>CSMA/CA</td>
<td>19 Mbit/s</td>
<td>54 Mbps @ 20MHz</td>
<td>- Same as 802.11b</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE 802.11n</td>
<td>20 MHz &amp; 40 MHz</td>
<td>2.4 GHz &amp; 5 GHz</td>
<td>OFDM, CCK</td>
<td>CSMA/CA</td>
<td>180 Mbit/s</td>
<td>600 Mbps @ 40MHz &amp; 4 Special Streamers</td>
<td>- Same as 802.11b/11a</td>
</tr>
</tbody>
</table>

**Throughput depends on**  
radio transmission environment, packet size & # active transmitter

**OFDMA =** Orthogonal Frequency Division Multiplexing  
**CCK=** Complementary Code Keying  
**CSMA/CA=** Carrier Sense Multiple Access/ Collision Avoidance
802.11 Medium Access Control Legacy

- **MAC Frame Types:**
  - Data
  - Control: RTS, CTS & ACK
  - Management: Beacon

- **Distrib. Coord. Func. (DCF):**
  - Uses a CSMA/CA algorithm
  - Senses the medium first
  - Frame transmitted when channel idle for $\geq$ DIFS + backoff timer
  - Otherwise a backoff time $B$ is randomly in interval $[0, CW_{\text{min}}]$
  - Post-backoff ensure fairness between stations
  - Has no QoS-priory “best effort”
  - MAC layer retransmits lost packet:
    - 7 data packets
    - 4 RTS packets

---

DCF Method Signal Flow

- **SIFS** = Short Interframe Space. 16us for .11a and 10us for .11b/g
- **DIFS** = DCF Interframe Space = SFIS + 2 x Slot Time
- **PIFS** = PCF Interframe Space = SIFS + Slot Time
- **Slot Time** = 20us for .11b & 9us for .11a , .11g is 9us when all STA high-speed otherwise 20us
- **Backoff** = Random * Slot Time

<table>
<thead>
<tr>
<th>IEEE 802.11a,g</th>
<th>CW$_{\text{min}}$</th>
<th>CW$_{\text{max}}$</th>
<th>SlotTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>1023</td>
<td>9us (9us)</td>
<td></td>
</tr>
<tr>
<td>3f</td>
<td>1023</td>
<td>20us (20us)</td>
<td></td>
</tr>
</tbody>
</table>
**802.11 Medium Access Control Legacy Cont.**

- **Point Coordination Function (PCF)**
  - Contention-free frame transfer
  - Single Point Coordinator (PC) controls access to the medium. AP acts as PC.
  - PC transmits beacon packet when medium is free for PIFS time period. PCF has higher priority than DCF (PIFS < DIFS)
  - PCF not used b/c not ideal for real-time traffic:
    - Unachieved performance when traffic load increase.
    - Polling schemes prolong the delay in WLAN
IEEE 802.11e/WMM-SA “QoS” Overview

- **Enhanced DCF Channel Access (EDCA)-prioritized QoS**
  - Contention based
  - DiffServ-Service like
  - Traffic can be classified into 8 different classes
  - Each station has 4 Access Categories (AC)
  - VoWLAN assigned highest priority to transmit
  - HP post-backoff < LP post backoff
  - Perform well under light/moderate load condition

**Diagram: 802.11e EDCA vs Legacy 802.11**

**Legend:**
- **AC0**: Voice
- **AC1**: Video
- **AC2**: Video
- **AC3**: Data
- **AC4**: Video
- **AC5**: Video
- **AC6**: Video
- **AC7**: Background

**Key Terms:**
- **AIFS**: Arbitration Interframe Spacing
- **DIFS**: Distributed Interframe Spacing
- **PIFS**: Point Interframe Spacing
- **SIFS**: Short Interframe Spacing

**Beacon frames** contain information on # of stations in BSS, channel utilization, available capacity & QoS capability.
IEEE 802.11e/ WMM-SA “QoS” Overview Cont.

