Design Issues in Voice over Wireless LAN

Michael F. Finneran
dBrn Associates, Inc.
(516) 569-4557
mfinneran@att.net
My background...

- Independent consultant, writer, and industry analyst
- Over 30-years experience in telecommunications
- Management and engineering positions at ITT, AT&T, and MDS
- Presented over 2000 training programs in the US, Europe, Asia, Africa, and Latin America
- Published over 200 columns and articles in *Business Communications Review*, *Computerworld*, *ACUTA Journal*...
- Spoken at numerous industry conferences including InterOp, VoiceCon, Mobile Business Expo, ComNet, Wall Street Tech Assn.
- Currently writing a book to be titled *The Complete Guide to Voice over Wireless LANs*
- MBA in Marketing and MIS from Northwestern University and a member of IEEE
Outline

- Solution Elements: Infrastructure, Handsets, Management Systems
- RF Planning and Management
- Voice Quality Issues
- Network Capacity Considerations
- Voice Compression and VAD Impact
- Quality of Service Options: WMM, SVP, ATC
- Call Access Control/Load Balancing
- Hand-off Capabilities
- Security Options
- Battery Life
- Network Management Requirements
Basic Characteristics of Wi-Fi Networks

- **Wireless LAN technology described in the IEEE 802.11 standards:**
  - Maximum range: Around 100 m
  - Operates in unlicensed radio spectrum; no protection from interference from other users.
  - Maximum raw bit rate 11 Mbps or 54 Mbps but declines with:
    - Distance
    - Obstructions in the radio path
    - Interference from other users

- **Shared Media:**
  - All users vie for access to a shared channel
  - Protocol and channel contention reduce maximum throughput to 50% of raw data rate

- **QoS:**
  - Initially no ability to prioritize voice traffic, but that is now available with 802.11e/Wi-Fi Multimedia (WMM)

- **Security:**
  - Had been a major issue but has now been addressed with new options like WPA and WPA2 (802.11i)

- **Battery Life:**
  - Unlike cellular, not designed for power optimization
Elements in the VoWLAN Network

- **WLAN Voice Handsets**
  - Four primary categories:
    - Consumer (e.g. Vonage and Skype Wi-Fi Phones)
    - General office
    - "Ruggedized"
    - Integrated WLAN/cellular
  - Mobile Computers, PDAs, and Laptops with softphone client software are also an option

- **Voice Signaling**
  - WLAN Proprietary: SpectraLink, Vocera (Use separate telephony server)
  - IP PBX Proprietary: Cisco SCCP, Siemens (Use same telephony server as wired phones)
  - SIP-based: Works with any SIP-compliant server

- **WLAN Infrastructure**
  - Normally shared with data, so QoS is essential to ensure voice quality in high traffic periods
  - Must provide coverage throughout the facility, not just in conference rooms and other public areas
  - Separate voice WLAN becoming more practical (Dual radio APs)

- **Interface to Wired PBX System**
  - Exchange calls and support feature transparency
  - Feature transparency varies by product
VoWLAN Configuration

- **VoWLAN Handsets**: Cisco, SpectraLink, Siemens, RIM, Vocera, etc.
- **Telephony Server**: Manages connections for VoWLAN Handsets
- **Wireless LAN**: WLAN Switch-based solutions are preferred as they typically include handoff capability

![Diagram of VoWLAN Configuration]

- LAN Switch
- Wired IP Telephones
- Traditional Telephone Services
- Trunk Gateway
- Telephony Server
- 802.11 Equipped Handsets
Each wireless LAN requires a radio channel (Selected in the AP)
- Home/small office networks require only one channel
- Large-scale networks are configured with overlapping cells
   - There are 3 non-interfering channels in the 2.4 GHz band, and 23 in the 5 GHz band
   - Channels should not be reused in adjacent cells
   - Some coverage overlap is recommended for load balancing
   - Excessive overlap causes "association thrashing"
WLAN Design/Operations Challenges

- **Dense, Pervasive Coverage:** Whereas data WLANs might cover defined work areas, a voice network must be available throughout the facility and provide good signal coverage to ensure efficient operation.
- **Network Layout:** Site planning required to ensure adequate capacity and coverage.
- **Channel Assignment:** Channel assignment and power adjustment needed to limit co-channel interference.
- **Security:** If security information is stored in each access point, a security exposure is created if an access point is stolen.
- **Traffic Monitoring:** Manual process of collecting performance statistics from APs.
- **Detecting Rogue/Spoofed APs and Ad Hoc Networks:** Requires periodic manual sweeps or a separate continuous monitoring system (e.g., AirMagnet, AirDefense, etc).
WLAN Switch Solution

Wireless LAN Controller:
Centralizes the operation, security, and network management functions and uses a relatively "dumb" access point.

Client device associates with the central controller.

