Voice-over-Wi-Fi Implementation with Single Stream 802.11n

The 802.11n standard provides for increased throughput and greater range in VoWiFi devices. This article looks in detail at the benefits as well as the implementation issues for mobile devices.

Written By Narasimhan Venkatesh, Redpine Signals

Published in Portable Design, September-2008
www.portabledesign.com

The growth of wireless networks based on the IEEE 802.11 Wireless LAN family of standards has been one of the most outstanding success stories of the technology industry in recent years. Apart from the standards themselves, the universal pervasion of WLANs has been assisted and accelerated by the availability of interoperability testing and certification by the Wi-Fi Alliance—so much so that the term “Wi-Fi” is widely used interchangeably with “WLAN.”

The initial growth of WLAN was in its intended role of providing a wireless data networking capability as a replacement to a wired LAN connection. However, as its capabilities grew—with the standards being enhanced to offer higher data rates, better quality of service and special modes such as power-save—it quickly became an integral part of a large variety of electronic devices including phones, gaming devices, music players, sensors and other consumer devices. Among these, one of the fastest growing applications has been the transport of voice over the wireless network—thanks in part to the popularity of several commercial Voice-over-IP (VoIP) services.

The Wi-Fi Alliance, taking cognizance of the significant potential of Voice-over-Wi-Fi (VoWiFi), has released a certification program called Voice-Personal that helps ensure that the underlying requirements of VoWiFi in Wi-Fi devices are met, in a home or small office environment. Expanding their focus of certification beyond protocol adherence and interoperability, the Wi-Fi CERTIFIED Voice-Personal program focuses on a specific application and is based on performance testing. The program was released in July 2008 and Redpine Signals’ Lite-Fi is among the first products to support the certification.

In this article, we provide a background to VoWiFi performance by examining the factors that enable it to provide a satisfying user experience. We elaborate on some of these requirements and describe how they are implemented in VoWiFi devices.

Requirements of VoWiFi

Voice has traditionally been carried over fixed latency, connection-oriented, low error rate transport medium. These attributes have to be specially provided for in networks

based on WLAN. From a user's point of view, the experience of a voice call over WLAN would be similar to that over an alternative designed-for-voice network if certain requirements are met. These include the following:

Latency: A two-way, interactive communication like voice requires the medium to introduce limited packet latency. The connection should permit a tempo of speech to that in a face-to-face conversation. The generally accepted limit on latency in a VoWiFi network is 50 ms.

Jitter: This is the variation of the time of arrival of packets. Although handled by a jitter buffer at the receiving end, the network is nevertheless required to curb this.

Packet drops: The protocols employed to carry voice packets do not provide for a mechanism to re-transmit packets lost in transmission. Indeed, even if they did, it would not be effective since a retransmitted packet would almost certainly have latency requirements violated. The WLAN protocol, of course, does provide for packet retries at the MAC level and this mechanism helps take care of the occasional packet errors that occur even in good channel conditions. VoWiFi devices are expected to limit packet loss to a few percent in good to average channel conditions.

Power savings: A wireless device would be actually communicating only part of the time—wireless phone, for instance, would be "in use" typically only an hour or two a day. However, the devices would be expected to be "on" all the time—ready to receive a call if one was to come in, and ready to respond to the user to make a call instantly. The original 802.11 specifications do provide for a client device to be in a "sleep" mode and wake up occasionally to check for pending packets, but this power-save specification is not helpful for voice calls where packets arrive every 20 to 30 ms. The 802.11e standard and the Wi-Fi certification of WMM-PS provide for viable power-save states while maintaining other requirements specific to voice calls. This article describes this in detail.

Range of operation: Voice requires a bandwidth that is only a small fraction of the data rate possible in a Wi-Fi network, but it requires it reliably in a location-independent manner. The wireless client implementation at the physical layer is therefore required to handle the multipath and interference scenarios that occur in corners and other remote locations of offices and homes.

