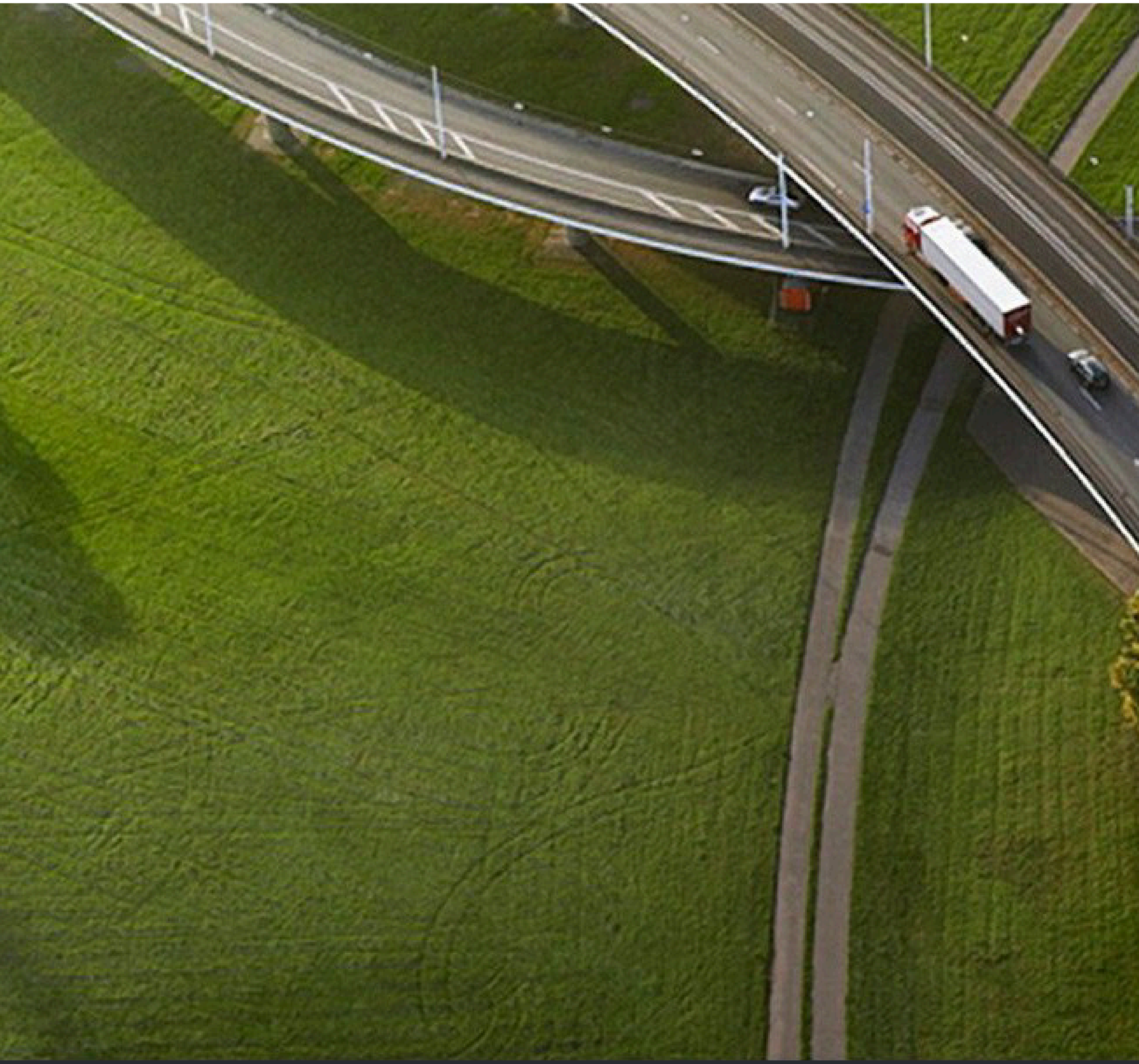
unify
atos collaboration solutions



System Planning
OpenScape WL 4 / OpenScape WL4 Plus

Planning Guide

A31003-M2000-P103-01-76A9

Provide feedback to further optimize this document to edoku@atos.net

As reseller please address further presales related questions to the responsible presales organization at Unify or at your distributor. For specific technical inquiries you may use the support knowledgebase, raise - if a software support contract is in place - a ticket via our partner portal or contact your distributor.

