Harmonize
your enterprise

System Planning
OpenStage WL 3 / OpenStage WL3 Plus

Planning Guide

A31003-M2000-P102-2-76A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Reference No.: A31003-M2000-P102-2-76A9

Harmonize your enterprise

unify.com

Contents

Introduction

This document is intended as a guide for considerations on WLAN infrastructure planning and installation to obtain maximum performance with respect to voice quality. The document handles the RF aspects in the 2.4 GHz and 5 GHz band of a multi-cell WLAN system with a focus on Access Point (AP) placement.

In addition to theoretical discussions of the RF environment in a WLAN system, this document also provides practical examples of how to place APs and verify the placement with the built-in site survey tools included in the VoWiFi Handset.

How to Use this Document

We recommend the use of the WLAN infrastructure manufacturer's installation guide for system planning, logical connection, and configuration of the WLAN system and APs. This document is intended for use alongside the WLAN manufacturer's documentation in order to maximize the voice quality in the VoWiFi system.

General

Introduction to Wireless Planning

Adding Voice to a Wireless LAN

Data and voice traffic has different characteristics and thus put different requirements on the design of the WLAN network.

Data clients, like a laptop set up to use its wireless card for browsing the Internet, tries to use the max packet size that is allowed to transport the relative high amount of data that modern web pages contain. It also uses TCP as its transport protocol and therefore the connection to the web server can withstand delays and loss of packets since the protocol is defined to overcome any glitches in the transfer of data.

Voice clients, on the other hand, use a relative small packet size, but instead require regular access to the radio channels because packets are generated in a steady stream. Since the voice data packet is small, it is important that the overhead created by the protocols is as small as possible. Using UDP instead of TCP reduces the overhead. The acknowledgements that are used in the TCP protocol for every packet sent are also eliminated in the UDP protocol. Since UDP also lacks other features that TCP has, an additional protocol is used, so packets can be sorted in the right order and the voice recorded will be played back at the correct time. This protocol is RTP.

The following table illustrates the differences:

	Data transport	**Voice transport**
Protocol:	FTP, HTTP over TCP.	RTP over UDP.
Packet size:	Varies from small to large up to max size depending on application.	Small All the same size < 300 Bytes.
Sensible to lost packets:	No. Uses built in recovery process in TCP.	Yes. Will result in bad voice quality.
Sensible for delays:	No. Can stand delays of several minutes.	Yes. Requires steady access to the channel.
Sensible for disconnection:	Not always. Session may be restored where interrupted.	Call will be dropped.

In short, the behaviour of the two traffic types - data and voice - make it difficult to design a WLAN for mixed traffic. The demand they put on the WLANs design is nearly diametrical on every point.

Many current WLAN networks are used for data only and seem to be working just fine. Most users do not notice that the WLAN may suffer of congestion, packet loss, and retransmissions etc. The applications are tolerant against such errors and there is no information visible on a laptop about the performance of the network. Slow loading of web pages are accepted and is blamed either on the software or on the Internet and not on the WLAN. When adding VoWiFi to such a network those problems will raise to the surface and be experienced as bad voice quality and will be blamed on the handset.

Furthermore, the design problems gets even more complex if Wi-Fi RFID tagging and location traffic is also using the WLAN, because it requires a completely different design.

The best solution to avoid these design problems is to use separation of traffic types, either physical or logical, so they do not interfere with each other.

Physical separation

A WLAN network can either operate on the IEEE 802.11 2.4 GHz (b/g) or a 5 GHz (a) band. Depending on the WLAN APs used, a network may support either one of those bands or both if the AP is equipped with dual radios. In such a case, the WLAN network can be thought of as two independent WLANs which are physically separated by the usage of different frequencies.

An AP that has only one radio must be using protocol features that mitigate the effects of having different traffic types and patterns in the WLAN.

Physical separation of traffic types in a wire line network is achieved by pulling two cables side by side. It is quite common that IT departments build a second totally independent network used only for management of infrastructure devices that have additional management ports, for example a WLAN controller. The management network will still be functional if the normal network breaks down. Physical separation of WiFi traffic is, however, not possible in any another way than using different radio channels for different traffic types.

If voice has to share the channels with any other type of data, WMM priority protocol must be used.

Logical separation

All clients in a wireless cell have equal access rights to the air if priority schemes are not used. Laptops that uses streaming audio and video applications, like a video conferencing tool, require not just high bandwidth but they will also require steady regular access to the network. The large video packets will take up a lot of the bandwidth and thus the available airtime for a voice call will be less.

Using the IEEE 802.11e standard or WMM will give voice packets, if configured correctly, a higher probability to use the air than other types of packets. This standard will stop data clients from monopolizing the WLAN.

In a network it is possible to use information found in the headers of the packets to identify traffic types and to treat the traffic differently on its route to the destination based on that information.

The information that is written to or read from the headers can be used to prioritize a certain traffic type above another type.

Logical separation of Voice and Data traffic on the same channel

In a wired converged data network, traffic types are often logically separated using Virtual LANS (VLANS). This allows the administrator of the network to set up rules in the switches and routers that treat the traffic types differently depending on the VLAN association of a device. Having devices on separate VLANs (but still on the same physical LAN) will hide the visibility of a device from any other device that is not on the same VLAN. It will also reduce the impact of broadcasts sent in the LAN since only devices in the same VLAN will receive broadcasts. The LAN will actually be divided in smaller broadcast domains, each with its own range of IP-addresses.

Some of the benefits of using VLANs are:

- The possibility to create a separate subnet for management of devices and thus blocking any normal users from tampering with configuration.
- The separation of guest traffic from corporate data traffic which only give guests access to the Internet.
- Reducing the broadcast domain.
- Separating traffic types.
- Protecting devices from access by unauthorized personnel.
- Give priority in the network for some kind of traffic.
- Using role-based access rights and access to a VLANs depending on users group membership.
- Create security rules and allow the use of internal firewalls.

It is important to understand that devices on separate VLANs will not be able to talk with each other if there are no devices in the network that will route the traffic between the virtual networks.

Thus, if using separate VLANs for voice and data devices, for example having a voice VLAN with a Unite messaging server, there must be a route for the managing traffic coming from the data network to the device and also for sending messages from a data device (PC) to the Unite messaging server.

NOTE: **:** Do not implement VLAN without having a clear understanding of which devices that need to talk with each other.

NOTE: **:** Virtual LANs has nothing to do with today's popular Virtual Machine Technology.

VLANs in the air

When using VLANs, a special tag is inserted into the wired data frame, indicating which of the VLANs a frame belongs to. This tag is not defined in a wireless frame and consequently VLANs do not exist in the air. To logically separate traffic types in the air, it is possible to create several SSIDs on the APs. Different SSIDs can be used for different staff categories and guests. In the APs the SSIDs on the wireless side are mapped together with defined VLANs on the wired side and thus give the impression of having VLANS defined in the wireless media.

SSID information is sent out in the beacon packet from the AP normally every 100ms as broadcast packets. Broadcast packets are sent out from the AP at the lowest configured supported speed. Most vendors are using multiple beacons, one for each SSID. The total airtime taken up by the beacons, probe requests and probe responses, will then rise significantly especially if beacons have to be sent out at the lowest speed due to presence of legacy 802.11b devices in the WLAN.

Some APs today allow configuration of up to 16 SSIDs per radio. This traffic can easily consume more than 30% of the bandwidth. A WLAN client may also pick up SSID information from neighboring WLANs, which makes this effect even more pronounced.

It is recommended to limit the use of multiple SSIDs, and the lowest speeds should be turned off.

Combination of Data and Voice Channel Assignments

The handset supports both a and b/g, and it is recommended to have the data and voice traffic on different bands, but not necessary have data on the -a band.

Depending on the existing data and/or voice network, and choice of new installation preferences, the WLAN can be set up as follows, see tables below:

Legacy Network Not Using Any 802.11n APs

b/g	a	Comment
Customer is running single radio APs. Most vendors single radio APs are using the b/g band.		
Data/Voice	-	Due to the limited amount of channels available, any WiFi device must share the airtime. Since voice requires a steady access to the media, it is important to minimize the impact of the other devices in the WLAN by changing the randomness of getting access to the channel. Standard 802.11 implementation does not support any type of admission or congestion control; data is served to clients on a “best effort“ basis. The adoption of WiFi alliance's WMM specification will help, but not solve all of the problems with admission/congestion control. If data clients must operate in the same band as handsets, they must be Wi-Fi Multimedia (WMM) compliant and support 802.11g. Any 802.11b only clients will reduce the overall performance and is not recommended to use. If any legacy b/g-client causes heavy traffic or does not support WMM (QoS), this device should possibly be phased out, be replaced with more modern equipment and moved over to the a-radio band.

