

# VoWLAN Myths Busted



?!  
□ □

When using WLAN for voice, there are totally different requirements for the WLAN than if only non-real time applications such as browsing, e-mail, file transfer etc are used. A lot of articles, white papers etc are available on the Internet that contains “old truths” about WLAN operation. Some information is just old, some is erroneous. This document explains some of the requirements for VoWLAN and “busts” old myths...

## 1 “VoWLAN has bad speech quality”

One of the most common misunderstandings is that voice over WLAN by design has “bad speech quality”.

By default, the Ascom i75 is using the G.711 codec, which provides an uncompressed, digitised audio stream. Compared to DECT that uses G.726 ADPCM, the Ascom i75 produces an audio stream with higher audio quality.

However, DECT operates in a protected RF band and each call has its bandwidth needs reserved through an allocated frequency and time slot. For WLAN, all 2.4 GHz devices share the total amount of bandwidth on a best effort basis. Therefore, the audio quality can be degraded when external RF interference sources are present or when the capacity is close to the limit.

**Conclusion:** The audio quality of VoWLAN is better than DECT, but the quality is not guaranteed, degradation may occur due to wireless congestion.

## 2 “VoWLAN is insecure”

Legacy 802.11 with WEP as the only encryption/authentication scheme had vulnerabilities and weaknesses that could lead to eavesdropping, intrusion attacks etc.

However, the amendment 802.11i specifies the use of 802.1X port-based authentication through an external server (RADIUS). With the right choice of authentication algorithm (EAP method) that supports mutual authentication over a secure link,

the authentication is considered to be very secure and suitable for business-critical use.

As protection for eavesdropping, user spoofing and replay attacks, 802.11i specify the use of AES-CCMP. AES is selected by NIST (National Institute of Standards and Technology) as a standard encryption algorithm (FIPS 197).

The details of AES-CCMP are beyond the scope of this document, but the scheme provides strong encryption together with integrity check and countermeasures against replay attacks.

**Conclusion:** With the right choice of security scheme, 802.11 can be considered safe.

## 3 “To prevent unauthorised users from accessing the WLAN, don’t broadcast the SSID”

The statement above is a real lie. The SSID or ESSID is only a common identifier for multiple APs that belong to the same network.

The SSID must be known by a wireless client in order to connect to the WLAN. However, knowing the SSID is not enough to establish a connection if the WLAN is protected by some security mechanism (WEP, WPA etc).

The SSID is sent in clear text in probes, associations etc., so hiding the SSID does NOT keep your SSID a secret.

**Conclusion:** The SSID has nothing with security to do; it is only an identifier of the network.

#### 4 “Plan the cells so the cell overlap is 15-25%”

Somebody said this a long time ago, but nobody seems to remember how the overlap in percentage shall be defined. If the overlap is defined in percentage of cell areas, the 15-25% may be a correct value, but how easy is it to estimate an area?

It is stated in a world leading training program for WLAN that the overlap shall be measured as percentage of the distance. Some basic calculations shows that an overlap of 25% by distance gives a cell overlap by around 2.5 dB... Ascom recommendation is an overlap by 10dB.

**Conclusion:** Never talk about cell overlap in terms of percentage, use real measures, dBm for power and dB for attenuation/gain.

#### 5 “One AP is enough to cover the whole building, because I can ‘see’ the AP with my ‘sniffer’”

What have the sniffer seen? Is the reception continuous or sporadic?

It is probably correct that the sniffer can receive a few beacons or some probe responses at quite a large distance. However these frames are sent with the lowest basic rate, (often 1Mbps) which has a longer range than higher, preferred data rates. As soon as any other WLAN traffic is present, this weak signal will be over-run by stronger RF sources.

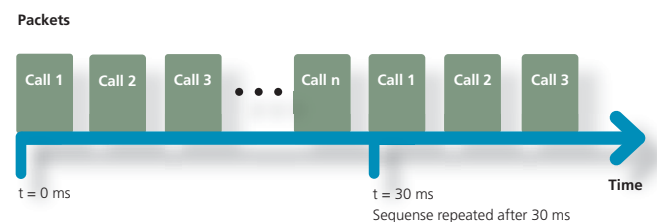
All 802.11-compliant devices try to co-operate, but only down to around -76dBm. For the Ascom i75, the co-channel rejection ratio is around 15dB, which means that if the received signal is more than 15 dB stronger than the interferer, the reception might be successful.

**Conclusion:** Coverage is not enough because the identity can be “seen” everywhere. Use the proper site survey tools.

#### 6 “One call needs 64 kbps... max calls per AP should be approx 54Mbps divided by 64Kbps”

The phrase is as wrong as it can get... First, the voice stream needs 64Kbps in each direction, which equals 128Kbps. Then add overhead due to protocol headers and round upwards, approximately 200Kbps per call.

However, the limitation for maximum number of calls per AP is not related to bandwidth but to time domain constraints: Every 30 ms (Ascom i75 default) one downlink and one uplink speech packet shall be transmitted per call. How many packets can be transmitted before a cycle is completed and the first phone needs to transmit its next speech packet?