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-P103-01-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

unify.com

Contents

Introduction

This document describes how to plan for an optimal VoWiFi System when deploying the OpenScape WLAN Phone WL4. This document is intended as a guide for considerations on Wireless Local Area Network (WLAN) infrastructure planning and installation to obtain maximum performance with respect to voice quality. The document handles the Radio Frequency (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 with the WLAN manufacturer’s documentation to maximize the voice quality in the VoWiFi system.

Overview

Data and voice traffic have different characteristics and thus put different requirements on the design of the WLAN. This chapter describes how to set up a WLAN designed for mission-critical data communication, especially Voice over Internet Protocol (VoIP) traffic.

Introduction to Wireless Planning

When designing for mission-critical data communication, it is important to have short roaming times and low-latency communication to avoid disruptions/breaks in the voice communication. Most data traffic functions well even if all the considerations for a mission-critical, low-latency network are not met.

Data applications, like browsers, try to use the maximum packet size that is allowed to transport the relative high amount of data that modern web pages contain. They also use Transport Control Protocol (TCP) as 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 applications, on the other hand, use a relatively 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 User Datagram Protocol (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 is played back at the correct time. This protocol is Real-time Transport Protocol (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 maximum size depending on application.	Small. All the same size < 300 Bytes.
Sensible to lost packets	No. Uses built-in recovery process in TCP.	Yes. Results 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 can be dropped.

In short, the behavior of the two traffic types - data and voice - makes 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 congestion, packet loss, retransmissions, and so on. 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 rise to the surface and they are experienced as bad voice quality and they are blamed on the handset.

Furthermore, the design problems get even more complex if Wi-Fi RFID tagging and location traffic are also using the WLAN, because they require a completely different design.

The best solution to avoid these design problems is to separate traffic types, either physically (see Physical Separation on page 6) or logically (see Logical Separation on page 6), so they do not interfere with each other.

Physical Separation

A WLAN network can either operate on the IEEE 802.11 2.4 GHz or a 5 GHz 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 that 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 the 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 Wi-Fi 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, Wi-Fi Multimedia (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 use streaming audio and video applications, like a video conferencing tool, require not only high bandwidth but also steady regular access to the network. The large video packets take up a lot of the bandwidth and thus the available airtime for a voice call is less.

Using the IEEE 802.11e standard or WMM gives voice packets, if configured correctly, a higher probability to use the air than other types of packets. This standard stops 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 Local Area Network (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) hides the visibility of a device from any other device that is not on the same VLAN. It also reduces the impact of broadcasts sent in the LAN since only devices in the same VLAN receive broadcasts. The LAN is actually divided into smaller broadcast domains, each with its own range of IP-addresses.

Some of the benefits of using VLANs are:

- Creating a separate subnet for managing devices and thus blocking any normal user from tampering with configuration.
- Separating guest traffic from corporate data traffic, which only gives guests access to the Internet.

- Reducing the broadcast domain.
- Separating traffic types.
- Protecting devices from access by unauthorized personnel.
- Giving priority in the network for some kind of traffic.
- Using role-based access rights and access to a VLAN depending on user group membership.
- Creating security rules and allowing the use of internal firewalls.

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

Thus, if using separate VLANs for voice and data devices, there must be a route for managing traffic coming from the data network to the device.

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

NOTICE: Virtual LANs have 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 Service Set IDentifiers (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 then rises significantly.

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 turn off the lowest speeds.

5GHz Radar Protection in DFS Channels

This section briefly explains how radar detection in Dynamic Frequency Selection (DFS) channels works, and how to mitigate its impacts on wireless networks.

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.

At regular intervals the AP continuously probes for radar detection and moves 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 are dropped. If the handset is dropped by the AP due to such a switch, the data traffic is delayed for a short while. This may result in a short disruption in a voice call, but would probably not be noticed for other types of data traffic. 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.

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

Band	Channel	Type of channels
UNII-1	36,40,44,48	Non-DFS
UNII-2	52,56,60,64	DFS
UNII-2e	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144[1] [2]	DFS
UNII-3	149, 153, 157, 161, 165	Non-DFS, allowed in some countries

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 then has to perform passive scanning, which means that it only listens for beacons. For a voice client, this affects 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.