Customer Is Running Dual Radios a/b/g APs

b/g	a	Comment
Data (b-radio)	Data + Voice	This scenario is common with older APs that use only b-radio in the 2.4 GHz band. Sharing the bandwidth for data and voice on the a-band is essentially the same as for the b/g radio. Since the bandwidth is shared by the two traffic types, WMM shall be used. This leaves the b-radio free for any legacy clients like bar-code scanners. Most bar-code scanners send little amounts of data. There are more non-overlapping channels to choose from in the 5 GHz band, but special considerations must be taken to plan for the limitations of the available channels due to the use of radars in the same band. (See Section , “802.11a Radar Protection, Dynamic Frequency Selection (DFS)”, on page -13.)

b/g	a	Comment
Data (b/g)	Voice	If the WLAN contains of a lot of b/g data clients, it can be preferable to keep them in the 2.4 GHz band and have all voice clients use the 5 GHz band. The same planning considerations apply if DFS-channels not are used.
Voice (g)	Data	This allows the 2.4 GHz band to be dedicated to voice and all data clients, if possible, are moved to the a-band.

Customer Is Adding 802.11n APs and Is Also Keeping Old APs

It is not uncommon that, when upgrading a b/g WLAN with a second radio for 5.0 GHz, new APs have to be installed (if there is no slot reserved in the AP for a second radio).

Most modern APs include support for the 802.11n standard. When a second AP is installed, old APs may be left in place to ensure that there is no interruption of the current service. The new 5.0 GHz network can then be tuned and configured for n-support and HT-enabled devices can be moved over to the new WLAN.

This also requires additional cable drops and PoE switch ports, running two systems side by side.

Customer buys new APs for the a/n-radio only and keeps the old single-radio b/g APs intact.

New APs set to use only the a-radio. High throughput (HT) only in Greenfield mode.

b/g old AP	a new AP	Comment
Voice + data (legacy) 20 MHz only	Data (HT) 40 GHz only	This may be a solution when upgrading to 802.11n. All laptops can then benefit from the HT speeds of the a/n radio, and the higher amount of channels to choose from. Non-HT clients like handsets stay on the old APs. There is no need for 802.11n support on the b/g band. Upgrade old b-clients if possible to g-clients.

Customer buys new APs for the a/n-radio as an extension and keeps the old dual-radio b/g/a APs intact.

The customer adds a new area to its existing WLAN, for example an extra building, and wants to benefit from 802.11n in the new building.

b/g/a old AP	a/g new AP	Comment
Voice + data (legacy) 20 MHz only	a-radio: Data(HT) and Greenfield mode 40 GHz only g-radio: Voice + data (legacy) 20 MHz only	All laptops can then benefit from the HT speeds of the a/n radio, and the higher amount of channels to choose from. Non-HT clients like handsets must be supported on both the old and new APs. There is no need for 802.11n support on the b/g band. If possible, upgrade old b-clients to g-clients.

Customer buys new APs for the n-radio and keeps the old a/b/g dual radio APs intact.

The customer adds n-supported APs across the complete site.

b/g old AP	a old+new AP	Comment
Voice + data (legacy) 20 MHz only	Data(HT) 40 GHz only DFS+non DFS Greenfield	Turn off the a-radio in the a/b/g APs. This leaves the old AP to support only b/g clients. New APs set to use only the a-radio. HT only Greenfield mode.

Customer buys new APs for the n-radio and keeps the old a/b/g APs intact. Running dual 5.0 GHz radios

b/g	a	Comment
- Old AP Data (legacy) 20 MHz only	New AP Data (HT) DFS Old AP Voice -(no HT),non-DFS, 20 MHz only.	This will allow the voice traffic to run on the non-DFS (Dynamic Frequency Selection) channels and the data traffic to run on the DFS channels. See also, Section , “802.11a Radar Protection, Dynamic Frequency Selection (DFS)”, on page -13.

Customer Has Already Invested in 802.11n Dual Band APs and Has Replaced All Old APs in the Same Position

In installations that support 802.11n from the beginning, or for a WLAN that has been forklifted to support 802.11n, the following scenario may be relevant:

b/g/n	a/n	Comment
Legacy mode	Legacy mode	Customer runs the APs in legacy mode. See above for possible combinations since in this case 802.11n features are not turned on.
Voice + data (legacy) 20 MHz only Mixed mode	Data (HT), 40 MHz Greenfield	The a/n radio is set for Greenfield mode only. Only HT clients accepted and no 20 MHz support. Laptops may benefit from all enhancements in the 802.11n standard like MIMO, dual bandwidth channels etc.
Data (HT) 20 MHz only Mixed mode	Voice (no HT) 20 MHz only Mixed mode	Keep all data clients on the g/n radio. Laptops will benefit from all 802.11n enhancements except the use of double bandwidth channels, since the amount of channels will be dramatically reduced. Note: The handset does not support either Greenfield or 40 MHz modes.
Legacy data	Voice 20 MHz + Data (HT) 40 MHz non-DFS Mixed mode or Voice 20 MHz + Data (HT) 20 MHz Mixed mode	Voice and data are both on the a/n radio. Using 40 MHZ channels for data will reduce the amount of channels possible by half for the handset. Best combination is to move voice over to a/n.

b/g/n	a/n	Comment
Legacy data	Voice 20 MHz Data 20 MHz or 40 MHz Greenfield mode	Note: Greenfield mode is not supported in the handset.

802.11 a-radio Support in the Handset

802.11a Radar Protection, Dynamic Frequency Selection (DFS)

Several of the radio channels (the DFS-channels) available in the 5 GHz band are also used by a multitude of radars both for civilian and military purposes; for an example in aviation, weather radars.

To stop WLAN devices from interfering with radar installations, a radar detection feature must be run on those channels. WiFi radios using this feature send out a specific probe to test for radar existence before they can turn on the radio. When booting an AP it will look for channels that are free from radar traffic and pick one of those. Many AP vendors therefore do not allow an administrator to manually set the channel.

At regular intervals the AP continuously probes for radar detection and will move away from the channel if a radar is detected. Then the AP must dynamically select another channel to use. The probing sequence is quite slow but happens without any disruption in the traffic to/from the associated clients. When the AP moves to another channel, the client may be disassociated for a short while.

The handset supports 802.11h channel-switch announcements, but these are not guaranteed to make the switch seamless. For example, if the AP chooses another DFS channel, the AP must probe for radar on that channel for 60 seconds; hence, the clients associated will be dropped. If the handset is dropped by the AP due to such a switch, an ongoing call may experience a short disruption. Because of this, it is recommended to avoid using DFS channels for voice. If DFS channels must be used due to channel planning make sure that all non-DFS channels also are used.

NOTE: **:** Never use more than 8 channels for voice since this will introduce delayed roaming and jitter.

The following table lists the DFS and non-DFS channels on the 5 GHz band:

Band	Channel	ETSI (EU/EFTA etc)	FCC (US etc)
UNII-1	36,40,44,48	Non-DFS	Non-DFS
UNII-2	52,56,60,64	DFS	DFS
UNII-2e	100,104,108,112, 116,120,124,128,132, 136,140	DFS	DFS **Note:** 120, 124, 128 excluded.*
UNII-3	149,153,157,161	n/a	Non-DFS
ISM	165		

* For the FCC regulatory domain US and others countries the following rules apply for the UNII-2e band:
- Devices will not transmit on channels which overlap the 5600 - 5650 MHz band (Ch 120, 124 and 128).
- For outdoor use any installation of either a master or a client device within 35 km of a Terminal Doppler Weather Radar (TDWR) location shall be separated by at least 30 MHz (center-to-center) from the TDWR operating frequency. Table of current TWDR are to be found in the FCC document "443999 D01 Approval of DFS UNII Devices v01" located at:
https://apps.fcc.gov/kdb/GetAttachment.html?id=33781

Due to the regulations of the DFS channels, a client that does not support radar detection is not allowed to actively scan for APs in these channels. The client will then have to perform passive scanning which means that it only listens for beacons. For a voice client, this will affect an ongoing call to some degree by introducing a slight increase in jitter in the voice stream.
The handset can use the DFS channels, but the voice quality may be distorted and roaming delayed. The DFS channel scan algorithm is optimized and uses both passive scanning and active scanning when it is regulatory ensured that transmitting is allowed.

NOTE: **:** Since the passive part of the scan phase is limited to 70 ms, a beacon interval of less than 70 ms (e.g. 60 ms) will give the best roaming performance.