Roaming: A VoWiFi user in a large office could easily wander beyond the range of his Access Point while attending a call. Although enterprises are equipped with sufficient access points so as to provide Wi-Fi connectivity throughout the premises, the switch-over from one AP to the other—roaming—must be done quickly enough to keep the voice connection unbroken to the user. The mechanisms involved in roaming are described in greater detail in the sections that follow.

The QoS mechanisms provided in the standards help meet these performance requirements. The WMM certification from the Wi-Fi Alliance verifies for the right implementation of these mechanisms and ensures interoperability with other certified

client and access point products. The 802.11n standard provides for increased throughputs as well as greater range. Range improvement through techniques such as STBC and beamforming, however, do benefit VoWiFi devices. More importantly, the uniform use of 802.11n even in handheld clients is of great benefit to an enterprise that has installed 11n equipment since it ensures that the throughput advantages of 802.11n are preserved.

In the following sections, we elaborate on the important considerations of low-power operation and enterprise-wide roaming in VoWiFi client devices.

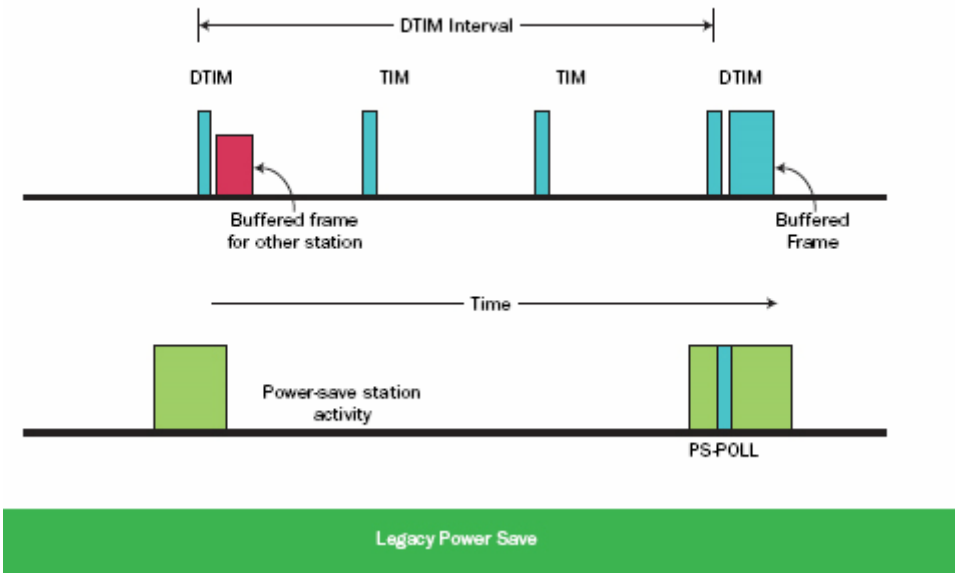
Power Save

VoWiFi phones may be stand-alone phones, or may be integrated with other telephony devices like mobile handsets and cordless handsets. In all cases, the devices are battery operated and sensitive to power consumption. There are two functional modes in these devices from the power consumption point of view. The first is during the state when a phone is kept “on” and is waiting for a call. The power consumed in this mode will determine the standby time of the phone. The second mode is during an active call—this would determine the talk time of the phone. In this section we will go through the various power saving techniques the 802.11 standard offers and their applicability to VoWiFi.

Legacy Power Save Mode

The 802.11 standard allows stations to go into power save and wake-up periodically to listen to the access point’s beacons. The AP buffers the packets of a station if the latter is in power-save mode and indicates the availability of pending packets in the beacon frame. The station, when it wakes up, receives and processes the beacon to check for pending packets and goes back to sleep, that is, power save mode, if there are no pending packets buffered for it. If there are pending packets as indicated in the beacon, the station would continue to stay in the active state and would send a PS-POLL frame to retrieve each of the buffered packets. It goes into sleep state when the “more data” flag is cleared in the received data or management frames. The access point also buffers the broadcast packets for the stations in power save state and delivers them after the DTIM beacon. Stations, therefore, have to wakeup for DTIM beacons to receive broadcast packets. Figure 1 shows the wakeup profiles of two stations in power save.