Support for 802.11 krv

The handset normally monitors the Received Signal Strength Indication (RSSI) level and performs a scan to find a better AP when the signal strength drops below a certain level. If it finds a better candidate AP, it attempts to roam to it. If not, it continues to scan periodically.

The more channels the handset has to scan, the longer each scan round takes. This is especially true for DFS channels, where only time-consuming passive scanning can be performed. Longer scan times mean bigger risk that voice quality is affected. This is why it is strongly recommended to limit the number of channels the handset has to scan, and avoid using DFS channels if possible.

One recommended way to limit the number of channels the handset has to scan is to enable 802.11k in infrastructure.

NOTICE: For OpenScape WLAN Phone WL4, 802.11k should be enabled both in the infrastructure and the handsets.

[1] Channel 144 is slightly outside the specified band (5.710–5.730 GHz).

[2] In some countries the following rules apply for the UNII-2e band:

- Devices will not transmit on channels that 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 can be found in the FCC document “443999 D01 Approval of DFS UNII Devices v01r04”.

When 802.11k is used, each AP holds a list of the channels used by its neighbors, and sends this list to newly associated clients. Then the handset only needs to scan the channels present in the latest received Neighbor List when trying to roam from an AP. In this setup, a full scan of all channels is performed only if the OpenScape WL4 handset has failed to find a roaming candidate in the Neighbor List.

It is of vital importance for the roaming performance that the APs deliver a good-quality Neighbor List when 802.11k is used.

Similar functionality is achieved with the part in 802.11v standard called BSS Transition Management. With this functionality the handset asks the AP for the best roaming candidates and scans in a similar way to when receiving a neighbor list.

NOTICE: OpenScape WLAN Phone WL4 does not currently support 802.11v.

Use the standard 802.11k(v) together with 802.11r fast roaming to ensure the fastest roaming.

To improve the performance of the occasional full scans, take into account the following configuration guidelines:

- The amount of channels enabled on the handset should be minimized to the channels that are used in the WLAN system. Based on the used product, see the Configuration Manual, OpenScape WLAN Phone WL4 to get the details on how to limit the amount of channels.
- The amount of channels enabled in the WLAN system should be minimized.

If 802.11k(v) is enabled, following these guidelines increases handset and network performance.

If 802.11k(v) is not used, it is highly recommended to follow these guidelines.

Wired LAN and Backbone Requirements

Quality of Service 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 packet-based priority by the Stations (STAs) should be used. Each packet is 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 determines what Access Category (AC) will handle the frame.

Four ACs are defined in the WMM specification:

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

WMM maps the UP 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 Real-time Transport Protocol (RTP) frames.
- SIP signalling DSCP value (0x1A (26), Assured Forwarding 31 for both handset types).

IEEE 802.11 Priority Field

The 802.11 UP is sent using the 2-bit QoS Control Field in the 802.11 Medium Access Control (MAC) header.

IEEE 802.1q Priority Field

The structure of the VLAN tag defined in 802.1Q is illustrated in Figure 1: Structure of a VLAN Tag on page 10.

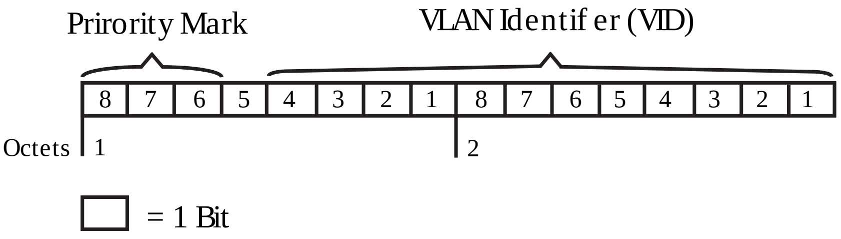


Figure 1: Structure of a VLAN Tag

NOTICE: 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 Type of Service (ToS) Field for both the DSCP (new standard) value and IP Precedence (old standard) is illustrated in the Figure 2: Diffserv Redefinition of ToS Field on page 11.