Authentication Server

LAN Switch

“Thin” Access Point

Wireless LAN Controller
Voice Quality

- **Fundamental Quality**
  - Voice quality is a factor of voice coding and packet loss

- **Transit Delay**
  - WLANs typically add about 20- to 30-msec additional delay to the path
  - End-to-End Objective: Max. 150 msec one-way delay

- **Jitter**
  - The contention-based operation of the WLAN will increase jitter
  - Adaptive jitter buffers are preferred, as fixed-size buffers would have to be set to accommodate the worst-case performance

---

### Comparison of Voice Coding Systems

<table>
<thead>
<tr>
<th>Standard</th>
<th>Bit Rate</th>
<th>Encoding Time</th>
<th>Loss Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 PCM</td>
<td>64 Kbps</td>
<td>.25 msec</td>
<td>10%</td>
</tr>
<tr>
<td>G.726 ADPCM</td>
<td>24 K or 32 Kbps</td>
<td>.25 msec</td>
<td>5%</td>
</tr>
<tr>
<td>G.729A</td>
<td>8 Kbps</td>
<td>25 msec</td>
<td>1%- 2%</td>
</tr>
<tr>
<td>G.723.1</td>
<td>5.3 K or 6.3 Kbps</td>
<td>67.5 msec</td>
<td>1%</td>
</tr>
<tr>
<td>iLBC (Skype)</td>
<td>13.3 K or 15.2 Kbps</td>
<td>70 or 45 msec</td>
<td>5%</td>
</tr>
<tr>
<td>BV16</td>
<td>16 Kbps</td>
<td>10 msec</td>
<td>5%</td>
</tr>
</tbody>
</table>
WLANs Impact on Latency

- Network Latency has been the major complaint with packet voice systems
- Requirement: One-way latency <150 msec

<table>
<thead>
<tr>
<th>Hardwired IP</th>
<th>Alcatel OMNI PCX</th>
<th>Avaya S8700/G650</th>
<th>Cisco IP Com Sys</th>
<th>ShoreTel ShoreTel5</th>
<th>Siemens HiPath 4000</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 (64 K)</td>
<td>57 msec</td>
<td>67 msec</td>
<td>54 msec</td>
<td>47 msec</td>
<td>54 msec</td>
</tr>
<tr>
<td>G.729 (8 K)</td>
<td>42 msec</td>
<td>76 msec</td>
<td>71 msec</td>
<td>55 msec</td>
<td>81 msec</td>
</tr>
<tr>
<td>WLAN</td>
<td>81 msec</td>
<td>92 msec</td>
<td>90 msec</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>G.711 (64 K)</td>
<td>87 msec</td>
<td>92 msec</td>
<td>92 msec</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>G.729 (8 K)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Miercom, Business Communications Review, January 2005
Voice Compression/Voice Activity Detection

- Voice Compression
  - Given the limited transmission capacity of a WLAN, you might think that voice compression (e.g. G.729a, G.723.1) would be important.
  - However, there is so much overhead in the WLAN protocol, the impact is actually rather minor.
  - Further, the wired LAN will be using 64 Kbps voice, so we generally use 64 Kbps over the WLAN as well.

- Voice Activity Detection/Silence Suppression
  - VAD was initially described as one of the major efficiency factors in VoIP.
  - As it is rarely used in the wired LAN, we don’t use it in the WLAN either.
Theoretical Maximum Calls

Theoretical Maximum Calls Per WLAN (20 msec Voice Sampling)

<table>
<thead>
<tr>
<th>Codec</th>
<th>802.11b Network</th>
<th>802.11a or g Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11 Mbps</td>
<td>5.5 Mbps</td>
</tr>
<tr>
<td>G.711</td>
<td>23</td>
<td>16</td>
</tr>
<tr>
<td>G.729A</td>
<td>30</td>
<td>24</td>
</tr>
<tr>
<td>G.723.1</td>
<td>44</td>
<td>36</td>
</tr>
<tr>
<td>Skype iLBC</td>
<td>28</td>
<td>22</td>
</tr>
</tbody>
</table>


Note: This analysis assumes “perfect scheduling”, no collisions, and no network overhead - something that will never happen! “Real world” maximums would be about 50% of these numbers.
Capacity/Quality of Service

- **Capacity**: Available throughput on the WLAN serving that area
  - Radio link used (802.11a, b, Mixed b/g)
  - Signal strength (signal/noise ratio) determines transmission rate and affects retransmissions and overall network efficiency

- **Quality of Service**
  - *Any technique that is used in a packet network to give preferred access to one class of traffic over another with the goal of improving performance in terms of delay, jitter, and packet loss for those preferred classes*
    - Switches and routers provide QoS by maintaining separate queues
    - WLANs provide QoS by defining different waiting intervals and back-off counters for different classes ("Access Categories")
    - QoS does not create capacity, it manages scarcity!
      - *If you push someone to the front of the line, you're pushing someone else to the back of the line*
IEEE 802.11e for QoS