- HCF Controlled Channel Access (HCCA)
  - HCF combines polled and CSMA/CA channel access
  - Adapted in WMM-SA
  - Parameterized QoS; promise predefined delay limit for real-time traffic
  - Polling based-polling frames brings added overhead
  - Can start polling period at any time unlike PCF
  - Perform well under heavy load
  - “InServ-Service like”
  - Specify time interval for STA “TDM-service like”
  - More into enterprise solution
  - HCF doesn’t reduce overhead rather improves air traffic control “QoS”; contention loss is reduced and jitter is predictable/low
• Call Admission Control: STA ask AP permission
  – STAs negotiate QoS/characteristics of packet stream expected to send/receive (TSPECs):
    • Nominal MSDU
    • Mean Data Rate- based on Nominal MSDU & packetization period
    • Minimum PHY Rate
    • Surplus Bandwidth Allowance
    • Medium Time
  – If TSPEC rejected due to congestion, STA may use larger packed size → reduce number of packet/Sec → reduce loading
  – Issues with TSPECs
    • With VoIP media characteristics/codec defined after 200 OK message.
    • Doesn't contain “Urgent” Field to indicate priority call “911”
IEEE 802.11e/ WMM-SA “QoS” Overview Cont.

- Transmission Opportunity (TXOP)
  - Defines when a STA has the right to transmit:
    - Starting time
    - Maximum duration
  - Prevent hogging the channel “unpredictable delay”
  - STAs transmit multiple MSDU consecutively from same AC “CFB”
    - Increase system throughput in mixed environment voice/data/video
    - Not suitable for voice communications b/c voice packets are periodic

CFB = Contention-Free Burst  MSDU = MAC Service Data Unit
• Major challenge of VoWLAN is battery life
  • Legacy Power Save:
    – STA wakes up every 100ms to listen to AP beacon & TIM
    – Only one data frame is sent at a time
    – Ping-pong fashion
    – Increase application latency 100 or 300 ms
  • WMM Power Save “U-APSD”
    – Power save behavior is negotiated during association “TSPEC”
    – AP buffer voice/data frames within each AC queue till receive a trigger
    – Clients can initiate download at any time no need to wait for TIM
    – SAT transmits uplink frame that act as trigger frame every 20 ms “packetized period”
    – When no call in progress STA doesn’t poll
    – 15 to 40% battery life save w/low latency

U-APSD = Unscheduled-Automatic Power Save Delivery  TIM = Traffic Information Map
VoWLAN Handheld Power Management

- Handheld devices today face the challenge of maximizing battery lifetimes.
- Increase battery capacity limited by increasing size and weight if the batteries.
- Major power consumers in a Wi-Fi phone:
  - Radio/WLAN subsystem
  - Host processors
  - LCD
  - Backlight
  - DSP
  - Analog codec
  - Flash, SDRAM
  - LED
  - System on Chip
  - Drainage current, etc.
- Frequency scaling on the cost of a slower processing capability to complete tasks.

\[ P = C \times V^2 \times F \]

- \( P \) = Dynamic power consumption
- \( V \) = The supply voltage
- \( C \) = Average switched capacitance/cycle
- \( F \) = The clock Frequency
VoWLAN Security

Security at Layer -2 :

- Wired Equivalent Privacy (WEP)
  - 40 bit – 128 bits key,
  - RC4 symmetric encryption algorithm
  - Authentication easy to break
  - Open System Authentication
    - Any client can authenticate itself
    - WEP used for encryption with right key
  - Shared Key Authentication
    - Four way challenge-response handshake
    - Pre shared WEP key used for encryption “manual”
- Data Integrity:
  - CRC
  - IV is clear-text – 24 bit
    - keys may repeat every $2^{24} = 1.6x10^7$ packets (a few hours of busy traffic)
- 802.11i:
  - Confidentiality
    - Pre-shared key (PSK)
      - Residential & SHO
      - 256 bit key
    - TKIP known as WPA “firmware upgrade”
    - AES “CCMP” known as WPA2 “hardware upgrade”
      - Increased overhead
      - More processing time/delay
  - Data Integrity:
    - More secure message integrity MIC
  - 802.1x: client/server; network authentication & Key establishment
    - Enterprise solution: EAP-TLS use certificate to authenticate network to user and Vice-versa to clients to be issued certificate not cost effective
    - EAP-TTLS & PEAP: use certificate to authenticate server to client, client uses password schemes (CHAP, PAP, etc.) to authenticate themselves to server to clients no longer need for certificates
    - Hard to implement in inter-domain

Basic WEP encryption:
RC4 keystream XORed with plaintext

802.1x: “authentication” EAPOL

The two modes in WPA for Enterprise and Personal

<table>
<thead>
<tr>
<th>Mode</th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
</table>

Security at Layer -3 “Network Layer”: IPsec “VPN”
- Site-to-site connections
- Some ISPs block IPsec or charge more
- Suite of protocols:
  - Key management protocol: IKE, Kerberos
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)
- Has impact on packet overhead size that diminish benefit of low-bit-rate codes
- Security and efficiency are conflicting requirements - IPsec affecting:
  - Speech quality
  - Channel capacity
  - Delay voice packet

Security at Layer -4 “Application Layer”:
- SSL-TLS “VPN”:
  - Web client-to-server
  - Suitable for most nomadic
  - Integrate with other protection tech. to identify malicious traffic
- SRTP → key management not yet standardized
VoWLAN Security Cont.