802.11 n-radio Support in the Handset

The 802.11n standard uses advanced radio technology to boost high throughput levels and more resilient communications links. This is achieved by using multiple antennas and multiple radios in the WLAN equipment (MIMO). The technology can be used to achieve higher speeds or extend the coverage area, where higher speeds will be available further from the AP, and thus the transmission will take shorter time compared with a 802.11a/g transmission.

In the 802.11n specification, a tighter use of the protocols has resulted in less overhead and better use of the channel. This will improve the max speed from 54 Mbps to 75 Mbps.

In 802.11n networks it is also possible to double the throughput by using channels twice as wide (40MHz) than the 802.11b/g/a standards are using (20 MHz). The technique is called channel bonding and combines two adjacent channels into a wider channel, and thus effectively reduces the amount of channels to half.

The standard allows the use of clients that support single channel or double channel width at the same time, but with a reduced set of channels.

The 802.11n standard also allows the use of very large frames to reduce the amount of ACKs needed. This reduces the large overhead known in WiFi, and throughput is raised dramatically from the traditionally 50% up to 90% of the max bandwidth.

The 802.11n builds on the same frequency bands as the 802.11b/g and 802.11a radios and is designed to coexist with older clients. Legacy clients will use lower speeds than the 802.11n clients.

To really benefit from 802.11n, a WLAN that utilizes the 802.11n enhanced standards should be configured for Greenfield mode. This means that no non-802.11n devices should be present in the coverage area. In most cases it is impossible to create such an environment, so 802.11n will run in what is called a mixed/protected mode which will reduce the maximum throughput.

The current 802.11n standards is really only beneficial for data clients like a laptop that are set up for high definition video conferencing or for downloading large files from a server.

The implementation of 802.11n protocol features to be used in handsets have been carefully examined, and features which will not benefit voice have not been implemented.

The MIMO features require more than one radio channel and antennas, which will consume more power and hardware space in the handset. Double sized channel (40MHz) support reduces the amount of channels to half which makes channel planning much more difficult. Using short guide interval (SGI) makes a client more sensitive to interference and may not benefit a moveable client like a handset.

Using 802.11n mixed mode frame when transmitting creates larger overhead (double headers) than if using legacy mode.

The following table lists some 802.11n features in the handset:

802.11n feature	Supported	Comment
Greenfield mode	N	Greenfield mode is unsupported.
40 MHz channel bonding	N	Channel bonding is used to increase bandwidth and a VoWiFi client will not gain much with these higher rates. The handset will not use 40 MHz channels but can operate in that environment if allowed by the system. Battery lifetime is also negatively affected if using 40MHz channel width instead of 20MHz channel width.
SGI	N	Using Short Guard Interval (SGI) increases the probability for transmission errors and is therefore not applied by the handset.
MIMO	N	The handset uses SISO because it does not need to communicate with higher bandwidth and to extend battery lifetime.
Block ACK	Y	Block ACK is supported but not always beneficial to use for VoWiFi.

NOTE: The handset supports, but does not make use of, 40 MHz channel bonding. The handset will prefer the use of legacy data rates in the uplink direction since the MCS rates introduce more overhead.

The amount of channels that can be used for 2.4 and 5GHz bands is illustrated in the table in the section Section , “Basic Cell Planning”, on page -19.

Battery Considerations

Speech Time and Standby Time

Both the speech time and the standby time is greatly affected by the configuration of the network and the power save mode used.

The standby time can be increased several times by following the instructions in chapter Section , “Beacon Period”, on page -28 and Section , “DTIM Interval”, on page -28.

During a call, the power savings are significant with the handset in U-APSD mode compared to Active mode. Note that given times are approximate since there are numerous of variables that affect both the speech and standby time. If the network supports U-APSD, it is strongly recommended to use it.

NOTE: If U-APSD is unsupported by the infrastructure, the handsets will use Active mode even if they are configured to use U-APSD.

If U-APSD is unsupported by the infrastructure, consider the following regarding PS-Poll and Active mode: PS-Poll mode consumes less power than Active mode and thereby extends the speech time. However, PS-Poll mode is designed for low-density residential installations with a single user per AP and cannot meet high speech quality requirements. Therefore, PS-Poll mode is not recommended for use when high speech quality is required; in this case, Active mode is a better choice.

Battery Lifetime

Since the number of charging cycles needed are dependent on the power consumption, the lifetime of the battery is highly dependent of the settings used. A poor network setup with no power save functionality will decrease the lifetime dramatically.

Wired LAN/Backbone Requirements

There are several things to consider when designing a network for VoWiFi:

In order to achieve optimal performance for VoWiFi, the wireless infrastructure should be connected to a switched network (that is, there are no hubs or repeaters).

In a switched network the transmission delay should not be an issue, but if voice traffic is routed, a significant transmission delay could be added.

If the transmission delay is too long an echo will appear in the voice path impacting the systems voice quality. The transmission delay will also add to the speech delay.

Jitter in voice packages will also add to the speech delay since the portable will adjust the jitter buffer size.

See also section <Blue>Chapter , “Known Problems”.

Quality of Service (QoS) Recommendations

To be able to provide voice grade communication over WLAN, the use of WMM or 802.11e is a necessity. These standards define the mapping of priorities on the WLAN to priorities on the wired LAN using either Layer 2 (CoS, Class of Service) or Layer 3 priorities Differentiated Services Code Point (DSCP). Traffic shaping in the switches should be avoided and instead the use of packet-based priority by the STAs should be used. Each packet will be prioritized, according to the standards mentioned above, depending on the packet type.

Priority is primarily needed for wireless prioritization and secondarily for wired LAN prioritization.

The User Priority (UP) or DSCP value of the frame will determine what Access Category will handle the frame.

Four Access Categories (ACs) are defined in the WMM specification:

- AC_BK (background)
- AC_BE (best effort)
- AC_VI (video)
- AC_VO (voice)

WMM maps the User Priority used in the 802.11 frames to a corresponding priority on the wired LAN 802.3 frame.

- Layer 2 priority uses the 802.1p priority field in the 802.1Q VLAN tag, on the wired side of the AP/controller.
- Recommended value for 802.1p priority for voice is 6.
- For both the wired and wireless side of the AP or controller:
- Recommended value for the DSCP value is 46 (EF, Expedited Forwarding) for RTP frames.
- SIP signalling DSCP value (0x1A (26), Assured Forwarding 31 for both handset types).

For further information regarding the infrastructure, see Ascom Interoperability Reports for respective system.

IEEE 802.11 Priority Field

The 802.11 User Priority is sent using the 2 bit QoS Control Field in the 802.11 MAC header.

IEEE 802.1q Priority Field.

The structure of the VLAN Tag defined in 802.1Q is illustrated in the <Blue>Figure 1.

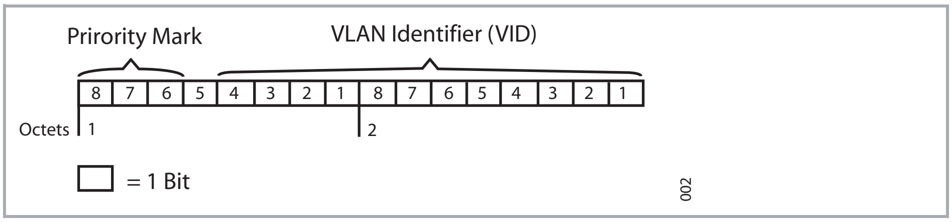

Figure 1 Structure of a VLAN Tag.

NOTE: The use of the 802.1Q VLAN tag does not require an implementation of a full-blown VLAN system since by default all devices belong to the same VLAN and thus can communicate with each other. This VLAN is often called the native VLAN, and often has a VLAN ID of 0.

DiffServ, DSCP Value

The structure of the use of the ToS Field for both the DSCP (new standard) value and IP Precedence (old standard) is illustrated in the <Blue>Figure 2.

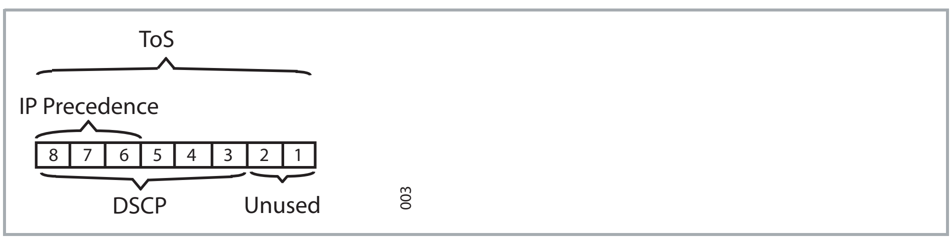

Figure 2 Diffserv Redefinition of ToS Field.