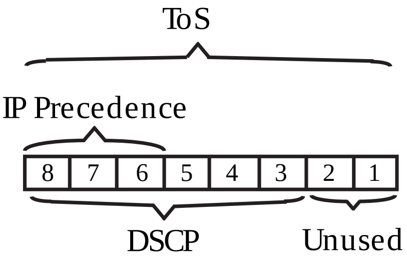


Figure 2: Diffserv Redefinition of ToS Field

NOTICE: The 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 Quality of Service

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.

End-to-End QoS for voice traffic guarantees that high load on a part of the network does not cause delays for the voice packets which would cause short disruptions/delays in the voice call. Other types of data traffic can handle the delays in a graceful way and while the traffic will go slower, it would not significantly affect the user experience. Hence, for other data traffic than voice, assuming default QoS classification and delivery in the network as “best effort”, there is no requirement of End-to-End QoS.

Uplink : Handset to Access Point

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 preserves the 802.1D user priority by copying the value into the 802.1p priority tag. The IP DSCP value is unaffected by the transition to the wired network.

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

NOTICE: 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 does not accept such a frame because the frame is not a standard Ethernet frame.

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

Downlink : Access Point 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 Differentiated Services Code Point (DSCP). In the AP, a rule can be created that maps 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, and so on.

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 are delivered to/ from the handset until the authentication is successfully completed.

It is recommended to use Wi-Fi Protected Access (WPA2). If WPA2 security is used together with 802.1X authentication, it is strongly recommended to use either 802.11r fast BSS transition (FT) or proactive key caching (also called opportunistic key caching). These features are supported by the handset and enable the reuse of an existing PMKSA (Pairwise Master Key Security Association) when roaming between APs. Roaming and handover times are reduced significantly since only fresh session encryption keys need to be exchanged by the 4-way handshake.

When either WPA2-PSK, Opportunistic key caching or Fast BSS Transition is used, roaming during a voice call can often be made seamless.

- 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.

Basic Cell Planning

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

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

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

5 GHz

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 automatically adjusts the usage to the so-called regulatory domain.

NOTICE: 802.11d is not allowed in the US.

The 5 GHz band consists of several sets of channels listed in the table below. See also 5GHz Radar Protection in DFS Channels on page 7.

NOTICE: If using even wider 802.11ac channels, the number of available channels is further reduced.

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)

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

NOTICE: Using 40/80/160 MHz channels reduces the number of non-DFS channels. Make sure that all non-DFS channel are used before adding DFS channels.

Multi-cell System

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 on the radio of the handset. Other wireless analyzers can be used to provide additional assistance during a site survey.

To avoid short disruptions/delays in voice calls, the basic approach to cell planning is to have sufficient overlap between adjacent cells, see Figure 3: Cell overlap between adjacent cells on page 15. This is done in order to ensure that sufficient radio signal strength is present during a handover between the cells.

For other types of data traffic than voice, provided that there is adequate coverage, the cell planning can be a bit relaxed without affecting the user experience.