Malware

Self-replicating
- Standalone
- Needs host program

Non-replicating
- Hidden function
- Hidden presence
  - Not evasive
  - Evasive against detection

Examples:
- Worms
- Viruses
- Trojan horses
- Bots, spyware
- Rootkits

*Note: malware often have multiple characteristics and fall in more than one category*
VoWLAN Security Cont.

Defenses

Preventative
- Patching
- Antivirus/anti-spyware updates
- Close unnecessary ports
- Vulnerability assessment/penetration testing

Defensive/reactive
- Host-based
  - Active
    - Personal firewall
  - Passive
    - Antivirus/anti-spyware/rookit detection
    - Virtual machine/sandbox
    - Host-based IDS
    - Honey pot, black holes
    - IDS
- Network-based
  - Passive
  - Active
  - Blocking
    - Network admission control
  - Deception
  - Redirection
  - Slowing down
  - Rate Throttle
  - Trap

Sapm filtering
Whitelists/blacklist
Firewalls
Access control list
Network Access Control Conceptual View “Admission Control”

THE GOAL

1. End user attempts to access network
   - Initial access is blocked
   - Single-sign-on or web login

2. NAC Server gathers and assesses user / device information
   - Username and password
   - Device configuration and vulnerabilities

3a. Noncompliant device or incorrect login
   - Access denied
   - Placed to quarantine / Captive Portals for remediation

3b. Device is compliant
   - Placed on “certified devices list”
   - Network access granted

NAC Goals:
- Mitigation of zero-day attacks
- Policy enforcement
- Identify and access management

VoWLAN Security Cont.
VoWLAN Security Cont.

Best Practice

VLAN Prevent:
- Toll fraud
- Denial of Service (DoS) attacks
- Eavesdropping & Interception

SSID: Data
Security: PEAP + AES
AP Channel:
SSID “Data” = VLAN 1
SSID “Voice” = VLAN 2
SSID “Visitor” = VLAN 3

802.1Q Wired Network w/VLANs

SSID= Service Set ID, PEAP= Protected Extensible Authentication Protocol, AES= Advanced Encryption Standard, LEAP= Lightweight Extensible Authentication Protocol
Mobile Phone Security Policy:

- ISO/IEC 27002 for remote access policy recommendation
- Who owns his/her mobile phone?
- Do not go for the slick one!
- Devices vendors don’t care about anti-malware so use third-party mobile security package
- What to look for in mobile phone security software
  - Effectiveness
  - Features
  - Ease of Use
  - Installation & Updates
  - Technical Help/Support
VoWALN Scanning Types

- **Scanning required for many functions.**
  - finding and joining a network
  - finding a new AP while roaming

- **Passive Scanning**
  - Switch for 1st channel then listen for Beacon frames
  - Measure S/N Ratio
  - Switch to new channel then listen for Beacon frames
  - Till all channels scanned
  - **Handover delay > 600 ms**
  - **Power intensive b/c receiver powered up for 100ms**

- **Active Scanning**
  - On each channel Send a Probe, wait for a Probe Response
  - Beacon or Probe Response contains information necessary to join new network.
  - **Handover delay between 110 & 160 ms depend on number of STA within BSS**
  - Fast Handover delay “scan non-overlap ch.” around 25 to 30 ms
  - **Less power intensive**

- **AP Neighbor list (802.11k)**
  - Each AP sends down list of “suitable” neighbor APs based RF measurement

- **Site Table Info.**
  - The last APs we associated with
  - APs we can hand off to but haven’t visited yet
  - APs that we have pre-authentication with

---

**Active Scanning Type**

1. STA send Probe
2. APs send Prob Response
3. STA sends Authentication request
4. AP sends Authentication Response
5. STA sends Association request
6. AP sends Association Response

---

Image credits: Bicsi
VoWLAN Coverage/Handover

- **Intra-ESS:**
  - Handoffs between access points in same ESS
  - APs sharing same SSID
  - Same IP subnet

- **Intra-ESS: Layer-2 “Horizontal”**
  - Handoffs between access points in same ESS
  - APs sharing same SSID
  - Separate subnet
  - AP handle tunnel phone's traffic to back to home AP