figure 1



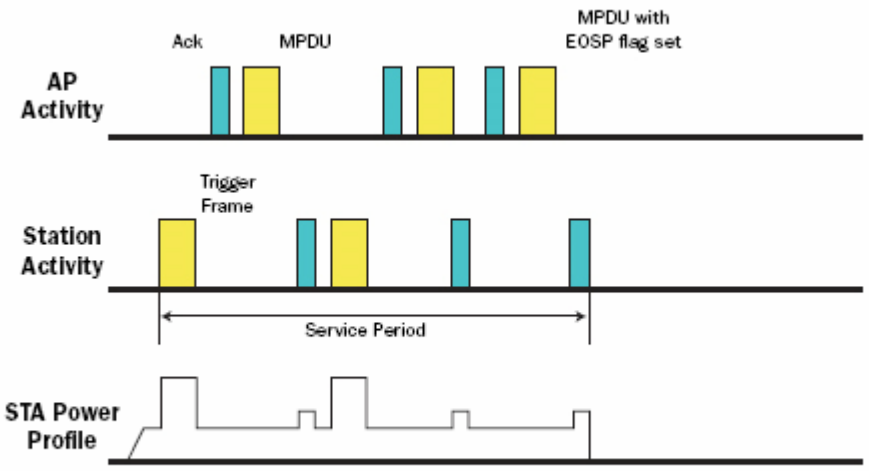
Legacy Power Save

VoWiFi stations during standby can use this mode. The station, however, will not be able to stay in this mode once the call starts as packets could suffer a latency of, say, 100 ms, for a beacon interval of 100 ms, which is not acceptable for VoWiFi.

APSD

APSD, or Automatic Power Save Delivery, was made available in 802.11e. It defines U-APSD, or un-scheduled APSD, and S-APSD, or scheduled APSD. APSD provides a more efficient way of retrieving buffered packets from an AP. With S-APSD, all buffered packets are delivered to a station at a pre-intimated time with respect to the TSF. The station would have to wake up before this and must be ready to receive these packets. In U-APSD, the station would have to send a trigger frame and the AP would deliver the corresponding delivery-enabled frames. It can use any pending data packets as trigger frames or it can send a null frame if there are no pending packets. The station would then continue receiving the packets until it receives a frame with EOSP flag set. Figure 2 shows the frame exchanges in a U-APSD service period. The Wi-Fi WMM-PS certification includes U-APSD operation. VoWiFi stations can use APSD mode during a call. The wakeup period can be configured based on the codec rate. State-of-the-art WLAN modules, including Redpine's Lite-Fi, consume less than 20mW during a VoWiFi call through the use of these power-save techniques.