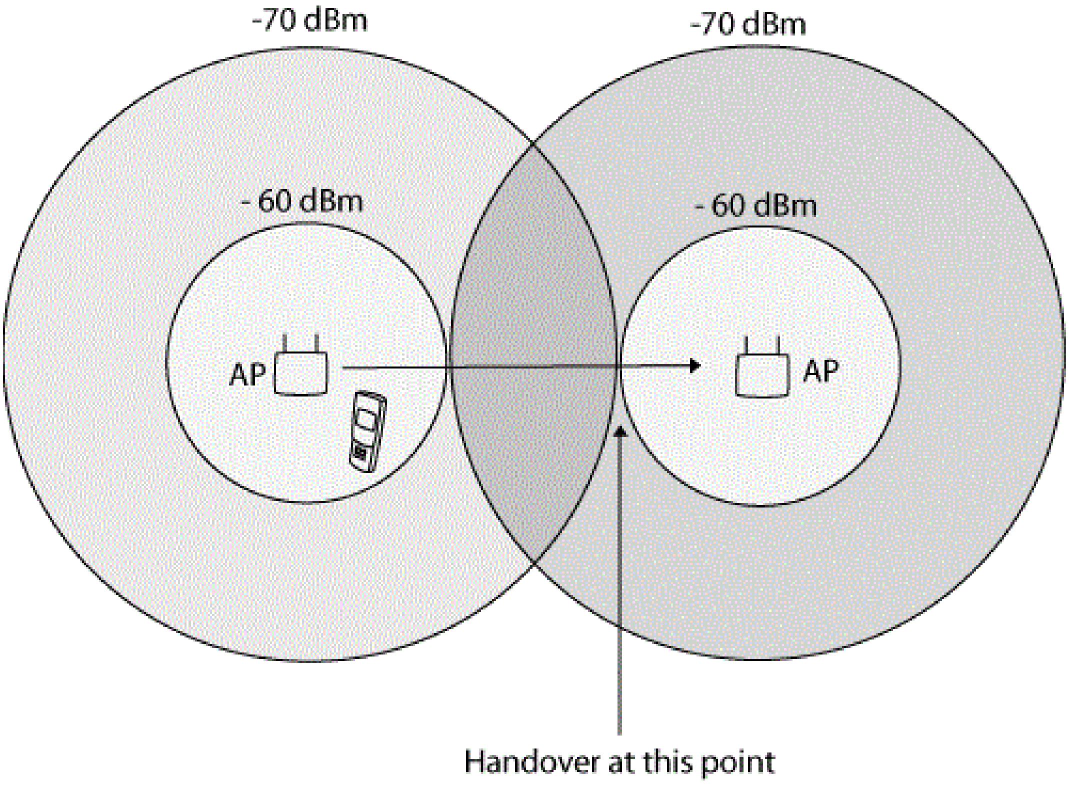


Figure 3: Cell overlap between adjacent cells

The distance between the APs is often a trade-off between the amount of APs and the 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 RF Signal Corruption in VoWiFi System on page 16.

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

NOTICE: The illustration in Figure 3: Cell overlap between adjacent cells on page 15 is valid when all APs’ transmission power are configured to 100 mW

(20 dBm). Since the Unify handset transmission power is pre-configured to approximately 100 mW, this ensures a symmetric wireless link.

The illustration also is valid for other transmission power settings.

Transmission Rate

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 rate spans only affect 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 takes longer.

As an 802.11 STA moves away from an AP, the Tx rate is lowered to increase the range. This has effects on the capacity in the cell. Since all STAs in a cell share 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 VoWiFi System

There are several causes of signal corruption in a VoWiF 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 in 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 table below.

Table 1: Estimation of attenuation for different construction materials for -b/g radio

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

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

Co-Channel Interference

There are only three non-overlapping channels available in the 2.4 GHz band at 20 MHz that result in a high probability of channel reuse 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.

NOTICE: 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 is enough distance separation before the reuse of the same channel is needed. For a multi-storey building with a large floor area, it is 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 share the RF channel as if they were present in one cell.

2) Error introduction. The STAs introduce transmission errors due to the “hidden node problem” described in Hidden Node Problem on page 19.

Clear Channel Assessment

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 an 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.

Clear Channel Assessment (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 Figure 4: CCA might cause problems even for far away STAs on page 19.