NOTE: Which version of the standard used depends on the software implementation of the switch port. An older device receiving a DSCP field set using the 6 bit code may interpret this as a 3-bit code and drop the last 3 bits, thus efficiently changing the value when the packet is forwarded.

End-to-End QoS

To achieve QoS for a phone call, it is important that QoS is enabled or managed all the way between the two endpoints. By following a speech packet as it travels along the path between the endpoints, it is possible to identify all network segments and transitions where QoS needs to be managed.

Uplink, Handset to AP

The prioritization in the uplink (from handset to AP) is handled by the handset. An internal classification is done at the low-level MAC software and ensures that voice packets are transmitted prior to any other data. All voice packets are marked both with an 802.1D user priority (Layer 2) as well as IP DSCP (Layer 3). By default, the handset marks the DSCP field with the appropriate standard value for real-time data.

Downlink to Wired Network

The AP will preserve the 802.1D user priority by copying the value into the 802.1p priority tag. The IP DSCP value will be unaffected by the transition to the wired network.

NOTE: The 802.1p priority tag is likely not preserved if VLANs are not configured throughout the wired network. If the packets will travel across different subnets, the router configuration needs to cope with preservation of the 802.1p priority tag.

NOTE: Any device that assigns QoS information to a data frame must be connected to a port in the LAN switch which is defined as a trunk port. A trunk port in a switch accepts a frame as legal when it is extended with a VLAN tag.

Normally an access port in a switch will not accept such a frame because the frame is not a standard Ethernet frame.

NOTE: The priority tag can be changed by any intermediate device by an administrator creating rules in the device.

Downlink, AP to Handset

As stated in the section about WMM, if QoS is configured properly, voice packets will gain high priority and thereby minimize latency and packet inter-arrival jitter.

But how does an AP know which packets to prioritize? Two basic methods are defined:

- WMM default (Layer 2 to Layer 2 mapping).
  The classification is done by translating the Layer 2 802.1p priority tag into one of four Access categories and vice versa. This requires that the 802.1p priority tag is preserved in the wired network all the way to the APs Ethernet interface. In most cases, this requires the use of VLAN. A VLAN header includes the 802.1p priority tag.
- IP DSCP mapping (Layer 3 to Layer 2 mapping).
  All IP packets contain a field used for prioritization. This value is called DSCP - Differentiated Services Code Point. In the AP, a rule can be created that map packets with a specific DSCP value to the access category voice and thereby gain priority by using WMM channel access.
  If no classification is done, the downlink packets (from the AP to the handset) will contend for transmission time on the same conditions as all other data traffic. The impact will be bad speech at random occasions when other clients might create load on the system by some heavy file transfer etc.

Security Considerations

The handset can be configured to use various encryption and/or authentication schemes. The use of extensive encryption/authentication schemes can cause incidents of dropped speech during handover due to the time to process the authentication. No speech frames will be delivered to/from the handset until the authentication is successfully completed.

It is recommended to use WPA2. If WPA2 security will be used together with 802.1X authentication, it is strongly recommended to use proactive key caching (also called opportunistic key caching). This feature is supported by the handset and enables the reuse of an existing PMKSA (Pairwise Master Key Security Association) when roaming between Access Points. Roaming and handover times are reduced significantly since only fresh session encryption keys needs to be exchanged by the 4-way handshake.

WPA2-PSK authentication time is reduced by having the initial keys pre-computed in the handset, however encryption keys are exchanged by a 4-way handshake with the AP and may cause a short loss of speech during handover.

For handover times with different security settings on particular WLAN infrastructure, see the appropriate configuration notes in respective VoWiFi configuration manual.

The following security functions are not recommended:

- WEP is not recommended.
- Shared key authentication should be avoided since this authentication scheme makes it easier to crack the encryption key.
- MAC address filtering is not recommended because it does not provide any real protection, only increased administration.
- Hidden SSID is not recommended because it does not provide any real protection and it makes it more difficult for WLAN clients to roam passively.

Certificate

NOTE: Only applicable for handset.

In addition to above security measures, the use of a certificate can help to secure the wireless connection. Once downloaded to the handset, the certificate gives as a permanent access right authentication to the specific user of the handset.

The reverse of the medal is that the handling of the handset is troublesome when using a certificate. A Site Administrator has to handle the administration, which can not be done by the user (it requires the PDM software and the OpenStage WL3 Desktop Programmer cradle). The Administrator must also avoid mixing the handsets when handing them out to the right user.

NOTE: When using a certificate in a handset, the shared phone function cannot be used.

Basic Cell Planning

Cell planning for traditional cordless telephony systems (DECT) deals with coverage and additional capacity reinforcement. Normally, a sufficient number of channels are available to plan the cells for frequency reuse at a distance large enough to limit the effects of co-channel interference.

2.4 GHz-radio b/g/n, Handsets

IEEE 802.11 operation in the 2.4 GHz band only provides the use of three non-overlapping channels, channel 1, 6 and 11. Use of other channels than 1, 6 and 11 has a negative impact on performance in the system since those channels will interfere with each other. The usage of channels other than 1, 6 and 11 will cause a performance reduction. This is not only due to RF interference, but also due to the protocol specification.

Existing systems deployed using four channels (1, 5, 9 and 13) may still may be used. When four-channel systems are used (and 802.11b rates are enabled) there is a risk of increased adjacent channel interference and packet loss, especially when other (three-channel) systems are in the proximity. This may increase with higher channel utilization and traffic load.

NOTE: The use of 802.11n 40 MHz double channels is not recommended since the amount of channels will be reduced to only two (ETSI) or one (FCC).

5.0 GHz-radio a/n, Handsets

In the 5 GHz band there are plenty of non-overlapping channels to choose from. The specific usage and amount of channels that can be used varies with country regulations. The support of the 802.11d in an AP and in the handset will automatically adjust the usage to the so called regulatory domain.

The 5 GHz band consists of several sets of channels listed in the table below. See also Section , "802.11a Radar Protection, Dynamic Frequency Selection (DFS)", on page -13.

Radio	ETSI	FCC
2.4GHz, 802.11b/g/n 20MHz	3	3
5GHz, 802.11a/n 20MHz	4 + 15 (DFS)	9 + 12 (DFS)
2.4GHz, 802.11n 40MHz	2	1
5GHz, 802.11n 40MHz	2 + 7 (DFS)	4 + 5 (DFS)

NOTE: The handset supports, but does not make use of, 40 MHz channel bonding. The channels to support in the handset can be configured using PDM, or the Device Manager(WSG).

NOTE: For examples on channel placing layouts refer to manufacturers planning documentation.

For a multi-cell system based on 802.11 the following factors affects the cell planning:

- Coverage
- Capacity
- Roaming
- Noise interference

The wireless cell planning is done using an AP placement tool which estimates the placement of APs based on the building/campus characteristics. It is recommended that a site survey is done using the built-in tools in the handset. The tool provides a true measurement of the RF environment based upon the radio of the handset. Other wireless analyzers can be used to provide additional assistance during a site survey.

The basic approach to cell planning is to have sufficient overlap between adjacent cells in order to ensure that sufficient radio signal strength is present during a handover between the cells, see <Blue>Figure 3.

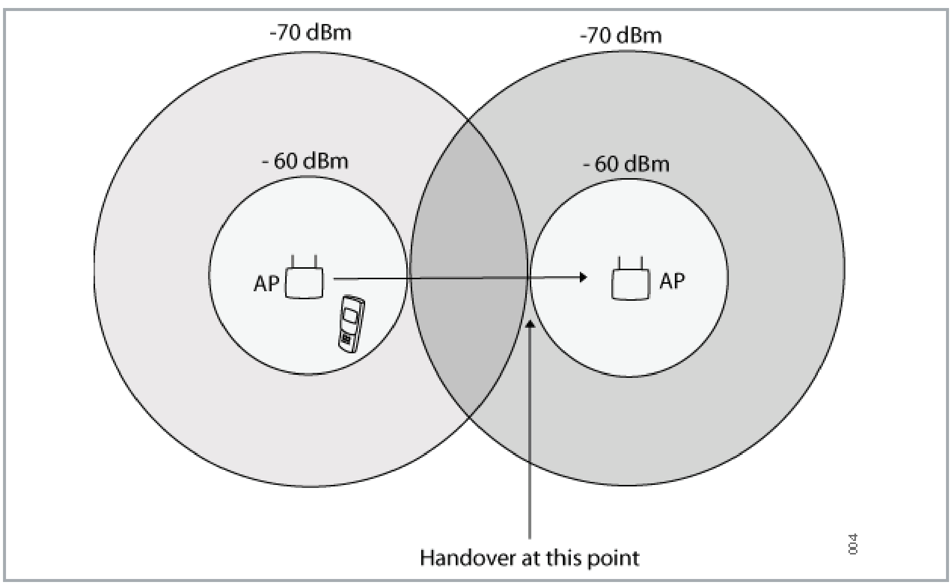

Figure 3 Cell overlap between adjacent cells

The distance between the APs is often a trade-off between the amount of APs and coverage.