- **Inter-ESS: Layer-3 “Vertical”**
  - Handoffs between different APs/network providers
  - New IP address
  - Security associated will be different
  - In general not seamless

- **Inter-Network:**
  - Handoffs between 802.11 and others wireless network (e.g., GSM)
  - Requires call-signaling & network -infrastructure support

- **Roaming Support:**
  - STA associates with strongest AP
  - STA stays connected till AP disassociated
  - When disassociated STA scan all ch. to find strongest AP
  - STA authenticates/associates with new AP

- **Cell Handoff Interval:**
  - \( H = \frac{(2 \times R \times (1-2 \times D/100))}{S} \)

**ESS** = Extended Service Set  **SSID** = Service Set Identifier
• Delay incurred during handover due to:
  – Discovery “probe delay Passive-Scanning” 90% total overall delay
  – Re-authentication; authentication & re-association

• **End-to-end delay budget should be < 250ms:**
  – Transmission; propagation + MAC (collision + backoff)
  – Processing
  – Codec
  – Standards

• 802.11 standard issues
  – Doesn’t allow STA associated with two APs simultaneously
    • **Break-before-make** handover unlike cellular technology
      “make-before-brake”
  – With re-authentication 802.1x & .11i handover takes 300-500ms
    • Include scanning, joining new ch, authentication & association.
    • Establish secure key introduce delay “four handshake”
  – Doesn’t prevent SATs being authenticated with multiple APs
    • This authentication is tunneled through current AP & resulted pairwise keys cached in Site Table → handover delay shortened
VoWLAN Coverage/Handover Cont.

- **Recommended 15%-20% cell overlap to avoid dead spots**
- Closely placed APs cause STAs to roam too often
- **Place VoWLAN AP every 300m² instead of 500m²**
- **Further Enhancement**
  - 802.11r-fast handover:
    - cache context “neighbor graph”
  - 802.11K-Radio resource measurement enhancements
    - Channel report sent by AP
    - Neighboring Report sent by AP
  - 802.21 “make before brake”
    - Enabling seamless handover between heterogeneous network types
VoWLAN Fast Secure Handover

Layer 2 “Horizontal” - Same IP Subnet & using 802.1x/EAP

Central Authentication Server

With CAS handover delay reduced from 500ms to 100ms

802.1x Master-Secret (certificate, password, etc.) → Pairwise Master Key → Pairwise Transparent Key → Per Packet Key
VoWLAN Fast Secure Roaming Layer 3 “Vertical”-Different IP Subnet

1. Client associates with AP and receives an IP address, optionally using WPA (802.1x) or VPN for security.
2. Control “B” creates client database: MAC & IP, security context & association, QoS, etc.
3. Client roams to new subnet or roams out of radio coverage and returns.
4. Client associates with new AP & controller. Client database is copied to new controller.
5. New controller recognizes roaming event and provides client with the same initial IP address.

GRE = Generic Routing Encapsulation is a tunneling protocol.
VoWLAN Capacity

- What is the max. number of voice call AP can support?
  - Ask your vendor
- Channel Capacity is function of:
  - Transmission rate “throughput”
  - Voice packet payload length depended on encoding
  - Packetization interval
- Capacity enhancement solutions:
  - Enhanced air access MAC “HCF”
  - Header compression
  - Frame aggregation

Timing Overhead of single Voice Frame over 802.11b

<table>
<thead>
<tr>
<th>Delay component</th>
<th>Time (μs)</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCF Inter Frame Space (DIFS)</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Average channel access delay due to CA</td>
<td>310</td>
<td>31/2 slots × 20 μs</td>
</tr>
<tr>
<td>Voice Frame (G.729)</td>
<td>14.55</td>
<td>20/1.375(Mbps)</td>
</tr>
<tr>
<td>RTP/UDP/IP encapsulation</td>
<td>29.09</td>
<td>40/1.375</td>
</tr>
<tr>
<td>LLC/SNAP encapsulation</td>
<td>7.27</td>
<td>10/1.375</td>
</tr>
<tr>
<td>MAC header and trailer</td>
<td>20.36</td>
<td>28/1.375</td>
</tr>
<tr>
<td>PLCP preamble and header</td>
<td>192</td>
<td>Long preamble</td>
</tr>
<tr>
<td>Short Inter Frame Space (SIFS)</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>PLCP preamble and header (for ACK)</td>
<td>192</td>
<td>Long preamble</td>
</tr>
<tr>
<td>MAC header and trailer (for ACK)</td>
<td>10.18</td>
<td>14/1.375</td>
</tr>
<tr>
<td>Total</td>
<td>835.45</td>
<td></td>
</tr>
</tbody>
</table>

With DCF to transmit 22us (30 byte) voice payload takes 835 us → 3% efficiency

Packetization Overhead = \(\frac{40+34+24}{40+34+24+160 \text{ (G.711)}}\) ≈ 40%
VoWLAN Capacity Cont.