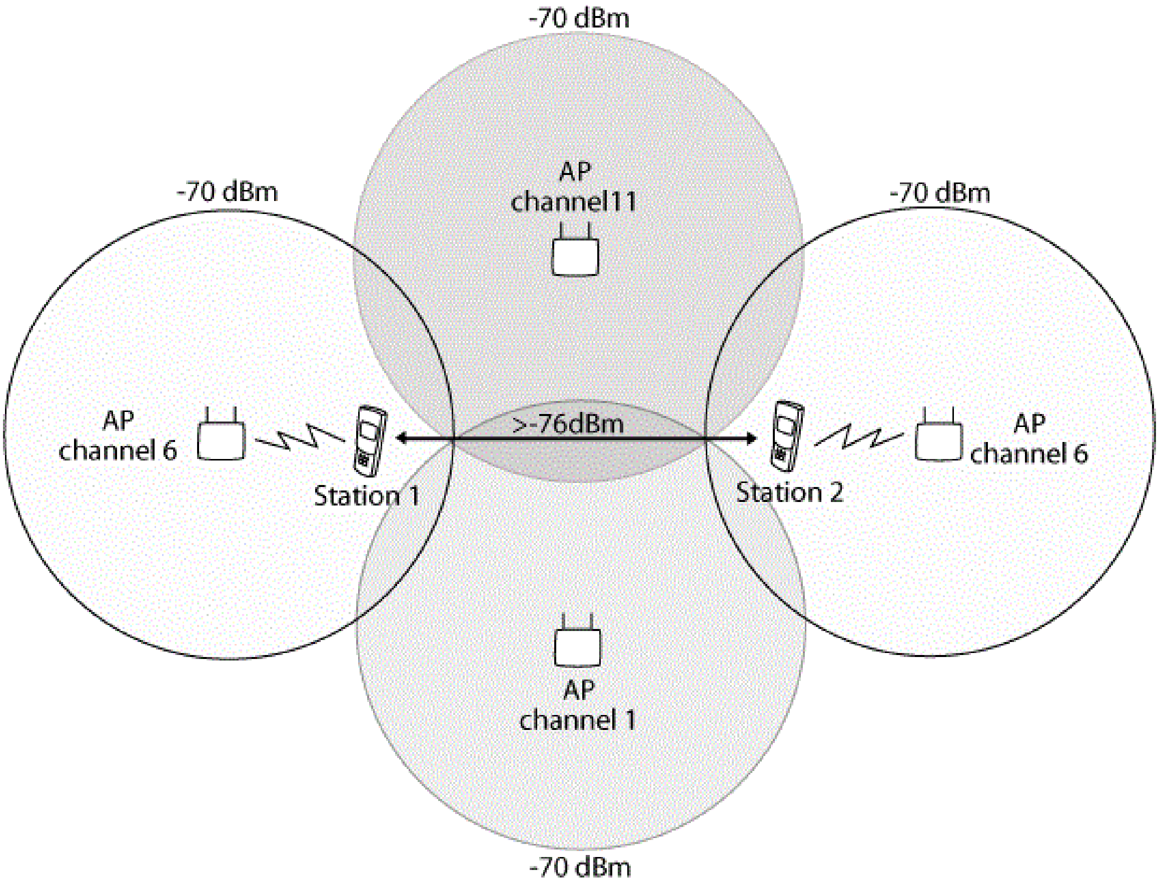


Figure 4: CCA might cause problems even for far away STAs

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 affects 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, and automation.

Hidden Node Problem

The “Listen before Talk” mechanism, mentioned in Clear Channel Assessment on page 18, 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.

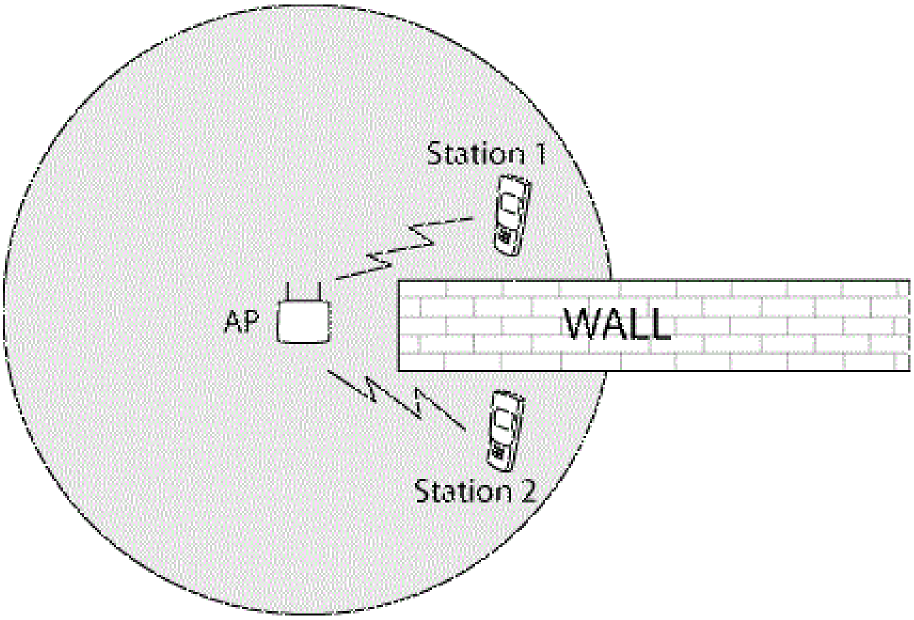


Figure 5: STAs and an AP showing simultaneous transmission and collision

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” reduces the performance.