To make up for fading effects in an indoor office environment it is recommended that the radio signal strength at the cell coverage boundary does not drop below -70 dBm. The APs should be placed to overlap their boundaries by approximately 6–10 dB.

This means that when the STA reaches a point where the RSSI is -70 dBm, the STA is also inside the adjacent cell and the RSSI from that AP is between -60 to -64 dBm. For information on distance attenuation and attenuation in construction materials, see Section , "RF Signal Corruption in an VoWiFi System", on page -21.

The recommendations above ensure a fading margin of approximately 20dB which should be appropriate for “normal” environments.

NOTE: The illustration in <Blue>Figure 3 is valid when all APs’ transmission power are configured to 100mW (20dBm). Since the handset transmission power is pre-configured to approximately 100 mW, this ensures a symmetric wireless link.

Note that the illustration also is valid for other transmission power settings, but the same power setting must be set in both the handset and AP.

Range vs. Transmission Rate

In order to maintain high capacity in each cell, the radio signal strength must be sufficient at all places in the cell where STAs are expected.

802.11 STAs have the possibility to choose transmission (Tx) rate on a per packet basis. The rates spans from 1Mbit/s to 54Mbit/s (a/b/g) 65Mbit/s (n) and only affects the payload portion of each packet. The different Tx rates are obtained by the use of different modulation schemes. A higher transmission rate uses a more complex modulation scheme than a lower transmission rate.

- The lower the transmission rate, the more energy per bit is available at the receiver's detector. Thereby the transmission range is increased by lowering the transmission rate and thus the transmission will take longer.

As an 802.11 STA moves away from an AP, the Tx rate is lowered in order to increase the range. This has effects on the capacity in the cell. Since all STAs in a cell shares the capacity (air time), a reduction in Tx rate for one STA reduces the overall available capacity for all STAs in that cell.

RF Signal Corruption in an VoWiFi System

There are several causes of signal corruption in a VoWiFi system, and the primary causes are signal attenuation due to distance, penetration losses through walls and floors and multipath propagation.

Free Space Loss

Free space loss (FSL) means that there is a weakening of the RF signal due to a broadening of the wave front (signal dispersion). The RF signals grow weaker as the cell grows larger or the distance becomes greater.

Distance Attenuation

The distance attenuation is highly dependent on the construction of the building, floor plan layout and wall construction material. Some rough figures of attenuation for different materials are presented in the tables below.

b/g	
Material	**Attenuation**
Concrete	12 dB
Brick Wall	10 dB
Dry Wall	5 dB
Window	1 dB
Elevator Shaft	30 dB
Thin Door	2 dB
Book Shelf	2 dB
Plasterboard wall	3 dB

NOTE: The attenuation for the -a radio is, from a general point of view, higher than for -b/g.

Multipath Propagation 802.11n Radios

In relation to the two causes of signal corruption mentioned above, the main concern should be the -a and -b/g radio difference of multipath (reflection, refraction, diffraction and scattering causing signal upfade) and delay spread of the RF signal path (causing signal downfade or even signal corruption) between the handset and AP.

Multipath is that the receiver not only contains a direct line-of-sight radio wave, but also a larger number of reflected radio waves. Because of multipath reflections, the channel impulse response of a wireless channel looks like a series of pulses.

The VoWiFi network has to be designed in such a way that the adverse effect of these reflections is minimized.

The MIMO feature used in the 802.11n standard utilizes more than one radio and one antenna at the same time. This allows the AP and STA to use multiple streams of data which are separated in the air by their phase because they have travelled different paths.

In a legacy WiFi network, receiving signals with different travel path and phase will cause the signal to be corrupted and thus, not possible to be decoded by the receiver.

In the 802.11n standard the multipath signals can be decoded by the individual antennas/radios, where each transmitter and receiving antenna may be able to form a spatial stream. If the antenna pairs are in line of radio sight to each other this will work just fine. Contradictory to what most people are taught in classes that multipath is beneficial for 802.11n, even if the signals have been reflected in several ways on its route to the receiver, too much multipath is bad for 802.11n. Each signal stream can be corrupted in the same way as a single legacy stream, if the multipath propagation is too large.

The difference with the 802.11n standard is that to a certain degree it can tolerate multipath and it can use it to create multiple spatial streams. The establishment of multiple spatial streams is up to the AP and the STA to negotiate. For a moving target like a voice handset this of course will be more difficult since the radio environment changes constantly.

Co-Channel Interference

There are only three non-overlapping channels available in the 2.4 GHz band at 20 MHz which results in a high probability of channel re-use within a close proximity.

In b/g/n 40MHz channels should be avoided in the 2.4 GHz band. With 40 MHz channel width, only one or two channels can be used in the WLAN system (depending on country regulations). Further, interference with neighboring WLANs is more likely due to increased coverage.

There are 19 channels available in total in Europe and 24 in the USA (FCC channels), whereof there are four non-DFS in Europe and nine non-DFS in the USA. Data traffic only can use DFS channels, but it is not recommended for voice, since handsets can not use active scanning due to DFS regulations.

NOTE: The handset can use the DFS channels, but the Voice quality may be distorted.

How closely these channels are reused is dependent on the geometrical prerequisites of the site that shall be covered. If it is a one-floor hallway only, there will be enough distance separation before re-use of the same channel is needed. For a multi-story building with a large floor area, it will be impossible to have coverage at all places without having adjacent cells that use the same channel to some extent.

Installing two adjacent cells working on the same channel introduces the following problems:

1. Capacity reduction. All STAs in the two cells will share the RF channel as if they were present in one cell.
2. Error introduction. The STAs will introduce transmission errors due to the “hidden node problem” described in Section , “Hidden Node Problem”, on page -24.

Clear Channel Assessment, CCA

a/b/g

802.11 specifies a distributed channel access function that basically can be summarized as “listen before talk”. The “listen” procedure is called clear channel assessment and reports if the media (air) is busy or idle. If a STA wants to transmit a packet, it must first determine if the media is idle, then it can transmit the packet. If the media is busy, the STA has to wait for the media to be idle. The same channel access rules apply for an AP.

CCA is affected also by non-802.11 RF signals in the 2.4 GHz band.

Even if APs that use the same channel are placed far away, there can be STAs present in the cells that are closer and thereby causing transmission interruptions, see <Blue>Figure 4.

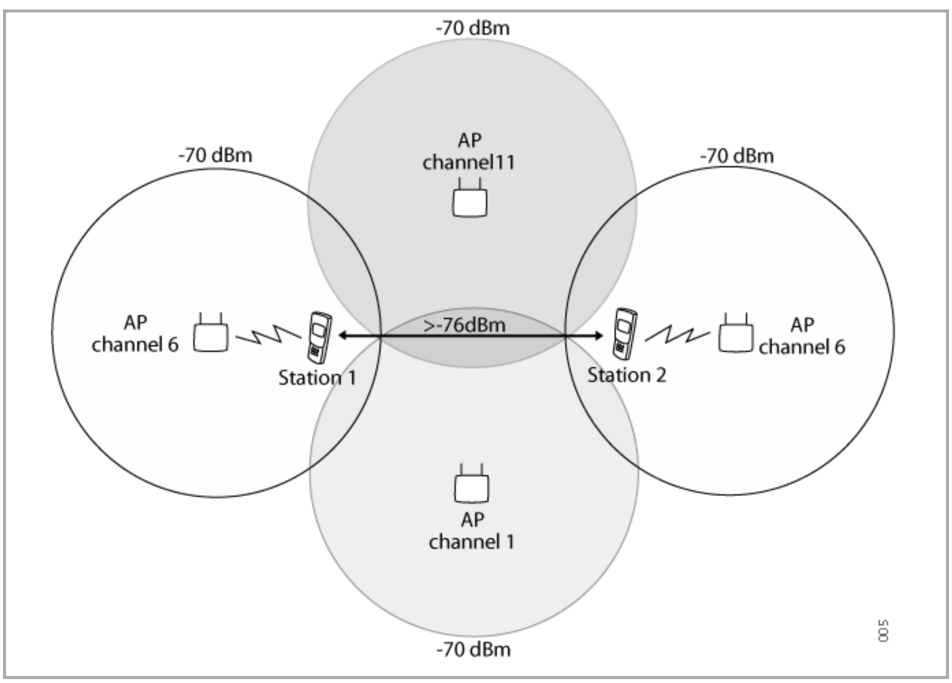

Figure 4 CCA might cause problems even for far away STAs

Handset a/b/g

If the handset detects an energy level that is stronger then -70 dBm or confirmed 802.11 traffic it will consider the air as occupied and not transmit. For example, if it hears an AP with -80 dBm and can identify it as 802.11 traffic, it will not transmit. A non 802.11 disturbance at -72 dBm will, however, not stop the handset from transmitting.