Repetitive pattern of voice packet transmission with cycle 30ms.

The figure above shows that there is a need to transmit n packets in 30ms. How long time does one packet transmission require? This is dependant on the mode (802.11b or 802.11g), the Tx rate, if the medium was occupied when the transmission was to begin and some random factor for collision avoidance. This is quite hard to calculate since statistics and probability is involved. Also other traffic such as management frames is present, so the available “air-time” is reduced.

As a theoretical maximum, around 80 calls per AP can be obtained (with Ascom i75 default settings). In our lab research we have easily reached 50 simultaneous calls on one standard off-the-shelf AP. Those numbers of calls will only be possible in a controlled environment and should not be used for deployment calculations.

The numbers of calls is heavily dependant on the AP manufacturer’s design of the real-time sensitive MAC and will vary between different APs.

**Conclusion:** Don’t measure the voice capacity in bits/s, bandwidth calculations can be done for a WAN link etc, but for VoWLAN the time domain is the most critical.

## 7 “An 802.11g Access Point delivers 54Mbit/s of data”

The throughput discussion is probably the most common misunderstanding around 802.11 operations.

It is correct that the maximum payload data rate is transmitted with a radio communication technique that is delivering 54 Mbit/s. However, due to 802.11 protocol overhead and inter-packet transmission guard time, the theoretical maximum throughput is around 35Mbit/s.

Since the channel access mechanism in 802.11 involves random functions for collision avoidance, the real-life throughput peaks just above 30 Mbit/s.

**Conclusion:** The data rate stated is only the maximum data modulation rate and does not state the throughput capacity.

## 8 “WLAN roaming is crap, it uses break before make”

This is true to some extent, a WLAN STA is not allowed to be associated to more than one AP at a time, meaning that in the handover moment downlink packets may be sent to the old AP and thereby get discarded.

WLAN roaming is an action by the client and the basic roaming time is mostly dependant on the client implementation. Many WLAN clients (mostly laptop internal/external card) uses roaming algorithms that results in a gap when scanning and leaving the old AP and associating to the new AP.

The Ascom i75 uses the time slices between the cyclic speech packets to proactively scan for an AP while still connected to the old AP. Due to smart internal timing; the re-association to the new AP is done between two speech packet transmissions which form the basics of the algorithm for a seamless handover. In case of handover the downlink packets must be re-routed to the new AP and is thus subject to infrastructure performance (both APs and the wired LAN).

Use of heavy authentication scheme will affect the hand-over performance, but 802.11i specify methods for pre-authentication and key caching which will speed up the handover process.

**Conclusion:** Since VoWLAN is packet based and time-discrete, seamless handover is possible by smart time slicing.

### Ascom

Wireless Solutions  
P.O. Box 8783 SE-402 76 Göteborg, Sweden  
T +46 31 55 93 00 F +46 31 55 20 31  
www.ascom.com/ws

## 9 “A few 802.11b clients can be allowed on my 802.11g network”

Unfortunately, 802.11b clients will reduce the performance significantly for all clients on the network. 802.11g mandates the use of a special protection mode that will help “b” and “g” clients to co-operate without interfering with each other. This protection mode involves the use of transmission of additional frames proactively before all g mode frames. The protection mode is activated as soon as one single 802.11b STA or AP is present. Also the timing is different (= slower) when a network is running in b mode.

**Conclusion:** 802.11b clients have a huge impact on the performance for the network, causing all clients to use protection mode.

## 10 “VoWLAN phones consumes so much power that the phone gets warm and the battery only lasts for two hours of talking”

This was the case in the past, but new power-saving functions have been standardised by IEEE in the amendment IEEE802.11e and is called U-APSD (Unscheduled Automatic Power Save Delivery). U-APSD is also adopted by the Wi-Fi Alliance under the name WMM Power save.

U-APSD is excellent for a two-way real-time data stream, just like a phone call, and is by design combined with the advantage of packet prioritisation.

A well designed embedded system together with the U-APSD power-saving algorithms have made it possible for talk-times above 10 hours, even with a slim-line battery.

**Conclusion:** VoWLAN phones using the latest standardised power-saving algorithms have talk times that is comparable to other cellular phone technologies.

<b>AES</b>	Advanced Encryption Standard
<b>AP</b>	Access Point
<b>BSS</b>	Basic Service Set
<b>EAP</b>	Extensible Authentication Protocol
<b>ESSID</b>	Extended Service Set Identifier
<b>MAC</b>	Medium Access Control
<b>QoS</b>	Quality of Service
<b>SSID</b>	Service Set Identifier
<b>STA</b>	Station
<b>VoWLAN</b>	Voice over Wireless Local Area Network
<b>WEP</b>	Wired Equivalent Privacy
<b>WLAN</b>	Wireless Local Area Network
<b>WPA</b>	WiFi Protected Access