figure 2

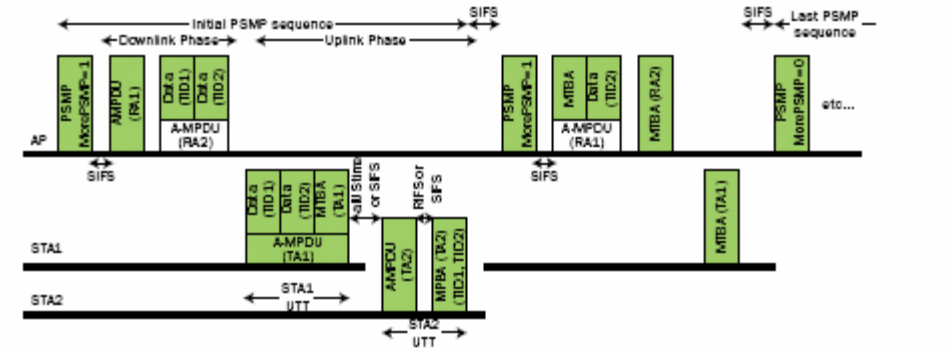


Frame exchanges during a U-APSD activity

PSMP

U-APSD being contention-based is only suitable when there are only a few VoWiFi clients in the network. When the number of VoWiFi clients starts increasing, packet collisions rise and adversely affect the QoS requirements of VoWiFi. Also, a station may have to wake up and wait for its turn to be serviced by the AP, consuming power during the period. Power Save Multi Poll, or PSMP, made available in the draft 8-2.11n standard, addresses these issues. In this mechanism, the AP sends a PSMP frame in which it communicates the uplink and downlink time slots for each of the stations. Figure 3 shows the frame exchanges in PSMP. MTBA, or Multi-TID Block Ack, is also a technique introduced in 802.11n to be used in conjunction with PSMP. With MTBA, a single block-ack frame can include block-acks of different TIDs. A station would have to wake up for PSMP and, with the knowledge of its slot times, would be able to go back to sleep until its uplink or downlink slot time arrives. Usually, though, there would be a fixed cost to going to sleep and coming out of it, and it may not be worthwhile going into a sleep mode for a short duration. The primary advantage of PSMP is seen, therefore, only when there are several VoWiFi clients active at the same time.

figure 3



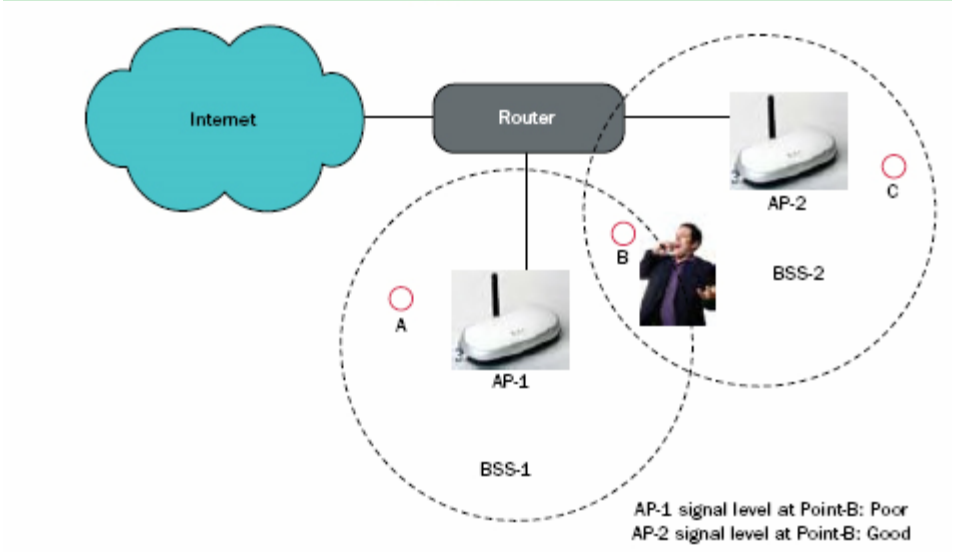
PSMP Frame Exchanges

Roaming

Roaming or handoff is a key requirement of VoWiFi and influences the design of networks supporting VoWiFi in a large way. A mobile STA needs to roam from one AP to another when it moves out of its BSS range, or when the current operating channel conditions get deteriorated. While switching from one AP to the other, at the worst case, an application session may be terminated—requiring it to be re-started after the handover is completed; or in other cases may either experience a temporary outage or at the best case a delay in transfer of packets for a short period of time. Voice applications would not tolerate an outage or session termination, and even a delay in delivery of queued up packets must be minimized—ideally to about 50 ms or less if the mobile user is not to notice a brief degradation in connection quality. In order to maintain application continuity without compromising the key aspects of the connection such as security and power save mode, a VoWiFi-capable mobile station would require using an intelligent roaming mechanism.

In order to understand the challenges of roaming, it is important to understand the process involved in 802.11 roaming. A typical scenario is illustrated in Figure 4.

figure 4



Roaming scenario while moving from point A to C

As shown in Figure 4, a mobile user starts from point A and connects to AP-1 as that is the only AP within his range. He then moves towards point C, via point B. The signal quality of AP-1 at point B is poor relative to that of AP-2. At this point, the Wi-Fi-enabled mobile device should detect AP-2, and seamlessly switch from AP-1 to AP-2 without causing disruption to the user's voice call. This switching involves following tasks, which are to be performed by the mobile STA:

• Discover available Access Points in the vicinity

• Disconnect from its current associated AP

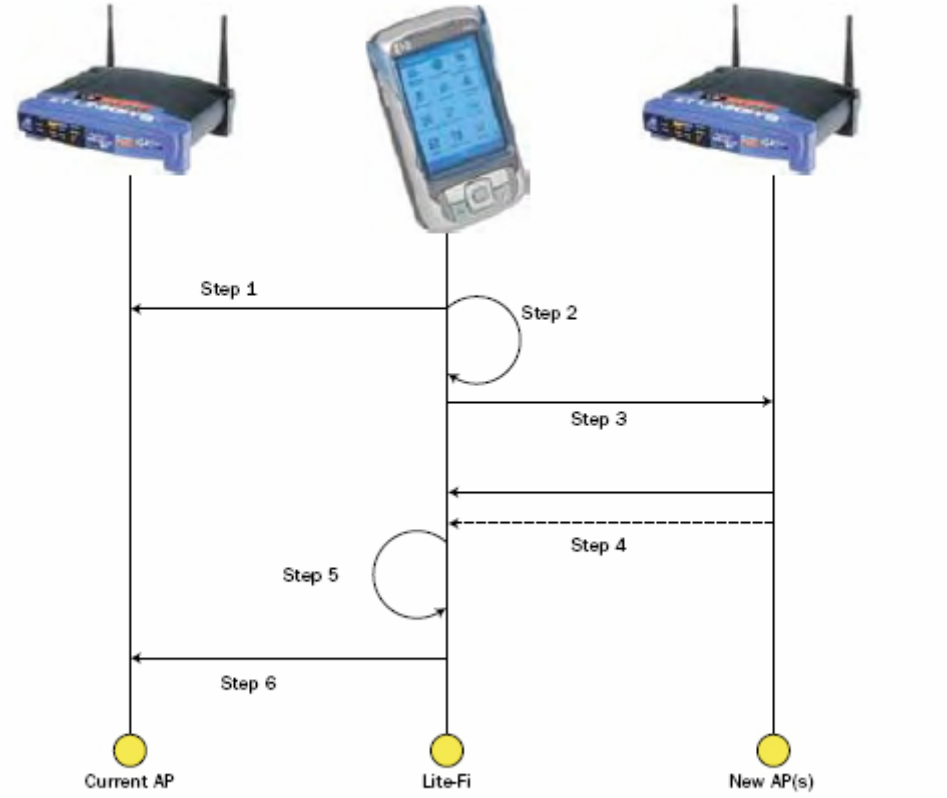
• Establish a connection with the new AP

Generally, in normal traffic conditions, the 802.11 disconnecting process can be completed in less than 1 ms. But discovering APs in the vicinity and establishing a connection with the new AP in, say, an enterprise security mode, can take longer—even more than one second. This latency is, of course, not tolerated by voice applications, which are highly sensitive to packet delays. In practice, clients minimize the AP-discovery and connection establishment delay through a combination of the standards-based and proprietary techniques that generally involve completing most of the tasks that are part of the roaming process in advance.

The IEEE standard defines two methods for discovering Access Points, one through passive scan and the other through active scan. It does not, however, address how a mobile STA can discover APs once an active connection exists between the STA and an AP. As shown in Figure 5, clients use proprietary background scan methods to discover

the available networks on different channels, while maintaining connectivity with the current AP.

figure 5



Background scan mechanism

Step 1: The client indicates to the current AP that it is going into power save mode by sending a null frame with PS bit set.

Step 2: It moves to a different channel.

Step 3: It sends a broadcast probe request that would be read by all APs within range in that channel.

Step 4: The client collects the BSS list based on one or more probe responses or beacons received from APs in that channel.

Step 5: The client reverts back to its previous operating channel.

Step 6: It informs the AP that it is coming out of PS mode by sending a null frame with PS bit off, and resumes data transfer.

During a VoIP call, the client would have only about 20 ms between packets to carry out this background scan. It may, therefore, have to repeat this in case all desired channels are not scanned during one opportunity.