As described in Basic Cell Planning on page 14, enough overlap between adjacent cells is needed to have sufficient radio signal strength at all places and enough margin when roaming between cells. However, the co-channel interference problem, described in Co-Channel Interference on page 18, 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 Clear Channel Assessment on page 18. The CCA does 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 requires 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 Figure 6: Recommended placement of AP to receive coverage around corners on page 21.

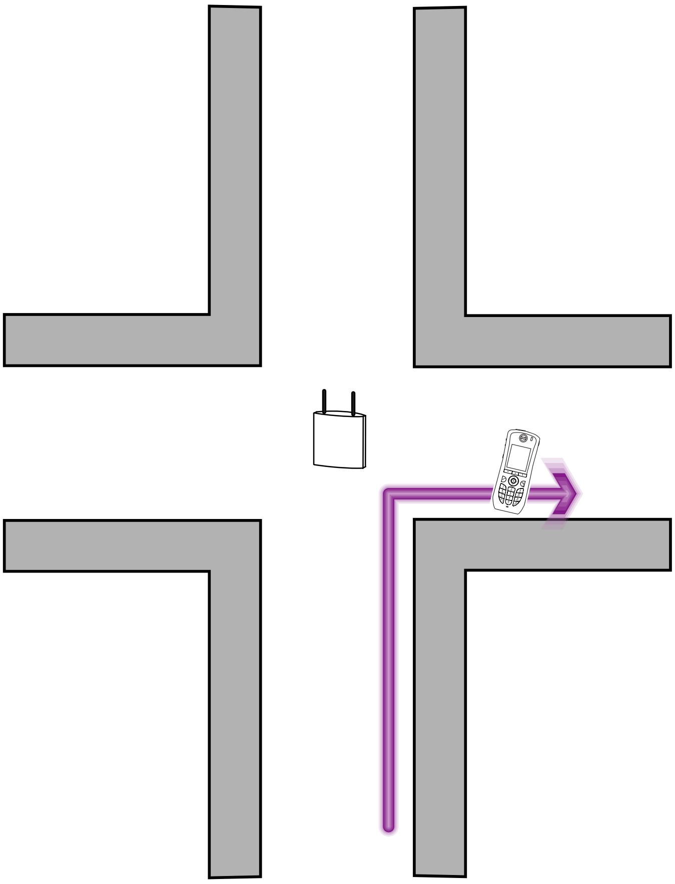


Figure 6: Recommended placement of AP to receive coverage around corners

In a building with thick walls APs may need 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 Figure 7: Recommended placement of AP to reduce roaming between APs in separate rooms on page 22. If too many APs are placed in the corridor, the roaming problem is just moved to the corridor APs.

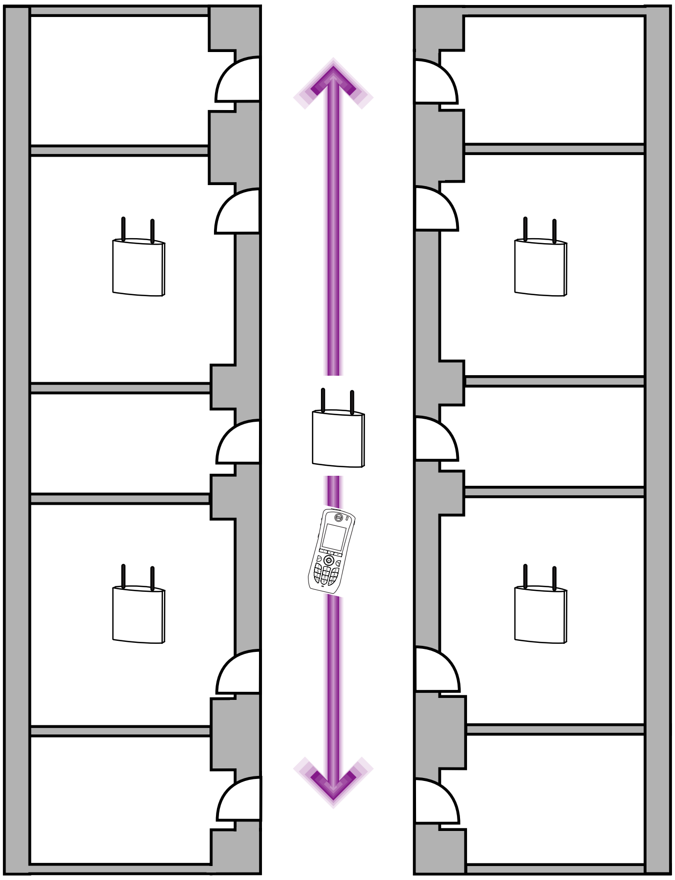


Figure 7: Recommended placement of AP to reduce roaming between APs in separate rooms