The IEEE developed a new protocol option designated 802.11e that will provide Quality of Service (QoS) capability

IEEE 802.11e defines two options:

1. Enhanced Distributed Control Access (EDCA)/Wi-Fi Alliance WMM Certified
   - Contention-based protocol with priority access
   - Provides prioritized channel access, *not* consistent delay

2. Hybrid Controlled Channel Access (HCCA)/Wi-Fi Alliance WMM-SA Certified
   - Contention-free, polled access for consistent delay service
   - The AP takes control of the network periodically and polls selected stations
   - Includes a signaling protocol where stations define requirements for bandwidth, latency, and jitter
   - Wi-Fi Alliance suspended certification due to "lack of interest"
Only EDCA/WMM is being implemented at this time

- Four Access Categories are Defined
  1. Voice
  2. Video
  3. Data (Same as current DCF traffic)
  4. Background Data

- Different waiting intervals (AIFS) and back-off counters for each

Backward compatible with all existing Wi-Fi Certified devices:

- Existing devices are all Access Category 3 (i.e. "Data") by default
- The standard essentially defines two categories above existing devices and one below
WMM Impact on Performance

Source: Wi-Fi Alliance
Vendor Proprietary Techniques

SpectraLink Voice Priority (SVP)
- Most popular technique used today
- Operates only through approved access points (VIEW Certified)
- Basic Capabilities
  - Prioritize Outbound Voice Packets
    - Requires compliant access point
  - Stream Voice Packets
    - Send sequential packets after a SIFS interval
  - Prioritize Voice Retransmissions
    - In the event of a collision, voice back-off set to zero

Meru Networks- Air Traffic Control™
- Proprietary over-the-air scheduling algorithm
- Full overlay (rather than cellular) RF layout
QoS and Call Access Control

**Quality of Service**
- High Priority
- Low Priority

**Data devices pushed to the back of the line!**

**Call Access Control/Load Balancing**
- Excess callers "steered" to alternate AP
- Maximum call load

When the access point is at its defined maximum call capacity, excess users are steered to an alternate AP (Stations may be allowed to "roam in")
Three Generations of WLAN Security

1. Pre-Security: WEP's rudimentary security features are inadequate for enterprise use and require additions or “work arounds”
   a. Dynamic WEP: WEP encryption with an authentication protocol that provides a new key for every session
   b. VLAN/VPN Configuration: Used a secure tunnel over the wireless link

   - Wi-Fi Protected Access (WPA) and its Temporal Key Integrity Protocol
   - WPA Enterprise uses 802.1x for authentication and key distribution

   - IEEE 802.11i privacy based on the Advanced Encryption Standard (AES)
   - Enterprise version also uses 802.1x for authentication and key distribution
WLAN Hand-off Options

Voice devices will be far more mobile than data devices, so the ability to hand-off calls between APs will be critical

◆ **IEEE 802.11r**
  - Developing standard for fast, secure WLAN handoffs
  - Standard not expected before late-2007!!

◆ **IEEE 802.21:**
  - Standard for Local and Metropolitan Area Networks: Media Independent Handover Services defining hand-offs among all 802-series technologies (LANs, Bluetooth, WiMax, etc.)

◆ **Vendor Proprietary Options- WLAN Switch**
  - Most WLAN switches can provide fast (50- to 150-msec), secure handoffs
  - Actual time may increase if the handoff must cross IP subnets or if the station must reauthenticate
  - Multiple strategies are being used to improve handoff times including key caching and shared inter-subnet tunnels
  - Handoffs in 150msec should be more than adequate for voice users
Voice over WLAN Handsets

- **Cisco:**
  - 7920
- **RIM Blackberry**
  - Blackberry 7270
- **Spectralink**:
  - NetLink e340 - General Office Use
  - NetLink h340 - Healthcare
  - NetLink i640 - Ruggedized
  - NetLink 8020/8030
- **Siemens**
  - optiPoint WL1
  - optiPoint WL2
- **Vocera**
  - Communications Badge
- **WLAN/Cellular**
  - Nokia, Samsung, Motorola, etc
- **Prices start at around $350**
## VoWLAN Handset Comparison