Having built a list of APs, the client is ready to roam when it's time to. The decision to roam is the responsibility of the client. Designers of client devices use their own proprietary mechanisms in making this decision. Factors such as Received Signal Strength Indicator (RSSI), signal-to-noise ratio, frequency of packet re-tries are among those that the client devices analyze in deciding to roam. Sometimes a fresh background scan may take place upon one of these measures reaching a critical value.

The next important task during roaming is connection establishment with the new AP. Depending on the security settings of the AP, this may involve the 802.1x/Extensible Authentication Protocol (EAP) mechanism. The 802.1x/EAP is a time-consuming process based on the EAP type that is employed. The simplest 802.1x authentication, which uses Lightweight EAP (LEAP) method, can take a minimum of 100 ms to a maximum of 1.2s, depending on network conditions. The VoWiFi capable mobile STA should minimize this time to less than around 50 ms for meeting the constraints of the voice application.

In the open system mode, there is no need for 802.1x/EAP authentication. As a result, in this mode, the client can typically complete the roaming process in less than 20 ms, through its active-join mechanism.

In WPA/WPA2 Pre-Shared Key (PSK) security mode, the reassociation process requires an additional 4-way handshake, but not 802.1x/EAP. This handshake takes additional time, but typically would be done within the constraints of VoWiFi.

The advanced WPA/WPA2 enterprise security mode involves the most time-consuming 802.1x/EAP authentication together with the four-way handshake mechanism, during reassociation. As mentioned earlier, this process may take more than 1s, which is beyond the targeted delay for VoWiFi. In order to meet this requirement, the IEEE standard proposes a pre-authentication technique, wherein the client completes the 802.1x/EAP process with the new AP through the distribution system before it decides to roam to this AP. During handoff, therefore, the client would only need to use four-way handshake to obtain the PTK from the new AP. As a result, the client would only take as much time to roam as in the PSK case.

Future roaming methods would use provisions in the forthcoming 802.11k and 11r standards. 11k defines quantifiable measurements on current BSS and neighboring BSSs, so that a mobile STA can make an informed decision to roam from one BSS to the other; and 11r helps a mobile STA by providing a standardized approach to fast BSS transition to minimize roaming time. And there are also proprietary mechanisms being followed today to hasten the roaming process in enterprise security modes.

Certification

Apart from Voice-Personal, there are several certification programs from the Wi-Fi Alliance that are relevant for VoWiFi devices. Certified products have a distinct edge in their ability to provide a uniform user experience in diverse scenarios. The quality of service requirements of VoWiFi are provided by WMM, which covers traffic classes and the priorities afforded to each. WMM-PS helps conserve battery life while a voice or multimedia application is in progress. WPS—Wi-Fi Protected Setup facilitates easy setup of security using a Personal Identification Number (PIN) or a button located on the Wi-Fi device. Voice-Personal, as mentioned earlier, helps ensure the delivery of good quality voice over a Wi-Fi network in a home environment, while the forthcoming Voice-Enterprise certification would do the same in an enterprise environment, adding the requirements of roaming and enterprise security to the test suite to bring about a complete VoWiFi experience in offices and public locations.

Redpine Signals, Inc., San Jose, CA.
(408) 748-3385. [www.redpinesignals.com].

Author Bios

Narasimhan Venkatesh is chief wireless architect at Redpine Signals and has over 20 years experience in communications engineering with expertise in wireless systems design, telecommunications and optical networking. Mr. Venkatesh's responsibilities include leading the development of wireless algorithms and hardware at Redpine's development center in Hyderabad. Mr. Venkatesh holds a Masters Degree in Electrical Engineering from the Indian Institute of Technology, Madras, India.

Peddi Indukuri is a product manager at Redpine Signals. He is responsible for managing all product and customer deliverables for Redpine's WLAN related products. Mr. Indukuri holds an M.B.A from Lancaster University Management School, U.K, a top-30 global B-school, and B.Tech in Computer Science & Engineering from S.V. University, India.

Subba Reddy is an engineering manager at Redpine Signals. He leads the engineering team involved in the design and development of ultra low power WLAN related products. Mr. Reddy is an M.Tech. in Electronics Design and Technology from Indian Institute of Science, Bangalore, India.