**Throughput Effect:**

- Transmission rate affected by channel condition & distance
- 80.11b is around 6Mbps & 802.11a/g around 26/17Mbps
- VoIP capacity can not be estimated based on raw data throughput:
  - **Common mistake:**
    - Assuming 10Kb/s voice source, theoretical capacity of 802.11b is 11Mbps/10Kbps =1100 → **550** two-way VoIP sessions.
    - In practice only a few VoIP users can be supported in 802.11b!
    - Low payload to overhead ratio for short VoIP packets and inherent inefficiency in 802.11 MAC
VoWLAN Capacity Cont.

Packet Interval/Vocoder Effect:

- Voice call # increase w/packet interval increase
- 10/10/30ms intervals used for G.711/G.729/ G.723
- Many vendor select 30ms
- VoWLAN 802.11a 5x than VoWLAN 802.11b
- But larger packetization interval \(ightarrow\) more end-to-end delay
VoWLAN Location Tracking

How to track a E911/E112 VoIP caller’s location

- WLAN:
  - RF fingerprinting traces signal strength for every signal heard by AP

- Cellular:
  - Network provides the ability to do Global Position System for mobile phones
VoWLAN Deployment

• Fixed-Mobile Convergence (FMC):
  – Allows mobile phones to connect to Wi-Fi networks when available

• Enterprise FMC:
  – IP PBX-Centric:
    • vendor specific
  – IP PBX-independent:
    • Special client software on the hand set
  – Carrier-Centric:
    • No need to integration with enterprise IP PBX
    • Compensate for poor in-home cellular coverage
    • UMA most successful form
VoWLAN Deployment Cont.

Carrier-Centric:

• Unlicensed Mobile Access (UMA):
  – Allows mobile phones to connect to Wi-Fi networks when available
  – Make-before-break handoffs
  – Switch to cellular network as they move out-of-range of WLAN AP “hot spot”
VoWLAN Deployment Cont.

• IP Multimedia System (IMS):
  – Aid the access of multimedia and voice applications from wireless and wireline terminals “FMC”
  – Dual-mode telephony use VoIP in both the cellular and Wi-Fi via IMS
  – SIP based
  – IMS is like re-invent the public Internet with new singling control overlay
VoWLAN Challenges and Solutions

• Packet Loss:
  – Challenge: RTP: packet loss < 3%
  – Solution: Packet loss concealment & redund. algor.

• Latency:
  – Challenge: One way latency “G.114” ≤ 150 mSec
  – Solution: 802.11e/WMM + wired QoS mechanism

• Jitter:
  – Challenge: Packet arrival time ≤ 30 mSec
  – Solution: Jitter buffer, 802.11e/WMM + wired QoS

• Bandwidth Management:
  – Challenge: loaded network/SW with adv. encoding
  – Solution: load balancing, call admiss. control
VoWLAN Challenges and Solutions Cont.

- **Handset Battery Life**
  - Challenge: improve talk/standby time to 4+/100+ Hrs
  - Solution: U-ASPD, propriety

- **Security**
  - Challenge: avoid eavesdropping, maintain access control
  - Solution: WAP2 (wireless) + VLAN (wired), 802.1x

- **Hand off**
  - Challenge: Maintain connection/quality <50 ms
  - Solution: 802.11r, propriety, 802.11k/.11v (future)
VoWLAN Challenges and Solutions

• Coverage & Capacity
  – Challenge: Pervasive coverage, no dropped call, etc.
  – Solution: HCF, propriety, frame aggregation

• Location Tracking
  – Challenge: meet E911 and E112 requirements
  – Solution: WLAN appliance, GSM/CDMA tracking
Recommendations

• Determine the need for VoWLAN
• Make sure that WLAN coverage is sufficient
• Verify WLAN is ready for VoWLAN
• Ensure VoWLAN compatibility with enterprise WLAN
• Gain experience with single-mode phones before introducing dual-mode “smart phones”
• Understand enterprise security polices & develop “culture security”
• Deploy VoWLAN single console Management
  – Planning correct coverage, density, resilient, performance “QoS”
  – Enables a holistic view of entire network
  – Key for enterprise-wide policy enforcement
Question?