Hidden Node Problem

The “Listen before Talk” mechanism, mentioned in Section , “Clear Channel Assessment, CCA”, on page -23, works as long as all STAs in a cell can hear each other. However, when STAs are positioned at the cell boundaries on opposite sides of the AP, they can not hear each others transmissions. Therefore if they transmit at the same time, collision is likely to occur at the AP which will not be able to receive an error free frame from any of the two STAs.

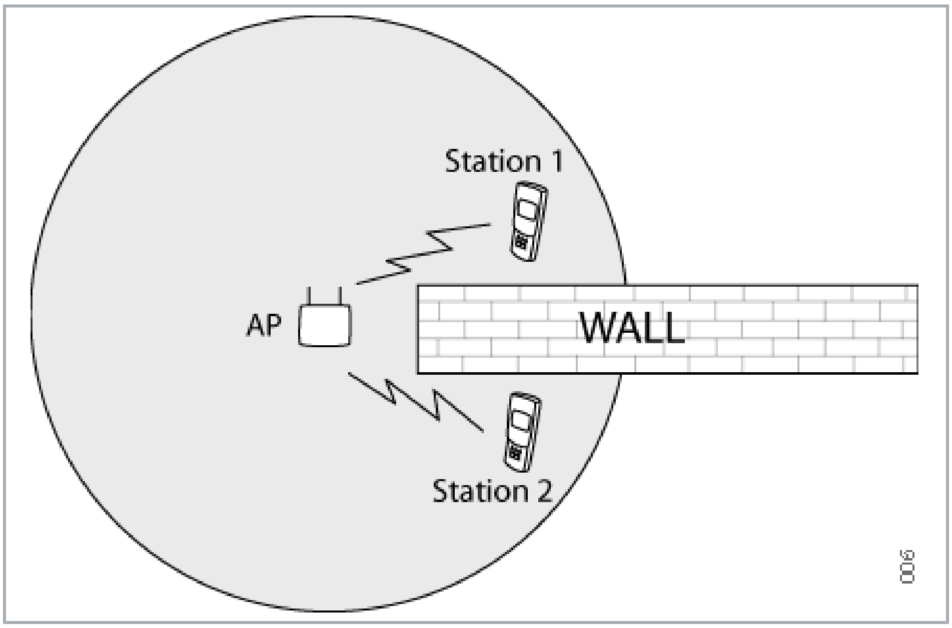

Figure 5 2 STAs and an AP showing simultaneous transmission and collision

The hidden node problem is accentuated when adjacent cells use the same channel. One common solution to this problem is to use Request-To-Send/Clear-To-Send (RTS/CTS). However, the use of RTS/CTS introduces overhead for all clients in the cell and is not recommended.

AP Placement for Optimal Performance

There is a contradiction between the two essential requirements for optimal AP placement. Good performance requires good coverage, but “over-coverage” will reduce the performance.

As described in <Blue>Chapter , “Basic Cell Planning”, enough overlap between adjacent cells is needed in order to have sufficient radio signal strength at all places and enough margin when roaming between cells. However, the co-channel interference problem, described in <Blue>Chapter , “Co-Channel Interference”, is reduced by increasing the distance between APs working on the same channel.

This means that for every unique combination in the cell planning, these two requirements must be proved against each other to obtain the optimal placement.

The AP distance to avoid co-channel interference is described in Section , “Clear Channel Assessment, CCA”, on page -23. The CCA will not introduce any transmission interrupts if the APs or STAs are separated to -76 dBm. However, if two APs on the same channel are transmitting at the same time, the handset will require the interfering signal to be attenuated at least 15 dB compared to their “own” signal.

Different systems have different RF characteristics in terms of co-channel interference suppression, adjacent channel rejection and clear channel assessment. This might have some effect and different systems behave differently with the same set-up.

It is important not only to think of coverage but also on people´s moving patterns, and place the APs so it gives coverage around corners, along walking paths and through thick doors. For optimal coverage around corners, it is recommended to place an AP in the crossroad, see <Blue>Figure 6 below.

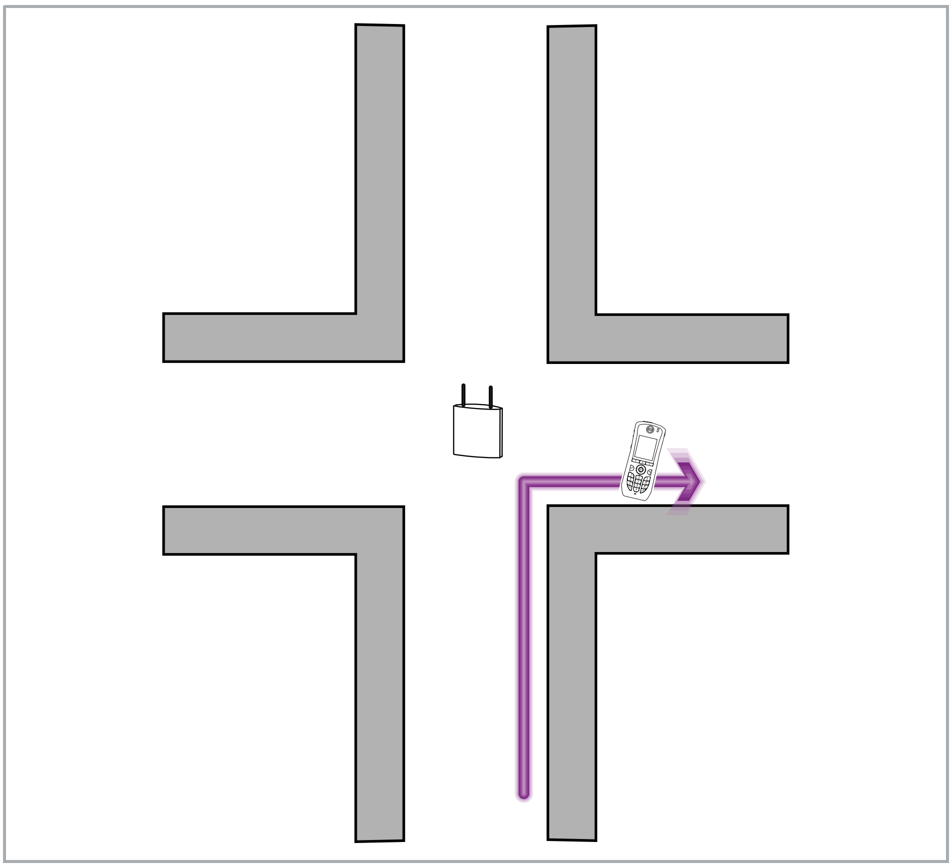

Figure 6 Recommended placement of AP to receive coverage around corners.

In a building with thick walls APs may be needed to be placed inside the rooms for optimal coverage. Then a placement of an AP in the walking path outside these rooms is recommended to minimize the amount of roamings, see <Blue>Figure 7 below. Note that if too many APs are placed in the corridor, the roaming problem is just moved to the corridor APs.