<table>
<thead>
<tr>
<th></th>
<th>Cisco 7920</th>
<th>BlackBerry 7270</th>
<th>SpectraLink 8020/30</th>
<th>Siemens optiPoint WL2</th>
<th>Vocera Comms Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN</td>
<td>802.11b</td>
<td>802.11b</td>
<td>802.11a, b, g</td>
<td>802.11b/g</td>
<td>802.11b</td>
</tr>
<tr>
<td></td>
<td>G.711</td>
<td>G.711</td>
<td>G.711</td>
<td>G.711</td>
<td>G.711</td>
</tr>
<tr>
<td></td>
<td>G.729a</td>
<td></td>
<td>G.729a</td>
<td>G.729a/723</td>
<td>Prop. 8K</td>
</tr>
<tr>
<td></td>
<td>WEP/WPA &amp; 2</td>
<td>WEP</td>
<td>WEP/WPA &amp; 2</td>
<td>WEP/WPA</td>
<td>WEP/WPA</td>
</tr>
<tr>
<td></td>
<td>802.1x LEAP</td>
<td>802.1x LEAP</td>
<td>802.1x LEAP</td>
<td>802.1x LEAP, EAP-TLS</td>
<td>802.1x LEAP</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Battery Life

◆ Every Wi-Fi device has a radio transmitter and a receiver
  ✤ The transmitter creates the greater power draw when active
  ✤ The receiver must be on continuously to sense incoming calls
  ✤ An 802.11b transmitter requires less power than 802.11a or g
  ✤ Power conservation was not one of the primary goals in the development of the WLAN protocols
    ◇ Cell phones are typically 10/100 (hrs talk-time/hrs standby)
    ◇ Wi-Fi handsets are typically 3/30 or 4/40 (hrs talk-time/hrs standby)
    ◇ SpectraLink’s 8000 series claim 8/160 (hrs talk-time/hrs standby)

◆ Power Save Mode:
  ✤ Option in the original Wi-Fi standards that allows idle devices to turn off their receivers
  ✤ Must turn on ten times per second to hear Beacon Messages from the AP and send PS-Poll messages to retrieve each buffered frame
  ✤ The 100 msec turn on interval increases timing variation (jitter) for voice
New Power Save Options

- **Automatic Power Save Delivery/WMM Power Save**
  - New option in 802.11e
  - Sleeping device turns on more frequently (e.g. 20 msec) to reduce jitter
  - Transmits fewer packets; does not need to send a PS-Poll to retrieve each buffered frame

- **Other Battery Conservation Strategies**
  - Some WLAN switches filter ARP requests and other broadcast traffic to reduce battery load
  - Good RF Coverage: If a client is sending at a higher data rate, its transmitter is on for a shorter interval and requires fewer retransmissions
  - Transmit Power Control (TPC) can allow the AP to adjust the client transmit power to the minimum required to receive the transmission
  - The IEEE is considering a "paging mode" for idle phones modeled on the cellular network approach
VoWLAN Security

- Users still cite security concerns as a reason not to deploy WLANs
- That viewpoint is essentially out-of-date - we can secure WLANs
- Three generations of WLAN security solutions:
  1. Pre-Security: WEP's rudimentary security features are inadequate for enterprise use and require additions or “work arounds”
    a. Dynamic WEP: WEP encryption with an authentication protocol that provides a new key for every session
    b. VLAN/VPN Configuration: Use a secure tunnel over the wireless link
  2. Current Acceptable Security- WPA Certified:
    - Wi-Fi Protected Access (WPA) and its Temporal Key Integrity Protocol
    - WPA Enterprise uses 802.1x for authentication and key distribution
  3. Best Practices Security- WPA2 Certified:
    - IEEE 802.11i privacy based on the Advanced Encryption Standard (AES)
    - Enterprise version also uses 802.1x for authentication and key distribution
Network Management Requirements

- Post-installation RF Site Survey
- Help desk training/Troubleshooting procedures
- Capacity planning

Network Performance Statistics:
- Calls Per Access Point (Average and Maximum)
- Calls Denied/Load Balanced per Access Point
- Percent of Calls Dropped per Access Point
- Percent of Packet Retransmissions per Access Point
- Average Data Rate Used per Access Point
- Average and Maximum Handoff Times

Call Detail Recording
- Some systems can now monitor SIP signaling exchange and link to record the calling and called numbers
Section Conclusion

◆ WLAN voice is an emerging market

◆ Some critical issues to bear in mind:
  ❖ Data service may be restricted to conference rooms, but voice service must be available throughout the facility
  ❖ A centrally-controlled WLAN Switch should be part of any installation that requires more than a few access points
  ❖ Good voice performance requires dense coverage (few callers per AP and good signal/noise ratio for higher data rates)
  ❖ Call access control and load balancing are also essential in ensuring voice quality
  ❖ If voice and data devices share the same channel, QoS will be needed to prioritize voice (or build a separate WLAN for voice)
  ❖ Wi-Fi is a "power hog" so battery life will be an important consideration in network design
  ❖ Voice users have high expectations regarding quality and reliability
Our Speakers

- Ben Gibson, Director- Mobility Solutions
  Cisco Systems

- Peter Thornycroft, VoWLAN Product Director
  Aruba Networks

- Nate Walker, Senior Director- Product Management
  Meru Networks