Conflicting Interests with RTLS Placement

Many infrastructure vendors recommend another approach when placing AP for optimal Wi-Fi-based localization. Since it is easier to determine the position of a device when the AP and signal strength combination is unique at any place, APs are often placed in rooms instead of corridors and at the perimeter of a floor plan instead of the center.

Such placement conflicts with the ones described earlier in this chapter where it becomes beneficial to have larger areas where people’s moves are covered by as few as possible APs.

Infrastructure Dependant Features

This chapter includes information on tools and features dependant on the WLAN infrastructure.

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, very frequent dynamic changes (that happen multiple times per day) 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, dropped calls.

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

Load Balancing

Some WLAN infrastructures have an automatic load balancing feature. The purpose is to dynamically move stations between APs to avoid overload and to spread the load. The move of the stations is done by forcing them to connect to another AP than the current one.This forced transition causes a loss of speech frames and, in worst case, the call is disconnected.

OpenScape WLAN Phone WL4

OpenScape WLAN Phone WL4 does not support any procedure for a smooth transition of stations between APs. Instead, the move is done by deauthenticating the handset until it associates to another AP.

Regulatory Domain - 802.11d

NOTICE: 802.11d is not allowed in the US.

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

At start-up, the handset is passively listening for information about which regulatory domain is present before making any transmissions. To ensure that the local frequency rules are not violated, the recommendation is to enable the use of 802.11d.

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.

Related Documents

OpenScape WLAN Phone WL4 VoWiFi System Migration Guide

Configuration Manual, OpenScape WLAN Phone WL4

Migration

This section illustrates differences and features that should be taken into consideration when introducing new products to an existing network consisting of other Unify products. To get the specific details on migration from WL3 to OpenScape WLAN Phone WL4, see the OpenScape WLAN Phone WL4 VoWiFi System Migration Guide.

Interoperability OpenScape WLAN Phone WL4

WLAN

The OpenScape WLAN Phone WL4 supports 802.11ac/WiFi 5. Since 802.11ax/WiFi 6 is backwards compatible with WiFi 5, the handset can coexist in a WiFi 6 environment. The relatively low bandwidth requirements and high mobility of a VoIP handset means that the benefit of actually using WiFi 6 in the handset would be limited.

Client Behavior Experience

A WLAN designer and installer must know how a specific client behaves in different types of environments. By building on experience from installations done previously it is possible for a skilled technician to estimate the performance of a client at a new site.

If a site is using mixed clients of the same type, like for example two brands or series of VoWiFi phones, their performance in different environment must be fully understood.

Each client has it its own design depending on what components are used, for example antenna design, firmware and device drivers, power levels, housing and more.

This could mean that a WLAN where a specific type of Wi-Fi phone works with sufficient performance can have other handsets connected with different levels of voice quality.

Replacing Handsets: Test and Evaluation Considerations

If the decision is to forklift the handset installation and replace all WL3 handsets with OpenScape WLAN Phone WL4, the project must be considered as a new installation, and several issues should be taken in consideration:

- Despite the fact that all Unify products can be deployed in the same network system, it is still recommended to perform a test before deploying, for example OpenScape WLAN Phone WL4 in an environment with WL3 handsets.
- Perform a walk-through test while in call mode to estimate the voice quality and the roaming behavior.
- The deployer should also carefully test that the VoIP and WLAN protocols work as expected. Shortly said, there may always be some incapability at a site due to the complexity of the installation.
- A WLAN site survey should be performed as the radio chip set in WL3 differs from the ones in OpenScape WLAN Phone WL4.
- Features like the use of certificates, base lining and license handling require an update of the software.

Typically there are three things that should be evaluated using the tools in the handset:

- Roaming candidates.
- Roaming performance (where and when roaming occurs).

- Voice quality in walk and talk test.

This can be done by measurement only, and of course by listening to real calls.