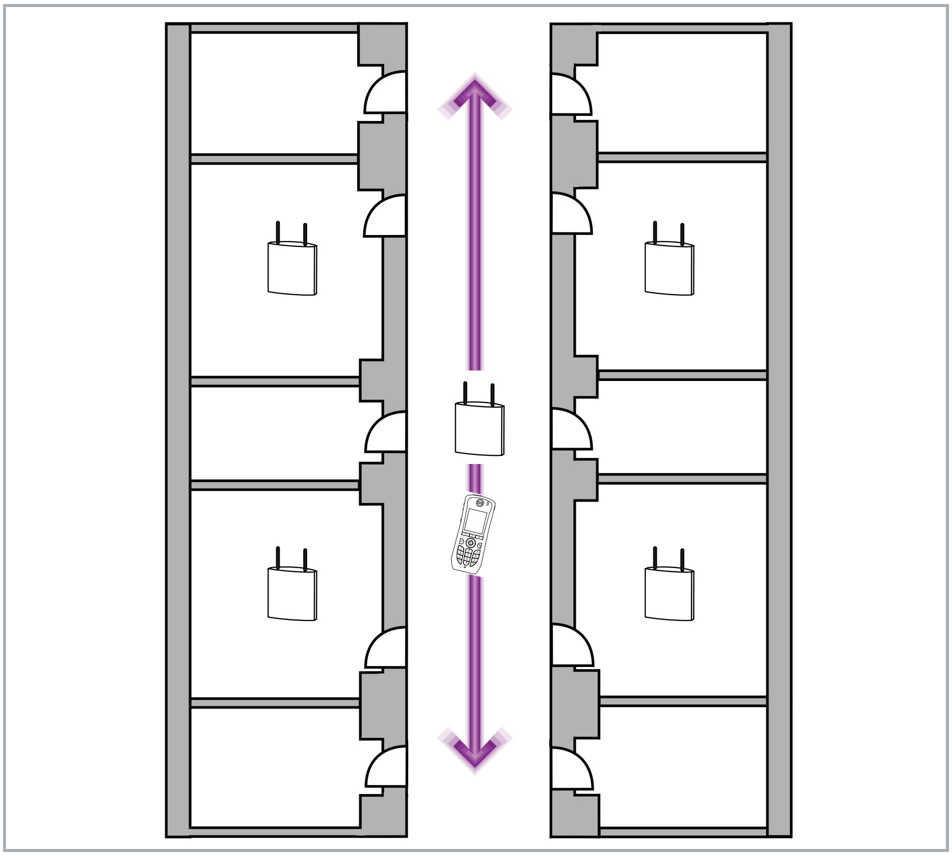

Figure 7 *It is recommended to place an AP in the middle of the walking path to reduce roaming between APs in separate rooms.*

Infrastructure Dependant Features

Automatic RF Adaptations in WLAN Systems

Many WLAN infrastructures make use of an internal tool that is changing the AP channels and/or transmit power level in a dynamic way. The intention of the tool is to compensate for changes in the RF environments due to layout changes of furnishings and/or AP failure.

However, these dynamic changes make the RF environment inconsistent and are not recommended when real-time applications like VoWiFi are deployed. The effects of dynamic RF adaptations when APs switch channels are dropped speech frames and, at worst, the call can be dropped.

If the power level is changed, the link budgets may be asymmetrical with co-channel interference as a result, which will make the WLAN system perform poorly. The handset monitors the output power of the APs and will automatically adapt itself to match in best way possible.

Load Balancing

Some WLAN infrastructures have an “automatic load balancing” feature. The purpose is to dynamically “move” stations between APs in order to avoid overload and to spread the load. The “move” of stations is done by forcing them to connect to another AP than the current one.

Unfortunately, IEEE 802.11 does not provide any procedure for a smooth transition of stations between APs. Instead, the move is done by deauthenticating the station until it associates to another AP.

This forced transition will cause a loss of speech frames, and in worst case the call will be disconnected.

Tools in the Handset

There are a number of tools present in the handset to assist in verification of a WLAN system deployment. For information on how to use the tools, see User Manual, OpenStage WL3 / OpenStage WL3 Plus WLAN Handset.

The basic set of tools includes:

- View with all APs and their corresponding RSSI. Possibility to filter APs based on SSID and/or channel
- Configurable range beep level

AP Configuration

Regulatory Domains - 802.11d

IEEE 802.11d was developed to support the use of equipment across regulatory domains around the world without violation of local frequency rules.The 802.11d regulatory domain information is broadcasted in beacons and contains information on which channels and power levels that are allowed. Since this capability is broadcasted, no regulatory domain configuration is needed at the client side.

To ensure that there is no violation of local frequency rules, the recommendation is to enable the use of 802.11d. At start-up, the handset is listening passively for information about which regulatory domain is present before making any transmissions. This ensures that there is no violation of local frequency rules.

In the WLAN infrastructure, the AP must have the ability to include the country code information element in its beacons and probe responses (Support of IEEE 802.11d). If the WLAN infrastructure does not support the 802.11d information, the handset must be configured manually with regulatory domain information.

Transmission Data Rates

For 2.4 GHz, the option to enable/disable some data rates should not be left to much consideration. As a rule of thumb, all data rates may be enabled. If a transmission fails, the STA will use the next suitable data rate for the re-transmission. In many cases, the STAs rate fallback algorithms is based and optimized for the use of all rates.

If 802.11b only clients should not be allowed to associate to the network and the AP does not have a specific “802.11g clients only” option, this can be accommodated by setting at least one of the 802.11g data rates to “required”.

n-radio

MCS Index	Data Rates Mbps 20 MHz Channel
	800ns Standard Guard Interval
0	6.5

MCS Index	Data Rates Mbps 20 MHz Channel
1	13
2	19.5
3	26
4	39
5	52
6	58.5
7	65

Short/Long Radio Preamble

This only affects the transmissions at 802.11b speeds. The use of short preamble reduces the time spent on the preamble considerably. Only old 802.11b equipment uses long preamble and should not be present on a high performing VoWiFi system.

The 5 GHz band uses a preamble but there is no option to use short or long.

Beacon Period

A beacon is a periodic broadcast transmission from the AP to all STAs in the BSS. The beacon has multiple purposes:

- To synchronize all clients within a BSS
- Beacon contains a traffic indication to notify STAs in power-save mode that the AP has buffered packets waiting for delivery
- To advertise capabilities or changes in capabilities

The most important issue for configuration of the beacon period is the traffic indication for power-saving STAs. STAs in power-save mode wake up at every beacon transmission and check the traffic indication message for any frames being buffered in the AP (i.e. delivery of frames to a STA in power-save mode is only done after a beacon transmission).

This means that a long beacon period will increase the battery life, but also increase the response time to power-save clients.

A short beacon period will decrease battery life and response time. See also Section , “DTIM Interval”, on page -28.

The beacon period is specified in number of 802.11 TUs (Time Units). One TU is 1.024 ms, however to make it easier most APs asks for the value in number of ms. The recommended default value is 100 ms.

DTIM Interval

DTIM (Delivery Traffic Indication Message) interval is the periodic interval when broadcasts and multicasts are delivered in a BSS.

The handset in idle mode utilizes power-save mode and wakes up only at every DTIM interval to receive broadcasts/multicasts and to check the traffic indication message for any buffered frames in the AP. (See section about beacon period).

This means that the DTIM interval in conjunction with the beacon period affects the battery life and the data response time. For good battery conservation and reasonable response times we recommend a DTIM interval of 5 if a beacon period of 100ms is used.

Transmission Power

By default the handset adapts its output power to the APs, but the output power can be configured in five steps between 0-20 dBm as well. Make sure that the APs and clients are configured to use the same output power to avoid asymmetric communication link budgets. The use of anything else in the APs creates an asymmetric communication link budget and is not recommended.

NOTE: The handset can be configured up to 20 dBm on the a and b/g band (note that between 14-20 dBm no fixed steps can be set because of a power amplifier).

Recommended Settings

Basic Configuration

b/g/n		
Item	**Recommended Settings**	**Description**
Radio	802.11g	With a g only network the stations do not need to use protection against b only stations. The transmission rate will be up to 54 Mbps.
	802.11b/g	Mixed mode where b only and g stations coexist will affect the g stations to use protection and the throughput will be decreased.
Transmitting power	Set to match desired cell size.	The default setting for the handset is Auto power. Auto power settings for the APs should be used to ensure a symmetric link. If the output power is manually set in the AP, make sure the APs and clients are configured to use the same output power to avoid asymmetric communication link budgets. Refer to Section , “Transmission Power”, on page -29.
Radio channel	1, 6, 11 (Option for existing systems only: 1, 5, 9, 13)	Do not configure a channel for use that is four or less channels from other channels within the RF range. Doing so will lower the throughput of the WLAN for the stations within those channels.
Regulatory domain (802.11d)	Enabled	
Radio preamble	Short	Long preamble will work but will decrease overall throughput when using b data rates
Beacon period	100 ms	Higher value will increase battery life and decrease throughput. Lower value will decrease battery life and increase throughput.
DTIM interval	5	DTIM setting is related to the beacon interval. The value of 5 is recommended when the beacon interval is 100ms.
Antenna diversity	Enable	Disabled antenna diversity may introduce RF shadows at certain spots.
Short slot time	Enable	This feature will increase the throughput if no b stations are associated at the AP.

a/n		
Item	**Recommended Settings**	**Description**
Radio	802.11a	The transmission rate will be up to 65 Mbps.
Transmitting power	Set to match desired cell size.	If the output power is reduced make sure the APs and clients are configured to use the same output power to avoid asymmetric communication link budgets. Refer to Section , “Transmission Power”, on page -29.
Radio channel	UNII-1, UNII-3	Non-DFS, UNII-3 (only FCC) UNII-2/UNII-2e are DFS channels which can be used, but the Voice quality may be distorted.
Regulatory domain (802.11d)	Enabled	It is important to enter the country code for the regulatory domain.
Beacon period	100 ms*	Higher value will increase battery life and decrease throughput. Lower value will decrease battery life and increase throughput.
DTIM interval	5	DTIM setting is related to the beacon interval. The value of 5 is recommended when the beacon interval is 100ms.
Antenna diversity	Enable	Disabled antenna diversity may introduce RF shadows at certain spots.

* The format of this parameter may differ depending on AP manufacturer, see Ascom Interoperability Reports.

Recommended Security Settings

Handset		
Authentication method	**Encryption method**	**Description**
WPA2-PSK	AES-CCMP	Medium roaming performance Medium security level
PEAP-MSC-HAP v.2*	AES-CCMP	Medium roaming performance** High security level
EAP-FAST	AES-CCMP	Medium roaming performance** High security level
EAP-TLS	AES-CCMP	Medium roaming performance** Very high security level

* The server-certificate is verified by the handset.

** If proactive key caching (Opportunistic key caching) or Pre-Authentication with PMKSA caching is enabled on the WLAN infrastructure.

0.0.1 Quality of Service

Item	Recommend-ed Settings	Description
WMM	Enable*	Disabled QoS may work but there will be no guarantee for high voice quality.

* For the specific infrastructure, see the Interoperability Report.

Identifier

Item	Recommend-ed Settings	Description
SSID	Max. 32 char	A unique identifier which stations use to associate with the AP.
Broadcast SSID	Enable	A broadcasted SSID will assist the WLAN clients to roam passively

Infrastructure Dependant Features

Item	Recommend-ed Settings	Description
Automatic RF adaptation	Disabled	Dynamic changes make the RF environment inconsistent.
Load balancing	Disabled	A forced transition of a client will cause loss of speech frames.

Known Problems

b/g/n

802.11 operates in the 2.4GHz Industrial Scientific Medical (ISM) band. This band is unlicensed and many different wireless equipment uses this band with various radio techniques.

As described in Section , “Clear Channel Assessment, CCA”, on page -23, the CCA makes 802.11 equipment sensitive to other transmissions. This applies to all RF signals, not only other 802.11 equipment.

If CCA problems occur, it will affect the transmission part of the link between the AP and the handset. If the uplink speech (from the handset) drops, the problem is near the handset. Check for nearby equipment such as wireless surveillance cameras, Bluetooth gadgets, WiDi devices, ZigBee/ Z-wave for HVAC controls, Light controls, automation etc.

a/n

DFS channels.

Data traffic in a b/g/n network with large aggregated packets might delay voice traffic.

802.11n

A full-blown 802.11n AP will also saturate the wired link to the Ethenet switch since it can easily pump out more than 100 Mbps of data. Thus to benefit from the 802.11n standard the link to the switch must be upgraded to support Gigabit, otherwise the AP will have to queue data frames and eventually throw away packets.

If the wired network contains a lot of APs connected to the same switch or if wireless traffic has to be route to a common device like a WLAN controller on the wired LAN, the switch itself or the common device may become a bottleneck.

Abbreviations and Glossary

802.11a	IEEE 802.11 standard for transmission rate of up to 54Mbps, operates in the 5GHz spectrum.
802.11b	IEEE 802.11 standard for transmission rate of up to 11Mbps, operates in the 2.4GHz spectrum.
802.11g	IEEE 802.11 standard for transmission rate of up to 54Mbps, operates in the 2.4GHz spectrum.
802.11d	IEEE 802.11 standard for regulatory domains.
802.11e	IEEE 802.11 standard that defines Quality of Service (QoS) for WLAN.
802.11i	IEEE standard security protocol for 802.11 wireless networks that was developed to replace the original WEP protocol.
802.11n	IEEE 802.11 standard for transmission rate of up to 600 Mbps, operates in the 2.4GHz and 5GHz spectrum.
AES	Advanced Encryption Standard.
AP	Access Point: a radio transceiver providing LAN connection to wireless devices.
BSS	Basic Service Set
CAC	Call Admission Control
CCA	Clear Channel Assessment
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code (CBC-MAC) Protocol
CCKM	Cisco Centralized Key Management
Channel bonding	A mode of operation in which two channels are combined to increase performance in some environments.
Delay spread	Measure of the multipath richness of a channel. Because of multipath reflections, the channel impulse response of a wireless channel looks like a series of pulses.
Device Manager	An application that handles devices such as handsets and chargers. It exists in two variants; one server based (delivered in an Ascom Elise product like WSG) and one stand-alone Windows application (PDM).
DiffServ	Differented Services (TOS field)
dBm	Power ratio in decibels (dB) referenced to one milliwatt (mW).
DFS	Dynamic Frequency Selection
DSCP	Differentiated Services Code Point
DTIM	Delivery Traffic Indication Message
EAP	Extensible Authentication Protocol.
EAP-FAST	EAP-Flexible Authentication via Secured Tunnel.
EAP-TLS	EAP-Transport Layer Security.
EDCF	802.11e Enhanced Distributed Coordination Function.
ESSID	Extended Service Set Identifier: used in an infrastructure WLAN that includes an AP.
ETSI	European Telecommunications Standards Institute.
FCC	Federal Communications Commission.
FSL	Free Space Loss.

Greenfield mode	A pure high throughput (HT) mode where packets are transmitted without a legacy-compatible part.
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol: global standard that defines how to send data from one device to another over the wired and wireless media.
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output. Handles the use of multiple radio chains.
Multipath	The receiver not only contains a direct line-of-sight radio wave, but also a larger number of reflected radio waves.
OTA	Over-the-air
PEAP MSC-HAP	Protected EAP Microsoft Challenge Handshake Authentication Protocol.
PoE	Power over Ethernet
QoS	Quality of Service: Defines to what extent transmission rates, error rates etc. are guaranteed in advance.
RF	Radio Frequency.
RFID	Radio Frequency Identification.
RSSI	Received signal strength indication.
RTP	Real-time Transport Protocol
SGI	Short Guard Interval, a tighter intersymbol time gap in a WiFi transmission that reduces the idle overhead and may improve throughput with around 10%.
SISO	Single-Input and Single-Output, the use of only one antenna both in the AP and STA.
SNR	Signal-to-noise-ratio.
SSID	Service Set IDentifier. The name assigned to a wireless Wi-Fi network.
STA	Station: a mobile device in an IEEE802.11 WLAN system.
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOS	Type of Service
TSpec	Traffic Specification.
UDP	User Datagram Protocol.
UP	User Priority.
VLAN	Virtual Local Area Network.
VoWiFi	Voice over Wireless Fidelity: is a wireless version of VoIP and refers to IEEE 802.11a, 802.11b or 802.11g network.
WEP	Wired Equivalent Privacy
Wi-Di	Wireless Display, an Intel technology to transmit a laptop's display to a TV-screen or Projector using WiFi.
Wi-Fi	Brand of Wi-Fi Alliance, which certifies interoperability of products and services based on IEEE 802.11 technology.
Wi-Fi Direct	A WiFi standard that allows devices to talk with each other without the need of an access point. Formerly known as Wi-Fi peer-to-peer. Implementations use a soft AP software in the device and the ad-hoc protocol for connection.
PDM	Portable Device Manager: Used for management of portables, editing of parameters and updating the portables with new software.

WLAN	Wireless Local Area Network (LAN): A type of LAN in which data is sent and received via high-frequency radio waves rather than cables or wires.
WMM™	Wi-Fi Multimedia™: Offers QoS functionality for WiFi networks.
WSG	Wireless Service Gateway: a module that enables wireless services to and from the WiFi Handsets in a WLAN system. It also includes the Device Manager.
WPA2™	Wi-Fi Protected Access™: A set of security features for wireless networks based on IEEE 802.11i.
ZigBee	IEEE 802.15.4 standard that operates in several bands among them 2.4GHz band, using direct sequences spread spectrum using low speed and low power radios. Used for applications like telemetry, electronic signs in retail and control applications, for example, HVAC (Heating, Ventilation and Air Condition).